SEMINAR 1

Problema 1. Să se determine mulţimile X, Y a.î.

(i) $X \cup Y = \{1,2,3,4,5,6,7,8,9\}$, (ii) $X \cap Y = \{4,6,9\}$, (iii) $X \cup \{3,4,5\} = \{1,3,4,5,6,8,9\}$, (iv) $Y \cup \{2,4,8\} = \{2,4,5,6,7,8,9\}$.

Soluţie: Din (ii) avem $\{4,6,9\} \subset X, Y$. Trebuie să vedem care sunt elementele ce trebuiesc adăugate la mulţimea $\{4,6,9\}$ pentru a fi îndeplinite condiţiile condiţiile (iii) şi (iv).

$$\underbrace{X \cap Y = \{4,6,9\}}$$
$$\underbrace{X \cup \{3,5\}}_{\{1,3,4,5,6,8,9\}} \qquad \underbrace{Y \cup \{2,8\}}_{\{2,4,5,6,7,8,9\}} \qquad \text{4 este în } X \text{ şi } Y$$

Obţinem $X = \{1,4,6,8,9\}$ şi $Y = \{4,5,6,7,9\}$. Vedem că acestea verifică toate condiţiile.

Problema 2. Fie funcţia $f : \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}, f(x,y) = x^2 - y^2$. Arătaţi că $\mathrm{Im}(f) = \mathbb{Z}\backslash\{4k+2 | k \in \mathbb{Z}\}$.

Cu $\mathrm{Im}(f)$ am notat imaginea funcţiei f. $\mathrm{Im}(f) = \{z \in \mathbb{Z} \mid (\exists)(x,y) \in \mathbb{Z}\times\mathbb{Z}$ a. î. f(x, y) = z$\}$.

Soluţie: Notăm clasele de resturi modulo 4 cu: $\hat{0} = \{4k \mid k \in \mathbb{Z}\}$, $\hat{1} = \{4k+1 \mid k \in \mathbb{Z}\}$, $\hat{2} = \{4k+2 \mid k \in \mathbb{Z}\}$, $\hat{3} = \{4k+3 \mid k \in \mathbb{Z}\}$. După cum se ştie din clasa a XII-a acestea se pot aduna şi înmulţi. Astfel avem $\hat{0}^2 = \hat{0}$, $\hat{1}^2 = \hat{1}$, $\hat{2}^2 = \hat{0}$, $\hat{3}^2 = \hat{1}$. De exemplu considerăm $(4k+3) \in \hat{3}$. $(4k+3)^2 = 16k^2 + 24k + 9 = 4(4k^2+6k+2)+1 \in \hat{1}$. Deci pentru $x \in \mathbb{Z} \Rightarrow \hat{x}^2 \in \{\hat{0}, \hat{1}\}$. Pentru $x, y \in \mathbb{Z}$ avem $x^2 - y^2 \in \{\hat{0}, \hat{1}, \widehat{-1} = \hat{3}\}$. Acest calcul arată că $\nexists z \in \mathbb{Z}$. a.î. $z^2 \in \hat{2}$. Deci avem incluziunea "$\subseteq$".

"$\supseteq$": Pentru numerele de tipul $4k, 4k+1, 4k+3, k \in \mathbb{Z}$ arătăm că sunt diferenţe de pătrate de numere întregi.

$4k = (k+1)^2 - (k-1)^2 = (k+1+k-1)(k+1-k+1) = 2k \cdot 2 = 4k$

$4k+1 = (2k+1)^2 - (2k)^2$ şi $4k+3 = (2k+2)^2 - (2k+1)^2$

Problema 3. Fie funcţia $f : \longrightarrow \mathbb{R}, f(x,y) = (x-\sqrt{2})^2 + (y - \frac{1}{3})^2$. Arătaţi că f este injectivă. ($\mathbb{Z}^2 = \mathbb{Z}\times\mathbb{Z}$.)

Soluţie: $f(x,y)$ este pătratul distanţei în plan de la (x,y) la $(\sqrt{2}, \frac{1}{3}) = \omega$. Din definiţie f este injectivă $\Leftrightarrow [(\forall)(x,y) \neq (x',y') \in \mathbb{Z}^2 \Rightarrow f(x,y) \neq f(x',y')$.

Fie $f(x,y) = f(x',y') \Leftrightarrow (x-\sqrt{2})^2 + (y-\frac{1}{3})^2 = (x'-\sqrt{2})^2 + (y'-\frac{1}{3})^2$. Desfacem pătratele, reducem termenii asemenea şi obţinem

$$x^2 - x'^2 + y^2 - y'^2 - \frac{2}{3}(y-y') = 2\sqrt{2}(x-x')$$

.

Ştim că $x, y, x', y' \in \mathbb{Z}$. Dacă $x \neq x'$ atunci $\sqrt{2} = \frac{x^2-x'^2+y^2-y'^2-\frac{2}{3}(y-y')}{2(x-x')} \in \mathbb{Q}$, ceea ce este absurd. Deci $x = x'$. Egalitatea devine $y^2 - y'^2 - \frac{2}{3}(y-y') = 0 \Leftrightarrow (y-y')(y+y'-\frac{2}{3}) = 0$. Dacă $y \neq y'$ atunci $y + y' = \frac{2}{3} \in \mathbb{Z}$, ceea ce este o contradinţie. Deci avem şi $y = y'$. Am obţinut: $f(x,y) = f(x',y') \Rightarrow (x,y) = (x',y')$, adică f este injectivă.

Problema 4. Considerăm funţia $f : \mathcal{P}(\{1,2,3,4\}) \longrightarrow \mathcal{P}(\{1,2\}) \times \mathcal{P}(\{1,3\})$, definită prin $f(A) = (A \cap \{1,2\}, A \cap \{1,3\})$. Să se expliciteze f şi să se verifice dacă este injectivă sau surjectivă.

Soluţie: $|\mathcal{P}(\{1,2,3,4\})| = 2^4$. În general numărul submulţimilor mulţimii $[n] = \{1,2,\dots,n\}$ este 2^n. Deci numărul elementelor mulţimii $\mathcal{P}(\{1,2\}) \times \mathcal{P}(\{1,3\})$ este $2^2 \cdot 2^2 = 2^4 = 16$.

De exemplu $f(\varnothing) = (\varnothing,\varnothing) = f(\{4\})$, $f(\{1\}) = (\{1\},\{1\}) = f(\{1,4\})$. Deci f nu este injectivă. Cum f o funcţie între mulţimi de acelaşi cardinal şi f nu este injectivă, atunci nu poate fi nici surjectivă.

De exemplu $(\{1\},\varnothing) \notin \mathrm{Im}(f)$. $\{1\}$ pe prima componentă se obţine din intersecţia mulţimii $\{1,2\}$ cu $\{1\}$, $\{1,3\}$, $\{1,4\}$ sau cu $\{1,3,4\}$. Dar pe a două poziţie avem intersecţia dintre $\{1,3\}$ şi una dintre aceste mulţimi iar această intersecţie este diferită de $\varnothing$. Similar$(\varnothing,\{1\}) \notin \mathrm{Im}(f)$.

Problema 5. Fie $a,b \in \mathbb{N}^\star$, $A = [a] = \{1,2,\dots,a\}$, $B = [b] = \{1,2,\dots,b\}$. Arătaţi că:
(i) Numărul funcţiilor $f : A \longrightarrow B$ este b^a.
(ii) Dacă $a \leqslant b$, numărul funcţiilor injective $A \longrightarrow B$ este $\frac{b!}{(b-a)!}$.
(iii) Numărul funcţiilor strict crescătoare $A \longrightarrow B$ este $C_b^a = \binom{b}{a}$.
(iv) Numărul funcţiilor crescătoare $A \longrightarrow B$ este $C_{a+b-1}^a = \binom{a+b-1}{a}$.
Soluţie:
(i) Pentru $(\forall)\ j \in [a]$, $f(j) \in [b]$. Deci $f(j)$ poate lua oricare dintre cele b valori. O funcţie între două mulţimi finite este caracterizată de mulţimea valorilor sale, adică de imagine, care în acest caz este $f(1), f(2),\dots,f(a)$, sau fără virgule $f(1)f(2)\dots f(a)$. Deci fiecare funcţie de la A la B poate fi gândită ca un cuvânt de lungime a cu litere în alfabetul $[b]$. Astfel numărul funcţiilor de la A la B este egal cu numărul cuvintelor de lungime a cu litere în alfabetul $[b]$. Cum fiecare literă a cuvântului poate lua b valori, numărul acestor cuvinte este b^a, care este şi numărul tuturor funcţiilor de la A la B.

(ii) Funcţiile injective $f : A \longrightarrow B$ se identifică cu acele cuvinte lungime a cu litere distincte în alfabetul $[b]$. Deci prima literă poate lua b valori, dar odatfixată această literă următoarea literă poate fi oricare dintre cele b elemente, mai puţin cea aleasă pe prima poziţie, deci pentru a doua poziţie avem la dispoziţie $b-1$ alegeri. Similar, pentru a treia poziţie, odată fixate valorile primelor două poziţii, vom avea $b-2$ alegeri. În sfârşit pentru ultima vom avea $b-a+1$ alegeri. Deci mulţimea funcţiilor injective $f : A \longrightarrow B$ este $b(b-1)(b-2)\dots(b-a+1) = \frac{b!}{(b-a)!}$.

(iii) Fie $f : A \longrightarrow B$, f strict crescătoare $\Leftrightarrow 1 \leqslant f(1) = x_1 < f(2) = x_2 < \dots < f(a) = x_a \leqslant b$. Deci a da o funcţie strict crescătoare de la A la $B \Leftrightarrow$ a da un şir de elemente $1 \leqslant x_1 < x_2 < \dots x_a \leqslant b \Leftrightarrow$ a da o submulţime cu a elemente a lui B. Numărul acestor submulţimi, prin definiţie este C_b^a, în notaţie anglo-americană $\binom{b}{a}$.

(iv) Fie $f : A \longrightarrow B$, f crescătoare. Imaginea unei astfel de funcţii este $1 \leqslant f(1) = x_1 \leqslant f(2) = x_2 \leqslant \dots \leqslant f(a) = x_a \leqslant b \Leftrightarrow 1 \leqslant x_1 < x_2 + 1 < x_3 + 2 < \dots x_a + a - 1 \leqslant b + a - 1$. Deci a da o funcţie crescătoare este echivalent cu a da o submulţime de cardinal a din mulţimea $\{1,2,\dots,b+a-1\}$. Numărul acestor submulţimi este prin definiţie $C_{b+a-1}^a = \binom{b+a-1}{a}$.

Problema 6. (Principiul includerii-excluderii) Pentru orice mulţime finită X notăm cu $|X|$ cardinalul acesteia, adică numărul de elemente. Fie $A_1,\dots,A_n$ mulţimi finite. Atunci

$$|\bigcup_{i=1}^n A_i| = \sum_{K \subset [n]} (-1)^{|K|+1} |\bigcap_{i \in K} A_i|.$$

Pentru $n = 2$, avem formula binecunoscută $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$.
Soluţie: Pentru $n = 2$ formula de mai sus se demonstrază uşor şi foarte intuitiv cu diagrame Venn. De fapt, orice element din $A_1 \cup A_2$ este sau din A_1 sau din A_2, cele din intersecţia $A_1 \cap A_2$ fiind numărate şi în A_1 şi în A_2. Deci trebuie să le scădem o dată.

Se face inducţie după n. Să demonstrăm $P2 \longrightarrow P3$: Avem trei mulţimi finite, A_1, A_2, A_3 şi vom considera $A_1 \cup A_2$ o mulţime şi A_3 a doua mulţime. APlicăm $P2$. Deci

$$|A_1 \cup A_2 \cup A_3| = |(A_1 \cup A_2) \cup A_3| = |A_1 \cup A_2| + |A_3| - |(A_1 \cup A_2) \cap A_3|, \text{folosind } P2 \text{ obţinem} =$$
$$= |A_1| + |A_2| - |A_1 \cap A_2| + |A_3| - |(A_1 \cap A_3) \cup (A_2 \cap A_3)| =$$
$$= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

Temă Demonstraţi $P3 \longrightarrow P4$ şi $Pn \longrightarrow P(n+1)$.

Problema 7. Să se determine numărul funţiilor surjective $[k] \longrightarrow [n]$, unde $k \geqslant n$.

Soluţie: Numărul funcţiilor surjective este n^k minus numărul funcţiilor ce nu sunt surjective. O funcţie $f : [k] \longrightarrow [n]$ dacă există cel puţin $i \in [n]$ a.î. $i \notin \mathrm{Im}(f)$.

Notăm cu $N_i = \{f : [k] \longrightarrow [n] | i \notin \mathrm{Im}(f)\}$. Funcţiile ce nu sunt surjective sunt cele din $\bigcup_{i=1}^n N_i$, iar numărul acestora, folosind principiul includerii-excluderii este $|\bigcup_{i=1}^n N_i| = \sum_{K \subset [n]} (-1)^{|K|+1} |\bigcap_{i \in K} N_i|$. $|N_i| = (n-1)^k$, pentru că N_i este mulţimea funcţiilor de la mulţimea $[k]$ la mulţimea $[n] \backslash \{i\}$ de cardinal $n-1$. Similar pentru o mulţime de indici $K \subset [n]$, de cardinal p, avem avem $|\bigcap_{i \in K} N_i| = (n-p)^k$.

Deci numărul funcţiilor surjective este $n^k - |\bigcup_{i=1}^n N_i| = n^k - \sum_{K \subset [n]} (-1)^{|K|+1} |\bigcap_{i \in K} N_i| = n^k + \sum_{K \subset [n]} (-1)^{|K|} |\bigcap_{i \in K} N_i| = n^k + \sum_{p=1, K \subset [n], |K|=p}^n (-1)^{|K|} |\bigcap_{i \in K} N_i| = n^k + \sum_{p=1}^n (-1)^p C_n^p (n-p)^k = n^k - C_n^1 (n-1)^k + C_n^2 (n-2)^k - \ldots (-1)^{n-1} C_n^{n-1} 1^k$.

SEMINAR 2

Problema 1. Fie mulţimile $A = \{1, 2, 3, 4\}, B = \{a, b, c, d\}$ şi funcţia $f : A \longrightarrow B$ dată prin

$$1 \mapsto a, 2 \mapsto b, 3 \mapsto c, 4 \mapsto d$$

Pentru orice $X \subset A$ şi orice $Y \subset B$, calculaţi $f(X)$ şi respectiv $f^{-1}(Y)$.

Soluţie: Submulţimile mulţimii A sunt în număr de $2^4 = 16$. Acestea sunt $\varnothing, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}\{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}$.

Imaginea directă a acestor mulţimi este $f(\varnothing) = \varnothing, f(\{1\}) = \{a\}, f(\{2\}) = \{b\}, f(\{3\}) = \{c\}, f(\{4\}) = \{d\}, f(\{1, 2\}) = \{a, b\}, f(\{1, 3\}) = \{a, c\}, f(\{1, 4\}) = \{a, d\}, f(\{2, 3\}) = \{b, c\}$, $f(\{2, 4\}) = \{b, d\}, f(\{3, 4\}) = \{c, d\}, f(\{1, 2, 3\}) = \{a, b, c\}, f(\{1, 2, 4\}) = \{a, b, d\}$, $f(\{1, 3, 4\}) = \{a, c, d\}, f(\{2, 3, 4\}) = \{b, c, d\}, f(\{1, 2, 3, 4\}) = \{a, b, c, d\}$.

Imaginile inverse ale submulţimilor mulţimii $\{a, b, c, d\}$ sunt

$f^{-1}(\varnothing) = \varnothing, f^{-1}(\{a\}) = \{1\}, f^{-1}(\{b\}) = \{2\}, f^{-1}(\{c\}) = \{3\}, f^{-1}(\{d\}) = \{4\}, f^{-1}(\{a, b\}) = \{1, 2\}, f^{-1}(\{a, c\}) = \{1, 3\}, f^{-1}(\{a, d\}) = \{1, 4\}, f^{-1}(\{b, c\}) = \{2, 3\}, f^{-1}(\{b, d\}) = \{2, 4\}$, $f^{-1}(\{c, d\}) = \{3, 4\}, f^{-1}(\{a, b, c\}) = \{1, 2, 3\}, f^{-1}(\{a, b, d\}) = \{1, 2, 4\}, f^{-1}(\{a, c, d\}) = \{1, 3, 4\}$, $f^{-1}(\{b, c, d\}) = \{2, 3, 4\}), f^{-1}(\{a, b, c, d\}) = \{1, 2, 3, 4\}$.

Problema 2. Pentru orice mulţimi X, Y notăm cu $H(X, Y)$ mulţimea funcţiilor de la X la Y. Fie A, B, C trei mulţimi nevide şi fie funcţia

$$\alpha : H(A, H(B, C)) \to H(A \times B, C)$$

definită prin $\alpha(f)(a, b) = f(a)(b)$ pentru orice $f \in H(A, H(B, C)), a \in A, b \in B$.
(i) Arătaţi că α este bijectivă,
(ii) Explicitaţi $\alpha(f)$ pentru $f \in H(\{1, 2, 3\}, H(\{4, 5, 6\}, \{a, b, c, d\}))$, dată prin
$f(1) = \begin{pmatrix} 4 & 5 & 6 \\ a & b & d \end{pmatrix}$, $f(2) = \begin{pmatrix} 4 & 5 & 6 \\ b & a & c \end{pmatrix}$, $f(3) = \begin{pmatrix} 4 & 5 & 6 \\ c & c & a \end{pmatrix}$.

Soluţie:
(i) Fie $f, g \in H(A, H(B, C))$, a.î. $\alpha(f) = \alpha(g) \Leftrightarrow (\forall)(a, b) \in A \times B, \quad \alpha(f)(a, b) = \alpha(g)(a, b) \Leftrightarrow f(a)(b) = g(a)(b)$, egaltate valabilă pentru orice $b \in B \Rightarrow f(a) = g(a)$, egalitate valabilă pentru orice $a \in A \Rightarrow f = g$. Deci α este injectivă.

Considerăm o funcţie $F : A \times B \longrightarrow C$. Definim $f : A \longrightarrow H(B, C)$ prin $f(a)(b) := F(a, b)$. Prin definiţia lui f, avem $\alpha(f) = F$. Deci α este surjectivă.
(ii) $\alpha(f)(1, 4) = f(1)(4) = a, \alpha(f)(1, 5) = f(1)(5) = b, \alpha(f)(1, 6) = f(1)(6) = d, \alpha(f)(2, 4) = f(2)(4) = b, \alpha(f)(2, 5) = f(2)(5) = a, \alpha(f)(2, 6) = f(2)(6) = c, \alpha(f)(3, 4) = f(3)(4) = c, \alpha(f)(3, 5) = f(3)(5) = c, \alpha(f)(3, 6) = f(3)(6) = a$.

Problema 3. Arătaţi că mulţimea $\mathbb{Q}$ a numerelor raţionale este numărabilă.

Soluţie: $\mathbb{Z}, \mathbb{N}$ sunt mulţimi numărabile. Folosind un rezultat din curs $\Rightarrow \mathbb{Z} \times \mathbb{N}^\star$ este numărabilă iar $\mathbb{Q}$ se identifică cu mulţimea claselor de echivalenţă $\mathbb{Z} \times \mathbb{N}^\star / \sim$, unde $(x, y) \sim (p, q) \Leftrightarrow xq = yp$. Deci $\mathbb{Q}$ este numărabilă.

Problema 4. Fie A o mulţime nevidă şi $f : \mathcal{P}(A) \longrightarrow A$ o funcţie. Notăm cu

$$B := A \backslash \{f(X) \mid X \subseteq A, f(X) \in X\}$$

(i) Arătaţi că există $D \in \mathcal{P}(A) \backslash \{B\}$ cu $f(D) = f(B)$.
(ii) Găsiţi un D în cazul $A = \{1, 2, 3\}$ şi

$$f = \begin{pmatrix} \varnothing & \{1\} & \{2\} & \{3\} & \{1,2\} & \{1,3\} & \{2,3\} & \{1,2,3\} \\ 1 & 2 & 3 & 1 & 3 & 2 & 1 & 1 \end{pmatrix}$$

Soluţie: (i) Fie $f(B) = b$. Dacă $b \in B$, atunci $f(B) = b \notin B$. O contradicţie.

Deci $b \notin B \Leftrightarrow (\exists) D \subset A$ a.î. $f(D) = b \in D$. $D \neq B$ pentru că $b \in D \backslash B$ şi $f(D) = f(B)$.

Rezultă că nu există funcţii injective de la mulţimea părţilor unei mulţimi $\mathcal{P}(A)$, la mulţimea nevidă A.

(ii) Pentru exemplul dat $\{f(X) \mid X \subseteq A, f(X) \in X\} = \{1\}$, $(X = A)$ iar $B = A \backslash \{1\} = \{2, 3\}$. $f(\varnothing) = f(\{3\}) = f(A) = f(B) = 1$. Avem deci în acest caz trei exemple de mulţimi $D \neq B$ pentru care $f(D) = f(B)$.

Problema 5. Fie A, B, C trei mulţimi. Arătaţi că $A\Delta(B\Delta C) = (A\Delta B)\Delta C$ unde $X\Delta Y = (X \backslash Y) \cup (Y \backslash X)$ este diferenţa simetrică a mulţimilor X, Y.

Soluţie: $A\Delta(B\Delta C) = A\Delta B\Delta C = (A\Delta B)\Delta C$ este reprezentată în figura de mai jos de regiunea colorată cu albastru.

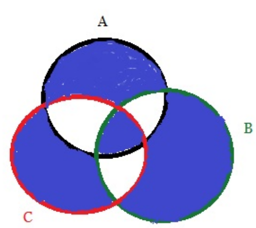


Figura 1: $A\Delta B\Delta C$

SEMINAR 3

Problema 1. Fie $n \geqslant 1$ şi notăm cu $\varphi(n)$ numărul întregilor pozitivi $\leqslant n$ primi cu n (funcţia φ *se numeşte indicatorul lui Euler*). Să se arate că

$$\varphi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_s})$$

unde $p_1, p_2, \dots p_s$ sunt factorii primi ai lui n.

Soluţie: Un număr prim cu n este un număr k pentru care cel mai mare divizor comun (c. m. m. d. c.) al numerelor n şi k este 1. Notaţia consacrată pentru c.m.m.d.c.$\{n, k\}$ este (n, k).

Considerăm descompunerea în factori primi ai lui $n = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s}$.

Pentru fiecare $1 \leqslant j \leqslant s$ notăm cu $A_j = \{1 \leqslant k \leqslant n \mid p_j | k\}$ muţimea numerelor naturale cel mult egale cu n ce se divid cu p_j .

Dorim să calculăm numărul elementelor mulţimii $A_1 \cup A_2 \cup \dots \cup A_n$. Numărul căutat este cardinalul complementarei acestei mulţimi, deci $\varphi(n) = n - |A_1 \cup A_2 \cup \dots A_n|$.

Pentru calculul $|A_1 \cup A_2 \cup \dots A_n|$ folosim principiul includerii-excluderii şi avem

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{L \subset [s]} (-1)^{|L|+1} | \cap_{i \in L} A_i|$$

Avem $A_j = \{p_j \cdot 1, p_j \cdot 2, p_j \cdot \frac{n}{p_j}\}$. Deci $|A_j| = \frac{n}{p_j}$.

$A_{i_1} \cap A_{i_2} = \{1 \leqslant k \leqslant n \mid p_{i_1} | k$ şi $p_{i_2} | k\}$ şi $|A_{i_1} \cap A_{i_2}| = \frac{n}{p_{i_1} p_{i_2}}$.

Similar pentru mulţimea de indici $L = \{i_1, i_2, \dots, i_l\}$, avem
$A_{i_1} \cap \dots \cap A_{i_l} = \{1 \leqslant k \leqslant n \mid p_{i_1} | k \ , \dots \ , \ p_{i_l} | k\}$ ce are cardinalul $|A_{i_1} \cap \dots \cap A_{i_l}| = \frac{n}{p_{i_1} \cdots p_{i_l}}$.

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{i=1}^{s} (-1)^2 |A_i| + \sum_{1 \leqslant i_1 < i_2 \leqslant s} (-1)^3 |A_{i_1} \cap A_{i_2}| + \dots + \sum_{1 \leqslant i_1 < \dots < i_l \leqslant s} (-1)^{l+1} |A_{i_1} \cap \dots \cap A_{i_l}| +$$
$$+ (-1)^{s+1} |A_1 \cap A_2 \cap \dots A_s| =$$

$$= \sum_{i=1}^{s} \frac{n}{p_i} - \sum_{1 \leqslant i_1 < i_2 \leqslant s} \frac{n}{p_{i_1} p_{i_2}} + \dots + (-1)^{l+1} \frac{n}{p_{i_1} \dots p_{i_l}} + (-1)^{s+1} \frac{n}{p_{i_1} \dots p_{i_s}}.$$

Deci $\varphi(n) = n - |A_1 \cup A_2 \cup \dots \cup A_n|$. Dând factor comun pe n şi schimbând semnele în suma de mai sus obţinem

$$\varphi(n) = n(1 - \sum_{i=1}^{s} \frac{1}{p_i} + \sum_{1 \leqslant i_1 < i_2 \leqslant s} \frac{1}{p_{i_1} p_{i_2}} + \dots + (-1)^l \frac{1}{p_{i_1} \dots p_{i_l}} + (-1)^s \frac{1}{p_{i_1} \dots p_{i_s}}) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_s})$$

Problema 2. Arătaţi că numărul permutărilor fără puncte fixe ale mulţimii $[n]$ este

$$n!(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!})$$

.

Soluţie: Notăm cu $A_i = \{\sigma \mid \sigma(i) = i\}$ mulţimea tuturor permutărilor lui $[n]$ ce au pe i ca punct fix. Atunci $A_1 \cup A_2 \cup \ldots \cup A_n$ reprezintă toate permutările ce au puncte fixe. Trebuie să aflăm $|A_1 \cup A_2 \cup \ldots \cup A_n|$, iar numărul permutărilor fără puncte fixe este $n! - |A_1 \cup A_2 \cup \ldots \cup A_n|$, unde după cum bine se ştie numărul permutărilor este $n!$.

Folosim din nou principiul includerii-excluderii

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{K \subset [n]} (-1)^{|K|+1} | \cap_{i \in K} A_i|$$

Pentru $K = \{i_1, i_2, \ldots i_k\}$, avem $A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k} = \{\sigma \mid \sigma(i_j) = i_j, (\forall) 1 \leqslant j \leqslant k\} =$ $= \{\sigma : [n] \backslash K \longrightarrow [n] \backslash K \mid \sigma \text{ permutare}\}$. Deci $|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}| = (n-k)!$. Vedem că acest număr este acelaşi pentru toate mulţimile $K \subset [n]$ cu $|K| = k$. Avem $C_n^k = \binom{n}{k}$ submulţimi de cardinal k ale mulţimii $[n]$.

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{\substack{K \subset [n], \\ |K| = k}} | \cap_{i \in K} A_i| = \sum_{k=1}^{n} (-1)^{k+1} C_n^k \cdot (n-k)! =$$

$$= \sum_{k=1}^{n} (-1)^{k+1} \frac{n!}{k!(n-k)!)} \cdot (n-k)! = \sum_{k=1}^{n} (-1)^{k+1} \frac{n!}{k!} = n! \sum_{k=1}^{n} (-1)^{k+1} \frac{1}{k!}$$

Numărul permutărilor fără puncte fixe este $n! - \sum_{k=1}^{n} (-1)^{k+1} \frac{1}{k!} = n!(1 + \sum_{k=1}^{n} (-1)^{k+2} \frac{1}{k!}) =$

$$= n!(1 + \sum_{k=1}^{n} (-1)^{k} \frac{1}{k!}) = n!(\sum_{k=0}^{n} (-1)^{k} \frac{1}{k!}).$$

Problema 3. Folosind definiţia arătaţi că relaţia de congruenţă modulo n este relaţie de echivalenţă pe $\mathbb{Z}$.

Soluţie: Pentru un $n \in \mathbb{N}, n \geqslant 2$ definim $x \equiv y \pmod n \Leftrightarrow n \mid (x-y) \Leftrightarrow x - y = n \cdot k, k \in \mathbb{Z}$.
Arătăm că relaţia definită mai sus este reflexivă simetrică şi tranzitivă.

- Reflexivitatea: $x - x = 0 = n \cdot 0 \Rightarrow x \equiv x \pmod n$.
- Simetria: Fie $x \equiv y \pmod n \Leftrightarrow x - y = n \cdot k \Rightarrow y - x = n \cdot (-k)$. Cum $k \in \mathbb{Z} \Rightarrow (-k) \in \mathbb{Z}$. Deci $y \equiv x \pmod n$
- Tranzitivitatea: Fie $x \equiv y \pmod n$ şi Fie $y \equiv z \pmod n$, $x - y = n \cdot p, y - z = n \cdot q$ cu $p, q \in \mathbb{Z}$. Atunci $x - z = x - y + y - z = n \cdot (p + q)$ şi $p + q \in \mathbb{Z}$.

Problema 4. Considerăm relaţiile α şi β pe $\mathbb{R}$.
$x \alpha y$ dacă $x - y \in \mathbb{Z}$ dacă $x - y \in \mathbb{Z}$ şi $x \beta y$ dacă $|x - y| < 2$. Să se studieze care din aceste relaţii sunt relaţii de echivalenţă.

Soluţie:
Relaţia α:

- Reflexivitatea: $x - x = 0 \in \mathbb{Z} \Rightarrow x \alpha x$
- Simetria: dacă $x - y = k \in \mathbb{Z} \Rightarrow y - x = -(x - y) = -k \in \mathbb{Z}$. Deci $x \alpha y \Rightarrow y \alpha x$.
- Tranzitivitatea: dacă $x - y = p \in \mathbb{Z}$ şi $y - z = q \in \mathbb{Z}$, atunci $x - z = x - y + y - z = p + q \in \mathbb{Z}$. Deci $x \alpha y$ şi $y \alpha z \Rightarrow x \alpha z$.

Aşadar α este relaţie de echivalenţă.

Relaţia β:
• Reflexivitatea: $|x-x| = 0 < 2 \Rightarrow x\beta x$.
• Simetria: dacă $|x-y| < 2 \Rightarrow |-(y-x)| < 2 \Rightarrow |-1||(y-x)| < 2 \Rightarrow |y-x| < 2$, deci $x\beta y \Rightarrow y\beta x$.
• Tranzitivitatea: Relaţia β nu este tranzitivă: de exemplu $|0-1,3| = 1,3 < 2, |1,3-2,2| = 0,9 < 2$, dar $|0-2,2| = 2,2 > 2$.
Deci relaţia β nu este o relaţie de echivalenţă pe $\mathbb{R}$.

Problema 5. Să se studieze injectivitatea şi surjectivitatea funcţiei $f : \mathbb{R} \longrightarrow \mathbb{R}$ definită prin $f(x) = x^2 + 2x + 2$.

Soluţie: Vedem că $f(x) = (x+1)^2 + 1$.
• Injectivitatea: fie $x_1, x_2 \in \mathbb{R}$ a.î. $f(x_1) = f(x_2) \Leftrightarrow x_1^2+2x_1 = x_2^2+2x_2 \Leftrightarrow (x_1-x_2)(x_1+x_2+2) = 0 \Rightarrow x_1 = x_2$ sau $x_1 = -x_2-2$. Deci f nu este injectivă pentru că $f(-x-2) = f(x)$, şi $-x-2 \neq x, (\forall)x \in \mathbb{R}\backslash\{-1\}$.
• Surjectivitatea: trebuie să verificăm că pentru $(\forall)y \in \mathbb{R}, (\exists)x \in \mathbb{R}$ a.î. $f(x) = y \Leftrightarrow x^2 + 2x + 2 - y = 0$. Soluţiile sunt $x_{1,2} = -1 \pm \sqrt{1-(2-y)} = -1 \pm \sqrt{y-1}$. Vedem că dacă $y < 1$ atunci soluţiile $x_{1,2} \notin \mathbb{R}$.
Funcţia $f(x) = x^2+2x+2 = (x+1)^2+1$ este bijectivă dacă considerăm $f : [-1,\infty) \longrightarrow [1,\infty)$, iar inversa este $f^{-1} : [1,\infty) \longrightarrow [-1,\infty), f^{-1}(x) = -1+\sqrt{x-1}$. Verificaţi că $f \circ f^{-1} = \mathrm{id}_{[1,\infty)}$ şi $f^{-1} \circ f = \mathrm{id}_{[-1,\infty)}$

Problema 6. Studiaţi dacă funţia $f : \mathbb{R} \longrightarrow \mathbb{R}, f(x) = \frac{x^3+3x}{2}$ este bijectivă şi inversa este

$$g : \mathbb{R} \longrightarrow \mathbb{R}, g(x) = \sqrt[3]{x+\sqrt{x^2+1}} + \sqrt[3]{x-\sqrt{x^2+1}}$$

Soluţie:
• Injectivitatea: fie $x_1, x_2 \in \mathbb{R}$ a.î. $f(x_1) = f(x_2) \Leftrightarrow x_1^3+3x_1 = x_2^3+3x_2 \Leftrightarrow (x_1-x_2)(x_1^2+x_1x_2+x_2^2+3) = 0$. $x_1^2+x_1x_2+x_2^2 \geqslant 0$ pentru $(\forall)x_1, x_2 \in \mathbb{R}$. (Pentru $x_1 = x_2 = 0 \Rightarrow x_1^2+x_1x_2+x_2^2 = 0$. Pentru $(x_1,x_2) \neq (0,0)$, $x_1^2+x_1x_2+x_2^2 = x_2^2((\frac{x_1}{x_2})^2 + \frac{x_1}{x_2} + 1)$. Trinomul din ultima paranteză este strict pozitiv pentru toate valorile reale ale fracţiei $\frac{x_1}{x_2}$). Deci $(x_1^2+x_1x_2+x_2^2+3 > 0$ pentru $(\forall)x_1, x_2 \in \mathbb{R}$. Astfel, $(x_1-x_2)(x_1^2+x_1x_2+x_2^2+3) = 0 \Rightarrow x_1 = x_2$, deci funcţia este injectivă.
• Surjectivitatea: Menţionez soluţia ecuaţiei de gradul 3. Fiecare ecuaţie de grad 3 se poate reduce printr-o schimbare de variabile la o ecuaţie de forma $x^3+qx+r = 0$. Se caută rădăcină de forma $u = \alpha+\beta$. Avem $\alpha\beta = -\frac{q}{3}$ iar $\alpha^3 = \frac{1}{2}\left(-r+\sqrt{r^2+\frac{4q^3}{27}}\right)$.
Fie $y \in \mathbb{R}$, dorim să găsim $x \in \mathbb{R}$ a.î. $f(x) = y \Leftrightarrow x^3+3x-2y = 0$.
Căutăm soluţie de tipul $\alpha+\beta$, unde $\alpha^3 = \frac{1}{2}\left(2y+\sqrt{(4y)^2+\frac{4\cdot 27}{27}}\right) = y+\sqrt{y^2+1}$, de unde $\alpha = \sqrt[3]{y+\sqrt{y^2+1}}$. Cum $y^2+1 > 0$ pentru $(\forall)y \in \mathbb{R}$, avem $\alpha \in \mathbb{R}$.
$\beta = -\frac{1}{\alpha} = -\sqrt[3]{\frac{1}{y+\sqrt{y^2+1}}} = -\sqrt[3]{\frac{y-\sqrt{y^2+1}}{y^2-(y^2+1)}} = \sqrt[3]{y-\sqrt{y^2+1}}$.
Deci soluţia ecuaţiei $f(x) = y$ este $u = \sqrt[3]{y+\sqrt{y^2+1}} + \sqrt[3]{y-\sqrt{y^2+1}} \in \mathbb{R}$, de unde tragem concluzia că f este surjectivă.
Deci funcţia f este bijectivă. Verificaţi faptul că funcţia $g(x)$ dată în enunţ (care vedeţi că provine din rezolvarea ecuaţiei $f(x) = y$) este inversa funcţiei f.

SEMINAR 4

Problema 1. Considerăm relaţiile γ şi δ pe $\mathbb{R}$.
(i) $x\gamma y$ dacă $x + y \in \mathbb{Z}$
(ii) $x\delta y$ dacă $x + y\sqrt{2} \in \mathbb{R}\backslash\mathbb{Q}$.
Să se studieze dacă γ, δ sunt reflexive, simetrice, tranzitive.

Soluţie:
(i) $\exists x \in \mathbb{R}$ pentru care $x + x \notin \mathbb{Z}$, de exemplu $1,2 + 1,2 \notin \mathbb{Z}$, sau $\sqrt{2} + \sqrt{2} = 2\sqrt{2} \notin \mathbb{Z}$. Deci γ nu este reflexivă.

Este simetrică: dacă $x\gamma y \Leftrightarrow x + y \in \mathbb{Z}$. $y + x = x + y \in \mathbb{Z} \Rightarrow y\gamma x$.

Nu este tranzitivă: $1,3 + 0,7 = 2 \in \mathbb{Z}$; $\quad 0,7 + 2,3 = 3 \in \mathbb{Z}$, dar $1,3 + 2,3 = 3,6 \notin \mathbb{Z}$.
(ii) $x + x\sqrt{2} = x(1 + \sqrt{2})$. Dacă $\exists x \in \mathbb{R}$ a.î. $x(1 + \sqrt{2}) \in \mathbb{Q}$, atunci γ NU este reflexivă.
$x(1 + \sqrt{2}) = \frac{p}{q} \Leftrightarrow x = \frac{p}{q(1+\sqrt{2})} = \frac{p(1-\sqrt{2})}{q(-1)} = \frac{p}{q}(\sqrt{2} - 1) \in \mathbb{R}$. Deci δ NU este reflexivă. NU este nici simetrică. De exemplu $\sqrt{2}\delta 1$ pentru că $\sqrt{2}+1\cdot\sqrt{2} \in \mathbb{R}\backslash\mathbb{Q}$, dar $1+\sqrt{2}\cdot\sqrt{2} = 3 \in \mathbb{Z} \subset \mathbb{Q}$, deci 1 nu este în relaţia δ cu $\sqrt{2}$. δ NU verifică nici axioma tranzitivităţii. De exemplu $\sqrt{2}\delta 1$, $1\delta(\sqrt{2} - 1)$, (avem $1+(\sqrt{2}-1)\cdot\sqrt{2}) = 1+2-\sqrt{2} = 3-\sqrt{2} \in \mathbb{R}\backslash\mathbb{Q}$), dar $\sqrt{2}+(\sqrt{2}-1)\cdot\sqrt{2}) = \sqrt{2}+2-\sqrt{2} = 2 \in \mathbb{Z} \subset \mathbb{Q}$. Deci $\sqrt{2}$ nu este în relaţia δ cu $\sqrt{2} - 1$.

Problema 2. Pe mulţimea numerelor complexe $\mathbb{C}$ definim relaţia $z \sim w \Leftrightarrow z - w \in \mathbb{R}$. Arătaţi că $\sim$ este relaţie de echivalenţă, determinaţi clasele de echivalenţă şi un sistem de reprezentanţi.

Soluţie:
(i) reflexivitatea: $z - z = 0 \in \mathbb{R}$ pentru $\forall z \in \mathbb{C}$, deci $z \sim z$.
(ii) simetria: dacă $z - w \in \mathbb{R}$, atunci $w - z = -(z - w) \in \mathbb{R}$, de unde $w \sim z$.
(iii) tranzitivitatea: dacă $z - w \in \mathbb{R}$ şi $w - u \in \mathbb{R}$, atunci $z - u = z - w + w - u \in \mathbb{R}$, adică $z \sim u$.

Avem astfel o relaţie de echivalenţă.

Fie $z \in \mathbb{C}$, clasa de echivalenţă a lui $z, [z] = \{z + x \mid x \in \mathbb{R}\}$ ceea ce reprezintă o dreaptă orizontală ce trece prin z. Ecuaţia acesteia este $y = \mathrm{Im}(z)$. Sistemul de reprezentanţi este *axa imaginară*.

Problema 3. Fie X o mulţime infinită. Pe $\mathcal{P}(X)$ definim relaţia $A \sim B \Leftrightarrow A\Delta B$ este finită. (Δ reprezintă diferenţa simetrică a mulţimilor). Arătaţi că $\sim$ este o relaţie de echivalenţă.

Soluţie: $A\Delta A = \varnothing, |\varnothing| = 0$, deci $A \sim A$. $B\Delta A = A\Delta B$, deci $A \sim B \Rightarrow B \sim A$. Fie $A \sim B$ şi $B \sim C$. $A\Delta C \subset (A\Delta B) \cup (B\Delta C)$, care este o mulţime finită, fiind reuniune de două mulţimi finite.

Problema 4. Considerăm operaţiile algebrice pe $\mathbb{N}$:
(i) $x * y = x + 1$,
(ii) $x * y = x$,
(iii) $x * y = xy + 1$,
(iv) $x * y = 0$,
(v) $x * y = \max\{x, y\}$.

Precizaţi dacă sunt asociative, comutative sau posedă element neutru.

Soluţie:
(i) $(x * y) * z = (x + 1) * z = x + 1$. $x * (y * z) = x * (y + 1) = x + 1$. Operaţia este asociativă. Avem $x * y = x + 1 \neq y + 1 = y * x$. Deci operaţia nu este comutativă. Nu are nici element neutru pentru că $x * e = x \Leftrightarrow x + 1 = x \Leftrightarrow 1 = 0$, ceea ce este fals.
(ii) $(x*y)*z = x*z = x, x*(y*z) = x*y = x$. De aici $(x*y)*z = x*(y*z)$. $x*y = x \neq y = y*x \Rightarrow$ operaţia nu este comutativă. $x * e = x \Leftrightarrow x = x$. $e * x = x \Leftrightarrow e = x$ ptr. $\forall x \in \mathbb{N}$. Deci nu există un element neutru.
(iii) $(x*y)*z = (xy+1)*z = (xy+1)z+1 = xyz+z+1$. Pe de altă parte $x*(y*z) = x*(yz+1) = x(yz + 1) + 1 = xyz + x + 1$. Cele două cantităţi nu sunt egale pentru $\forall x, y, z \in \mathbb{N}$, deci operaţia nu este asociativă. Este comutativă pentru că $x * y = xy + 1 = yx + 1 = y * x$. Elementul neutru trebuie să satisfacă $x * e = x \Leftrightarrow xe + 1 = x \Leftrightarrow x(e - 1) = -1$ pentru $\forall x \in \mathbb{N} \Rightarrow \nexists e \in \mathbb{N}$ cu această proprietate.
(iv) Operaţia este asociativă $(x * y) * z = 0 = x * (y * z)$, comutativă $x * y = 0 = y * x$, şi nu are element neutru.
(v) Este asociativă: $(x*y)*z = \max\{\max\{x, y\}, z\} = \max\{x, y, z\} = \max\{x, \max\{y, z\}\} = x*(y*z)$. Este comutativă $x * y = \max\{x, y\} = \max\{y, x\} = y * x$. Elementul neutru este 0, (dacă $0 \in \mathbb{N}$), altfel 1.

Problema 5. Fie $a, b, c \in \mathbb{Z}, b \neq 0$. Pe $\mathbb{Z}$ definim operaţia $x * y = axy + b(x + y) + c$. Arătaţi că $M_{a,b,c} = (\mathbb{Z}, *)$ este monoid $\Leftrightarrow b = b^2 - ac$ şi $b|c$. Mai mult, pentru $a \neq 0$, avem izomorfismele de monoizi $M_{a,b,c} \simeq M_{a,1,0} \simeq K_a$, unde K_a este monoidul multiplicativ $\{am + 1 \mid m \in \mathbb{Z}\}$.

Soluţie: Impunând condiţia de asociativitate care trebuie să fie adevărată pentru $\forall x, y, z \in \mathbb{Z}$ şi făcând socotelile elementare găsim $b^2 - b - ac = 0$. Pentru elementul neutru e avem $x * e = x$ pentru $(\forall) x \in \mathbb{Z}$. $x * e = x \Leftrightarrow x(ae + b - 1) + be + c = 0, (\forall) x \in \mathbb{Z} \Rightarrow be + c = 0$ şi $ae + b - 1 = 0$, deci $e = -\frac{c}{b} \in \mathbb{Z} \Leftrightarrow b|c$. Cu această expresie a lui e şi înmulţind cu b ecuaţia $ae + b - 1 = 0$ devine $b^2 - b - ac = 0$.

Deci $M_{a,b,c} = (\mathbb{Z}, *)$ este monoid $\Leftrightarrow b = b^2 - ac$ şi $b|c$.

Presupunem acum că $a \neq 0$ şi $M_{a,b,c}$ este monoid, deci $b|c$ şi deci $d = \frac{c}{b} \in \mathbb{Z}$, de unde $c = bd$. Din $b^2 = b + ac$ împărţind cu b şi înlocuind obţinem $b = 1 + ad$. $c = bd = (1 + ad)d$. Următoarele corespondenţe sunt izomorfisme de monoizi. $f : M_{a,b,c} \longrightarrow M_{a,1,0}, f(x) = x + d$ şi $g : M_{a,1,0} \longrightarrow K_a, g(x) = ax + 1$.

SEMINAR 5

Soluţii probleme temă

Problema 1. În primul rând $(\mathbb{N},+)$, $(\mathbb{N},\max)$, $(\mathbb{N},\text{c.m.m.m.c})$ sunt monoizi. Notăm cu c.m.m.m.c$\{a,b\} = [a,b]$. Elementul neutru pentru adunare este 0, ca şi pentru operaţia max. Pentru $[\ ,\ ]$ elementul neutru este 1. Adunarea este asociativă. Pentru a două operaţie pe $\mathbb{N}$ avem $\max\{\max\{a,b\},c\} = \max\{a,b,c\} = \max\{a,\max\{b,c\}\}$. Similar pentru operaţia de luare a c.m.m.m.m.c . Avem deci trei monoizi.

Dacă presupunem că $f : (\mathbb{N},+) \longrightarrow (\mathbb{N},\max)$ este izomorfism atunci $f(2a) = f(a+a) = \max\{f(a),f(a)\} = f(a)$, pentru orice $a \in \mathbb{N}^\star$. Deci f nu este injectiv. Contradicţie.

Similar, dacă presupunem că $g : (\mathbb{N},+) \longrightarrow (\mathbb{N},\text{c.m.m.m.c})$ este izomorfism, atunci $g(2a) = g(a+a) = [g(a),g(a)] = g(a)$, pentru orice $a \in \mathbb{N}^\star$. Deci g nu este injectiv. Contradicţie.

Doi monoizi izomorfi trebuie să aibă proprietăţi similare. Pentru orice $a,b \in \mathbb{N} \Rightarrow \max\{a,b\} \in \{a,b\}$, dar $[a,b] \notin \{a,b\}$ în general. Deci nici ultimii doi monoizi nu sunt izomorfi.

Problema 2. $(\mathbb{N},+)$ este monoidul liber generat de un element, acesta fiind 1.

Considerăm $f : (\mathbb{N},+) \longrightarrow (\mathbb{N},+)$ morfism. Atunci $f(0) = 0$ şi $f(1) = a \in \mathbb{N}$. $f(2) = f(1+1) = f(1)+f(1) = 2a$. Se demonstrează foarte uşr prin inducţie că $f(n) = n \cdot a$. Deci $\text{End}(\mathbb{N},+) = \{f : \mathbb{N} \longrightarrow \mathbb{N} \mid f\text{morfism}\} = \mathbb{N}$.

Fie acum $g : (\mathbb{N},\max) \longrightarrow (\mathbb{N},\max)$ morfism. Pentru $i < j; i,j \in \mathbb{N}^\star$ avem $g(\max\{i,j\}) = \max\{g(i),g(j)\} \Leftrightarrow g(j) = \max\{g(i),g(j)\} \Rightarrow g(i) \leqslant g(j)$.

Am obţinut $\text{End}(\mathbb{N},\max) = \{g : \mathbb{N} \longrightarrow \mathbb{N} \mid g \text{ crescătoare}\}$.

Fie $h : (\mathbb{N},+) \longrightarrow (\mathbb{N},\max)$ morfism. $h(1) = a, h(2) = h(1+1) = \max\{h(1),h(1)\} = h(1)$. Se demonstrează $h(n) = h(1)$.

Deci $\text{Hom}((\mathbb{N},+),(\mathbb{N},\max)) = \{h : \mathbb{N} \longrightarrow \mathbb{N} \mid h(0) = 0, h(n) = a, \forall n \in \mathbb{N}^\star\}$

Fie $k : (\mathbb{N},\max) \longrightarrow (\mathbb{N},+)$ morfism, atunci $k(\max\{i,i\}) = k(i)+k(i) \Leftrightarrow k(i) = k(i)+k(i), \forall i \in \mathbb{N} \Rightarrow k(i) = 0$.

Deci $\text{Hom}((\mathbb{N},\max),(\mathbb{N},+)) = \{0\}$, morfismul nul.

Problema 3. Dacă $f : (\mathbb{N},\max) \longrightarrow (\mathcal{P}(\mathbb{N}),\cup)$ este morfism de monoizi atunci $f(0) = \varnothing$ şi $f(i) = A_i \subset \mathbb{N}$. Mai mult pentru $i < j; i,j \in \mathbb{N}^\star, f(\max\{i,j\}) = f(i) \cup f(j) \Leftrightarrow f(i) = f(i) \cup f(j) \Leftrightarrow A_i = A_i \cup A_j \Rightarrow A_i \subseteq A_j$. Dar f dorim să fie injectiv deci pentru $i \neq j \Rightarrow A_i \neq A_j$. Avem astfel pentru $i < j,\ A_i \subsetneq A_j$.

Putem lua $f : \mathbb{N} \longrightarrow \mathbb{N}, f(n) = [n] = \{1,2,\ldots,n\}$.

Probleme seminar

$U(\mathbb{Z}_n,\cdot) = \{\hat{x} \mid x \in \mathbb{Z}, (x,n) = 1\} = \{\hat{x} \mid \exists \hat{y} \in \mathbb{Z} \text{ cu } \hat{x}\hat{y} = \hat{1}\}$, grupul unităţilor din $(\mathbb{Z}_n,\cdot)$. $U(\mathbb{Z}_n,\cdot)$ este subgrup al monoidului $(\mathbb{Z}_n,\cdot)$. $|U(\mathbb{Z}_n)| = \varphi(n) = n(1-\frac{1}{p_1})\ldots(1-\frac{1}{p_s})$, unde descompunerea în factori primi a numărului n este $p_1^{r_1}\cdots p_s^{r_s}$.

Problema 0. Să se scrie tabla legii de compoziţie a grupului $U(\mathbb{Z}_6, \cdot)$.

Soluţie: $U(\mathbb{Z}_6) = \{\hat{1}, \hat{5}\}$. $6 = 2\cdot 3$, deci $|U(\mathbb{Z}_6)| = 6\cdot(1-\frac{1}{2})(1-\frac{1}{3}) = 2$. Tabla legii de compoziţie este:

$\cdot$	$\hat{1}$	$\hat{5}$
$\hat{1}$	$\hat{1}$	$\hat{5}$
$\hat{5}$	$\hat{5}$	$\hat{1}$

Vedem că aceasta este similară cu tabla adunării lui $(\mathbb{Z}_2, +)$. $\mathbb{Z}_2 = \{\hat{0}, \hat{1}\}$ şi avem

$+$	$\hat{0}$	$\hat{1}$
$\hat{0}$	$\hat{1}$	$\hat{1}$
$\hat{1}$	$\hat{1}$	$\hat{0}$

.

Problema 1. Să se scrie tabla legii de compoziţie a grupului $U(\mathbb{Z}_8, \cdot)$.

Soluţie: $U(\mathbb{Z}_8) = \{\hat{1}, \hat{3}, \hat{5}, \hat{7}\}$. $8 = 2^3$, deci $|U(\mathbb{Z}_8)| = 8 \cdot (1 - \frac{1}{2}) = 4$. Tabla legii de compoziţie este:

$\cdot$	$\hat{1}$	$\hat{3}$	$\hat{5}$	$\hat{7}$
$\hat{1}$	$\hat{1}$	$\hat{3}$	$\hat{5}$	$\hat{7}$
$\hat{3}$	$\hat{3}$	$\hat{1}$	$\hat{7}$	$\hat{5}$
$\hat{5}$	$\hat{5}$	$\hat{7}$	$\hat{1}$	$\hat{3}$
$\hat{7}$	$\hat{7}$	$\hat{5}$	$\hat{3}$	$\hat{1}$

Problema 2. Să se scrie tabla legii de compoziţie a grupului $U(\mathbb{Z}_{10}, \cdot)$.

Soluţie: $U(\mathbb{Z}_{10}) = \{\hat{1}, \hat{3}, \hat{7}, \hat{9}\}$. $10 = 2 \cdot 5$, deci $|U(\mathbb{Z}_{10})| = 10 \cdot (1 - \frac{1}{2})(1 - \frac{1}{5}) = 4$. Tabla legii de compoziţie este:

$\cdot$	$\hat{1}$	$\hat{3}$	$\hat{7}$	$\hat{9}$
$\hat{1}$	$\hat{1}$	$\hat{3}$	$\hat{7}$	$\hat{9}$
$\hat{3}$	$\hat{3}$	$\hat{9}$	$\hat{1}$	$\hat{7}$
$\hat{7}$	$\hat{7}$	$\hat{1}$	$\hat{9}$	$\hat{3}$
$\hat{9}$	$\hat{9}$	$\hat{7}$	$\hat{3}$	$\hat{1}$

Se vede că tabla înmulţirii grupului $U(\mathbb{Z}_8, \cdot)$ este diferită de tabla grupului $U(\mathbb{Z}_{10}, \cdot)$.

Problema 3. Să se scrie tabla legii de compoziţie a grupului $U(\mathbb{Z}_{12}, \cdot)$.

Soluţie: $U(\mathbb{Z}_{12}) = \{\hat{1}, \hat{5}, \hat{7}, \hat{11}\}$. $12 = 2^2 \cdot 3$, deci $|U(\mathbb{Z}_{12})| = 12 \cdot (1 - \frac{1}{2})(1 - \frac{1}{3}) = 4$. Tabla legii de compoziţie este:

$\cdot$	$\hat{1}$	$\hat{5}$	$\hat{7}$	$\hat{11}$
$\hat{1}$	$\hat{1}$	$\hat{5}$	$\hat{7}$	$\hat{11}$
$\hat{5}$	$\hat{5}$	$\hat{1}$	$\hat{11}$	$\hat{7}$
$\hat{7}$	$\hat{7}$	$\hat{11}$	$\hat{1}$	$\hat{5}$
$\hat{11}$	$\hat{11}$	$\hat{9}$	$\hat{7}$	$\hat{1}$

Se vede că tabla înmulţirii grupului $U(\mathbb{Z}_8, \cdot)$ este similară cu tabla grupului $U(\mathbb{Z}_{12}, \cdot)$.

Problema 4. Să se scrie tabla legii de compoziţie $(\mathbb{Z}_4, +)$.

Soluţie: $\mathbb{Z}_4 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}\}$. Tabla adunării este:

$+$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{3}$	$\hat{0}$	$\hat{1}$
$\hat{3}$	$\hat{3}$	$\hat{0}$	$\hat{1}$	$\hat{2}$

Se vede că această tablă este similară cu tabla în mulţirii pe $U(\mathbb{Z}_{10})$.

Problema 5. Să se scrie tabla legii de compoziţie a grupului diedral D_3.

Soluţie: $D_3 = \{1 = \mathrm{id}_\triangle, \rho, \rho^2, s_1, s_2, s_3\}$, unde ρ este rotaţia în sens antiorar cu $120°$ în jurul centrului triunghiului echilateral, iar s_j reprezintă reflecţia faţă de mediatoarea l_j care trece prin vârful j al triunghiului echilateral 123. Operaţia $\circ$ este compunerea funcţiilor care sunt şi izometrii ale planului, compunere care este asociativă şi are ca element neutru $1 = \mathrm{id}_\triangle$. De exemplu $\rho s_1 = \rho \circ s_1$, prima dată aplicăm s_1 şi apoi ρ.

$\circ$	1	ρ	ρ^2	s_1	s_2	s_3
1	1	ρ	ρ^2	s_1	s_2	s_3
ρ	ρ	ρ^2	1	$\rho s_1 = s_3$	$\rho s_2 = s_1$	$\rho s_3 = s_2$
ρ^2	ρ^2	1	ρ	$\rho^2 s_1 = s_2$	$\rho^2 s_2 = s_3$	$\rho^2 s_3 = s_1$
s_1	s_1	$s_1\rho = s_2$	$s_1\rho^2 = s_3$	$s_1^2 = 1$	$s_1 s_2 = \rho$	$s_1 s_3 = \rho^2$
s_2	s_2	$s_2\rho = s_3$	$s_2\rho^2 = s_1$	$s_2 s_1 = \rho^2$	$s_2^2 = 1$	$s_2 s_3 = \rho$
s_3	s_3	$s_3\rho = s_1$	$s_3\rho^2 = s_2$	$s_3 s_1 = \rho$	$s_3 s_2 = \rho^2$	$s_3^2 = 1$

$\circ$	1	ρ	ρ^2	s_1	s_2	s_3
1	1	ρ	ρ^2	s_1	s_2	s_3
ρ	ρ	ρ^2	1	s_3	s_1	s_2
ρ^2	ρ^2	1	ρ	s_2	s_3	s_1
s_1	s_1	s_2	s_3	1	ρ	ρ^2
s_2	s_2	s_3	s_1	ρ^2	1	ρ
s_3	s_3	s_1	s_2	ρ	ρ^2	1

Problema 6. Să se demonstreze că orice grup G în care $x^2 = 1$ pentru orice $x \in G$ este abelian.

Soluţie: Dacă în grupul G avem $x^2 = 1$, înmulţind această relaţie cu x^{-1} obţinem $x^2 x^{-1} = 1 \cdot x^{-1} \Leftrightarrow 1 \cdot x = x^{-1} \Leftrightarrow x = x^{-1}$. Scriem relaţia din ipoteză pentru xy, unde x, y sunt arbitrare în G. Avem $(xy)^2 = 1 \Leftrightarrow (xy)(xy) = 1$. Înmulţim la stânga cu x^{-1} şi la dreapta cu y^{-1} şi obţinem $yx = x^{-1}y^{-1} = xy$. Deci grupul este abelian (comutativ).

Problema 7. Pe mulţimea (-1, 1) considerăm operaţia $x * y = \frac{x+y}{1+xy}$. Să se demonstreze că $((-1, 1), *)$ este grup.

Soluţie: Arătăm că (-1, 1) este parte stabilă pentru $*$. $x \in (-1, 1) \Leftrightarrow |x| < 1$. Deci pentru $|x| < 1$ şi $|y| < 1 \Rightarrow |x| \cdot |y| < 1 \Leftrightarrow |xy| < 1 \Leftrightarrow -1 < xy < 1 \Leftrightarrow 0 < 1 + xy < 2$. În particular $1 + xy \neq 0$.

Arătăm că $x * y + 1 > 0$. $x * y + 1 = \frac{x+y}{1+xy} + 1 = \frac{x+y+1+xy}{1+xy} = \frac{(1+x)(1+y)}{1+xy}$. Fiecare paranteză a numărătorului cât şi numitorul sunt pozitive, deci $x * y + 1 > 0 \Leftrightarrow -1 < x * y$.

Pentru $x * y - 1 < 0$ avem: $x * y + 1 = \frac{x+y}{1+xy} - 1 = \frac{x+y-1-xy}{1+xy} = -\frac{(1-x)(1-y)}{1+xy}$. Fiecare paranteză a numărătorului este strict pozitivă, ca şi numitorul. Deci fracţia este strict negativă. Astfel $x * y < 1$.

Asociativitate: $(x * y) * z = \frac{\frac{x+y}{1+xy} + z}{1 + \frac{x+y}{1+xy} z} = \frac{x+y+z+xyz}{1+xy+xz+yz} = x * (y * z)$.

Elementul neutru este 0.

Inversul fiecărui element $x \in (-1, 1)$ este $-x$.

Cu toate acestea $((-1, 1), *)$.

SEMINAR 6

Problema 1. Să se arate că $((-1,1),*) \simeq ((0,\infty),\cdot)$, unde $x*y=\frac{x+y}{1+xy}$.

Soluţie: Considerăm $f:(-1,1)\longrightarrow(0,+\infty), f(x)=\frac{1-x}{1+x}$. Este clar că $\lim_{x\to-1} f(x)=+\infty$ şi $\lim_{x\to 1} f(x)=0$. Trebuie să demonstrăm că f este morfism şi este funcţie bijectivă.

• morfism:

$$f(x*y)=\frac{1-x*y}{1+x*y}=\frac{1-\frac{x+y}{1+xy}}{1+\frac{x+y}{1+xy}}=\frac{1-x-y+xy}{1+x+y+xy}=\frac{(1-x)(1-y)}{(1+x)(1+y)}=\frac{1-x}{1+x}\cdot\frac{1-y}{1+y}=f(x)\cdot f(y).$$

• f injectivă: $f(x_1)=f(x_2)\Leftrightarrow\frac{1-x_1}{1+x_1}=\frac{1-x_2}{1+x_2}\Leftrightarrow(1-x_1)(1+x_2)=(1-x_2)(1+x_1)\Leftrightarrow -x_1+x_2=x_1-x_2\Leftrightarrow 2x_2=2x_1\Leftrightarrow 2x_2=2x_1\Leftrightarrow x_1=x_2$

• f surjectivă: fie $y\in(0,+\infty)$, trebuie să rezolvăm ecuaţia $f(x)=y$. Avem $\frac{1-x}{1+x}=y\Leftrightarrow 1-x=y+xy\Leftrightarrow 1-y=x(1+y)\Rightarrow x=\frac{1-y}{1+y}\in(-1,1)$.

Deci f este izomorfism.

Definiţie: Fie G un grup şi $x\in G$ un element al lui G.
Dacă $x^n\neq 1$ pentru $\forall n>0$, atunci spunem că ordinul lui x şi notăm $\mathrm{ord}(x)$, este ∞.
Dacă $\exists k>0$ cu $x^k=1$, atunci $\mathrm{ord}(x)=\min\{k\in\mathbb{N}^*\mid x^k=1\}$.

Problema 2. Fie G un grup şi $a,b\in G$ elemente de ordin finit, m şi n. Presupunem că $ab=ba$ şi că $(m,n)=1$. Arătaţi că ab are ordinul mn.

Problema 3. Demonstraţi că grupurile $(\mathbb{Z}_4,+)$ şi $(U(\mathbb{Z}_{10}),\cdot)$ sunt izomorfe.

Tabla adunării pe $\mathbb{Z}_4$ este:

$+$	$\hat0$	$\hat1$	$\hat2$	$\hat3$
$\hat0$	$\hat0$	$\hat1$	$\hat2$	$\hat3$
$\hat1$	$\hat1$	$\hat2$	$\hat3$	$\hat0$
$\hat2$	$\hat2$	$\hat3$	$\hat0$	$\hat1$
$\hat3$	$\hat3$	$\hat0$	$\hat1$	$\hat2$

Să precizăm ordinele elementelor grupului $\mathbb{Z}_4$. Avem:
$\hat1+\hat1+\hat1+\hat1=\hat0\Leftrightarrow 4\cdot\hat1=\hat0\Rightarrow\mathrm{ord}(\hat1)=4$,
$\hat2+\hat2=\hat0\Leftrightarrow 2\cdot\hat2=\hat0\Rightarrow\mathrm{ord}(\hat2)=2$,
$\hat3+\hat3+\hat3+\hat3=\hat0\Leftrightarrow 4\cdot\hat3=\hat0\Rightarrow\mathrm{ord}(\hat3)=4$.

$U(\mathbb{Z}_{10})=\{\overline{1},\overline{3},\overline{7},\overline{9}\}$ şi tabla înmulţirii este:

$\cdot$	$\overline1$	$\overline3$	$\overline7$	$\overline9$
$\overline1$	$\overline1$	$\overline3$	$\overline7$	$\overline9$
$\overline3$	$\overline3$	$\overline9$	$\overline1$	$\overline7$
$\overline7$	$\overline7$	$\overline1$	$\overline9$	$\overline3$
$\overline9$	$\overline9$	$\overline7$	$\overline3$	$\overline1$

Ordinele elementelor grupului $U(\mathbb{Z}_{10})$ sunt:
$\overline{3}\cdot\overline{3}\cdot\overline{3}\cdot\overline{3}=\overline{1}\Rightarrow \mathrm{ord}(\overline{3})=4$,
$\overline{7}\cdot\overline{7}\cdot\overline{7}\cdot\overline{7}=\overline{1}\Rightarrow \mathrm{ord}(\overline{7})=4$,
$\overline{9}\cdot\overline{9}=\overline{1}\Rightarrow \mathrm{ord}(\overline{9})=2$.

Astfel un izomorfism trebuie să transforme un element de un anumit ordin într-un element de acelaşi ordin. Avem $\hat{0}\mapsto\overline{1},\hat{2}\mapsto\overline{9},\hat{1}\mapsto\overline{3},\hat{3}\mapsto\overline{7}$ sau $\hat{0}\mapsto\overline{1},\hat{2}\mapsto\overline{9},\hat{1}\mapsto\overline{7},\hat{3}\mapsto\overline{3}$. se verifică uşor că acestea sunt izomorfisme.

Produsul direct a două grupuri G_1, G_2 este $G_1\times G_2$, operaţia este produsul pe componente. Elementele din G_1 comută cu cele din G_2.

Problema 4. Să se scrie tabla grupului $(\mathbb{Z}_2\times\mathbb{Z}_2,+)$. Să se demonstreze că $(U(\mathbb{Z}_8),\cdot)$ este izomorf cu grupul $(\mathbb{Z}_2\times\mathbb{Z}_2,+)$.

Soluţie: Notăm elementele din $\mathbb{Z}_2\times\mathbb{Z}_2$: $0=(\hat{0},\hat{0}), a=(\hat{1},\hat{0}), b=(\hat{0},\hat{1}), a+b=(\hat{1},\hat{1})$. Adunarea se face pe componente. Avem $a+b=b+a$ pentru că adunăm pe fiecare componentă cu $\hat{0}$. Tabla adunării este

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

$+$	0	a	b	$a+b$
0	0	a	b	$a+b$
a	a	0	$a+b$	b
b	b	$a+b$	0	a
$a+b$	$a+b$	b	a	0

Vedem că $\mathrm{ord}(a)=\mathrm{ord}(b)=\mathrm{ord}(a+b)=2$.

Pentru $U(\mathbb{Z}_8)=\{\hat{1},\hat{3},\hat{5},\hat{7}\}$ avem $\mathrm{ord}(\hat{3})=\mathrm{ord}(\hat{5})=\mathrm{ord}(\hat{7})=2$. Cele două grupuri sunt izomorfe. Sunt grupuri cu doi generatori şi orice izomorfism este determinat de valorile pe generatori. De exemplu $0\mapsto\hat{1}, a\mapsto\hat{3}, b\mapsto\hat{5}, a+b\mapsto\hat{3}\cdot\hat{5}=\hat{7}$.

Grupul $\mathbb{Z}_2\times\mathbb{Z}_2$ se numeţe grupul lui Klein.

Problema 5. Orice grup cu 4 elemente este izomorf sau cu $(\mathbb{Z}_4,+)$ sau cu $(\mathbb{Z}_2\times\mathbb{Z}_2,+)$.

Soluţie: Ordinul grupului este numărul de elemente al acestuia. Se ştie că pentru orice $x\in G, \mathrm{ord}(x)|\ |G|$. Deci pentru un grup G cu 4 elemente, orice element $1\neq x\in G\Rightarrow \mathrm{ord}(x)\in\{2,4\}$.

• pentru orice $1\neq x, \mathrm{ord}(x)=2\Leftrightarrow x^2=1\Leftrightarrow x=x^{-1}$. Considerăm $1\neq y\neq x$, şi $y^2=1$ de unde $y^{-1}=y$. xy este un alt element. Am demonstrat în seminarul 5 că orice grup pentru care orice $x\in G, x^2=1$ este abelian. Deci $yx=xy$. Astfel elementele grupului sunt $1,x,y,xy$, cele diferite de 1 de ordin 2. Acesta este grupul Klein.

• $\exists x\in G, \mathrm{ord}(x)=4$. Deci avem $x^4=1$ şi elementele grupului $G=\{1,x,x^2,x^3\}$. Să vedem că acestea sunt distincte. $1\neq x$ pentru că $\mathrm{ord}(x)=4$ iar $\mathrm{ord}(1)=1$. Dacă $x^2=1$ atunci $\mathrm{ord}(x)=2<4$, ceea ce contrazice ipoteza. Deci $x^2\neq 1$. Dacă $x^2=x\Rightarrow x=1$, ceea ce este fals. Deci $1\neq x^2\neq x$. Similar se arată că $1\neq x^3\neq x$ şi $x^3\neq x^2$. Deci $(G,\cdot)\simeq\ (Z_4,+)$. Acesta este de fapt grupul ciclic cu 4 elemente scris multiplicativ sau aditiv.

Problema 6. Să se arate că $D_3 \simeq S_3$.

Soluţie: D_3 este generat de ρ rotaţia cu $120°$ în sens antiorar în jurul centrului şi s oricare dintre cele trei simetrii. Vom considera $s = s_3$, simetria faţă de mediatoarea l_3 ce trece prin vârful 3. Acţiunea rotaţiei ρ pe vârfurile 1, 2, 3 ale triunghiului este : $(1,2,3) \longmapsto (2,3,1)$. Ac ciunea simetriei $s = s_3$ pe vârfurile triungiului este $(1,2,3) \longmapsto (2,1,3)$. ρ şi s sunt generatorii grupului D_3, adică fiecare element se poate scrie ca un cuvânt în puterile lui ρ şi ale lui s. Ca mulţime $D_3 = \{1, \rho, \rho^2, s, \rho s, \rho^2 s\}$. Corespondenţa $\rho \mapsto a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ şi $s \mapsto b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ defineşte un izomorfism între D_3 şi S_3. În ambele grupuri operaţia este compunerea aplicaţiilor care se face de la dreapta la stânga.

Problema 7. Orice grup cu 6 elemente este izomorf sau cu $\mathbb{Z}_6$ sau cu grupul permutărilor S_3.

Soluţie: Folosim din nou faptul că pentru orice $x \in G, \text{ord}(x) | \, |G|$.

• $\nexists x \in G, \text{ord}(x) = 6$. Atunci $(\forall) x \neq 1$ poate avea ordinul 2 sau 3. Aplicând teorema Cauchy rezultă că există în G un element $x, \text{ord}(x) = 3$ şi un element $y, \text{ord}(y) = 2$. Bineînţeles $x \neq y$, pentru că au ordine diferite. Avem $1 \neq x \neq x^2 \neq 1$. Putem avea $y = x^2$? Dacă ar fi adevărat atunci $1 = y^2 = (x^2)^2 = x^4$. Deci $x^4 = 1 = x^3 (\text{ord}(x) = 3) \Rightarrow x = 1$, ceea ce este fals. Deci $y \notin \{1, x, x^2\}$. În G avem elementele $\{1, x, x^2, y, xy, x^2 y\}$.

- dacă $yx = 1 \Rightarrow x = y^{-1} = y$ - fals
- dacă $yx = x \Rightarrow y = 1$ - fals
- dacă $yx = x^2 \Rightarrow y = x$ - fals
- dacă $yx = y \Rightarrow x = 1$ - fals
- dacă $yx = xy$ nu avem o contradicţie, grupul care se obţine este abelian
- o altă variantă este ca $yx = x^2 y \Leftrightarrow yxy^{-1} = x^2 \Leftrightarrow yxy = x^2$.

1: $yx = xy$. Notăm $xy = a$. $a^2 = (xy)^2 = xyxy = xyyx = x^2$, $a^3 = aa^2 = (xy)x^2 = yxx^2 = y$, $a^4 = x^4 = xx^3 = x$, $a^5 = a^2 a^3 = x^2 y$, $a^6 = (a^3)^2 = y^2 = 1$. Am obţinut un element de ordin 6, deci o contradicţie.
2. $yx = x^2 y$. În acest caz avem $yx^2 = yxx = x^2 yx = x^2 x^2 y = x^4 y = xy$. Deci în acest caz $G = \{1, x, x^2, y, xy, x^2 y\}$, iar $yx = x^2 y$ şi $yx^2 = xy$. Acesta este grupul $S_3 \simeq D_3$.

• $\exists x \in G, \text{ord}(x) = 6$, atunci
$G = \{1, x, x^2, x^3, x^4, x^5\}$, adică grupul ciclic cu 6 elemente. Similar cu demonstraţia din problema 5, aceste elemente sunt distincte. Deci $(G, \cdot) \simeq (\mathbb{Z}_6, +)$.

SEMINAR 7

Să se determine subgrupurile şi să se descrie laticea acestora pentru grupurile, $\mathbb{Z}_p$ cu p prim, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_6$, D_3, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times Z_4$, $\mathbb{Z}_8$, D_4, Q grupul cuarternionilor.

Determinaţi subgrupurile normale ale grupurilor D_3, D_4, Q.

- **Grupuri $\mathbb{Z}_p$ cu p prim**

  $\mathbb{Z}_p = \{\hat{0}, \hat{1}, \ldots, \widehat{p-1}\}$. p prim $\Rightarrow \text{ord}(\hat{j}) = \frac{p}{(p,j)} = p$, $(\forall)1 \leqslant j \leqslant p-1$.

  Deci $\mathbb{Z}_p =< \hat{1} >=< \hat{2} >= \ldots =< \widehat{p-1} >$, adică poate fi generat de oricare dintre elementele $\hat{1}, \ldots, \widehat{p-1}$.

  Teorema Lagrange ne spune că într-un grup finit G, pentru orice subgrup $H < G$, avem $|H|||G|$. În cazul de faţă pentru $G = \mathbb{Z}_p$, dacă $H < \mathbb{Z}_p$, atunci $|H||p$, dar p este prim şi deci $|H| \in \{1, p\}$, deci $H = \hat{0}$ sau $H = \mathbb{Z}_p$. Deci Z_p cu p prim nu are subgrupuri proprii adică $\nexists H$ a.î.$1 \lneq H \lneq \mathbb{Z}_p$.

  În fiecare dintre figurile următoare segmentul ce uneşte două subgrupuri reprezintă incluziunea subgrupului scris mai jos în cel scris mai sus.

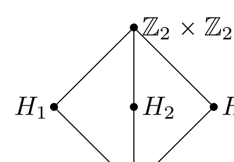
  Pentru $\mathbb{Z}_p$ laticea subgrupurilor este

- **Grupul Klein $\mathbb{Z}_2 \times \mathbb{Z}_2$.**

  $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\hat{0}, \hat{0}), (\hat{1}, \hat{0}), (\hat{0}, \hat{1}), (\hat{1}, \hat{1})\}$. Ordinul oricărui element diferit de $(\hat{0}, \hat{0})$ este 2. Fiecare dintre aceste elemente generează un subgrup de ordin 2.

  Astfel $H_1 =< (\hat{1}, \hat{0}) >= \{(\hat{0}, \hat{0}), (\hat{1}, \hat{0})\}, H_2 =< (\hat{0}, \hat{1}) >= \{(\hat{0}, \hat{0}), (\hat{0}, \hat{1})\}, H_3 =< (\hat{1}, \hat{1}) >= \{(\hat{0}, \hat{0}), (\hat{1}, \hat{1})\}$.

  $|H_1| = |H_2| = |H_3| = 2$. Laticea subgrupurilor este următoarea

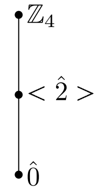


- **Grupul $\mathbb{Z}_4$.**

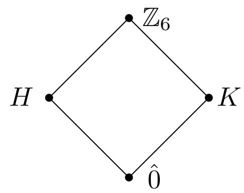
  $\mathbb{Z}_4 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}\}$. Avem $\text{ord}(\hat{0}) = 1$, $\text{ord}(\hat{1}) = 4 = \text{ord}(\hat{3})$ şi $\text{ord}(\hat{2}) = \hat{2}$.

  Deci $\mathbb{Z}_4 =< \hat{1} >=< \hat{3} >$. Avem un subgrup propriu $< \hat{2} >= \{\hat{0}, \hat{2}\}$.

Laticea subgrupurilor pentru $\mathbb{Z}_4$ este



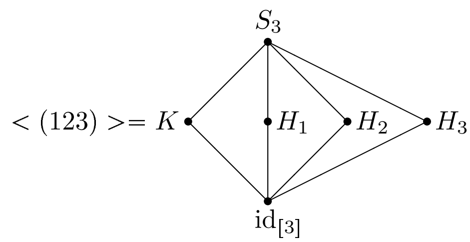
- **Grupul $\mathbb{Z}_6$.**
 $\mathbb{Z}_6 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}\}$. Avem $\text{ord}(\hat{0}) = 1$, $\text{ord}(\hat{1}) = 6 = \text{ord}(\hat{5})$, $\text{ord}(\hat{2}) = \text{ord}\,\hat{(}4) = \frac{6}{(2,6)} = \frac{6}{(4,6)} = \frac{6}{2} = 3$.
 Deci $\mathbb{Z}_6 =< \hat{1} >=< \hat{5} >$, $H =< \hat{2} >=< \hat{4} >= \{\hat{0}, \hat{2}, \hat{4}\}$ iar $K =< \hat{3} >= \{\hat{0}, \hat{3}\}$. $|H| = 3$ iar $|K| = 2$.
 Laticea subgrupurilor pentru $\mathbb{Z}_6$ este:



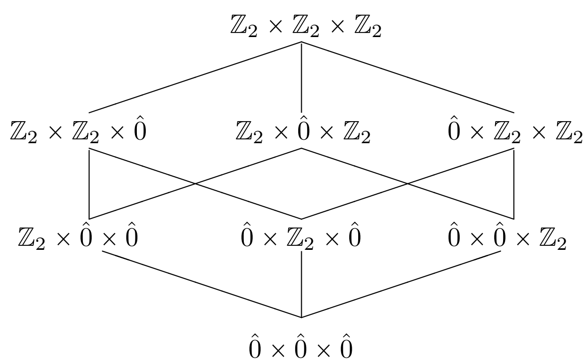
 Până aici toate grupurile prezentate sunt abeliene şi deci subgrupuriloe acestora sunt în fiecare caz este normale.

- **Grupul $D_3 \simeq S_3$.**
 Acesta este primul grup din lista celor propuse spre studiu care nu este abelian.
 Voi folosi permutări.
 $S_3 = \{\text{id}_{[3]}, a = (123), a^2 = (132), b = (12), ab = (123)(12) = (13), a^2b = (132)(12) = (23)\}$. În scrierea uzuală $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ şi $b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. În scrierea folosită anterior se scriu de fapt imaginile elementelor prin permutarea respectivă. Mai mult, în această scriere a unei permutări elementele fixate de permutare NU sunt menţionate. Astfel, $a(1) = 2, a(2) = 3, a(3) = 1$. Aşa apare scrierea compactă $a = (123)$. Pentru b avem $b(1) = 2, b(2) = 1, b(3) = 3$, de unde $b = (12)$.
 Pentru grupul S_3 avem $a^3 = \text{id}_{[3]}, b^2 = (ab)^2 = (a^2b)^2 = \text{id}_{[3]}$. Mai avem relaţia $ba = a^2b$. Deci $\text{ord}(a) = \text{ord}(a^2) = 3$, $\text{ord}(b) = \text{ord}(ab) = \text{ord}(a^2b) = 2$.
 Subgrupurile grupului S_3, primul neabelian pe care-l studiem, sunt:
 $K =< a >=< a^2 >= \{\text{id}_{[3]}, a, a^2\}$, $H_1 =< b >= \{\text{id}_{[3]}, b\}$, $H_2 =< ab >= \{\text{id}_{[3]}, ab\}$, $H_3 =< a^2b >= \{\text{id}_{[3]}, a^2b\}$.
 K este un subgrup de index 2, deci normal. H_1, H_2, H_3 sunt de index 3. Din teorie nu reiese că sunt normale.
 Să facem o verificare pentru unul dintre acestea.
 Elementul $b \in H_1$ îl vom conjuga cu $a^2 \in S_3$. $a^3 = \text{id}_{[3]} \Rightarrow a^{-1} = a^2$ şi $(a^2)^{-1} = a$. Avem $a^2b(a^2)^{-1} = a^2ba = baa = ba^2 \notin H_1$. Deci conjugarea lui $b \in H_1$ cu un element din S_3 NU este un element din H_1, deci H_1 nu este normal.
 Nici subgrupurile H_2 şi H_3 nu sunt normale.

Laticea subgrupurilor în acest caz este

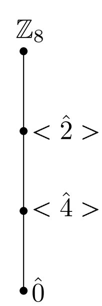


- **Grupul $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.**
  Toate elementele diferite de identitate sunt de ordin 2.
  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\hat{0},\hat{0},\hat{0}),(\hat{1},\hat{0},\hat{0}),(\hat{0},\hat{1},\hat{0}),(\hat{0},\hat{0},\hat{1}),(\hat{1},\hat{1},\hat{0}),(\hat{1},\hat{0},\hat{1}),(\hat{0},\hat{1},\hat{1}),(\hat{1},\hat{1},\hat{1})\}$
  Laticea subgrupurilor este

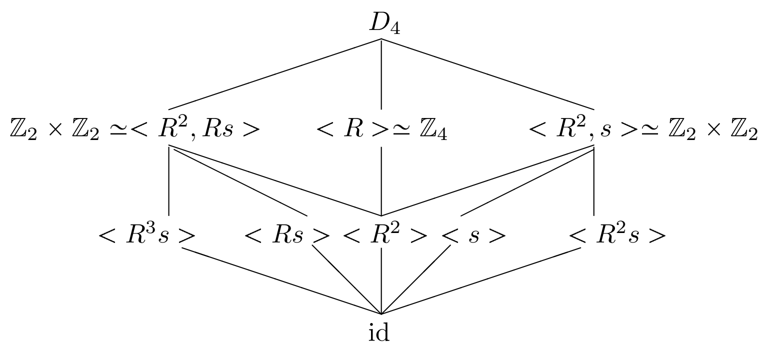


Toate subgrupurile sunt normale, grupul $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ fiind abelian.

- **Grupul $\mathbb{Z}_8$.**
  $\mathbb{Z}_8 = \{\hat{0},\hat{1},\hat{2},\hat{3},\hat{4},\hat{5},\hat{6},\hat{7}\}$.
  Elementele nenule au ordinele: $\mathrm{ord}(\hat{1}) = \mathrm{ord}(\hat{3}) = \mathrm{ord}(\hat{5}) = \mathrm{ord}(\hat{7}) = 8$, $\mathrm{ord}(\hat{2}) = \mathrm{ord}(\hat{6}) = 4$ şi $\mathrm{ord}(\hat{4}) = 2$.
  $\mathbb{Z}_8 =< \hat{1} >=< \hat{3} >=< \hat{5} >=< \hat{7} >$,
  $< \hat{2} >=< \hat{6} >= \{\hat{0},\hat{2},\hat{4},\hat{6}\} \simeq \mathbb{Z}_4$,
  $< \hat{4} >= \{\hat{0},\hat{4}\} \simeq \mathbb{Z}_2$.
  Toate subgrupurile sunt normale pentru că $\mathbb{Z}_8$ este abelian.
  Laticea subgrupurilor este



- **Grupul diedral $\mathcal{D}_4$.**
  Grupul simetriilor pătratului este generat de R, rotaţia cu $90°$ în sens antiorar în jurul centrului pătratului şi s una din cele patru simetrii ale pătratului. Avem relaţiile $R^4 = s^2 = \mathrm{id}$ şi $R^3 s = sR$. Alte relaţii care se deduc din acestea sunt $R^2 s = sR^2, Rs = sR^3$. Grupul nu este abelian.
  $D_4 = \{\mathrm{id}, R, R^2, R^3, s, Rs, R^2 s, R^3 s\}$.
  $\mathrm{ord}(R) = \mathrm{ord}(R^3) = 4 = \frac{4}{(3,4)} = 4$.
  $\mathrm{ord}(R^2) = \mathrm{ord}(s) = \mathrm{ord}(Rs) = \mathrm{ord}(R^2 s) = \mathrm{ord}(R^3 s) = 2$.
  De exemplu $(R^2 s)^2 = R^2 s R^2 s = sR^2 R^2 s = sR^4 s = s\,\mathrm{id}\,s = s^2 = \mathrm{id} \Rightarrow \mathrm{ord}(R^2 s) = 2$.



$< R^2 > \lhd < R > \lhd D_4$. Nu rezultă imediat că $< R^2 > \lhd D_4$. Trebuie să facem conjugarea. Este suficient cu generatorii grupului D_4. Conjugarea lui R^2 cu R ne dă R^2, fiind puteri ale lui R. $sR^2 s^{-1} = sR^2 s = ssR^2 = \mathrm{id}\, R^2 = R^2$. Conjugarea păstrează subgrupul $< R^2 >$, deci acesta este normal în D_4.

Nu acelaşi lucru se întâmplă pentru subgrupurile $< s >, < Rs >, < R^2 s >, < R^3 s >$.

Voi face conjugarea cu generatorii R şi s pentru subgrupul $< Rs >$. $R^4 = \mathrm{id} \Rightarrow R^{-1} = R^3$.

Avem $R(Rs)R^{-1} = RRsR^3 = sR^2 R^3 = sR^5 = sR = R^3 s \notin < Rs >$. Deci $< Rs >$ nu este normal în D_4.

Vedem că $< Rs > \lhd < R^2, Rs > \lhd D_4$, dar $< Rs >$ nu este subgrup normal în D_4.

• Fie G un grup şi $\mathrm{Aut}(G) = \{f : G \longrightarrow G \mid f \text{ automorfism}\}$. Este uşor de văzut că $\mathrm{Aut}(G)$ este grup: compunerea morfismelor este asociativă, id_G este elementul neutru la compunere iar fiecare automorfism (morfism bijectiv) are un invers.

Considerăm $\mathrm{Inn}(G) = \{\varphi_g : G \longrightarrow G \mid \varphi_g(x) = gxg^{-1}, \forall x \in G\}$ subgrupul automorfismelor interioare.

Demonstrăm că φ_g este automorfism al grupului G.

- φ_g morfism: $\varphi_g(xy) = g(xy)g^{-1} = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi_g(x)\varphi_g(y)$.
- φ_g injectiv: $\varphi_g(x) = \varphi_g(y) \Leftrightarrow gxg^{-1} = gyg^{-1}$. Înmulţind la stânga cu g^{-1} şi la dreapta cu g obţinem $x = y$.
- φ_g surjectiv: Fie $y \in G$. Trebuie să rezolvăm ecuaţia $\varphi_g(x) = y$ în funţie de x. $\varphi_g(x) = y \Leftrightarrow gxg^{-1} = y \Leftrightarrow x = g^{-1}yg$. Deci pentru $\forall y \in G, \exists x = g^{-1}yg \in G$ a.î. $\varphi_g(x) = y$.

Considerăm aplicaţia $F : G \longrightarrow \mathrm{Inn}(G)$ definită prin $F(g) = \varphi_g$. Demonstrăm că F este morfism. Trebuie arătat că $F(g_1 g_2) = F(g_1) \circ F(g_2)$.

$F(g_1 g_2) = \varphi_{g_1 g_2}$. $\varphi_{g_1 g_2}(x) = g_1 g_2 x (g_1 g_2)^{-1} = g_1 g_2 x g_2^{-1} g_1^{-1} = g_1(g_2 x g_2^{-1}) g_1^{-1} = \varphi_{g_1}(g_2 x g_2^{-1}) = \varphi_{g_1}(\varphi_{g_2}(x)) = (\varphi_{g_1} \circ \varphi_{g_2})(x) \Rightarrow \varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2}$, adică $F(g_1 g_2) = F(g_1) \circ F(g_2)$.

SEMINAR 8

Tema 7 Problema 1. Voi descrie subgrupurile grupului abelian $\mathbb{Z}_2 \times \mathbb{Z}_4$.

$\mathbb{Z}_2 \times \mathbb{Z}_4 = \{e = (\hat{0}, \overline{0}), (\hat{0}, \overline{1}), (\hat{0}, \overline{2}), (\hat{0}, \overline{3}), (\hat{1}, \overline{0}), (\hat{1}, \overline{1}), (\hat{1}, \overline{2}), (\hat{1}, \overline{3})\}$.

$\mathrm{ord}(e) = 1, \mathrm{ord}((\hat{0}, \overline{1})) = 4, \mathrm{ord}((\hat{0}, \overline{2})) = 2, \mathrm{ord}((\hat{0}, \overline{3})) = 4, \mathrm{ord}((\hat{1}, \overline{0})) = 2, \mathrm{ord}((\hat{1}, \overline{1}) = 4, \mathrm{ord}((\hat{1}, \overline{2})) = 2, \mathrm{ord}((\hat{1}, \overline{3})) = 4$.

Subgrupuri: e,

$< (\hat{0}, \overline{2}) >= \{e, (\hat{0}, \overline{2})\}$ subgrup de ordin 2,

$< (\hat{1}, \overline{0}) >= \{e, (\hat{1}, \overline{0})\}$ subgrup de ordin 2,

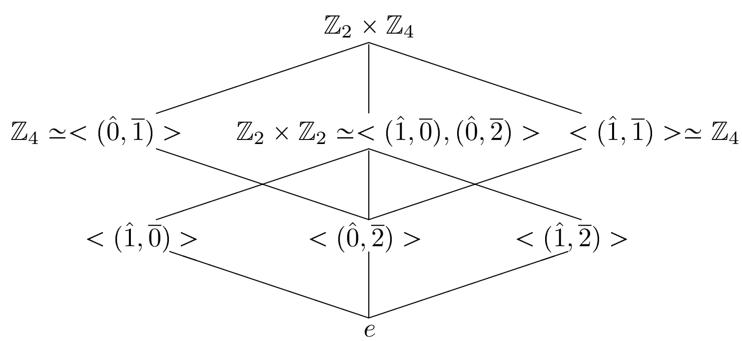
$< (\hat{1}, \overline{2}) >= \{e, (\hat{1}, \overline{2})\}$ subgrup de ordin 2,

$< (\hat{0}, \overline{1}) >= \{e, (\hat{0}, \overline{1}), (\hat{0}, \overline{2}), (\hat{0}, \overline{3})\} =< (\hat{0}, \overline{3}) >$ subgrup de ordin 4

$< (\hat{1}, \overline{1}) >= \{e, (\hat{1}, \overline{1}), (\hat{0}, \overline{2}), (\hat{1}, \overline{3})\} =< (\hat{1}, \overline{3}) >$ subgrup de ordin 4.

Dar $(\hat{0}, \overline{2}) + (\hat{1}, \overline{0}) = (\hat{1}, \overline{2})$, $(\hat{1}, \overline{0}) + (\hat{1}, \overline{2}) = (\hat{0}, \overline{2})$ şi $(\hat{1}, \overline{2}) + (\hat{0}, \overline{2}) = (\hat{1}, \overline{0})$.

Deci $\{e, (\hat{0}, \overline{2}), (\hat{1}, \overline{0}), (\hat{1}, \overline{2})\}$ formează un subgrup de ordin 4, izomorf cu grupul Klein. Laticea subgrupurilor este:



Toate subgrupurile sunt normale pentru că grupul $\mathbb{Z}_2 \times \mathbb{Z}_4$ este abelian.

Tema 7 Problema 3. Considerăm morfismul $F : G \longrightarrow \mathrm{Inn}(G)$ definit prin $F(g) = \varphi_g$.

Arătăm că $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$. Considerăm $f \in \mathrm{Aut}(G)$ şi $\varphi_g \in \mathrm{Inn}(G)$. $f \circ \varphi_g \circ f^{-1} \in \mathrm{Aut}(g)$. Avem $(f \circ \varphi_g \circ f^{-1})(x) = f(\varphi_g(f^{-1}(x))) = f(gf^{-1}(x)g^{-1}) = f(g)f(f^{-1}(x))(f(g))^{-1} =$
$= f(g)(f \circ f^{-1})(x)(f(g))^{-1} = f(g)\,\mathrm{id}_G(x)(f(g))^{-1} = f(g)x(f(g))^{-1} = \varphi_{f(g)}(x) \Rightarrow$
$\Rightarrow f \circ \varphi_g \circ f^{-1} = \varphi_{f(g)} \in \mathrm{Inn}(G)$. Deci conjugarea unui element din $\mathrm{Inn}(G)$ cu un element arbitrar din $\mathrm{Aut}(G)$ ne dă un element din $\mathrm{Inn}(G)$. Astfel $\mathrm{Inn}(G)$ este subgrup normal în $\mathrm{Aut}(G)$.

Determinăm acum subgrupul $\mathrm{Ker}(F) = \{g \in G \mid F(g) = \mathrm{id}_G\} = \{g \in G \mid \varphi_g = \mathrm{id}_G\}$.

$\varphi_g = \mathrm{id}_G \Leftrightarrow \varphi_g(x) = \mathrm{id}_G(x), (\forall)x \in G \Leftrightarrow gxg^{-1} = x, (\forall)x \in G \Leftrightarrow gx = xg, (\forall)x \in G$.

Deci $\mathrm{Ker}(F) = \{g \in G \mid gx = xg, (\forall)x \in G\}$. Acest subgrup normal (nucleul oricărui morfism este un subgrup normal) în G se numeşte centrul grupului G şi se notează cu $Z(G)$. Este subgrupul elementelor care comută cu toate elementele grupului G.

Problema 1. Demonstraţi că orice subgrup finit generat al grupului $(\mathbb{Q},+)$ este ciclic.

Soluţie: Considerăm $H =< \frac{p_1}{q_1}, \dots, \frac{p_n}{q_n} >< \mathbb{Q}$, unde $q_j \in \mathbb{N}^\star$ pentru orice $1 \leqslant j \leqslant n$. Considerăm $s = [q_1, q_2, \dots, q_n]$, c.m.m.m.c. al numitorilor şi fractiile echivalente $\frac{p_1}{q_1} = \frac{p'_1}{s}, \dots \frac{p_n}{q_n} = \frac{p'_n}{s}$.

Atunci $H =< \frac{p_1}{q_1}, \dots, \frac{p_n}{q_n} >=< \frac{p'_1}{s}, \dots, \frac{p'_n}{s} >=< \frac{1}{s} >$ pentru că oricare dintre generatorii $\frac{p'_j}{s} = \frac{1}{s} + \ldots + \frac{1}{s}$ sumă cu p'_j termeni dacă $p'_j > 0$ şi opusul acestei sume dacă $p'_j < 0$.

Problema 2. Determinaţi morfismele între grupurile aditive $\mathbb{Z}_{12}$ şi $\mathbb{Z}_{18}$.

Soluţie: Fie $f : \mathbb{Z}_{12} \longrightarrow \mathbb{Z}_{18}, f$ morfism. Întrucât $\mathbb{Z}_{12} =< \hat{1} >$, grup ciclic generat de $\hat{1}$, este suficient să dăm valoarea lui f pe generatorul $\hat{1}$
(pentru fiecare $\hat{g} \in \mathbb{Z}_{12}, f(\hat{g}) = f(\hat{1} + ... + \hat{1}),$ cu g termeni în sumă, $= f(\hat{1}) + ... + f(\hat{1}) = gf(\hat{1})$).

Fie aşadar $f(\hat{1}) = \overline{k} \in \mathbb{Z}_{18}$. Ştim că ordinul elementului divide ordinul grupului, deci $\mathrm{ord}(\overline{k})|18$.

Dar $f(\hat{0}) = \overline{0}$ (f morfism), $\overline{0} = f(\hat{0}) = f(\widehat{12}) = f(12 \cdot \hat{1}) = 12f(\hat{1}) = 12 \cdot \overline{k}$. Dar $\mathrm{ord}(\overline{k})$ este cel mai mic număr natural nenul cu proprietatea $p \cdot \overline{k} = \overline{0}$. Deci $\mathrm{ord}(\overline{k})|12$. Deci $\mathrm{ord}(\overline{k})$ divide şi 12 şi 18, deci $\mathrm{ord}(\overline{k})$ divide c.m.m.d.c (12,18) = 6. Astfel $\mathrm{ord}(\overline{k}) \in \{1, 2, 3, 6\}$. Vom nota cu $f_{\overline{k}}$ morfismul cu valoarea în $\hat{1}$ egală cu $\overline{k}$. Deci $f_{\overline{k}}(\hat{1}) = \overline{k}$.

Dacă $\mathrm{ord}(\overline{k}) = 1 \Rightarrow \overline{k} = \overline{0}$ şi $f_{\overline{0}}$ este morfismul nul, $\mathrm{Im}(f_{\overline{0}}) = \{\overline{0}\}$,

dacă $\mathrm{ord}(\overline{k}) = 2 \Rightarrow \overline{k} = \overline{9}$, $f_{\overline{9}}(\hat{1}) = \overline{9}$, $\mathrm{Im}(f_{\overline{9}}) = \{\overline{0}, \overline{9}\}$

dacă $\mathrm{ord}(\overline{k}) = 3 \Rightarrow \overline{k} \in \{\overline{6}, \overline{12}\}$, $f_{\overline{6}}(\hat{1}) = \overline{6}$, $\mathrm{Im}(f_{\overline{6}}) = \{\overline{0}, \overline{6}, \overline{12}\} = \mathrm{Im}(f_{\overline{12}}); f_{\overline{12}}(\hat{1}) = \overline{12}$,

dacă $\mathrm{ord}(\overline{k}) = 6 \Rightarrow \overline{k} \in \{\overline{3}, \overline{15}\}$, $f_{\overline{3}}(\hat{1}) = \overline{3}$, $\mathrm{Im}(f_{\overline{6}}) = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}\} = \mathrm{Im}(f_{\overline{15}}); f_{\overline{15}}(\hat{1}) = \overline{15}$,

Aceste morfisme se pot şi aduna şi avem $\mathrm{Hom}(\mathbb{Z}_{12}, \mathbb{Z}_{18}) \simeq \mathbb{Z}_6$. Tabla adunării este

$+$	$f_{\overline{0}}$	$f_{\overline{3}}$	$f_{\overline{6}}$	$f_{\overline{9}}$	$f_{\overline{12}}$	$f_{\overline{15}}$
$f_{\overline{0}}$	$f_{\overline{0}}$	$f_{\overline{3}}$	$f_{\overline{6}}$	$f_{\overline{9}}$	$f_{\overline{12}}$	$f_{\overline{15}}$
$f_{\overline{3}}$	$f_{\overline{3}}$	$f_{\overline{6}}$	$f_{\overline{9}}$	$f_{\overline{12}}$	$f_{\overline{15}}$	$f_{\overline{0}}$
$f_{\overline{6}}$	$f_{\overline{6}}$	$f_{\overline{9}}$	$f_{\overline{12}}$	$f_{\overline{15}}$	$f_{\overline{0}}$	$f_{\overline{3}}$
$f_{\overline{9}}$	$f_{\overline{9}}$	$f_{\overline{12}}$	$f_{\overline{15}}$	$f_{\overline{0}}$	$f_{\overline{3}}$	$f_{\overline{6}}$
$f_{\overline{12}}$	$f_{\overline{12}}$	$f_{\overline{15}}$	$f_{\overline{0}}$	$f_{\overline{3}}$	$f_{\overline{6}}$	$f_{\overline{9}}$
$f_{\overline{15}}$	$f_{\overline{15}}$	$f_{\overline{0}}$	$f_{\overline{3}}$	$f_{\overline{6}}$	$f_{\overline{9}}$	$f_{\overline{12}}$

Cum adunăm în general două funcţii $f, h : A \longrightarrow (B, +)$, unde pe B avem o operaţie de adunare.

$f + h : A \longrightarrow B$ este o altă funcţie şi aceasta este definită $(f + h)(a) = f(a) + h(a)$. În acest fel adunăm şi morfismele între $\mathbb{Z}_{12}$ şi $\mathbb{Z}_{18}$.

Să exemplificăm pentru două morfisme. Să vedem că $f_{\overline{9}} + f_{\overline{6}} = f_{\overline{15}}$.

$(f_{\overline{9}} + f_{\overline{6}})(\hat{1}) = f_{\overline{9}}(\hat{1}) + f_{\overline{6}}(\hat{1}) = \overline{9} + \overline{6} = \overline{15} = f_{\overline{15}}(\hat{1})$.

Mai mult pentru orice $\hat{k} \in \mathbb{Z}_{12}$, $(f_{\overline{9}}+f_{\overline{6}})(\hat{k}) = f_{\overline{9}}(\hat{k})+f_{\overline{6}}(\hat{k}) = f_{\overline{9}}(k\hat{1})+f_{\overline{6}}(k\hat{1}) = kf_{\overline{9}}(\hat{1})+kf_{\overline{6}}(\hat{1}) = k(f_{\overline{9}}(\hat{1}) + f_{\overline{6}}(\hat{1})) = k(\overline{9} + \overline{6}) = k\overline{15} = kf_{\overline{15}}(\hat{1}) = f_{\overline{15}}(k\hat{1}) = f_{\overline{15}}(\hat{k})$. Deci $f_{\overline{9}} + f_{\overline{6}} = f_{\overline{15}}$. Vedem că este suficient să verificăm egalitatea pe generatorul $\hat{1}$.

În general avem $\mathrm{Hom}(\mathbb{Z}_p, \mathbb{Z}_q) \simeq \mathbb{Z}_{(p,q)}$.

Problema 3. Arătaţi că singurul morfism de grupuri de la $(\mathbb{Q}, +)$ la $(\mathbb{Z}, +)$ este cel nul.

Soluţie: Fie $f : (\mathbb{Q}, +) \longrightarrow (\mathbb{Z}, +)$ morfism de grupuri. Deci $f(0) = 0$ şi $f(1) = k \in \mathbb{Z}$. Dar $1 \in \mathbb{Q}$ se poate scrie ca fracţie $\frac{p}{p} = 1, (\forall)p \in \mathbb{N}^\star$. $k = f(1) = f(\frac{p}{p}) = pf(\frac{1}{p}) \Rightarrow p|k$ pentru $(\forall)p \in \mathbb{N}^\star$.

De aici $k = 0$. Dar f este morfism deci $f(n) = nf(1) = n \cdot 0 = 0, (\forall) n \in \mathbb{N}$. Dacă $m \in \mathbb{Z}, m < 0$,, atunci $0 = f(0) = f(m - m) = f(m) + f(-m) = f(m) + 0 \Rightarrow f(m) = 0$. $0 = f(\frac{p}{p}) = pf(\frac{1}{p}) \Rightarrow f(\frac{1}{p}) = 0 \Rightarrow f(\frac{r}{p}) = rf(\frac{1}{p}) = r \cdot 0 = 0$.

Problema 4. Calculaţi tabla de înmulţire a grupului factor $Q/\{\pm 1\}$ unde Q este grupul cuaternionilor.

Soluţie: Notăm $H = \{\pm 1\}$, unde $1 = I_2$. $< \mathbf{j} > \cap < \mathbf{k} >= \{\pm I_2\}$. H fiind intersecţie de subgrupuri normale este un subgrup normal al grupului Q, deci Q/H este grup. Elementele sunt $\overline{H}$ pe care o vom nota cu $\overline{1_H}$.

$\bar{\mathbf{j}} = \{\pm \mathbf{j}\}$, $\bar{\mathbf{k}} = \{\pm \mathbf{k}\}$, $\overline{\mathbf{jk}} = \{\pm \mathbf{jk}\}$.

$\bar{\mathbf{j}}^2 = \overline{\mathbf{j^2}} = \overline{-I_2} = \overline{1_H}$.

$\bar{\mathbf{k}}^2 = \overline{\mathbf{k^2}} = \overline{-I_2} = \overline{1_H}$.

$\overline{\mathbf{jk}}^2 = \overline{(\mathbf{jk})^2} = \overline{\mathbf{jkjk}} = \overline{-\mathbf{jjkk}} = \overline{I_2(-I_2)} = \overline{-I_2} = \overline{1_H}$.

Tabla înmulţirii a grupului factor $Q/\{\pm 1\}$ este

$\cdot$	$\overline{1_H}$	$\bar{\mathbf{j}}$	$\bar{\mathbf{k}}$	$\overline{\mathbf{jk}}$
$\overline{1_H}$	$\overline{1_H}$	$\bar{\mathbf{j}}$	$\bar{\mathbf{k}}$	$\overline{\mathbf{jk}}$
$\bar{\mathbf{j}}$	$\bar{\mathbf{j}}$	$\overline{1_H}$	$\overline{\mathbf{jk}}$	$\bar{\mathbf{k}}$
$\bar{\mathbf{k}}$	$\bar{\mathbf{k}}$	$\overline{\mathbf{jk}}$	$\overline{1_H}$	$\bar{\mathbf{j}}$
$\overline{\mathbf{jk}}$	$\overline{\mathbf{jk}}$	$\bar{\mathbf{k}}$	$\bar{\mathbf{j}}$	$\overline{1_H}$

Problema 5. Arătaţi că funcţia

$$f : (\mathbb{Z} \times \mathbb{Z}, +) \longrightarrow (\mathbb{Z} \times \mathbb{Z}_2, +),\ f(a, b) = (a - b, \hat{a})$$

este morfism de grupuri. Deduceţi că grupul factor $\mathbb{Z} \times \mathbb{Z} / < (2, 2) >$ este izomorf cu $\mathbb{Z} \times \mathbb{Z}_2$.

Soluţie $f((a, b) + (c, d)) = f(a + c, b + d) = (a + c - (b + d), \widehat{a + c}) = (a - b + c - d, \hat{a} + \hat{c}) = (a - b, \hat{a}) + (c - d, \hat{c}) = f(a, b) + f(c, d)$. Deci f este morfism.

Identificăm $\mathrm{Ker}(f) = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid f(a, b) = (0, \hat{0})\}$. $f(a, b) = (0, \hat{0}) \Leftrightarrow (a - b, \hat{a}) = (0, \hat{0}) \Rightarrow a - b = 0$ şi $\hat{a} = \hat{0} \Rightarrow a = b$ şi $a = 2k$. Deci $\mathrm{Ker}(f) = \{(2k, 2k) \mid k \in \mathbb{Z}\} =< (2, 2) >$.

Să demonstrăm că f este surjectiv. Considerăm $(x, \hat{y}) \in \mathbb{Z} \times \mathbb{Z}_2$ şi trebuie să găsim $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ a.î. $f(a, b) = (x, \hat{y}) \Leftrightarrow (a - b, \hat{a}) = (x, \hat{y}) \Leftrightarrow a - b = x$ şi $a = y + 2k$ (luăm $k = 0$). Deci $b = a - x = y - x, a = y$. Deci pentru orice $(x, \hat{y}) \in \mathbb{Z} \times \mathbb{Z}_2$ am găsit $(y, y - x) \in \mathbb{Z} \times \mathbb{Z}$ a.î. $f(y, y - x) = (y - y + x, \hat{y}) = (x, \hat{y}) \in \mathbb{Z} \times \mathbb{Z}_2$. Deci $\mathrm{Im}(f) = \mathbb{Z} \times \mathbb{Z}_2$.

Din teorema fundamentală de izomorfism avem $\mathbb{Z} \times \mathbb{Z}/\mathrm{Ker}(f) \simeq \mathbb{Z} \times \mathbb{Z}_2$.

Problema 6. Considerăm grupul produs semidirect $\mathbb{Z} \rtimes \mathbb{Z}_2$ cu operaţia dată prin

$$(x, \hat{a})(y, \hat{b}) = (x + (-1)^a y, \widehat{a + b}) \text{ pentru} (x, \hat{a}) \text{ şi } (y, \hat{b}) \in \mathbb{Z} \times \mathbb{Z}_2$$

(i) Calculaţi ordinul fiecărui element

(ii) Găsiţi două elemente de ordin doi cu produsul de ordin infinit.

Soluţie: (i) Considerăm elementele de tip $(x, \hat{0}), x \in \mathbb{Z}$. $(x, \hat{0})^2 = (x, \hat{0}) \cdot (x, \hat{0}) = (x + (-1)^0 x, \widehat{0 + 0}) = (2x, \hat{0})$. Pentru $p \in \mathbb{N}^\star$ avem $(x, \hat{0})^p = (px, \hat{0})$ (se demonstrează prin inducţie). Deci avem $\mathrm{ord}((x, \hat{0})) = \infty$.

Elementele $(x,\hat{1}), x \in \mathbb{Z}$. $(x,\hat{1})^2 = (x,\hat{1})\cdot(x,\hat{1}) = (x+(-1)^1x, \widehat{1+1}) = (0,\hat{0})$, unde $(0,\hat{0})$ este elementul neutru pentru operaţia dată ($(x,\hat{y})(0,\hat{0}) = (x+(-1)^y0, \widehat{y+0}) = (x,\hat{y})$). Deci $\mathrm{ord}((x,\hat{1})) = 2$.

(ii) Avem $(x,\hat{1})\cdot(0,\hat{1}) = (x,\hat{0})$. Fiecare din elementele membrului stâng sunt de ordin 2, iar elementul din membrul drept este de ordin infinit.

Problema 7. Arătaţi că grupul $(\mathbb{C}^\star,\cdot)$ este izomorf cu $(\mathbb{R},+)\times(\mathbb{R},+)/\mathbb{Z}$.

Soluţie: Orice număr $z \in \mathbb{C}$ se scrie $z = |z|(\cos(t) + i\sin(t))$, unde $|z| > 0$ şi $t = \arg(z) \in [0,2\pi)$ şi $i = \sqrt{-1}$. Ştim că $|z_1z_2| = |z_1|\cdot|z_2|$ şi $\arg(z_1z_2) \equiv \arg(z_1) + \arg(z_2)(\mod 2k\pi), k \in \mathbb{Z}$.

Grupurile $((0,+\infty),\cdot) \simeq (\mathbb{R},+)$ sunt izomorfe via izomorfismul ln, $(\ln(x_1\cdot x_2) = \ln(x_1)+\ln(x_2))$.

Aplicaţia $(\mathbb{R},+) \longrightarrow (\mathbb{S}^1,\cdot), t \mapsto (\cos(2\pi t) + i\sin(2\pi t))$ este un morfism cu nucleul $\mathbb{Z}$. Deci din teorema fundamentală de izomorfism rezultă că $(\mathbb{R},+)/\mathbb{Z} \simeq (\mathbb{S}^1,\cdot)$.

Izomorfismul cerut este $f : \mathbb{C}^\star \longrightarrow \mathbb{R}\times\mathbb{R}/\mathbb{Z}, f(z) = (\ln(|z|), \arg(z))$. Este un morfism pentru că $f(z_1\cdot z_2) = (\ln(|z_1z_2|), \arg(z_1z_2)) = (\ln(|z_1|)+\ln(|z_2|), \arg(z_1)+\arg(z_2)) = (\ln(|z_1|), \arg(z_1)) + (\ln(|z_2|), \arg(z_2)) = f(z_1)+f(z_2)$. Este uşor de văzut că f este bijectivă. Deci f este un izomorfism.

SEMINAR 9

Problema 1. Fie permutarea $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 9 & 8 & 6 & 5 & 4 & 1 & 3 & 7 \end{pmatrix} \in S_9$.

(i) Scrieţi pe σ ca produs de cicli disjuncţi.
(ii) Calculaţi ordinul permutării σ.
(iii) Calculaţi signatura permutării σ.

Soluţie:
(i) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 9 & 8 & 6 & 5 & 4 & 1 & 3 & 7 \end{pmatrix} = (1297)(38)(47)$. Reamintesc că 5 nu se scrie pentru că este element fixat de σ. Cicli disjuncţi permută.
(ii) Pentru un produs de cicli disjuncţi $c_1c_2 \dots c_p, \mathrm{ord}(c_1c_2 \dots c_p) = [\mathrm{ord}(c_1), \mathrm{ord}(c_2), \dots, \mathrm{ord}(c_p)]$, unde $[,,..,]$ reprezintă c.m.m.m.c al numerelor dintre parantezele drepte.

Deci $\mathrm{ord}(\sigma) = [4, 2, 2, 1] = 4$.
(iii) Signatura unei transpoziţii este -1. Deci $\mathrm{sgn}(\sigma) = (-1)^{\text{numărul de transpoziţii}}$.

$(1297) = (12)(29)(97)$, (în general un ciclu de lungime k este produsul unui ciclu a $k-1$ transpoziţii).

Deci $\sigma = (1297)(38)(47) = (12)(29)(97)(38)(47)$, deci $\mathrm{sgn}(\sigma) = -1$.

Problema 2. Scrieţi grupul diedral D_6 ca un subgrup al lui S_6.

Soluţie: Este sufiecient să scriem generatorii R, s, unde R este rotaţia în sens antiorar cu $60°$, iar s este simetria în dreapta ce uneşte mijlocul a două muchii.

$R \rightsquigarrow (123456)$ iar $s \rightsquigarrow (16)(25)(34)$. R este un element de ordin 6 iar s are ordinul 2.
$R^2 \rightsquigarrow (135)(246), R^3 \rightsquigarrow (14)(25)(36), R^4 \rightsquigarrow (153)(246), R^5 \rightsquigarrow (165432)$.
Vă rămâne să scrieţi celelalte elemente de ordin 2, care corespund simetriilor $Rs, R^2s, R^3s, R^4s, R^5s$.

Problema 3. Listaţi elementele subgrupului lui S_8 generat de $(1256)(3478)$ şi $(1357)(2864)$ (prezentarea prin permutări a grupului cuternionilor).

Soluţie: Notăm $j = (1256)(3478)$ şi $k = (1357)(2864)$. Vedem că şi pentru j şi pentru k cei doi 4 cicli comută fiind pe mulţimi diferite de indici.

Astfel $j^2 = (15)(26)(37)(48) = (15)(37)(26)(84) = k^2$.
$j^3 = (1256)^3(3478)^3 = (1652)(3874)$, $k^3 = (1357)^3(2864)^3 = (1753)(2468), j^4 = k^4 = e$.
$jk = (1256)(3478)(1357)(2864) = (1458)(2367)$,
$kj = (1357)(2864)(1256)(3478) = (1854)(2763) = (jk)^3$
$(jk)^2 = (15)(48)(26)(37) = (kj)^2 = j^2 = k^2$.
Deci $< j, k >= \{e, j, k, j^3, k^3, jk, kj = (jk)^3, j^2 = k^2 = (jk)^2 = (kj)^2\}$.

Problema 4. Listaţi subgrupurile lui A_4 precizând care sunt normale.

Soluţie: A_4 este subgrupul altern al grupului S_4, format din permutările pare. Am precizat mai sus că un ciclu de lungime k este produsul unui ciclu a $k-1$ transpoziţii, deci signatura unui ciclu de lungime k este $(-1)^{k-1}$. Elementele grupului A_4 sunt:
e,
$(12)(34), (13)(24), (14)(23)$,
$(123), (132), (124), (142), (134), (143), (234), (243)$.

Subgrupurile sunt: e, $<(12)(34)>=\{e,(12)(34)\}$, $<(13)(24)>=\{e,(13)(24)\}$, $<(14)(23)>=\{e,(14)(23)\}$,
$<(12)(34),(13)(24)>=\{e,(12)(34),(13)(24),(14)(23)\}$,
$<(123)>=\{e,(123),(132)\}$, $<(124)>=\{e,(124),(142)\}$, $<(134)>=\{e,(134),(143)\}$,
$<(234)>=\{e,(234),(243)\}$ şi bineînţeles A_4.
Dintre acestea, conjugând cu elemente din A_4 vedem că în afară de e şi A_4 subgrupul $<(12)(34),(13)(24)>=\{e,(12)(34),(13)(24),(14)(23)\}$ este normal în A_4.

Problema 5. În S_7 considerăm subgrupul $C=<(123),(12)(4567)>$. Listaţi elementele lui C ştiind că $|C|=12$.

Soluţie: Fie $a=(123)$, $b=(12)(4567)$. $a^2=(132), a^3=e=b^4$. $b^2=(46)(57), b^3=(12)(4765)$.
$ab=(123)(12)(4567)=(12)(23)(12)(4567)=(13)(4567)$,
$ba=(12)(4567)(123)=(12)(4567)(12)(23)=(12)(12)(23)(4567)=(23)(4567)$.
Se vede că $(ab)^2=(ba)^2=b^2=(46)(57)$, $(ab)^3=(13)(4765)$, $(ba)^3=(23)(4765)$.
$a^2b=(132)(12)(4567)=(23)(4567)=(13)(4567)=ba$,
$ba^2=(12)(4567)(132)=(12)(132)(4567)=(13)(4567)=ab$.
$ab^2=b^2a=(123)(46)(57)$, $a^2b^2=b^2a^2=(132)(46)(57)$.
Deci $C=\{e,a,a^2,b,b^2,b^3,ab,ba,(ab)^3,(ba)^3,ab^2,a^2b^2\}$.

Problema 6. Examinând ordinul elementelor, arătaţi că grupurile D_6, A_4 şi C nu sunt izomorfe.

Soluţie: Considerăm numai elementele netriviale
D_6:
2 elemente de ordin 6: R, R^5
2 elemente de ordin 3: R^2, R^4.
7 elemente de ordin 2: $R^3, s, Rs, R^2s, R^3s, R^4s, R^5s$.
A_4 :
8 elemente de ordin 3: $(123), (132), (124), (142), (134), (143), (234), (243)$
3 elemente de ordin 2: $(12)(34), (13)(24), (14)(23)$.
C :
2 elemente de ordin 6: ab^2, a^2b^2.
6 elemente de ordin 4: $b, b^3, ab, ba, (ab)^3, (ba)^3$.
2 elemente de ordin 3: a, a^2,
1 element de ordin 2: $b^2=(ab)^2=(ba)^2$.

Problema 7. Fie $K=\{\mathrm{id},(12)(34),(13)(24),(14)(23)\}$. Arătaţi că:
(i) K este subgrup normal în S_4.
(ii) Scrieţi clasele lui S_4 modulo K.
(iii) S_4/K este izomorf cu S_3.

Soluţie: *(i)* Ştim că $S_4 =< (12),(23),(34) >$. Deci va trebui să verificăm conjugarea elementelor din K cu aceşti generatori.
$(12)(12)(34)(12) = (34)(12) = (12)(34), (12)(13)(24)(12) = (14)(23), (12)(14)(23)(12) = (13)(24),$
$(23)(12)(34)(23) = (13)(24), (23)(13)(24)(23) = (12)(34), (23)(14)(23)(23) = (23)(14) = (14)(23),$
$(34)(12)(34)(34) = (34)(12) = (12)(34), (34)(13)(24)(34) = (14)(23), (34)(14)(23)(34) = (13)(24).$

Vedem că toate elementele din K conjugate cu generatorii lui S_4 ne dau elemente din K. Deci K este normal.

(ii) Voi scrie elementele grupului S_4.

$e,$
$(12),(13),(14),(23),(24),(34),$
$(12)(34),(13)(24),(14)(23),$
$(123),(132),(124),(142),(134),(143),(234),(243),$
$(1234),(1243),(1324),(1342),(1423),(1432).$

Trebuie să vedem care sunt mulţimile σK cu $\sigma \in S_4$.

Prima clasă a lui S_4 modulo K este chiar K. Considerăm σ transpoziţie.

$(12)K = \{(12),(12)(12)(34),(12)(13)(24),(12)(14)(23)\} = \{(12),(34),(1324),(1423)\} = (34)K = (1324)K = (1423)K,$

$(13)K = \{(13),(13)(12)(34),(13)(13)(24),(13)(14)(23)\} = \{(13),(1234),(24),(1432)\} = (24)K = (1234)K = (1432)K,$

$(14)K = \{(14),(14)(12)(34),(14)(13)(24),(14)(14)(23)\} = \{(14),(1243),(1342),(23)\} = (23)K = (1243)K = (1342)K,$

$(123)K = \{(123),(123)(12)(34),(123)(13)(24),(123)(14)(23)\} = \{(123),(134),(243),(142)\} = (134)K = (243)K = (142)K,$

$(132)K = \{(132),(132)(12)(34),(132)(13)(24),(132)(14)(23)\} = \{(132),(234),(124),(143)\} = (234)K = (124)K = (143)K.$

Acestea sunt cele şase clase modulo K.

(iii) $f : S_4 \longrightarrow S_3$ decriem un morfism pe generatori. $(12) \mapsto (12), (23) \mapsto (23), (34) \mapsto (12)$. Este clar că $(12)(34) \mapsto (12)^2 = e$.

$(13) = (12)(23)(12) = (23)(12)(23)$ iar $(24) = (23)(34)(23)$, de unde
$(13)(24) \mapsto (23)(12)(23)(23)(12)(23) = e.$

Am demonstrat că $(12)(34)$ şi $(13)(24) \in \mathrm{Ker}(f)$, deci şi produsul acestora $(14)(23) \in \mathrm{Ker}\, f$.

Deci $\mathrm{Ker}(f) = K$ şi f este surjectiv. Folosind teorema fundamentală de izomorfism rezultă că $S_4/K \simeq S_3$.

Problema 8. Fie D_5 subgrupul lui S_5 generat de (12345) şi $(25)(34)$.

(i) Scrieti elementele lui D_5.
(ii) Listaţi subgrupurile lui D_5 precizând care sunt normale.

Soluţie:*(i)* Fie $r = (12345)$ şi $s = (25)(34)$.

$D_5 = \{e, r, r^2 = (13524), r^3 = (14253), r^4 = (15432), s, rs = (12)(35), r^2s, r^3s, r^4s\}$

(ii) $< (12345) >$ este normal. Mai sunt subgrupuri de ordin 2 generate fiecare de câte o simetrie. Acestea nu sunt normale.

SEMINAR 10

Problema 1. Arătaţi că $A = \{\frac{a+b\sqrt{5}}{2} \mid a, b \in \mathbb{Z}, a \equiv_2 b\}$ este subinel al lui $\mathbb{R}$ cu o infinitate de elemente inversabile.

Soluţie: • Arătăm că $(A,+)$ este subgrup în $(\mathbb{R},+)$.
Fie $\frac{a+b\sqrt{5}}{2}, \frac{c+d\sqrt{5}}{2} \in A; a,b,c,d \in \mathbb{Z}$, a şi b au aceeaşi paritate, c şi d sunt de aceeaşi paritate.
$\frac{a+b\sqrt{5}}{2} - \frac{c+d\sqrt{5}}{2} = \frac{(a-c)+(b-d)\sqrt{5}}{2}$. Este clar că $a-c, b-d \in \mathbb{Z}$ şi pentru că a şi b au aceeaşi paritate şi respectiv c şi d au aceeaşi paritate, atunci $a-c$ şi $b-d$ au aceeaşi paritate.
• A este parte stabilă în raport cu înmulţirea.

$$\frac{a+b\sqrt{5}}{2} \cdot \frac{c+d\sqrt{5}}{2} = \frac{(ac+5bd)+(ad+bc)\sqrt{5}}{4} = \frac{\frac{(ac+5bd)}{2} + \frac{(ad+bc)\sqrt{5}}{2}}{2}.$$

Considerăm cazul a şi b impare şi c şi d tot impare, $a = 2p+1, b = 2q+1, c = 2x+1, d = 2y+1$.

$$\frac{(ac+5bd)}{2} = \frac{4px+2p+2x+1+20qy+10q+10y+5}{2} = 2px+p+x+10qy+5q+5y+3 =$$

$$= 2px+10qy+p+x+4(q+y)+q+y+3 \in \; Z$$

,
Mai mult $\frac{(ac+5bd)}{2} \equiv_2 p+x+q+y+1$.

$$\frac{(ad+bc)}{2} = \frac{4py+2p+2y+1+4qx+2q+2x+1}{2} = 2py+p+y+2qx+q+x+1 \in \mathbb{Z}.$$

$$\frac{(ad+bc)}{2} = 2py+p+y+2qx+q+x+1 \equiv_2 p+y+q+x+1 \equiv_2 p+x+q+y+1 \equiv_2 \frac{(ac+5bd)}{2}.$$

Făcând calcule similare pentru celelate parităţi rezultă că $\frac{a+b\sqrt{5}}{2} \cdot \frac{c+d\sqrt{5}}{2} \in A$, deci A este parte stabilă faţă de " $\cdot$ ".
A este inel cu unitate, unitatea fiind $1 = \frac{2+0\sqrt{5}}{2}$, $2,\ 0 \in \mathbb{Z}, 2 \equiv_2 0$.
• $\frac{1+\sqrt{5}}{2}$ este inversabil, inversul acestuia este $\frac{-1+\sqrt{5}}{2}$ pentru că $\frac{1+\sqrt{5}}{2} \cdot \frac{-1+\sqrt{5}}{2} = \frac{-1^2+(\sqrt{5})^2}{4} = \frac{-1+5}{4} = 1$.
Toate elementele $(\frac{1+\sqrt{5}}{2})^k, k \in \mathbb{N}$ sunt inversabile cu inversele $(\frac{-1+\sqrt{5}}{2})^k$.

Problema 2. Arătaţi că $A = \{\frac{a+b\sqrt{7}}{2} \mid a, b \in \mathbb{Z}, a \equiv_2 b\}$ nu este subinel în $\mathbb{R}$.

Soluţie: • $(A,+)$ este subgrup al lui $\mathbb{R}$.
• A NU este parte stabilă faţă de $\cdot$. Voi da un exemplu:
$\frac{1+\sqrt{7}}{2} \cdot \frac{3+\sqrt{7}}{2} = \frac{3+7+\sqrt{7}+3\sqrt{7}}{4} = \frac{10+4\sqrt{7}}{4} = \frac{5+2\sqrt{7}}{2}$. $5, 2 \in \mathbb{Z}$, dar $5 \not\equiv_2 2$. Deci produsul elementelor NU este în A.

Problema 3. Fie A un inel şi $x \in A$ cu $x^n = 0$ pentru un anume $n \geqslant 1$ (un astfel de element se numeşte *element nilpotent*). Arătaţi că x este zero-divizor şi $1 + x$ este element inversabil.

Soluţie: Cel mai mic $n \geqslant 1$ cu proprietatea că $x^n = 0$ se numeşte ordin de nilpotenţă. Deci pentru n ordinul de nilpotenţă a lui x avem $x \cdot x^{n-1} = x^n = 0$. Deci $x \in Z(A)$, unde $Z(A)$ sunt divizorii lui 0 din inelul A.

$(1+x)(1-x+x^2-\ldots \pm x^{n-1}) = 1 \pm x^n = 1$, (+ pentru n impar şi $-$ pentru n par) pentru că $x^n = 0$.

Problema 4. Determinaţi elementele nilpotente din inelul $\mathbb{Z}_{12}$. Daţi un exemplu de zero-divizor care nu este nilpotent.

Soluţie: $Z(\mathbb{Z}_{12}) = \{\hat{k} \in \mathbb{Z}_{12} \mid (k, 12) \neq 1\} = \{\hat{2}, \hat{2}, \hat{3}, \hat{4}, \hat{6}, \hat{8}, \hat{9}, \hat{10}\}$.

$\hat{4}^2 = \hat{4} \Rightarrow \hat{4}^k = 4, (\forall) k \in \mathbb{N}$ este un zero-divizor care NU este nilpotent.

Problema 5. Fie $n \geqslant 2$. Arătaţi că $\hat{a} \in \mathbb{Z}_n$ este nilpotent dacă şi numai dacă a se divide cu toţi factorii primi ai lui n.

Soluţie: Vedem că se verifică afirmaţia din această problemă pentru $\hat{6} \in \mathbb{Z}_{12}$. $12 = 2^2 \cdot 3$ şi $6 = 2 \cdot 3$.

Considerăm descompunerea în factori primi ai lui $n, n = p_1^{s_1} p_2^{s_2} \ldots p_k^{s_k}, s_j \geqslant 1$.

"$\Rightarrow$" Fie $\hat{a} \in \mathbb{Z}_n$ nilpotent. Deci există $t \geqslant 2$ a.î. $\hat{a}^t = \hat{0} \Leftrightarrow a^t = q \cdot n$ pentru un $q \in \mathbb{N}$. Deci pentru $\forall 1 \leqslant j \leqslant k$, $p_j \mid a^t$, dar p_j este prim, de unde rezultă $p_j \mid a$.

"$\Leftarrow$" $a = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ cu $a_j \leqslant s_j$, $(\forall) j, 1 \leqslant j \leqslant k$. $a^u = (p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k})^u = p_1^{ua_1} p_2^{ua_2} \ldots p_k^{ua_k}$.

$\hat{a}$ este nilpotent cu ordinul de nilpotenţă cel mai mic u a.î. $ua_j \geqslant s_j$, $(\forall)\ j, 1 \leqslant j \leqslant k$.

Problema 6. Arătaţi că

$$A = \{\begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z}\}$$

este un subinel în $\mathcal{M}_2(\mathbb{R})$.

Soluţie: • $(A, +)$ este subgrup al $(\mathcal{M}_2(\mathbb{R}), +)$.

Fie $\begin{pmatrix} a & 0 \\ b & a \end{pmatrix}, \begin{pmatrix} c & 0 \\ d & c \end{pmatrix} \in A$. $\begin{pmatrix} a & 0 \\ b & a \end{pmatrix} - \begin{pmatrix} c & 0 \\ d & c \end{pmatrix} = \begin{pmatrix} a-c & 0 \\ b-d & a-c \end{pmatrix}$ cu $a-c, b-d \in \mathbb{Z}$.

• A parte stabilă faţă de "$\cdot$".

$\begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & 0 \\ d & c \end{pmatrix} = \begin{pmatrix} ac & 0 \\ bc+ad & ac \end{pmatrix}$, $ac, bc+ad \in \mathbb{Z}$.

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in A$.

Problema 7. Fie A inelul din problema precedentă. Determinaţi $U(A)$ şi $Z(A)$.

Soluţie:

• $U(A)$: Căutăm $\begin{pmatrix} a & 0 \\ b & a \end{pmatrix}$ a.î. $\exists \begin{pmatrix} x & 0 \\ y & x \end{pmatrix}$ cu proprietatea $\begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \cdot \begin{pmatrix} x & 0 \\ y & x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Leftrightarrow$ $\begin{pmatrix} ax & 0 \\ bx+ay & ax \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{cases} ax & = 1 \\ bx+ay & = 0 \end{cases}.$

Din prima ecuaţie, pentru că $a, x \in \mathbb{Z} \Rightarrow a = x \in \{\pm 1\}$ iar a doua ecuaţie devine $a(b+y) = 0 \Rightarrow b = -y$.

$U(A) = \{\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ b & -1 \end{pmatrix} \mid b \in \mathbb{Z}\}$. De menţionat că inversa matricei $\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$ este $\begin{pmatrix} 1 & 0 \\ -b & 1 \end{pmatrix}$, iar inversa matricei $\begin{pmatrix} -1 & 0 \\ b & -1 \end{pmatrix}$ este $\begin{pmatrix} -1 & 0 \\ -b & -1 \end{pmatrix}$.

$Z(A)$: Căutăm $\begin{pmatrix} a & 0 \\ b & a \end{pmatrix}$ a.î. $\exists \begin{pmatrix} x & 0 \\ y & x \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ cu proprietatea

$\begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \cdot \begin{pmatrix} x & 0 \\ y & x \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Leftrightarrow \begin{pmatrix} ax & 0 \\ bx+ay & ax \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow \begin{cases} ax & = 0 \\ bx+ay & = 0 \end{cases}$

Din prima ecuaţie avem $a = 0$ sau $x = 0$.

Presupunem $a \neq 0$, deci din prima ecuaţie rezultă $x = 0$. A doua ecuaţie devine $ay = 0$, de unde $y = 0$.

A rezultat $x = y = 0$, deci matricea 0_2, dar trebuie ca $\begin{pmatrix} x & 0 \\ y & x \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Deci $a = 0$. A doua ecuaţie devine $bx = 0$. a, b nu pot fi simultan nule, deci $x = 0$.

$Z(A) = \{\begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix} \mid b \in \mathbb{Z}\}$.

Problema 8. Arătaţi că

$$F = \{\begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \mid a, b \in \mathbb{Z}_2\}$$

este un subinel în $\mathcal{M}_2(\mathbb{Z}_2)$. Este F corp ?

Soluţie: • $(F, +)$ este subgrup al $(\mathcal{M}_2(\mathbb{Z}_2), +)$.

$\begin{pmatrix} a & b \\ b & a+b \end{pmatrix} - \begin{pmatrix} c & d \\ d & c+d \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ b-d & a+b-c-d \end{pmatrix}$ cu $a-c, b-d \in \mathbb{Z}_2$.

• F este parte stabilă în raport cu "$\cdot$".

$\begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \cdot \begin{pmatrix} c & d \\ d & c+d \end{pmatrix} = \begin{pmatrix} ac+bd & ad+bc+bd \\ bc+ad+bd & bd+ac+ad+bc+bd \end{pmatrix} \in F.$

Considerăm $\begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \in F \backslash \{0_2\}$, deci a, b nu sunt simultan $\hat{0}$.

$\det \begin{pmatrix} a & b \\ b & a+b \end{pmatrix} = a(a+b) - b^2 = a^2 + ab + b^2$ (lucrăm peste $\mathbb{Z}_2$). Cantitatea $a^2 + ab + b^2 = \hat{0} \Leftrightarrow a = b = \hat{0}$, ceea ce nu este adevărat. Astfel $\det \neq \hat{0}$, adică $\det \begin{pmatrix} a & b \\ b & a+b \end{pmatrix} = \hat{1}$ şi deci matricea este inversabilă. Deci F este corp. Elementele lui F sunt:

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

SEMINAR 11

Problema 1. Determinaţi idealele inelului $\mathbb{Z}_{12}$.

Soluţie: $\mathbb{Z}_{12} = \mathbb{Z}/12\mathbb{Z}$. Din teorema de corespondenţă idealele $\overline{J}$ ale inelului $\mathbb{Z}_{12}$ sunt în bijecţie cu idealele J, $12\mathbb{Z} \subset J \subset \mathbb{Z}$. Dintr-un rezultat de la curs ştim că toate idealele inelului $\mathbb{Z}$ sunt de forma $n\mathbb{Z}$. Incluziunea $12\mathbb{Z} \subset n\mathbb{Z}$ implică $n|12$, de unde $n \in \{1, 2, 3, 4, 6, 12\}$.
Deci idealele $\overline{J} \subset \mathbb{Z}_{12}$ sunt $\mathbb{Z}/12\mathbb{Z}, 2\mathbb{Z}/12\mathbb{Z}, 3\mathbb{Z}/12\mathbb{Z}, 4\mathbb{Z}/12\mathbb{Z}, 6\mathbb{Z}/12\mathbb{Z}, 12\mathbb{Z}/12\mathbb{Z}$.

Problema 2. Determinaţi idealele (stângi/drepte/bilaterale) ale inelului de matrice $\mathcal{M}_2(\mathbb{Z}_2)$.

Soluţie: $\mathbb{Z}_2 = \{\hat{0}, \hat{1}\}$, $|\mathbb{Z}_2| = 2$ de unde $|\mathcal{M}_2(\mathbb{Z}_2)| = 16$. Voi scrie tabla înmulţirii pe $\mathcal{M}_2(\mathbb{Z}_2)$. Elementele inelului $\mathcal{M}_2(\mathbb{Z}_2)$ sunt $0 = \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}$, $A_1 = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}$, $A_2 = \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{0} & \hat{0} \end{pmatrix}$, $A_3 = \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{1} & \hat{0} \end{pmatrix}$, $A_4 = \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}$, $A_5 = \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{0} & \hat{0} \end{pmatrix}$, $A_6 = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{1} & \hat{0} \end{pmatrix}$, $I = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}$, $A_7 = \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}$, $A_8 = \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{0} & \hat{1} \end{pmatrix}$, $A_9 = \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{1} & \hat{1} \end{pmatrix}$, $A_{10} = \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix}$, $A_{11} = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{1} & \hat{1} \end{pmatrix}$, $A_{12} = \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{0} & \hat{1} \end{pmatrix}$, $A_{13} = \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}$, $1 = \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix}$.

Tabla înmulţirii este:

$\cdot$	0	A_1	A_2	A_3	A_4	A_5	A_6	I	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A_1	0	A_1	A_2	0	0	A_5	A_1	A_1	A_2	A_2	0	A_2	A_1	A_5	A_5	A_5
A_2	0	0	0	A_1	A_2	0	A_1	A_2	A_1	A_2	A_5	A_5	A_5	A_2	A_1	A_5
A_3	0	A_3	A_4	0	0	A_9	A_3	A_3	A_4	A_4	0	A_4	A_3	A_9	A_9	A_9
A_4	0	0	0	A_3	A_4	0	A_3	A_4	A_3	A_4	A_9	A_9	A_9	A_4	A_3	A_9
A_5	0	A_1	A_2	A_1	A_2	A_5	0	A_5	A_5	0	A_5	A_1	A_2	A_1	A_2	0
A_6	0	A_6	A_8	0	0	1	A_6	A_6	A_8	A_8	0	A_8	A_6	1	1	1
I	0	A_1	A_2	A_3	A_4	A_5	A_6	I	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	1
A_7	0	A_3	A_4	A_1	A_2	A_9	A_6	A_7	I	A_8	A_5	A_{12}	A_{13}	A_{10}	A_{11}	1
A_8	0	0	0	A_6	A_8	0	A_6	A_8	A_6	A_8	1	1	1	A_8	A_6	1
A_9	0	A_3	A_4	A_3	A_4	A_9	0	A_9	A_9	0	A_9	A_3	A_4	A_3	A_4	0
A_{10}	0	A_3	A_4	A_6	A_8	A_9	A_1	A_{10}	A_{11}	A_2	1	A_{13}	A_{12}	A_7	I	A_5
A_{11}	0	A_6	A_8	A_3	A_4	1	A_1	A_{11}	A_{10}	A_2	A_9	A_7	I	A_{13}	A_{12}	A_5
A_{12}	0	A_1	A_2	A_6	A_8	A_5	A_3	A_{12}	A_{13}	A_4	1	A_{11}	A_{10}	I	A_7	A_9
A_{13}	0	A_6	A_8	A_1	A_2	1	A_3	A_{13}	A_{12}	A_4	A_5	I	A_7	A_{11}	A_{10}	A_9
1	0	A_6	A_8	A_6	A_8	1	0	1	1	0	1	A_6	A_8	A_6	A_8	0

Ideale la dreapta: $\{0, A_1, A_2, A_5\}$, $\{0, A_3, A_4, A_9\}$, $\{0, A_6, A_8, 1\}$
Ideale la stânga: $\{0, A_1, A_3, A_6\}$, $\{0, A_2, A_4, A_8\}$, $\{0, A_5, A_9, 1\}$
Singulerele ideale bilaterale sunt 0 şi inelul $\mathcal{M}_2(\mathbb{Z}_2)$.

Problema 3. Arătaţi că idealul generat de 2 şi X în $\mathbb{Z}[X]$ nu este principal.

Soluţie: Un ideal principal este un ideal generat de un singur element. Idealul generat de 2 şi X, $I =< 2, X >$ este diferit de tot inelul $\mathbb{Z}[X]$ (1 nu se scrie ca o combinaţie de 2 şi X cu coeficienţi polinoame).

Presupunem că $I =< 2, X >=< f >$, deci în particular $< 2, X >\subset< f >\Rightarrow f|X$ şi $f|2$. Din $f|X \Rightarrow f = \pm 1$ sau $f = \pm X$. Dar cum $I \neq \mathbb{Z}[X]$, $f \neq \pm 1$, deci $f = \pm X$. Relaţia $f|2$ devine $\pm X|2$, ceea ce este o contradicţie. Deci I nu este principal.

Problema 4. Fie A şi B două inele comutative. Arătaţi că idealele inelului produs direct $A\times B$ sunt de forma $I \times J$ cu I ideal al lui A şi J ideal a lui B.

Soluţie: Demonstrăm că $I \times J$ este ideal în inelul $A \times B$.

Considerăm morfismul de inele $\varphi : A \times B \longrightarrow A/I \times B/J, \varphi(a, b) = (a + I, b + J)$. Este un morfism surjectiv de inele, iar $\text{Ker}(\varphi) = I \times J$, este ideal în $A \times B$ (ca nucleul unui morfism de inele).

Demonstrăm acum că orice ideal din inelul $A \times B$ este produs direct de ideale din cele două inele. Fie $K \subset A \times B$, ideal. Considerăm morfismele proiecţie pe cei doi factori $p : A \times B \longrightarrow A$ şi $q : A \times B \longrightarrow B$.

Arătăm că $K = p(K) \times q(K)$.

Fie $(x, y) \in K, (x, y) = (x, 0) + (0, y)$, deci $K \subset p(K) \times q(K)$.

Fie $(x, y), (x', y') \in K$, arbitrare şi deci $(x, y') \in p(K) \times q(K)$ un element arbitrar.

$(x, y') = (1, 0)(x, y) + (0, 1)(x', y') \in K$. De aici egalitatea $K = p(K) \times q(K)$.

Problema 5. Determinanţi idealele inelului produs direct $\mathbb{Z} \times \mathbb{Q}$.

Soluţie: Singurele ideale ale unui corp k sunt 0 şi k. Deci, folosind **problema 4** idealele inelului $\mathbb{Z} \times \mathbb{Q}$ sunt $0, n\mathbb{Z} \times \mathbb{Q}, n \geqslant 1$.

Problema 6. Arătaţi că nu există morfisme de inele între $\mathbb{Z}[i]$ şi $\mathbb{Q}$. ($i = \sqrt{-1}$).

Soluţie: $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ este inelul întregilor lui Gauss.

Un morfism de inele $f : \mathbb{Z}[i] \longrightarrow \mathbb{Q}$ are proprietatea $f(1) = 1$ (1 este unitatea faţă de înmulţire atât în $Z[i]$ cât şi în $\mathbb{Q}$). $f(2) = f(1 + 1) = f(1) + f(1) = 2$.

Fie $f(i) = x \in \mathbb{Q}$, valoarea elementului i prin morfismul f.

Dar $2 = (1 + i)(1 - i)$. De aici $2 = f(2) = f((1 + i)(1 - i)) = f(1 + i)f(1 - i) = (f(1) + f(i))(f(1) - f(i)) = (1 + x)(1 - x) = 1 - x^2$. Deci $x^2 = -1$ cu $x \in \mathbb{Q}$. Absurd.

Deci nu există morfism de inele $f : \mathbb{Z}[i] \longrightarrow \mathbb{Q}$.

Problema 7. Calculaţi tablele de adunare şi înmulţire ale inelului factor $\mathbb{Z}[i]/ < 2 >$. Câte ideale are acest inel ?

Soluţie: Avem următoarele clase în $\mathbb{Z}[i]/ < 2 >$.

- $a = 2p, b = 2q, p, q \in \mathbb{Z}$; $\widehat{a + bi} = \widehat{0}$,
- $a = 2p + 1, b = 2q, p, q \in \mathbb{Z}$; $\widehat{a + bi} = \widehat{1}$,
- $a = 2p, b = 2q + 1, p, q \in \mathbb{Z}$; $\widehat{a + bi} = \widehat{i}$,
- $a = 2p + 1, b = 2q + 1, p, q \in \mathbb{Z}$; $\widehat{a + bi} = \widehat{1 + i}$.

Tabla adunării:

$+$	$\hat{0}$	$\hat{1}$	$\hat{i}$	$\widehat{1+i}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{i}$	$\widehat{1+i}$
$\hat{1}$	$\hat{1}$	$\hat{0}$	$\widehat{1+i}$	$\hat{i}$
$\hat{i}$	$\hat{i}$	$\widehat{1+i}$	$\hat{0}$	$\hat{1}$
$\widehat{1+i}$	$\widehat{1+i}$	$\hat{i}$	$\hat{1}$	$\hat{0}$

Tabla înmulţirii:

$\cdot$	$\hat{0}$	$\hat{1}$	$\hat{i}$	$\widehat{1+i}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{i}$	$\widehat{1+i}$
$\hat{i}$	$\hat{0}$	$\hat{i}$	$\hat{1}$	$\widehat{1+i}$
$\widehat{1+i}$	$\hat{0}$	$\widehat{1+i}$	$\widehat{1+i}$	$\hat{0}$

Idealele inelului $\mathbb{Z}[i]/ < 2 >$ sunt $\hat{0}$, $\mathbb{Z}[i]/ < 2 >= \{\hat{0}, \hat{1}, \hat{i}, \widehat{1+i}\}$ şi $< 1+i >= \{\hat{0}, \widehat{1+i}\}$. Deci inelul are trei ideale, toate bilaterale, inelul fiind comutativ.

Problema 8. Arătaţi că
(i) funcţia $f : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_5, f(a+bi) = \widehat{a+2b}$ este morfism de inele.
(ii) Inelul factor $\mathbb{Z}[i]/ < 2-i >$ este izomorf cu $\mathbb{Z}_5$.

Soluţie:
(i) $f((a+bi)+(c+di)) = f((a+c)+(b+d)i) = (a+c)\widehat{+2}(b+d) = a+2\widehat{b+c}+2d = \widehat{a+2b}+\widehat{c+2d} = f(a+bi)+f(c+di)$.

$f((a+bi)\cdot(c+di)) = f((ac-bd)+(ad+bc)i) = (ac-bd)\widehat{+2}(ad+bc) = (ac+4bd)\widehat{+2}(ad+bc)$ (în $\mathbb{Z}_5, -1 \equiv_5 4$) $= (a+\widehat{2b)(c}+2d) = (\widehat{a+2b})\cdot(\widehat{c+2d}) = f(a+bi)\cdot f(c+di)$.

$f(0) = \hat{0}, f(1) = \hat{1}$.

(ii) Morfismul este surjectiv deoarece pentru $(\forall)\hat{x} \in \mathbb{Z}_5, (\exists)x+0i \in \mathbb{Z}[i]$, a.î. $f(x+0i) = \widehat{x+2\cdot 0} = \hat{x}$.

" $\mathrm{Ker}(f) =< 2-i >$ "

" $\subseteq$ " Fie $a+bi \in \mathbb{Z}[i] \Leftrightarrow \widehat{a+2b} = \hat{0} \in \mathbb{Z}_5 \Leftrightarrow a+2b = 5k, k \in \mathbb{Z} \Leftrightarrow a = 5k-2b$.

Deci un element arbitrar din $\mathrm{Ker}(f)$ este de forma $(5k-2b)+bi, b, k \in \mathbb{Z}$. Pentru a arăta incluziunea trebuie să vedem că $(5k-2b)+bi \in< 2-i >$, adică trebuie să găsim $m, n \in \mathbb{Z}$ a.î. $(5k-2b)+bi = (m+ni)(2-i) \Leftrightarrow (5k-2b)+bi = (2m+n)+(-m+2n)i$.

Sistemul $\begin{cases} 2m+n & = & 5k-2b \\ -m+2n & = & b \end{cases}$. Înmulţim cu 2 ecuaţia a doua şi adunăm cele două ecuaţii. Obţinem $n = k$. Introducând în prima ecuaţie obţinem $m = 2k-b$.

Deci $(5k-2b)+bi = ((2k-b)+ki)(2-i) \in< 2-i >$.

" $\supseteq$ " Este suficient să verificăm că $(2-i) \in \mathrm{Ker}(f)$. $f(2-i) = 2\widehat{+2(-}1) = \widehat{2-2} = \hat{0}$.

Din teorema fundamentală de izomorfism pentru inele rezultă că $\mathbb{Z}[i]/ < 2-i > \simeq \mathbb{Z}_5$.

Problema 9. Arătaţi că inelul factor $\mathbb{Z}[i]/ < 2+2i >$ nu este izomorf cu $\mathbb{Z}_8$.

Soluţie: Inelul $\mathbb{Z}_8$ are zero-divizori $\{\hat{2}, \hat{4}, \hat{6}\}$, dar şi elementele nilpotente $\hat{2}$ cu ordinul de nilpotenţă 3 şi $\hat{4}$ cu ordinul de nilpotenţă 2.

Arătăm că în $\mathbb{Z}[i]/ < 2+2i >$ nu există nilpotenţi de ordin 2.

Considerăm $a+bi \notin < 2+2i > \Leftrightarrow a, b$ nu sunt simultan pare (adică $a+bi \neq 0 \in \mathbb{Z}[i]/ < 2+2i >$). Arătăm că $(a+bi)^2 \neq 0$ în $\mathbb{Z}[i]/ < 2+2i >$.

Presupunem că $(a+bi)^2 = 0 \in \mathbb{Z}[i]/ < 2+2i > \Leftrightarrow (\exists) m, n \in \mathbb{Z}$ a.î. $(a+bi)^2 = (2+2i)(m+ni) \Leftrightarrow (a^2-b^2) + 2abi = 2(m-n) + 2(m+n)i$.

Cum a, b nu sunt simultan pare avem trei cazuri:

• $a = 2p+1$, $b = 2q$

$a^2 - b^2 = 4p^2 + 4p + 1 - 4q^2$ este impar deci nu poate fi egal cu $2(m-n)$.

• $a = 2p$, $b = 2q+1$

$a^2 - b^2$ este impar (similar calcului de mai sus).

• $a = 2p+1$, $b = 2q+1$

$a^2 - b^2 = 4p^2 + 4p + 1 - 4q^2 - 4q - 1 = 4(p^2 - q^2) + 4(p-q) = 4(p-q)(p+q+1)$,

$2ab = 2(2p+1)(2q+1)$.

Obţinem sistemul $\begin{cases} 2(m-n) & = & 4(p-q)(p+q+1) \\ 2(m+n) & = & 2(2p+1)(2q+1) \end{cases} \Leftrightarrow \begin{cases} m-n & = & 2(p-q)(p+q+1) \\ m+n & = & (2p+1)(2q+1) \end{cases}$

Adunând cele două ecuaţii obţinem $2m = 2(p-q)(p+q+1) + (2p+1)(2q+1) \Leftrightarrow 2m - 2(p-q)(p+q+1) = (2p+1)(2q+1)$, adică un număr par este egal cu un număr impar, ceea ce este absurd.

Deci $\mathbb{Z}[i]/ < 2+2i >$ nu are nilpotenţi de ordin 2, deci nu poate fi izomorf cu $\mathbb{Z}_8$, care elementul $\widehat{4}$ nilpotent de ordin 2.

SEMINAR 12

Problema 1. Arătaţi că inelul $\mathbb{Z}_{1001}$ este izomorf cu un produs direct de corpuri.

Soluţie: Se aplică Corolarul 2 din Cursul 12 pentru inelul $A = \mathbb{Z}$, şi elementele $7, 11, 13 \in \mathbb{Z}\backslash\{\pm 1\}$, care sunt prime şi deci coprime.
$1001 = 7 \cdot 11 \cdot 13$ şi deci $\mathbb{Z}_{1001} \simeq \mathbb{Z}_7 \times \mathbb{Z}_{11} \times \mathbb{Z}_{13}$. 7, 11, 13 fiind numere prime rezultă că $\mathbb{Z}_7, \mathbb{Z}_{11}, \mathbb{Z}_{13}$ sunt corpuri.

Problema 2. Arătaţi că:
(i) $\widehat{77}$ este element nilpotent în inelul $\mathbb{Z}_{847}$,
(ii) inelul $\mathbb{Z}_{847}$ nu este izomorf cu un produs direct de corpuri.

Soluţie:
(i) $847 = 7 \cdot 11^2$. Problema 5 din Seminar 10 spune că $\hat{x} \in \mathbb{Z}_n$ este nilpotent dacă şi numai dacă x se divide cu toţi factorii primi ai lui n. $77 = 7 \cdot 11$ se divide cu 7 şi 11, factorii primi ai numărului 847. Deci $\widehat{77}$ este nilpotent.
$\widehat{77}^2 = \widehat{77^2} = \widehat{7^2 \cdot 11^2} = 7 \cdot \widehat{7 \cdot 11^2} = \hat{7} \cdot \widehat{7 \cdot 11^2} = \hat{7} \cdot \hat{0} = \hat{0}$. Deci ordinul de nilpotenţă este 2.
(ii) Aplicând acelaşi Corolar 2 din Curs 12, $\mathbb{Z}_{847} \simeq \mathbb{Z}_7 \times \mathbb{Z}_{121}$, dar $\mathbb{Z}_{121}$ nu este corp ($\widehat{11}$ este nilpotent, $\widehat{11}^2 = \hat{0}$).

Problema 3. Rezolvaţi sistemul de congruenţe în $\mathbb{Z}$:
$x \equiv 3 (\mathrm{mod}\, 5)$, $x \equiv 7 (\mathrm{mod}\, 11)$, $x \equiv 8 (\mathrm{mod}\, 13)$

Soluţie: Sistemul de nilpotenţe se rezolvă conform algoritmului din Curs 12.
$a = a_1 \cdot a_2 \cdot a_3 = 5 \cdot 11 \cdot 13 = 715$. $b_1 = \frac{a}{a_1} = \frac{715}{5} = 143$, $b_2 = \frac{a}{a_2} = \frac{715}{11} = 65$, $b_3 = \frac{a}{a_3} = \frac{715}{13} = 55$.
$b_1 \equiv_5 3$; c_1 inversul lui $3 (\mathrm{mod}\, 5)$ este 2.
$b_2 \equiv_{11} 10$; c_2 inversul lui $10 (\mathrm{mod}\, 11)$ este 10.
$b_3 \equiv_{13} 3$, c_3 inversul lui $3 (\mathrm{mod}\, 13)$ este 9.
$x = 143 \cdot 2 \cdot 3 + 65 \cdot 10 \cdot 7 + 55 \cdot 9 \cdot\ 8 = 9368 \equiv_{715} 73$.
Deci soluţia este $x = 73 + 715k, k \in \mathbb{Z}$.
Se verifică imediat că $73 \equiv 3 (\mathrm{mod}\, 5)$, $73 \equiv 7 (\mathrm{mod}\, 11)$ şi $73 \equiv 8 (\mathrm{mod}\, 13)$.

Problema 4. Arătaţi că numerele
(i) numerele $2 + i, 2 - i$ sunt comaximale în $\mathbb{Z}[i]$,
(ii) inelul factor $\mathbb{Z}[i]/ < 5 >$ este izomorf cu $\mathbb{Z}_5 \times \mathbb{Z}_5$. (folosiţi **problema 8** din seminarul 11).

Soluţie:
(i) Arătăm că idealele generate de cele elemente sunt comaximale.
$(2 + i) \cdot (-1) + (2 - i)(1 + i) = -2 - i + (2 + 1 + 2i - i = -2 - i + 3 + i = 1$. Deci cele două ideale generate de $(2 + i)$ şi $(2 - i)$ sunt comaximale.
(ii) Aplicăm Corolar 1 din Cursul 12 pentru inelul $\mathbb{Z}[i]$ şi elementele $(2 + i)$, $(2 - i)$ şi obţinem $\mathbb{Z}[i]/(2 + i)(2 - i)\mathbb{Z}[i] \simeq \mathbb{Z}[i]/(2 + i)\mathbb{Z}[i] \times \mathbb{Z}[i]/(2 - i)\mathbb{Z}[i]$.
$(2 + i)(2 - i) = 5$ şi izomorfismul de mai sus se scrie

$$\mathbb{Z}[i]/ < 5 > \simeq \mathbb{Z}[i]/ < (2 + i) > \times \mathbb{Z}[i]/ < (2 - i) >$$

Pentru a termina trebuie să demonstrăm că cele dpuă inele factor din membrul drept sunt fiecare izomorfe cu $\mathbb{Z}_5$. În Problema 8 din Seminar 11 am arătat că $\mathbb{Z}[i]/ < (2-i) > \simeq \mathbb{Z}_5$.

Similar vom demonstra că $\mathbb{Z}[i]/ < (2+i) > \simeq \mathbb{Z}_5$.

Considerăm $\alpha : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_5, \alpha(a+bi) = \widehat{a-2b}$.

• Arătăm că α este morfism.

$\alpha((a+bi)+(c+di)) = \alpha((a+c)+(b+d)i) = \widehat{(a+c)-2(b+d)} = \widehat{(a-2b)+(c-2d)} = \widehat{a-2b} + \widehat{c-2d} = \alpha(a+bi) + \alpha(c+di)$.

$\alpha((a+bi)\cdot(c+di)) = \alpha((ac-bd)+(ad+bc)i) = \widehat{(ac-bd)-2(ad+bc)} = \widehat{(ac+4bd)-2(ad+bc)}$ (în $\mathbb{Z}_5, -1 \equiv_5 4$) $= \widehat{(a-2b)(c-2d)} = \widehat{(a-2b)} \cdot \widehat{(c-2d)} = \alpha(a+bi)\cdot\alpha(c+di)$.

$\alpha(0) = \widehat{0}, \alpha(1) = \widehat{1}$.

• α este surjectiv pentru că $(\forall)\widehat{a} \in \mathbb{Z}_5$, $(\exists) a+0i \in \mathbb{Z}[i]$ a.î. $\alpha(a+0i) = \widehat{a}$.

• $\mathrm{Ker}(\alpha) =< (2+i) >$.

" $\subseteq$ " Fie $a+bi \in \mathbb{Z}[i] \Leftrightarrow \widehat{a-2b} = \widehat{0} \in \mathbb{Z}_5 \Leftrightarrow a-2b = 5k, k \in \mathbb{Z} \Leftrightarrow a = 2b+5k$.

Deci un element arbitrar din $\mathrm{Ker}(f)$ este de forma $(2b+5k)+bi, b, k \in \mathbb{Z}$. Pentru a arăta incluziunea trebuie să vedem că $(5k+2b)+bi \in < 2+i >$, adică trebuie să găsim $m, n \in \mathbb{Z}$ a.î. $(5k+2b)+bi = (m+ni)(2+i) \Leftrightarrow (5k+2b)+bi = (2m+n)+(-m+2n)i$.

Sistemul $\begin{cases} 2m-n &= 5k+2b \\ m+2n &= b \end{cases}$. Înmulţim cu 2 prima ecuaţie şi adunăm cele două ecuaţii. Obţinem $m = 2k+b$. Introducând în a doua ecuaţie obţinem $n = -k$.

Deci $(5k+2b)+bi = ((2k+b)-ki)(2+i) \in < 2+i >$.

" $\supseteq$ " Este suficient să verificăm că $2+i \in \mathrm{Ker}(\alpha)$. $\alpha(2+i) = \widehat{2-2\cdot 1} = \widehat{2-2} = \widehat{0}$.

Din teorema fundamentală de izomorfism pentru inele rezultă că $\mathbb{Z}[i]/ < 2-i > \simeq \mathbb{Z}_5$.

Deci $\mathbb{Z}[i]/ < 5 > \simeq \mathbb{Z}_5 \times \mathbb{Z}_5$.

Problema 5. Aplicaţi Lema Chineză a Resturilor pentru idealele $I =< 2, 1+\sqrt{-5} >$, $J =< 3, 1+\sqrt{-5} >$ în inelul $\mathbb{Z}[\sqrt{-5}]$ pentru a deduce că inelul factor $\mathbb{Z}[\sqrt{-5}]/ < 1+\sqrt{-5} >$ este izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Soluţie: Pentru a aplica LCR trebuie să demonstăm că $I+J = \mathbb{Z}[\sqrt{-5}]$. Avem $2\cdot(-1)+3\cdot 1 = 1$. Deci I şi J sunt comaximale.

Din LCR rezultă că $\mathbb{Z}[\sqrt{-5}]/(I \cap J) \simeq \mathbb{Z}[\sqrt{-5}]/I \times \mathbb{Z}[\sqrt{-5}]/J$.

Trebuie să arătăm că: $I \cap J =< 1+\sqrt{-5} >$, $\mathbb{Z}[\sqrt{-5}]/I \simeq \mathbb{Z}_2$ şi $\mathbb{Z}[\sqrt{-5}]/J \simeq \mathbb{Z}_3$.

• $I \cap J =< 1+\sqrt{-5} >$.

" $\supseteq$ " $1+\sqrt{-5} \in I, 1+\sqrt{-5} \in J \Rightarrow < 1+\sqrt{-5} > \subseteq I \cap J$.

" $\subseteq$ " Fie $u \in I \cap J$. $u = 2p+(1+\sqrt{-5})q; p, q \in \mathbb{Z}[\sqrt{-5}]$ şi $u = 3s+(1+\sqrt{-5})t; s, t \in \mathbb{Z}[\sqrt{-5}]$. Deci $u = 2(a+b\sqrt{-5})+(1+\sqrt{-5})(c+d\sqrt{-5}); a, b, c, d \in \mathbb{Z}$ şi
$u = 3(x+y\sqrt{-5})+(1+\sqrt{-5})(z+w\sqrt{-5}); x, y, z, w \in \mathbb{Z}$.

Făcând calculele şi adunând termenii asemenea va rezulta sistemul
$\begin{cases} 2a+c-5d &= 3x+z-5w \\ 2b+c+d &= 3y+z+w \end{cases}$.

Scădem ecuaţia a doua din prima şi obţinem $2(a-b)-6d = 3(x-y)-6w \Leftrightarrow 2(a-b) = 3[(x-y)+2(d-w)]$, toate numerele fiind în $\mathbb{Z}$. De aici $(a-b) = 3k, k \in \mathbb{Z}$, deci $a = 3k+b$.

Am obţinut $u = 2(3k+b+b\sqrt{-5})+(1+\sqrt{-5})q = 6k+2b(1+\sqrt{-5})+(1+\sqrt{-5})q = (1+\sqrt{-5})(1-\sqrt{-5})k+2b(1+\sqrt{-5})+(1+\sqrt{-5})q = (1+\sqrt{-5})[(1-\sqrt{-5})k+2b+q]$. Paranteza dreaptă reprezintă un element din $\mathbb{Z}[\sqrt{-5}]$.

Deci am arătat că $u \in < 1+\sqrt{-5} >$.

• $\mathbb{Z}[\sqrt{-5}]/I \simeq \mathbb{Z}_2$.

Considerăm morfismul $\beta : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}_2, \beta(a + b\sqrt{-5}) = \widehat{a+b}$. Trebuie arătat că β este morfism surjectiv de inele şi $\mathrm{Ker}(\beta) = I$.

$\beta((a+b\sqrt{-5})+(c+d\sqrt{-5})) = \beta((a+c)+(b+d)\sqrt{-5}) = \widehat{(a+c)+(b+d)} = \widehat{(a+b)+(c+d)} = \widehat{a+b} + \widehat{c+d} = \beta(a+b\sqrt{-5}) + \beta(c+d\sqrt{-5})$

$\beta((a+b\sqrt{-5}) \cdot (c+d\sqrt{-5})) = \beta((ac-5bd)+(ad+bc)\sqrt{-5}) = \widehat{(ac-5bd)+(ad+bc)} = (-5 \equiv_2 1) = \widehat{(ac+bd)+(ad+bc)} = \widehat{a(c+d)+b(c+d)} = \widehat{(a+b)(c+d)} = \widehat{(a+b)} \cdot \widehat{(c+d)} = \beta(a+b\sqrt{-5}) \cdot \beta(c+d\sqrt{-5})$.

$\beta(0) = \hat{0}, \beta(1) = \hat{1}$ ceea ce implică şi faptul că β este surjectiv.

$\mathrm{Ker}(\beta) = I$.

" $\supseteq$ " $\beta(2) = \hat{2} = \hat{0}, \beta(1+\sqrt{-5}) = \widehat{1+1} = \hat{2} = \hat{0}$.

" $\subseteq$ " Fie $a+b\sqrt{-5} \in \mathrm{Ker}(\beta) \Leftrightarrow \widehat{a+b} = \hat{0} \Leftrightarrow a+b = 2k \Leftrightarrow a = -b+2k$. Deci un element arbitrar din $\mathrm{Ker}(\beta)$ este de forma $-b+2k+b\sqrt{-5} = -2b+2k+b+b\sqrt{-5} = 2(-b+k)+(1+\sqrt{-5})b \in I$.

Din teorema fundamentală de izomorfism pentru inele obţinem $\mathbb{Z}[\sqrt{-5}]/I \simeq \mathbb{Z}_2$.

• $\mathbb{Z}[\sqrt{-5}]/J \simeq \mathbb{Z}_3$.

Considerăm morfismul $\gamma : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}_3, \gamma(a + b\sqrt{-5}) = \widehat{a+2b}$.

Se demonstrează ca şi mai sus că γ este morfism surjectiv de inele şi $\mathrm{Ker}(\gamma) = J$.

$\gamma((a+b\sqrt{-5}) \cdot (c+d\sqrt{-5})) = \gamma((ac-5bd)+(ad+bc)\sqrt{-5}) = \widehat{(ac-5bd)+2(ad+bc)} = (-5 \equiv_3 1 \equiv_3 4) = \widehat{(ac+4bd)+2(ad+bc)} = \widehat{a(c+2d)+2b(c+2d)} = \widehat{(a+2b)(c+2d)} = \widehat{(a+2b)} \cdot \widehat{(c+2d)} = \gamma(a+b\sqrt{-5}) \cdot \gamma(c+d\sqrt{-5})$.

Problema 6. Găsiţi un idempotent netrivial în inelul $\mathbb{Z}[\sqrt{-5}]/ < 1+\sqrt{-5} >$.

Soluţie: În problema precedentă am arătat că $\mathbb{Z}[\sqrt{-5}]/ < 1+\sqrt{-5} > \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$. Un idemponent netrivial în $\mathbb{Z}_2 \times \mathbb{Z}_3$ este $(\hat{1}, \overline{0})$. Elementul corespunzător perechii $(\hat{1}, \overline{0})$ în $\mathbb{Z}[\sqrt{-5}]/ < 1+\sqrt{-5} >$ este 3.

Să vedem că este idempotent.

$3^2 = 9 = 3+6$. Dar $6 \equiv_{1+\sqrt{-5}} = 0 (6 = (1+\sqrt{-5})(1-\sqrt{-5}))$. Deci $3^2 \equiv_{1+\sqrt{-5}} 3$, adică clasa lui 3 este idempotent.

Problema 7. Aplicaţi Lema Chineză a Resturilor pentru idealele $I =< X >, J =< X-1 >$ în inelul $\mathbb{Z}[X]$ pentru a deduce că inelul factor $\mathbb{Z}[X]/ < X^2 - X >$ este izomorf cu $\mathbb{Z} \times \mathbb{Z}$.

Soluţie: I şi J sunt comaximale pentru că $X \cdot 1 + (X-1) \cdot (-1) = X - X + 1 = 1$.

Folosind Corolar 1 din Curs 12 obţinem

$$\mathbb{Z}[X]/X(X-1)\mathbb{Z}[X] \simeq \mathbb{Z}[X]/X\mathbb{Z}[X] \times \mathbb{Z}[X]/(X-1)\mathbb{Z}[X]$$

. Trebuie să arătăm izomorfismele $\mathbb{Z}[X]/X\mathbb{Z}[X] \simeq \mathbb{Z}$ şi $\mathbb{Z}[X]/(X-1)\mathbb{Z}[X] \simeq \mathbb{Z}$.

• $\mathbb{Z}[X]/ < X > \simeq \mathbb{Z}$.

Considerăm aplicaţia $\delta : \mathbb{Z}[X] \longrightarrow \mathbb{Z}$, $\delta(f(X)) = f(0)$, unde $f(X) \in \mathbb{Z}[X]$.

Dacă $f(X) = \sum_{i=0}^{n} a_i X^i$, atunci $\delta(f(X)) = a_0$. δ este morfism de inele.

$\delta(f(X) + g(X)) = \delta(\sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{p} b_i X^i) = \delta(\sum_{i=0}^{\max\{n,p\}} (a_i + b_i) X^i) = a_0 + b_0$
$= \delta(f(X)) + \delta(g(X))$

$\delta(f(X) \cdot g(X)) = \delta(\sum_{i=0}^{n+p} (\sum_{h+k=i} a_h b_k) X^i) = a_0 b_0 = \delta(f(X))\delta(g(X))$.

Pentru orice polinom constant c, $\delta(c) = c$. Acest lucru arată că δ este surjectiv. Pentru $\forall c \in \mathbb{Z}, \exists c \in \mathbb{Z}[X]$ a.î. $\delta(c) = c$.

$\delta(X) = 0 \Rightarrow < X > \subset \mathrm{Ker}(\delta)$.

Fie $f(X) \in \mathrm{Ker}(\delta)$, deci $\delta(f(X)) = 0 \Leftrightarrow f(0) = 0 \Leftrightarrow X \mid f(X) \Leftrightarrow f(X) = X \cdot g(X)$, cu $g(X) \in \mathbb{Z}[X] \Leftrightarrow f(X) \in < X >$. Deci $\mathrm{Ker}(\delta) \subset < X >$.

Din teorema fundamentală de izomorfism obţinem $\mathbb{Z}[X]/ < X > \simeq \mathbb{Z}$.

• $\mathbb{Z}[X]/ < X - 1 > \simeq \mathbb{Z}$.

Se consideră aplicaţia $\tau : \mathbb{Z}[X] \longrightarrow \mathbb{Z}, \tau(f(X)) = f(1)$.

• Fie $c \in \mathbb{Z}$, în acest caz $\tau(c) = c$. Deci τ este surjectiv.

• $\tau(f(X) \cdot g(X)) = \tau(\sum_{k=0}^{n+p}(\sum_{i+j=k} a_i b_j)X^k) = \sum_{k=0}^{n+p}(\sum_{i+j=k} a_i b_j) = (a_0 + a_1 + \ldots + a_n)(b_0 + b_1 + \ldots + b_p) = f(1)g(1) = \tau(f(X))\tau(g(X))$.

• $\mathrm{Ker}(\tau) = < X - 1 >$.

" $\subset$ " Fie $f(X) \in \mathrm{Ker}(\tau) \Leftrightarrow \tau(f(X)) = 0 \Leftrightarrow f(1) = 0 \Rightarrow (X - 1) \mid f(X)$ (teorema Bezout) $\Leftrightarrow f(X) = (X - 1)g(X) \Leftrightarrow f(X) \in < X - 1 >$

" $\supset$ " $\tau(X - 1) = 1 - 1 = 0 \Rightarrow (X - 1) \in \mathrm{Ker}(\tau) \Leftrightarrow < X - 1 > \subset \mathrm{Ker}(\tau)$.

Din teorema fundamentală de izomorfism rezultă că $\mathbb{Z}[X]/ < X - 1 > \simeq \mathbb{Z}$.

Problema 8. Arătaţi că inelul factor $\mathbb{Z}[X]/ < X^2 - 1 >$ nu este izomorf cu $\mathbb{Z} \times \mathbb{Z}$.

Soluţie: În inelul factor $\overline{X^2} = \overline{1}$, deci în acest inel factor polinoamele au cel mult grad 1. Voi lucra cu clase modulo $< X^2 - 1 >$, fără a mai folosi notaţia bar.

$\mathbb{Z} \times \mathbb{Z}$ are patru idempotenţi $(0, 0), (1, 0), (0, 1), (1, 1)$.

Fie $a + bX \in \mathbb{Z}[X]/ < X^2 - 1 >$.

Este idempotent dacă verifică relaţia $(a + bX)^2 = a + bX \Leftrightarrow a^2 + 2abX + b^2 = a + bX \Leftrightarrow \begin{cases} a^2 + b^2 & = & a \\ 2ab & = & b \end{cases}$. A doua ecuaţie este $b(2a - 1) = 0$, cu $a, b \in \mathbb{Z}$. Deci $a \neq \frac{1}{2}$, de unde singura posibilitate este $b = 0$.

Prima ecuaţie devine $a^2 - a = 0$, adică $a \in \{0, 1\}$. Deci idempotenţii din $\mathbb{Z}[X]/ < X^2 - 1 >$ sunt 0 şi 1. Deci $\mathbb{Z}[X]/ < X^2 - 1 >$ are numai doi idempotenţi faţă de $\mathbb{Z} \times \mathbb{Z}$ care are patru.

Deci inelele nu pot fi izomorfe.

Avem $\mathbb{Z}[X]/ < X^2 - 1 > \simeq A = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x - y \text{ par}\}$ izomorfism care se demonstrează folosind aplicaţia $\tau : \mathbb{Z}[X] \longrightarrow A,\ \tau(f(X)) = (f(1), f(-1))$. Se demonstrează similar ca în **problema 7** că τ este morfism de inele, este surjectiv şi $\mathrm{Ker}(\tau) = < X^2 - 1 >$.

SEMINAR 13

Problema 1. Calculaţi caracteristica inelelor $\mathbb{Z}_2 \times \mathbb{R}, \mathbb{Z}_4 \times \mathbb{Z}_6$ şi $\mathbb{Z}[i]/ < 2+2i >$.

Soluţie: $\text{car}(\mathbb{Z}_2 \times \mathbb{R}) = 0$.

$\text{ord}(\hat{1}, \bar{1}) = [\text{ord}(\hat{1}), \text{ord}(\bar{1})] = [4, 6] = 12 \Rightarrow \text{car}(\mathbb{Z}_4 \times \mathbb{Z}_6) = 12$.

Notăm $L = \mathbb{Z}[i]/ < 2+2i >$. $\text{car}(L) = \text{ord}(1_L)$ în grupul aditiv $(L, +)$. Deci este cel mai mic număr natural a.î. $n \cdot 1_L = 0 \Leftrightarrow n \cdot 1_L \in < 2+2i >$. $1_L = 1$. Vrem să găsim $n \in \mathbb{N} \subset \mathbb{Z} \subset < 2+2i >$. Fie $(a+bi) \in \mathbb{Z}[i]$ a.î. $(a+bi)(2+2i) \in \mathbb{Z} \Leftrightarrow 2(a-b+(a+b)i) \in \mathbb{Z} \Leftrightarrow a+b = 0 \Leftrightarrow b = -a$. Deci elementele întregi din idealul $< 2+2i >$ sunt $2 \cdot (a-(-a)) = 2 \cdot 2a = 4a$.

Deci cel mai mic număr natural care aparţine idealului $< 2+2i >$ este 4.

Avem $1+1+1+1 = 4 = (1-i)(2+2i) \equiv_{<2+2i>} 0$ şi astfel $\text{car}(L) = 4$.

Problema 2. Fie A un inel şi $f : \mathbb{Q} \longrightarrow A$ un morfism de inele. Calculaţi caracteristica inelului A.

Soluţie: Pentru orice morfism de inele $\text{Ker}(f)$ este ideal în $\mathbb{Q}$. $\mathbb{Q}$ este corp deci singurele ideale ale sale sunt 0 şi $\mathbb{Q}$.

- Dacă $\text{Ker}(f) = \mathbb{Q}$, atunci f este morfismul nul, dar f este morfism de inele şi $f(1) = 1$. O contradicţie.
- Deci varianta posibilă este $\text{Ker}(f) = 0$, adică f este injectivă. Astfel pentru orice $n \in \mathbb{N}^\star$ $f(n) = f(1+1+\cdots+1) = f(1)+f(1)+\cdots+f(1) = n \cdot 1_A \neq 0$ (f este injectivă şi $n \neq 0$). Deci $\text{car}(A) = 0$.

Problema 3. Presupunem cunoscut faptul că inelul factor

$$L = \mathbb{Z}_2[X]/ < X^3 + X + \hat{1} >$$

are ordinul 8. Arătaţi că L este corp şi grupul său multiplicativ este generat de $\hat{X}$.

Soluţie: Putem arăta că L este corp în două moduri.

- Avem următorul rezultat: Fie K un corp şi $f(X) \in K[X]$ un polinom ireductibil. Atunci $K[X]/(f)$ este corp.

$f(X) = X^3 + X + \hat{1}$ este ireductibil peste $\mathbb{Z}_2[X]$ pentru că $f(\hat{0}) = f(\hat{1}) = \hat{1}$ (nu are rădăcini în $\mathbb{Z}_2$ deci nu poate fi factorizat peste $\mathbb{Z}_2[X]$.)

- În L avem $\widehat{X^3} = -\hat{X} - \hat{1} = \hat{X} + \hat{1}$ (lucrăm cu coeficienţi $\mathbb{Z}_2$ şi $-\hat{1} = \hat{1}$).

Deci $L = \{a + b\hat{X} + c\hat{X}^2 \mid a, b, c \in \mathbb{Z}_2\} = \{\hat{0}, \hat{1}, \hat{X}, \hat{X}^2, \hat{X}+\hat{1}, \hat{X}^2+\hat{1}, \hat{X}^2+\hat{X}, \hat{X}^2+\hat{X}+\hat{1}\}$. Arătăm că orice element nenul este inversabil menţionând inverul fiecărui element.

$\hat{1}$ este propriul invers.

$\hat{X} \cdot (\hat{X}^2 + \hat{1}) = \hat{X}^3 + \hat{X} = \hat{X} + \hat{1} + \hat{X} = 2\hat{X} + \hat{1} = \hat{1}$. Deci $\hat{X}$ şi $\hat{X}^2 + \hat{1}$ sunt inverse unul altuia.

$\hat{X}^4 = \hat{X} \cdot \hat{X}^3 = \hat{X}(\hat{X} + \hat{1}) = \hat{X}^2 + \hat{X}$.

$\hat{X}^2(\hat{X}^2 + \hat{X} + \hat{1}) = \hat{X}^4 + \hat{X}^3 + \hat{X}^2 = \hat{X}^2 + \hat{X} + \hat{X} + \hat{1} + \hat{X}^2 = 2\hat{X}^2 + \hat{X} + \hat{1} = \hat{1}$. Deci $\hat{X}^2$ şi $\hat{X}^2 + \hat{X} + \hat{1}$ sunt inverse unul altuia.

$(\hat{X} + \hat{1})(\hat{X}^2 + \hat{X}) = \hat{X}^3 + \hat{X}^2 + \hat{X}^2 + \hat{X} = \hat{X} + \hat{1} + 2\hat{X}^2 + \hat{X} = 2\hat{X} + \hat{1} = \hat{1}$. Astfel $\hat{X} + \hat{1}$ şi $\hat{X}^2 + \hat{X}$ sunt inverse unul altuia.

Deci am toate elementele nenule sunt inversabile şi astfel L este corp.

Să vedem acum că $L\backslash\{0\}$ este generat de $\widehat{X}$.
Avem $\widehat{X}^2$,
$\widehat{X}^3 = \widehat{X} + \widehat{1}$,
$\widehat{X}^4 = \widehat{X}^2 + \widehat{X}$,
$\widehat{X}^5 = \widehat{X}\widehat{X}^4 = \widehat{X}(\widehat{X}^2 + \widehat{X}) = \widehat{X}^3 + \widehat{X}^2 = \widehat{X} + \widehat{1} + \widehat{X}^2 = \widehat{X}^2 + \widehat{X} + \widehat{1}$,
$\widehat{X}^6 = \widehat{X}^3\widehat{X}^3 = (\widehat{X} + \widehat{1})(\widehat{X} + \widehat{1}) = \widehat{X}^2 + 2\widehat{X} + \widehat{1} = \widehat{X}^2 + \widehat{1}$,
$\widehat{X}^7 = \widehat{X}\widehat{X}^6 = \widehat{X}(\widehat{X}^2 + \widehat{1}) = \widehat{X}^3 + \widehat{X} = \widehat{X} + \widehat{1} + \widehat{X} = 2\widehat{X} + \widehat{1} = \widehat{1}$.
Deci toate elementele nenule sunt obţinute ca puteri ale lui $\widehat{X}$.

Problema 4. Rezolvaţi în corpul cuaternionilor $\mathbb{H}$ ecuaţia

$$(1 + 2i + 3j + 4k)x = -37 + 4i + 9j + 8k.$$

Soluţie: $\mathbb{H} = \{a + b\underline{i} + cj + dk \mid a, b, c, d \in \mathbb{R}\}$. În această expresie a este coeficientul matricei identitate 2×2.
$\underline{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$. La seminar am scris ultima intrare din matrice i în loc de $-i$. Este greşit. Forma scrisă aici este corectă. Elementul i din matrice este $\sqrt{-1}$. $j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ iar $k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Aici $1 = I_2$, este elementul neutru la înmulţirea matricelor. Avem relaţiile $\underline{i}^2 = j^2 = k^2 = \underline{i}jk = -1$, $\underline{i}j = k = -j\underline{i}$, $jk = \underline{i} = -kj$, $k\underline{i} = j = -\underline{i}k$.
De aici voi folosi notaţia i pentru matricea $\underline{i}$.
Avem de rezolvat ecuaţia $(1 + 2i + 3j + 4k)(a + bi + cj + dk) = -37 + 4i + 9j + 8k$. făcând înmulţirile conform relaţiilor de mai sus şi adunând termenii asemenea obţinem
$(a-2b-3c-4d)+(2a+b-4c+3d)i+(3a+4b+c-2d)j+(4a-3b+2c+d)k = -37+4i+9j+8k$.
Egalând coeficienţii obţinem sistemul de 4 ecuaţii cu 4 necunoscute:
$\begin{cases} a - 2b - 3c - 4d &= -37 \\ 2a + b - 4c + 3d &= 4 \\ 3a + 4b + c - 2d &= 9 \\ 4a - 3b + 2c + d &= 8 \end{cases}$ care are soluţia $a = 1, b = 3, c = 4, d = 5$.
Deci $x = 1 + 3i + 4j + 5k \in \mathbb{H}$.

Problema 5. Fie inelul factor

$$M = \mathbb{Z}[i]/ < 3 > .$$

Arătaţi că M este corp şi grupul său multiplicativ e generat de $\widehat{1+i}$. În această problemă $i = \sqrt{-1}$.

Soluţie: $M = \{\widehat{0}, \widehat{1}, \widehat{2}, \widehat{i}, \widehat{2i}, \widehat{1+i}, \widehat{1+2i}, \widehat{2+i}, \widehat{2+2i}\}$.
Pentru că $1 + 1 + 1 = 3 \in< 3 >$, deci $\mathrm{car}(M) = 3$.
Arătăm ca şi în **problema 3** că fiecare element nenul este inversabil.
$\widehat{2} \cdot \widehat{2} = \widehat{4} \equiv_{<3>} \widehat{1}$, deci $\widehat{2}$ este propriul invers.
$\widehat{i} \cdot \widehat{2i} = \widehat{-2} \equiv_{<3>} \widehat{1}$, de unde deducem că $\widehat{i}$ şi $\widehat{2i}$ sunt inverse unul altuia.
$(\widehat{1+i}) \cdot (\widehat{2+i}) = \widehat{2} - \widehat{1} + \widehat{i} + \widehat{2i} = \widehat{1} + \widehat{3i} \equiv_{<3>} \widehat{1}$. Am obţinut că $\widehat{1+i}$ şi $\widehat{2+i}$ sunt inverse unul altuia.
$(\widehat{1+2i}) \cdot (\widehat{2+2i}) = \widehat{2} - \widehat{4} + \widehat{2i} + \widehat{4i} = -\widehat{2} + \widehat{6i} \equiv_{<3>} \widehat{1}$. Deci $\widehat{1+2i}$ şi $\widehat{2+2i}$ sunt inverse unul altuia.

Trebuie sămai arătăm că $M \backslash \{\widehat{0}\}$ este generat de $\widehat{1+i}$.
$(\widehat{1+i})^2 = 1 + \widehat{2i - 1} = \widehat{2}i$,
$(\widehat{1+i})^3 = 1 + \widehat{3i - 3} - i = \widehat{1+2i}$,
$(\widehat{1+i})^4 = (\widehat{1+i})^2 \cdot (\widehat{1+i})^2 = \widehat{2}i \cdot \widehat{2}i = \widehat{-4} = -\widehat{1} = \widehat{2}$,
$(\widehat{1+i})^5 = (\widehat{1+i}) \cdot (\widehat{1+i})^4 = (\widehat{1+i}) \cdot \widehat{2} = \widehat{2+2i}$,
$(\widehat{1+i})^6 = ((\widehat{1+i})^2)^3 = (\widehat{2}i)^3 = \widehat{-8i} = \widehat{i}$,
$(\widehat{1+i})^7 = (\widehat{1+i}) \cdot (\widehat{1+i})^6 = (\widehat{1+i}) \cdot (\widehat{i}) = (\widehat{i-1}) = (\widehat{2+i})$.
$(\widehat{1+i})^8 = ((\widehat{1+i})^4)^2 = \widehat{2}^2 = \widehat{4} = \widehat{1}$.

Problema 6. Explicitaţi morfismul lui Frobenius pentru corpul M din exemplul precedent.

Soluţie: Am menţionat că $\mathrm{car}(M) = 3$. Morfismul Frobenius este $F : M \longrightarrow M, F(x) = x^3$. Deci pentru orice $\widehat{a+bi} \in M$, $F(\widehat{a+bi}) = \widehat{a+bi}^{\,3} = a^3 + 3a^2 bi \widehat{+ 3a} b^2 i^2 + b^3 i^3 = a\widehat{^3 - b^3} i$.