dumitru.stamat@fmi.unibuc.ro

Exam: $\leq 10p$
Seminar: $\leq 2p$

≤ 10 "+"

1. Mulțimi, funcții
2. Relații de (echivalență, ordine)
3. Semigrupuri, monoizi
4. Grupuri $\mathbb{Z}$, $\mathbb{Z}_n$, D_n, S_n
5. Inele și corpuri, $\mathbb{Q}$, $\mathcal{M}_n(\mathbb{R})$
6. Inele de polinoame, $K[x_1, \ldots, x_n]$
7. Aritmetica din $\mathbb{Z}$, $K[X]$
8.* Polinoame simetrice. Relațiile lui Newton

-Mulțimi-

Teoria naivă a mulțimilor (Cantor)

„O colecție de obiecte bine precizate”

Descrierea unei mulțimi

Explicite

$\{$luni, marți, miercuri, joi, vineri$\}$

Printr-o proprietate comună a el. sale

zilele săptămânii în care seria 15 are ore

Convenție: mulțimi: A, B, C
elemente: a, b, c

$x \in A$
$x \notin A$

$A \subseteq B$ „mulțimea A este inclusă în mulțimea B”

$A \subset B$ „A inclus strict în B”
$(A \subsetneq B)$ $(A \neq B)$

$A = B$ dacă au aceleași el.
↳ se verifică prin verificarea dublei incluziuni:
$A \subseteq B$, $B \subseteq A$

Def

Dacă $A \cap B = \emptyset \Rightarrow A, B$ = mulțimi disjuncte

Proprietăți:

1. $A \cap B \subseteq A \subseteq A \cup B$
2. $A \cap B = B \cap A$
   $A \cup B = B \cup A$
   Dar $(A \setminus B) \cap (B \setminus A) = \emptyset$
   $A \Delta B = B \Delta A$
3. $(A \cup B) \cup C = A \cup (B \cup C)$ - asoc.
   $(A \cap B) \cap C = A \cap (B \cap C)$
   $(A \setminus B) \setminus C \neq A \setminus (B \setminus C)$
   $(A \Delta B) \Delta C = A \Delta (B \Delta C)$
4. $A \cup B = A \Leftrightarrow B \subseteq A$
   $A \cap B = A \Leftrightarrow A \subseteq B$
5. $(A \cup B) \cap C = (A \cup B) \cap (A \cup C)$ distrib.
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Legile lui De Morgan:

Fie $A, B \subseteq X$
$C_X(A \cup B) = C_X A \cap C_X B$
$C_X(A \cap B) = C_X A \cup C_X B$

Perechea ordonată (a, b) înțelegem $\{a, \{a, b\}\}$

$(a, b) = (a_1, b_1) \Leftrightarrow a = a_1,\ b = b_1$

Dem

$\{a, \{a, b\}\} = \{a_1, \{a_1, b_1\}\} \Leftrightarrow a = a_1$
și
$\{a, b\} = \{a_1, b_1\} = \{a, b_1\}$
$\Rightarrow b = b_1$

- Mulțimea vidă: $\emptyset$
- **Operații:**

Fie A, B, C, mulțimi

Reuniunea:
$A \cup B = \{x \mid x \in A$ sau $x \in B\}$

Intersecția:
$A \cap B = \{x \mid x \in A$ și $x \in B\}$

Diferența:
$A \setminus B = \{x \mid x \in A$ și $x \notin B\}$

Diferența simetrică
$A \Delta B = (A / B) \cup (B / A)$

Complementara
$A \subseteq X$
Complementara mulțimii A față de X:
$C_X A = X \setminus A$

Produs Cartezian
$A \times B = \{(a, b) \mid a \in A$ și $b \in B\}$
$A^n = \underbrace{A \times A \times \ldots \times A}_{n \text{ ori}} = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A, (\forall) i = \overline{1, n}\}$

Mulțimea părților unei mulțimi
Dat A, notăm $P(A) = \{B \mid B \subseteq A\}$

$A = \{1, 2\}$ $B = \{2, 3\}$
$P(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$
$A \times B = \{(1, 2), (1, 3), (2, 2), (2, 3)\}$

-Funcții-

Fie A și B mulțimi nevide

O func. f de la A la B este o regulă prin care oricărui el. $a \in A$ îi corespunde exact un el. din B

$f : A \to B$ $\qquad$ $A \ni x \mapsto f(x) \in B$

domeniul func. f $\qquad$ codomeniul func. f

$1_A : A \to A$ func. identitate

(id_A) $\quad x \mapsto x$

(I_A)

Def

O func. de la A la B = o submulțime C din $A \times B$ cu prop. că $(\forall)\, a \in A$, $(\exists)\, b_a \in B$ a.î. $(a, b_a) \in C$ cu notația $f(a) = b_a$

Def

$f : A \to B$ și $g : A_1 \to B_1$ sunt egale dacă $A = A_1$, $B = B_1$ și $f(x) = g(x)$, $(\forall)\, x \in A = A_1$

Temă: Fie $f : A \to B$, arătați că dacă $g : B \to A$ satisface $g \circ f = 1_A$ și $f \circ g = 1_B$ atunci f este bij. și $f^{-1} = g$

Def

Fie $f : A \to B$ și $g : B \to C$

Compunerea

$$A \xrightarrow{f} B \xrightarrow{g} C$$
$$x \mapsto f(x) \mapsto g(f(x))$$

$g \circ f : A \to C$ este func. dată prin $(g \circ f)(x) = g(f(x))$, $(\forall)\, x \in A$

Prop

Asociativitatea compunerii:

$f : A \to B$, $g : B \to C$, $h : C \to D$

$(h \circ g) \circ f = h \circ (g \circ f)$

Clase speciale de funcții

func. injective:

$(\forall)\, x_1, x_2 \in A$ cu $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

func. surjective:

dacă $(\forall)\, y \in B$, $(\exists)\, x \in A$ a.î. $f(x) = y$

func. bijective:

f - inj. și f - surj.

func. inverse

Dacă $f : A \to B$ este bij., atunci def. $f^{-1} : B \to A$, func. care asociază $y \in B \mapsto x \in A$, $f(x) = y$

$f^{-1} \circ f = 1_A$

$f \circ f^{-1} = 1_B$

Seminar

- 10 p examen
- 2 p seminar (2 lucrări x 1p)
- gabriela.petcu@s.unibuc.ro

Funcții

A, B = 2 mulțimi

$f: A \longrightarrow B$

$A \ni x \longmapsto f(x) \in B$

domeniu codomeniu

$Im(f) = f(A) = \{f(x) : x \in A\}$

$A_1 \subseteq A \rightarrow f(A_1) = \{f(x) : x \in A_1\}$

↳ imaginea lui A_1 prin f

$B_1 \subseteq B \rightarrow f^{-1}(B_1) = \{x \in A : f(x) \in B_1\}$

↳ preimagine / imaginea inversă a lui B_1 prin f

f = inj. $\Leftrightarrow$ orice paralelă la Ox inter. G_f în cel mult un punct

f = surj $\Leftrightarrow$ ($\forall$) paralelă la Ox dusă printr-un punct al codomeniului inters. G_f în cel puțin 1 pct.

Temă: Studiați bij. func:

a) $f: \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$

b) $g: \mathbb{R} \to \mathbb{R}$, $g(x) = 5x + 2$

c) $h: \mathbb{Z} \to \mathbb{Z}$, $h(x) = 5x + 2$

d) $k: \mathbb{R}_A \to \mathbb{R}_A$, $f(x) = x^2 + 6x + 2$

Temă 2: $f: \mathbb{R} \to \mathbb{R}$

$$f(x) = \begin{cases} x+1, & x \leq 2 \\ 2x+1, & x > 2 \end{cases}$$

a) f = bij?

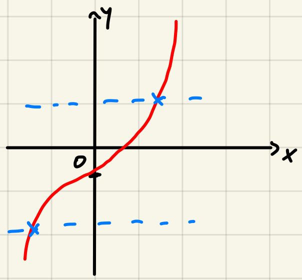
b) Det: $f([-1;3))$

$f^{-1}((0,2])$

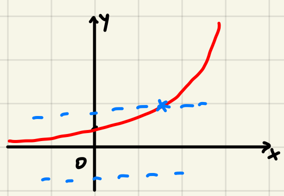
Aplicații

2) $f: \mathbb{R} \to \mathbb{R}$, $f(x) = 4x - 3$

f = bij?



3) $f: \mathbb{R} \to \mathbb{R}$, $f(x) = e^x$



4) A, B = 2 mulțimi

Card(A) ($|A|$) = a, $|B| = b$

a) Nr. func. de la A la B

Pt. fiecare el. din A, avem b variante

$\underbrace{b \cdot b \cdot b \cdot \ldots \cdot b}_{a \text{ ori}} = b^a$

b) Nr. func. inj. de la A la B ($b \geq a$)

$A_b^a = \frac{b!}{(b-a)!}$

c) bij. de la A la B ($a = b$)

$A_b^b = \frac{b!}{0!} = b! = d = Per.$

Obs

- $|A \cup B| = |A| + |B| - |A \cap B|$

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

Principiul includerii și excluderii

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{i<j}^{n} |A_i \cap A_j| + \sum_{i<j<k}^{n} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n+1} \left|\bigcap_{i=1}^{n} A_i\right|$$

d) nr. func. surjective de la A la B

$|A| = a \quad |B| = b$

Det. nr. de func. nesurjective $\overset{not}{=} N$

$B = \{1, 2, \dots, b\}$

Definim $B_i := \{f : A \to B : i \notin \mathrm{Im}(f)\}$

$i = \overline{1,b}$

$B_1 \cup B_2 \cup \dots \cup B_b =$ mulțimea tuturor func. nesurj. $\overset{not}{=} N$

$|B_i| = (b-1)^a$

$|B_i \cap B_j| = (b-2)^a$

$\vdots$

$|B_{i_1} \cap B_{i_2} \cap \dots \cap B_{i_k}| = (b-k)^a$

$N = \sum_{i=1}^{b} |B_i| - \sum_{i<j} |B_i \cap B_j| + \sum_{i<j<k} |B_i \cap B_j \cap B_k| - \dots + (-1)^{b+1} \cdot |\bigcap_{i}^{j} B_i|$

$N = b(b-1)^a - C_b^2 (b-2)^a + C_b^3 (b-3)^a - \dots + (-1)^b \cdot C_b^{b-1} \cdot 1^a - 0 =$

$= \sum_{i=1}^{b} (-1)^{i+1} \cdot C_b^i (b-i)^a$

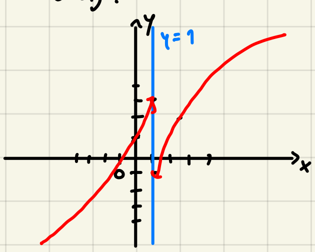
$\Rightarrow$ Nr. func. surj. $= b^a - N$

$A_1 \subseteq A \to f(A_1) = \{f(x) : x \in A_1\}$

$B_1 \subseteq B \to f^{-1}(B_1) = \{x \in A : f(x) \in B_1\}$

5) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \begin{cases} 2x+1, & x \le 1 \\ 3x-4, & x > 1 \end{cases}$

a) b = bij?



x	$-\infty$	1	$+\infty$
$f(x)$	$-\infty$	$3 \;\vdots\; -1$	$+\infty$

$\mathrm{Im}(f) = (-\infty; 3] \cup (-1; +\infty)$

$(-\infty; 3] \cap (-1; +\infty) \neq \emptyset \Rightarrow$ nu este inj.

$\mathrm{Im}(f) = \mathbb{R} \Rightarrow$ este surj.

b) Det.:

$f([1,3]) = \{3\} \cup (-1, 5] = (-1, 5]$

$f(1) = 3$

$3 \cdot 1 - 4 = -1$

$f(3) = 5$

$\cdot\, f^{-1}((-3, 4])$

$f^{-1}((-2, 0)) = (-\frac{3}{2}; \frac{1}{2}) \cup (1, \frac{4}{3})$

• Prop. legate de compunere

Prop

Fie $f, f' : A \to B$, $g, g' : B \to C$, func.:

1) $f, g = \text{inj} \Rightarrow g \circ f = \text{inj}$.
2) $f, g = \text{surj} \Rightarrow g \circ f = \text{surj}$.
3) $f, g = \text{bij} \Rightarrow g \circ f = \text{bij}$
   $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$
4) $g \circ f = \text{inj} \Rightarrow f = \text{inj}$.
5) $g \circ f = \text{surj} \Rightarrow g = \text{surj}$.
6) $g \circ f = \text{bij} \Rightarrow f = \text{inj}$. și $g = \text{surj}$.
7) $g \circ f = g \circ f'$ și $g = \text{inj} \Rightarrow f = f'$
   (ie putem simplifica la stânga cu o func. inj.)
8) $g \circ f = g' \circ f$ și $f = \text{surj} \Rightarrow g = g'$
9) $f : A \to B = \text{inj} \Leftrightarrow (\exists)\ r : B \to A$ cu prop. că $r \circ f = 1_A$
   (r = retractă a lui f)
10) $f : A \to B = \text{surj} \Leftrightarrow (\exists)\ s : B \to A$ cu prop. că $f \circ s = 1_B$
   (s = secțiune a lui f)

Sol

1) $g \circ f : A \to C$

Fie $x_1, x_2 \in A$ cu $(g \circ f)(x_1) = (g \circ f)(x_2)$

$$\left.\begin{array}{l} g(f(x_1)) = g(f(x_2)) \\ g = \text{inj}. \end{array}\right\} \Rightarrow \left.\begin{array}{l} f(x_1) = f(x_2) \\ f = \text{inj}. \end{array}\right\} \Rightarrow x_1 = x_2 \Rightarrow g \circ f = \text{inj}.$$

2) Temă

3) 1) + 2) $\Rightarrow$ 3) (prima parte)

$f : A \to B$, $g : B \to C$ $\qquad g \circ f : A \to C$

$f^{-1} : B \to A$, $g^{-1} : C \to B$ $\qquad (g \circ f)^{-1} : C \to A$

$f^{-1} \circ g^{-1} : C \to A$

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ \underbrace{(g^{-1} \circ g)}_{1_B} \circ f = f^{-1} \circ f = 1_A$$

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ \underbrace{(f \circ f^{-1})}_{1_B} \circ g^{-1} = g \circ g^{-1} = 1_C$$

Deci $f^{-1} \circ g^{-1} = (g \circ f)^{-1}$

Sol

5) $g \circ f = \text{surj}$.

Fie $z \in C \xRightarrow[g \circ f = \text{surj}.]{} (\exists)\ x \in A$ cu $(g \circ f)(x) = z$

$g(f(x)) = z$ cu $f(x) \in B$

$\Rightarrow z \in \operatorname{Im} g \Rightarrow g = \text{surj}$.

8) $g : B \to C$

$$\left.\begin{array}{l} \text{Fie } y \in B \xRightarrow{f = \text{surj}.} (\exists)\ x \in A \text{ cu } f(x) = y \\ (g \circ f)(x) = (g' \circ f)(x) \\ g(f(x)) = g'(f(x)) \Rightarrow g(y) = g'(y) \end{array}\right\} \Rightarrow g = g'$$

Funcția caracteristică

Fie E, mulțime, $A \subseteq E$

Func. $\chi_A : E \to \{0, 1\}$, func. caract. a lui A (în E)

$$\chi_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases}$$

Prop

Fie $A, B \subseteq E$

$\Rightarrow A = B \Leftrightarrow \chi_A = \chi_B$

Prop

Fie A = mulțime nevidă finită și $f : A \to A$ o func.

Echivalente:
1) f = inj.
2) f = surj.
3) f = bij.

Dem

Presup. $A = \{a_1, a_2, \ldots, a_n\}$, $n = |A|$

1) $f = \text{inj}. \Rightarrow f(a_1), f(a_2), \ldots, f(a_n)$ = distincte
   $\Rightarrow \operatorname{Im} f$ = codomeniu
   $\Rightarrow f$ = surj.

2) $f = \text{surj}. \Rightarrow a_1 = f(a_{i_1})$
   $a_2 = f(a_{i_2})$
   ....
   $a_n = f(a_{i_n})$
   $a_i \neq a_j \Rightarrow a_{i_1}, a_{i_2}, \ldots, a_{i_n}$ = distincte
   $\Rightarrow f$ = inj.

Familii indexate

Șir $(x_n)_{n\in\mathbb{N}}$ $x_0, x_1, \dots, x_n$

Un șir pe M este o func. $x:\mathbb{N}\to M$
$x_n = x(n)$

- Putem defini noțiunea de șir, mulțime indexată după o mulțime I de indici, $(x_i)_{i\in I}$ = func. $x: I \to M$
notăm $x_i = x(i), (\forall) i\in I$

- I, o mulțime de indici
$(\forall) i\in I \underset{(asoc.)}{\rightsquigarrow} A_i$, o mulțime
$(A_i)_{i\in I}$ = o familie indexată după I

$\bigcup_{i\in I} A_i = \{x : (\exists)\, i\in I \text{ cu } x\in A_i\}$

$\bigcap_{i\in I} A_i = \{x : x\in A_i, (\forall)\, i\in I\}$

$(A_i)_{i\in I}, (B_j)_{j\in J}$

$(A_i)_{i\in I} \times (B_j)_{j\in J} = \{(x,y) : x\in \bigcup_{i\in I} A_i \text{ și } y\in \bigcup_{j\in J} A_j\}$

$(\bigcup_{i\in I} A_i) \cap (\bigcup_{j\in J} B_j) = \bigcup_{(i,j)\in I\times J} (A_i\cap B_j)$

$(\bigcap_{i\in I} A_i) \cup (\bigcap_{j\in J} B_j) = \bigcap_{(i,j)\in I\times J} (A_i\cup B_j)$

$(A_i)_{i\in I}$ $\prod_{i\in I} A_i = \{f : I \to \bigcup_{i\in I} A_i \mid f(i)\in A_i, (\forall) i\in I\}$
↳ funcții de selecție

Axioma alegerii

Prod cartezian de mulțimi nevide indexate după o mulțime nevidă este nevid

Imagini și preimagini

Fie $f: A\to B$, o func.

Def

Pt. $U\subseteq A$ notăm $f(U) = \{f(x) : x\in U\}$, imaginea lui U prin f (imaginea directă)

Pt. $V\subseteq B$ notăm $f^{-1}(V) = \{x\in A : f(x)\in V\}$, preimaginea lui V prin f (imaginea inversă)

$f(A)$ = Imaginea func. f
$= \operatorname{Im} f$

Prop

Fie $f: A\to B$, o func.

1) Dacă $U_1 \subseteq U_2 \subseteq A \Rightarrow f(U_1) \subseteq f(U_2)$
2) Dacă $V_1 \subseteq V_2 \subseteq B \Rightarrow f(V_1) \subseteq f(V_2)$
3) $f(U_1\cup U_2) = f(U_1)\cup f(U_2)$
4) $f^{-1}(V_1\cup V_2) = f^{-1}(V_1)\cup f^{-1}(V_2)$
5) $f(U_1\cap U_2) \subseteq f(U_1)\cap f(U_2)$
cu egal dacă f = inj.
6) $f^{-1}(V_1\cap V_2) = f^{-1}(V_1)\cap f^{-1}(V_2)$
7) Fie $U\subseteq A$
$f^{-1}(f(U)) \supseteq U$, cu egal pt. f = inj.
8) Fie $V\subseteq B$
$f(f^{-1}(V)) \subseteq V$, cu egal pt. f = surj.

Relații

Fie A, B, 2 mulțimi

Def

O submulțime ρ a prod. cartezian $A\times B$ se numește relație de la A la B (între)

Dacă $A=B$ și $\rho\subseteq A\times A$, ρ este o relație (binară) pe mulțimea A

Inversa relației $\rho\subseteq A\times B$
este $\rho^{-1} = \{(y,x) : y\in B, x\in A, (x,y)\in\rho\}$, relație de la B la A

Def

Relația diagonală $\Delta_A = \{(x,x) : x\in A\}$

- $\rho\subseteq A\times B$, $\rho_2 \subseteq B\times C$

Compunerea:

$\rho_1\circ\rho_2 = \{(x,z)\in A\times C : (\exists)\, y\in B \text{ cu } (x,y)\in\rho_1 \text{ și } (y,z)\in\rho_2\}$

Temă

$\rho\subseteq A\times B \Rightarrow \rho\circ\Delta_B = \rho$
$\Delta_A\circ\rho = \rho$

Compunerea relațiilor este asociativă

Obs

O func. $f: A\to B$
relație $\rho_f\subseteq A\times B$
"$\{(x, f(x)) : x\in A\}$
↳ se mai numește și graficul func. f

Obs

Dat $\rho\subseteq A\times B$, $(\exists) f: A\to B$ cu $\rho_f = \rho$
$\Leftrightarrow (\forall)\, x\in A, (\exists)!\, y\in B$ cu $(x,y)\in\rho$

Seminar 2

2) $f: A \to B$

a) dacă f = inj $\Rightarrow$ $(\exists)\, r: B \to A$ a.î. $r \circ f = 1_A$
(r = retractă; r = unică dacă f = bij.)

b) dacă f = surj. $\Rightarrow$ $(\exists)\, s: B \to A$ a.î. $f \circ s = 1_B$
(s = secțiune; s = unică dacă f = bij.)

a) dacă $b \in Im(f) \Rightarrow (\exists)!\, x$ a.î. $f(x) = b \Rightarrow r(b) = x$
dacă $b \notin Im(f) \Rightarrow$, $r(b) = x_0$
Fie $x_0 \in A$
$(r \circ f)(x) = r(f(x)) = r(b) = x$

b) Temă

Funcția caracteristică a unei mulț.
E = mulț, $A \subseteq E$
$\chi_A : E \to \{0,1\}$; $\chi_A(e) = \begin{cases} 0, & e \notin A \\ 1, & e \in A \end{cases}$

Prop $A, B \subseteq E$

1) $\chi_A = \chi_B \Leftrightarrow A = B$
2) $(\chi_A)^2 = \chi_A$
3) $\chi_\emptyset = 0$; $\chi_E = 1$
4) $\chi_{\bar{A}} = 1 - \chi_A$
$\bar{A}$ = compl. lui A în E $(E \setminus A)$
5) $\chi_{A \cap B} = \chi_A \cdot \chi_B$
6) $\chi_{A \cup B} = \chi_A + \chi_B - \chi_A \cdot \chi_B$
7) $\chi_{A \setminus B} = \chi_A (1 - \chi_B)$
8) $\chi_{A \Delta B} = (\chi_A - \chi_B)^2$, $A \Delta B = (A \setminus B) \cup (B \setminus A)$

Aplicație

Dem. că Δ = asoc.

$(A \Delta B) \Delta C = A \Delta (B \Delta C)$
$\Leftrightarrow$
$\chi_{(A \Delta B) \Delta C} = \chi_{A \Delta (B \Delta C)}$
$\Leftrightarrow$

$$\chi_{(A\Delta B)\Delta C} = (\chi_{A\Delta B} - \chi_C)^2 \underset{(2)}{\equiv} \chi_{A\Delta B} - \chi_C \underset{(2)}{\equiv} (\chi_A - \chi_B)^2 - \chi_C \underset{(2)}{\equiv} \chi_A + \chi_B + \chi_C$$

Analog

$\chi_{A \Delta (B \Delta C)} \underset{(2)}{=} (\chi_A + \chi_B + \chi_C)$

$\chi_{(A\Delta B)\Delta C} \underset{(2)}{\equiv} \chi_{A\Delta(B\Delta C)}$

$2 \underset{(2)}{\equiv} 4 \Rightarrow 2 \% 2 = 4 \% 2$

$1 \underset{(2)}{\equiv} 3$

$-1 \underset{(2)}{\equiv} 1$

P.I.E. $\to |A_1 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| \ldots + (-1)^{n+1} |\bigcap_{i=1}^{n} A_i|$

Aplicații

1) $n \geq 1$, $\underbrace{\varphi(n)}_{\text{indicatorul lui Euler}}$ = nr. numerelor nat. $\leq n$ și prime cu n

Arătați că $\varphi(n) = n \cdot (1-\frac{1}{p_1})(1-\frac{1}{p_2}) \ldots (1-\frac{1}{p_k})$

unde $n = p_1^{e_1} \cdots p_k^{e_k}$ (p_i = fact prim dim din desc. lui n)

Fie $A_i = \{x : x \vdots p_i, x < n\}$

$|A_i| = \frac{n}{p_i} \to |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}| = \frac{n}{p_{i_1} \cdots p_{i_k}}$

$\varphi(n) = n - |A_1 \cup \ldots \cup A_k|$

$|A_1 \cup \ldots \cup A_k| = \sum_{i=1}^{k} \frac{n}{p_i} - \sum_{i<j} \frac{n}{p_i \cdot p_j} + \ldots + (-1)^{k+1} \cdot \frac{n}{p_1 \cdots p_k} =$

$= n\left(\frac{1}{p_1} + \ldots + \frac{1}{p_k} - \frac{1}{p_1 \cdot p_2} - \ldots - \frac{1}{p_{k-1} \cdot p_k} + \ldots + (-1)^{k+1} \cdot \frac{1}{p_1 \cdots p_k}\right)$

$\varphi(n) = n\left(1 - \frac{1}{p_1} - \ldots - \frac{1}{p_k} + \ldots + (-1)^{k} \frac{1}{p_1 \cdot p_k}\right)$

inducție: $P(k)$ = adv. $\to P(k+1)$

$\varphi(12) = 12 \cdot (1-\frac{1}{2})(1-\frac{1}{3}) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$ ($\{1, 5, 7, 11\}$)

$12 = 2^2 \cdot 3$

$\varphi(24) = 24 \cdot (1-\frac{1}{2})(1-\frac{1}{3}) = 8$

2) A = mult. cu n el.

Det. nr. de partiții cu k factori ale lui A

• $\underbrace{M_1 \to M_j}_{\text{nevide}}$, partiție a lui M

$\begin{cases} 1) \; M_1 \cup \ldots M_j = M \\ 2) \; (\forall) \, i \neq j, \; M_i \cap M_j = \emptyset \end{cases}$

$$S = k^n - \sum_{i=1}^{k} (-1)^{i+1} \cdot C_k^i \cdot (k-1)^n$$

exp. $A = \{1,2,3,4\}$, $k = 3$

1	2	3, 4
1	2, 3	4
1	2, 4	3
1, 2	3	4
1, 3	2	4
1, 4	2	3

$\{1,2,3,4\} \xrightarrow[f]{} \{1,2,3\}$

$\{1\} \to 1$ | $\{2,3\} \to 1$
$\{2,3\} \to 2$ $\neq$ $\{1\} \to 2$
$\{4\} \to 3$ | $\{4\} \to 3$

$3!$

nr. func. surj. de la $\underset{|A|=n}{A} \to \underset{B=k}{B} \overset{not}{=} S$

$$\boxed{\frac{S}{k!}}$$

Temă: det. nr. permutărilor fără pct. fixe ale unei mulț. cu n el. (P.I.E.)

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ ✓ $\quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ NU

Relații între mulțimi

$A, B =$ mulțimi (nevide)

$a \rho b$ = a este în relația ρ cu b, unde $\rho \subseteq A \times B$

compunere:

$$\left.\begin{array}{l}\rho_1 \subseteq A \times B \\ \rho_2 \subseteq B \times C\end{array}\right| \Rightarrow \rho_1 \circ \rho_2 = \{(x,z) : (\exists) y \in B \text{ a.î. } x \rho_1 y \text{ și } y \rho_2 z\} \subseteq A \times C$$

Ex:

$A = B = C = \mathbb{Z}$

1) $a \rho_1 b \Leftrightarrow a-b \vdots 5$

$a \rho_2 b \Leftrightarrow a-b \vdots 7$

$\rho_1 \circ \rho_2$

Caut $y \in \mathbb{Z}$ a.î. $a \rho_1 y$ și $y \rho_1 b$

$\Leftrightarrow a-y \vdots 5$ și $y-b \vdots 7$

$\Leftrightarrow \begin{array}{l} a-y = 5t \\ y-b = 7s \end{array}$

$\left.\begin{array}{l} y = a-5t \\ y = 7s+b \end{array}\right\} \Rightarrow \begin{array}{l} a-5t = 7s+b \\ a-b = 7s+5t \end{array}$

$\left\{\begin{array}{l} n = p \cdot x + q \cdot y \\ \text{dacă } (p,q) = 1 \end{array}\right.$

? ce numere (a,b) au prop. că $a-b = 7s + 5t$

R: $a-b$ poate fi orice multiplu de c.m.m.d.c$(7,5) = 1$

$\Rightarrow$ toate

$\Rightarrow \rho_1 \circ \rho_2 = \mathbb{Z} \times \mathbb{Z}$

toate nr. sunt în relație $\rho_1 \circ \rho$

Temă:

a) $a \rho_1 b \Leftrightarrow a-b \vdots 4$
$a \rho_2 b \Leftrightarrow a-b \vdots 2$

b) $a \rho_1 b \Leftrightarrow a-b \vdots 11$
$a \rho_2 b \Leftrightarrow a-b \vdots 3$

Care e $\rho_1 \circ \rho_2$?

Curs 3

Relații de echivalență. Relații de ordine

Def

O relație ρ pe $M \neq \emptyset$ se numește:

1) **reflexivă** dacă $(x,x) \in \rho \Rightarrow x\rho x$, $(\forall) x \in M$
2) **simetrică** dacă $(\forall) x,y \in M \Rightarrow x\rho y \Rightarrow y\rho x$
3) **antisimetrică** dacă $(\forall) x,y \in M \Rightarrow x\rho y$ și $y\rho x \Rightarrow x=y$
4) **tranzitivă** dacă $(\forall)$ $x,y,z \in M \Rightarrow x\rho y$ și $y\rho z \Rightarrow x\rho z$

Def

Familia de mulțimi $(A_i)_{i\in I}$ este o partiție a mulțimii M dacă:

1) $A_i \neq \emptyset$, $(\forall) i \in I$
2) $A_i \cap A_j = \emptyset$, $(\forall) i \neq j$ din I
3) $\bigcup_{i\in I} A_i = M$

Def

O relație pe M se numește **relație de echivalență** dacă este reflexivă, simetrică și tranzitivă

Def

Mulțime $S \subseteq M$ se numește **sistem de reprezentanți** pentru rel. de echiv. dacă S conține câte exact un element din fiecare clasă de echiv.

Def

Fie ρ o relație de echivalență pe $M \neq \emptyset$.
Pt. $x \in M$, notăm $\hat{x} = \{y \in M : x\rho y\}$
↳ **clasa de echivalență** a elementului x
$(\hat{x}, \bar{x}, [x])$

Prop

Dată $(A_i)_{i\in I}$ o partiție a mulțimii M, relația $\sim$ pe M
$(\forall)$ $x,y \in M$, $x \sim y \Leftrightarrow (\exists) i \in I$ cu $x \in A_i$ și $y \in A_i$
este o relație de echivalență pe M ale cărei clase de echivalență sunt $(A_i)_{i\in I}$

Notăm $M/\rho = \{\hat{x} : x \in M\}$
↳ **mulțimea factor**
(mulțimea și spațiul cât)

Problemă:

Fie M o mulțime cu n elemente
Det. nr. de relații de echivalență pe M.

$\pi : M \to M/\rho$ este o surj. numită **proiecția canonică** / **aplicată**
$x \longmapsto \hat{x}$

Sol:

nr de relații de echiv. este nr de partiții ale lui M
nr. de partiții ale lui M cu k factori: $\frac{1}{k!}$ din nr. de func. surj. $f : M \to \{1,2,\dots,k\}$

Prop. Fie ρ, rel. de echiv. pe M

1) **$(\forall) x \in M$, $x \in \hat{x}$**
2) **$(\forall) x,y \in M$: $\hat{x} = \hat{y}$ ori $\hat{x} \cap \hat{y} = \emptyset$**
$\hat{x} = \hat{y} \Leftrightarrow x\rho y$

Dem

Să presupunem că $x\rho y$: $\hat{x} = \hat{y}$
Fie $z \in \hat{x} \Rightarrow z\rho x \xrightarrow{x\rho y} z\rho y \Rightarrow z \in \hat{y}$
$\Rightarrow \hat{x} \subseteq \hat{y}$
Analog $\hat{y} \subseteq \hat{x}$ $\Big\} \Rightarrow \hat{x} = \hat{y}$

Să pp. că $x \not\rho\, y$: $\hat{x} \cap \hat{y} = \emptyset$
Dacă P.R.A., $(\exists)$ $z \in \hat{x} \cap \hat{y} \Rightarrow z \in \hat{x}$ și $z \in \hat{y}$
$\Rightarrow z\rho x$ și $z\rho y \overset{(S)}{\Rightarrow} x\rho z$ și $z\rho y$
$\overset{(T)}{\Rightarrow} x\rho y$, contradicție

3) **$\bigcup_{x\in M} \hat{x} = M$**

Prop

Fie ρ o rel. pe $M \neq \emptyset$
Notăm $\tilde{\rho} = \Delta_M \cup (\rho \cup \rho^{-1}) \cup (\rho \cup \rho^{-1})^2 \cup \dots = \bigcup_{i\geq 0} (\rho \cup \rho^{-1})^i$
$(\rho^0 = \Delta_M$, $(\rho \cup \rho^{-1})^2 = (\rho \cup \rho^{-1}) \circ (\rho \cup \rho^{-1}))$

Atunci $\tilde{\rho}$ este o rel. de echiv. pe M, și este cea mai mică (în sensul incluziunii) relație de echiv. pe M ce conține ρ

Ex:

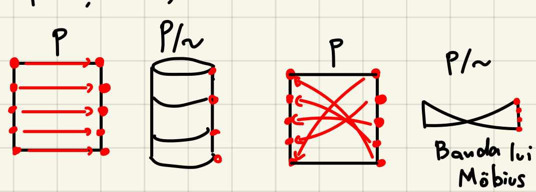
1) Pe M, $\Delta_M = \{(x,x) : x \in M\}$ este o rel. de echiv.
$\hat{x} = \{x\}$
$M/\Delta_M = \{\hat{x} : x \in M\} = \{\{x\} : x \in M\}$

Sistem de reprezentanți: M

Obs

Clasele de echiv. ale relației ρ de echiv. form. o partiție a mulțimii M

3)



2) Pe M def. $\sim$ prin $(\forall) x,y \in M$, $x \sim y$
$\hat{x} = M$
$M/\sim = \{M\}$

1) Fie $n \in \mathbb{N}$. Pe $\mathbb{Z}$ def. rel. $\sim_n$

$(\forall)\, x, y \in \mathbb{Z}$, $x \sim y$ dacă $n \mid x-y$

(i.e. $(\exists)\, m \in \mathbb{Z}$ a.î. $n \cdot m = x-y$)

Atunci $\sim_n$ este o rel. de echiv. pe $\mathbb{Z}$ numită **congruența modulo n**, $x \equiv_n y$, $x \equiv y \pmod n$

dacă $n=0$, $x \sim_0 y \Leftrightarrow x = y$

Notăm cu $\mathbb{Z}_n = \mathbb{Z}/\sim_n$

Pt. $i \in \mathbb{Z}$, $\hat{i} = \{x \in \mathbb{Z} : i \sim_n x\}$

$(n \mid i-x)$

$i - x = q \cdot n,\ q \in \mathbb{Z}$

$\hat{i} = \{i + q \cdot n : q \in \mathbb{Z}\}$

Sistem de repr.: $\{0, 1, 2, \dots, n-1\}$

$\mathbb{Z}_n = \{\hat{0}, \hat{1}, \hat{2}, \dots, \widehat{n-1}\}$

Adunare pe $\mathbb{Z}_n$:

$\hat{x} + \hat{y} = \widehat{x+y}$

(este def. în func. de repr. claselor)

Ar trb. verif. că nu depinde de repr. aleși

Fie $\hat{x} = \hat{x}_1$, $\hat{y} = \hat{y}_1$ $\Rightarrow \widehat{x+y} = \widehat{x_1+y_1}$

$n \mid x - x_1$, $n \mid y - y_1$ $\Rightarrow n \mid x - x_1 + y - y_1$

$n \mid x + y - (x_1 + y_1)$

$\mathbb{Z}_5 \to \mathbb{Z}$

$\hat{x} \to 2x^2+1$

$\hat{0} \mapsto 1$ $\neq$

$\hat{5} \mapsto 2 \cdot 25 + 1 = 5$

Teorema (prop. de universalitate a mult. factor)

Fie $\sim$ o rel. de echiv. pe M și $f: M \to A$ o func.

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi_\sim"'] & A \\ M/\sim \arrow[ur, dashed, "\hat{f}"'] & \end{tikzcd}$$

Atunci $(\exists)\, \hat{f}: M/\sim \to A$, cu prop. că $\hat{f} \circ \pi_\sim = f \Leftrightarrow$ $(\forall)\, x, y \in M$ cu $x \sim y \Rightarrow f(x) = f(y)$

$\hat{f}(\hat{x}) = f(x)$

Def

O mult. total ordonată se numește și **lanț**.

Rel. de ordine

Def

O rel. ρ pe $M \neq \emptyset$ se numește rel. de ordine pe M dacă este:
(1) reflexivă
(2) antisimetrică
(3) tranzitivă

Notăm (M, ρ), mulțime ordonată

Def

ρ este o ordine totală pe M dacă $(\forall)\, x, y \in M$, $x \rho y$ sau $y \rho x$
(orice 2 el. din M sunt comparabile)

Uzual notăm o rel. de ordine cu „$\leq$"

$x \leq y$

$x \leq y$ și $y \leq z \Rightarrow x \leq z$

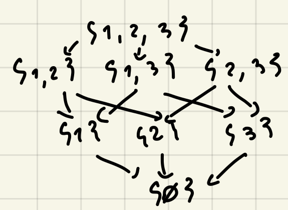
$x \leq y$ și $y \leq x \Rightarrow x = y$

Ex:

1) (M, Δ_M) e rel. de ordine care nu e totală
2) $(\mathbb{R}, \leq) \Rightarrow$ mult. total ordonată
3) $M \rightsquigarrow P(M) = \{A : A \subseteq M\}$
   $(P(M), \subseteq)$ este o mult. ord.
   dacă $|M| \geq 2$, ord. nu e totală
   $\{x_1\} \nsubseteq \{x_2\}$
4) Dacă ρ este o rel. de ord. pe $M \Rightarrow \rho^{-1}$ este rel. de ord. pe M
   $(M, \rho) \rightsquigarrow (M, \rho^{-1})$
   $(\mathbb{R}, \leq)$ $(\mathbb{R}, \geq)$
5) $(M, \leq)$
   Strictă
   $x < y \Rightarrow x \leq y$ și $x \neq y$

Diagrama Hasse

$(M, \leq)$, mult. ord, îi asociem un graf orientat:
- vârfurile sunt el. din M
- muchiile: $x \to y$ dacă $x < y$ și $(\nexists)\, z \in M$ cu $x < z$ și $z < y$



Seminar 3

Relații între mulțimi

Def

- A, B = mult.
- $\rho \subseteq A \times B$ - relație

$a \rho b$ sau $(a,b) \in \rho$

Def

$$\left.\begin{array}{l}\rho_1 \subseteq A\times B \\ \rho_2 \subseteq B \times C\end{array}\right| \Rightarrow \rho_1 \circ \rho_2 = \{(x,z) : (\exists)\, y \in B \text{ a.î. } x\rho_1 y \text{ și } y \rho_2 z\} \subseteq A \times C$$

Ex

1) Pe $\mathbb{R}\times\mathbb{R}$, $a\rho_1 b \Leftrightarrow a \le b$

$a \rho_2 b \Leftrightarrow a \ge b$

$\rho_1 \circ \rho_2$

Caut $y \in \mathbb{R}$ a.î. $a\rho_1 y$ și $y \rho_2 b$

$\Rightarrow a \le y$ și $y \ge b$

$\Rightarrow \rho_1 \circ \rho_2 = \mathbb{R} \times \mathbb{R}$

Def

ρ = rel. pe A

(1) ρ = reflexivă $\Leftrightarrow (\forall)\, x \in A,\ x\rho x$

(2) ρ = simetrică $\Leftrightarrow (\forall)\, x,y \in A$ cu $x\rho y \Rightarrow y \rho x$

(3) ρ = antisimetrică $\Leftrightarrow (\forall)\, x,y\in A$ cu $x\rho y$ și $y \rho x \Rightarrow x = y$

(4) ρ = tranzitivă $\Leftrightarrow (\forall)\, x,y,z \in A$ cu $x\rho y$ și $y \rho z \Rightarrow x \rho z$

Def

Dacă ρ are prop. (1), (2), (4), e rel. de echiv. $\rightsquigarrow$ „$\sim$"

Dacă ρ are prop. (1), (3), (4), e rel de ordine $\rightsquigarrow$ „$\le$"

$\sim$: rel. de echiv pe A

$[x] = \{y \in A : x \sim y\}$

$\hookrightarrow$ clasa de echiv. a lui x

$A/\sim$ = mulț. tuturor claselor de echiv.

- un SCR (sistem complet de repr.)

$S \subseteq A$ care conține câte un repr. din fiecare clasă de echiv.

1) Stabiliți dacă urm. relații sunt de echiv.:

a) $x \sim y \Leftrightarrow x - y \in \mathbb{Z}$

b) $x \sim y \Leftrightarrow |x-y| < 2$

c) $x \sim y \Leftrightarrow x + y \in \mathbb{Z}$

a) R: Fie $x \in \mathbb{R}$

$x \sim x \Rightarrow 0 \in \mathbb{Z} \Rightarrow R$.

S: Fie $x, y \in \mathbb{R}$

$x - y \in \mathbb{Z} \Leftrightarrow -(x-y) \in \mathbb{Z}$

$\Leftrightarrow y - x \in \mathbb{Z} \Rightarrow y \sim x \Rightarrow S$

T: Fie $x,y,z \in \mathbb{R}$

$$\left.\begin{array}{l} x\sim y \Rightarrow x - y \in \mathbb{Z} \\ y \sim z \Rightarrow y - z \in \mathbb{Z}\end{array}\right\} \Rightarrow x - y + y - z \in \mathbb{Z}$$

$\Rightarrow x - z \in \mathbb{Z} \Rightarrow x \sim z \Rightarrow T$

R, S, T $\Rightarrow$ rel. de echiv.

b) R: Fie $x \in \mathbb{R}$

$x \sim x \Rightarrow |x - x| < 2 \Rightarrow 0 < 2 \Rightarrow R$

S: Fie $x, y \in \mathbb{R}$

$x \sim y \Rightarrow |x-y| < 2 \Rightarrow -2 < x - y < 2 \,/\cdot(-1)$

$-2 < y - x < 2 \Rightarrow y \sim x \Rightarrow S$

T: Fie $x,y,z \in \mathbb{R}$

$x \sim y \Rightarrow |x-y| < 2 \Rightarrow -2 < x - y < 2$

$y \sim z \Rightarrow |y - z| < 2 \Rightarrow -2 < y - z < 2$

„+"

$-4 < x - z < 4$

Contraexemplu: $x = 0$, $y = 1$, $z = 2$

$$\left.\begin{array}{l}|x-y| = 1 < 2 \\ |y-z| = 1 < 2 \\ |x - z| = 2\end{array}\right\} \Rightarrow \text{nu e } T. \Rightarrow \sim \text{ nu e rel. de echiv.}$$

2) Stab. dacă urm. rel. este de echiv. pe $\mathbb{C}$

a) $z \sim w \iff |z| = |w|$

R: Fie $x \in \mathbb{C}$

$x \sim x \iff |x| = |x|$ „A"

S: Știm că $x \sim y \Rightarrow |x| = |y| \iff |y| = |x| \iff y \sim x$

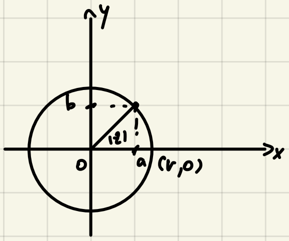
T: Știm că $x \sim y$ și $y \sim z \Rightarrow$

$\left.\begin{array}{l}|x|=|y|\\|y|=|z|\end{array}\right| \Rightarrow |x| = |z| \Rightarrow x \sim z$

$\Rightarrow \sim$ este rel. de echiv.

b) Det. un SCR $\rightsquigarrow [0,+\infty)$

$z = a+bi \rightsquigarrow (a,b)$



Temă: St. dacă $z \sim w \iff z-w \in \mathbb{R}$ este rel. de echiv. pe $\mathbb{C}$

$a+bi - c+di = (a-c)+(b-d)i$

Temă: Pe $\mathbb{R}$: $x \sim y \iff x \le y$

a) Det. dacă $\sim$ = rel de echival

b) Este $\sim$ antisimetrică

3) Pe $\mathbb{Z}$: $x \sim y \iff x - y \,\vdots\, 3$

a) St. dacă $\sim$ = rel. de echiv.

b) Det. un SCR.

$x - y \,\vdots\, 3 \iff x \underset{(3)}{\equiv} y$

$[0] = \{3k : k \in \mathbb{Z}\} = \{\dots, -3, 0, 3, \dots\}$

$[1] = \{3k+1 : k \in \mathbb{Z}\} = \{\dots, -2, 1, 4, \dots\}$

$[2] = \{3k+1 : k \in \mathbb{Z}\} = \{\dots, -1, 2, 5, \dots\}$

$SCR = \{0, 1, 2\}$

4) Pe $\mathbb{N} \times \mathbb{N}$: $(m,n) \sim (p,q) \iff m+q = n+p$

a) **temă**: rel. de echiv.

b) Un SCR?

$(m,n) \rightsquigarrow m-n \rightsquigarrow$ sol. a ec. $y+n=m$

$[(m,n)] \rightsquigarrow (a,b)$ cu $a-b = m-n \iff a+n = b+m$

Ex: $(2,5) \rightsquigarrow 2-5 = -3 \to (3,6), (4,7)$

$SCR: \{(0,k) : k \in \mathbb{N}^*\} \cup \{(k,0) : k \in \mathbb{N}^*\} \cup \{(0,0)\}$

Rel. de ordine

*) $(A, \le)$:

1) dacă $\le$ = rel. de ord. $\Rightarrow (A, \le)$ = mulț. parțial ord.

2) dacă $\le$ = rel. de ord. $+ (\forall) a,b \in A \rightsquigarrow a \le b$ sau $b \le a$ $\Big| \Rightarrow (A, \le)$ = mulț. total ord.

Obs

El. minimal = un el. care nu este mai mare decât niciun alt element

El. minim = un el. care este mai mic decât celelalte elemente

El. maximal = un el. care nu este mai mic decât niciun alt element

El. maxim = un el. care este mai mare decât celelalte elemente

Ex

5) Pe $\mathbb{N}$, $x | y \iff (\exists) k \in \mathbb{N}$ a.î. $y = k \cdot x$

a) Det. dacă $(\mathbb{N}, |)$ = MPO

b) Arătați că $(\mathbb{N}, |) \ne$ MTO

c) Det. el. minimale, maximale, minimul, maximul (dacă există)

$D(n)$ = Mulț. div. naturali ai lui n

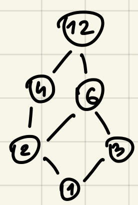
$DP(n)$ = Mulț. div. proprii ai lui n $= D(n) \setminus \{1, n\}$

Ex:

$D(12) = \{1, 2, 3, 4, 6, 12\}$

$DP(12) = \{2, 3, 4, 6\}$

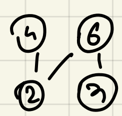
$D(12)$:



minim = 1

maxim = 12

$DP(12)$:



minimale: 2, 3

maximale: 4, 6

Temă:

$DP(40)$, $DP(60)$

(cu diagrama Hasse)

Curs 4

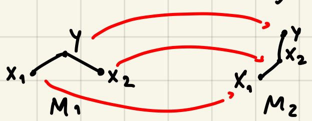
Def

Fie $(M_1, \le_1)$ și $(M_2, \le_2)$ mult. ord.
O func. $f: M_1 \to M_2$ se numește **morfism** de mult. ord.
(sau aplicație monotonă) dacă: $(\forall)\, x, y \in M_1: x \le_1 y \Rightarrow f(x) \le_2 f(y)$)

Dacă în plus f este bij. și $f^{-1}: M_2 \to M_1$ este morfism de mult. ordonate, spunem că f este **izomorfism** de mult. ord.

Obs

Dacă f-monotonă și f-bijecție $\not\Rightarrow f^{-1}$ este monotonă



$x_1 \le_2 x_2$, dar $f^{-1}(x_1) \not\le_1 f^{-1}(x_2)$
(nu sunt comp.)

lanț = (sub)mult. total ord. (M_2)

Def

O mult. ord. s.n. **inductiv ordonată** dacă orice lanț are un majorant.

Lema lui Zorn

Orice mult. nevidă inductiv ordonată are măcar un el. maximal

Def

O mult. ord. este **bine ordonată** dacă orice submult. nevidă are un prim element (minim)

Ex: $(\mathbb{N}, \le)$ ~~$(\mathbb{Z}, \le)$~~

Prop

$(M, \le)$ = bine ord. $\Rightarrow$ total ord.

Dem

Fie $x \ne y \in M$
$\{x, y\}$ are minim $\Rightarrow x \le y$ sau $y \le x$

Teorema lui Zermelo

Pe orice mult. nevidă se poate defini o relație de bună ord.

Legi de compoziție. Monoizi

- Fie $M \ne \emptyset$

Def

O lege de comp. (binară) pe M este o func. $f: M \times M \to M$

Notații: $\circ, *, \cdot, +, \#$

$\circ(x, y) \overset{not}{=} x \circ y$

Fie $(M, *)$, operație pe M

Def

- $*$ este **asoc.** dacă $(a * b) * c = a * (b * c)$, $(\forall)\, a, b, c \in M$
- $*$ este **comut.** dacă $a * b = b * a$, $(\forall)\, a, b \in M$
- $e \in M$ este **el. neutru** pt. „$*$" dacă $e * a = a * e = a$, $(\forall)\, a \in M$ (dacă există, e unic)
- Spunem că $a \in M$ este **inversabil** în M dacă $(\exists)\, a' \in M$ cu $a * a' = a' * a = e$

dacă „$*$" e asoc. cu el. neutru și a = inversabil, atunci a' = unic

Def

Un **semigrup** este o mult. nevidă M pe care avem o operație asoc. $(M, *)$

Def

Un **monoid** este un semigrup unde op. are el. neutru

De obicei operația: „$\cdot$" sau „$+$"
↳ cazul comutativ

Ex: $(\mathbb{N}, +)$ - monoid
$(\mathbb{N}^*, \cdot)$ - monoid
$(\mathbb{N}^*, +)$ - semigrup comutativ (nu e monoid)
$(2\mathbb{N}+1, \cdot)$ - monoid
$(2\mathbb{N}, +)$ - monoid
$(2\mathbb{N}, \cdot)$ - semigrup

$(\mathbb{R}, +)$ - monoid comutativ
$([3, \infty), +)$ - semigrup

Fie $M \ne \emptyset$
$\mathcal{F}(M) = \{f: M \to M \mid f\text{-func.}\}$
$(\mathcal{F}(M), \circ)$ - monoid, comutativ $\Leftrightarrow |M| = 1$
(el. neutru 1_M)

$\mathcal{B}(M) = \{f: M \to M \mid f\text{-bij.}\} \subseteq \mathcal{F}(M)$
↳ sunt el. inversabile din $(\mathcal{F}(M), \circ)$

Def

Fie M_1 și M_2, monoizi, cu e_1, resp. e_2 el. neutre
func. $f: M_1 \to M_2$, se numește **morfism de monoizi**
dacă $f(a\cdot b) = f(a)\cdot f(b)$, $(\forall)\, a,b\in M_1$
$f(e_1) = e_2$
dacă în plus, f = bij. $\Rightarrow$ f: **izomorfism de monoizi**

Obs

1) f - izo. de monoizi $\Rightarrow$ f^{-1} - izo. de monoizi
2) $f: M_1 \to M_2$ și $g: M_2 \to M_3$ sunt morf. de mono. $\Rightarrow$ $g\circ f$ = morf. de mono.

Def

O submulț. $A \subseteq (M,\cdot)$ se numește **submonoid** în M dacă $a\cdot b\in A$, $(\forall)\, a,b\in A$ și $e_M\in A$

A - submono. în $M \Rightarrow (A,\cdot)$ - monoid

$4\mathbb{Z}_{12} = \{\hat0, \hat4, \hat8\} \subsetneq (\mathbb{Z}_{12},\cdot)$
monoid, dar nu e submonoid

Prop

O intersecție de submono. ai lui $(M,\cdot)$ este submonoid

Def

Fie S, submulț. în monoidul $(M,\cdot)$. Atunci
$\bigcap H$ este cel mai mic submonoid din M ce conține S
$S\subseteq H\subseteq M$, H submonoid
$\parallel$ not
$\langle S\rangle$ - submonoidul generat de S

Ex:

$S=\emptyset$, $\langle\emptyset\rangle = \{e_M\}$
Altfel $\langle S\rangle = \{x_1^{n_1}\cdot x_2^{n_2}\cdots x_r^{n_r} : r\in\mathbb{N},\ x_1,\dots,x_r\in S,\ n_1,\dots,n_r\in\mathbb{N}\}$

Prop

$(\mathbb{N},+)$ este un monoid generat de 1
$\mathbb{N} = \{n\cdot 1 : n\in\mathbb{N}\}$
Dar $(\mathbb{N}^*,\cdot)$ nu este finit generat

Teoremă

Submono. lui $(\mathbb{N},+)$ sunt finit generați

Monoid liber generat de o mulț.

Fie A o mulț. „alfabet"
cuvânt = { șir $x_1, x_2, \dots, x_n$ de el. din alfabet, $(x_i\in A, (\forall)\, i)$
finit
sau
cuvântul vid „⊔"
$F(A)$ = mulț. cuv. pe A

$A=\{x\}$
$F(A)=\{⊔, x, xx, xxx, \dots\}$
$A=\{a,b\}$
$F(A)=\{⊔, a, b, ab, ba, aaa, \text{etc.}\}$

2 cuvinte sunt egale $\Rightarrow$ $x_1x_2\dots x_n = y_1y_2\dots y_m \Leftrightarrow n=m$ și $(x_i=y_i, (\forall)\, i)$
cu operația de concatenare
$F(A)$ este un monoid, numit monoidul liber peste A

Reguli de calcul $(M,\cdot)$ monoid

$(a^n)^m = a^{n\cdot m}$
$a^{n+m} = a^n\cdot a^m$, $(\forall)\, n,m\in\mathbb{N}$, $a\in M$
$ab=ba \Rightarrow (ab)^n = a^n\cdot b^n$

Convenție
$a^0 = e_M$

Fie M - submono. în $(\mathbb{N},+)$
Notez $\gcd(M)$ - c.m.m.d.c. al el. lui M

Obs

Dacă notăm $d := \gcd(M)$, atunci $\frac{1}{d}M$ este un submonoid în $(\mathbb{N},+)$ cu $\gcd(\frac{1}{d}M)=1$ $\quad M \underset{(izo.)}{\simeq} \frac{1}{d}M$

Def

Un submonoid $M\subseteq(\mathbb{N},+)$ cu prop. că $\gcd(M)=1$ se numește **semigrup numeric**

Prop

Submonoidul $M\subseteq(\mathbb{N},+)$ este un semigrup numeric $\Leftrightarrow |\mathbb{N}\setminus M|<\infty$

Ex

$M=\langle 3,7\rangle = \{a\cdot 3+b\cdot 7,\ a,b\in\mathbb{N}\}$
$=\{0,-,-,3,-,-,6,7,-,9,10,-,12,13,14 \longrightarrow\}$
$\gcd(M)=\gcd(3,7)$ și $|\mathbb{N}\setminus M| = 6<\infty$ "F(M)" "c(M)"
$\max(\mathbb{N}-M)$ = **nr. Frobenius** al semi.
$=F(M)$
$c(M)=F(M)+1$ = **conductorul semi.**

Obs

$10 = 1\cdot3+1\cdot7$
$21 = 7+7+7 = \underbrace{3+3+\dots+3}_{7\text{ ori}}$ $\Rightarrow$ descompunerea poate să nu fie unică ca sumă de generatori ai lui M

Problemă

Fie M_1, M_2 - monoizi, $S\subset M_1$ cu $\langle S\rangle = M_1$
Dată o func. $f: S\to M_2$, poate fi aceasta prelungită la un morfism de monoizi $\bar f: M_1\to M_2$

Ex: $M_1=\langle 3,7\rangle$ $\quad M_2$
$f:\{3,7\}\to M_2$
$f(3)=\alpha$
$f(7)=\beta$ $\Rightarrow$ $f(10) = f(3)+f(7) = \alpha+\beta$
$f(21) = f(3\cdot 7) = 3\cdot f(7) = 3\beta$
$= f(7\cdot 3) = 7\cdot f(3) = 7\alpha$

Dacă se poate ajunge la $\bar f: \langle 3,7\rangle\to M_2$ trebuie ca $\boxed{3\beta = 7\alpha}$

Întrebare: mai găsim și alte restricții

Teoremă

Fie $A\neq\emptyset$ și M - monoid.
Orice func. $f: A\to M$ se prelungește la un morfism (surj.) de monoizi $\bar f: F(A)\to M$ prin $\bar f(x_1 x_2\dots x_n) = f(x_1) f(x_2)\dots f(x_n)$

Seminar 4

$(D_{p(n)}, |) = MTO \iff n = p^{\alpha}, p = prim$

$p \cdot p^2 \cdot \ldots \cdot p^{\alpha-1}$

$(M, \circ)$ = semigrup

$\circ$ = asoc.

$(M, \circ)$ = monoid

$\circ$ = asoc.
$\circ$ are el. neutru

• $(3\mathbb{N}+1, +)$
↳ nu e l.c. $(3\mathbb{N}+1$ nu e p.s.$)$

Arătați că $(\mathbb{Z}_n, +)$ - monoid com.

„+" - com, asoc., cu el. n.

$\mathbb{Z}_n = \{\hat{0}, \hat{1}, \ldots, \widehat{n-1}\}$

„+" - com. $\iff \hat{x} + \hat{y} = \hat{y} + \hat{x}$, $(\forall)\ \hat{x}, \hat{y} \in \mathbb{Z}_n$

$\hat{x} + \hat{y} = \widehat{x+y} = \widehat{y+x} = \hat{y} + \hat{x}$

„+"- asoc. $\iff (\hat{x} + \hat{y}) + \hat{z} = \hat{x} + (\hat{y} + \hat{z})$, $(\forall)\ \hat{x}, \hat{y}, \hat{z} \in \mathbb{Z}_n$

$(\hat{x} + \hat{y}) + \hat{z} = \widehat{x+y} + \hat{z} = \widehat{x+y+z}$
$\hat{x} + (\hat{y} + \hat{z}) = \hat{x} + \widehat{y+z} = \widehat{x+y+z}$

„+"- el. neutru

$e = \hat{0}$
$\hat{x} + \hat{0} = \hat{0} + \hat{x} = \hat{x} \Rightarrow (\mathbb{Z}_n, +)$ = monoid com.

Morfisme

$(M_1, \circ), (M_2, \perp)$ monoizi

$g: M_1 \to M_2$ morf
$\iff$
1) $f(a \circ b) = f(a) \perp f(b)$, $(\forall)\ a, b \in M_1$
2) $f(e_1) = e_2$
3) izomorfism dacă f = bij

1) a) $f: (\mathbb{N}, +) \to (\mathbb{N}, \cdot)$
$f(n) = 27^n$ ↳ morfism

(1) $f(n+m) = 27^{n+m} = 27^n \cdot 27^m = f(n) \cdot f(m)$
(2) $f(0) = 27^0 = 1$

b) temă $f: (\mathbb{Z}, \cdot) \to (\mathbb{N}, \cdot)$, $f(x) = |x|$

c) temă $f: (P(B), \cup) \to (P(B), \cap)$, $f(X) = B \setminus X$

Def

$A \subseteq M$ submonoid dacă:
↳ monoid
1) $a \circ b \in A$, $(\forall)\ a, b \in A$
2) $e_M \in A$

Există submonoizi în $\mathbb{N} \times \mathbb{N}$ care să nu fie finit generați

$(\mathbb{N}, +) = \langle 1 \rangle$ - finit generat
$(\mathbb{N}, \cdot) = \langle$toate nr. prime$\rangle$ - infinit gen.

$\{(1,1); (1,2); \ldots\} = N$

Pp. că N = f.g.
$N = \langle (a_1, b_1); \ldots; (a_n, b_n) \rangle$

$(1, x) = x_1 \cdot (a_1 + b_1) + x_2 \cdot (a_2 + b_2) + \ldots + x_n (a_n + b_n)$

$x_i \in \mathbb{N}$

$\Rightarrow (\exists)\ (a_k, b_k) = (1, x)$, $x_k = 1$
$x_j = 0$, $(\forall)\ j \neq k$

„F" din principiul cutiei

Semigrupuri numerice

$M \subseteq \mathbb{N}$ cu $\gcd(M) = 1$
sub
mono

M = semigr. numeric

$\gcd(M)$ = cmmdc.-ul generatorilor lui M

(1) $M = \langle 4, 5 \rangle = \{4 \cdot a_1 + 5 \cdot a_2 \mid a_1, a_2 \in \mathbb{N}\}$
$= \{0, -, -, -, 4, 5, -, -, -, 8, 9, 10, -, \underbrace{12, 13, 14, 15,} \mapsto\}$

$|\mathbb{N} \setminus M| = 6$

$C(M) = 12$
$F(M) = 11$

(2) $M = \langle 5, 6, 7 \rangle = \{0, -, -, -, -, 5, 6, 7, -, -, \underbrace{10, 11, 12, 13, 14,} \mapsto\}$

$|\mathbb{N} \setminus M| = 6$
$C(M) = 10$
$F(M) = 9$

Temă

a) $\langle a, a+1, a+2 \rangle$
$C(M) = ?$
$F(M) = ?$

Seminar 5

Test: 17.11

$M = \langle a, a+1 \rangle, a > 2$

$F(M) = a(a-1)-1$

$M = \langle a, a+1, a+2 \rangle, a > 2$

$\langle 7,8,9 \rangle = \{0, \bar{1}, \dots, \bar{6}, 7, 8, 9, \bar{10}, \dots, \bar{13}, 14, 15, 16, 17, 18, \bar{19}, \bar{20}, \underbrace{21, 22, 23, 24, 25, 26, 27}_{7}, \dots\}$

$1+6, 3+4, 5+2, 7$

$F(M) = \frac{a(a-1)}{2} - 1$ (pt. a = impar)

$\langle 8,9,10 \rangle = \{0, \dots, \bar{7}, 8, 9, 10, \dots, \bar{15}, 16, 17, 18, 19, 20, \dots, \bar{23}, 24, 25, 26, \dots, 30, \dots, \bar{31}, 32, 33, 34, \dots\}$

$1+7, 3+5, 5+3, 7+1, 8$

$F(M) = (1+3+\dots+(a-1)) \cdot 2 - 1 =$

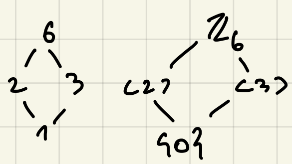
$= \frac{a^2}{2} - 1$ (pt. a = par)

Grupuri

$(G, \cdot)$ - grup dacă:
1. P.S.
2. Asoc.
3. El. neutru
4. toate el. sunt inv.
5*. com.

Def

$H \leq G$ subgrup dacă:
1. H e p.s.
2. $(\forall) x \in H, x^{-1} \in H$



1) $(G, \cdot)$ grup, $H \subset G$, H = finită

Dacă $(\forall) x, y \in H$, $xy \in H$, arăt. că $H \leq G$

Vrem ca $(\forall) x \in H$, $x^{-1} \in H$

Fie $x \in H \Rightarrow \underbrace{x, x^2, x^3, \dots}_{\text{infinit}} \in H$ (finit)

$\Rightarrow (\exists)\, i > j$ a.î.

$x^i = x^j \rightsquigarrow i - j > 0 \Rightarrow i - j \geq 1$

$\Rightarrow x^{i-j} = e$

① dacă $x = e \Rightarrow x^{-1} = e \in H$

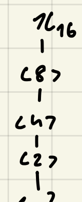
② $x \neq e$

$x^{i-j} = e \Rightarrow i - j > 1$

$\Rightarrow i - j - 1 > 0$ | $x^{i-j-1} \in H$

$x^{i-j} = x^{i-j-1} \cdot x = e$ | $x^{i-j-1} = x^{-1}$ ✓

$\mathbb{Z}_{16}$:



2) Det. subgr. lui $\mathbb{Z}_n$

a) $n = 6$

$\mathbb{Z}_6 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}\}$

$\langle \hat{0} \rangle = \{\hat{0}\}$

$\langle \hat{1} \rangle = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}\} = \mathbb{Z}_6 = \langle \hat{5} \rangle$

$\langle \hat{2} \rangle = \{\hat{0}, \hat{2}, \hat{4}\} = \langle \hat{4} \rangle$

$\langle \hat{3} \rangle = \{\hat{0}, \hat{3}\}$

$\langle \hat{4} \rangle = \{\hat{0}, \hat{2}, \hat{4}\}$

$\langle \hat{5} \rangle = \mathbb{Z}_6$

$\langle k \rangle = \langle \text{cmmdc}(k, n) \rangle$

$D_6 = \{1, 2, 3, 6\}$

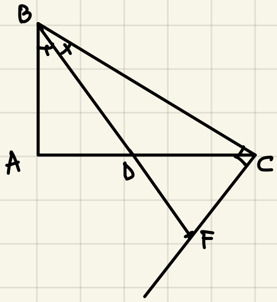
$\langle k_1, \dots, k_p \rangle = \langle \text{cmmdc}(k_1, \dots, k_p, n) \rangle$

3) Det. subgr. lui $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$

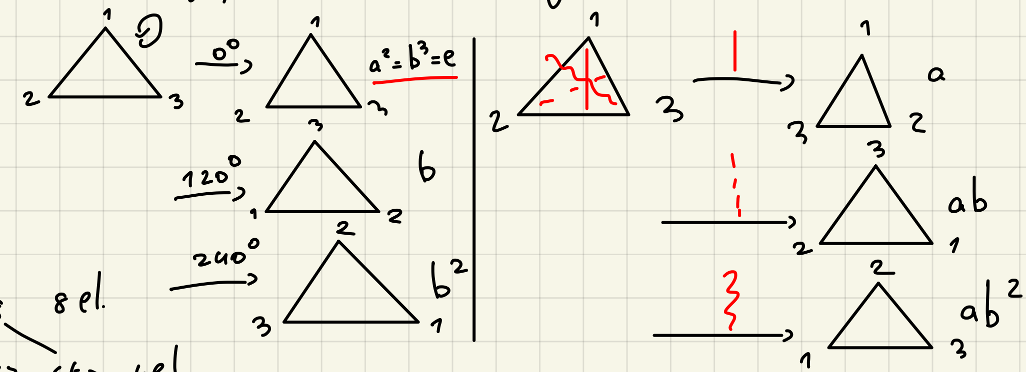
$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$

$\{(0,0)\}$; $\{(0,0); (0,1)\}$; $\{(0,0); (1,0)\}$, $\{(0,0); (1,1)\}$

$\{(0,0); (1,0); (0,1)\}$ NU

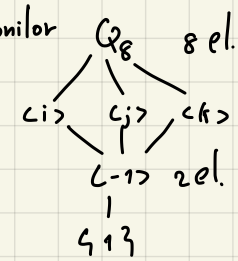


5) Det. D_3 = grupul izometriilor Δ echi. $\rightsquigarrow \varphi = \frac{360}{3} = 120$



4) Q_8 = grupul cuaternionilor

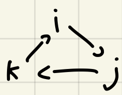
$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$



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

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

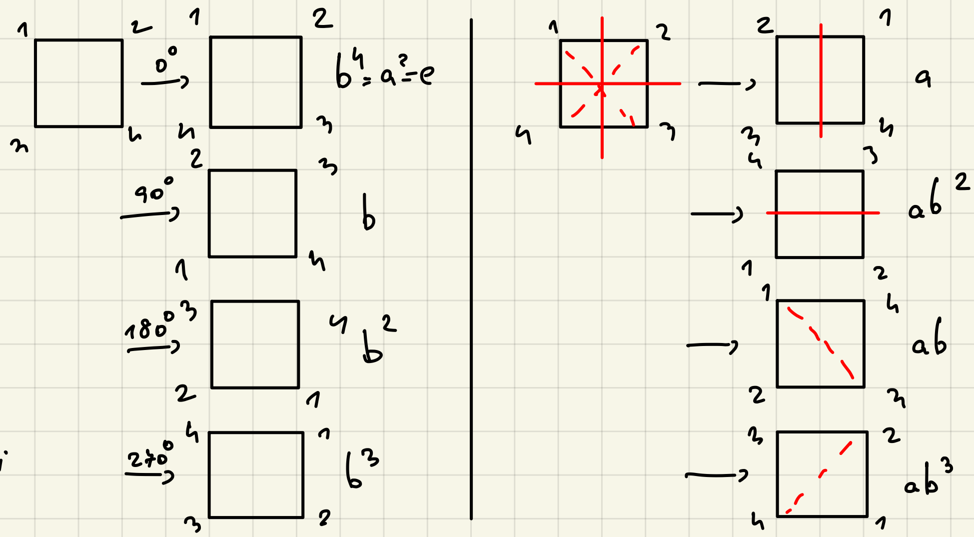
$i^2 = j^2 = k^2 = -1$



$i \cdot j = k$
$j \cdot i = -k$
$j \cdot k = i$
$k \cdot j = -i$
$k \cdot i = j$
$i \cdot k = -j$

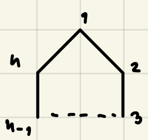
1 = el. neutru
$\langle -1 \rangle = \{-1, 1\}$
$\langle i \rangle = \{1, -1, i, -i\}$
$\langle j \rangle = \{1, -1, j, -j\}$
$\langle k \rangle = \{1, -1, k, -k\}$

6) Det. D_4 (izo. pătratului) $\varphi = 90°$



Temă

Det. $D_n \to$ poligon reg. cu n laturi



$$D_4 = \begin{cases} a, a^2 = b^4 = e \\ b, b^2, b^3 \\ ab, ab^2, ab^3 \end{cases}$$

10.11.2023

Str. Alg. în Info

1) $(\mathbb{Q}, +)$ = finit generat ?

Obs: G = finit generat $\Rightarrow$ generat de un nr. finit de generatori (i.e. o submulț. finită a sa)

pp. că e finit generat $(\mathbb{Q}, +)$

$$\mathbb{Q} = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z} \right\} \text{ și } \{ b \neq 0 \}$$

$$\mathbb{Q} = \left\langle \frac{a_1}{b_1}, \dots, \frac{a_n}{b_n} \right\rangle, \; a_i, b_i \in \mathbb{Z}, \; b_i \neq 0$$

Fie $n = \max(b_i) \longrightarrow \frac{a_i}{b_i} \in \left\langle \frac{1}{n!} \right\rangle = \left\langle \frac{1}{1 \cdot 2 \cdot \ldots \cdot n} \right\rangle$

cu $a_i, b_i \in \mathbb{Z}, \; b_i \neq 0$

$$\mathbb{Q} = \left\langle \frac{1}{n!} \right\rangle \quad \text{fie } \frac{1}{(n+1)!}$$

$$\frac{1}{(n+1)!} = k \cdot \frac{1}{n!}, \; k \in \mathbb{Z}$$

$$k = \frac{1}{n+1} \notin \mathbb{Z} \Rightarrow \text{ctd. deci}$$

$(\mathbb{Q}, +)$ nu este finit generat

Seminar 6

1) pag. precedentă

- $\langle \frac{1}{2} \rangle = \{\frac{1}{2}\cdot k : k \in \mathbb{Z}\} = \{0, \frac{1}{2}, -\frac{1}{2}, 1, -1, \dots\}$
- $\langle \frac{3}{5}, \frac{2}{3} \rangle = \{\frac{3}{5}\cdot x + \frac{2}{3} y \mid x, y \in \mathbb{Z}\}$
  $= \{\frac{9x+10y}{15}, x, y \in \mathbb{Z}\} = \{\frac{1}{15}\cdot t, t \in \mathbb{Z}\} = \langle \frac{1}{15} \rangle$
- $\langle 9, 10 \rangle = \langle \text{cmmdc}(9,10) \rangle = \mathbb{Z}$
- $\langle \frac{2}{3}, -\frac{1}{5}, \frac{1}{2} \rangle = \{\frac{1}{30} t, t \in \mathbb{Z}\}$

Def

G = grup finit, $a \in G$

- $\text{ord}(G)$ = nr de el. al lui G
- $\text{ord}(a)$ = cel mai mic nr. natural n cu prop. că $a^n = e$

Dacă $(\exists)\ p \in \mathbb{N}$ a.î. $a^p = e \Rightarrow n \mid p$

Teoremă

$\underset{\text{subgrup}}{H} \le G \Rightarrow \text{ord}(H) \mid \text{ord}(G)$

2) **Prop. ord. unui el.**

(1) $\text{ord}((x,y)) = \text{cmmmc}(\text{ord}(x), \text{ord}(y))$, $(x,y) \in G_1 \times G_2$

(2) $\text{ord}(x^{-1}) = \text{ord}(x)$

(3) $\text{ord}(xy) = \text{ord}(yx)$

(4) $\text{ord}(xyx^{-1}) = \text{ord}(y)$

(5) Dacă $xy = yx$ și $\text{cmmdc}(\text{ord}(x), \text{ord}(y)) = 1$
$\text{ord}(xy) = \text{ord}(x) \cdot \text{ord}(y)$

(6) $\text{ord}(x^k) = \dfrac{\text{ord}(x)}{\text{cmmdc}(\text{ord}(x), k)}$

Dem

(1) $\text{ord}(x) = n$, $\text{ord}(y) = m$
$\Rightarrow x^n = e_1$, $y^m = e_2$
$\Rightarrow \text{ord}((x,y)) = \text{cmmmc}(n,m)$

(2) $\text{ord}(x^{-1}) = \text{ord}(x)$
$\text{ord}(x^{-1}) = p_1$, $\text{ord}(x) = p$
$(x^{-1})^{p_1} = e$, $x^p = e$
$\left.\begin{array}{l} \Rightarrow x^{-p_1} = e \Rightarrow p \mid p_1 \\ (x^{-1})^p = x^{-p} = e \Rightarrow p_1 \mid p \end{array}\right\} \Rightarrow p_1 = p$

(3) $\text{ord}(xy) = \text{ord}(yx)$
obs: $xy \ne yx$ (nu mereu) $\Rightarrow (xy)^k \ne x^k \cdot y^k$

Notăm: $\text{ord}(xy) = k$, $\text{ord}(yx) = p$
$\Rightarrow (xy)^k = e$ și $(yx)^p = e$
$(xy)^k = e$
$\Rightarrow \underbrace{xy \cdot xy \cdot \ldots \cdot xy}_{k \text{ ori}} = e$
$y \mid x \cdot (yx)^{k-1} \cdot y = e$
$(yx)^k \cdot y = y$
$(yx)^k = e \Rightarrow p \mid k$

$(yx)^p = e \Rightarrow y(xy)^{p-1} \cdot x = e$
$\Rightarrow (xy)^p \cdot x = x \Rightarrow (xy)^p = e$
$\Rightarrow k \mid p$

$\Rightarrow k = p$

Temă: (4), (5)

(6) Notăm: $\text{ord}(x^k) = l$, $\text{ord}(x) = n$ | $\text{cmmdc}(n,k) = d$
↳ vrem: $l = \frac{n}{d}$

$n = d \cdot n'$, $k = d \cdot k'$, $(n', k') = 1$
$\Rightarrow d \cdot n' \mid d \cdot k' \cdot l$

$x^n = e$, $(x^k)^l = e$
$x^{kl} = e$
$\Rightarrow n \mid kl$

$\left.\begin{array}{l} n' \mid k' \cdot l \\ (n', k') = 1 \end{array}\right\} \Rightarrow n' \mid l$

$\underline{k \cdot n' = n \cdot k'}$
$(x^k)^{n'} = x^{k \cdot n'} = x^{n \cdot k'} = e$
$\Rightarrow l \mid n'$

$\Rightarrow l = n'$
$\Rightarrow l = \frac{n}{d}$

$\text{ord}(\hat{x}) = ?$ cu $\hat{x} \in \mathbb{Z}_n$

$(\mathbb{Z}_{12}, +)$ $\qquad \text{ord}(\hat{x}) = \dfrac{n}{\text{cmmdc}(x,n)},\ \hat{x} \in \mathbb{Z}_n$

$\text{ord}(\hat{4}) = 3$

$\text{ord}(\hat{3}) = 4$

$\text{ord}(\hat{5}) = 12$

Obs

$(\mathbb{Z}_p, +)$ p = prim

$\Rightarrow \text{ord}(\hat{x}) = p$

- Câți generatori are $(\mathbb{Z}_n, +)$

$\langle \hat{x} \rangle = \mathbb{Z}_n$

↳ nr. de nr. prime cu n din $\mathbb{Z}_n$

$\Rightarrow \varphi(n) = n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k})$

$n = p_1^{e_1} \cdots p_k^{e_k}$

$\mathbb{Z}_8 = \langle \hat{1} \rangle, \langle \hat{3} \rangle, \langle \hat{5} \rangle, \langle \hat{7} \rangle$

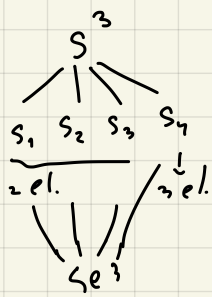
- $D_3 \sim S_3$

↳ grup. perm. cu 3 el.

$\text{ord}(S_3) = \text{ord}(D_3) = 3! = 6$

Subgr. $\sim S_3$:

- $\text{ord}(\langle \overset{S_1}{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}} \rangle) = 2$
- $\text{ord}(\langle \overset{S_2}{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}} \rangle) = 2$
- $\text{ord}(\langle \overset{S_3}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}} \rangle) = 2$
- $\text{ord}(\langle \overset{S_4}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}} \rangle) = 3$



$\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \rangle = S_3$

- $(\mathbb{Z}_n, \cdot)$ = monoid com. $\rightsquigarrow U((\mathbb{Z}_n, \cdot))$ = grup abelian

↳ $\varphi(n)$ elemente

- $(\mathbb{Z}_8, \cdot)$ = de ce nu e grup

$\hat{4}$ nu are invers

2) 0 nu este inversabil cu "·"

$\hat{x} \in U((\mathbb{Z}_n, \cdot))$

$\Leftrightarrow \gcd(x, n) = 1$

Curs 7

Subgrupuri normale. Grupul factor. Teorema de izomorfism

$(G,\cdot)$ grup, $H \le G$ subgrup

Pe G avem rel. de echivalență stg./dr. modulo H

$x \sim_s y \bmod H \iff x^{-1}y \in H$ $\quad \hat{x} = xH$

$x \sim_d y \bmod H \iff xy^{-1} \in H$ $\quad \bar{x} = Hx$

Def

Subgrupul H al lui G se numește **subgrup normal** în G dacă cele 2 rel. de echiv. de mai sus coincid

Notație: $H \trianglelefteq G$

$(x^{-1}y \in H \iff xy^{-1} \in H) \iff xH = Hx, (\forall) x \in G$ $\quad /x^{-1}$

$\iff xHx^{-1} = H, (\forall) x \in G$

$\iff xHx^{-1} \subseteq H, (\forall) x \in G$

$(\forall) x \in G, (\forall) h \in H, xhx^{-1} \in H$

Ex:

1) $\{1\} \trianglelefteq G$

Fie $x \in G, h \in H$

$xhx^{-1} = x \cdot x^{-1} = 1 \in H$

$G \trianglelefteq G$

2) Dacă G este grup abelian, orice subgrup al său este normal în G

$xHx^{-1} = \cancel{xx^{-1}}H = H$

3) În $(S_3, \circ)$, subgrupul $H = \langle(1,2)\rangle$ nu este normal

$\langle(1,2)\rangle \not\trianglelefteq (S_3, \circ)$

Găsim un $x \in S_3$, $h \in \langle(1,2)\rangle$ a.î. $xhx^{-1} \notin \langle(1,2)\rangle$

$H = \{e, (1,2)\}$

pt $x = (1,3)$

$x^{-1} = (3,1) = (1,3)$

$h = (1,2)$

$xhx^{-1} = (1,3)\cdot(1,2)\cdot(1,3) =$

$= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2,3)$ Deci $\langle(1,2)\rangle \not\trianglelefteq S_3$

$1 \to 3 \to 3 \to 1$

$2 \to 2 \to 1 \to 3$

4) Dacă $H_1 \trianglelefteq H_2$ și $H_2 \trianglelefteq H_3 \not\Rightarrow H_1 \trianglelefteq H_3$

5) Orice subgrup în $Z(G)$ este normal în G

$Z(G) \overset{def}{=} \{a \in G : ag = ga, (\forall) g \in G\}$

$H \le Z(G) \Rightarrow H \trianglelefteq G$

6) Dacă $[G:H] = 2 \Rightarrow H \trianglelefteq G$

$\hat{1} = \bar{1} = H \Rightarrow (\forall) x \notin H$ $\quad xH = Hx = G \setminus H \Rightarrow H \trianglelefteq G$

7) Dacă $f: G_1 \to G_2$ morf. de grupuri, atunci $\ker f \trianglelefteq G_1$ (nucleul său)

Știm că $\ker f \le G_1$

$\ker f = \{x \in G_1 : f(x) = \underset{(e_2)}{1}\}$

Fie $x \in G_1, h \in \ker f$

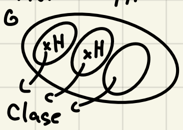
$xhx^{-1} \in \ker f$

$f(xhx^{-1}) = f(x) \cdot \underbrace{f(h)}_{1} \cdot f(x^{-1}) = f(x) \cdot f(x)^{-1} = 1 \in \ker f$

$\Rightarrow \ker f \trianglelefteq G_1$

Fie $H \trianglelefteq G$

Notăm $G/H = (G/H)_s = (G/H)_d$



Pe mult. cât G/H avem o struct. de grup indusă de G prin: $\hat{x} \cdot \hat{y} = \widehat{xy}$, $(\forall)\, x, y \in H$

unde $\hat{1}$ = el. neutru

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

Numim $(G/H, \cdot)$ grupul factor G modulo H

$\pi : G \longrightarrow G/H$, $x \longmapsto \hat{x}$ — proiecția canonică este morfism de grupuri

• operația e bine definită

Fie $\hat{x} = \hat{a}$ și $\hat{y} = \hat{b}$

$x^{-1}a \in H$ $\quad y^{-1}b \in H$

și $xa^{-1} \in H$ $\quad yb^{-1} \in H$

Vrem $\widehat{xy} = \widehat{ab}$

$(xy)^{-1}ab = y^{-1}x^{-1}ab$

$= \underbrace{y^{-1}(x^{-1}a) \cdot y}_{\in H \ (H \trianglelefteq G)} \cdot \underbrace{y^{-1}b}_{\in H \ (\hat{y} = \hat{b})} \in H$

• asociativitatea

$(\hat{x} \cdot \hat{y}) \cdot \hat{z} = \widehat{xy} \cdot \hat{z} = \widehat{xyz}$

$\hat{x} \cdot (\hat{y} \cdot \hat{z}) = \hat{x} \cdot \widehat{yz} = \widehat{xyz}$

• el. neutru

$\hat{1} \cdot \hat{x} = \widehat{1x} = \hat{x} = \widehat{x \cdot 1} = \hat{x} \cdot \hat{1}$

• invers

$\widehat{x^{-1}} \cdot \hat{x} = \widehat{x^{-1}x} = \hat{1} = \widehat{x \cdot x^{-1}} = \hat{x} \cdot \widehat{x^{-1}}$

$\Rightarrow \hat{x}^{-1} = \widehat{x^{-1}}$

Ex:

1) În $(\mathbb{Z}, +)$ considerăm subgrupul normal $n\mathbb{Z}$ și

$x \sim y \bmod n\mathbb{Z} \Leftrightarrow x - y \in n\mathbb{Z}$

$\Leftrightarrow n \mid x - y$

$\Leftrightarrow x \equiv y \bmod n$

$\mathbb{Z}/n\mathbb{Z} = \{\hat{0}, \hat{1}, \dots, \widehat{n-1}\}$ grup factor cu operația $\hat{x} + \hat{y} = \widehat{x+y}$

este grupul $(\mathbb{Z}_n, +)$

Teorema fundamentală de izomorfism

Fie $f : G_1 \to G_2$ un morfism de grupuri.

Atunci $\ker f \trianglelefteq G_1$ și f induce un izomorfism de grupuri $G_1/\ker f \simeq \operatorname{Im} f$

$\hat{x} \longmapsto f(x)$

Dem

$\ker f \trianglelefteq G_1$ ✓

Notăm $\bar{f} : G_1/\ker f \to G_2$ dată prin $\bar{f}(\hat{x}) = f(x)$, $(\forall)\, \hat{x} \in G/\ker f$

• $\bar{f}$ e bine definită (nu depinde de reprez. ales)

$\hat{x} = \hat{y} \Leftrightarrow xy^{-1} \in \ker f \Leftrightarrow f(xy^{-1}) = 1 \Leftrightarrow f(x) \cdot f(y)^{-1} = 1 \Leftrightarrow f(x) = f(y)$

• $\bar{f}$ este morfism de grupuri

$\bar{f}(\hat{x} \cdot \hat{y}) = \bar{f}(\widehat{xy}) = f(xy) = f(x) \cdot f(y) = \bar{f}(\hat{x}) \cdot \bar{f}(\hat{y})$

• $\bar{f}$ este injectivă

$\hat{x} \in \ker \bar{f} \Leftrightarrow \bar{f}(\hat{x}) = 1 \Leftrightarrow f(x) = 1 \Leftrightarrow x \in \ker f$

$\Leftrightarrow \hat{x} = \widehat{\ker f} = \hat{1}$

• $\operatorname{Im} \bar{f} = \operatorname{Im} f$

$\bar{f}$ este morfism injectiv de grupuri cu $\operatorname{Im} \bar{f} = \operatorname{Im} f$

$\Rightarrow G_1/\ker f \simeq \operatorname{Im} f$

Ex: Fie $f : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$

$f(x) = \cos(2\pi x) + i\sin(2\pi x)$, $(\forall)\, x \in \mathbb{R}$

f este morfism de grupuri

$f(x+y) = f(x) \cdot f(y)$ (Moivre)

$\ker f = \{x \in \mathbb{R} : f(x) = 1 = 1 + i \cdot 0\} = \mathbb{Z}$

$\cos(2\pi x) = 1$

$\sin(2\pi x) = 0$

$\operatorname{Im} f$ = nr. complexe de modul 1

$U \overset{not}{=} \{z \in \mathbb{C} \mid |z| = 1\}$

Din teoria fund. izo. la grupuri:

$(\mathbb{R}/\mathbb{Z}, +) \simeq (U, \cdot)$

Grupuri ciclice

Un grup s.n. grup ciclic dacă poate fi generat de un singur el.

$G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$

Teoremă

Un grup este ciclic $\Leftrightarrow$ este izomorf cu $\mathbb{Z}$ (dacă e gr. inf.) sau este izomorf cu $(\mathbb{Z}_n,+)$ (dacă are n el.)

Dem „$\Leftarrow$" $\mathbb{Z}$ este ciclic
$\mathbb{Z}_n$ este grup ciclic

„$\Rightarrow$" Pp. că $(\exists)$ $a \in G$ cu $G = \langle a \rangle$

Fie $f : \mathbb{Z} \to G$, $f(k) = a^k$

$\operatorname{Im} f = \langle a \rangle = G$

f morfism de grupuri:

$f(k+l) = f(k) \cdot f(l)$

$a^{k+l} = a^k \cdot a^l$ ✓

Notăm $H = \ker f \trianglelefteq (\mathbb{Z},+)$

$\Rightarrow (\exists)\, n \in \mathbb{Z}$ cu $\ker f = n\mathbb{Z}$

Caz 1: $n = 0 \Rightarrow \ker f = \{0\}$

$\mathbb{Z}/\ker f \simeq \operatorname{Im} f \Rightarrow \underbrace{\mathbb{Z}/\{0\}}_{= \mathbb{Z}} \simeq G \Rightarrow G \simeq (\mathbb{Z},+)$

Caz 2: $n > 0 \Rightarrow \ker f = n\mathbb{Z}$

$\Rightarrow \underbrace{\mathbb{Z}/n\mathbb{Z}}_{\mathbb{Z}_n} \simeq \operatorname{Im} f = G \Rightarrow G \simeq (\mathbb{Z}_n,+)$

Teoremă

Dacă G e grup ciclic, atunci orice subgrup în G și orice grup factor al lui G sunt grupuri ciclice

Dem: Cf. teoremei anterioare, e suficient să considerăm cazurile $G = \mathbb{Z}$ și $G = \mathbb{Z}_n$

$G = \mathbb{Z}$ și $H \leq G \Rightarrow (\exists)\, m \in \mathbb{N}$ cu $H = \langle m \rangle$, deci H - grup ciclic

$(\mathbb{Z},+)$ abelian $\Rightarrow$ $(\forall)$ subgr. e normal în $\mathbb{Z}$

$G = (\mathbb{Z}_n,+)$, $n \geq 2$

$H \leq G \Rightarrow (\exists)\, d \mid n$ a.î. $H = \langle d \rangle$, deci H e ciclic

$\mathbb{Z}_n$ abelian $\Rightarrow H \trianglelefteq (\mathbb{Z}_n,+)$

$\mathbb{Z}_n/\langle \hat{d} \rangle = \langle \bar{1} \rangle$ automat grup ciclic $\simeq (\mathbb{Z}_d,+)$

$d \mid n \Rightarrow \langle \hat{d} \rangle = \{\hat{0}, \hat{d}, \widehat{2d}, \dots, \widehat{(\frac{n}{d}-1)d}\}$
$\hookrightarrow \frac{n}{d}$ el.

$\left|\mathbb{Z}_n/\langle \hat{d} \rangle\right| \overset{def}{=} [\mathbb{Z}_n : \langle \hat{d} \rangle] \underset{\text{Lagrange}}{\overset{\text{Th.}}{=}} \frac{|\mathbb{Z}_n|}{|\langle \hat{d} \rangle|} = \frac{n}{n/d} = d$

Corolar:

Fie p nr. prim. Atunci orice grup cu p el. este izomorf cu $(\mathbb{Z}_p,+)$

Dem:

$|G| = p \Rightarrow (\forall)\, x \in G \setminus \{1\}$ $\operatorname{ord} x = p$

$\Rightarrow \langle x \rangle = G$

$\Rightarrow G$ ciclic cu p el. $\overset{\text{Th.}}{\Rightarrow} (G,\cdot) \simeq (\mathbb{Z}_p,+)$

Seminar 7

Permutări:

$(S_n, \circ)$ = grup cu $n!$ el.
(necom. dacă $n \geq 3$)

$S_n = \{\sigma : \{1,\dots,n\} \to \{1,\dots,n\} \mid \text{bij}\}$

permutare : $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}$

ciclu de lung k : $(i_1\ i_2 \dots i_k)(x) = \begin{cases} i_2, & x = i_1 \\ i_3, & x = i_2 \\ \vdots & \\ i_1, & x = i_k \\ x, & x \notin \{i_1, \dots, i_k\} \end{cases}$

• transpoziție: ciclu de lung. 2

Ex: S_3

$(1\ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$(1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

• Câți ciclii de lung. k sunt în S_n

$$\frac{A_n^k}{k} = \frac{n!}{(n-k)! \cdot k}$$

1) $\text{ord}(\hat{x}) = \dfrac{n}{\gcd(x,n)}$, $\hat{x} = (\mathbb{Z}_n, +)$

$\text{ord}(\hat{x}) = k \Rightarrow \hat{x} \cdot \hat{k} = \hat{0}$
$\Rightarrow x \cdot k = M_n \Rightarrow n \mid x \cdot k$

$\gcd(n,x) = d$
$\Rightarrow \begin{array}{l} x = d \cdot a \\ n = d \cdot b \end{array}, (a,b) = 1$

$\Rightarrow d \cdot b \mid d \cdot a \cdot k$
$\Rightarrow b \mid k$

$\Rightarrow k = b$

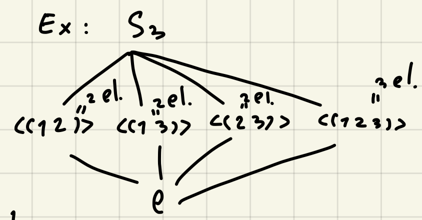
$\text{ord}(x) = \dfrac{n}{d} = \dfrac{n}{\gcd(n,x)}$

Subgrup normal

• $H \leq G$ (grup) = subgrup $\Leftrightarrow x \cdot y^{-1} \in H$, $(\forall)\ x, y \in H$
$[H \leq G]$

• $H \leq G$ = normal $\Leftrightarrow x \cdot h \cdot x^{-1} \in H$,
$(\forall)\ h \in H$, $x \in G$ $[H \trianglelefteq G]$

Ex:



$3! = 6$

$S_3 = \{e, (1\,2), (2\,3), (1\,3), (1\,2\,3), (3\,2\,1)\}$

$\overset{\wr}{e}$, $\overset{\wr}{(1\,2)}$, $\overset{\wr}{(2\,3)}$, $\overset{\wr}{(1\,3)}$, $\overset{\wr}{(3\,2\,1)}$, $\overset{\wr}{(1\,2\,3)}$

1) $H = \langle (1\,2) \rangle$ este normal?

$(1\,2\,3)(1\,2)(3\,2\,1) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\,3) \notin H \Rightarrow$
$H \ntrianglelefteq$ normal

$\underbrace{[G:H]}_{\text{indicele subgr. în grup}} = \dfrac{\text{ord}(G)}{\text{ord}(H)}$

• Dacă $[G:H] = 2 \Rightarrow H \trianglelefteq G$

2) $H = \langle (1\,2\,3) \rangle = A_3$

$\dfrac{\text{ord}(S_3)}{\text{ord}(H)} = 2 \Rightarrow H \trianglelefteq S_3$

Grupul factor

$H \trianglelefteq G \longrightarrow G/H = \{\hat{x} : x \in G\}$
$= \{xH : x \in G\}$

$S_3/A_3 = \{\sigma \circ A_3 : \sigma \in S_3\} = \{\hat{e}, \widehat{(1\,2)}\}$

$A_3 = \{e, (1\,2\,3), (2\,1\,3)\}$

$e \cdot A_3 = A_3$
$(1\,2)A_3 = \{(1\,2), (2\,3), (1\,3)\} = (1\,3)A_3 = (2\,3)A_3$

$(1\,2)(1\,2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\,3)$

Teorema fundamentală de izomorfism
(pt. grupuri)

$f : G_1 \to G_2$, morfism de gr.

$\Rightarrow \begin{cases} ① \ \ker f \trianglelefteq G_1 \\ ② \ G_1/\ker f \underset{\text{izo}}{\simeq} \text{Im} f \end{cases}$

$\hat{x} \longmapsto f(x)$

$\ker f = \{x : f(x) = 0\}$

Temă:

$f : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$
$f(x) = \cos 2\pi x + i \sin 2\pi x$

a) $\ker f = ?$ $\text{Im} f = ?$

b) ? $\Rightarrow$ T.F.I.

Seminar 8

Permutări

Thm

$\sigma \in S_n \Rightarrow \sigma$ se scrie în mod unic ca prod. de cicluri disjuncte

Ex

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

$$\sigma = (1\,2\,3\,4)(5\,9)\underbrace{(6)}\,(7\,8)$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 7 & 6 & 4 & 5 & 1 \end{pmatrix}$$

$$\tau = (1\,2\,3\,7)(4\,6\,5)$$

- $\underset{x \in S_n}{\mathrm{ord}(x)} = \mathrm{lcm}$(lungimile ciclurilor disjuncte din descompunere)

$$\mathrm{ord}(\sigma) = [4, 2, 1, 2] = 4 \Rightarrow \sigma^4 = e$$

$$\mathrm{ord}(\tau) = [4, 3] = 12 \Rightarrow \tau^{12} = e$$

1) $S_n = \langle (1, i),\ i = \overline{2,n} \rangle$

- $(a_1, \dots, a_k) \begin{cases} \to (a_1, a_2)(a_2, a_3)\dots(a_{k-1}, a_k) \\ \to (a_1, a_k)(a_1, a_{k-1})\dots(a_1, a_2) \end{cases}$

- Știm $S_n = \langle (i,j) : 1 \le i < j \le n \rangle$

$\left.\begin{array}{l} i = 1 \to (i,j) = (1,j) \\ i \neq 1 \to (i,j) = (1,i)(1,j)(1,i) \end{array}\right\} \Rightarrow S_n = \langle (1,k) : k = \overline{2,n} \rangle = \langle (1,2), (1,3) \dots (1,n) \rangle$

Def

(i,j) = inversiune

$i < j$ și $\sigma(i) > \sigma(j) \to \mathrm{inv}(\sigma)$ = nr. inv. lui σ

Def

$\varepsilon(\sigma) = (-1)^{\mathrm{inv}(\sigma)}$

(signatura)

obs

1) $\underbrace{(a_1 \dots a_k)}_{c} \begin{cases} \to \mathrm{ord}(c) = k \\ \to \varepsilon(c) = (-1)^{k-1} \end{cases}$

2) $\sigma = c_1 \dots c_p \to \varepsilon(\sigma) = \varepsilon(c_1)\varepsilon(c_2)\dots\varepsilon(c_p)$

$\Rightarrow \varepsilon(\sigma) = (-1)^{n-p}$ (punem în desc. și (a))

$\begin{cases} \bullet\ \varepsilon(\sigma) = 1 \Rightarrow \sigma = \text{pară} \\ \bullet\ \varepsilon(\sigma) = -1 \Rightarrow \sigma = \text{impară} \end{cases}$

Exc

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

a) Desc. în cicluri și transp.

b) $\mathrm{ord}(\sigma)$, $\varepsilon(\sigma)$

c) $\sigma^{2019} = ?$

d) Rez. ec. $x^4 = \sigma$

c) $\sigma^{2019} = \sigma^{2016} \cdot \sigma^3 = \sigma^3$

$\mathrm{ord}(\sigma) = 4 \Rightarrow \sigma^{4k} = e$

$$\sigma = \underset{c_1}{(1\,2\,5\,7)}\,\underset{c_2}{(3\,9)}\,\underset{c_3}{(4)}\,\underset{c_4}{(6\,10\,8\,11)}$$

$$\sigma^3 = c_1^3 c_2^3 c_4^3$$

$\mathrm{ord}(c_1) = 4 \Rightarrow c_1^3 = c_1^{-1} = (1\,7\,5\,2)$

$$c_1: \begin{tikzcd} 1 \arrow[r] & 2 \arrow[d] \\ 7 \arrow[u] & 5 \arrow[l] \end{tikzcd} \qquad c_1^{-1}: \begin{tikzcd} 1 \arrow[d] & 2 \arrow[l] \\ 7 \arrow[r] & 5 \arrow[u] \end{tikzcd}$$

$\mathrm{ord}(c_2) = 2 \Rightarrow c_2^3 = c_2 = (3\,9)$

$\mathrm{ord}(c_4) = 4 \Rightarrow c_4^3 = c_4^{-1} = (6\,11\,8\,10)$

$$\begin{tikzcd} 6 \arrow[r] & 10 \arrow[d] \\ 11 \arrow[u] & 8 \arrow[l] \end{tikzcd}$$

$$\Rightarrow \sigma^3 = (1\,7\,5\,2)(3\,9)(6\,11\,8\,10)$$

d) $x^4 = \sigma = (1\,2\,5\,7)(3\,9)(4)(6\,10\,8\,11)$

$\varepsilon(\sigma) = -1$

Dacă $(\exists)\, x \in S_{11} \Rightarrow \varepsilon(x^4) = \varepsilon(\sigma)$ Fals

$\Rightarrow \varepsilon(x^4) = (\varepsilon(x))^4 = 1$

2) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 6 & 7 & 2 & 1 & 4 & 8 \end{pmatrix} \in S_8$

a) Desc. în C + T

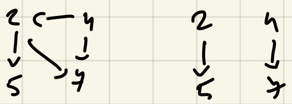
b) $ord(\sigma)$, $\varepsilon(\sigma)$

c) $\sigma^{1004} = ?$

d) Rez. în $S_8 \to x^2 = \sigma$

a) $(1\,3\,6)(2\,5)(4\,7)(8) =$

$= (1\,6\,3)(4\,2\,7\,5)$



$x^2 = (1\,3\,6)(2\,5)(4\,7)$

$x \in S_8 \Rightarrow x = k_1 \dots k_s$

$x^2 = k_1^2 \dots k_s^2$

ex

$(1\,3\,6)^2 = (1\,6\,3)$

$(1\,2\,3\,4\,5\,6)^2 = (1\,3\,5)(2\,4\,6)$

• $(1\,3\,6)$ - provine dintr-un ciclu de lung. 3 (pt. că e unicul ciclu de lung 3)

$(a_1\, a_2\, a_3)^2 = (1\,3\,6)$

$(a_1\, a_3\, a_2) = (1\,3\,6) \Rightarrow (1\,6\,3)$

• $(2\,5)(4\,7) = (a_1\, a_2\, a_3\, a_4)^2$

$(2\,5)(4\,7) = (a_1\, a_3)(a_2\, a_4)$

$(2\,4\,5\,7)$

$(4\,2\,7\,5)$

$S = \{(1\,6\,3)(2\,4\,5\,7)\ ;\ (1\,6\,3)(4\,2\,7\,5)\}$

3) Rez. ec. $x^2 = (1\,2\,3)(4\,5\,6) \in S_6$

4) $Hom(\mathbb{Q}, \mathbb{Z}) = ?$

↳ mult. morf. de gr. $(\mathbb{Q},+) \to (\mathbb{Z},+)$

↳ Fie $f: \mathbb{Q} \to \mathbb{Z}$ morfism

$f(x) = \underbrace{f(\frac{x}{n}) + f(\frac{x}{n}) + \dots + f(\frac{x}{n})}_{n \text{ ori}}$

$f(x) = n \cdot f(\frac{x}{n})$, $f(\frac{x}{n}) \in \mathbb{Z}$

$\Rightarrow f(x) ⋮ n, (\forall) n \in \mathbb{Z}^*$

$\Rightarrow f(x) \equiv 0$ (pt. că 0 e singurul nr. întreg divizibil cu orice n întreg)

5) $Hom(\mathbb{Z}_3, \mathbb{Z}_7) = ?$; $(\mathbb{Z}_3,+), (\mathbb{Z}_7,+)$

Fie $f: \mathbb{Z}_3 \to \mathbb{Z}_7$

$f(\hat{x}) = f(\underbrace{\hat{1}+\hat{1}+\dots+\hat{1}}_{x \text{ ori}}) = \widetilde{x \cdot f(\hat{1})} = \tilde{x}\,\tilde{a}$, $x \in \mathbb{Z}$

$f(\hat{1}) = \tilde{a} \in \mathbb{Z}_7$

$\tilde{0} = f(\hat{3}) = \widetilde{3 \cdot a} \Rightarrow 3 \cdot a ⋮ 7 \Rightarrow a ⋮ 7 \Rightarrow a = 0$

$\Rightarrow f(\hat{x}) = \tilde{0}$

6) $Hom(\mathbb{Z}_4, \mathbb{Z}_8)$

.....

$\tilde{0} = f(\hat{4}) = \widetilde{4a} \Rightarrow 4a ⋮ 8 \Rightarrow a ⋮ 2$, $\tilde{0} \in \mathbb{Z}_8$, $a \in \mathbb{Z}_8$

$\hat{x} \mapsto \tilde{0}$

$\hat{x} \mapsto \widetilde{2x}$

$\hat{x} \mapsto \widetilde{4x}$

$\hat{x} \mapsto \widetilde{6x}$

Temă: $Hom(\mathbb{Z}_n, \mathbb{Z}_m)$

Seminar 10

$(\mathbb{R}, +, \cdot)$ = inel dacă:

1) $(\mathbb{R}, +)$ gr. com (A, En, Es, C)

$0_{\mathbb{R}}$ - En

$-a$

2) $(\mathbb{R}, \cdot)$ - monoid (A, En)

$1_{\mathbb{R}}$ - En

a^{-1}

3) $\cdot$ = distrib. față de $+$

$a(b+c) = ab + ac$

$(a+b)c = ac + bc$

Obs

1) $(\mathbb{R}, \cdot)$ - monoid com.

$\Rightarrow (\mathbb{R}, +, \cdot)$ - inel. com.

2) Dacă $(\mathbb{R} \setminus \{0\}, \cdot)$ - grup

$\Rightarrow \mathbb{R}$ = corp

1) $(\mathbb{N}, +, \cdot) \neq$ inel

2) $(\mathbb{Z}, +, \cdot)$ = inel

3) $(\mathbb{Q} / \mathbb{R} / \mathbb{C}, +, \cdot)$ = corpuri

4) $M_n(\mathbb{Z})$ = inel

Elemente într-un inel $(\mathbb{R}, +, \cdot)$

1) $x \in \mathbb{R}$ idempotent dacă $x^2 = x$, $x^n = x$, $(\forall) n \geq 2$

ex: $M_2(\mathbb{Z}) \to \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

2) $x \in \mathbb{R}$, nilpotent dacă $(\exists)\, n \in \mathbb{Z}$ a.î. $x^n = 0$

3) $x \in \mathbb{R}$ div. al lui zero dacă $(\exists)\, 0 \neq y \in \mathbb{R}$ a.î.

$xy = 0$ sau $yx = 0$

Obs

$\emptyset \neq I \subseteq_{\text{inel}} \mathbb{R}$ ideal dacă: 1) $x - y \in I$, $(\forall)\, x, y \in I$

2) $(\forall)\, x \in I$, $r \in \mathbb{R}$, $xr \in I$, $rx \in I$

1) Un corp are 2 ideale $0, \mathbb{R}$

2) $I = (a_1, \ldots, a_n) \Rightarrow I$ = finit generat

3) $I = (a) \Rightarrow I$ = principal

Teorema fund. de izo. de inele:

$f: R_1 \to R_2$ morf. de inele $\begin{cases} 1) f(a+b) = f(a) + f(b) \\ 2) f(a \cdot b) = f(a) \cdot f(b) \\ 3) f(1_{R_1}) = 1_{R_2} \end{cases}$

$\Rightarrow$ 1) $\ker f$ = ideal în R_1

2) $R_1 / \ker f \underset{\text{izo}}{\simeq} \operatorname{Im} f$

Se folosește:

1) pt. a arăta că o mulț. e ideal

2) Dacă alegem f = morf. surj.

$\hookrightarrow R_1 / \ker f \simeq R_2$

Aplicații

1) Stab. dacă I, J ideale în $M_2(\mathbb{Z})$

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

$J = \{\begin{pmatrix} 2a & 2b \\ 2c & 2d \end{pmatrix}, a,b,c,d \in \mathbb{Z}\}$

cu def:

1) $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} - \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \in I \Leftrightarrow \begin{pmatrix} a-x & 0 \\ b-y & c-z \end{pmatrix} \in I$ „A"

2) $\underbrace{\begin{pmatrix} x & y \\ z & t \end{pmatrix}}_{\in M_2(\mathbb{Z})} \underbrace{\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}}_{\in I} = \begin{pmatrix} & 4c \\ & \end{pmatrix} \notin I$ $4c \neq 0$

$\Rightarrow I \neq$ ideal

J = ideal cum discutat,

2) Arăt. că (∀) ideal din $M_2(\mathbb{Z})$ este de forma $M_2(n\cdot\mathbb{Z})$

(1) $M_2(n\mathbb{Z})$ = ideal
- cu def.
- cu T.F.I.

$f: M_2(\mathbb{Z}) \longrightarrow M_2(\mathbb{Z}_n)$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix}$ morf. surj.

$\ker f = M_2(n\mathbb{Z})$ = ideal în $M_2(\mathbb{Z})$

Obs

$\mathbb{Z} \to n\mathbb{Z}$ = ideal generat de n

$(2,4) \to 2x+4y$
$= (2)$

$(3,5) \to 3x+5y$
$= \mathbb{Z}$

(2) I = ideal în $M_2(\mathbb{Z})$ și arăt. că $I = M_2(n\mathbb{Z})$

J = mulțimea el. matricelor din I

$J = n\mathbb{Z}$

$\begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & n \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ n & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & n \end{pmatrix} \in I$

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} n & m \\ p & q \end{pmatrix} = \begin{pmatrix} n & m \\ 0 & 0 \end{pmatrix}$ etc

3) R_1, R_2 inele com.

Arătați că $(\forall)$ ideal din $R_1 \times R_2$

este de forma $I_1 \times I_2$

unde I

4) Dec. dacă:

a) $(X^3 - 2X^2, X^4) = (X^2)$ în $\mathbb{Z}[X]$

$X^3 - 2X^2 = X^2(X-2)$

$X^4 = X^2 \cdot X^2$

$\Downarrow$

$I_1 \subseteq I_2$

Dem că $I_2 \subseteq I_1$

$X^2 \in I_1$?

$I_1 = \{f \cdot (X^3 - 2X^2) + g \cdot (X^4)\}$

$f = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n$

$(X^3 - 2X^2) f = a_0 X^3 + a_1 X^4 + a_2 X^5 + \dots + a_n X^{n+3}$
$\quad - 2a_0 X^2 + 2a_1 X^3 - \dots - 2a_n X^{n+2}$

Pot să aleg g a.î.:

$(X^3 - 2X^2) f + g X^4 =$

$= a_0 X^3 - 2a_0 X^2 + 2a_1 X^3$

$\Rightarrow a_0 = -\frac{1}{2} \notin \mathbb{Z}$

$\Rightarrow I_1 \neq I_2$

Temă: $(X^3 - X + 2, X^2 + X) = \mathbb{Z}[X]$?

$= \mathbb{Q}[X]$?

5) Det. nilpotenții din $\mathbb{Z}_n$

$x \in \mathbb{Z}_n$ nil. dacă $(\exists)\, t \in \mathbb{N}$ a.î. $x^t = 0$

$n = p_1^{e_1} \cdots p_k^{e_k}$

x - nil $\Leftrightarrow$ $x = p_1 \cdot \ldots \cdot p_k \cdot p$

„$\Rightarrow$" $x^t = 0$ (nilp.)

pp. că $x \nmid p_i \Rightarrow (\forall)\, t \in \mathbb{N},\ x^t \nmid p_i^{e_i} \Rightarrow x^t \nmid n$

$\Rightarrow x^t \neq 0$ în $\mathbb{Z}_n$

„$\Leftarrow$" $x^{\max(e_1, \ldots, e_k)} = 0$ ✓

$\mathbb{Z}_{48} \to 0, 6, 12, 18, 24, 30, 36, 42$ = nilp.

$48 = 2^3 \cdot 3$

6) Arătați că nilp. = ideal într-un inel com.

$\text{nilp} = \{x \in R \mid (\exists)\, n \in \mathbb{N}$ a.î. $x^n = 0\}$

1) $0 \in I$? $0^n = 0,\ (\forall)\, n$

2) $\underset{I}{x} - \underset{I}{y} \in I \Leftrightarrow (x-y)^n = 0$

aleg $n = a+b$

unde $x^a = 0,\ x^b = 0$

3) $\underset{R}{r} \cdot \underset{I}{x} \in I \Leftrightarrow (r \cdot x)^n = 0$

$\Rightarrow r^n \cdot \underbrace{x^n}_{0} = 0$

$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k \cdot b^{n-k}$

Seminar 11

$I \subseteq R$ ideal: $\begin{cases} 1) x-y \in I, (\forall) x,y \in I \\ 2) xr \in I, rx \in I, (\forall) x \in I, r \in R \end{cases}$

1) $(R,+,\cdot)$ = inel

R = corp $\Leftrightarrow$ R are doar 2 ideale

R-inel $\Rightarrow$ R are cel puțin 2 ideale: 0, R

„$\Rightarrow$"

R = corp dacă $(\underset{(e_2)}{R\setminus\{0\}}, \cdot)$ e grup $\Rightarrow$ $(\forall) x \in R\setminus\{0\}$, $(\exists)$ $x^{-1} \in R$ a.î. $x \cdot x^{-1} = 1$

Pp. că $(\exists)$ I ideal în R $(I \neq \emptyset)$

Fie $x \in I$, $r = x^{-1} \in R$ $\Big| \Rightarrow x \cdot r \in I \Rightarrow x \cdot x^{-1} \in I \Rightarrow 1 \in I \Rightarrow \underline{I = R}$

„$\Leftarrow$"

R are doar 2 ideale $\Rightarrow$ 0, R ideale în R

Pp că R nu e corp

$\Rightarrow (\exists)$ $x \in R$ a.î. $x \cdot y \neq 1$, $(\forall) y \in R$

Fie $I \subseteq R$ cu $I = (x)$ ideal, dar $1 \notin I \Rightarrow$ R are cel puțin 3 ideale, 0, R, I (fals)

$\Rightarrow$ $\underline{R \text{ corp}}$

TFI

$f: R_1 \to R_2$ morf de inele

Atunci: 1) $\ker f$ = ideal în R_1

2) $R_1/\ker f \simeq \operatorname{Im} f$

2) A = inel com, $a \in A$

Dem. că $\underbrace{A[X]}_{R_1} / \underbrace{(X-a)}_{\ker f} \simeq \underbrace{A}_{R_2 = \operatorname{Im} f}$

Morf. inele: 1) $f(a+b) = f(a) + f(b)$

2) $f(a \cdot b) = f(a) \cdot f(b)$

3) $f(1_{R_1}) = 1_{R_2}$

Caut $\varphi: A[X] \to A$ morf. surj. de inele

$\varphi(f(x)) = f(a)$ (morf de eval în a)

1) Morf. de inele

1.1) $\varphi(f(x) + g(x)) = \varphi(f(x)) + \varphi(g(x))$

$\varphi((f+g)(x))$

$(f+g)(a) = f(a) + g(a)$

1.2) Analog

1.3) $\varphi(1) = 1$

Din 1), 2), 3)

$\Rightarrow$ $A[X]/(X-a) \simeq A$

2) $\ker \varphi = \{f \in A[X] : \varphi(f) = 0\}$

$\ker \varphi = (X-a)$

$f(a) = 0 \Leftrightarrow f$ are răd. $a \Leftrightarrow f = (x-a) \cdot g$

3) φ = surj.

$\Leftrightarrow (\forall) y \in A, (\exists) f \in A[X]$ a.î. $\varphi(f(x)) = y \Leftrightarrow f(a) = y$

$f(x) = x - a + y$

$\Rightarrow \varphi$ surj.

3) Verif. de. I

1) $\overbrace{(X^2-1, X+2)}=\mathbb{Z}[X]$ | $I_1=I_2 \iff \begin{cases} I_1\subseteq I_2 \\ I_2\subseteq I_1\end{cases}$

„$\subseteq$" ✓

„$\supseteq$"

$$\begin{array}{r|l} X^2-1 & X+2 \\ -X^2-2X & X-2 \\ \hline -2X-1 & \\ +2X+4 & \\ \hline \boxed{3} & \end{array} \Rightarrow X^2-1=(X+2)(X-2)+3$$

$f\in I \Rightarrow f=(X^2-1)\cdot f_1+(X+2)\cdot f_2=$

$=(X+2)(X-2)\cdot f_1+3f_1+(X+2)f_2=$

$=\underbrace{(X+2)}((X-2)f_1+f_2)+\underbrace{3}f_1\in I$

$\Rightarrow I=(X+2,3)$

$1\in I$?

$1=(X+2)g_1+3g_2$ | evaluat în $x=-2$

$\Downarrow$

$1=3g_2 \Rightarrow g_2=\frac{1}{3}\notin\mathbb{Z}$

$\Rightarrow I\neq\mathbb{Z}[X]$

? $I=\mathbb{Q}[X]$? Da $1=(X+2)\cdot 0+3\cdot\frac{1}{3}$

2) $I_1=(X^2-3X+2, X+2)$

$I_2=(X^3-X+1, X-2)$

$I_1=I_2$ în $\mathbb{Z}[X]$

Obs

$f/(X-a)$ dă restul $f(a)$

θ $\underbrace{\mathbb{Z}[X]}_{R_1}/\underbrace{(X^2-X)}_{\ker f}\simeq\underbrace{\mathbb{Z}\times\mathbb{Z}}_{R_2}$

"Im f"

$\ker f=(X^2-X)=\{f: f=(X^2-X)\cdot g\}$

$=\{f\in\mathbb{Z}[X]: f=X(X-1)g\}$

$\Rightarrow \{f\in\mathbb{Z}[X]: f$ are rad. 0 și 1$\}$

$\Downarrow$

$f(0)=0$ și $f(1)=0$

$\underset{\ker f}{f(f)}=(0,0)$

$f(f(X))=(f(0),f(1))$

1) f morf.

1) $f(f+g)=((f+g)(0);(f+g)(1))=$

$=(f(0)+g(0); f(1)+g(1))=(f(0),f(1))+(g(0),g(1))=f(f)+f(g)$ ✓

2) Analog

3) $f(1)=(1,1)$

3) Surj.

$(\forall)\ a,b\in\mathbb{Z}$, $(\exists)\ f\in\mathbb{Z}[X]$ a.î. $f(f)=(a,b)$

$\Rightarrow f(0)=a \Rightarrow n=a$

$f(1)=b \Rightarrow m+a=b\Rightarrow m=b-a$

$f=mX+n$

$f=(b-a)X+a$

$\Uparrow$

$\mathbb{Z}[X]$

T.F.I.

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

2) $\ker f=(X^2-X)$

$\ker f=\{f\in\mathbb{Z}[X]: f(f)=(0,0)\}$

$\Updownarrow$

$(f(0),f(1))=(0,0) \iff \begin{cases} f(0)=0\\ f(1)=0\end{cases} \Rightarrow f$ are rad. 1 și 0

deci $f=(X-1)X\cdot g$

$\Rightarrow f=(X^2-X)\cdot g$

$\Rightarrow \ker f=(X^2-X)$

8) Rez în $\mathbb{Z}$:

$$\begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 5 \pmod{22} \end{cases}$$

dacă $(7, 22) = 1 \Rightarrow \mathbb{Z}_7 \times \mathbb{Z}_{22} \simeq \mathbb{Z}_{154}$

$\Rightarrow S = \{x_0 + 154k, k \in \mathbb{Z}\}$

$x_0 \in \{0, 1, \dots, 153\}$

$3 \to 10 \to 17 \to 24 \to 31 \to 38 \to \dots \to 115$

$5 \to 27 \to 49 \to 71 \to \dots \dots \dots \to 115$

$S = \{115 + 154k\}$

Obs (LCR)

Dacă $\gcd(n, m) = 1$

$\Rightarrow \mathbb{Z}_n \times \mathbb{Z}_m = \mathbb{Z}_{n \cdot m}$

Seminar 12

Alg. lui Euclid, $D = \mathbb{Z}$ sau $k[X]$

input: $a, b \in D$

output: $d = \gcd(a, b)$

while $b \neq 0$

$a : b = q$, rest r, $q, r \in D$

$a \leftarrow b$, $b \leftarrow r$

$d = a$

Exp: 1) $a = 348$, $b = 24$

$348 = 24 \cdot 14 + \boxed{12}$ r

$24 = 12 \cdot 2 + \underline{0}$

$\Rightarrow \gcd = 12$

~~Det.~~ Găsiți $m, n \in \mathbb{Z}$ a.î.

$m \cdot a + n \cdot b = \gcd(a, b)$

$12 = m \cdot 348 + n \cdot 24$

$12 = 348 \cdot 1 + (-14) \cdot 24$

$\Rightarrow m = 1, n = -14$

2) $a = 3737$, $b = 1517$

....

$m = 13$

$n = -32$

1) Verif. dacă $\hat{153}$ este inv. în $\mathbb{Z}_{461}$ și det. inversul dacă există.

Obs

$\hat{a}$ = inv. în $\mathbb{Z}_b$ dacă $(a, b) = 1$

$461 = 153 \cdot 3 + 2$

$153 = 2 \cdot 76 + 1$

$2 = 1 \cdot 2 + 0$

$\hat{1} = 153 \cdot m + 461 \cdot n \mid \bmod 461$

$\hat{1} = \hat{153} \cdot \hat{m}$

$1 = 153 - 2 \cdot 76$

$1 = 153 - (461 - 153 \cdot 3) \cdot 76$

$1 = 153 \cdot 229 - 461 \cdot 76$

$\Rightarrow (\hat{153})^{-1} = \hat{229}$

2) $\widehat{23}$ în $\mathbb{Z}_{120}$

$\Rightarrow \widehat{47}$

3) Det. câtul și restul împ. lui f la g în $\mathbb{Q}[X]$

$f = X^3 - 5X + 3$

$g = 2X + 3$

4) Stabiliți dacă f = inversabil în $\mathbb{Q}[X]/(X^3+1) = R$

$f = X^2 + 1$

f inv. dacă $(\exists)\, g$ a.î. $f \cdot \hat{g} = \hat{1}$

obs

$F \in \mathbb{Q}[X] \to F : (X^3+1) \to \underset{\text{(rest)}}{G}$ cu grad$(G) \le 2$

$\downarrow$

$\hat{g} = aX^2 + bX + c$

$(X^2+1)(aX^2+bX+c) = \hat{1}$

$aX^4 + bX^3 + cX^2 + aX^2 + bX + c$

$\underbrace{aX(X^3+1)}_{\hat{0}} - aX + \underbrace{b(X^3+1)}_{\hat{0}} - b + cX^2 + aX^2 + bX + c = \hat{1}$

$X^2(a+c) + X(b-a) + (c-b) = \hat{1}$

$\Rightarrow \begin{cases} a + c = 0 \Rightarrow c = -a \\ b - a = 0 \Rightarrow a = b \\ c - b = 1 \Rightarrow -a - a = 1 \end{cases}$

$-2a = 1$

$a = -\frac{1}{2} = b$

$c = \frac{1}{2}$

$\hat{g} = -\frac{1}{2} - \frac{1}{2}X + \frac{1}{2}$ - inv. lui f

b) $R = \mathbb{Q}[X]/(X^3+1)$

$f = X^2 - 1$

$f \in R$ div al lui zero dacă $(\exists)\ g \in R$, $g \neq \hat{0}$ a.î. $\hat{f} \cdot \hat{g} = \hat{0}$

$f = X^2 - 1 = (X-1)\underline{(X+1)}$

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

$\Downarrow$

$g = (X^2 - X + 1) \neq 0 \Rightarrow f \cdot g = (X-1)p = \hat{0}$

5) Stab. dacă $f = \hat{4}X + \hat{3}$ este inv. în $\mathbb{Z}_5[X]/(X^2 + \hat{1})$

Seminar 13

1) $x \in \mathbb{Z}$

$$\begin{cases} x \equiv 1 \pmod 3 \\ 3x \equiv 4 \pmod 5 \\ 4x \equiv 1 \pmod 7 \end{cases}$$

$(3,5)=1 \Rightarrow \hat{3}$ inv. în $\mathbb{Z}_5$
$(\hat{3} \cdot \hat{2} = \hat{1})$

$\Rightarrow 3x = 4 \,/\cdot 2$
$x \equiv 3 \pmod 5$

$(4,7)=1 \Rightarrow 4$ inv. în $\mathbb{Z}_7$
$(\hat{4} \cdot \hat{2} = \hat{1})$

$\Rightarrow 4x \equiv 1 \,/\cdot 2$
$x \equiv 2 \pmod 7$

$$\Rightarrow \begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

$(3,5)=1, (3,7)=1, (5,7)=1$

$\xRightarrow{LCR} (\exists)\, x_0 \in \mathbb{Z}_{3\cdot5\cdot7} = \mathbb{Z}_{105}$ sol.

$\cancel{8}, \cancel{16}, \cancel{23}, \cancel{30}, \cancel{37}, \cancel{44}, \cancel{51}, 58$

$x_0 = 58$
$\Downarrow$
$x = 105 \cdot p + 58$

Algoritm sist. de ec. modulare

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases} \quad (n_i, n_j) = 1$$

I. $n = n_1 \cdot n_2 \cdot \ldots \cdot n_k$

II. $n_i' = \frac{n}{n_i}$

III. t_i = inversul lui n_i' mod n_i

IV. $x_0 \equiv a_1 n_1' t_1 + a_2 n_2' t_2 + \ldots + a_k n_k' t_k \pmod n$
$\hookrightarrow x = n \cdot p + x_0,\ p \in \mathbb{Z}$

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

I. $n = 105$

II. $n_1' = 35$
$n_2' = 21$
$n_3' = 15$

III. $35 \equiv \underline{2} \pmod 3 \Rightarrow t_1 = 2$ (inv. lui 2)
$21 \equiv 1 \pmod 5 \Rightarrow t_2 = 1$ (inv. lui 1)
$15 \equiv 1 \pmod 7 \Rightarrow t_3 = 1$ (inv. lui 1)

IV. $x_0 = 1 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 =$
$= 70 + 63 + 30 = 163$
$163 \equiv 58 \pmod{105}$
$\Rightarrow x_0 = 58 \Rightarrow x = 105 \cdot p + 58,\ p \in \mathbb{Z}$

2) A = inel, $a \in A$ nilpotent
$\Rightarrow a \cdot X^i$ nilpotent în $A[X]$

a = nilp $\Rightarrow (\exists)\ t \in \mathbb{N}$ a.î. $a^t = 0$

$(a \cdot X^i)^t = a^t \cdot X^{ti} = 0$
$\Rightarrow a \cdot X^i$ = nilpotent

3) A = inel comutativ
a = nilpotent ; u = inversabil
$\Downarrow$
$u + a$ = inversabil

Seminar 14

Thm

$f = a_0 + a_1 X + \dots + a_n X^n \in A[X]$

1) f = nil. $\Leftrightarrow$ a_i = nilpotent, $(\forall)\ i = \overline{0,n}$

2) f = inv. $\Leftrightarrow$ a_0 = inv.
a_i = nil., $(\forall)\ i = \overline{1,n}$

"$\Leftarrow$"

$f = \underbrace{\underbrace{a_0}_{i} + \underbrace{a_1 X}_{n}}_{i} + \dots + \underbrace{a_n X^n}_{n}$

$i \dots i$

Aplicație:

1) Det. nr. de poli. nil./inv. din $\mathbb{Z}_{12}[X]$, grad 4

- $12 = 2^2 \cdot 3 \Rightarrow \hat{a}$ = nil. in $\mathbb{Z}_{12}$
  dacă $a \in M6 \Rightarrow \hat{a} = \hat{0}, \hat{6}$

- $(a, 12) = 1 \Rightarrow a$ = inv
  $\Rightarrow \hat{a} = \hat{1}, \hat{5}, \hat{7}, \hat{11}$

$a_0 + a_1 X + a_2 X^2 + a_3 X^3 + a_4 X^4,\ a_4 \neq \hat{0}$

NILP: $a_0 \to a_3$ $\{\hat{0}, \hat{6}\}$ $\quad 2^4 = 16$
a_4 $\{\hat{6}\}$

INV: a_0 $\{\hat{1}, \hat{5}, \hat{7}, \hat{11}\}$ $\quad 4 \cdot 2^3 = 32$
$a_1 \to a_3$ $\{\hat{0}, \hat{6}\}$
a_4 $\{\hat{6}\}$

3) Det. poli. ired. de grad ≤ 4 din $\mathbb{Z}_2[X]$

grad 1: $X + \hat{1}$; X

grad 2: $X^2 + bX + 1 \Rightarrow X^2 + X + 1$
$X = 1$: $\hat{1} + b + \hat{1} \neq \hat{0}$

grad 3: $X^3 + bX^2 + cX + 1$
$X = \hat{1}$: $\hat{1} + b + c + \hat{1} = \hat{1}$
$\Rightarrow b \neq c \Rightarrow (\hat{1}, \hat{0}); (\hat{0}, \hat{1})$

$X^3 + X + \hat{1}$
$X^3 + X^2 + \hat{1}$

2) Desc. $X^n - 1$ in fact. ired in $\mathbb{Q}, \mathbb{R}, \mathbb{C}[X]$ pt. $n = 2, 3, 4, 6$

$n = 2$: $X^2 - 1 = \underbrace{(X-1)(X+1)}_{\text{ired. in } \mathbb{Q}, \mathbb{R}, \mathbb{C}}$

$n = 3$: $X^3 - 1 = \underbrace{(X-1)(X^2+X+1)}_{\text{ired. in } \mathbb{Q}, \mathbb{R}}$

in $\mathbb{C}$ $= (X-1)(X-\varepsilon_1)(X-\varepsilon_2)$

$n = 4$: $X^4 - 1 = (X^2-1)(X^2+1) = \underbrace{(X-1)(X+1)(X^2+1)}_{\text{ired. in } \mathbb{Q}, \mathbb{R}}$

in $\mathbb{C}[X]$: $(X-1)(X+1)(X-i)(X+i)$

$n = 6$: $X^6 - 1 = (X^3-1)(X^3+1) = \underbrace{(X-1)(X^2+X+1)(X+1)(X^2-X+1)}_{\text{ired. in } \mathbb{Q}, \mathbb{R}}$

in $\mathbb{C}[X]$

$(X-1)(X+1)(X-\varepsilon_1)(X+\varepsilon_1)(X-\varepsilon_2)(X+\varepsilon_2)$

grad 4: $\to$ 3+1: nu are răd.

2+2: $(X^2+X+1)(X^2+X+1) = X^4 + \cancel{X^3} + X^2 + \cancel{X^3} + \cancel{X^2} + \cancel{X} + X^2 + \cancel{X} + 1 =$
$= X^4 + X^2 + 1$

$X^4 + aX^3 + bX^2 + cX + 1$

$X = 1 \to a + b + c = \hat{1} \Rightarrow 100, 010, 001, 111$

$X^4 + X^3 + 1,\ X^4 + X + 1,\ X^4 + X^3 + X^2 + X + 1$

Obs

A = inel de caracteristică p = nr. prim

$F: A \to A$, $F(k) = k^p$ = morf. de inele

$\Rightarrow F(k_1+k_2) = k_1^p + k_2^p = (k_1+k_2)^p$

$\hookrightarrow \mathbb{Z}_7$: car $\mathbb{Z}_7 = 7$

4) Desc. în $\mathbb{Z}_7$: $\overset{f=}{X^{56}} - X^{49} - X^7 + 1$ în $\mathbb{Z}_7[X]$
în fact. ired.

$f = X^{7\cdot 8} - X^{7\cdot 7} - X^{7\cdot 1} + 1^{7\cdot 1} =$

$= (X^8 - X^7 - X^1 + 1)^7$

$f = (X^7(X-1) - (X-1))^7 = ((X^7-1)(X-1))^7 = ((X-1)^7(X-1))^7 = ((X-1)^8)^7 = (X-1)^{56}$

5) $f = X^4 + 2X^3 + 3X^2 + X + 1$
ired în $\mathbb{Q}[X]$

Obs

$f = a_0 + a_1 X + \dots + a_n X^n \in \mathbb{Z}[X]$

f ired. în $\mathbb{Z}[X] \Leftrightarrow$ f ired în $\mathbb{Q}[X]$
$\gcd(a_0, \dots, a_n) = 1$

1) $g_1 \cdot g_3 \to$ răd.

$\frac{u}{v}$ = răd. $\Leftrightarrow$ $u \mid \underset{}{a_0} \overset{}{=} 1$, $v \mid a_n = 1$ $\Rightarrow \frac{u}{v} = \pm 1$

$x = -1$: $1 - 2 + 3 - 1 + 1 \neq 0$
$\Rightarrow$ nu are răd.

$g_2 \cdot g_2 = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + (a_0 b_2 + a_1 b_1 + a_2 b_0) X^2 + (a_1 b_2 + b_1 a_2) X^3 + a_2 b_2 X^4 = f$

h g $\in \mathbb{Z}[X]$

$(a_0 + a_1 X + a_2 X^2)(b_0 + b_1 X + b_2 X^2) = f$

$a_0 b_0 = 1 \Rightarrow a_0 = b_0 = \pm 1$

$a_2 b_2 = 1 \Rightarrow a_2 = b_2 = \pm 1$

$a_0 b_1 + a_1 b_0 \Rightarrow a_0 (b_1 + a_1) = 1 \Rightarrow b_1 + a_1 = a_0 = \pm 1$

$a_1 b_2 + b_1 a_2 = 2$

$a_2 (b_1 + a_1) = 2$

$\pm 1 \cdot \pm 1 = 2$ F

$\Rightarrow f$ ired în $\mathbb{Z}[X] \Rightarrow f$ ired. în $\mathbb{Q}[X]$

Criteriul Eisenstein

$f = a_0 + a_1 X + a_2 X^2 + \dots + X^n \in \mathbb{Z}[X]$
$(a_n = 1)$

$(\exists)\, p \in \mathbb{N}$ a.î. $\left.\begin{array}{l} p \mid a_i\,;\ i = \overline{0, n-1} \\ p^2 \nmid a_0 \end{array}\right\} \Rightarrow f$ ired. în $\mathbb{Q}[X]$

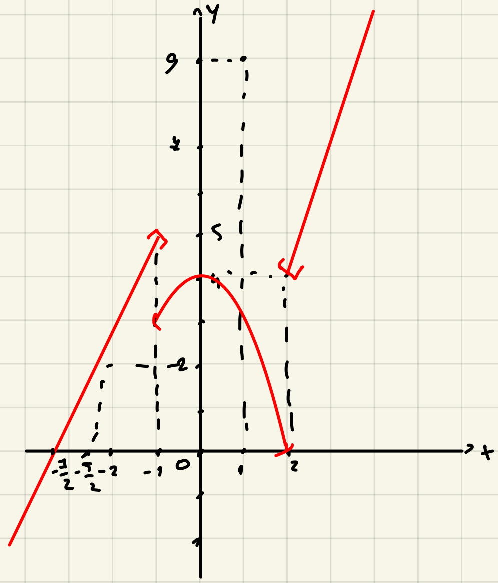
Ex: $f = X^4 + 2X^3 + 12X^2 + 24X + 2$

$\left.\begin{array}{l} p = 2 \mid 2, 12, 24 \\ 4 \nmid 2 \end{array}\right\} \Rightarrow f$ ired. în $\mathbb{Q}[X]$

1.

$f:\mathbb{R}\to\mathbb{R}$, $f(x)=\begin{cases}2x+7, & x\le -1\\ -x^2+4, & -1<x<2\\ 3x-2, & x\ge 2\end{cases}$

$f(-3)=1 \quad f(-1)=5$



$4-x^2=(2-x)(2+x)=$
$=-(x-2)(x+2)$

$V_x=\frac{-b}{2a}=0$

$V_y=\frac{-b^2+4ac}{4a}=$
$=-\frac{16}{4}=4$

a) $f([-3,2])=(0,5]$

$f^{-1}([0,2])=[-\frac{7}{2};-\frac{5}{2}]\cup(\sqrt{2};2)$

$2x+7=0 \Rightarrow x=-\frac{7}{2}$

$2x+7=2 \Rightarrow x=-\frac{5}{2}$

$-x^2+4=2$

$-x^2=-2$

$x^2=2$

$x=\pm\sqrt{2}$

b) f nu este inj;

$y=4$ este atins şi când $x=0$, şi când $x=-\frac{3}{2}$, şi când $y=2$

f este surj:

$Im(f)=\mathbb{R}$

c) $f^{-1}(y)$

$y\in(3,4]$

pt. acești y, există câte 3 x a.î. $f(x)=y$

3.

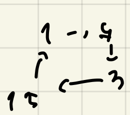
$c_1 \quad c_2 \quad c_3 \quad c_4 \quad c_5$

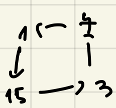
a) $(1\ 7\ 3\ 15)(2\ 9)(4\ 10\ 6\ 8\ 14)(5\ 13)(11\ 12)$

b) $ord(\sigma)=cmmmc(4,2,5)=20$

$\Rightarrow \sigma^{2023}=\sigma^3=c_1^3c_2^3c_3^3c_4^3c_5^3$

$ord(c_1)=4 \Rightarrow c_1^3=c_1^{-1}=(1\ 15\ 3\ 7)$



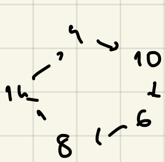


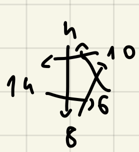
$\sigma^3=(1\ 15\ 3\ 7)(2\ 9)(4\ 8\ 10\ 14\ 6)(5\ 13)(11\ 12)$

$ord(c_2)=2 \Rightarrow c_2^4=c_2$

Analog c_4 şi c_5

$ord(c_3)=5 \Rightarrow c_3^3=c_3^{-2}=(4\ 8\ 10\ 14\ 6)$





c) $\tau^3=\sigma$

$(1\ 2)^3=(1\ 2)$

$(1\ 2\ 3\ 4)^3=(1\ 4\ 3\ 2)$

$(1\ 2\ 3\ 4\ 5)^3=(1\ 4\ 2\ 5\ 3)$

$(1\ 2\ 3\ 4\ 5\ 6)^3=(1\ 4)(2\ 5)(3\ 6)$

$(a\ b\ c\ d)^3=(1\ 7\ 3\ 15)$

$(a\ d\ c\ b)=(1\ 7\ 3\ 15)$

$\Rightarrow (a\ b\ c\ d)=(1\ 15\ 3\ 7)$

$(a\ b\ c\ d\ e)^3=(4\ 10\ 6\ 8\ 14)$

$(a\ d\ b\ e\ c)=(4\ 10\ 6\ 8\ 14)$

$\Rightarrow (a\ b\ c\ d\ e)=(4\ 6\ 14\ 10\ 8)$

$(a\ b\ c\ d\ e\ f)^3=(2\ 9)(5\ 13)(11\ 12)$

$(a\ d)(b\ e)(c\ f)=(2\ 9)(5\ 13)(11\ 12)$

$+(9\ 13\ 11\ 2\ 5\ 12)$

$\tau=(1\ 15\ 3\ 7)(4\ 6\ 14\ 10\ 8)(2\ 9)(5\ 13)(11\ 12)$

$\tau=(1\ 15\ 3\ 7)(4\ 6\ 14\ 10\ 8)(2\ 5\ 11\ 9\ 13\ 12)$

$\Rightarrow \tau=(1\ 15\ 3\ 7)(4\ 6\ 14\ 10\ 8)(2\ 13\ 11\ 9\ 5\ 12)$

$\tau=(1\ 15\ 3\ 7)(4\ 6\ 14\ 10\ 8)(2\ 5\ 12\ 9\ 13\ 11)$

$\tau=(1\ 15\ 3\ 7)(4\ 6\ 14\ 10\ 8)(2\ 13\ 12\ 9\ 5\ 11)$

2.

$f_1(x) = \frac{1}{x}$ $\quad f_2(x) = \frac{1}{1-x}$

Dem. că f_1, f_2 bij. din D în D

f_1 inj. $\Leftrightarrow (\forall)\, x_1, x_2 \in D,\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

$f(x_1) = f(x_2) \Leftrightarrow \frac{1}{x_1} = \frac{1}{x_2} \Leftrightarrow x_1 = x_2$

f_1 surj. $\Leftrightarrow (\forall)\, y \in D, (\exists)\, x \in D$ a.î. $f(x) = y$

Fie $y \in D$

$\frac{1}{x} = y \Rightarrow x = \frac{1}{y} \in D$

Analog f_2

$f_1^2 = f_1 \circ f_1 = \frac{1}{\frac{1}{x}} = x$

$\Rightarrow \text{ord}(f_1) = 2$

$f_2^2 = f_2 \circ f_2 = \frac{1}{1 - \frac{1}{1-x}} = \frac{1}{\frac{x}{x-1}} = \frac{x-1}{x}$

$f_2^3 = f_2 \circ f_2 \circ f_2 = \frac{1}{1 - \frac{x-1}{x}} = \frac{1}{\frac{1}{x}} = x$

$\Rightarrow \text{ord}(f_2) = 3$

b) $f_0 = x \quad f_1 = \frac{1}{x} \quad f_2 = \frac{1}{1-x} \quad f_3 = \frac{x-1}{x}$

$f_3 \circ f_1 = \frac{\frac{1}{x} - 1}{\frac{1}{x}} = \frac{\frac{1-x}{x}}{\frac{1}{x}} = \frac{1-x}{x} \cdot x = 1 - x$

$\Rightarrow f_4 = 1 - x$

$f_3 \circ f_4 = \frac{1-x-1}{1-x} = -\frac{x}{1-x} = \frac{x}{x-1}$

$\Rightarrow f_5 = \frac{x}{x-1}$

4. $\mathbb{Z}[i\sqrt{2}] = \{a + bi\sqrt{2} \mid a, b \in \mathbb{Z}\}$

a) $1 \in \mathbb{Z}[i\sqrt{2}]$

$x = a + bi\sqrt{2},\ y = c + di\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$

$x - y = a - c + (b-d)i\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$

$xy = ac + adi\sqrt{2} + bci\sqrt{2} - 2bd =$

$= ac - 2bd + (ad + bc)i\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$

$\Rightarrow \mathbb{Z}[i\sqrt{2}] \subset (\mathbb{C}, +, \cdot)$

b) Fie $x = a + bi\sqrt{2},\ x' = a' + b'i\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$

$xx' = 1$

$(a + bi\sqrt{2})(a' + b'i\sqrt{2}) = 1$

$\Rightarrow a + bi\sqrt{2} = \pm 1$

$\Rightarrow b = 0,\ a = \pm 1$

Deci $U(\mathbb{Z}[i\sqrt{2}]) = \{\pm 1\}$

c) $I = (1 + i\sqrt{2})$

$I = \{(1 + i\sqrt{2}) \cdot (c + di\sqrt{2}) \mid c, d \in \mathbb{Z}\}$

$\Leftrightarrow$

$c + di\sqrt{2} + ci\sqrt{2} - 2d$

$\Leftrightarrow$

$c - 2d + (c + d)i\sqrt{2}$

„$\Rightarrow$" $a + bi\sqrt{2} \in I \Leftrightarrow$ $\begin{array}{l} c - 2d = a \\ \underline{c + d = b} \end{array}$

„$-$"

$-3d = a - b$

$\Rightarrow d = \frac{b-a}{3}$, dar $d \in \mathbb{Z}$

$\Rightarrow 3 \mid b - a \Leftrightarrow 3 \mid a - b$

„$\Leftarrow$"

$3 \mid a - b \Rightarrow a - b = 3n,\ n \in \mathbb{Z}$

$\Rightarrow a = b + 3n$

$a + bi\sqrt{2} = b + 3n + bi\sqrt{2}$

$(1 + i\sqrt{2})(1 + i\sqrt{2}) = 1 + i\sqrt{2} + i\sqrt{2} - 2 = -1 + 2i\sqrt{2}$

$\underbrace{\mathbb{Z}[i\sqrt{2}]}_{R_1} / \underbrace{I}_{\ker f} \simeq \underbrace{\mathbb{Z}_3}_{R_2}$

Fie $f : \mathbb{Z}[i\sqrt{2}] \to \mathbb{Z}_3$

a.î. $\ker f = I$

$f(x) = \widehat{a - b}$

I. $x \sim y \Leftrightarrow 2 \mid x+y$

1. R

$x \sim x \Leftrightarrow 2 \mid 2x$ „A"

S

$x \sim y \Leftrightarrow 2 \mid x+y \Leftrightarrow 2 \mid y+x \Leftrightarrow y \sim x$

T

$\left.\begin{matrix} x \sim y \Leftrightarrow 2 \mid x+y \\ y \sim z \Leftrightarrow 2 \mid y+z \end{matrix}\right\} \Rightarrow 2 \mid x+2y+z \Leftrightarrow 2 \mid x+z \Leftrightarrow x \sim z$

3. $x \sim y \Leftrightarrow x \equiv y \pmod 2$

$\mathbb{Z}/\sim = \{\hat{0}, \hat{1}\}$

$\mathbb{Z}/\sim$ ciclic și finit

$\Rightarrow \mathbb{Z}/\sim \simeq \mathbb{Z}_2$ structură unică

II.

1. $(\mathbb{Z}_7 \times \mathbb{Z}_{19}, +)$

$(\bar{3}, \hat{7})$

$3x = 7n$

$7x = 19m$

3	6	2	5	1	4	0	3	6	1	4	0	3	6	2	5	1	4	0
7	14	2	9	16	4	11	18	6	13	1	8	15	3	10	17	5	12	0
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

$\text{ord}(\bar{3}, \hat{7}) = 19$

III.

$(1\ 9\ 2)(3\ 10\ 5\ 8\ 7)(4\ 6) =$

$= (1 9)(9 2)(3 10)(10 5)(5 8)(8 7)(4 6)$

1 2 3 4

$(1\ 3\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$

$(1 3)(3 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$

2. $\varepsilon(\sigma) = (-1)^2 \cdot (-1)^4 \cdot (-1) = -1$

$\sigma^{2022+9} = \sigma^{2031}$

$\text{ord}(\sigma) = \text{cmmmc}(3, 5, 2) = 30$

$\Rightarrow \sigma^{2031} = \sigma^{21} = (1\ 9\ 2)^{21} (3\ 10\ 5\ 8\ 7)^{21} (4\ 6)^{21} =$

$$\begin{array}{r|l} 2031 & 30 \\ 180 & 67 \\ \hline 231 & \\ 210 & \\ \hline 21 & \end{array}$$

$= (3\ 10\ 5\ 8\ 7)(4\ 6)$