

Seminar 1

4.10.2021

Multimi (Notări)

A - multime $|A| =$ cardinalul lui A

(not) $\text{card}(A)$

$$|A| < \infty \Leftrightarrow A \text{-multime finită}$$

A, B multimi $A \neq B \Leftrightarrow A \setminus B \neq \emptyset \Leftrightarrow (\exists x) x \in A \text{ și } x \notin B$

$A = B \Leftrightarrow (A \subseteq B \text{ și } B \subseteq A) \Leftrightarrow (A \cap B = A \text{ și } A \cap B = B)$

Ex1 Dem. $\left\{ x \mid x = \frac{a+1}{2a+1}, a \in \mathbb{R} \setminus \left\{ -\frac{1}{2} \right\} \right\} = \mathbb{R} \setminus \left\{ \frac{1}{2} \right\}$.

ca $\frac{a+1}{2a+1} \neq \frac{1}{2}$ $\Rightarrow 2a+2 = 2a+1 \Rightarrow 0=1 \Rightarrow \text{pp e falsă} \Rightarrow A \subseteq B$

" \subseteq " $\frac{a+1}{2a+1} = \frac{1}{2} \Rightarrow 2ab+b = a+1 \Leftrightarrow b = \frac{a+1}{2a+1} \Leftrightarrow a = \frac{1-b}{2b-1} \in \mathbb{R} \Rightarrow B \subseteq A$

" \supseteq " Fie $b \in \mathbb{R} \setminus \left\{ \frac{1}{2} \right\} = B$ $a(2b-1) = 1-b$ $\Leftrightarrow b \neq \frac{1}{2}$

Din (1) și (2) $\Rightarrow A = B$.

(vezi mai târziu LCR)
Lema climeră a resturilor

Ex2 Dem. $(3N+2) \cap (5N+1) = 15N+11$

ca $\begin{array}{c} \parallel \\ A \\ \parallel \\ B \\ \parallel \\ C \end{array}$

" \supseteq " Fie $a \in 15N+11 \Rightarrow a = 15m+11 \quad p+m \in \mathbb{N}$

$\begin{array}{l} // \\ 3 \cdot (5m+3)+2 \Rightarrow a \in A \\ 5(3m+2)+1 \Rightarrow a \in B \end{array}$

$\Rightarrow a \in A \cap B$

" \subseteq " Fie $a \in A \cap B \Rightarrow a = 3m+2 = 5m+1 \quad p+m \in \mathbb{N}$

$\begin{array}{l} a \in A \\ a \in B \end{array}$

$3m+2 = 5m+1 \Rightarrow 3m = 5m-1 \Rightarrow 3 \mid 5m-1 \Rightarrow m=3k+2 \quad \Rightarrow m=3k+2$

$(m \in 3\mathbb{N}) \text{ sau } m \in 3\mathbb{N}+1 \text{ sau } m \in 3\mathbb{N}+2 \quad p+m \in \mathbb{N}$

$m=3k+1 \quad m=3k+2$

$(5(3k+2)-1 = 15k+10-1 = 3(5k+3) \quad ; \quad 3m = 3(5k+3) \Rightarrow m=5k+3)$

$a = 3m+2 = 3(5k+3)+2 = 15k+11, k \in \mathbb{N} \Rightarrow a \in C \Rightarrow A \cap B \subseteq C$

Dim (1) si (2) $\Rightarrow A \cap B = C$.

Ex3 Def A, B stiind ca: (1) $A \cup B = \{1, 2, 3, 4, 5\}$, (2) $A \setminus B = \{1, 3\}$

(3) $A \cap B \neq \{3, 4, 5\}$.

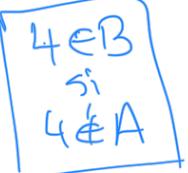
Dim (2) $\Rightarrow 1, 3 \in A$ si $1, 3 \notin B$

$$\xrightarrow{(1), (3)} 2 \in A \text{ si } 2 \in B$$

$$A = \{1, 2, 3\}$$

$$B = \{2, 4, 5\}$$

$\emptyset \subseteq C$
 $\Leftrightarrow C$ multime

$4 \in A \cup B$ \Rightarrow 

$5 \in A \cup B$ \Rightarrow 

$2 \in A \cap B$ ($\Rightarrow A \cap B \neq \{3, 4, 5\}$)
 \Rightarrow Alte posibilitati
(1), (3) pt A:
 $A = \{1, 2, 3\}, A = \{1, 2, 3, 4\}, A = \{1, 2, 3, 5\}$
 $A = \{1, 2, 3, 4, 5\}$

Ex4 $|A|=?$ $A = \{x \in \mathbb{Q} \mid x = \frac{m^2+1}{2m^2+m+1} \mid m \in \{1, 2, \dots, 1000\}\}$.

Exc 4

$$|A|=? \quad A = \left\{ x \in \mathbb{Q} \mid x = \frac{a^2+1}{2a^2+a+1} \mid m \in \{1, 2, \dots, 1000\} \right\}.$$

Fie $x, y \in A \Rightarrow (\exists) a, b \in \{1, \dots, 1000\}$ a.s. $x = \frac{a^2+1}{2a^2+a+1}, y = \frac{b^2+1}{2b^2+b+1}$

$$\text{Dacă } x=y \Rightarrow \frac{a^2+1}{2a^2+a+1} = \frac{b^2+1}{2b^2+b+1} \Rightarrow$$

$$(a^2+1)(2b^2+b+1) = (b^2+1)(2a^2+a+1) \Leftrightarrow \\ 2a^2b^2 + a^2b + a^2 + 2b^2 + b + 1 = 2b^2a^2 + ab^2 + b^2 + 2a^2 + a + 1$$

$$a^2b - ab^2 + b^2 - a^2 + b - a = 0$$

$$ab(a-b) - (a-b)(a+b) - (a-b) = 0$$

$$(a-b)(ab-a-b-1) = 0 \Rightarrow \underline{\underline{a=b}} \text{ sau } \underline{\underline{ab-a-b-1=0}}$$

$$a(b-1) - (b-1) = *2$$

$$(b-1)(a-1) = 2 \xrightarrow{a, b \in \mathbb{N}^*} \begin{cases} a-1=1 \\ b-1=2 \end{cases}$$

$$\begin{cases} a=2 \\ b=3 \end{cases}$$

$$\begin{cases} a-1=2 \\ b-1=1 \end{cases}$$

$$\begin{cases} a=3 \\ b=2 \end{cases}$$

$$\frac{3^2+1}{2 \cdot 3^2+3+1} = \frac{10}{22}$$

$$x=y = \frac{z^2+1}{2z^2+z+1} = \left(\frac{5}{11} \right)$$

|A|=999

Exc 1

$$\text{Fie } A = \{1, 2, \dots, m\}.$$

- 1) Cate multipli de 7 (k im general) conține multimea A?
- 2) Cate elemente ale multimi A sunt divizibile cu 2 și cu 3? (sau)
- 3) Cate elemente ale lui A nu sunt divizibile cu 2 și nici cu 3?
- 4) Dc $m=2021$ determinati nr. maxim de elemente ale unei submultimi B ale lui A a.s. produsul elementelor lui B să nu fie divizibil cu 36.

1) $B_k = \{x \in A \mid k|x\}$ $|B_7| = \left[\frac{m}{7}\right]$, $|B_k| = \left[\frac{m}{k}\right]$

$m = k \cdot q + r$ $0 \leq r < k-1$

$(q = \left[\frac{m}{k}\right])$ $B_k = \{k \cdot 1, k \cdot 2, \dots, k \cdot q\}$

2) $D = \{x \in A \mid 2|x \text{ și } 3|x\} = \{x \in A \mid 6|x\} = B_6 \Rightarrow |D| = \left[\frac{m}{6}\right]$

$B_2 \cap B_3$

$C = \{x \in A \mid 2|x \text{ sau } 3|x\} = B_2 \cup B_3$

$|C| = |B_2 \cup B_3| = |B_2| + |B_3| - |B_2 \cap B_3| = \left[\frac{m}{2}\right] + \left[\frac{m}{3}\right] - \left[\frac{m}{6}\right]$

$B_2 \cap B_3 = B_6$

3) $E = \{x \in A \mid 2 \nmid x \text{ și } 3 \nmid x\} = (A \setminus B_2) \cap (A \setminus B_3) = L_A B_2 \cap L_A B_3$

$= L_A (B_2 \cup B_3) = A \setminus (B_2 \cup B_3) = A \setminus C \Rightarrow |E| = m - \dots$

Principiul incluziunii și excluderii: Fie A_1, \dots, A_m multimi finite.

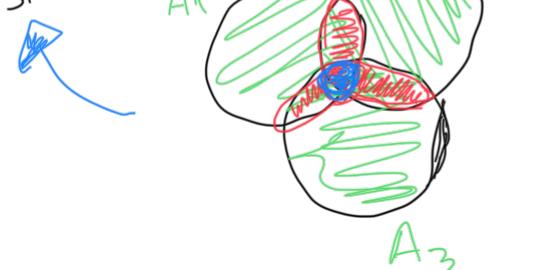
$m \geq 2$. Atunci avem:

$$|\bigcup_{i=1}^m A_i| = \sum_{i=1}^m |A_i| - \sum_{1 \leq i_1 < i_2 \leq m} |A_{i_1} \cap A_{i_2}| + \sum_{1 \leq i_1 < i_2 < i_3 \leq m} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| - \dots + (-1)^{k+1} \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq m} |A_{i_1} \cap \dots \cap A_{i_k}| + \dots + (-1)^{m+1} |A_1 \cap \dots \cap A_m|$$

(*)

Ca particular $\boxed{m=3}$

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$



Demo (P.I.E) Primă inducție după m ! (Termă!) $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$ ✓

- 1) Etapa de verificare: $\boxed{m=2}$ $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$
- 2) Etapa de demonstrare: Pp (*) aden pt. $m-1 \rightarrow$ și dem pt m .

$$\left| \bigcup_{i=1}^m A_i \right| = \left| \left(\bigcup_{i=1}^{m-1} A_i \right) \cup A_m \right| \stackrel{\text{PIE}}{=} \left| \bigcup_{i=1}^{m-1} A_i \right| + |A_m| - \left| \left(\bigcup_{i=1}^{m-1} A_i \right) \cap A_m \right| = C_1 //$$

ip.ind

ip ↗ + $|A_m| -$ ↘ = ...

Aplicații la P.I.E.

- (2) Câte numere naturale mai mici sau egale cu 1.000.000 sunt de forma x^2 sau de forma x^3 sau de forma x^5 , unde x este un număr natural.
- (1) Într-un cuestionar adresat la 100 elevi, statistică arată că 61 joacă fotbal, 30 joacă handbal și 13 joacă volei. Dintre cei care joacă fotbal, 30 joacă handbal și volei, 7 joacă handbal și volei. Căți dintre elevi practică toate sporturile?
- (3) Calculați $f(m)$. ($f: \mathbb{N}^* \rightarrow \mathbb{N}$ - funcția indicatorul lui Euler)
- (4) Să se determine numărul permutărilor multinișii $\{1, \dots, n\}$ care au cel puțin 1 pct. fix.
- $(S_n = \{f: \{1, \dots, n\} \rightarrow \{1, \dots, n\} \mid f \text{ funcție bijectivă}\} \rightarrow \text{multinișii } \{1, \dots, n\})$

- (1) $A \rightarrow$ multinișul elevilor care joacă fotbal
 $B \rightarrow$ handbal
 $C \rightarrow$ volei

$$|A|=61, |B|=30, |C|=13, |A \cup B \cup C|=100$$

$$|A \cap B|=11, |B \cap C|=3, |A \cap C|=7$$

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

$$\textcircled{2} \quad A = \{ a \leq 10^6 \mid a = x^2, x \in \mathbb{N} \} = \{ 0, 1, 2, \dots, (10^3)^2 \}$$

$$B = \{ b \leq 10^6 \mid b = x^3, x \in \mathbb{N} \} = \{ 0, 1, 2, \dots, (10^2)^3 \}$$

$$C = \{ c \leq 10^6 \mid c = x^5, x \in \mathbb{N} \} = \{ 0, 1, 2, \dots, 15^5 \}$$

$$X = \{ 0, 1, 2, \dots, 10^6 \}$$

$$D = X \setminus (A \cup B \cup C)$$

$$|D| = |X \setminus (A \cup B \cup C)| = |X| - |A \cup B \cup C| = 10^6 + 1 - |A \cup B \cup C|$$

???

$$|D| = |X \setminus (A \cup B \cup C)| \quad \text{A} \cup B \cup C \subseteq X$$

TEMA

Este adevarat ca $P^+ M, N$ multimi:

$$|M \setminus N| = |M| - |N| \Leftrightarrow M \supseteq N \quad \text{OK}$$

$$|M \setminus N| = |M| - |N|$$

FALS

$$M = \{1, 2, 3\} \quad N = \{1, 4\}$$

$$M \setminus N = \{2, 3\}$$

$$|A|=1001, |B|=101, |C|=16.$$

$$A \cap B = \{ n \leq 10^6 \mid n = k^2, n = p^3, k, p \in \mathbb{N} \} \quad \text{def}$$

$$A \cap C = \{ n \leq 10^6 \mid n = k^{10}, k \in \mathbb{N} \}$$

$$B \cap C = \{ n \leq 10^6 \mid n = k^{15}, k \in \mathbb{N} \}$$

TEMA! $|A \cap B|, |A \cap C|, |B \cap C|$

$$\textcircled{1} \quad \begin{array}{l} \text{"\geq"} \\ \text{"\leq"} \end{array} \quad m = x^6 = (x^3)^2 = (x^2)^3.$$

$$\begin{array}{l} \text{"\geq"} \\ \text{"\leq"} \end{array} \quad m = l^2 \quad l \in \mathbb{N} \quad m = p^3$$

$$P_p \frac{m \geq 2}{(0=0^2=0^3)} \quad \frac{(1=1^2=1^3)}{\square}$$

$$m = p_1^{d_1} \cdots p_k^{d_k} \quad P_{p_1} \cdots P_{p_k} \text{ prime} \neq \frac{d_1, \dots, d_k \geq 1}{k \geq 1}$$

(multiplata descomp. in factori primi)

$$\left\{ \begin{array}{l} m = l^2 \quad \Leftrightarrow \quad 2 | d_1, 2 | d_2, \dots, 2 | d_k \\ m = p^3 \quad \Leftrightarrow \quad 3 | d_1, 3 | d_2, \dots, 3 | d_k \end{array} \right. \quad \Leftrightarrow \quad m = t^6, t \in \mathbb{N}$$

$(6 | d_1, 6 | d_2, \dots, 6 | d_k)$

$$\left\{ \begin{array}{l} 2|2j \\ 3|3j \\ (2,3)=1 \end{array} \right. \Leftrightarrow 6|d_j$$

$$A \cap B \cap C = \{ x \leq 10^6 \mid x = l^{30}, l \in \mathbb{N} \} \quad |A \cap B \cap C| = 2$$
$$= \{ 0^{30}, 1^{30} \}$$

Aplicând P.I.E. calculează $|A \cup B \cup C| = \dots$

Seminar 3

18.10.2021

$$\left\{ \begin{array}{l} \text{P.I.E} \quad A_1, \dots, A_m \text{ multini finite} \\ |\bigcup_{i=1}^m A_i| = \sum_{i=1}^m |A_i| - \sum_{1 \leq i_1 < i_2 \leq m} |A_{i_1} \cap A_{i_2}| + \dots + (-1)^{m-1} |A_1 \cap \dots \cap A_m| \end{array} \right.$$

③ Calculati $f(m)$, $m \geq 1$. $f(m) = \{k \mid 1 \leq k \leq m, k \in \mathbb{N}, (k, m) = 1\}$

Notez au $B = \{1, \dots, m\} \setminus A$. éclar

Note: $m \geq 1$

$m=1$ (*) OK

$m > 1$

$m = p_1^{d_1} \cdots p_n^{d_n}$ cu p_1, \dots, p_n prime \neq date 2; $d_1, \dots, d_n \geq 1$.

$(24, 30) = 2^3 \cdot 3^1$

$24 = 2^3 \cdot 3^1$

$30 = 2^1 \cdot 3^2 \cdot 5^1$

$B = \{k \mid 1 \leq k \leq m, k \in \mathbb{N}, (k, m) \neq 1\}$

$(\exists) i \in \{1, \dots, n\}$ a.s. $p_i \mid k$.

$$A_i = \{k \mid 1 \leq k \leq m, k \in \mathbb{N}, p_i \mid k\} \quad (i=1, 2)$$

$$|A_i| = \left[\frac{m}{p_i} \right] = \frac{m}{p_i} \quad (A_i)_{i=1, m}$$

$$\text{i)} A_i \cap A_j = \{ k | 1 \leq k \leq m, k \in \mathbb{N}, p_i^k \neq p_j^k \}$$

$$= \{ k | 1 \leq k \leq m, k \in \mathbb{N}, p_i p_j | k \}$$

$$P_i \overline{P_k} \rightarrow [P_i P_j] \mid k$$

" commonc($P_i P_j$)
 $\{\} i \neq j$

$i_1 \leq i_2 \leq i_3 \leq \dots \leq i_t \leq n$ ($t \leq n$)

$$A_{i_1} \cap \dots \cap A_{i_t} = \left\{ k \in \mathbb{N} \mid 1 \leq k \leq m, p_{i_1} | k, \dots, p_{i_t} | k \right\}$$

$$= \left\{ k \in \mathbb{N} \mid 1 \leq k \leq m, p_{i_1} \cdot p_{i_2} \cdots p_{i_t} | k \right\}$$

$$P_{i_1}^{1/k} \dots P_{i_k}^{1/k} = \left(P_{i_1} \dots P_{i_k} \right)^{1/k}$$

$\pi_{ijk} \in \{P_{ij}, P_{jk}, P_{ki}\}$ (prime + 2 cases)

$$|A_{i_1} \cap \dots \cap A_{i_t}| = \frac{m}{p_{i_1} \dots p_{i_t}}$$

$$|B| = |A_1 \cup \dots \cup A_n| \stackrel{\text{PiE}}{=} \sum_{i=1}^n |A_i| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| + \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n|$$

$$|B| = \sum_{i=1}^n \frac{m}{p_i} - \sum_{1 \leq i_1 < i_2 \leq n} \frac{m}{p_1 p_2} + \dots + (-1)^{n-1} \cdot \frac{m}{p_1 p_2 \dots p_n}$$

$$|A| = m - |B| = m - \sum_{i=1}^n \frac{m}{p_i} + \sum_{1 \leq i < j \leq n} \frac{m}{p_i p_j} - \dots + (-1)^{n-1} \frac{m}{p_1 p_2 \dots p_n} =$$

$$f(m) = m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_n}\right)$$

Am folosit:
 $(n-d_1)(n-d_2)\dots(n-d_n)$
 $= 1 - \sum_{i=1}^n d_i + \sum_{1 \leq i < j \leq n} d_i d_j - \dots + (-1)^{n-1} d_1 \dots d_n$

④ (veriS2) $\{ \sigma \in S_m \mid \sigma \text{ are cel putin } 1 \text{ pct. fix}\} = |A|$

$$\sigma \in S_m = \{ f : \{1, \dots, m\} \rightarrow \{1, \dots, m\} \mid f \text{ fct. bijectiv}\}$$

$$\forall \sigma \in A \Leftrightarrow \sigma \text{ are cel putin } 1 \text{ pct fix} \Leftrightarrow (\exists k \in \{1, \dots, m\} \text{ a.i. } \sigma(k) = k)$$

$$A_k = \{ \sigma \in S_m \mid \sigma(k) = k \} \quad (\#) \quad k = \overline{1, m}$$

$$\sigma \in A_1 \cup \dots \cup A_m.$$

$$\sigma \in A \Leftrightarrow \sigma \in A_1 \cup \dots \cup A_m$$

$$A = A_1 \cup \dots \cup A_m$$

$$|A| = |\bigcup_{i=1}^m A_i| \stackrel{\text{PiE}}{=} \sum_{i=1}^m |A_i| - \sum_{1 \leq i < j \leq m} |A_i \cap A_j| + \dots + (-1)^{m-1} |A_1 \cap \dots \cap A_m|$$

$$|A_k| = (m-1)! \quad (\#) \quad k = \overline{1, m}$$

$$(A_k = \{ \sigma \in S_m \mid \sigma(\{1, \dots, m\} \setminus \{k\}) \})$$

veri
exe, wrm

$$(\#) i \neq j \Rightarrow |A_i \cap A_j| = (m-2)!$$

$$(A_i \cap A_j = \{ \sigma \in S_m \mid \sigma(i) = i \text{ si } \sigma(j) = j \})$$

$$|A| = \sum_{i=1}^m (m-i)! - \sum_{1 \leq i < j \leq m} (m-2)! + \dots + (-1)^{m-1}.$$

Ex 1 Fie M o multime finită și $f: M \rightarrow M$ o funcție. Atunci:

a) f inj \Leftrightarrow b) f surj \Leftrightarrow c) f bij.

Obs Dacă M nu e finită atunci concluzia nu mai are loc.
 $f: N \rightarrow N$ $f(n) = n+1$ inj, mesuraj; $f: N \rightarrow N$ $f(n) = \begin{cases} n-2, & n \geq 2 \\ 1, & \text{mergi} \end{cases}$ surj, neinj.

Denum $M = \{a_1, \dots, a_m\}$ $f(M) = \{f(a_1), \dots, f(a_m)\}$.

(c) \Rightarrow a), b) evidentă

a) \Rightarrow c): f inj $\Rightarrow |f(M)| = M = m$

$\xrightarrow{\text{def}} f$ surj. $\Rightarrow f$ bij.

$M = \{a_1, \dots, a_m\}$
 $f(M) \subseteq M \Rightarrow f(M) = M$
 $|f(M)| = m$

b) \Rightarrow c): f surj $\Rightarrow f(M) = M$ ($\xrightarrow{(1)} |f(M)| = m$)
Pp abs. că f nu e inj $\xrightarrow{\text{def}} (\exists i \neq j)$ a.s. $f(a_i) = f(a_j)$

$\{f(a_1), \dots, f(a_m)\} \leq m-1$ $\xrightarrow{\text{cu (1)}} |f(M)| \leq m-1$

\Rightarrow pp e falsă $\Rightarrow f$ e inj $\Rightarrow f$ e bij.

Ex 2 Să se arate că fct. $f: N \rightarrow \mathbb{R}$, $f(n) = \{\sqrt[n]{2}\}$ e injectivă.

Rezolvare

Fie $m, n \in \mathbb{N}$ a.i. $f(m) = f(n) \Rightarrow \{\sqrt[m]{2}\} = \{\sqrt[n]{2}\}$

$$\sqrt[m]{2} - \sqrt[n]{2} \in \mathbb{Q}$$

$$\Rightarrow (m-n)\sqrt[mn]{2} \in \mathbb{Z} \Rightarrow (m-n)\sqrt[mn]{2} \in \mathbb{Z}$$

$\left(\begin{array}{l} \text{Dc } g \in \mathbb{Q}, \\ t \in \mathbb{R} \setminus \mathbb{Q} \Rightarrow \\ \Rightarrow t \cdot g \in \mathbb{R} \setminus \mathbb{Q} \end{array} \right)$

f e inj

$$m=n$$

$$m-n=0$$

| Ex 3) Să se studieze inj. (surj., bij.) fct. $f: \mathbb{R} \rightarrow \mathbb{R}$
 în funcție de parametrul real m , unde
 $f(x) = \begin{cases} x^2 + m, & x \leq 0 \\ mx, & x \in (0, 1) \\ m^2 - x, & x \geq 1 \end{cases}$ (Tema: pt. m arbitrar)

Sol $[m=1]$ Calc. în plus $f([-1, 3])$, $f'([0, 1])$ $g(1)=g(-1)=2$

$f(x) = \begin{cases} x^2 + 1, & x \leq 0 \\ x, & x \in (0, 1) \\ 1-x, & x \geq 1 \end{cases}$

Graficul este $\frac{f}{\text{bij}}$

$\frac{f}{\text{inj}} \quad \frac{f}{\text{swj}} \quad \frac{f}{\text{bij}}$

$g(x) = \begin{cases} x^2 + 1, & x \leq 1 \\ 1-x, & x > 1 \end{cases}$
 $g \text{ este inj.}$
 $h(x) = \begin{cases} x+1, & x \leq 1 \\ x-6, & x > 1 \end{cases}$
 $h(0) = h(7)$
 $h \text{ nu e inj.}$

$f([-1, 3]) = f([-1, 0] \cup (0, 1) \cup [1, 3]) =$ ✓

$= f([-1, 0]) \cup f((0, 1)) \cup f([1, 3])$
 $= [-1, 2] \cup (0, 1) \cup [-2, 0] = [-2, 2]$

$f(A \cup B) = f(A) \cup f(B)$ ✓
 $\Leftrightarrow y \in f(A \cup B) \Rightarrow \exists x \in A \cup B \text{ sau } x \in B \text{ cu } y = f(x) \Leftrightarrow y \in f(A) \text{ sau } y \in f(B) \Rightarrow f(x) \in f(A) \text{ sau } f(x) \in f(B) \Rightarrow f(x) \in f(A \cup B)$
 $\Leftrightarrow y \in f(A) \cup f(B) \Rightarrow y \in f(A) \text{ sau } y \in f(B) \Rightarrow \exists x \in A \text{ sau } x \in B \text{ cu } y = f(x) \Leftrightarrow y \in f(A) \text{ sau } y \in f(B) \Rightarrow y \in f(A \cup B)$

① Fie M o multime si $A, B \subseteq M$. Def.
 $f: P(M) \rightarrow P(A) \times P(B)$, $f(X) = (X \cap A, X \cap B)$

Anatati ca:

$$\textcircled{1} \quad f \text{ e inj} \Leftrightarrow A \cup B = M$$

$$\textcircled{2} \quad f \text{ e surj} \Leftrightarrow A \cap B = \emptyset$$

$$\textcircled{3} \quad f \text{ e bij} \Leftrightarrow A = \bigcup_M B. \quad \text{Im arest ca, afilati inversa lui } f.$$

\downarrow
evident dim $\textcircled{1}$ si $\textcircled{2}$

Denum $\textcircled{1}$ "=>" Stim ca f e inj.

$$\text{Pp. abs. ca } A \cup B \subsetneq M \Rightarrow \exists x \in M \text{ s.t. } x \notin A \cup B$$

$$x = \{x\} \subseteq M$$

$$\phi \subseteq M$$

$$f(x) = (x \cap A, x \cap B) = (\{x\} \cap A, \{x\} \cap B) = (\phi, \phi)$$

$$f(\phi) = (\phi \cap A, \phi \cap B) = (\phi, \phi)$$

f nu e inj \Rightarrow Pp. facuta e falsa $\Rightarrow A \cup B = M$.

"=<" Stim ca $A \cup B = M$.

Fie $X, Y \subseteq M$ a.s. $f(x) = f(y)$

$$(x \cap A, x \cap B) = (y \cap A, y \cap B)$$

$$\Rightarrow \begin{cases} x \cap A = y \cap A \\ x \cap B = y \cap B \end{cases}$$

$$(x \cap A) \cup (x \cap B) = x \cap (A \cup B) = x \cap M \stackrel{x \subseteq M}{=} x$$

$$(y \cap A) \cup (y \cap B) = y \cap (A \cup B) = y \cap M \stackrel{y \subseteq M}{=} y$$

$\Rightarrow f$ e injectiva



② "=>" Stim ca f e surjectiva.

Pp red. la absurd ca $A \cap B \neq \emptyset \Rightarrow \exists x \in A \cap B$. (*)

Ca sa aratam ca f nu e surjectiva trebuie sa gasim

un element $(C, D) \in P(A) \times P(B)$ a.i. $f(x) \neq (C, D)$

$\Rightarrow X \in P(M)$ ($\Rightarrow X \subseteq M$).

Consideram $(\{x\}, B \setminus \{x\}) \in P(A) \times P(B)$.

Cum f e suriectivă $\Rightarrow (\exists) X \in P(M)$ a.i.

$$f(x) = (\{x\}, B \setminus \{x\}) \Rightarrow \begin{cases} X \cap A = \{x\} \\ X \cap B = B \setminus \{x\} \end{cases} \quad \begin{matrix} (1) \\ (2) \end{matrix}$$

$$(X \cap A, X \cap B)$$

$$\text{Dim (1)} \Rightarrow x \in X. \quad \left| \Rightarrow x \in X \cap B = B \setminus \{x\} \Rightarrow x \in B \right.$$

$$\Rightarrow P_P f \text{ facuta e falsă} \Rightarrow A \cap B = \emptyset.$$

$$\boxed{\Leftrightarrow} \quad \text{Stim că } A \cap B = \emptyset. \quad (\square)$$

Fie $(X, Y) \in P(A) \times P(B) \Rightarrow X \subseteq A, Y \subseteq B$. (o)

$$f(Z) = (X, Y)$$

$$(Z \cap A, Z \cap B)$$

$$Z \cap A = X \Rightarrow X \subseteq Z \quad \left| \Rightarrow \begin{matrix} X \cup Y \\ \subseteq Z \end{matrix} \right.$$

$$Z \cap B = Y \Rightarrow Y \subseteq Z$$

$$X, Y \subseteq M \Rightarrow X \cup Y \subseteq M$$

$$f(X \cup Y) = ((X \cup Y) \cap A, (X \cup Y) \cap B) =$$

$$= ((X \cap A) \cup (Y \cap A), (X \cap B) \cup (Y \cap B)) =$$

$$= (X \cup (Y \cap A), (X \cap B) \cup Y) =$$

$$= (X \cup \emptyset, \emptyset \cup Y) = (X, Y) \Rightarrow f \text{ e surj.} \quad \square$$

$$A \cap B = \emptyset$$

$$\square$$

③ $f \in \text{bij} \Leftrightarrow A = \bigcup_M B (\Leftrightarrow (A \cup B = M \text{ și } A \cap B = \emptyset))$

Functie

$g: P(A) \times P(B) \rightarrow P(M)$

este fct. inversă
leu f

$$g(X, Y) = X \cup Y$$

(Tb. arătat:

$$(f \circ g)(X, Y) = f(X \cup Y) \stackrel{A \cap B = \emptyset}{=} (X, Y) \quad \begin{matrix} \text{(1)} \\ (X, Y) \in P(A) \times P(B) \end{matrix} \quad \begin{matrix} \text{fog} = 1_{P(A) \times P(B)} \\ g \circ f = 1_{P(M)} \end{matrix}$$

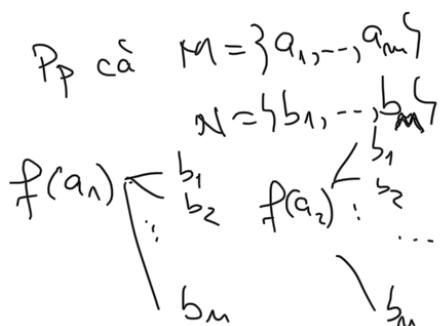
$$\begin{aligned} (g \circ f)(Z) &= g(f(Z)) = g(Z \cap A, Z \cap B) = \\ &= (Z \cap A) \cup (Z \cap B) = Z \cap (A \cup B) = \\ &= Z \cap M = Z \quad \begin{matrix} A \cup B = M \\ (Z) \in P(M) \end{matrix} \end{aligned}$$

[Prob] Fie M, N 2 multimi finite cu $|M| = m, |N| = n$.

Calculati:

- ① $\#\text{fct. definite pe } M \text{ cu valori in } N (= |\{f | f: M \rightarrow N, f \text{ fct.}\})$ = ?
- ② $|\{f | f: M \rightarrow N, f \text{ fct. injectivă}\}| = ?$
- ③ $|\{f | f: M \rightarrow N, f \text{ fct. surjectivă}\}| = ?$
- ④ $|\{f | f: M \rightarrow N, f \text{ fct. bijectivă}\}| = ?$

① n^m (Ind. după m) sau



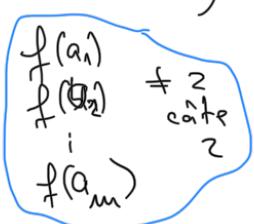
② $f \text{ inj} \Rightarrow |M| = |\{f(m)\}| \leq |N| = n$
 $f \text{ fct}, \{f(m)\} \subseteq N$

Prin urmare, daca $m < n$ atunci $\# = 0$.

Daca $\boxed{m \leq n}$ $\Rightarrow \# = A_m^n$ (def. combinatorică
a aranjamentelor)

nr. de submultimi
ordonate cu n elemente
ale unei multimi cu
 m elemente

$\{f(a_1), \dots, f(a_m)\}$
cu m elem.
e o submultime
a lui $\{b_1, \dots, b_n\}$



$$\textcircled{4} \quad f \text{ bijectivă} \Rightarrow |M| = |N|$$

Dacă $m \neq n \Rightarrow \# = 0$

Dacă $m = n \Rightarrow \# = n!$

$$\textcircled{3} \quad f \text{ surj} \Rightarrow |M| \geq |N|$$

Dacă $m < n \Rightarrow \# = 0.$

Altfel, $m \geq n$. (aplic P.I.E.)

$$|T| = n^m$$

$X = \{f \mid f: M \rightarrow N, f \text{ fct. suriectivă}\} \subseteq T \Rightarrow f \mid f: M \rightarrow N, f \text{ fct.}$

$X = \{f \mid f: M \rightarrow N, f \text{ fct. mesurivă}\}$
 $T \setminus X = \{f \mid f: M \rightarrow N, f \text{ fct. mesurivă, } \exists m \in \text{suriectivă}\}$

$$|X| = |T| - |T \setminus X| \quad (!)$$

$\frac{|X|}{|T|} = \frac{|T| - |T \setminus X|}{|T|} = \frac{|T|}{|T|} - \frac{|T \setminus X|}{|T|} = 1 - \frac{|T \setminus X|}{|T|}$

$f \text{ mesurivectivă} \stackrel{\text{def}}{\Rightarrow} \text{Im } f \subset N \Rightarrow (\exists) b \in N \text{ a.s. } b \notin \text{Im } f$

$(\exists) b \in N \text{ a.s. } b \neq f(a) \Leftrightarrow a \in \text{Im } f$

$N = \{b_1, b_2, \dots, b_m\}$. Notează cu $A_i = \{f \mid f: M \rightarrow N, f \text{ functie a.s. } b_i \in \text{Im } f\}$

$f: M \rightarrow N \text{ nu e surj} \Rightarrow (\exists) i = \overline{1, m} \text{ a.s. } f \in A_i \Rightarrow$

$\Rightarrow T \setminus X \stackrel{\text{def}}{=} \bigcup_{i=1}^m A_i$. Aplic P.I.E pt a calcula $|T \setminus X|$

$$|T \setminus X| = |\bigcup_{i=1}^m A_i| \stackrel{\text{def}}{=} \sum_{i=1}^m |A_i| - \sum_{1 \leq i < j \leq m} |A_i \cap A_j| + \dots + (-1)^{m-1} |A_1 \cap A_2 \cap \dots \cap A_m|$$

$$|A_i| = (n-i)^m \quad (\forall) i = \overline{1, m}$$

$A_{i_1} \cap \dots \cap A_{i_k} = \{f \mid f: M \rightarrow N \text{ f. functie a.s. } \text{Im}(f) \subseteq N \setminus \{b_{i_1}, \dots, b_{i_k}\}\}$

$\underset{1 \leq i_1 < \dots < i_k \leq m}{|A_{i_1} \cap \dots \cap A_{i_k}|} = (n-k)^m \quad (\forall) 1 \leq i_1 < \dots < i_k \leq m.$

$$(|A_1 \cap A_2 \cap \dots \cap A_m| = 0)$$

$$|\Gamma \setminus X| = C_m^1 (m-1)^{m-1} - C_m^2 (m-2)^{m-2} + \dots + (-1)^{m-1} C_m^{m-1} 1^{m-1} \Rightarrow$$

$$\text{înlocuind în } \textcircled{1} \Rightarrow |X| = m^m - C_m^1 (m-1)^{m-1} + C_m^2 (m-2)^{m-2} - \dots + (-1)^m C_m^{m-1}$$

[Prb3] Fie $f: A \rightarrow B$ o funcție. Să se arate că:

- ① f e surj $\Leftrightarrow (\exists) g: B \rightarrow A$ a.i. $f \circ g = \mathbb{1}_B$
- ② f e inj $\Leftrightarrow (\exists) h: B \rightarrow A$ a.i. $h \circ f = \mathbb{1}_A$.

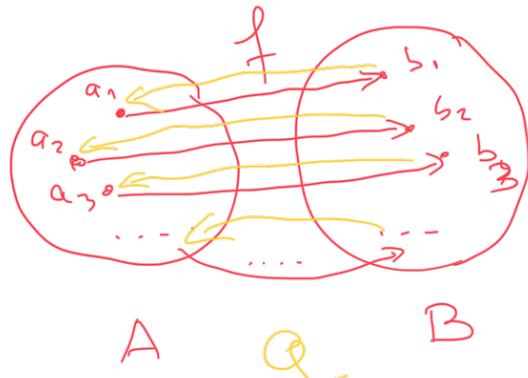
REMA \Leftrightarrow

Obs Dacă f e surj $\stackrel{C_2}{\Leftrightarrow} |B| \leq |A|$ (folosind ① $\Rightarrow (\exists) g: B \rightarrow A$)

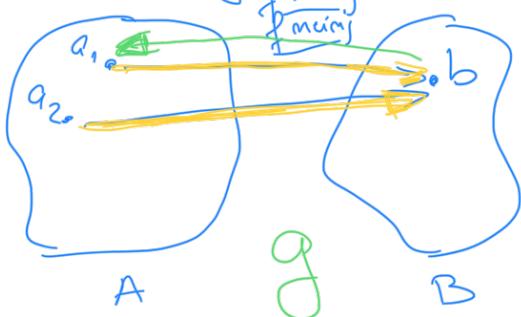
a.i. $f \circ g = \mathbb{1}_B \stackrel{C_2}{\Leftrightarrow} g$ inj ($\Leftrightarrow f$ surj) $\Rightarrow |B| \leq |A|$

① $\stackrel{n \Rightarrow h}{\Leftrightarrow}$ Stiu că f e surj
Cum construiesc g ?

Cazul 1 f bij



Cazul 2 f nebij (în cazul nostru f surj, f nu inj)



$g: B \rightarrow A$
Pt fiecare $b \in B$ alegem un element
 $a_b \in f^{-1}(b)$
preimaginea primă a

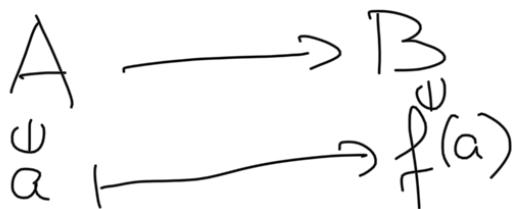
Definim $g: B \rightarrow A$
 $g(b) = a_b \quad (\forall) b \in B$.

$(f \circ g)(b) = f(g(b)) = f(a_b) = b \quad (\forall) b \in B \Rightarrow$
 $f \circ g = \mathbb{1}_B$.

(vezi Sun) Fie $f: A \rightarrow B$ funcție. Să se arate că:
 f e injectivă (\Rightarrow) $h: B \rightarrow A$ c.i. $h \circ f = \text{id}_A$.

\leftarrow
ovid

" \Rightarrow " f e inj. $(\forall) \frac{a_1 \neq a_2}{a_1, a_2 \in A} \Rightarrow \frac{f(a_1) \neq f(a_2)}{f \text{ injectivă} \Rightarrow |A| = |f(A)|}$



Notează cu $b_a := f(a)$

$h: B \rightarrow A$
 $\{f(a) | a \in A\} \xrightarrow{\text{!}}$

Vrem să construim

Avem 2 cazuri de analizat:

Cazul 1 $f(A) = B$ ($\Rightarrow f$ bijectivă) $\Rightarrow B = \{b_a | a \in A\}$

$h: B \rightarrow A$ $h(b_a) = a \quad (\forall) b_a \in B$

(Verificare: $(h \circ f)(a) = h(f(a)) = h(b_a) = a \quad (\forall) a \in A$)

Cazul 2 $f(A) \neq B$ Def. $h: B \rightarrow A$ astfel:

$\{b_a | a \in A\}$

$h(x) = \begin{cases} a & , x = b_a \\ a_0 & , x \in B \setminus f(A) \end{cases}$

unde $a_0 \in A$ este un element fixat oarecare

(Verificare) $(h \circ f)(a) = h(f(a)) = h(b_a) = a \quad (\forall) a \in A$)

Din (1) și (2) \Rightarrow (2) $h: B \rightarrow A$ c.i. $h \circ f = \text{id}_A$.

Aplicatie la ($f: A \rightarrow B$ surj $\Leftrightarrow (\exists g: B \rightarrow A$ a.i.)
 $f \circ g = \text{id}_B$)

Exemplu $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ $f(a,b) = a$ (proiectia canonica pe prima comp.)

f surj (nu e inj.)

Dem: Fie $m \in \mathbb{N}$ $f(m,0) = m$ $\xrightarrow[m]{\text{ales arbitrar}} \text{Im}(f) = \mathbb{N} \Rightarrow$
 $\Rightarrow f \text{ e surj.}$

$$f^{-1}(X) = \{(a,b) \in \mathbb{N} \times \mathbb{N} \mid f(a,b) \in X\}$$

$$X \subseteq \mathbb{N} \quad f^{-1}(\{0\}) = \{(a,b) \mid b \in \mathbb{N}\}$$

$$\text{De ex: } X = \{0\} \Rightarrow f^{-1}(\{0\}) = \{(a,b) \mid b \in \mathbb{N}\}$$

$$X = \{2, 3, 5, 7\} \Rightarrow f^{-1}(\{2, 3, 5, 7\}) = \{(a,b) \mid b \in \mathbb{N}\}$$

$$\{(7,b) \mid b \in \mathbb{N}\} \cup \{(5,b) \mid b \in \mathbb{N}\} \cup \{(3,b) \mid b \in \mathbb{N}\}$$

Dacă notăm $A_a = \{(a,b) \mid b \in \mathbb{N}\}$ atunci

$$f^{-1}(\{2, 3, 5, 7\}) = A_2 \cup A_3 \cup A_5 \cup A_7.$$

Cum construiesc? $g: \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ a.i. $f \circ g = \text{id}_{\mathbb{N}}$

$$f^{-1}(\{c\}) = \{(c,b) \mid b \in \mathbb{N}\} (= A_c)$$

$$g_1: \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N} \quad g_1(0) = (0,0) \quad g_1(1) = (1,1)$$

$$g_1(2) = (2,2) \dots \quad g_1(n) = (n,n), \dots$$

$$(f \circ g_1)(k) = f(g_1(k)) = f(k, k) = k \forall k \in \mathbb{N}$$

$$\Rightarrow f \circ g_1 = \mathbb{1}_N.$$

$$g_2: \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$$

$$g_2(0) = (0, 1) \quad g_2(1) = (1, 2) \dots$$

$$g_2(n) = (n, n+1)$$

Prb 2 Să se arate că pentru orice multime A nu există funcții surjective $f: A \rightarrow P(A)$

Prb 3 Să se arate că nu există funcții $f: \mathbb{R} \rightarrow \mathbb{R}$ a.s. $|f(x) - f(y)| > 1$

$$\text{c.u.) } x \neq y.$$

Dem Prb 2 Pp red. abs. că $\exists f: A \rightarrow P(A)$ o funcție surjectivă.
Considerăm submultimea lui A :
 $M = \{a \in A \mid a \notin f(a)\}$ (x)

$$A \ni a \mapsto \begin{cases} f(a) & \text{if } a \in M \\ \emptyset & \text{if } a \notin M \end{cases}$$

Dim faptul că f e surjectivă și $M \in P(A)$

$$\Rightarrow \exists b \in A \text{ a.s. } f(b) = M. \quad (1)$$

$$\text{1)} \underline{b \in M} \stackrel{(1)}{=} f(b) \Rightarrow b \in f(b) \stackrel{\text{def. } M}{\Rightarrow} b \notin M \quad \text{x}$$

$$\text{2)} \underline{b \notin M} \stackrel{(1)}{=} f(b) \Rightarrow b \notin f(b) \stackrel{\text{def. } M}{\Rightarrow} \underline{b \in M} \quad \text{x}$$

Prin urmare, $\text{pp} \in \text{falsă} \Rightarrow \text{nu } \exists \text{ fct. surj. } f: A \rightarrow \mathcal{P}(A)$. ✓

Comentariu Cum $g: A \rightarrow \mathcal{P}(A)$ $g(a) = \{a\}$ $\forall a \in A$

este injectivă $\Rightarrow |A| \leq |\mathcal{P}(A)|$.

Din Prb 2 \Rightarrow nu există funcții bijective def $f: A \rightarrow \mathcal{P}(A)$ (pt. că nu există surjective) $\Rightarrow C_3$

$|A| < |\mathcal{P}(A)|$.

Observație $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \dots$

$|R|$ obtinut o nouă (în particular, cum $R \cong \mathcal{P}(\mathbb{N})$, folosind Prb 2, a fost învățată că R nu e demne de numărabilă)

Prb 4 Găsiți imaginea funcției $f: \mathbb{Z}^2 \rightarrow \mathbb{Z}$

$$f(x,y) = x^2 - y^2.$$

Dem Prb 3 Pp. reducere la absurd că \exists fct. $f: R \rightarrow R$ a.t. $|f(x) - f(y)| \geq 1 \quad (\forall x \neq y)$

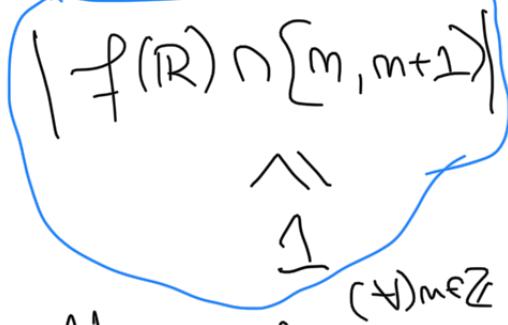
f e injectivă

$|f(R)| = |R| \stackrel{C_4}{\Rightarrow} f(R) \in \text{numărabilă. (1)}$

$R \subseteq \bigcup [m, m+1] \quad (\forall x \in R \quad x \in [\lfloor x \rfloor, \lceil x \rceil + 1])$

$m \in \mathbb{Z}$

$$|f(x) - f(y)| > 1 \Leftrightarrow x \neq y \Rightarrow$$



(oricare interval $[m, m+1]$ găsește cel mult o valoare)
a lui f

$$f(R) = f(R) \cap R = f(R) \cap \left(\bigcup_{m \in \mathbb{Z}} [m, m+1] \right)$$

$\subseteq \bigcup_{m \in \mathbb{Z}} (f(R) \cap [m, m+1])$

one cel mult
1 elem

$\Rightarrow f(R)$ e
finită
sau
numărabilă
(*)

X (R)

$\Rightarrow P_p$ e falsă \Rightarrow Nu (\exists) funcții

$$f: R \rightarrow R \text{ a.s. } |f(x) - f(y)| > 1 \quad (\exists x \neq y)$$

(*) : Observăm că $f(R)$ ar fi imbijective
cu o submultime a lui \mathbb{Z} ; deci ar fi finită
dacă e finită și ar fi numărabilă dacă
e infinită.

Prbs Arătați că oricare 2 dim următoarele
multimi sunt echipotente:

$(-\infty; a]$; $[b, +\infty)$, $[c, d]$, $[c, d)$, $(c, d]$, (c, d) ,
 $(0, 1)$, \mathbb{R} , \mathbb{R}_+ , $\mathbb{Q}(\mathbb{N})$, \mathbb{C} , \mathbb{R}_+^* . - (vezi C4 pt.
 ammitte bijectii)

Sol Prb4 $f: \mathbb{Z}^2 \rightarrow \mathbb{Z}$ $f(x, y) = x^2 - y^2$
 $\mathbb{Z} \times \mathbb{Z}$

Calculati $\text{Im } f$. $\text{Im}(f) = \{ k \mid k \in \mathbb{Z} \text{ s.t. } \exists x, y \in \mathbb{Z} \text{ such that } k = x^2 - y^2 \}$

$x \text{ par} \Rightarrow x = 2l, l \in \mathbb{Z}$ $x^2 = (2l)^2 = 4l^2 \Rightarrow x^2 \text{ da restul } 0 \text{ la imp cu 4}$

$x \text{ impar} \Rightarrow x = 2l+1, l \in \mathbb{Z}$ $x^2 = (2l+1)^2 = 4l^2 + 4l + 1 =$
 $= 4l(l+1) + 1 \Rightarrow x^2 \text{ da restul } 1 \text{ la imp. cu 4}$

Restul imp. lui x^2 la 4 poate fi $\underline{0 \text{ sau } 1}$. \Rightarrow
 Restul imp. lui $x^2 - y^2$ la 4 poate fi

\Rightarrow Restul imp. lui $x^2 - y^2$ la 4 poate fi
 $0, 1$ sau 3 ($0/\cancel{1} - 0/\cancel{1} \rightsquigarrow \begin{matrix} 0-0, 0-1, 1-0, 1-1 \\ \cancel{0} \quad \cancel{-1} \quad \cancel{1} \quad \cancel{0} \end{matrix}$)



$\text{Im}(f) \subseteq \mathbb{Z} \setminus \{4k+2 \mid k \in \mathbb{Z}\} = \mathbb{Z} \setminus \{4\mathbb{Z} + 2\}. (*)$

$k=5$ $x^2 - y^2 = 5$ ec in $\mathbb{Z} \times \mathbb{Z}$

$$(x-y)(x+y) = 5$$

$$\begin{cases} x-y=5 \\ x+y=1 \end{cases} \rightsquigarrow \begin{cases} x=3 \\ y=-2 \end{cases}$$

I) k impar, i.e. $k \in (4\mathbb{Z}+1) \cup (4\mathbb{Z}+3)$

$$x^2 - y^2 = k$$
$$(x-y)(x+y) = k$$

$$\begin{cases} x-y = k \\ x+y = 1 \end{cases}$$

$$x = \frac{k+1}{2} \in \mathbb{Z} \text{ (} k \text{ impar)}$$

$$y = \frac{1-k}{2} \in \mathbb{Z} \text{ (} k \text{ impar)}$$

Deci ec $x^2 - y^2 = k$, k impar, are solutie

(de exemplu $x = \frac{k+1}{2}$, $y = \frac{1-k}{2}$)

II) k par, $k \in 4\mathbb{Z}$ $k = 4t$.

$$x^2 - y^2 = k$$
$$(x-y)(x+y) = k$$

$$\begin{cases} x+y = \frac{k}{2} \\ x-y = 2 \end{cases}$$

$$2x = \frac{k}{2} + 2 = 2t + 2$$

$$x = t + 1$$

$$y = t - 1$$

Prin urmare, pt $k \in 4\mathbb{Z}$ ec $x^2 - y^2 = k$ are solutie (de ex. $x = \frac{k}{4} + 1$, $y = \frac{k}{4} - 1$)

Dim I \subseteq II + (*) \Rightarrow Im(f) = $\mathbb{Z} \setminus (4\mathbb{Z} + 2)$

Prbs

Bijecție între \mathbb{R} și \mathbb{R}_+^*

$$\mathbb{R} \xrightarrow{f} \mathbb{R}_+^*$$

$$f(x) = e^x \quad (\forall x \in \mathbb{R})$$

$$\mathbb{R}_+^* \xrightarrow{g} \mathbb{R}$$

$$g(x) = \ln(x) \quad (\forall x \in \mathbb{R})$$

Seminar 6

8.11.2021

Reamintese:

Def Fie $A \neq \emptyset$. \sim o relație binară pe A . " \sim " s.m. relație de echivalență pe A dacă îndeplinește simultan condițiile:

- 1) reflexivă: $a \sim a \quad \forall a \in A$
- 2) simetrică: $a \sim b \Rightarrow b \sim a$
- 3) transitivă: $a \sim b, b \sim c \Rightarrow a \sim c$

Def \sim o relație binară pe mult. $A \neq \emptyset$ reprezentată a submultime, a lui $A \times A$

Def \sim relație binară pe mult. $A \neq \emptyset$ reprezentată a submultime, a lui $A \times A$

Def Fie " \sim " o rel. de echiv. pe mult. $A \neq \emptyset$.
 ① submultime $S \subseteq A$ s.m. SCR ("sistem complet de reprezentanți") pentru " \sim " dacă S conține exact o sătucă un element din fiecare clasă de echivalență. Deci

② rel. binară pe mult. A este antisimetrică dacă:
 $a \sim b, b \sim a \Rightarrow a = b$

Se $S \in SCR$ dacă:

- 1) $\forall a \in A \exists s \in S$ a.s. $a \sim s$ ($\Leftrightarrow [a] = [s]$)
- 2) $\forall s_1, s_2 \in S$ atunci $s_1 \neq s_2 \Rightarrow [s_1] \cap [s_2] = \emptyset$, unde $[a]$ repr. clasa de echiv. a unui element $a \in A$. ($[a] = \{b \in A \mid a \sim b\}$)

Exemplu ① Fie " $\equiv_{(\text{mod } 5)}$ " pe \mathbb{Z} $a \equiv b \pmod{5} \Leftrightarrow 5 | a - b$

$$S = \{b \in \mathbb{Z} \mid a \equiv b \pmod{5}\}; \text{ de ex.}$$

$$\mathbb{Z}_0 = \{5k \mid k \in \mathbb{Z}\}$$

$$\mathbb{Z}_1 = \{5k+1 \mid k \in \mathbb{Z}\}$$

$$\mathbb{Z}_2 = \{5k+2 \mid k \in \mathbb{Z}\}$$

$$\mathbb{Z}_3 = \{5k+3 \mid k \in \mathbb{Z}\}$$

$$\mathbb{Z}_4 = \{5k+4 \mid k \in \mathbb{Z}\}$$

$$a \equiv 0 \pmod{5} \text{ sau } a \equiv 1 \pmod{5}$$

$$= \{0, 1, 2, 3, 4\}$$

3 ex. de SCR distinse:

$$S_1 = \{0, 1, 2, 3, 4\}$$

$$S_3 = \{-5, -4, -3, -2, -1\}$$

$$S_2 = \{5, 6, 7, 8, 9\}$$

Def Fie $A = \{1, 2, 3\}$ și R mult. tuturor relațiilor binare pe A .

(Prb 19/24) Considerăm axiomele de: 1) reflexivitate; 2) simetrie; 3) transitivitate; 4) antisimetrie. Calculați imaginea funcției următoare:

$$g: R \rightarrow \{0, 1, 15\}$$

$$A = \{1, 2, 3\}$$

$$g(g) = a_1 + 2a_2 + 2^2a_3 + 2^3a_4 > \text{unde}$$

$a_i = 1$ (resp $a_i = 0$) dacă rel. binară g satisfacă (resp. nu satisfacă) axioma i).

(*) $k \in \{0, \dots, 15\}$ se scrie în mod unic (în bază 2) sub formă $k = b_0 + 2b_1 + 2^2b_2 + 2^3b_3 + 2^4b_4$. $k \in \text{Im}(g) \Leftrightarrow (\exists)n \in \mathbb{R}$ a.s. $g(n) = k \Leftrightarrow (\exists)n \in \mathbb{R}$ a.s. n satisfacă / nu satisfacă A), 2), 3), 4) conform b_1, b_2, b_3, b_4

$\boxed{k=0} \rightsquigarrow k = 0 + 2 \cdot 0 + 2^2 \cdot 0 + 2^3 \cdot 0 + 2^4 \cdot 0$

$0 \in \text{Im}(g) \Leftrightarrow (\exists)\rho_1 \in \mathbb{R}$ a.s. ρ_1 nu satisfacă ax. 1), 2), 3), 4)

$(b_1 = b_2 = b_3 = b_4 = 0)$

De ex $\rho_1 (\subseteq A \times A) = \{(1,2), (2,1), (1,3)\}$ nu satisfacă 1), 2), 3), 4)

$(g(\rho_1) = 0)$

② $\boxed{k=9} \rightsquigarrow g = 1 + 2 \cdot 0 + 2^2 \cdot 0 + 2^3 \cdot 1$ (scrierea unică în bază 2)

$g \in \text{Im}(g) \Leftrightarrow (\exists)\rho_2 \in \mathbb{R}$ a.s. ρ_2 satisfacă ax. 1), 4) și nu satisfacă ax. 2), 3).

De ex $\rho_2 (\subseteq A \times A) = \{(1,1), (2,2), (3,3), \underline{(1,2)}, \underline{(2,3)}\}$

$(g(\rho_2) = 9)$

③ $\boxed{k=4} \rightsquigarrow 4 = 0 + 2 \cdot 0 + 2^2 \cdot 1 + 2^3 \cdot 0$

De ex $\rho_3 (\subseteq A \times A) = \{(1,2), (2,1), (1,1), \underline{(1,3)}, \underline{(2,3)}\}$

$g(\rho_3) = 4$

ρ_3 nu e antisimetrică! (1 ≠ 2)

$(2,2) \notin \rho_3 \Rightarrow \rho_3$ nu e reflexivă!

$\rho_3 \in \text{transitivă} \Leftrightarrow$

$(1,2), (2,1) \in \rho_3 \Rightarrow (1,1) \in \rho_3$

$(1,2), (2,3) \in \rho_3 \Rightarrow (1,3) \in \rho_3$

$(2,1), (1,3) \in \rho_3 \Rightarrow (2,3) \in \rho_3$

$(1,3) \in \rho_3 ; (3,1) \notin \rho_3 \Rightarrow$

ρ_3 nu e simetrică

$\{(1,2), (2,3), (1,3)\}$

TEMĂ Calculați $\text{Im}(g)$. (10, 11 $\notin \text{Im}(g)$).

④ $M = 1 + 2 \cdot 1 + 2^2 \cdot 0 + 2^3 \cdot 1$

$M \in \text{Im}(g) \Leftrightarrow (\exists)\rho_4 \in \mathbb{R}$ a.s. ρ_4 satisfacă ax. 1), 2), 4) și nu satisfacă ax. 3).

Afirmă Dacă g e simetrică și antisimetrică $\Rightarrow \rho \in \text{transitivă}$

(în particular, astăzi înseamnă că $(\cancel{\rho}) \rho_4 \Rightarrow M \notin \text{Im}(g)$)

Bem Fie $(a,b) \in \rho$, $(b,c) \in \rho$. Tc. să arăt că $(a,c) \in \rho$

$\Downarrow \rho \text{ sim.}$

$(b,a) \in \rho$ $(a,b) \in \rho$ | $\xrightarrow{\text{paritatem}} a=b$ $(b,c) \in \rho$

Astfel
 să arăt
 similar
 și
 $a=c$
 b

Ex 2 Def. pe \mathbb{R} rel. binară " \sim " astfel: $x \sim y \Leftrightarrow x^2 - 3x = y^2 - 3y$. Arătăți că " \sim " este rel. de echivalență, calculati R_{\sim} , determinați cu SCR pt " \sim ". E bine definită funcția $f: R_{\sim} \rightarrow \mathbb{R}$, $f(t) = -t^2 + 3t + 7$? Dar $g: R_{\sim} \rightarrow \mathbb{R}$ $g(t) = t^2 + t + 1$?

Ex. 3 Pe \mathbb{C} def " \sim ": $z \sim y \Leftrightarrow |z| = |y|$. Arătăți că " \sim " este rel. de echiv., calculati \mathcal{O}_{\sim} , det. un SCR pt " \sim ".

Ex 2 $x \sim y \stackrel{\text{def}}{\Leftrightarrow} x^2 - 3x = y^2 - 3y$. Vrem să arăt că \sim e rel. de echiv. (adică satisface ax. 1, 2, 3)

Vream să arăt că \sim e rel. de echiv. (adică satisface ax. 1, 2, 3)

Deoarece $x^2 - 3x = x^2 - 3x \stackrel{\text{def}}{\Rightarrow} x \sim x \Rightarrow \sim \text{ e reflexivă. (1)}$

Fie $x, y \in \mathbb{R}$ a.s. $x \sim y \stackrel{\text{def}}{\Rightarrow} x^2 - 3x = y^2 - 3y \Rightarrow y^2 - 3y = x^2 - 3x$

$y \sim x \Rightarrow \sim \text{ e simetrică. (2)}$

Fie $x, y, z \in \mathbb{R}$ a.s. $x \sim y$ și $y \sim z \stackrel{\text{def}}{\Rightarrow} \begin{cases} x^2 - 3x = y^2 - 3y \\ y^2 - 3y = z^2 - 3z \end{cases} \Rightarrow x^2 - 3x = z^2 - 3z$

$\Rightarrow x \sim z \Rightarrow \sim \text{ e transițivă. (3)}$

Din (1), (2) și (3) ⇒ \sim e rel. de echivalență!

Pt un $x \in \mathbb{R}$ $\hat{x} = \{y \in \mathbb{R} \mid x \sim y\} = \{y \in \mathbb{R} \mid x^2 - 3x = y^2 - 3y\}$

clasa de echiv. a lui x

$x^2 - 3x = y^2 - 3y \Rightarrow x^2 - y^2 = 3x - 3y \Rightarrow (x-y)(x+y) = 3(x-y)$

sau $x+y=3$ ($\Rightarrow y=3-x$)

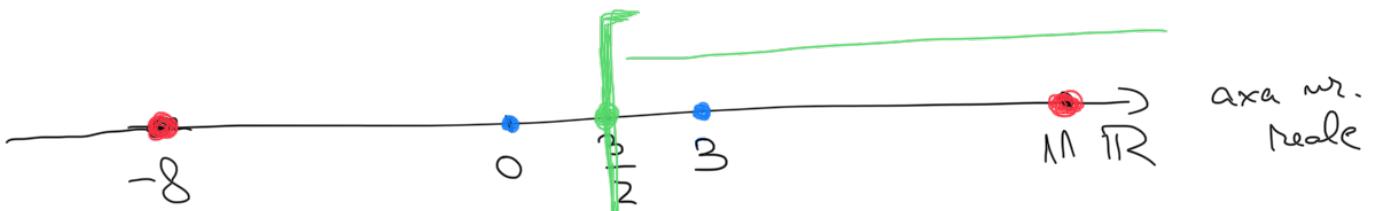
$\Rightarrow (x-y)(x+y-3)=0 \Rightarrow \hat{x} = \{x \in \mathbb{R} \mid x+y=3\}$

$\Rightarrow \hat{\frac{3}{2}} = \left\{ \frac{3}{2} \right\} \quad ; \quad \hat{x} = \left\{ x \in \mathbb{R} \mid x+y=3 \right\} \quad (\forall x \in \mathbb{R}, \exists \frac{3}{2})$

$\hat{-8} = \{-8, 11\} \quad \hat{0} = \{0, 3\}$

$$\mathbb{R}_N = \{x \mid x \in \mathbb{R}\} = \{x \mid x \in S\}$$

↑
SCR pt " \sim "



$$S = \left[\frac{3}{2}; +\infty \right) \quad \frac{3}{2} = \left\{ \frac{3}{2} \right\} \quad -8 = \{-8, M\}$$

Afirmatie $S = \left[\frac{3}{2}; +\infty \right)$ este un SCR pt " \sim ".

Denumib. să verific (vezi def. inceputul §6):

$$\begin{aligned} 1) & \forall a \in \mathbb{R} \quad \exists s \in S \text{ a.s. a.s.} \\ & \text{și } (\forall s_1, s_2 \in S) \quad s_1 \neq s_2 \Rightarrow s_1 \neq s_2. \end{aligned}$$

$$\begin{aligned} & (-\infty, \frac{3}{2}] \notin \text{SCR} \\ & \dots \\ & \therefore [0, \frac{3}{2}] \cup \left(\frac{3}{2}, +\infty \right) \end{aligned}$$

$$\begin{aligned} 1) & \text{ Fie } a \in \mathbb{R}. \quad \text{Dc } \begin{cases} a \geq \frac{3}{2} \text{ sau } s = a \text{ și } s \neq a \\ a < \frac{3}{2} \Rightarrow 3-a > 3-\frac{3}{2} = \frac{3}{2}. \text{ Iau } s = 3-a \text{ și } s \neq a. \end{cases} \end{aligned}$$

$$\begin{aligned} 2) & \text{ Fie } s_1, s_2 \in S \text{ a.i. } s_1 \neq s_2 \Rightarrow s_1 = s_2 \left(= \{s_1, 3-s_1\} \right) \Rightarrow \begin{cases} s_2 = s_1 \\ \text{sau} \\ s_2 = 3-s_1 \end{cases} \end{aligned}$$

$$\begin{aligned} & \text{Dc. } s_2 = 3-s_1 \Rightarrow s_1 + s_2 = 3 \\ & s_1, s_2 \in S = \left[\frac{3}{2}; +\infty \right) \Rightarrow s_1 + s_2 \geq \frac{3}{2} + \frac{3}{2} = 3 \quad \Rightarrow \\ & s_1 + s_2 = 3 \text{ implica } s_1 = \frac{3}{2}, s_2 = \frac{3}{2} \Rightarrow s_1 = s_2 \left(= \frac{3}{2} \right) \end{aligned}$$

$$s_1 + s_2 = 3 \quad \text{implica} \quad s_1 = \frac{3}{2}, s_2 = \frac{3}{2} \Rightarrow s_1 = s_2$$

Prin urmare, $s_1 \neq s_2 \Rightarrow s_1 = s_2$

$$S = \left[\frac{3}{2}; +\infty \right) \in \text{SCR}.$$

$$\text{E } f: \mathbb{R}_N \rightarrow \mathbb{R} \quad f(t) = -t^2 + 3t + 7 \text{ e funcție?}$$

Comentariu Este $f: \mathbb{Q} \rightarrow \mathbb{Z}$ $f\left(\frac{a}{b}\right) = a$ e funcție? NU

Dar $g: \mathbb{Q} \rightarrow \mathbb{Q}$ $g\left(\frac{a}{b}\right) = \frac{a}{b}$ e funcție ($= \Delta_{\mathbb{Q}}$)!

$$\begin{matrix} f\left(\frac{3}{\pi}\right) & f\left(\frac{\pi}{2}\right) \\ \pi = \frac{6}{2} & \\ \therefore 3 & \neq 6 \end{matrix}$$

$\downarrow D_c f = \frac{3}{2}$ $\hat{t} = \left\{ \frac{3}{2} \right\}$ f e bine definită în $\frac{3}{2}$.
 $D_c f + \frac{3}{2} \Rightarrow \hat{t} = \{t, 3-t\} (\Rightarrow \hat{t} = \overbrace{3-t})$
 f e corect definită dacă ($\forall t \in \mathbb{R}$) $f(\hat{t})$ nu depinde
 (bine) de alegera reprezentantului lui \hat{t} , i.e. (în
 acest caz) $f(\hat{t}) = f(\overbrace{3-t}) \Leftrightarrow \hat{t} \in \mathbb{R}_{\sim}$.
 $(f(\overbrace{3-t}) = -(3-t)^2 + 3(3-t) + 7 = -t^2 + 6t - t^2 + 9 - 3t + 7$
 $= -t^2 + 3t + 7 = f(\hat{t}))$

$\Rightarrow f$ e corect definită.

$$g: \mathbb{R}_{\sim} \rightarrow \mathbb{R}$$

$$g(\hat{t}) = t^2 + t + 1$$

$$\begin{array}{l} g(\hat{0}) = 0^2 + 0 + 1 = 1 \\ \cancel{\hat{0} = 3} \quad g(\hat{3}) = 3^2 + 3 + 1 = 13 \end{array}$$

$\Rightarrow g(\hat{0}) \neq g(\hat{3}) \Rightarrow g$ nu e
 funcție
 ((nu e corect
 definită))

Seminar 7

Ex 1 Re \mathbb{C} def. " \sim ": $z \sim y \Leftrightarrow |z| = |y|$. Ar. că " \sim " e rel. de echiv, def un SCR pt " \sim ".

- 1) $|z| = |z| \stackrel{\text{def}}{\Rightarrow} z \sim z \Rightarrow \sim$ e reflexivă
 - 2) $z \sim y \stackrel{\text{def}}{\Rightarrow} |z| = |y| \Rightarrow |y| = |z| \Rightarrow y \sim z \Rightarrow \sim$ e simetrică
 - 3) Fie $x, y, z \in \mathbb{C}$
 $x \sim y \stackrel{\text{def}}{\Rightarrow} |x| = |y|$
 $y \sim z \stackrel{\text{def}}{\Rightarrow} |y| = |z|$ | $\Rightarrow |x| = |z| \stackrel{\text{def}}{\Rightarrow} x \sim z \Rightarrow \sim$ e transitive
- " \sim " e rel. de echiv.

Din 1, 2, 3) $\Rightarrow \sim$ este

$$\hat{S} = \{y \in \mathbb{C} \mid z \sim y\} = \{y \in \mathbb{C} \mid |y| = |z|\}$$

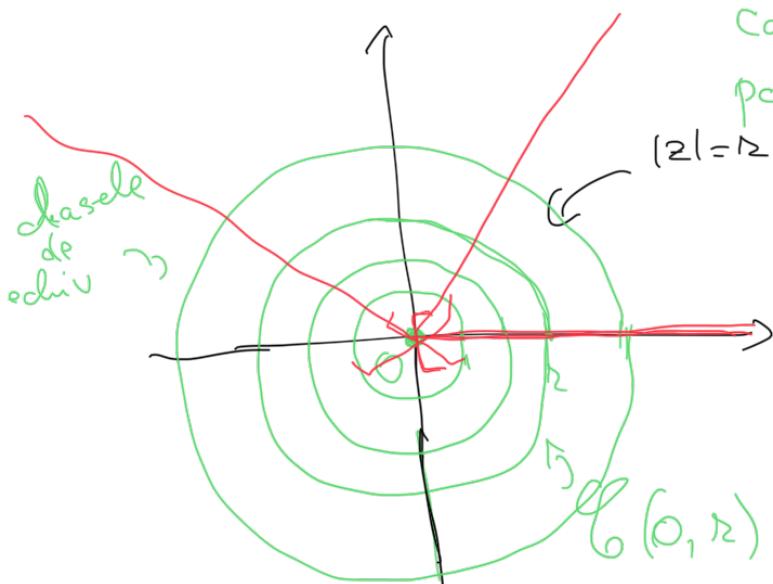
$$\text{Dc } z = \underline{0} \quad (\Rightarrow |z| = 0) \quad \hat{S} = \{0\}$$

$$\text{Dc } z \neq 0 \Rightarrow |z| = r \neq 0$$

$$\begin{array}{l} \overset{R^*}{\text{R}} \\ \text{R}_+ \end{array}$$

$$\hat{S} = \{y \in \mathbb{C} \mid |y| = r\} = \{r(\cos \alpha + i \sin \alpha) \mid \alpha \in [0, \pi]\}$$

SCR pt " \sim " este
 submultime S a lui \mathbb{C} a.i.
 1) $(\forall) z \in \mathbb{C} \quad (\exists) s \in S$ a.i. $z \sim s$
 2) $(\forall) s_1, s_2 \in S \quad s_1 \neq s_2 \Rightarrow s_1 \neq s_2$



mult. nr. complexe ale
 cercorilor afixe sunt.
 pct. cercului $C(O; r)$

Deci, un SCR pt. " \sim " este $S = R_+ = \{r \in R \mid r > 0\}$ (*) (similar se poate arăta că orice semidreaptă inclusă care pleacă din O este un SCR pt " \sim ")

Pt a demn (*) trebuie să arătăm:

- 1) $(\forall) z \in \mathbb{C} \quad z \sim |z|$ (deoarece $|z| = |(|z|)|$) și $|z| \in R_+ = S$

2) Fie $r_1, r_2 \in S$ $r_1 \neq r_2 \Rightarrow |r_1| \neq |r_2| \Rightarrow r_1 \sim r_2$

$S = R_+ \rightarrow \begin{cases} || & |r_1| \neq |r_2| \\ || & r_1 \neq r_2 \end{cases}$

Din 1), 2) $\Rightarrow S \in SCR$.

Ex2 Pe C^* def. " \sim " $z \sim y \Leftrightarrow \text{Ang}(z) = \text{Ang}(y)$. Arătă că " \sim " este rel. de echiv., calculând SCR pt " \sim ".

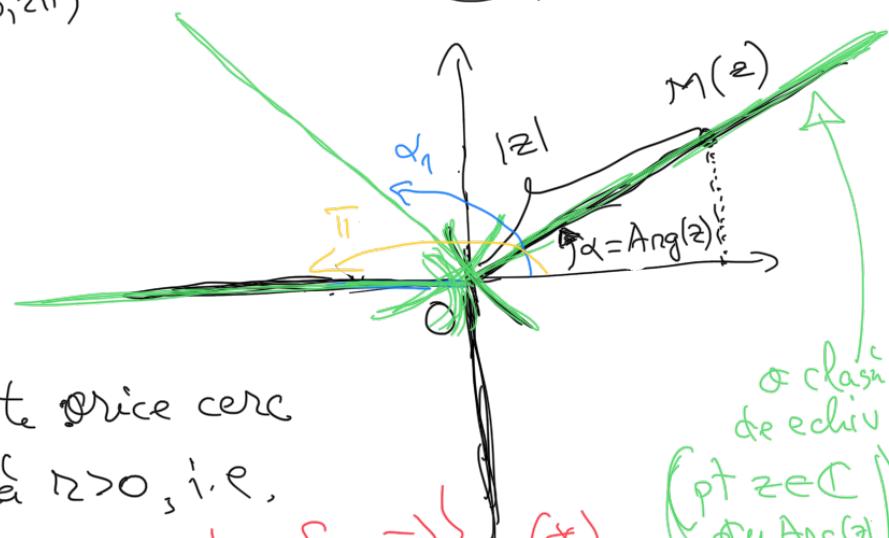
TEZA Arătă că " \sim " este rel. de echiv.

Fie $z \in C^*$ $\hat{z} = \{y \in C^* \mid z \sim y\} = \{y \in C^* \mid \text{Ang}(z) = \text{Ang}(y)\}$.

$$\begin{array}{l} \text{atib} \\ z = |z|(\cos \alpha + i \sin \alpha) \\ (|z| = \sqrt{a^2 + b^2}) \end{array}$$

$$\left\{ \begin{array}{l} \alpha = \text{Ang}(z) \\ \alpha \in [0, 2\pi) \end{array} \right.$$

$$\left\{ \begin{array}{l} r(\cos \alpha + i \sin \alpha) \mid r \in R^* \\ r \in [0, \infty) \end{array} \right.$$



În SCR pentru " \sim " este o serie cerc

cu centru în 0 și rază $r > 0$, i.e.

$$S = \{r(\cos \alpha + i \sin \alpha) \mid \alpha \in [0, 2\pi)\} \quad (*)$$

o clasă
de echiv
(pt $z \in C$)
(cu $\text{Ang}(z)$)
 α

Pentru a demonstra $(*)$ trebuie să arătăm:

1) Fie $z \in C^* \Rightarrow (\exists !) r, \alpha \in [0, 2\pi)$ a.t. $z = r(\cos \alpha + i \sin \alpha) \quad \begin{pmatrix} r = |z| \\ \alpha = \text{Ang}(z) \end{pmatrix}$

$$\begin{array}{c} \downarrow \\ z \sim r(\cos \alpha + i \sin \alpha); y \in S \\ y \end{array}$$

2) Fie $s_1, s_2 \in S$ a.s. $s_1 \neq s_2 \Rightarrow s_1 = r_1(\cos \alpha_1 + i \sin \alpha_1)$ $\alpha_1 \in [0, 2\pi)$
 $s_2 = r_2(\cos \alpha_2 + i \sin \alpha_2)$ $\alpha_2 \in [0, 2\pi)$

$$\Rightarrow \alpha_1 = \text{Ang}(s_1), \alpha_2 = \text{Ang}(s_2) \quad \begin{array}{l} \text{def} \\ \hline \sim \end{array} \quad s_1 \sim s_2.$$

Din 1), 2) $\Rightarrow S$ este un SCR pt " \sim ".

Ex.3 Fie $A \neq \emptyset$, $\emptyset \neq B \subseteq A$. Definim pe $P(A)$ relația ρ :

$$(*) X \rho Y \stackrel{\text{def}}{\iff} X \cap B = Y \cap B.$$

Să se arate că ρ e rel. de echiv. și $P(A)/\rho$ este un bijectie cu $P(B)$. ($\Rightarrow P(B)$ este un SCR pt ρ)

— $X \rho X \Rightarrow X \cap B = X \cap B \Rightarrow \rho$ e reflexivă

$$1) X \cap B = X \cap B \stackrel{\rho}{\Rightarrow} X \rho X \Rightarrow \rho$$
 e simetrică

$$2) X \rho Y \Rightarrow X \cap B = Y \cap B \Rightarrow Y \cap B \cap X \cap B \Rightarrow Y \rho X \Rightarrow \rho$$
 e

$$3) X \rho Y \Rightarrow X \cap B = Y \cap B \Rightarrow X \cap B = Z \cap B \Rightarrow X \rho Z \Rightarrow \rho$$
 e

$$Y \rho Z \Rightarrow Y \cap B = Z \cap B$$

Din 1, 2 și 3) $\Rightarrow \rho$ e rel. de echiv.

— $P(A)/\rho = \{[X] \mid X \in P(A)\}$ $[X] = \{y \in A \mid X \rho y\} =$
multimea
factor

clasa de echiv.
a subm. X

$\{y \in A \mid X \cap B = Y \cap B\}$

$$A \ni X \quad X \cap B = (X \cap B) \cap B \Rightarrow X \rho (X \cap B) \Rightarrow$$

$\Rightarrow [X] = [X \cap B]$ \Rightarrow Am arătat 1) dim: $P(B)$ e un SCR pt ρ .

2) Fie $y_1, y_2 \in P(B)$ a.i. $y_1 \neq y_2$ $\stackrel{\text{def}}{\iff} y_1 \cap B \neq y_2 \cap B$ $\Rightarrow y_1 \rho y_2$.

Din 1 și 2) $\Rightarrow P(B)$ este un SCR pt ρ .

Afirmatie: Funcția $f: P(A)/\rho \rightarrow P(B)$ $f([x]) = X \cap B$ este o bijectie. ($\Rightarrow P(B)$ este un SCR pt ρ și $P(A)$ în raport cu rel-de echiv. ρ)

Dem: \bullet f bine definită: fie $x, y \in P(A)$ a.i. $x \rho y$

$\Rightarrow X \cap B = Y \cap B \Rightarrow f([x]) = f([y]) \Rightarrow f$ e bine def.

• Fie $[x], [y] \in P(A)/\emptyset$ a.i. $f([x]) = f([y]) \Rightarrow f$

$X \cap B = Y \cap B \xrightarrow{\text{def}} X \setminus Y \xrightarrow[\text{C5}]{\text{Teorema}} [x] = [y] \Rightarrow f$ e injectivă

• f e surjectivă: Fie $y \in P(B) (\Rightarrow Y \cap B = Y)$

$$f([y]) = Y \cap B = Y \Rightarrow f$$
 e surj.

Dim $\textcircled{1}, \textcircled{2}$ și $\textcircled{3} \Rightarrow f$ e fct, bij.

Ex 4 (Construcția lui Z) Fie " \sim " rel. pe $\mathbb{N} \times \mathbb{N}$ def. prin $(a,b) \sim (c,d) \Leftrightarrow a+d = b+c$

An. că " \sim " e rel. de echiv. și că $\mathbb{N} \times \mathbb{N}/\sim$ este în bijecție cu \mathbb{Z} .

Ex 5 (Construcția lui Q) Fie " \sim " rel. pe $\mathbb{Z} \times \mathbb{N}^*$ def. prin $(a,b) \sim (c,d)$ dacă $ad = bc$. An. că " \sim " e rel. de echiv și $\mathbb{Z} \times \mathbb{N}^*/\sim$ este în bijecție cu \mathbb{Q} .

Ex 4: Excl! " \sim " e rel. de echiv.

$\widehat{(a,b)} = \{(c,d) \in \mathbb{N} \times \mathbb{N} \mid (a,b) \sim (c,d)\} = \{(c,d) \in \mathbb{N} \times \mathbb{N} \mid c-d = a-b\}$

Să demonstrem că $f: \mathbb{N} \times \mathbb{N}/\sim \rightarrow \mathbb{Z}$ este o funcție bijectivă

• f e bine def (*): Fie $(c,d) \sim (a,b) \Rightarrow c-d = a-b \Rightarrow f(\widehat{(c,d)}) = f(\widehat{(a,b)}) \Rightarrow f$ e bine def

\circlearrowleft f e inj: $\hat{(a,b)}, \hat{(c,d)} \in \mathbb{N} \times \mathbb{N}$ a.i. $f(\hat{(a,b)}) - f(\hat{(c,d)}) = \frac{\text{def}}{\varnothing}$
 fie $(\hat{a},\hat{b}), (\hat{c},\hat{d}) \in \mathbb{N} \times \mathbb{N}$ a.i. $a-b=c-d \Rightarrow a+d=b+c \Rightarrow (\hat{a},\hat{b}) \cap (\hat{c},\hat{d}) = \varnothing \Rightarrow \hat{(a,b)} = \hat{(c,d)}$

$\Rightarrow f$ e inj.

\circlearrowleft f e surj: fie $y \in \mathbb{Z}$
 $\exists x \rightarrow y \geq 0 \wedge f(\hat{(y,0)}) \stackrel{\text{def}}{=} \frac{y}{|x|} - 0 = y$
 $y < 0 \rightsquigarrow f(\hat{(0,-y)}) \stackrel{\text{def}}{=} \frac{0}{|x|} - (-y) = y$

$\{ \Rightarrow f$ e surj.
 $vladimir@fmi.unibuc.ro$

Pr. (generică)

Seminar 8

22.11.2021

Calculati restul împărțirii lui a^b la c , unde a, b, c sunt numere naturale care care.

Mai târziu $a^b \pmod{c}$

Ex $2021^{2021} \pmod{22}, 2022^{2022} \pmod{22}$

TEMA

$\begin{array}{c} \checkmark \\ 2021^{2021} \text{ în } \mathbb{Z}_{22} \end{array}$

$\bullet a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n} \quad (n \geq 2)$

$$\begin{aligned} 2021^{2021} &= 19^{2021} \pmod{22} \equiv (-3)^{2021} \pmod{22} \\ &\equiv -3^{2021} \pmod{22} \\ &\equiv -(-3)^{404} \cdot 3 \pmod{22} \\ &\equiv -(-3) \pmod{22} \equiv 19 \pmod{22} \end{aligned}$$

$$3^5 = \frac{243}{22} \pmod{22}$$

$$(a \equiv 1 \pmod{n}) \downarrow \text{restul împărțirii la } n$$

$$\begin{array}{r} 2021^{22} \\ 198 \quad | \\ \hline 22 \\ 19 \end{array}$$

T. Euler $(a, n) = 1$

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

$$\phi(22) = 22 \cdot \frac{1}{2} \cdot \frac{10}{11} = 10$$

Dem $\begin{aligned} -3^{2021} \pmod{22} &\equiv \\ &\equiv -3^{10 \cdot 202 + 1} \pmod{22} \\ &\equiv -(-3)^{202} \cdot 3 \pmod{22} \equiv -3 \pmod{22} \end{aligned}$

Euler +

Pabz Fie $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$. Def. pe G legea $x * y = \{x+y\}$ ($\{x+y\}$ înseamnă parte fracțională a lui $x+y$). Arăta că $(G, *)$ este un grup abelian.

" $*$ "-asociativitate: $a * (b * c) = a * \{b+c\} = \{a+\{b+c\}\} \quad (1)$

$$\{x\} = x - [x]$$

$$(a * b) * c = \{a+b\} * c = \{\{a+b\} + c\} \quad (2)$$

$$\begin{aligned} \{a+\{b+c\}\} &= a + \underline{\{b+c\}} - \underline{\{a+\{b+c\}\}} = a + b + c - \{b+c\} \\ &= a + b + c - \{b+c\} - (\{a+b+c\} - \{b+c\}) = \end{aligned}$$

$$\begin{aligned} &= a + b + c - \{a+b+c\} = \{a+b+c\} \\ &= a + b + c - \{a+b+c\} = \{a+b+c\} \end{aligned}$$

$$[x - \bar{x}] = [x]^k \quad k \in \mathbb{Z}$$

Analog se arată că $\{\{a+b\} + c\} = \{a+\{b+c\}\}$

$$\Rightarrow (1) = (2) \quad \forall a, b, c \in G$$

$\Rightarrow " * "$ este asociativă

" $*$ " este comutativă!

$$x * 0 = \{x+0\} = \{x\} = x = 0 * x \quad (\forall x \in G) \Rightarrow 0 \text{ este element neutru pt } *$$

neutru pt *

Fie $x, y \in G$ a.i. $x * y = 0 \Rightarrow 3x + y = 0 \Rightarrow x + y \in \mathbb{Z}$
 $x, y \in [0, 1] \Rightarrow 0 \leq x + y \leq 2$

$$\Rightarrow x + y \in \{0, 1\}$$

Dc $x + y = 0 \Rightarrow x = -y = 0$ (0 este inversul lui 0)

Dc $x + y = 1 \Rightarrow y = 1 - x$ (x este inversul lui $1-x$ ($\forall x \in G \setminus \{0\}$))

$\Rightarrow U(G) = G \Rightarrow (G, *)$ este grup abelian

Prb 3 "Calculati" toate morfismele de grupuri dintre:

$(\mathbb{Z}, +)$ și $(\mathbb{Z}, +)$; $(\mathbb{Z}, +)$ și $(\mathbb{Q}, +)$; $(\mathbb{Q}, +)$ și $(\mathbb{Z}, +)$

$(\mathbb{Z}_m, +)$ și $(\mathbb{Z}_n, +)$; $(\mathbb{Z}_m, +)$ unde $m, n \in \mathbb{N}$, $m, n \geq 2$.

(Determinam morfismele de grupuri $f: (\mathbb{R}, +) \rightarrow (\mathbb{R}, +)$ a.i. f să fie fct. continuă)

$f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$ morfism de gr. $\Rightarrow f(x+y) = f(x) + f(y)$

$(\Rightarrow f(0) = 0)$ $\begin{array}{l} \cancel{x=y=1} \\ \cancel{x=2, y=1} \\ \cancel{x \in \mathbb{Z}, y \in \mathbb{N}} \end{array}$ $\begin{array}{l} f(2) = f(1) + f(1) = 2f(1) \\ f(3) = f(2) + f(1) = 2f(1) + f(1) = 3f(1) \\ \text{dsm. că } f(n) = nf(1) \end{array}$ $\begin{array}{l} f(x_1 + \dots + x_n) \\ f(x_1) + \dots + f(x_n) \end{array}$

Prim ind. după $n \in \mathbb{N}$ se

$$n \in \mathbb{N}^* \quad f(-n) = ? \quad \begin{array}{l} f(0) = f(n+(-n)) \\ \parallel \\ 0 \end{array} \quad \begin{array}{l} \Downarrow \\ f(n) + f(-n) = 0 \end{array} \Rightarrow$$

$$f(-n) = -f(n) = -nf(1)$$

$$\Rightarrow f(k) = kf(1) \Leftrightarrow k \in \mathbb{Z} \Rightarrow f \text{ este perf. det. de } f(1)$$

Toate morf. de gr. de la $(\mathbb{Z}, +)$ în $(\mathbb{Z}, +)$ sunt date: $a \in \mathbb{Z}$

Toate morf. de gr. de la $(\mathbb{Z}, +)$ în $(\mathbb{Z}, +)$ sunt date: $a \in \mathbb{Z}$

$$f_a: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +) \quad f_a(k) = ka \quad (\forall k \in \mathbb{Z})$$

Generalizare Fie $(G, +)$ un grup abelian. Morfisme de grupuri

de la $(\mathbb{Z}, +)$ în $(G, +)$ sunt date de:
 $(a \in G \text{ oricare})$

$$f_a: (\mathbb{Z}, +) \rightarrow (G, +) \quad f_a(k) = ka \quad (\forall k \in \mathbb{Z})$$

$$(k \in \mathbb{N}^* \quad ka = \underbrace{a + \dots + a}_{k \text{ ori}} \quad ; \quad k < 0, k \in \mathbb{Z} \quad ka = \underbrace{(-a) + \dots + (-a)}_{-k \text{ ori}})$$

Fie $h: (\mathbb{Q}, +) \rightarrow (\mathbb{Q}, +)$ morf. de grupuri. $h(x+y) = h(x) + h(y)$
 $\forall x, y \in \mathbb{Q}$

La fel ca mai sus

$$h(k) = kh(1) \quad \forall k \in \mathbb{Z}$$

Ex $h\left(\frac{1}{2} + \frac{1}{2}\right) = h(1)$
 $x=y=\frac{1}{2} \quad h\left(\frac{1}{2}\right) + h\left(\frac{1}{2}\right) = 2h\left(\frac{1}{2}\right)$

Fie $g \in \mathbb{Q}^*$ $\Rightarrow g = \frac{a}{b}$ $b \neq 0, a \in \mathbb{Z}, b \in \mathbb{N} \quad (a, b) = 1$

$$h\left(b \cdot \frac{a}{b}\right) = h\left(\underbrace{\frac{a}{b} + \dots + \frac{a}{b}}_{b \text{ ori}}\right) \stackrel{\substack{\text{morf} \\ (b \in \mathbb{N})}}{=} h\left(\frac{a}{b}\right) + \dots + h\left(\frac{a}{b}\right) = b h\left(\frac{a}{b}\right)$$

||

$$h(a) = \underbrace{ah(1)}_{a \in \mathbb{Z}}$$

$$bh\left(\frac{a}{b}\right) = ah(1) \Rightarrow h\left(\frac{a}{b}\right) = \frac{a}{b} h(1) \Rightarrow h(g) = g h(1) \quad \forall g \in \mathbb{Q}$$

$\frac{a}{b} \in \mathbb{Q}^*$
oarecare

\Rightarrow Orice morfism de gr. de la $(\mathbb{Q}, +)$ în $(\mathbb{Q}, +)$ este de forma
 $f_a: (\mathbb{Q}, +) \rightarrow (\mathbb{Q}, +) \quad h_a(g) = ag \quad \forall g \in \mathbb{Q} \quad (a = \frac{h(1)}{h(0)})$

$a \in \mathbb{Q}$
arbitrari

Q1 Există o generalizare identică cu cea de mai sus în
casul $(\mathbb{Z}, +)$? **NU**

Def. morfismele de grupuri între 2 grupuri oarecare?

Q2 Există morfisme de grupuri între 2 grupuri oarecare. Funcție

Obs Fie $(G_1, *)$, (G_2, \circ) 2 grupuri oarecare. Funcție
 $\varphi: (G_1, *) \rightarrow (G_2, \circ)$ $\varphi(g) = s_{G_2}(g)$ $\forall g \in G_1$ este un morfism
de grupuri, numit și morfismul trivial.

Singurul morfism de grupuri de la $(\mathbb{Q}, +)$ în $(\mathbb{Z}, +)$ e

morfismul trivial. \nparallel

Fie $\varphi: (\mathbb{Q}, +) \rightarrow (\mathbb{Z}, +)$ un morfism de grupuri \Rightarrow
 $\Rightarrow \varphi = h_a$ cu $a \in \mathbb{Z}$ (deoarece $h_a(1) = a \in \mathbb{Z}$) $\begin{pmatrix} \text{morf.} \\ \text{trivial} \\ \text{et } h_a \end{pmatrix}$

Dacă $a \neq 0$ $\varphi\left(\frac{1}{2a}\right) = h_a\left(\frac{1}{2a}\right) = \frac{a}{2a} = \frac{1}{2} \notin \mathbb{Z} \Rightarrow$

\Rightarrow Nu există morfism de activitate de la $(\mathbb{Q}, +)$ în $(\mathbb{Z}, +)$.

Fie $f: (\mathbb{R}, +) \rightarrow (\mathbb{R}, +)$

f continuă.

$$f(x+y) = f(x) + f(y) \quad \forall x, y \in \mathbb{R}$$

P Orice nr. real poate fi scris ca limita unei siruri de nr. rationale.

La fel $f(q) = \lim_{n \rightarrow \infty} f(q_n)$ unde $q_n \in \mathbb{Q}$.

Fie $a \in \mathbb{R}$ și $(q_m)_m$ un sir de nr. reale. a.i. $\lim_{m \rightarrow \infty} q_m = a$.

$$\lim_{m \rightarrow \infty} f(q_m) = f\left(\lim_{m \rightarrow \infty} q_m\right) = f(a)$$

$\| q_m \in \mathbb{Q}$

continuă

$$\Rightarrow f(a) = a f(1)$$

$$\lim_{n \rightarrow \infty} (q_n f(1)) = f(1) \cdot \left(\lim_{n \rightarrow \infty} q_n\right) = f(1) \cdot a$$

$\| a \in \mathbb{R}$

Exe 1 Arătati că un grup (G, \cdot) în care $x^2 = 1 \ (\forall x \in G)$, este un grup abelian.

Denumire $x \cdot y = y \cdot x \ (\forall x, y \in G)$

$$(\forall x, y \in G) \Rightarrow x^2 \cdot y^2 = 1 = (xy)^2$$

$$x^2 \cdot y^2 = xy \cdot xy \mid \cdot x^{-1}$$

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

$$xy = yx \ (\forall x, y \in G)$$

$\Rightarrow (G, \cdot)$ este abelian.

Fie $G_1 = (\mathbb{Z}_4, +)$ $G_2 = (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ $G_3 = (\mathbb{Z}_8, +)$

$$[g^0 = e]$$

$$G_1 = (\mathbb{Z}_4, +)$$

tabla lui G_1

$$|G_1| = 4$$

$$\text{ord}(0) = 1$$

(Obs: Intr-un grup singular elementul de ordin 1 este elem. neutru.)

$$\text{ord}(1) = 4 \Rightarrow G_1 = \langle 1 \rangle$$

$$2+2=0 \Rightarrow \text{ord}(2)=2$$

$$\text{ord}(3) = 4 \Rightarrow G_1 = \langle 3 \rangle$$

$$\begin{aligned} 3+3 &= 2 \neq 0 \\ 3+3+3 &= 5 = 1 \neq 0 \\ 3+3+3+3 &= 0 \end{aligned}$$

Dacă (G, \cdot) grup și $g \in G$ are $\text{ord}(g) < \infty$. atunci

$$\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$$

$$G_2 = (\mathbb{Z}_2 \times \mathbb{Z}_2, +) \quad \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Definire (G, \cdot) un grup, $g \in G$. S.m. ordinul elem. g , $\text{ord}(g)$: fiind s.m. cu $\text{ord}(g)$.

$\text{ord}(g) =$ cel mai mic nr. nat. număr a.i. $g^m = 1$ (dacă există $m \in \mathbb{N}$ a.i. $g^m = 1$) sau ∞ dacă $g^{\infty} \neq 1$ (adică).

Exemplu

$$\textcircled{1} (\mathbb{Z}_m, +) \quad m \geq 2$$

$$\text{ord}(1) = m$$

$$\textcircled{2} (\mathbb{Z}, +) \quad \text{ord}(1) = \infty \quad \text{ord}(k) = \infty \quad k \neq 0$$

$$\textcircled{3} (G, \cdot) \rightarrow \text{grup}$$

că $\text{ord}(g) \mid |G|$
(vom demonstra că $e \rightarrow$ elem. neutru)

$$\text{ord}(e) = 1$$

$$|\langle g \rangle| = \text{ord}(g)$$

subgrup generat de g .

\oplus	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

$$\text{ord}((0,1)) = 2 = \text{ord}((1,0))$$

$$\text{ord}((0,0)) = 1 \quad \text{ord}((1,1))$$

$\swarrow \quad \searrow$

G este ciclic

G poate fi generat minimal de 2 elem.

$$G = \langle (0,1), (1,0) \rangle = \langle (0,1), (1,1) \rangle = \langle (1,0), (1,1) \rangle.$$

Exercițiu Fie grupul $\langle U(\mathbb{Z}_{19}), \cdot \rangle$ și $\langle U_4 = \{z \in \mathbb{C} \mid z^4 = 1\}, \cdot \rangle$, $\langle U(\mathbb{Z}_8), \cdot \rangle$. Identificați cu cine sunt izomorfe grupurile și precizați dacă sunt izomorfe între ele.

$$U(\mathbb{Z}_8) = \overline{\{1, 3, 5, 7\}}_{\mathbb{C}_8}$$

$$U(\mathbb{Z}_8) = \langle \bar{3}, \bar{5} \rangle = \langle \bar{3}, \bar{7} \rangle = \langle \bar{5}, \bar{7} \rangle$$

$$\text{ord}(\bar{3}) = \text{ord}(\bar{5}) = 2$$

$$\text{ord}(\bar{7})$$

$$U_4 = \{ \pm 1, \pm i \mid i^4 = 1 \}$$

tabla lui
 $U(\mathbb{Z}_8)$

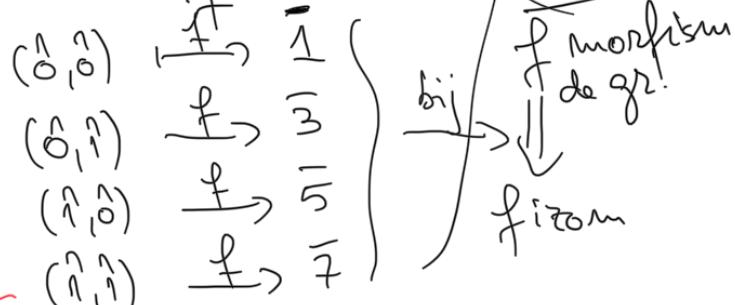
\cdot	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

tabloului
 (U_4)

•	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

Se observă că $U(\mathbb{Z}_8) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ (primă suprapunere a tabelelor) via bijecția:

$$(\mathbb{Z}_2 \times \mathbb{Z}_2, +) \cong U(\mathbb{Z}_8)$$



$$(\mathbb{Z}_4, +) \cong U_4$$

$\begin{array}{ccc} 0 & \xrightarrow{g_1} & 1 \\ 1 & \xrightarrow{g_1} & i \\ 2 & \xrightarrow{g_1} & -1 \\ 3 & \xrightarrow{g_1} & -i \end{array}$

 $\begin{array}{ccc} 0 & \xrightarrow{g_2} & 1 \\ 1 & \xrightarrow{g_2} & i \\ 2 & \xrightarrow{g_2} & -1 \\ 3 & \xrightarrow{g_2} & -i \end{array}$

Exc!
gr de gr
gr izom.

$$f((\overset{1}{0}, \overset{1}{1}) + (\overset{1}{1}, \overset{1}{0})) \stackrel{?}{=} f(\overset{1}{0}, \overset{1}{1}) \cdot f(\overset{1}{1}, \overset{1}{0})$$

$$f(\overset{1}{1}, \overset{1}{1})$$

$$\frac{1}{7}$$

$$\frac{1}{3} \cdot \frac{1}{5}$$

$$\frac{1}{7}$$

Obs Există 6 elemente între cele 2 grupuri!

$$g_2(\overset{1}{i}) = -i$$

Obs Există 2 izomorfii între cele 2 grupuri

Așteptăm că $(\mathbb{Z}_4, +)$ să nu fie izomorf cu $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$!

Pp red. abs. că există un izomorf de gr. $\varphi: (\mathbb{Z}_4, +) \rightarrow (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$

$\varphi(\overset{1}{1})$ are ordinul 2

$$\mathbb{Z}_2 \times \mathbb{Z}_2$$

$$\text{ord } \varphi(\overset{1}{1}) = 2$$

1. $\varphi(\overset{1}{1}) = (\overset{1}{0}, \overset{1}{0})$ și $\varphi(\overset{1}{0}) = (\overset{1}{0}, \overset{1}{0})$ este unică din celelalte 3 elemente.

$$\varphi(\overset{1}{1}) = (\overset{1}{0}, \overset{1}{0})$$

$$\varphi(\overset{1}{1}) + \varphi(\overset{1}{1}) = (\overset{1}{0}, \overset{1}{0})$$

II. φ nu este izomorf de gr.

$$\varphi(\overset{1}{1} + \overset{1}{1}) = \varphi(\overset{1}{2}) \quad \text{X } (\varphi \text{ bij})$$

\Rightarrow Pp e falsă
 \Rightarrow gr. nu sunt izomorfe.

Ex Să se arate că un grup cu 4 elemente este izomorf sau cu $(\mathbb{Z}_4, +)$ sau cu $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.

Obs ① Să se arate că orice grup cu p elemente, p prim, este izomorf cu $(\mathbb{Z}_p, +)$.

Prop Fie (G_1, \circ) și (G_2, \circ) 2 grupuri izomorfe și $x \in G_1$, a.s. $\text{ord}(x) = n$. Dacă $\varphi: G_1 \rightarrow G_2$ este un izomorf de grupuri \Rightarrow $\text{ord}(\varphi(x)) = n$.

Obs În particular, prop. ant. implică faptul că pentru

2 grupuri finite multiseturile date de ordinele elem. sunt identice.

Dem prop $f: (G_1, \cdot) \rightarrow (G_2, \circ)$ izomorfie $\Leftrightarrow \forall m \in \mathbb{N}, m < \infty$

ord(x) = m $\Rightarrow x^m = 1_{G_1} \wedge x^{m+1} \neq 1_{G_1}$

$f(x) \circ \dots \circ f(x) = f(x)^m$

$f(\underbrace{x \circ x \circ \dots \circ x}_{\text{non}}) = f(x^m) = f(1_{G_1}) = 1_{G_2}$

$\Rightarrow f(x)^m = 1_{G_2}$

ord(f(x)) ≤ m

Pp abs că $(\exists t \in \mathbb{N}^*, t < m$ a.i.

$f(x)^t = 1_{G_2}$

$\| f \text{ morf}$

$f(x^t) = 1_{G_2}$

$\Rightarrow f(x^t) = 1_{G_2}$

$f(1_{G_1}) = 1_{G_2}$

$\Rightarrow f \text{ bij}$

$\Rightarrow \text{ord}(x) \leq t < m \quad \text{doar}$

$\Rightarrow x^t = 1_{G_1} \Rightarrow \text{ord}(x) \leq t < m$

$\Rightarrow \text{Pp e falsă} \Rightarrow \text{ord}(f(x)) = m$.

$$U(\mathbb{Z}_{19}, \cdot) = \mathbb{Z}_{19} \setminus \{0\}$$

grup cu 18 elemente.

$$U(\mathbb{Z}_m, \cdot) = \{k \mid 1 \leq k \leq m, (k, m) = 1\}$$

$$|U(\mathbb{Z}_m, \cdot)| = \varphi(m)$$

Obs Se dem. (la mată în anul II, sem II) că un grup abelian cu m elemente este izomorf cu un produs direct de gr.
 $(\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \times \mathbb{Z}_{d_r})^+$ unde $1 < d_1 \leq \dots \leq d_r$, $d_1 | d_2 | \dots | d_r$, $d_1 \cdot d_2 \cdot \dots \cdot d_r = m$.

$18 = 18 = 3 \cdot 6 \Rightarrow$ un grup cu 18 elem. este izomorf cu $(\mathbb{Z}_3 \times \mathbb{Z}_6)^+$ sau cu $(\mathbb{Z}_3 \times \mathbb{Z}_6)^?$

Ex (Termă!) Există elemente de ordin 18 în $U(\mathbb{Z}_{19})$?

Exemplu Calculăm $\text{ord}(6)$

$$\begin{aligned} 6^{12} &= \hat{3}^6 = -\hat{2} \neq \hat{1} \\ 6^3 &= -\hat{2} \cdot \hat{6} = -\hat{12} = \hat{7} \neq \hat{1} \end{aligned}$$

$$\begin{aligned}\hat{c}^4 &= \hat{4} & \hat{c}^5 &= -\hat{14} = \hat{5} & \hat{c}^6 &= \hat{49} = \hat{1} \\ \hat{c}^8 &= \hat{16} = -\hat{3} & \hat{c}^9 &= \hat{6} \cdot \hat{5} = \hat{20} = \hat{1} & \Rightarrow \boxed{\text{ord}(\hat{c}) = 9}\end{aligned}$$

Ex Să se arate că un grup cu 4 elemente este izomorf ori cu $(\mathbb{Z}_4, +)$ ori cu $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.

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

- ① Dacă G are un element de ordin 4 și G este ciclic $\xrightarrow[\text{S9}]{\text{verifi.}} (G, \cdot) \cong (\mathbb{Z}_4, +)$ (au "aceleasi" table)
- ② $(\forall) x \in G \Rightarrow \text{ord}(x) \neq 4$. Lagrange $\Rightarrow \text{ord}(x) | 4 \Rightarrow \text{ord } x \in \{1, 2\}$.

Dar $\boxed{\text{ord}(x) = 1 \Leftrightarrow x = 1_G} \Rightarrow (\forall) x \in G \setminus \{1_G\} \Rightarrow \text{ord}(x) = 2$.

$$\Rightarrow x^2 = 1_G \quad (\forall) x \in G \Rightarrow G \text{ este abelian} ; \quad G = \{1_G, x, y, z\}$$

verifi S9, S8

$z = xy$ (deoarece $x \neq y \neq 1_G$ distincte 2 căte 2 : $xy \neq x \rightsquigarrow y \neq 1_G$)

$$xy \neq y \Rightarrow x \neq 1_G ; \quad xy = 1_G \Rightarrow y = x^{-1} = x \Rightarrow xy \neq 1_G \Rightarrow$$

izom.

$$\Rightarrow G = \langle x, y \rangle \cong (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$$

grupuri

$$\begin{array}{ccc} 1_G & \xrightarrow{\varphi} & (0, 0) \\ x & \xrightarrow{\varphi} & (1, 0) \\ y & \xrightarrow{\varphi} & (0, 1) \\ xy & \xrightarrow{\varphi} & (1, 1) \end{array}$$

$$\varphi(x \cdot y) = \varphi(x) + \varphi(y)$$

$\Rightarrow \varphi$ e izom. de grupuri.

φ e bijecție
 φ e morfism de grupuri! (Ex!)

verificări

Ex! Un grup cu 6 elemente este izomorf cu $(\mathbb{Z}_6, +)$ sau (S_3, \circ) .

abelian nonabelian

Ex! Fie p un nr. prim. Să se arate că un grup G cu p elemente este izomorf cu $(\mathbb{Z}_p, +)$.

Dem Fie (G, \cdot) un grup $|G| = p > 2$. Fie $x \in G \setminus \{1_G\} \Rightarrow \text{ord}(x) \neq 1$

T. Lagrange $\Rightarrow \text{ord}(x) | |G| = p$

$$\Rightarrow \text{ord}(x) = p. \Rightarrow G = \langle x \rangle = \{1_G, x, x^2, \dots, x^{p-1}\}$$

Fie $\varphi: G \longrightarrow (\mathbb{Z}_p, +)$ $\varphi(x^k) = \hat{k}$ (\forall)

$(x^0 = 1_G)$ atunci φ este morfism de grupuri bijectiv (= izom. de gr.)

f morf. de grupuri: $f(x^i \cdot x^j) = f(x^i) + f(x^j)$ (A) $i, j \in \{0, \dots, p-1\}$

$$f(x^i) + f(x^j) = \widehat{i} + \widehat{j} = \widehat{i+j}$$

(*)

$$f(x^i \cdot x^j) = f(x^{i+j}) \quad \begin{cases} \text{d.c. } i+j \leq p-1 \\ \text{d.c. } i+j > p \Rightarrow f(x^{i+j}) = f(x^p \cdot x^{i+j-p}) \\ \quad = f(1 \cdot x^{i+j-p}) = f(x^{i+j-p}) = \widehat{i+j-p} = \widehat{i+j} \end{cases}$$

(1) $0 \leq i, j \leq p-1$ (2)

Din (A), (1) și (2) \Rightarrow (0)

Ordinul unui element $(G, \circ) \rightarrow \text{grup.}$

Exc 1 Dacă $\text{ord}(x) = m < \infty$ atunci $\underbrace{k \in \mathbb{Z}}_{\text{a.i. }} x^k = 1_G \Leftrightarrow \underbrace{m \mid k}$.

Dem " \Leftarrow " $m \mid k \Rightarrow k = m \cdot a, a \in \mathbb{Z}$ $x^k = x^{m \cdot a} = (x^m)^a \xrightarrow{\text{ord}(x)=m} 1_G^a = 1_G$.

" \Rightarrow " P.p. red. la abs. că $m \nmid k$ $\Rightarrow k = m \cdot a + r$ cu $0 < r < m$

$$x^k = 1_G \Rightarrow x^{m \cdot a+r} = 1_G \Rightarrow (x^m)^a \cdot x^r = 1_G \xrightarrow{\substack{\text{||} \\ \text{ord}(x)=m}} 1^a \cdot x^r = 1_G \Rightarrow \boxed{x^r = 1_G} \quad (0 < r < m)$$

$\cancel{\text{d}} \quad (\text{ord}(x) = m) \Rightarrow \text{P.p. e falsă} \Rightarrow m \nmid k.$

Exc 2 Fie (G, \circ) un grup și $x \in G$ și $\text{ord}(x) = m < \infty$. Arătați că:

(A) $\forall k \in \mathbb{N} \quad \text{ord}(x^k) = \frac{m}{(m, k)}$, unde (m, k) reprez. c.m.m.d.c. dintre m și k .

Aplicații: **Exc 3** Calculați $\text{ord}(\widehat{144})$ în $(\mathbb{Z}_{1000}, +)$; $\text{ord}(\widehat{33})$ în $(\mathbb{Z}_{311}, +)$
 $\text{ord}(\widehat{75})$ în $(\mathbb{Z}_{500}, +)$.

Exc 4 Det. elem. de ordin 8 din $(\mathbb{Z}_6 \times \mathbb{Z}_{10}, +)$, elementele de ordin 4 din $(\mathbb{Z}_{12} \times \mathbb{Z}_{15}, +)$ și elementele de ordin 6 din $(\mathbb{Z}_{12} \times \mathbb{Z}_{36}, +)$

Fie $(m, k) = d \Rightarrow m = dm_1, k = dk_1, (m_1, k_1) = 1$.

Vrem să arătăm $\text{ord}(x^k) = \frac{m}{d} = m_1$.

$$\bullet (x^k)^{m_1} = x^{km_1} = x^{dkm_1} = (x^{dm_1})^{k_1} = (x^m)^{k_1} = (1_G)^{k_1} = 1_G$$

• A mai rămas de arătat că m_1 este cel mai mic nr. natural menajat

$$\text{a.i. } (x^k)^{m_1} = 1_G.$$

P.p. primă reducere la absurd că (\exists) $0 < t < m_1$ a.i. $(x^k)^t = 1_G \Rightarrow$

$$\Rightarrow x^{kt} = 1_G \xrightarrow[\text{ord}(x)]{\text{Exc 1}} m \mid kt \Rightarrow k \cdot t = m \cdot a \quad a \in \mathbb{Z}$$

$$\Rightarrow m_1 \mid k_1 t \quad | \quad \begin{array}{l} m_1 \mid t \Rightarrow m_1 \leq t \\ (m_1, k_1) = 1 \end{array} \quad \begin{array}{l} m_1 \leq t \\ 0 < t < m_1 \end{array} \quad \cancel{\Rightarrow} \quad \Rightarrow \text{pp. e falsă} \Rightarrow$$

$$\Rightarrow \text{ord}(x^k) = m_1 \left(= \frac{m}{(m, k)} \right)$$

$$\boxed{\text{Exc 3}} \quad (\mathbb{Z}_{m_1}, +) = \langle \overline{1} \rangle \quad \text{ord}(\overline{1}) = m_1 \quad \text{ord}(\overline{k}) = \frac{m}{(m, k)} \quad \overline{k} = \overbrace{\overline{1} + \overline{1} + \dots + \overline{1}}_{k \text{ ori}}$$

$$\text{în } (\mathbb{Z}_{1000}, +) \quad \text{ord}(\overline{144}) = \frac{1000}{(1000, 144)} = \frac{1000}{2^3} = 125$$

$$\text{în } (\mathbb{Z}_{311}, +) \quad \text{ord}(\overline{33}) = \frac{311}{(33, 311)} = \frac{311}{1} = 311$$

$$\boxed{\text{Exc 3.1}} \quad \text{Fie } U_{36} = \{ z \in \mathbb{C} \mid z^{36} = 1 \} \quad ((U_{36}, \cdot)) \cong (\mathbb{Z}_{36}, +)$$

$$U_{36} = \left\{ \cos \frac{2k\pi i}{36} + i \sin \frac{2k\pi i}{36} \mid k = 0, \dots, 35 \right\} = \left\{ \overline{1}, \overline{x_1}, \overline{x_1^2}, \dots, \overline{x_1^{35}} \right\},$$

$$\underbrace{\overline{z^m} = 1}_{\overline{z_1^m} = 1} \Rightarrow \overline{z_k} = \cos \frac{2k\pi i}{m} + i \sin \frac{2k\pi i}{m} \quad k \in \{0, 1, \dots, m-1\}$$

Moivne: $\overline{z_1^k} = \left(\cos \frac{2\pi i}{m} + i \sin \frac{2\pi i}{m} \right)^k = \left(\cos \frac{2k\pi i}{m} + i \sin \frac{2k\pi i}{m} \right) = \overline{z_k}$

$$\text{unde } \overline{x_1} = \cos \frac{2\pi i}{36} + i \sin \frac{2\pi i}{36}.$$

$$U_{36} = \langle \overline{x_1} \rangle$$

Calculați $\text{ord}(\cos \frac{2 \cdot 18\pi i}{36} + i \sin \frac{2 \cdot 18\pi i}{36})$ în (U_{36}, \cdot) !

$$\text{ord}(\overline{x_1^{18}}) \xrightarrow[\text{Exc 2}]{=} \frac{\text{ord } \overline{x_1}}{(\text{ord } \overline{x_1}, 18)} = \frac{36}{(36, 18)} = \frac{36}{18} = 2$$

sau: $\overline{x_1^{18}} = \cos \pi + i \sin \pi = -1$
 $\text{ord}(-1) = 2$

$$(\mathbb{Z}_m, +) \quad \text{ord}(\overline{k}) = \frac{m}{(m, k)}$$

$$\text{ord}(\overline{k}) = m \Leftrightarrow (m, k) = 1$$

Efectuarea de ordinul m dim $(\mathbb{Z}_m, +)$ (sau generatorii lui $(\mathbb{Z}_m, +)$)

sunt $\{ \overline{k} \mid (k, m) = 1 \}$.

Ex 3.2 $\cup(\mathbb{Z}_m, \cdot) \rightarrow$ grup cu $\varphi(m)$ elemente.

$$\cup(\mathbb{Z}_{31}, \cdot) = \mathbb{Z}_{31} \setminus \{0\} \quad (\varphi(31) = 31 - 1 = 30) \quad \text{Calculati } \overbrace{\mathbb{Z}_{31}}^{2020 \text{ im}}.$$

Euler $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$

$$2020^{2020} \equiv 5^{2020} \pmod{31} \equiv 5^{30 \cdot 67 + 10} \pmod{31}$$

$$\equiv (5^{30})^{67} \cdot 5^{10} \pmod{31} \equiv 5^{10} \pmod{31} \equiv 25^5 \pmod{31} \equiv -6^5 \pmod{31} \equiv \frac{2020}{10} \pmod{31}$$
$$\equiv -36^2 \cdot 6 \pmod{31} \equiv -5^2 \cdot 6 \pmod{31} \equiv -25 \cdot 6 \pmod{31} \equiv 6^2 \pmod{31} \equiv 5 \pmod{31}.$$

$\text{ord}(\hat{\zeta}^{2020})$ in $\cup(\mathbb{Z}_{31}, \cdot)$?

Ex 2 //

$$\frac{\text{ord}(\hat{\zeta})}{(\text{ord}(\hat{\zeta}), \text{ord}(\hat{\zeta}^2))} = \frac{3}{(2020, 3)} = \frac{3}{1} = 3$$

$$\text{ord}(\hat{\zeta}^{2020}) = \text{ord}(\hat{\zeta})$$

Vrem $\text{ord}(\hat{\zeta})$ (folosesc definitia, stim ca $\text{ord}(\hat{\zeta})$ in $\mathbb{Z}_{31}, \text{ord}(\hat{\zeta}) | 30$)

$$\hat{\zeta}^2 = \hat{\zeta}^5 \quad \hat{\zeta}^3 = \hat{\zeta}^{125} = \hat{\zeta} \quad \text{in } \mathbb{Z}_{31} \Rightarrow \boxed{\text{ord}(\hat{\zeta}) = 3}$$

Ex 3 Fie G_1, G_2 grupuri, $x \in G_1, y \in G_2$ a.s. $\text{ord}(x) = n < \infty$ si $\text{ord}(y) = m < \infty$. Atunci $\text{ord}((x,y)) = [n,m]$, unde $(x,y) \in G_1 \times G_2$.

grupul produs direct

Ex 4 e aplicatie directa la \uparrow si Ex 2.

Dem Fie $[n,m] = t \rightsquigarrow t \cdot d = n \cdot m \quad d = (n,m) \quad n = d \cdot n_1 \quad (n_1, m_1) = 1$

$$(x,y)^t = (x^t, y^t) = (x^{dm_1}, y^{dm_1}) =$$

$$= ((x^n)^{m_1}, (y^m)^{n_1}) = (1_{G_1}, 1_{G_2})$$

Fie $k \in \mathbb{N}^*$ a.s. $(x,y)^k = (1_{G_1}, 1_{G_2}) \Rightarrow \begin{cases} x^k = 1_{G_1} \xrightarrow{\text{Ex 1}} n | k \\ y^k = 1_{G_2} \xrightarrow{\text{Ex 1}} m | k \end{cases} \Rightarrow [n,m] | k$

$\xrightarrow{k \neq 0} t \leq k \Rightarrow t = \text{ord}((x,y))$.



Seminar, 11 - 13.12.2021

Ex. 1 : Tie grupul (S_4, \circ) , $H = \{e, (12)(34), (13)(24), (14)(23)\}$ subgrup im S_4 .

- Anătăti că H este subgrup normal im S_4 ($H \trianglelefteq S_4$)
- Astați că $S_4/H \cong S_3$.

Rez:

$$a. H \trianglelefteq S_4 \iff xH = Hx, \forall x \in G = S_4.$$

$$xHx^{-1} \subseteq H, \forall x \in G = S_4.$$

$$|S_4| = 4! = 24$$

Vor. 1 : Calcul

Vor. 2 : Verifică pe o multime de generatoare.

De ex., orice permutare poate fi scrisă ca produs de transpozitii, $\tau = z_1 z_2 \dots z_k$, z_i : transpozitie.

$\boxed{zH z^{-1} = H, \forall z \text{ transpozitie}}$

$$(z_1 z_2)H(z_1 z_2)^{-1} = z_1(z_2 H z_2^{-1})z_1^{-1} = z_1 H z_1^{-1} = H.$$

$$H = \{e, (12)(34), (13)(24), (14)(23)\}$$

Cate transpozitii sunt in S_4 ? - $C_4^2 = 6$.

Vor. 3: Tie $\sigma \in S_4$.

$$\sigma H \sigma^{-1} = H$$

$$\sigma (12)(34) \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \end{pmatrix}^{-1}$$

$$\begin{array}{ll} \sigma(1) \rightarrow 1 \rightarrow 2 \rightarrow \sigma(2) & \sigma(3) \rightarrow 3 \rightarrow 4 \rightarrow \sigma(4) \\ \sigma(2) \rightarrow 2 \rightarrow 1 \rightarrow \sigma(1) & \sigma(4) \rightarrow 4 \rightarrow 3 \rightarrow \sigma(3) \end{array}$$

$$(\sigma(1) \sigma(2))(\sigma(3) \sigma(4)) \in H$$

$$\sigma(13)(24) \sigma^{-1} = (\sigma(1) \sigma(3)) (\sigma(2) \sigma(4)) \in H$$

$$\sigma(14)(23) \sigma^{-1} = (\sigma(1) \sigma(4)) (\sigma(2) \sigma(3)) \in H$$

b. S_4/H , Th. Lagrange : $|G| = |H| \cdot |G:H|$
 L'indicele lui H în G .

$$|S_4|_H = \frac{|S_4|}{|H|} = \frac{24}{4} = 6.$$

! G grup cu 6 elemente $\Rightarrow G \cong \mathbb{Z}_6$ sau $G \cong S_3$

$$|S_4/H| = 6 \Rightarrow S_4/H \cong \mathbb{Z}_6 \quad S_4/H \cong S_3.$$

\forall grup ciclic, are elem. de ord. 6, commutativ

$S_4/H \cong \mathbb{Z}_6 \Rightarrow S_4/H$ are un elem. de ordim 6.

$\hat{\tau} \in S_4/H$, $\tau \in S_4$, $\tau^6 \in H$, 6 este minim.

$$\begin{aligned} S_4 = & \{e\} \cup \{(i j) \mid 1 \leq i < j \leq 4\} \cup \{(i j k) \mid 1 \leq i, j, k \leq 4\} \cup \\ & \text{6 transpozitii} \quad "A_3" \quad i \neq j \neq k \neq i \\ & \cup \{(i j)(k l) \mid \{i, j, k, l\} = \{1, 2, 3, 4\}\} \cup \frac{A_4}{3} = 8 \\ & \cup \{(i j k l) \mid \{i, j, k, l\} = \{1, 2, 3, 4\}\} \end{aligned}$$

! În S_4 nu există elem. de ordim 6.

Se obs. că în S_4/H nu există elem. de ord. 6 $\Rightarrow S_4/H \cong S_3$

Permutări

Ex. 1: Fie $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 1 & 2 & 9 & 7 & 8 & 3 & 6 & 10 & 4 \end{pmatrix} \in S_{10}$.

- Descompunem τ în produs de cicli disjuncti și în produs de transpozitii.
- Dăt. $\text{sgn}(\tau)$, ord(τ) să calculăm τ^{2021} .
- Rezolvă ecuația $\tau^2 \cdot \tau$ în S_{10} .
- Fie $g \in S_{10}$ cu $\text{ord}(g) = 10$. Este posibil ca $\text{sgn}(g) = 1$?
- Există permutări de ordin 30 în S_{10} ? De ordin 35?

Rez: a. $\tau = (1 \ 5 \ 7 \ 3 \ 2)(4 \ 9 \ 10)(6 \ 8)$
 $\tau = \underline{(1 \ 5)} \underline{(5 \ 7)} \underline{(7 \ 3)} \underline{(3 \ 2)} (4 \ 9) (9 \ 10) (6 \ 8)$.

$$1 \rightarrow 5 \rightarrow 7 \rightarrow 3 \rightarrow 2 \rightarrow 1$$

b. $\text{sgn}(\tau) = (-1)^{\text{nr. de transp.}} = (-1)^7 = -1$
 $= (-1)^{\text{nr. de inversions}}$

$$\text{Obs: } \text{sgm}(\tau\circ\sigma) = \text{sgm}(\tau) \cdot \text{sgm}(\sigma)$$

$$\tau = \underbrace{(1 \ 5 \ 7 \ 3 \ 2)}_{5\text{-ciclu}} \underbrace{(4 \ 9 \ 10)}_{3\text{-ciclu}} \underbrace{(6 \ 8)}_{2\text{-ciclu / transpozitie}}$$

$\forall \sigma \in S_m$, σ ciclu de lungime m

$$\text{sgm}(\sigma) = \begin{cases} -1 & m \text{ par} \\ 1 & m \text{ impar} \end{cases}$$

$$\text{ord}(\tau) = k \quad (\Rightarrow \tau^k = e \text{ si } k \text{ este minim.})$$

! $\tau = z_1 z_2 \dots z_k$ produs de cicli disjuncti

$$\text{ord}(\tau) = [\text{ord}(z_1), \text{ord}(z_2), \dots, \text{ord}(z_k)].$$

c ciclu de lungime m , $\text{ord}(c) = m$

$$\text{ord}(\tau) = [5, 3, 2] = 30 \quad \Rightarrow \quad \tau^{30} = e$$

$$\tau^{2021} = \tau^{30 \cdot 67 + 11} = \tau^{30 \cdot 67 + 11} = \tau^{11}$$

$$\Gamma = (1 \ 5 \ 7 \ 3 \ 2)(4 \ 9 \ 10)(6 \ 8)$$

$$\Gamma^2 = (1 \ 7 \ 2 \ 5 \ 3)(4 \ 10 \ 9), \quad \Gamma^3 = \dots$$

$$\Gamma^4 = \dots, \quad \Gamma^8 = \dots$$

$$\Gamma^{11} = \left((1 \ 5 \ 7 \ 3 \ 2)(4 \ 9 \ 10)(6 \ 8) \right)^{11} \stackrel{\text{ab} \cdot \text{ba}}{=} \textcircled{V}$$

$$= (1 \ 5 \ 7 \ 3 \ 2)^{11} \cdot (4 \ 9 \ 10)^{11} (6 \ 8)^{11}$$

$$= (1 \ 5 \ 7 \ 3 \ 2)(4 \ 10 \ 9)(6 \ 8)$$

$$(1 \ 5 \ 7 \ 3 \ 2)^{11} = (1 \ 5 \ 7 \ 3 \ 2)^{5 \cdot 2 + 1} = (1 \ 5 \ 7 \ 3 \ 2)$$

$$\begin{cases} C = (a_1 \ a_2 \ \dots \ a_k), \quad C^{-1} = (a_1 \ a_k \ a_{k-1} \ \dots \ a_2) \\ C^i \cdot a_j = a_{j+i}, \quad j+i \bmod k. \end{cases}$$

Obs: $(4 \ 9 \ 10)^2 = (4 \ 9 \ 10)^{-1}$ deoarece
 $\text{ord}(4 \ 9 \ 10) = 3.$

$$c. \quad \overline{z}^2 = \nabla$$

$$\operatorname{sgn}(\nabla) = -1$$

$$\operatorname{sgn}(z^2) = \operatorname{sgn}(z) \cdot \operatorname{sgn}(z) = 1.$$

! $z^\infty = \nabla$ Mai întâi verifică dacă $\operatorname{sgn}(\nabla) = 1$.

\Rightarrow ecuația nu are soluții,

$$d. \quad g \in S_{10}, \quad \operatorname{ord}(g) = 10.$$

$g = z_1 z_2 \dots z_K$ produs de cicl disjuncti

$$\operatorname{ord}(g) = 10 \quad \leftarrow \quad g = \text{ciclu de lungime } 10 \rightarrow \operatorname{sgn}(g) = -1$$

$$g = (i \ j) (\kappa \ l \ m \ n) \rightarrow \operatorname{sgn}(g) = (-1) \cdot 1$$

$$g = \begin{matrix} (1 \ 2) \\ 2 \end{matrix} \begin{matrix} (3 \ 4) \\ 2 \end{matrix} \begin{matrix} (5 \ 6 \ 7 \ 8 \ 9) \\ 5 \end{matrix} \stackrel{10}{\rightarrow} \operatorname{sgn}(g) = 1.$$

e. Permutări de ordin 30 - există

$$\operatorname{ord}(g) = 30, \quad g = z_1 z_2 \dots z_K \text{ deoc. în cicl disj.}$$

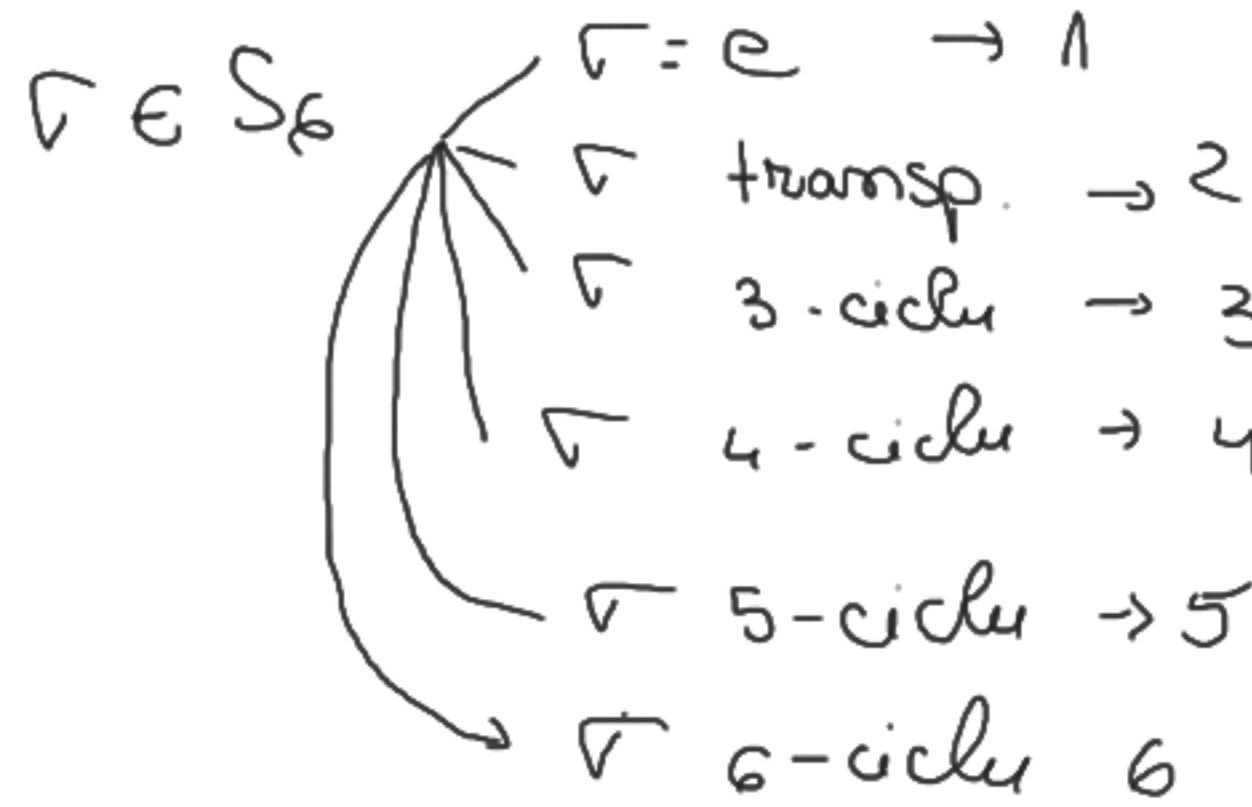
$$e_i = \operatorname{ord}(z_i)^{3^2}, \quad [l_1, l_2, \dots, l_K] = 30, \quad l_1 + l_2 + \dots + l_K \leq 10.$$

$$[l_1, l_2, \dots, l_k] = 35 = \underline{\underline{5 \cdot 7}}$$

Nu există permutări de ord. 35 în S_{10} .

Cel mai mic m a.s. există permutări de ordin m în S_m este $5 \cdot 7 = 12$.

Ex. 2: Def. toate ordimile posibile ale unei permutări
din S_6 .



$\text{ord}(\Gamma) \in \{1, 2, 3, 4, 5, 6\}$

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

$$\Gamma = (i \ j) (\kappa \ \ell) \rightarrow 2$$

$$\Gamma = (i \ j) (\kappa \ \ell) (m \ m) \rightarrow 2$$

$$\Gamma = (i \ j) (\kappa \ \ell \ m) \rightarrow 6$$

$$\Gamma = (i \ j) (\kappa \ \ell \ m \ m) \rightarrow 4$$

$$\Gamma = (i \ j \ k) (\ell \ m \ m) \rightarrow 3$$

Seminar 12

3.01.2022

Prob. 1

$$\text{Fie } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 7 & 2 & 3 & 1 & 8 & 5 & 6 \end{pmatrix} \in S_9 \quad (\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 6 & 9 & 1 & 2 & 4 & 7 & 10 & 8 \end{pmatrix} \in S_{10})$$

- 1) Descompuneti σ în produs de cicli disjuncti și în produs de transpozitii.
- 2) Aflati $\text{sgn}(\sigma)$ și calculati σ^{2022} , $\text{ord}(\sigma)$.
- 3) Det. toate permutările din S_9 (resp S_{10}) așa că $\sigma^3 = \tau$ (resp $\tau^3 = \sigma_1$).
- 4) Fie $\rho \in S_9$ cu $\text{ord}(\rho) = 9$. Poate fi ρ permutare pară?

(Același ecart, pt σ_1).

$$1) \quad \sigma = (1 \ 4 \ 2 \ 9 \ 6)(3 \ 7 \ 8 \ 5)$$

$$\sigma_1 = (1 \ 3 \ 6 \ 2 \ 5)(4 \ 9 \ 10 \ 8 \ 7)$$

$$\sigma = (1\ 4\ 1)(4\ 2\ 1)(2\ 9\ 1)(9\ 6\ 1)(3\ 7\ 1)(7\ 8\ 1)(8\ 5\ 1)$$

$$\sigma_1 = (1\ 3\ 1)(3\ 5\ 1)(5\ 2\ 1)(2\ 5\ 1)(4\ 9\ 1)(9\ 10\ 1)(10\ 8\ 1)(8\ 7\ 1)$$

Reamintim că $\text{sgn}: S_m \rightarrow \{-1, 1\}$ este morfism de grupuri și $\text{sgn}((i\ j)) = -1$
(veri C11)

$$\text{sgn}(\sigma) = (-1)^7 = -1$$

$$\text{sgn}(\sigma_1) = (-1)^8 = 1$$

Reamintim că $\text{ord}(\sigma) = \text{c.m.m.m.c.} (5, 4) = 20$ al lungimilor cicilor din descomp. în produs de cicli disjuncti a lui σ

$$\text{ord}(\sigma) = \text{c.m.m.m.c.} (5, 4) = 20$$

$$\text{ord}(\sigma_1) = [5, 5] = 5$$

$$\sigma^{2022} = \sigma^{20 \cdot 101 + 2} = (\sigma^{20})^{101} \cdot \sigma^2 = \sigma^2 =$$

$$\sigma_1 = (1 \ 3 \ 6 \ 2 \ 5)(4 \ 9 \ 10 \ 8 \ 7)$$

$$= (1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9)(1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9) = (1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9) =$$

$$= (1 \ 2 \ 6 \ 4 \ 9)(3 \ 8)(5 \ 7)$$

$$\sigma = (1 \ 4 \ 2 \ 9 \ 6)(3 \ 7 \ 8 \ 5) \Rightarrow \sigma^2 = (1 \ 4 \ 2 \ 9 \ 6)^2 (3 \ 7 \ 8 \ 5)^2 \stackrel{\text{veri}}{\underset{\substack{\text{cicli disj.} \\ \text{comute}}}{{\sim}}} \underset{\substack{\text{mai} \\ \text{jos}}}{}$$

$$(1 \ 2 \ 6 \ 4 \ 9)(3 \ 8)(5 \ 7)$$

$$\sigma_1^{2022} = \sigma_1^{5 \cdot 404 + 2} = (\sigma_1^5)^{404} \cdot \sigma_1^2 = \sigma_1^2 = (1 \ 6 \ 5 \ 3 \ 2)(4 \ 10 \ 7 \ 9 \ 8)$$

$$4) \quad \rho \text{ permutare pară} \quad (c \Rightarrow \text{sgn}(\rho) (\text{sau } \varepsilon(\rho)) = 1)$$

$$\rho \in S_9 \quad \boxed{\text{ord}(\rho) = 9}$$

(mai puțin ordinea)
sorieri cicilor

Reamintim: orice permutare se descompune în mod unic în produs de cicli disjuncti

$\rho \in S_9 \rightsquigarrow \rho = c_{i_1} \cdot c_{i_2} \cdot \dots \cdot c_{i_k} \rightarrow$ desc. im produs de cicli disj.

unde $i_1 + i_2 + \dots + i_k = 9$, dacă scriem și cicli de lungime 1, (resp. $i_1 + \dots + i_k \leq 9$ dacă nu scriem cicli de lungime 1) unde c_{i_j} este ciclu de lungime i_j .

$$\text{ord}(\rho) = \text{c.m.m.c.}(i_1, i_2, \dots, i_k) \Rightarrow (\exists) j \text{ a.i. } i_j = 9 \Rightarrow$$

$$i_1 + i_2 + \dots + i_k = 9$$

$$\Rightarrow \boxed{k=1} \text{ și } \boxed{i_1=9} \Rightarrow \rho \text{ este ciclu de lungime 9.} \Rightarrow \text{sgn}(\rho) = (-1)^{\frac{9-1}{1}}$$

$\Rightarrow \rho$ e permutare pară.

$$3) \quad z^3 = (1 \ 4 \ 2 \ 9 \ 6)(3 \ 7 \ 8 \ 5) = \tau$$

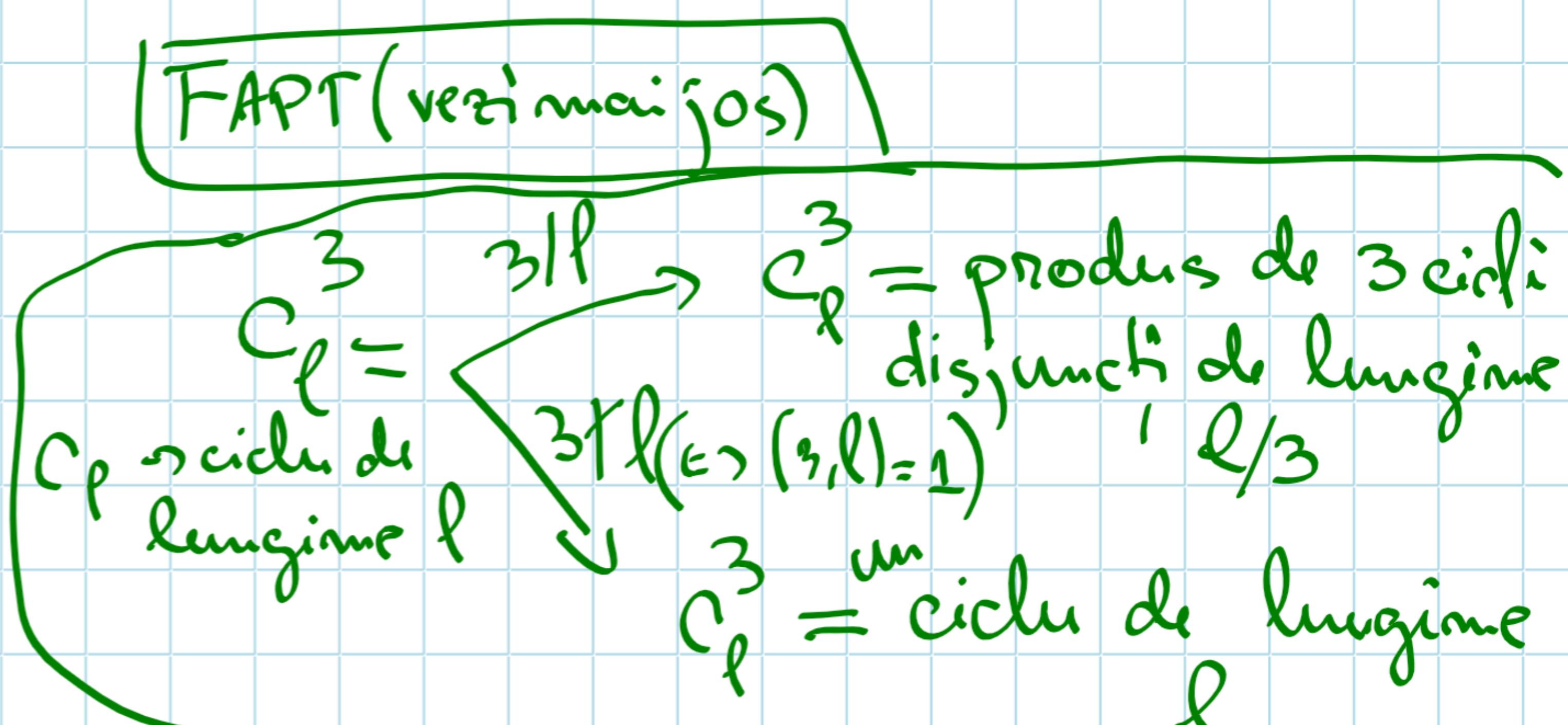
Pp. că $(\exists) z \in S_9$ a.i. $z^3 = \tau$. Fie $z = c_{i_1} \cdot c_{i_2} \cdot \dots \cdot c_{i_k} \rightarrow$ desc. lungimile sunt produs de cicli disjuncti;

$i_1 + \dots + i_k = 9 \quad 1 \leq k \leq 3 \quad (k=9)$

c_{i_j} - ciclu de lungime i_j . $\sum_{i=1}^k i_j = 9$

$$z^3 = \frac{\text{cidi}}{\text{disj.}} c_{i_1}^3 \cdot c_{i_2}^3 \cdot \dots \cdot c_{i_k}^3$$

comută



$$z^3 = \tau = (1 \ 4 \ 2 \ 9 \ 6)(3 \ 7 \ 8 \ 5) \implies$$

$$c_{i_1}^3 \cdot c_{i_2}^3 \cdot \dots \cdot c_{i_k}^3$$

unicitatea
desc.
im produs
de cicli
disjuncti

$3!i_j \cdot (4) \cdot j^{-1,k}$
(altfel $c_{i_j}^3 =$
produs de 3
cicli disj. de
lungime $i_j/3$)

Prin urmare $c_{i_j}^3$ e un ciclu de lungime i_j ($\forall j = 1, k$)

$\implies k=2$ și pot apărea ca $i_1=5$ și $i_2=4$. Deci $z = c_5 \cdot c_4$,

$$\begin{aligned} \zeta^3 &= C_5^3 \cdot C_4^3 \quad \text{cu} \quad C_5^3 = (1 \ 4 \ 2 \ 9 \ 6) \Rightarrow (C_5^3)^2 = (1 \ 4 \ 2 \ 9 \ 6)^2 \\ &\qquad\qquad\qquad C_5^3 = (3 \ 7 \ 8 \ 5) \\ &\qquad\qquad\qquad \Downarrow \\ &\qquad\qquad\qquad (C_4^3)^3 = (3 \ 7 \ 8 \ 5)^3 = (3 \ 5 \ 8 \ 7) \\ &\qquad\qquad\qquad C_4^3 = C_4^8 \cdot C_4 = C_4 \quad \boxed{C_4 = (3 \ 5 \ 8 \ 7)} \\ \Rightarrow \zeta &= (1 \ 2 \ 6 \ 4 \ 9)(3 \ 5 \ 8 \ 7) \quad (\text{Deci ec. } \zeta^3 = \sigma \text{ are sol. unica}) \end{aligned}$$

$$\zeta^3 = \sigma_1 = (1 \ 3 \ 6 \ 2 \ 5)(4 \ 9 \ 10 \ 8 \ 7)$$

Similat $\zeta = C_{i_1} \cdot C_{i_2} \cdots C_{i_k} \rightarrow$ descomp. produs de cicli disj.

$$\begin{aligned} \zeta^3 &= C_{i_1}^3 \cdot C_{i_2}^3 \cdots C_{i_k}^3 = (1 \ 3 \ 6 \ 2 \ 5)(4 \ 9 \ 10 \ 8 \ 7) . \text{ Analog} \\ \text{se arata } \boxed{pk=2} \quad i_1 &= i_2 = 5 \quad C_{i_1}^3 = (1 \ 3 \ 6 \ 2 \ 5) \Rightarrow C_{i_1} = (1 \ 6 \ 5 \ 3 \ 2) \\ &C_{i_2}^3 = (4 \ 9 \ 10 \ 8 \ 7) \Rightarrow C_{i_2} = (4 \ 10 \ 7 \ 9 \ 8) \end{aligned}$$

Ec $\zeta^3 = \sigma_1$ are sol. unica in S_{10} pe $\zeta = (1 \ 6 \ 5 \ 3 \ 2)(4 \ 10 \ 7 \ 9 \ 8)$.

Prb2 Dacă $\sigma = (a_1 \ a_2 \ \dots \ a_m) \in S_m$ este un m-ciclu atunci

(*) $i \in \{1, 2, \dots, m\}$ $\sigma^i(a_k) = a_{k+i}$, unde $k+i$ este înlocuit de restul $k+i \pmod m$ dacă $k+i > m$.

Denum Înd. după i cazul $i=2$ $\sigma^2(a_1) = \sigma(\sigma(a_1)) = \sigma(a_2) = a_3$

$\sigma = (a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow \dots \rightarrow a_m \rightarrow a_1)$ notatie $\sigma^2 = \begin{pmatrix} & \vdots \\ a_1 \dots a_2 \dots a_3 \dots a_m \dots a_m \\ a_3 \dots a_4 \dots a_5 \dots \sim a_1 \dots a_2 \end{pmatrix}$

Obs 1) Dacă σ e un m-ciclu atunci σ^i nu e neapărat un m-ciclu. Exemplu: $\sigma = (1 \ 2 \ 3 \ 4) \in S_4$ $\sigma^2 = \begin{pmatrix} 1 \rightarrow 3 \\ 2 \rightarrow 4 \\ 3 \rightarrow 1 \\ 4 \rightarrow 2 \end{pmatrix} = (1 \ 3)(2 \ 4)$

2) $\sigma^m = e$

Prb3 Fie σ un m-ciclu. Atunci σ^i este un m-ciclu ($\Leftrightarrow (i, m) = 1$).

Prb4 Fie σ un m-ciclu și $d|m$. Atunci σ^d este un produs de d cicli disjuncti de lungime $\frac{m}{d}$.

Pb 5 Nr. cicilor de lungime m din S_m ($m \leq n$) este egal cu

$$\frac{A_m^m}{m} = \frac{n(n-1) \cdots (n-m+1)}{m}$$

$$((i_1 i_2 \dots i_m) \sim (i_2 i_3 \dots i_m i_1) = \dots = (i_m i_1 \dots i_{m-1}))$$

Pb 6 Calculati nr. de permutari din S_4 , respectiv S_5 , care se scriu ca produs de 2-cicli disjuncti (\Leftrightarrow permutarile de ordin 2)

Obs! 2-ciclu = produs (cu un singur factor)

(*) $\sigma \in S_4 \rightsquigarrow$ produs de un 2-ciclu $\Rightarrow \sigma \in$ transp. $\rightsquigarrow (12), (13), (14)$
 $(23), (24), (34)$
 $\text{In total } \frac{A_4^2}{2} = \frac{4 \cdot 3}{2} = 6 \text{ permutari}$

\downarrow produs de 2 2-cicli disjuncti $\Rightarrow (12)(34), (13)(24), (14)(23)$
 $\text{In total } 3 \text{ permutari}$

Im S_4 avem 9 astfel de permutari (de ordin 2).

(**) $\sigma \in S_5 \rightsquigarrow \sigma = (i j) \text{ and Avem } C_5^2 (= \frac{A_5^2}{2}) \text{ transpozitii in } S_5.$

$\downarrow \sigma = (i j)(k l) \text{ cu } \{i, j\} \cap \{k, l\} = \emptyset$

$\downarrow \frac{C_5^2 \cdot C_3^2}{2} = \frac{10 \cdot 3}{2} = 15 \text{ permutari care se scriu ca produs de 2 2-cicli disjuncti.}$

Deci im S_5 avem $10 + 15 = 25$ permutari de ordin 2.

Pb 7 Determinati n a.s. există $\sigma \in S_7$ cu $\text{ord}(\sigma) = n$.

$\sigma = c_{i_1} \cdot c_{i_2} \cdots c_{i_k} \rightarrow$ disc. im produs de cicli disj.

 $\text{ord}(\sigma) = [i_1, \dots, i_k]$
 $i_1, \dots, i_k \leq 7$

Dacă σ = k - ciclu $k = \sqrt{7} \Rightarrow \text{ord}(\sigma) = k$

$8 = 2^3 = [i_1, \dots, i_k] \Rightarrow (\exists) i_j : i_j = 8 \quad (x, i_j \leq 7) \Rightarrow \nexists \sigma \in S_7 \text{ ord}(\sigma) = 8$

$9 = 3^2 = [i_1, \dots, i_k] \Rightarrow (\exists) i_j : i_j = 9 \quad (x, i_j \leq 7) \Rightarrow \nexists \sigma \in S_7 \text{ ord}(\sigma) = 9$

Evident $\text{ord}(\sigma) \neq p$ (A) p - prim $p > 7$.

$\sigma = (12)(34567) \Rightarrow \text{ord}(\sigma) = 10 ; \quad \sigma = (123)(4567) \Rightarrow \text{ord}(\sigma) = 12$

Afinitate

Multimea ordinelor elem. dim S_7 este {1, 2, 3, 4, 5, 6, 7, 10, 12}

" \geq " (vezi mai sus)

$$|S_7| = 7! \quad \sigma \in S_7 \xrightarrow{\text{Lagrange}} \text{ord}(\sigma) \mid 7! = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7$$

$$\boxed{\text{ord}(e) = 1}$$

$S_7 \ni \sigma = c_{i_1} \dots c_{i_k}$ desc. în produs de cicluri disjuncte c_{i_j} e ciclul lung $i_j > 1$

$$\Rightarrow i_1 + i_2 + \dots + i_k \leq 7$$

$$\begin{matrix} 1 \leq i_1, i_2, \dots, i_k \\ i_1 \leq i_2 \leq \dots \leq i_k \end{matrix} \Rightarrow 2k \leq i_1 + i_2 + \dots + i_k \quad | \approx \boxed{2k \leq 7} \Rightarrow k \leq 3$$

Avem 3 cazuri:

(I) $k=1$ $\Rightarrow \sigma = c_{i_1} \Rightarrow \sigma$ e un i_1 -ciclu ($i_1 \leq 7$) $\Rightarrow \text{ord}(\sigma) = i_1 \in \{2, \dots, 7\}$

(II) $k=2$ $\Rightarrow \text{ord}(\sigma) = [i_1, i_2] \quad i_1 + i_2 \leq 7 \quad 2 \leq i_1 \leq i_2$

$$\hookrightarrow (i_1, i_2) \in \{(2, 2), (2, 3), (2, 4), (2, 5), (3, 3), (3, 4)\} \rightsquigarrow$$

$$\rightsquigarrow \text{ord}(\sigma) \in \{2, 6, 4, 10, 3, 12\} = \{2, 3, 4, 6, 10, 12\}$$

(III) $k=3$ $\Rightarrow \text{ord}(\sigma) = [i_1, i_2, i_3] \quad i_1 + i_2 + i_3 \leq 7 \quad 2 \leq i_1 \leq i_2 \leq i_3$

$$\hookrightarrow (i_1, i_2, i_3) \in \{(2, 2, 2), (2, 2, 3)\} \Rightarrow \text{ord}(\sigma) \in \{2, 6\}$$

Din (I), (II) și (III) \Rightarrow " \subseteq " (Afinitatea este demonstrată.)

Seminar 13

10.01.2022

$$\boxed{\text{Exe 1}} \quad a\mathbb{Z} + b\mathbb{Z} = (a,b)\mathbb{Z}$$

$$a\mathbb{Z} \cap b\mathbb{Z} = [a,b]\mathbb{Z}$$

$$(a,b) = \text{c.m.m. d.c}(a,b)$$

$$[a,b] = \text{c.m.m.m.c}(a,b)$$

$$\text{Fie } d = (a,b) ; m = [a,b]$$

$$d = (a,b) \rightsquigarrow \begin{cases} a = da_1 \\ b = db_1 \end{cases} \quad (a_1, b_1) = 1 \rightsquigarrow [a,b] = dab_1$$

$$\text{Vrem } a\mathbb{Z} + b\mathbb{Z} \stackrel{?}{=} d\mathbb{Z}$$

$$\stackrel{"\leq"}{\text{?}} \quad \text{Fie } x \in a\mathbb{Z} + b\mathbb{Z} \Rightarrow x = y + z, y \in a\mathbb{Z}, z \in b\mathbb{Z}$$

$$y = ak, z = bl, k, l \in \mathbb{Z}$$

$$x = y + z = ak + bl = da_1k + db_1l = d(a_1k + b_1l) \in d\mathbb{Z}$$

$$\stackrel{"\geq"}{\text{?}} \quad \text{Alg. Euclid} \xrightarrow{(a,b)=d} d = m \cdot a + n \cdot b, \text{ pt } m, n \in \mathbb{Z}$$

$$\text{Fie } t \in d\mathbb{Z} \Rightarrow t = d \cdot u, u \in \mathbb{Z}$$

$$(m \cdot a + n \cdot b) \cdot u = a \cdot mu + b \cdot nu \in a\mathbb{Z} + b\mathbb{Z}.$$

$$a\mathbb{Z} \cap b\mathbb{Z} \stackrel{?}{=} m\mathbb{Z}$$

$$m = [a,b] ; m = da_1b_1 = ab_1 = ba_1$$

$$\stackrel{"\leq"}{\text{?}} \quad \text{Fie } x \in a\mathbb{Z} \cap b\mathbb{Z} \Rightarrow x \in a\mathbb{Z} \Rightarrow a|x \quad | \quad \Rightarrow [a,b]|x \Rightarrow m|x$$

$$x \in b\mathbb{Z} \Rightarrow b|x$$

$$\Downarrow \\ x \in m\mathbb{Z} \Rightarrow$$

$$\Rightarrow a\mathbb{Z} \cap b\mathbb{Z} \subseteq m\mathbb{Z}$$

$$\stackrel{"\geq"}{\text{?}} \quad \text{Fie } y \in m\mathbb{Z} \Rightarrow y = m \cdot k = a \cdot (b_1k) \in a\mathbb{Z} \quad | \quad \Rightarrow y \in a\mathbb{Z} \cap b\mathbb{Z} \Rightarrow$$

$$y = b \cdot (a_1k) \notin b\mathbb{Z}$$

$$\Rightarrow m\mathbb{Z} \subseteq a\mathbb{Z} \cap b\mathbb{Z}.$$

Aplicatie Calculati idealele 1) $(10\mathbb{Z} + 16\mathbb{Z}) \cap (18\mathbb{Z} + 3\mathbb{Z} \cap 15\mathbb{Z})$

$$2) \quad 20\mathbb{Z} + (15\mathbb{Z} \cap 60\mathbb{Z}) = 20\mathbb{Z} + 180\mathbb{Z} = 20\mathbb{Z}$$

$$2\mathbb{Z} \cap (18\mathbb{Z} + 15\mathbb{Z})$$

$$2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$$

Exe 2 Să se arate că $R = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \text{ impar} \right\}$ este un inel în raport

cu operațiile uzuale de adunare și înmulțire a nr. rationale. (Exe) Calculati $U(R)$.

$$\text{Defin} \quad U(R) = \left\{ a \in R \mid (\exists) b \in R \text{ a.s.t. } ab = ba = 1 \right\}. \quad 1_R = 1 = \frac{1}{1}$$

Fie $x \in U(R)$ $\Rightarrow x = \frac{c}{d}$, $c, d \in \mathbb{Z}$, d impar

$\bullet \quad \frac{2}{3} \in R \quad \frac{2}{3} \in U(R)? \text{NU} \quad \frac{2}{3} \cdot \boxed{\frac{3}{2}} = 1 \quad \frac{3}{2} \notin R$ decarece $\frac{3}{2}$ nu

se poate scrie sub forma $\frac{m}{n}$ cu $m, n \in \mathbb{Z}$, n impar ($\text{Defin: } \frac{3}{2} = \frac{m}{n} \Rightarrow 3m = 2n \Rightarrow 2|3m$)
 $(2, 3) = 1 \Rightarrow 2|m$ și n impar)

Afirmatie:

$$U(R) = \left\{ \frac{c}{d} \mid c, d \in \mathbb{Z}, c, d \text{ impari} \right\} \quad (m, n) = 1$$

" \subseteq " Fie $x \in U(R)$; $x = \frac{m}{n}$, $m, n \in \mathbb{Z}$, n impar $\frac{m}{n} \cdot \frac{n}{m} = 1$

$\frac{m}{n} \in R \Leftrightarrow m$ impar Deci $x = \frac{m}{n} \in R$, $(m, n) = 1$, $x \in U(R) \Rightarrow m$ impar

$$\Rightarrow x \in \left\{ \frac{c}{d} \mid c, d \in \mathbb{Z}, c, d \text{ impari} \right\}$$

" \supseteq " $\frac{c}{d}$ c, d impari $\frac{c}{d} \cdot \frac{d}{c} = 1$ $\frac{d}{c} \in R$ (decare c impar)

$$\Rightarrow \frac{c}{d} \in U(R) \quad \Rightarrow$$

Evc 3 $U(\mathbb{Z}[i]) = ?$ $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$

Anătâmu că $U(\mathbb{Z}[i]) = \{ \pm 1, \pm i \}$ $i^2 = -1$ $i = 0 + 1 \cdot i$

" \supseteq " $1 \cdot 1 = 1$ $(-1) \cdot (-1) = 1$ $i \cdot (-i) = 1$ $(-i) \cdot i = 1$ (1)

" \subseteq " Fie $z \in U(\mathbb{Z}[i]) \stackrel{\text{def}}{\Rightarrow} (\exists) w \in \mathbb{Z}[i]$ a.s.t. $z \cdot w = 1 \Rightarrow$ Trecem la modul

$$\Rightarrow |z| \cdot |w| = 1 \stackrel{i^2}{\Rightarrow} |z|^2 \cdot |w|^2 = 1$$

$$z \in \mathbb{Z}[i] \Rightarrow |z|^2 = a^2 + b^2 \in \mathbb{N} \quad / \quad |z|^2, |w|^2 \in \mathbb{N}$$

$\begin{matrix} z = a+bi \\ a, b \in \mathbb{Z} \end{matrix}$

$$|z|^2 (= |w|^2) = 1$$

$$|z|^2 = 1 \Rightarrow \begin{matrix} a^2 + b^2 = 1 \\ z = a+bi \\ \boxed{a, b \in \mathbb{Z}} \end{matrix}$$

$$\begin{cases} a^2 = 0 \\ b^2 = 1 \end{cases} \quad \text{ sau } \begin{cases} a^2 = 1 \\ b^2 = 0 \end{cases}$$

\Downarrow

$$\begin{cases} a = 0 \\ b = 1 \end{cases} \quad \text{ sau } \begin{cases} a = 0 \\ b = -1 \end{cases}$$

\Downarrow

$$z = i$$

$$\begin{cases} a = 1 \\ b = 0 \end{cases} \quad \text{ sau } \begin{cases} a = -1 \\ b = 0 \end{cases}$$

\Downarrow

$$z = -i$$

\Downarrow

$$z = 1$$

\Downarrow

$$z = -1$$

$$\Rightarrow z \in \{ \pm 1, \pm i \} \Rightarrow U(\mathbb{Z}[i]) \subseteq \{ \pm 1, \pm i \}.$$

(2)

$$\text{Dim (1) și (2) } \Rightarrow U(\mathbb{Z}[i]) = \{ \pm 1, \pm i \}.$$

Exc 4 Să se arate că $f: \mathbb{Z}[i] \rightarrow \mathbb{Z}_2$, $f(a+bi) = \overline{a+b}$ este un morfism de module.

Exc 5 Descrieți elementele imobilui fraction $\mathbb{Z}[i]/(3)$.
(am SCR pt \Rightarrow)

Reamintim Rîmînd com, I, memul I ideal al lui R $(R/I, +, \cdot)$ - imel, unde $\hat{a} + \hat{b} = \overline{a+b}$, $\hat{a} \cdot \hat{b} = \overline{ab}$; unde $R/I = \{\hat{a} | a \in R\}$, $\hat{a} = \overline{b} (\overset{\text{def}}{=}) a - b \in I$

$$R = \mathbb{Z}[i] \quad I = (3) (= 3\mathbb{Z}[i]) = \left\{ \begin{array}{l} 3 \cdot z \mid z \in \mathbb{Z}[i] \\ R = \mathbb{Z}[i] \end{array} \right\} = \left\{ \begin{array}{l} 3a + 3bi, a, b \in \mathbb{Z} \\ I = 3\mathbb{Z}[i] \end{array} \right\}$$

$$\hat{x} = \overline{y} \text{ în } R/I \Leftrightarrow x - y \in I \Leftrightarrow x - y = 3a + 3bi, \text{ pt}$$

mînto $a_0, b_0 \in \mathbb{Z}$.

$$\text{Um SCR} = \{c + di \mid c, d \in \{0, 1, 2\}\} \stackrel{\text{not}}{=} X \quad (|X| = 9)$$

$$\text{Fie } z \in \mathbb{Z}[i] \Rightarrow z = u + v \cdot i, u, v \in \mathbb{Z} \quad \text{Th. împ. cu rest} \Rightarrow \boxed{\begin{array}{l} u = 3k + r_1 \\ v = 3l + r_2 \\ r_1, r_2 \in \{0, 1, 2\} \end{array}}$$

$$z = u + vi = (3k + r_1) + (3l + r_2) \cdot i = 3(k + li) + (r_1 + r_2 \cdot i)$$

$$\Rightarrow z - (r_1 + r_2 \cdot i) = 3(k + li) \in 3\mathbb{Z}[i] \Rightarrow z - z_1 \in 3\mathbb{Z}[i] \Rightarrow$$

$$\Rightarrow \hat{z} = \hat{z}_1 \text{ în } \mathbb{Z}[i]/(3) \quad z_1 = r_1 + r_2 \cdot i \in X \Rightarrow \text{orice element}$$

$\dim \mathbb{Z}[i]$ are clasa modulo $3\mathbb{Z}[i]$ egală cu clasa unui element dim X

$$\text{Fie } c_1 + d_1 i, c_2 + d_2 i \in X \text{ a.s. } \hat{c}_1 + \hat{d}_1 i = \hat{c}_2 + \hat{d}_2 i \text{ în } \mathbb{Z}[i]/(3). \quad (1)$$

$$\Rightarrow c_1 + d_1 i - (c_2 + d_2 i) \in 3\mathbb{Z}[i] \stackrel{\text{def}}{\Rightarrow} (c_1 - c_2) + (d_1 - d_2)i \in 3\mathbb{Z}[i] \quad \text{pt } a, b \in \mathbb{Z}.$$

$$\xrightarrow{\text{egalit.}} \left\{ \begin{array}{l} c_1 - c_2 = 3a \\ d_1 - d_2 = 3b \end{array} \right. \Rightarrow \left. \begin{array}{l} 3 | c_1 - c_2 \\ 3 | d_1 - d_2 \end{array} \right\} \Rightarrow \begin{array}{l} c_1 = c_2 \\ d_1 = d_2 \end{array} \Rightarrow c_1 + c_2 i \\ \text{M.R. complexe} \quad \text{Cum } c_1, c_2, d_1, d_2 \in \{0, 1, 2\} \quad \text{d.p. } d_1 + d_2 i$$

\Rightarrow orice z elemente distințe dim X au clasele modulo $3\mathbb{Z}[i]$ diferite (2)

Dim (1) și (2) $\Rightarrow X$ este un SCR $\Rightarrow \mathbb{Z}[i]/(3) = \{ \hat{c+di} \mid c, d \in \{0, 1, 2\} \}$

Anătați că $X_1 = \{c+di \mid c, d \in \{-1, 0, 1\}\}$ este un SCR.

Excl $f: \mathbb{Z}[i] \rightarrow \mathbb{Z}_2$ $f(a+bi) = \hat{a+b}$ f e morfism de inele

(Apoi calculați $\text{Ker } f$, $\text{Im } f$ și "verifică" T.F.I la imole)

f e morfism de inele dc) $\begin{cases} 1) f(z_1 + z_2) = f(z_1) + f(z_2) \quad (\forall) z_1, z_2 \in \mathbb{Z}[i] \\ 2) f(z_1 \cdot z_2) = f(z_1) \cdot f(z_2) \quad (\forall) z_1, z_2 \in \mathbb{Z}[i] \\ 3) f(1_{\mathbb{Z}[i]}) = 1_{\mathbb{Z}_2} \end{cases}$

$$1_{\mathbb{Z}_2} = \hat{1}, 1_{\mathbb{Z}[i]} = 1$$

$$3) f(1) = f(1+0 \cdot i) \stackrel{\text{def}}{=} \hat{0+1} = \hat{1} \Rightarrow 3) \text{ e verificat}$$

$$2) \text{ Fie } z_1, z_2 \in \mathbb{Z}[i] \Rightarrow z_1 = a+bi, z_2 = c+di \quad a, b, c, d \in \mathbb{Z}$$

$$f(z_1 \cdot z_2) = f((a+bi) \cdot (c+di)) = f((ac-bd) + i(ad+bc)) \stackrel{\text{def}}{=} (ac-bd) + (ad+bc)$$

$$\begin{aligned} f(z_1) \cdot f(z_2) &= f(a+bi) \cdot f(c+di) \stackrel{\text{def}}{=} \hat{a+b} \cdot \hat{c+d} \stackrel{\text{fornu}}{=} \hat{(a+b)(c+d)} = \\ &= (ac+bd) + (ad+bc) \stackrel{\text{in } \mathbb{Z}_2}{=} (ac-bd) + (ad+bc) \Rightarrow \\ &\text{in } \mathbb{Z}_2 \quad \hat{k} = -\hat{k} = -k \end{aligned}$$

$$\Rightarrow f(z_1 \cdot z_2) = f(z_1) \cdot f(z_2) \quad (\forall) z_1, z_2 \in \mathbb{Z}[i]$$

1) Excl!

$\text{Im } f = \mathbb{Z}_2$ ($\Leftrightarrow f$ e morfism surjectiv) : $f(0) = \hat{0}, f(1) = \hat{1}$

$\text{Ker } f = \{a+bi \in \mathbb{Z}[i] \mid f(a+bi) = \hat{0}\} = \{a+bi \mid a, b \in \mathbb{Z} \text{ și } a+b \text{ par}\}$

$$\underbrace{a+b}_{\text{par}} \quad (\hat{a+b} = \hat{0} \text{ in } \mathbb{Z}_2 \Leftrightarrow 2 | a+b \Leftrightarrow a+b \text{ par})$$

Anătațim $\text{Ker } f = (1+i)$ (sau $(1+i)\mathbb{Z}[i]$)

idealul generat de $1+i$ în $\mathbb{Z}[i]$

" \exists " $1+i \in \text{Ker } f$ deoarece $1+1=2$, par. Cum $(1+i)\mathbb{Z}[i] = \{(1+i) \cdot z \mid z \in \mathbb{Z}[i]\}$

$$\Rightarrow f((1+i) \cdot z) \stackrel{\text{f}}{=} f(1+i) \cdot f(z) = \hat{0} \cdot \hat{f(z)} = \hat{0} \Rightarrow (1+i) \cdot z \in \text{Ker } f$$

$$\Rightarrow (1+i)\mathbb{Z}[i] \subseteq \text{Ker } f. \quad (1)$$

$$(\forall) z \in \mathbb{Z}[i] \Rightarrow$$

" \leq " Fie $z = a+bi \in \text{Ker } f$, adică $a, b \in \mathbb{Z}$ și $a+b \in \text{par.}$

$$a+bi = 2c - b + bi = 2c - b(1-i)$$

$$= 2c + b \cdot i(i+1)$$

$$= (1-i)(1+i) \cdot c + b \cdot i(i+1) = (i+1) \underbrace{[(1-i) \cdot c + bi]}_{\mathbb{Z}[i]} \Rightarrow$$

$$\begin{aligned} & \Rightarrow a+b = 2 \cdot c \\ & -(1-i) = i^2(1-i) \quad c \in \mathbb{Z} \\ & = i(i-i^2) = i(i+1) \end{aligned}$$

$$\Rightarrow a+bi \in (1+i)\mathbb{Z}[i] \quad (2)$$

$$\text{Dim (1) și (2)} \Rightarrow \text{Ker } f = (1+i)\mathbb{Z}[i]$$

$$\text{T.F. I la imple} \rightarrow \frac{\mathbb{Z}[i]}{\text{Ker } f} \cong \text{Im } f, \text{ adică}$$

$$\boxed{\frac{\mathbb{Z}[i]}{(1+i)} \cong \mathbb{Z}_2}$$

LCR Date $m_1, m_2, \dots, m_n \geq 2$ nr. mat a.i. $(m_i, m_j) = 1 \quad (\forall) i \neq j$ și $a_1, a_2, \dots, a_n \in \mathbb{Z}$ atunci sistemul de congruențe

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

are soluție unică modulo $m_1 \cdot m_2 \cdot \dots \cdot m_n$.

Algoritm de rezolvare ① Consider $N = m_1 \cdot m_2 \cdot \dots \cdot m_n$, $N_i = \frac{N}{m_i} \quad (\forall) i = 1, 2, \dots, n \quad (\Rightarrow (N_i, m_i) = 1)$

② Determinăm $x_1, \dots, x_n \in \mathbb{Z}$ a.i. $N_i x_i \equiv 1 \pmod{m_i} \quad (\forall) i = 1, 2, \dots, n$

③ Soluția unică modulo $m_1 \cdot m_2 \cdot \dots \cdot m_n$ este $x \pmod{N}$,

$$\text{unde } x = a_1 N_1 x_1 + \dots + a_n N_n x_n.$$

Ex $d = (a, b) \Rightarrow (\exists) m, t \in \mathbb{Z}$ a.s. $d = a \cdot m + b \cdot t$ (cu alg. Euklid se demonstrează și se determină)

Exemplu $a = 35, b = 24 \quad d = (35, 24) = 1 \quad \text{Vrem să rezolv congr.}$

$$ax \equiv 1 \pmod{b}$$

$$35 = 24 \cdot 1 + 11 \Rightarrow 11 = 35 - 24$$

$$24 = 11 \cdot 2 + 2 \Rightarrow 2 = 24 - (35 - 24) \cdot 2 = 24 \cdot 3 - 35 \cdot 2$$

$$11 = 2 \cdot 5 + 1 \Rightarrow 1 = 11 - 2 \cdot 5 = (35 - 24) - 5(24 \cdot 3 - 35 \cdot 2)$$

$$2 = 1 \cdot 2 + 0 \Rightarrow (35, 24) = 11 \cdot 35 - 16 \cdot 24$$

$$1 = 35 \cdot 11 - 24 \cdot 16$$

$$(1 = (35, 24) \quad 1 = 35 \cdot 11 + (-24) \cdot 16)$$

$$a \cdot x \equiv 1 \pmod{b}$$

$$a = 35, b = 24$$

Trăc la clasa modulo 24 și obțin $35 \cdot 11 \equiv 1 \pmod{24} \Rightarrow$

x căutat este, de exemplu, 11 (pot lua și $x = 35, \dots$) $\begin{matrix} x \pmod{24} \\ 11 \pmod{24} \end{matrix}$

Exercițiu Rezolvarea sistemelor de congruențe:

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \\ x \equiv 8 \pmod{9} \end{cases}$$

+ 1 exemplu, la alegere.

$$\begin{array}{l} \text{LCR} \\ \left. \begin{array}{l} (\star) \\ (M_i, M_j) = 1 \\ (\forall i \neq j) \\ M_1 \cdots M_n \geq 2 \end{array} \right\} \begin{array}{l} x \equiv a_1 \pmod{M_1} \\ \dots \\ x \equiv a_n \pmod{M_n} \end{array} \end{array}$$

Sist. (\star) de congruențe are soluție unică modulo $M_1 \cdot M_2 \cdot \dots \cdot M_n$.

Algoritm de rezolvare

$$\textcircled{1} N = M_1 \cdots M_n, N_i = \frac{N}{M_i} \quad (\forall i = 1, 2, \dots, n) \quad (\Rightarrow (N_i, M_i) = 1)$$

$$\textcircled{2} \text{ Determinăm } x_1, \dots, x_n \text{ a.i. } N_i x_i \equiv 1 \pmod{M_i}$$

\textcircled{3} Soluția unică modulo $M_1 \cdot M_2 \cdot \dots \cdot M_n$ este

$$x \pmod{N} \text{ unde } x = a_1 N_1 x_1 + \dots + a_n N_n x_n$$

Obs Cum putem folosi practic LCR? De exemplu, dacă

avem de calculat $a \pmod{n}$ (pt a, n date) atunci $\overset{\text{Fie}}{M = p_1^{d_1} \cdots p_k^{d_k}}$ descomp. în factori primi a lui n și calculez

$$\begin{cases} a \pmod{p_1^{d_1}} = a_1 \pmod{p_1^{d_1}} \\ \vdots \\ a \pmod{p_k^{d_k}} = a_k \pmod{p_k^{d_k}} \end{cases}$$

pe $a \pmod{n}$.

Cu LCR pot determina dim

$$\begin{array}{l} \text{Ex 1} \\ \left. \begin{array}{l} \text{Folosim met. diviz. algor.} \\ (\star) \end{array} \right\} \begin{array}{l} n \equiv 3 \pmod{5} \\ n \equiv 2 \pmod{7} \\ n \equiv 8 \pmod{9} \end{array} \end{array}$$

$$a_1 = 3, a_2 = 2, a_3 = 8$$

$$M_1 = 5, M_2 = 7, M_3 = 9$$

$$N = 5 \cdot 7 \cdot 9 \quad N_1 = \frac{N}{M_1} = 7 \cdot 9 \quad N_2 = 5 \cdot 9 \quad N_3 = 5 \cdot 7$$

$$N_1 x_1 \equiv 1 \pmod{M_1} \rightsquigarrow 63 x_1 \equiv 1 \pmod{5} \rightsquigarrow 3 x_1 \equiv 1 \pmod{5} \rightsquigarrow x_1 \equiv 2 \pmod{5} \quad (\Rightarrow x_1 \equiv -3 \pmod{5})$$

$$N_2 x_2 \equiv 1 \pmod{M_2} \rightsquigarrow 45 x_2 \equiv 1 \pmod{7} \rightsquigarrow 3 x_2 \equiv 1 \pmod{7} \rightsquigarrow -x_2 \equiv 2 \pmod{7} \rightsquigarrow x_2 \equiv 5 \pmod{7}$$

$$N_3 x_3 \equiv 1 \pmod{M_3} \rightsquigarrow 35 x_3 \equiv 1 \pmod{9} \rightsquigarrow -x_3 \equiv 1 \pmod{9} \rightsquigarrow x_3 \equiv 8 \pmod{9}$$

Soluția unică modulo $N = 5 \cdot 7 \cdot 9 = 315$ este $x \pmod{N}$, unde

$$x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3$$

$$= 3 \cdot 63 \cdot 2 + 2 \cdot 45 \cdot 5 + 8 \cdot 35 \cdot 8 = 378 + 450 + 2240 = 3068$$

$3068 \pmod{315} \equiv 233 \pmod{315}$, $\overset{\text{unică}}{\text{Soluție asistemului mod(315) este 233.}}$

Exc 2 Calculati restul imp. lui a^{a^b} la c , unde

$$a = 7, b = 8, c = 11.$$

Restul imp. lui 7^8 la 11. Vrem $7^8 \pmod{11}$

Th. Euler $m > 2, (a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$

Mic. Thm. Fermat p prim $a^p \equiv a \pmod{p}$. Dc. $(a, p) = 1$

$$a^{p-1} \equiv 1 \pmod{p}$$

$$2^8 = 2^{2^3} \neq (2^3)^3 = 2^{3 \cdot 3} = 2^9$$

$$(7, 11) = 1 \xrightarrow{\text{Euler}} 7 \equiv 1 \pmod{11}$$

Pentru a calcula $7^8 \pmod{11}$ este suficient să calculezi

$$7^8 \pmod{10}$$

Stim (cls V)

$$\text{u.c. a lui } 7^n \text{ e } \begin{cases} 7, & n \equiv 1 \pmod{4} \\ 9, & n \equiv 2 \pmod{4} \\ 3, & n \equiv 3 \pmod{4} \\ 1, & n \equiv 0 \pmod{4} \end{cases}$$

Că să afli ultima cifră a lui 7^8 (adică $7^8 \pmod{10}$)

este suficient să afli $8^8 \pmod{4} \equiv 0 \pmod{4}$

$$\text{Deci, } 8^8 \pmod{4} \equiv 0 \pmod{4} \Rightarrow 7^8 \equiv 1 \pmod{10} \Rightarrow$$

$$\Rightarrow 7^8 = 10k + 1.$$

$$7^8$$

$$7 \pmod{11}$$

$$7^{10k+1} \pmod{11} \equiv (7^0)^k \cdot 7^1 \pmod{11}$$

$$\equiv 7 \pmod{11}$$

$$7^{10} \equiv 1 \pmod{11}$$

$$(7^{10})^k \equiv 1 \pmod{11}$$

Teorema împărțirii cu rest

Exc 3 Aflati restul împărțirii lui: $x^{100} - 2x^{51} + 1$ la $x^2 - 1$.

$$mx^{n+1} - (m+1)x^n + 1 \text{ la } (x+1)^2, \quad m \in \mathbb{N}, n \geq 1.$$

Exc 4 Det. $m \in \mathbb{N}$ a.t. $x^2 + x + 1 \mid x^{2m} + x^m - 1$.

Exc 5) Det. $a, b \in \mathbb{R}$ a.s.t. $(x-1)^2 \mid ax^4 + bx^3 + 1$. (Tema!)

$$ax^4 + bx^3 + 1 = (x-1)^2 \cdot Q(x)$$

Then imp. cu rest $f(x), g(x) \in K[x]$, $g(x) \neq 0$ $f(x) = g(x) \cdot Q(x) + r(x)$
 $\text{grad}(r(x)) < \text{grad}(g(x))$

Exc 3 ① $f(x) = x^{100} - 2x^5 + 1$, $g(x) = x^2 - 1$ $f(x), g(x) \in \mathbb{Q}[x]$

$$f(x) = g(x) \cdot Q(x) + r(x) \quad \text{grad}(r(x)) < 2 \Rightarrow r(x) = ax + b$$

$$x^{100} - 2x^5 + 1 = (x^2 - 1) \cdot g(x) + ax + b$$

$$a, b \in \mathbb{Q}$$

$$\begin{array}{l} x=1 \\ \hline f(1) = 0 \cdot g(1) + a+b \Rightarrow a+b=0 \\ 1-2+1=0 \end{array}$$

$$\begin{array}{l} x=-1 \\ \hline f(-1) = 0 \cdot g(-1) - a+b \Rightarrow b-a=4 \\ (-1)^{100} - 2 \cdot (-1)^5 + 1 \\ 1+2+1=4 \end{array}$$

$$\Rightarrow 2b=4 \Rightarrow b=2 \Rightarrow a=-2 \Rightarrow \text{restul imp. lui } f \text{ la } g \text{ este } -2x+2.$$

② $f(x) = mx^{n+1} - (n+1)x^n + 1$, $g(x) = (x-1)^2$ $f(x), g(x) \in \mathbb{Q}[x] n \in \mathbb{N}$

Then. imp. cu rest $\rightsquigarrow (1) m x^{n+1} - (n+1)x^n + 1 = (x-1)^2 \cdot Q(x) + ax + b$
 $a, b \in \mathbb{Q}$

Derivez

$$f'(x) = (x-1)^2 \cdot g'(x) + 2(x-1) \cdot g(x) + a$$

$$m(n+1)x^{n+1} - (n+1) \cdot m \cdot x^{n-1}$$

$$\begin{array}{l} x=1 \\ \hline m(n+1) - (n+1) \cdot m = 0 \cdot g'(1) + 0 \cdot g(1) + a \Rightarrow a=0 \end{array}$$

Dim (1) și (2) \Rightarrow restul imp. este zero ($\Rightarrow f(x) = (x-1)^2 \cdot Q(x)$)

Sol. alternativă se poate da cu descompunerea lui f

Exc 4 Detva.i. $x^2 + x + 1 \mid x^{2m} + x^m + 1$.

Să stim că $x^{2m} + x^m + 1 = (x^2 + x + 1) \cdot Q(x)$

Răd. lui x^2+x+1 sunt $-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$, sau echivalent $\varepsilon, \varepsilon^2$, unde

$$\varepsilon = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}. \quad (\text{Moivre: } (\cos \alpha + i \sin \alpha)^n = \cos(n\alpha) + i \sin(n\alpha))$$

$\varepsilon^3 = 1 \quad \rightarrow \quad (\varepsilon - 1)(\varepsilon^2 + \varepsilon + 1) = 0 \quad \Rightarrow \quad \boxed{\varepsilon^2 + \varepsilon + 1 = 0}$

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

$$f(x) = (x^2 + x + 1) \circ g(x)$$

$$x = \varepsilon \quad \Rightarrow \quad f(\varepsilon) = 0 \quad \Rightarrow \quad \varepsilon^{2m} + \varepsilon^m + 1 = 0$$

$$x = \varepsilon^2 \quad \Rightarrow \quad f(\varepsilon^2) = 0 \quad \Rightarrow \quad \varepsilon^{4m} + \varepsilon^{2m} + 1 = 0$$

Tb. să "rezolv" "sistemu" folosind condițiile

$$\begin{cases} \varepsilon^3 = 1 \\ \varepsilon^2 + \varepsilon + 1 = 0 \end{cases}$$

$$\left. \begin{cases} \varepsilon^{2m} + \varepsilon^m + 1 = 0 \\ \varepsilon^{4m} + \varepsilon^{2m} + 1 = 0 \end{cases} \right\} \quad \begin{matrix} (*) \\ \text{si si det.} \end{matrix} \quad \begin{matrix} \text{si} \\ \text{n-ul!} \end{matrix}$$

$$\varepsilon^{4m} + \varepsilon^{2m} + 1 = \varepsilon^{3m} \cdot \varepsilon^m + \varepsilon^{2m} + 1 = (\varepsilon^3)^m \cdot \varepsilon^m + \varepsilon^{2m} + 1 = \varepsilon^{2m} + \varepsilon^m + 1 = 0$$

Prin urmare, avem de det. m stiind doar că $\varepsilon^{2m} + \varepsilon^m + 1 = 0$

Analyzează 3 cazuri în funcție de $m \pmod 3$

$$\text{I} \quad m \equiv 1 \pmod 3 \quad (\Leftrightarrow m = 3k+1)$$

$$\varepsilon^{2m} + \varepsilon^m + 1 = \varepsilon^{6k+2} + \varepsilon^{3k+1} + 1 = \\ = (\varepsilon^3)^k \cdot \varepsilon^2 + (\varepsilon^3)^k \cdot \varepsilon + 1 = \varepsilon^2 + \varepsilon + 1 = 0$$

\Rightarrow (I) $m \equiv 1 \pmod 3$ merge

$$\text{II} \quad m \equiv 2 \pmod 3 \quad (\Leftrightarrow m = 3k+2)$$

$$\varepsilon^{2m} + \varepsilon^m + 1 = \varepsilon^{6k+4} + \varepsilon^{3k+2} + 1 =$$

$$= (\varepsilon^3)^{2k+1} \cdot \varepsilon^2 + (\varepsilon^3)^k \cdot \varepsilon^2 + 1 = \varepsilon^2 + \varepsilon^2 + 1 = 0 \quad \Rightarrow \quad \text{(II) } m \equiv 2 \pmod 3$$

$$\text{III} \quad m \equiv 0 \pmod 3 \quad (\Leftrightarrow m = 3k) \Rightarrow \varepsilon^{2m} + \varepsilon^m + 1 = \varepsilon^{6k} + \varepsilon^{3k} + 1 = 1 + 1 + 1 = 3 \neq 0$$

\Rightarrow Niciun $m \equiv 0 \pmod 3$ nu merge.

Deci $x^2 + x + 1 \mid x^{2m} + x^m + 1 \quad (\Leftrightarrow m \equiv 1 \pmod 3 \text{ sau } m \equiv 2 \pmod 3)$

Răd. complexe ale lui $x^m - 1$ sunt $\{1, \omega, \omega^2, \dots, \omega^{m-1}\}$

$$\text{unde } \omega = \cos \frac{2\pi}{m} + i \sin \frac{2\pi}{m}.$$