STRUCTURI ALGEBRICE ÎN INFO

idempotenta în inel: $x^2=x$

distributivitate $\cap$ față de $\cup$

-//- $\cup$ -//- $\cap$

$$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$$

$$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$$

$$B\setminus A \overset{not.}{=} C_B A$$

Rel. lui De Morgan:

- $x\in C_B(A\cup A') = C_BA\cap C_BA'$.

$\Updownarrow$

$x\in B$ și $x\notin A\cup A'$

$x\notin A$ și $x\notin A'$

- $C_B(A\cap A')=(C_BA)\cup(C_BA')$

$A\subseteq B$

$i: A\to B$, $i(a)=a$, $\forall\, a\in A$ s.n. fct. incluziune

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ i \; \cup\!\!\mid & \nearrow & \\ A' & & \end{array}$$

$f\circ i \to$ s.n. restricția lui f la A' cu val. în B.
$= f|_{A'}$

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & f'' \searrow & \uparrow i \\ & & \operatorname{Im} f \end{array}$$

$\operatorname{Im} f = \{f(a) \mid a\in A\} \subseteq B$

$f''(a) = f(a)$, $\forall a\in A$: corestricția lui f la imagine

$i\circ f'' = f$.

$A_1\times A_2 \xrightarrow{p_1} A_1$

$A_1\times A_2 \xrightarrow{p_2} A_2$, $p_1(a_1,a_2)=a_1$, $p_2(a_1,a_2)=a_2$

$f_1: A_1\to B_1$

$f_2: A_2\to B_2$

$g: A_1\times A_2 \to B_1\times B_2$

$g(a_1,a_2)=(f_1(a_1), f_2(a_2)) \xrightarrow{not.} f_1\times f_2$

fct. car.: $A \subset T$

$\chi_A : T \to \{0,1\}$

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

$A = A' \Leftrightarrow \chi_A = \chi_{A'}$.

Ex.: 1) $\chi_{A \cap A'} = \chi_A \cdot \chi_{A'}$;

2) $\chi_{A \cup A'} = \chi_A + \chi_{A'} - \chi_A \cdot \chi_{A'}$

3) $\chi_{A \setminus A'} = \chi_A (1 - \chi_{A'})$

$$f : \begin{array}{ccc} A & \longrightarrow & B \\ \cup\!\! \mid & & \cup\!\! \mid \\ A' & & B' \end{array}$$

$f(A') = \{ f(a') \mid a' \in A' \} \subseteq B$

$A' = A$, $f(A) \overset{\text{not.}}{=} \operatorname{Im} f$

$f^{-1}(B') = \{ a \in A \mid f(a) \in B' \}$

$f^{-1}([-2,1]) = \{ x \in \mathbb{R} \mid \underset{x^2}{\underset{\shortparallel}{f(x)}} \in [-2,1] \} = [0,1]$.

• $f(M \cup N) \overset{?}{=} f(M) \cup f(N)$

$\left.\begin{array}{l} M \subseteq M \cup N \Rightarrow f(M) \subset f(M \cup N) \\ N \subseteq M \cup N \Rightarrow f(N) \subseteq f(M \cup N) \end{array}\right| \Rightarrow f(M) \cup f(N) \subseteq f(M \cup N)$.

$b \in f(M \cup N) \Rightarrow \exists\, a \in M \cup N$ a.î. $b = f(a)$

$\left.\begin{array}{l} a \in M \Rightarrow \underset{b}{\underset{\shortparallel}{f(a)}} \in f(M) \\ a \in N \Rightarrow \underset{b}{\underset{\shortparallel}{f(a)}} \in f(N) \end{array}\right| \Rightarrow f(M \cup N) \subseteq f(M) \cup f(N)$

• $f(M \cap N) \subseteq f(M) \cap f(N)$.

· $M \subseteq A$.

$f(M) \subseteq B$

$M \subseteq f^{-1}(f(M)) \subseteq A$.

$a \in M \Rightarrow f(a) \in f(M) \Leftrightarrow a \in f^{-1}(f(M))$.

· $P \subseteq Q \subseteq B \Rightarrow f^{-1}(P) \subseteq f^{-1}(Q)$.

$\boxed{a \in f^{-1}(P) \Leftrightarrow f(a) \in P.}$

· $P, Q \subseteq B$. $\quad f^{-1}(P \cap Q) \underset{\subseteq}{=} f^{-1}(P) \cap f^{-1}(Q)$

"$\supseteq$" $\quad a \in f^{-1}(P) \cap f^{-1}(Q) \Rightarrow f(a) \in P$ și $f(a) \in Q \Rightarrow$

$\Rightarrow f(a) \in P \cap Q \Rightarrow a \in f^{-1}(P \cap Q)$.

·
$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & & \cup\!\shortmid \\ & & P \end{array}$$

$P \subseteq B \Rightarrow f(f^{-1}(P)) \subseteq P$.

$b \in f(f^{-1}(P))$

$b = f(a)$, $a \in f^{-1}(P)$

$\Updownarrow$

$b = f(a) \in P$.

$$h / \left.\begin{array}{l} f \circ g = 1_B, \ g \circ f = 1_A \\ f \circ h = 1_B, \ h \circ f = 1_A \end{array}\right\} \Rightarrow g = h.$$

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

$g \overset{\text{not.}}{=} f^{-1}$ (când există)

$f : A \to B$ inv. $\Rightarrow$ f bij.

$\exists\, g : B \to A$ a.î. $f \circ g = 1_B$ → surj. ; $g \circ f = 1_A$ → inj. $\Rightarrow$ f inj., f surj.

f bij. $\Rightarrow$ f inv.

$g : B \to A$

$b = f(a)$ pt. unic

$g(b) = a$

Prod. cartezian al unei familii de mulțimi

$I \neq \emptyset$

A mulțime

$\varphi : I \to A$ s.n. familie de el. din A indexată după I ~~mulț.~~

$\varphi = (a_i)_{i \in I}$, $a_i = \varphi(i)$

~~$I = \{1, 2, \dots, n\}$~~ $(A_i)_{i \in I}$

$$\prod_{i \in I} A_i = \{ \varphi : I \to \bigcup_{i \in I} A_i \mid \varphi(i) \in A_i \ \forall i \in I \} =$$

– funcții

$$= \{ (a_i)_{i \in I} \mid a_i \in A_i, \forall i \in I \}$$

$$\prod_{i \in I} A_i = A^I .$$

$A_i = A$

Algebra: carte Dumitrescu

Semin. 20p — 10 p. (ex. la tablă) ; 5 p. (lucrare scrisă) ex: 1) $f : A \longrightarrow B$ cu prop. că $\exists M \subseteq A$ a.î. $M \subsetneq f^{-1}(f(M))$ f neinj.

2) — // — $P \subseteq B$ a.î. $f(f^{-1}(P)) \subsetneq P$ f nesurj.

$a \in f^{-1}(P) \Leftrightarrow f(a) \in P.$

$b \in f(M) \Leftrightarrow b = f(a),\ a \in M.$

prop.: • f inj. $\Leftrightarrow M = f^{-1}(f(M)),\ \forall M \subseteq A.$

„$\Rightarrow$" „$\supseteq$" $a \in f^{-1}(f(M)) \Leftrightarrow f(a) \in f(M) \Rightarrow \exists a' \in M$ a.î.

$f(a) = f(a') \Rightarrow a = a' \in M \Rightarrow a \in M.$

„$\Leftarrow$" $f(a) = f(a') \overset{?}{\Rightarrow} a = a'.$

$M = \{a\} \Rightarrow$ ~~$\{a\} = f^{-1}(f(a))$~~

$\{a\}.\ f(M) = \{f(a)\} \Rightarrow$

$\{a\} = M = f^{-1}(f(M)) = \{x \in A \mid f(x) \in f(M)\} =$

$= \{x \in A \mid f(x) = f(a)\} \Rightarrow$

$\Rightarrow a' \in \{a\} \Rightarrow a' = a.$

• f surj. $\Leftrightarrow f(f^{-1}(P)) = P,\ \forall P \subseteq B.$

se dem. la fel

$f : \mathbb{R} \longrightarrow \mathbb{R},\ f(x) = x^2.$

$M = [0, +\infty)$

$f(M) = [0, +\infty)$

$f^{-1}(f(M)) = \mathbb{R}$

$P = [-1, 0)$

$f^{-1}(P) = \emptyset$

$f(\emptyset) = \emptyset \subseteq [-1, 0).$

$A \subseteq T$, $\chi_A : T \longrightarrow \{0,1\}$, $\chi_A(t) = \begin{cases} 1, & t \in A \\ 0, & t \notin A \end{cases}$

Prop. : 1. $\chi_{A \cap A'} = \chi_A \cdot \chi_{A'}$.

2. $\chi_{A \cup A'} = \chi_A + \chi_{A'} - \chi_A \cdot \chi_{A'}$.

3. $\chi_{A \setminus A'} = \chi_A \underbrace{(1 - \chi_{A'})}_{\chi_{T \setminus A'}}$.

$A \cap (T \setminus A') = A \setminus A'$.

1. $x \in A \cap A' \Rightarrow \chi_{A \cap A'}(x) = 1$

$\Rightarrow \begin{cases} \chi_A(x) = 1 \\ \chi_{A'}(x) = 1 \end{cases} \Rightarrow$

$x \notin A \cap A' \Leftrightarrow \chi_{A \cap A'}(x) = 0$.

$x \notin \{ \} \Rightarrow x \notin A$ ~ $x \notin A'$

2. dacă $x \in A \cup A'$ $\Rightarrow$ (arbitrar ales) $\Rightarrow$ $\chi_{A \cup A'}(x) = 1$.

$\Rightarrow$ $x \in A$ sau $x \in A'$.

distingem : $x \in A$ și $x \notin A' \Rightarrow \chi_A(x) = 1$, $\chi_{A'}(x) = 0$,

$\chi_A(x) \cdot \chi_{A'}(x) = 0$

$x \in A$ și $x \in A'$

$x \notin A$ și $x \in A'$

dacă $x \notin A \cup A' \Rightarrow$ $x \notin A$ și $x \notin A'$.

3. dacă $x \in A \setminus A' \Leftrightarrow \chi_{A \setminus A'}(x) = 1$ și $x \in A$ și $x \notin A'$

$\Leftrightarrow$ $\chi_{A \setminus A'}(x) = 1$ și $\chi_A(x) = 1$ și $\chi_{A'}(x) = 0 \Leftrightarrow$

$\Leftrightarrow$ $1 = 1\,(1 - 0)$

$x \notin (A \setminus A') \Leftrightarrow$ $x \notin A$ sau $x \in A'$

$\chi_{A \setminus A'}(x) = 0$ $\chi_A(x) = 0$ sau $\chi_{A'}(x) = 1$

(nu mai contează celălalt factor)

$A \Delta B = (A \setminus B) \cup (B \setminus A)$

$(\mathcal{P}(T), \underset{\cdot}{\cap}, \underset{+}{\Delta})$ inel comutativ unitar

$A \Delta A = \emptyset$ (inel boolean)

$(\mathcal{P}(T), \cap) \to$ monoid

$(R, +, \cdot)$ inel com.

$(\mathcal{P}(T), \Delta) \to$ grup

$x + x = 0, \forall x \in R$

$x^2 = x$

$(A \cap A = A)$

- asociat. ✓
- neutru $(\emptyset)$
- el. sim. : $A \Delta A = (A \setminus A) \cup (A \setminus A) = \emptyset$

$(x+1)^2 = x+1$

$\cancel{x^2} + 2x + \cancel{1} = \cancel{x} + \cancel{1}$

$x + x = 0.$

1. $A \Delta (B \Delta C) = (A \Delta B) \Delta C$
2. $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$

$$\chi_{A \Delta B} = \chi_{(A \setminus B) \cup (B \setminus A)} = \chi_{A \setminus B} + \chi_{B \setminus A} - \chi_{A \setminus B} \cdot \chi_{B \setminus A} =$$

$$= \chi_A (1 - \chi_B) + \chi_B (1 - \chi_A) - \chi_A \underbrace{(1 - \chi_B) \cdot \chi_B (1 - \chi_A)}_{0} =$$

$$\cancel{= \chi_A \cdot \chi_B (1 - \chi_A - \chi_B + \chi_A \cdot \chi_B) +}$$

$$= \chi_A + \chi_B - 2 \chi_A \chi_B = \chi_A + \chi_B \pmod 2$$

dem 2. $\chi_{A \cap (B \Delta C)} = \chi_A \cdot \chi_{B \Delta C} = \chi_A (\chi_B + \chi_C) \pmod 2$

$$\chi_{(A \cap B) \Delta (A \cap C)} = \chi_{A \cap B} + \chi_{A \cap C} \pmod 2 =$$

$$= \chi_A \cdot \chi_B + \chi_A \cdot \chi_C = \chi_A (\chi_B + \chi_C) \pmod 2$$

$$(\mathcal{P}(T), \Delta, \cap) \underset{\text{izomorfism}}{\xrightarrow{\simeq}} (\{0, 1\}, \underset{\substack{\downarrow \\ \text{mod } 2}}{+}, \cdot)$$

$$(\mathbb{Z}_2, +, \cdot)$$

$A, B \subseteq M$

$$f : \mathcal{P}(M) \longrightarrow \mathcal{P}(A) \times \mathcal{P}(B)$$

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

1) f inj. $\Leftrightarrow$ $A \cup B = M$.

2) f surj. $\Leftrightarrow$ $A \cap B = \emptyset$

3) f bij. $\Leftrightarrow$ $\begin{matrix} A \cup B = M \\ A \cap B = \emptyset \end{matrix}$ $\Rightarrow$ $f^{-1} = ?$

1) „$\Leftarrow$" $f(X) = f(Y) \Rightarrow \begin{cases} X \cap A = Y \cap A \\ X \cap B = Y \cap B \end{cases} \Big| \overset{\cup}{\Rightarrow}$

dar $A \cup B = M$

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

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

$$\left.\begin{matrix} X \cap M = Y \cap M \\ \text{dar } X, Y \in \mathcal{P}(M) \end{matrix}\right| \Rightarrow X = Y.$$

„$\Rightarrow$" Pp. că $A \cup B \neq M \Rightarrow \exists m \in M$ a.î. $m \notin A \cup B$.

Fie $X_1 = \{m\}$, $X_2 = \emptyset$.

$$\left.\begin{matrix} f(X_1) = (X_1 \cap A, X_1 \cap B) = (\emptyset, \emptyset) \\ f(X_2) = (X_2 \cap A, X_2 \cap B) = (\emptyset, \emptyset) \end{matrix}\right| \Rightarrow$$

$\Rightarrow f(X_1) = f(X_2)$. (cu f inj.)

2) „$\Leftarrow$" $A \cap B = \emptyset$.

fie $(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(B)$

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

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

$$= (X, Y)$$

„$\Rightarrow$" f surj.

Pp. că $A \cap B \neq \emptyset$. Deci $\exists\, m \in A \cap B$.

$$\cancel{f(X) = (X \cap \{m\},}$$
$$\cancel{A = \{m\}}$$
$$\cancel{B = M.}$$

$$\cancel{f(X) = (X \cap \{m\}, X \cap M)}.$$

$A = \{$ $\quad X \cap A = \{m\} \Rightarrow m \in A$ și $m \in X$

$X \cap B = \emptyset \Rightarrow m \in X$ și $m \notin B$. $\Big|$ abs

din $m \in A \cap B$

$$f(X) = (\{m\}, \emptyset).$$

$$\cancel{X \cap (A \cup B) = (X \cap A) \cup (X \cap B) = \{m\}}$$

caut $X \in P(M)$ a.î. $X \cap A = \{m\}$ și $X \cap B = \emptyset$.

temă din cursul de Dumitrescu: pg. 23 ex. 11
24 ex. 12

11. Princ. incl. și excl.

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum |A_i| - \sum |A_i \cap A_j| + \ldots + (-1)^{n+1} |A_1 \cap \ldots \cap A_n|.$$

Inducție. $P(2)$: $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

reiese imediat din diagramă

Pp. $P(n)$ adevărat: $|A_1 \cup \ldots \cup A_n| = \sum |A_i| - \sum |A_i \cap A_j| + \ldots + (-1)^{n+1} \cdot$
$\cdot |A_1 \cap \ldots \cap A_n|$.

Însă, not. $M = A_1 \cup A_2 \cup \ldots A_n$, din $P(2) \Rightarrow$

$$|M \cup A_{n+1}| = |M| + |A_{n+1}| - |M \cap A_{n+1}| \overset{\text{ip. inducție}}{=}$$

$$= \sum_{i=1}^{n+1} |A_i| - \sum_{\substack{i,j=1 \\ i \neq j}}^{n} |A_i \cap A_j| + \ldots + (-1)^{n+1} |A_1 \cap \ldots \cap A_n| -$$

$$- |(A_1 \cup A_2 \cup \ldots \cup A_n) \cap A_{n+1}| \quad . (*)$$

din distributivitatea intersecției față de reuniune :

$$(A_1 \cup A_2 \cup \dots \cup A_n) \cap A_{n+1} = \bigcup_{i=1}^{n} (A_i \cap A_{n+1})$$

$$|(A_1 \cup \dots \cup A_n) \cap A_{n+1}| = |(A_1 \cap A_{n+1}) \cup \dots \cup (A_n \cap A_{n+1})| \overset{\text{ip. inducție}}{=}$$

$$= \sum_{i=1}^{n} |A_i \cap A_{n+1}| - \sum |(A_i \cap A_{n+1}) \cap (A_j \cap A_{n+1})| + \dots +$$

$$+ (-1)^{n+1} |(A_1 \cap A_{n+1}) \cap \dots \cap (A_n \cap A_{n+1})| =$$

$$= \sum_{i=1}^{n} |A_i \cap A_{n+1}| - \sum_{i<j} |A_i \cap A_j \cap A_{n+1}| + \dots +$$

$$+ (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n \cap A_{n+1}| .$$

Introducând în rel. în (*) :

$$|M \cup A_{n+1}| = \sum_{i=1}^{n+1} |A_i| - \sum_{i<j} |A_i \cap A_j| + \dots + (-1)^{n+2} |A_1 \cap \dots \cap A_{n+1}| .$$

12. $A = \{1, 2, \dots, a\}$, $B = \{1, 2, \dots, b\}$

a) $f : A \to B$.

$f(i)$ poate lua b valori

i poate lua a valori $\xrightarrow{\text{regula produsului}}$ $\underbrace{b \cdot b \cdots b}_{a \text{ ori}} = b^a$.

b) N_i = nr. injecții de la A la B

$f(1), f(2), \dots, f(a)$ repr. oricare a val. distincte

din b date, deci nr. submulț. ordonate $\left(A_b^a = \frac{b!}{(b-a)!}\right)$

la permutări : $a = b \Rightarrow N_i = \frac{n!}{0!} = n!$ $(0! = 1)$

c) $N_s = k^a - C_k^1 (k-1)^a + C_k^2 (k-2)^a + \ldots + (-1)^{k-1} C_k^{k-1}$.

Scad non-surjecțiile din nr. total.

$f: A \to B$ nu este surjecție dacă $\exists$ cel puțin un $i \in B$ a.î.

$i \notin \operatorname{Im} f$ $\quad (f(k) \neq i, \forall k \in A)$.

$N_{\bar{S}} = |S_1 \cup S_2 \cup \ldots \cup S_k|$, unde S_i = mulț. fct. ce nu-l au în imag. nu pe i. cf. P. incl. și excl.:

$N_{\bar{S}} = \sum |S_i| - \sum |S_i \cap S_j| + \ldots + (-1)^{k+1} \cdot |S_1 \cap S_2 \cap \ldots \cap S_k|$.

$|S_{i_1} \cap S_{i_2} \cap \ldots \cap S_{i_k}|$ repr. nr fct. ce pot lua doar

$(k-k)$ valori $\underset{(\text{nu cont. ordinea})}{\overset{a)}{\Rightarrow}}$ $(k-k)^a$ astfel de funcții.

Pt. fiec. astfel de k, avem $C_k^k \Rightarrow$

$N_S = k^a - C_k^1 \cdot (k-1)^a + C_k^2 (k-2)^a + \ldots + (-1)^{k-1} \cdot C_k^{k-1} + \underbrace{(-1)^k \cdot C_k^k \cdot 0}_{0}$

d) N_d: nr. fct. ~~strict~~ cresc. de la A la B.

f va fi complet definită de $f(1), f(2), \ldots, f(a)$,

iar $f(1) < f(2) < \ldots < f(a)$.

Alegând a el. din cele k, acestea pot fi distribuite ~~strict~~ în mod unic lui $f(1), f(2), \ldots, f(a)$. $\Rightarrow C_k^a$.

e) N_e: nr. fct. cresc. de la A la B $\quad (C_{a+k-1}^a)$.

$f(1) \leq f(2) \leq \ldots \leq f(a)$

Fie x_k, $k = \overline{1,k}$ nr. sol. ec. $f(i) = k$, unde $i \in \{1, 2, \ldots, a\}$.

avem că: $\quad x_1 + x_2 + \ldots + x_k = a \quad$ (unde pot fi nule)

Avem de ales valori de 1 (pt. x_i care sunt soluții) și „+"-uri

în nr. (a valori și $k-1$ „+"-uri) $\Rightarrow C_{a+k-1}^a = C_{a+k-1}^{k-1}$

(metoda *1)

Curs 2

<u>Rel. de echivalență</u>

$a \rho b \iff (a,b) \in \rho$, unde $\rho \subseteq A \times B$

$a \urcorner\rho b$, $a \not\rho b$

ex.: 1) $f: A \to B$, $G_f = \{(a, f(a)) \mid a \in A\} \subseteq A \times B$

Reciproc, $G \subseteq A \times B$, $\forall a \in A, (\exists!) b \in B$ a.î. $(a,b) \in G$ at., def. $f: A \to B$,

$f(a) = b$. cu prop. $(a,b) \in G$.

Obs. $G_f = G$.

2) $A \neq \emptyset$, $\rho = \{(a,X) \in A \times \mathcal{P}(A) \mid a \in X\} \subseteq A \times \mathcal{P}(A)$

$a \rho X \iff a \in X$.

ex.: 1) $A = \mathbb{Z}$ $\quad n \geq 2$

$a \equiv b \pmod{n} \iff n \mid a-b$

$\equiv \pmod{n} \subseteq \mathbb{Z} \times \mathbb{Z}$

2) $\Delta_A = \{(a,a) \mid a \in A\}$ diagonala mulț. A

$\Delta_A \subseteq A \times A$

3) $A = \mathbb{N}$

$< = \{(m,n) \in \mathbb{N} \times \mathbb{N} \mid m < n\} \subseteq \mathbb{N} \times \mathbb{N}$

$A = \{1,2,3,4\}$ $\quad < = \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$.

Def.: ρ: rel pe A

1) ρ este reflexivă dc. $a \rho a, \forall a \in A$

$\Delta_A \subseteq \rho$

2) ρ este simetrică dc. $a \rho b \Rightarrow b \rho a$

3) ρ tranzitivă dc. $a \rho b$ și $b \rho c \Rightarrow a \rho c$.

1), 2), 3) rel. de echiv. pe A

+ antisim. : rel. de ordine

ex.: $\mathbb{R}$ $x \sim y \iff x - y \in \mathbb{Z}$

Def.: ρ rel. de echiv. pe A

$a \in A$, $\hat{a} = \{ b \in A \mid a \rho b \}$.

Th.:

1) $a \in \hat{a}$

2) $\hat{a} = \hat{b} \iff a \rho b$

3) $\hat{a} = \hat{b}$ sau $\hat{a} \cap \hat{b} = \emptyset$.

2) $\hat{a} = \hat{b} \ni b \Rightarrow a \rho b$

$a \rho b \Rightarrow \hat{a} = \hat{b}$

„$\subseteq$" $\hat{a} \subseteq \hat{b}$

$x \in \hat{a} \Rightarrow \left.\begin{array}{l} x \rho a \\ a \rho b \end{array}\right| \Rightarrow x \rho b \Rightarrow x \in \hat{b}$.

3) $a \not\rho b \Rightarrow \hat{a} \cap \hat{b} = \emptyset$.

pp. că $\exists x \in \hat{a} \cap \hat{b} \Rightarrow \left.\begin{array}{l} x \rho a \Rightarrow a \rho x \\ x \rho b \end{array}\right| \Rightarrow a \rho b$.

Def. $A_i \subseteq A$, $i \in I$

1) $\bigcup_{i \in I} A_i = A$

2) $A_i \cap A_j = \emptyset, \forall i \neq j$

At. $(A_i)_{i \in I}$ s.n. partiție a lui A.

Dc. $(A_i)_{i \in I}$ este partiție a lui A, at. $\exists!$ ρ rel. de echiv. pe A a.î. clasele de echiv. ale lui ρ sunt $(A_i)_{i \in I}$.

$a \rho a' \iff \exists i \in I$ a.î. $a, a' \in A_i$.

$A/\rho = \{ \hat{a} \mid a \in A \}$.

rel. pe $\mathbb{N} \times \mathbb{N}$ a.î. $\mathbb{N} \times \mathbb{N} / \rho = \mathbb{Z}$.

$\mathbb{Z} \times \mathbb{Z} /_{\equiv (\mathrm{mod}\, 7)} = \{\hat{0}, \hat{1}, \dots, \hat{6}\}$

$p : A \longrightarrow A/\rho$, $p(a) = \hat{a}$.

p fct. surjectivă

surjecția canonică

$f : A \to B$, $a \, \rho_f \, a' \Leftrightarrow f(a) = f(a')$

rel. de echiv. asoc. lui f

$\hat{a} = \{ a' \in A \mid a' \rho_f a, \ f(a') = f(a) \}$

$a' \in f^{-1}(\{f(a)\})$

Prop. de universalitate a mulț. factor:

$A \neq \emptyset$, ρ rel. pe A

$$\begin{tikzcd} A \arrow[r, "p"] \arrow[dr, "f"'] & A/\rho \arrow[d, dashed] \\ & B \end{tikzcd}$$

$(\exists) \bar{f}$ a.î. $\bar{f} \circ p = f$.

$\bar{f} \circ p = f \Leftrightarrow (\bar{f} \circ p)(a) = f(a), \forall a \in A$.

$\bar{f}(\cancel{p(a)}\hat{a}) = f(a), \forall a \in A$.

$\hat{a'} = \hat{a} \Rightarrow \bar{f}(\hat{a'}) = \bar{f}(\hat{a}) = f(a)$.

$= f(a')$

$a' \rho a \Rightarrow f(a') = f(a)$ $\qquad \rho \subseteq \rho_f$.

$\rho \subseteq \rho_f \Rightarrow (\exists !) \bar{f} : A/\rho \to B$ a.î. $\bar{f} \circ p = f$.

$\bar{f}$ inj. $\Leftrightarrow \rho \supseteq \rho_f$

$\bar{f}$ surj. $\Leftrightarrow f$ surj.

„$\Rightarrow$" $\rho \subseteq \rho_f$

$a \rho_f a' \Rightarrow f(a) = f(a') \Leftrightarrow \bar{f}(\hat{a}) = \bar{f}(\hat{a'}) \underset{\bar{f} \text{ inj.}}{\Rightarrow} \hat{a} = \hat{a'} \Rightarrow a \rho a'$

$\rho = \rho_f$

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

$$\begin{tikzcd} \mathbb{R} \arrow[r] \arrow[dr, "f"'] & \mathbb{R}/\rho \arrow[d, "(\exists!)\ \bar{f}"] \\ & S = \{z \in \mathbb{C} \mid |z| = 1\} \end{tikzcd}$$

$(\exists!)\ \bar{f}$ inj. cu $\bar{f} \circ p = f$

f surj. $\Rightarrow \bar{f}$ surj.

Seminar 2

$f : \mathbb{N} \to \mathbb{N}$

$g : \mathbb{N} \to \mathbb{N}$

$f \circ g = 1_{\mathbb{N}}$ $\qquad$ f, g bij $\Rightarrow$ g inj.

$g \circ f \neq 1_{\mathbb{N}}$ $\qquad$ f surj.

$f : \mathbb{N} \to \mathbb{N},\ f(x) = 2x$

$g : \mathbb{N} \to \mathbb{N},\ g(x) = \left[\frac{x}{2}\right]$

$g(f(x)) = \left[\frac{2x}{2}\right] = [x] \overset{x \in \mathbb{N}}{=} x$

$f(g(x)) = 2 \cdot \left[\frac{x}{2}\right]$.

$f \circ g(1) = 0 \neq 1_{\mathbb{N}}(1)$

$g \circ f(1) = 1$.

$\rho \subseteq A \times A$ rel. de echiv.

$\exists\ \bar{\rho} \supseteq \rho$, $\bar{\rho}$ rel. de echiv. cea mai mică cu ac. prop.

$\boxed{\text{Arătați}}$ că $\bar{\rho} = \Delta_A \cup (\rho \cup \rho^{-1}) \cup (\rho \cup \rho^{-1})^2 \cup \ldots$

$\rho^{-1} = \{(x, y) \in A \times A \mid y \rho x\}$

$\rho^n = \{(x, y) \mid \exists s_1, s_2, \ldots, s_{n-1} \in A$ a.î. $x \rho s_1, s_1 \rho s_2, \ldots,$
$s_{n-1} \rho y\}$

20. A infinită, $\mathcal{F} = \{ g : A \to A \}$

$$f \sim g \Leftrightarrow D_{fg} = \{ a \in A \mid f(a) \neq g(a) \} \text{ finită.}$$

- $f \sim f \Leftrightarrow \underbrace{D_{ff}}_{=\emptyset} = \{ a \in A \mid f(a) \neq f(a) \}$ finită.

- $f \sim g \Rightarrow g \sim f$

$$D_{gf} = \{ a \in A \mid g(a) \neq f(a) \} = D_{fg} \text{ finită.}$$

- $\left. \begin{array}{l} f \sim g \\ g \sim h \end{array} \right| \overset{?}{\Rightarrow} f \sim h$ $\qquad$ $f(a) \neq g(a)$ finită, $g(a) \neq h(a)$ finită

$? \; D_{fh} = \{ a \in A \mid f(a) \neq h(a) \}$ finită.

$\exists$ o inf. de pct. din A a.î. care f și g coincid

$\exists$ o inf. de pct. de A a.î. care g și h coincid

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

fie $a \in A$,

$$\cancel{C_A X \cap C_A Y \supseteq C_A(\ldots), Z = \{}$$

$$\underset{\{ a \in A \mid f(a) \neq h(a) \}}{\overset{}{Z}} \subseteq X \cup Y \Rightarrow |Z| \leq |X \cup Y| \leq |X| + |Y| \Rightarrow$$

---

t: ex. 1) Aflați nr. rel. de echiv. pe $|A| = n$

2) $M = M_1 \times \ldots \times M_n$

ρ_i rel. de echiv. pe M_i, $i = \overline{1,n}$

Def. ρ o rel. de echiv. pe M a.î. M/ρ bij. $M_1/\rho_1 \times \ldots \times M_n/\rho_n$.

3) $\emptyset \neq B \subseteq A$

$\mathcal{P}(A)$, $X \rho Y \Leftrightarrow X \cap B = Y \cap B$.

$\mathcal{P}(A)/\rho$ în bij. cu $\mathcal{P}(B)$

27. $f: \mathbb{Z}_n \to \mathbb{C}$, $f(\hat{k}) = i^k$ bine-definită. n?

$n = 4h \Rightarrow$

$\hat{k} = \hat{l} \Rightarrow f(\hat{k}) = f(\hat{l}) \Leftrightarrow i^k = i^l \Leftrightarrow 4 / k-l$.

$4 / 4h / k-l$ $\qquad\qquad i^{k-l} = 1$

$n = 4k + r$, $r > 0$

$f(\hat{0}) = i^0 = 1$

$f(\hat{n}) = i^{4k+r} = (i^{4k}) \cdot i^r = i^r$, $r \neq 0 \Rightarrow i^r \neq 1$.

21. $z \sim w \Leftrightarrow z, w, 0$ col. $\Rightarrow \exists \lambda \in \mathbb{R}^*$ a.î. $z_2 = \lambda \cdot z_1$

Refl.: $z \sim z \Leftrightarrow 0, z$ col.

Sim.: $z_1 \sim z_2 \Rightarrow z_2 \sim z_1$

$\Downarrow$

$0, z_1, z_2$ col.

Tranz.: $z_1 \sim z_2$ și $z_2 \sim z_3 \Rightarrow z_1 \sim z_3$ col.

Clasele de echiv. $\hat{z} = \{x \mid x \in \mathbb{C}^*, x, 0$ și z col.$\}$

Sist. de repr.: Semicerc deschis la un capăt

22. $z_1 \sim z_2 \Leftrightarrow z_1 - z_2 \in \mathbb{R}$

reflex.: $z_1 \sim z_1 \Rightarrow 0 \in \mathbb{R}$

sim.: $z_1 \sim z_2 \Leftrightarrow z_1 - z_2 \in \mathbb{R} \Rightarrow z_2 - z_1 \in \mathbb{R} \Rightarrow z_2 \sim z_1$

tranz.: $\left.\begin{array}{l} z_1 \sim z_2 \Leftrightarrow z_1 - z_2 \in \mathbb{R} \\ z_2 \sim z_3 \Leftrightarrow z_2 - z_3 \in \mathbb{R} \end{array}\right\} \Rightarrow z_1 \sim z_3 \in \mathbb{R}$.

Clase de echiv.: $\hat{z}$: dreapta paralelă cu Ox și care trece prin afixul lui z.

sistem de repr.:

t: ex. 23, 24 x

de la op. algebrice pg. 34 ex. 39, 28, 35, 36, 41

4) ex. de diagrame

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "g"'] & B \arrow[d, "h"] \\ & C \end{tikzcd}$$

$\exists h$: și $h \circ f = g$.

5) $(\mathbb{N}^*, \cdot) \simeq (M_2, \cdot)$

$$M_2 = \{2k+1 \mid k \in \mathbb{N}\}$$

6) $M_3 = \{3k+1 \mid k \in \mathbb{N}\}$

$M_5 = \{5k+1 \mid k \in \mathbb{N}\}$

$(\mathbb{N}^*, \cdot), (M_3, \cdot), (M_5, \cdot)$ nu sunt izomorfi, oricare doi.

$\hat{a} = [a] = \{b \in A \mid b \rho a\}$ - clasa de echivalență a lui a

$f : A \to B$, $\quad a \rho_f a' \Leftrightarrow f(a) = f(a')$.

$A/\rho_f = \{f^{-1}(b) \mid b \in \operatorname{Im} f\}$

$\hat{a} = \{a' \in A \mid a' \rho_f a, \; f(a') = f(a)\}$.

$f^{-1}(b)$ ($b \in \operatorname{Im} f$).

Th. (Prop. de universalitate a mulț. factor)

ρ rel. de echiv. pe A. $f : A \to B$, cu ρ_f

$$\begin{tikzcd} A \arrow[r, "p"] \arrow[dr, "f"'] & A/\rho \arrow[d, "\bar{f}"] \\ & B \end{tikzcd}$$

$\rho \subseteq \rho_f \Rightarrow \exists\, \bar{f} : A/\rho \to B$ a.î. $\bar{f} \circ p = f$.

1) $\bar{f}$ inj. $\Leftrightarrow \rho = \rho_f$

2) $\bar{f}$ surj. $\Leftrightarrow f$ surj.

$\bar{f} : A/\rho \to B$, $\bar{f}([a]) = f(a)$.

$\bar{f}$ bine definită: $[a] = [b] \Rightarrow a \rho b$, dar $\rho \subseteq \rho_f$ $\Big| \Rightarrow a \rho_f b \Rightarrow f(a) = f(b)$.

$\bar{f}(p(a)) = f(a)$ $\forall a \in A$. $\bar{f}$ unică

1) $\bar{f}$ inj. $\Leftrightarrow$ $\bar{f}([a]) = \bar{f}([b]) \Rightarrow [a] = [b]$.

$\Updownarrow$

$f(a) = f(b) \Leftrightarrow a \rho_f b$

$a \rho_f b \Rightarrow a \rho b \Rightarrow \rho_f \subseteq \rho$, $\rho \subseteq \rho_f$ $\Big| \Rightarrow \rho = \rho_f$

2) $\operatorname{Im} \bar{f} = \operatorname{Im} f$.

1) Nr. rel. de echiv. pe A, cu $|A| = n$

(ex. 22)

A/ρ este o partiție a lui A pt. orice ρ rel. de echiv. pe A

$a \rho b \Rightarrow b \in \hat{a}$ $(b \in A_i)$

Reciproc, definim $a \sim b \Leftrightarrow \exists\, i \in I$ a.î. $a, b \in A_i$

Fie $M = \{\rho \,/\, \rho$ rel. de echivalență pe $A\}$.

Arăt că $\exists\, f :$ ~~M~~ mulț. partițiilor lui $A \longrightarrow M$.

$\cancel{\{A_i\}_i}$ $\{A_{i_1}, A_{i_2}, \dots, A_{i_k}\}$

Fie $f(\{A_i\}) = \sim$, unde A_i e o ~~mulțime (din partiția lui A)~~ partiție

$a \sim b \Leftrightarrow a, b \in A_i$.

$f(\{A_i\}) = f(\{A_j\}) \Rightarrow$ se obț. aceeași partiție $\Rightarrow$ f inj.

f surj.: pp. că $\exists \sim$ rel. de echiv. ce poate fi definită pe A.

Cum aceasta dă naștere unei partiții, înseamnă că acesteia îi va corespunde respectiva rel. de echiv.

$\Rightarrow$ f bij., $f^{-1}(\rho) = \{\hat{a}\}$.

nr. rel. de echiv. = Bell(n)

$$B_{n+1} = B_n + C_n^1 \cdot B_{n-1} + C_n^2 \cdot B_{n-2} + \dots + C_n^{n-1} \cdot B_1$$

$$B_{n+1} = \sum_{k=0}^{n} C_n^k \cdot B_k, \text{ cu } B_0 = 1,\ B_1 = 1,\ B_2 = 2,\ B_3 = 5 \dots$$

$$B_3 = B_2 + C_2^1 \cdot B_1 + C_2^2 \cdot B_0 =$$

$$= 2 + 2 \cdot 1 + 1 = 5$$

Pf

(20) ρ rel. binară pe M. $\Delta_M = \{(x,x) \mid x \in M\}$

$\rho^{-1} = \{(x,y) \mid y \rho x\}$

$\rho^n = \{(x,y) \mid \exists\, a_1, a_2, \dots, a_{n-1} \in M$ a.î. $x \rho a_1, a_1 \rho a_2, \dots, a_{n-1} \rho y\}$.

$\rho' = \Delta_M \cup (\rho \cup \rho^{-1}) \cup (\rho \cup \rho^{-1})^2 \cup \dots$

ρ': cea mai mică rel. de echiv. pe M, $\underline{\rho \subseteq \rho'}$

Dacă $(x,y) \in \rho' \Rightarrow$? ~~$x,y \in$~~ $\exists\, k \in \mathbb{N}^*$ a.î. $(x,y) \in (\rho \cup \rho^{-1})^k$.

Evident, $\underline{\rho' \text{ reflexivă}}$, căci $\Delta_M = \{(x,x) \mid x \in M\}$.

ρ' ~~reflex~~ simetrică: $(x,y) \in \rho' \Rightarrow (y,x) \in \rho'$

$(x,y) \in (\rho \cup \rho^{-1})^k \Rightarrow \exists\, a_1, a_2, \dots, a_{k-1} \in M$ a.î.

$(x, a_1) \in \rho \cup \rho^{-1}, (a_1, a_2) \in \rho \cup \rho^{-1}, \dots, (a_{k-1}, y) \in \rho \cup \rho^{-1}$.

~~Dacă $(x, a_1) \in \rho$~~

Dacă $(a_i, a_{i+1}) \in \rho \cup \rho^{-1} \Leftrightarrow (a_{i+1}, a_i) \in \rho \cup \rho^{-1}$

(dacă $(a_i, a_{i+1}) \in \rho \Rightarrow (a_{i+1}, a_i) \in \rho^{-1}$ și reciproc)

$\Rightarrow (y, a_{k-1}) \in \rho \cup \rho^{-1}, (a_{k-1}, a_{k-2}) \in \rho \cup \rho^{-1}, \dots,$

$(a_1, x) \in \rho \cup \rho^{-1} \Rightarrow (y,x) \in (\rho \cup \rho^{-1})^k \Rightarrow$

$\Rightarrow (y,x) \in \rho'$.

$\Rightarrow$ $\underline{\rho' \text{ simetrică}}$.

Fie $(x,y) \in \rho'$ și $(y,z) \in \rho' \Rightarrow (x,y) \in (\rho \cup \rho^{-1})^m$ și

$(y,z) \in (\rho \cup \rho^{-1})^n \Rightarrow \exists\, a_1, a_2, \dots, a_{m-1}, a'_1, a'_2, \dots, a'_{n-1}$ a.î.

$(x, a_1) \in \rho \cup \rho^{-1}, (a_1, a_2) \in \rho \cup \rho^{-1}, (a_2, a_3) \in \rho \cup \rho^{-1}, \dots$

$(a_{m-1}, y) \in \rho \cup \rho^{-1}, (y, a'_1) \in \rho \cup \rho^{-1}, \dots, (a'_{n-1}, z) \in \rho \cup \rho^{-1}$

$\Rightarrow (x,z) \in (\rho \cup \rho^{-1})^{m+n} \Rightarrow (x,z) \in \rho' \Rightarrow$

$\Rightarrow$ $\underline{\rho' \text{ tranzitivă}}$.

Fie R o rel. de echivalență ce o conține pe ρ. $\rho' \subseteq R$.

~~R tranzitivă $\Rightarrow$ R^n~~ Evident, $\rho^{-1} \subseteq R$ și $\Delta_M \subseteq R$.

arăt că $(\rho \cup \rho^{-1})^k \subseteq R, \forall k \in \mathbb{N}^*$.

fie $(x, y) \in (\rho \cup \rho^{-1})^k$, arbitrar, deci $\exists a_1, a_2, \dots, a_{k-1}$ a.î.

$(x, a_1) \in \rho \cup \rho^{-1}$, dar $\rho \cup \rho^{-1} \subseteq R \Rightarrow (x, a_1) \in R$

analog, $(a_1, a_2) \in R, \dots, (a_{k-1}, y) \in R$ $\Bigg\} \Rightarrow$

$\Rightarrow$ iterativ, $(x, y) \in R$.

Așadar, $\rho' = \Delta_M \cup (\rho \cup \rho^{-1}) \cup \dots \cup (\rho \cup \rho^{-1})^k \subseteq R \Rightarrow$

$\Rightarrow \rho'$ rel. de echiv. minimă cu ac. prop.

(21) ρ_i rel. de echiv. pe M_i, $i = \overline{1,n}$

$M = M_1 \times M_2 \times \dots \times M_n$

$(x_1, x_2, \dots, x_n) \, \rho \, (y_1, y_2, \dots, y_n) \Leftrightarrow x_i \rho_i y_i$

ρ rel. de echiv. pe M: evident $(x_1, \dots, x_n) \rho (x_1, \dots, x_n)$,

căci $x_i \rho x_i$, $i = \overline{1,n}$ $\Rightarrow$ $\underline{\rho \text{ refl.}}$

dacă $(x_1, \dots, x_n) \rho (y_1, \dots, y_n) \Rightarrow x_i \rho_i y_i \overset{\rho_i \text{ rel. de echiv.}}{\Rightarrow} y_i \rho_i x_i$

$\Rightarrow (y_1, \dots, y_n) \rho (x_1, \dots, x_n) \Rightarrow \underline{\rho \text{ sim.}}$

dacă $(x_1, \dots, x_n) \rho (y_1, \dots, y_n)$ și $(y_1, \dots, y_n) \rho (z_1, \dots, z_n)$

$\Rightarrow x_i \rho_i y_i$ și $y_i \rho_i z_i \Rightarrow x_i \rho_i z_i \Rightarrow$

$\Rightarrow (x_1, \dots, x_n) \rho (z_1, \dots z_n) \Rightarrow \underline{\rho \text{ tranz.}}$

$\Rightarrow \rho$ rel. de echiv. pe M.

$\exists f : M/\rho \to M_1/\rho_1 \times \dots \times M_n/\rho_n$, f bij.

~~$M/\rho = \{ m$~~ fie $\hat{m} \in M/\rho$, $\hat{m} = \{ b \in M / b \rho m \}$.

fie $m = (x_1, \dots, x_n)$. $b \rho m \Rightarrow b_i \rho_i x_i$, cu

$b = (b_1, \dots, b_n)$.

$f(\hat{m}) = (\hat{l}_1, \hat{l}_2, \dots, \hat{l}_n)$.

pt. Dacă $l \, \rho \, m$ şi $l' \, \rho \, m \Rightarrow l \, \rho \, l' \Rightarrow$

$l_i \, \rho \, l_i' \Rightarrow l_i' \in \hat{l}_i$.

$f(\hat{m}_1) = f(\hat{m}_2) = (\hat{l}_1, \hat{l}_2, \dots, \hat{l}_n) \Rightarrow$

$\Rightarrow l_i \, \rho_i \, x_i$ şi $l_i \, \rho_i \, x_i'$, unde x_i sunt comp. din m şi x_i' din $m_2 \Rightarrow x_i \, \rho_i \, x_i'$, $i = \overline{1,n} \Rightarrow m_1 \, \rho \, m_2 \Rightarrow$

$\Rightarrow \hat{m}_1 = \hat{m}_2 \Rightarrow$ $\underline{f \text{ injectivă}}$. (1)

$\forall \, (\hat{l}_1, \hat{l}_2, \dots, \hat{l}_n) \in M_1/\rho_1 \times \dots \times M_n/\rho_n$, $\exists$

$\hat{l} = (l_1, l_2, \dots, l_n) \in M/\rho$ a.î. $f(\hat{l}) = (\hat{l}_1, \hat{l}_2, \dots, \hat{l}_n)$

$\Rightarrow$ $\underline{f \text{ surj.}}$

$\overset{(1)(2)}{\Rightarrow} f$ bijectivă.

(23) A, $B \subseteq A$, ρ rel. pe $P(A)$ a.î.:

$X \, \rho \, Y \Leftrightarrow X \cap B = Y \cap B$

$\Rightarrow \rho$ rel. de echiv. pe $P(A)$:

$X \cap B = X \cap B$ (evident) $\Rightarrow \rho$ refl.

$X \rho Y \Rightarrow X \cap B = Y \cap B \overset{X \leftrightarrow Y}{\Rightarrow} Y \, \rho \, X \Rightarrow \rho$ simetr.

$\left.\begin{array}{l} X \, \rho \, Y \Rightarrow X \cap B = Y \cap B \\ Y \, \rho \, Z \Rightarrow Y \cap B = Z \cap B \end{array}\right| \Rightarrow X \cap B = Z \cap B \Rightarrow X \, \rho \, Z \Rightarrow \rho$ tranz.

$P(A) / \rho$ în bijecţie cu $P(B)$

Fie $\hat{S} \in P(A)/\rho$, $\hat{S} = \{ M \in P(A) \mid M \, \rho \, S \} =$

$= \{ M \in P(A) \mid M \cap B = S \cap B \}$

$f(\hat{S}) = S \cap B \in P(B)$. se dem. imediat că f inj şi surj.

(25) i) $(\mathbb{N}^*, \cdot) \cong (M_2, \cdot)$

$\cancel{2^{\frac{1}{2}(x+y)}+1}$

$\cancel{2x}$

$\cancel{f(n) = 2}$

$$\begin{cases} f(x\cdot y) = f(x)\cdot f(y) \\ f(1) = 1 \end{cases}$$

$$f(x) = 2\left[\frac{x}{2}\right] + 1.$$

3 5

f 7 5

$\cancel{1\ 2\ 3\ 4\ 5}$

$\cancel{1\ 3\ 5}$

$$f(1) = 1, \quad f(2) = 3$$

$$f(xy) = 2\left[\frac{xy}{2}\right] + 1.$$

$$f(x)\cdot f(y) = \left(2\left[\frac{x}{2}\right]+1\right)\left(2\left[\frac{y}{2}\right]+1\right) =$$

$$= 4\left[\frac{xy}{4}\right] + 1 + 2\left[\frac{x}{2}\right] + 2\left[\frac{y}{2}\right].$$

$$\left[\frac{xy}{2}\right] = 2\left[\frac{xy}{4}\right] + \left[\frac{x}{2}\right] + \left[\frac{y}{2}\right].$$

x, y

Coroolar de matrici: $f : \mathbb{N}^* \to M_2$ dacă $g : M_2 \to \mathbb{N}$ a.î. $f \circ g = 1_{M_2}$ și $g \circ f = 1_{\mathbb{N}}$. $\to f$ bijectivă

$$f(x) = \begin{cases} x, & x \text{ impar} \\ x \end{cases}$$

$\cancel{f(x) = 2^x - 1}$ $\quad \cancel{f(n) = \begin{cases} \frac{n+1}{n}, & n \text{ par} \\ 2\ldots, & n \text{ impar} \end{cases}}$ $\quad \cancel{f(n) =}$

$\cancel{f(2)}$

$\cancel{n \to 2n-1}$

$$f(1) = 1, \quad f(2) = 1, \quad f(3) = \qquad f(n) = \begin{cases} \quad , & n \text{ par} \\ \frac{n+1}{2}, & n \text{ impar} \end{cases}$$

$\cancel{g : (2n+1, \cdot) \to (\mathbb{N}^*, \cdot) \text{ bijectivă}}$.

$\cancel{f(n) = (-1)^n\left(\frac{n}{2} + \frac{1}{4}\right) - \frac{1}{4} + (-1)^n \cdot \frac{1}{4}}$

$\cancel{f(1) = -\left(\frac{1}{2} + \frac{1}{4}\right) - \frac{1}{4}\ 1.}$ $\quad \cancel{1 + \frac{1}{4}}$

$\cancel{f(2) = 1 + \frac{1}{4} - \frac{1}{4} = 1.}$

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

$$f(1) = 1, \quad f(2) = -$$

ex. 41: Atomul unui monoid: un el. neinversabil a care nu se poate scrie ca

? produsul / compunerea a 2 el. neinversabile.

~~ex. 43~~: Atomii lui $(\mathbb{N}^n, +)$ - monoid:

$$(a_1, a_2, \dots, a_n) = (a_1, \dots, a_i - 1, \dots, a_n) + (a_1, a_2, \dots, \cancel{a_j}, \dots, a_j - 1, \dots, a_n)$$

dacă $\exists\, i$ și j a.î. $a_i \geq 1, a_j \geq 1$, at. are loc egalitatea de mai sus,

căci orice n-uplu ce-l conține pe 1 est neinversabil ⇒

⇒ atomii au doar un element de 1:

$(1, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, 0, \dots, 0, 1)$. (n el)

$(\mathbb{N}^m, +) \cong (\mathbb{N}^n, +) \iff m = n$.

$f: \mathbb{N}^m \longrightarrow \mathbb{N}^n$, $f(x+y) = f(x) + f(y)$ și $f(0_m) = 0_n$.

dacă x, y neinversabile, at. $f(x)$ $x \neq 0_m, y \neq 0_m$ ⇒

⇒ $f(x) \neq 0_n, f(y) \neq 0_n$ ⇒ $f(x+y)$ ~~neinversabil~~ nu este atom

~~f(x~~ $f(x)$ și $f(y)$ neinversabile, $\forall\, x, y \in \mathbb{N}^m \setminus 0_m$ ⇒

cum însă f bijectivă ⇒ ~~x și f(x) au~~

dacă x este atom, atunci, ~~f(x)~~ dacă $f(x)$ nu ar fi atom,

ar $\exists\, y$ și $z \in \mathbb{N}^m$ a.î. $f(x) = f(y) + f(z)$, căci f bijectivă,

y și z nenule ⇒ $x = y + z$ ⇒ x nu este atom. abs

⇒ dacă x e atom și $f(x)$ este atom.

Analog și reciproca. Dacă $f(x)$ e atom și pp. că x nu e atom ⇒ $x = y + z$, y, z nenule. $f(x) = f(y+z) = f(y) + f(z)$,

cu $f(y), f(z)$ nenule ⇒ $f(x)$ nu e atom. abs

⇒ 2 monoizi izomorfi au ac. nr. de atomi.

dar nr. de atomi ai lui $\mathbb{N}^n$ este n ⇒ $m = n$ și reciproc.

ex. 45 : $(M_2, \cdot) \not\cong (M_3, \cdot)$

~~nr. de~~ atomii ~~ai~~ lui M_2 : nr. prime impare

atomii lui M_3 : nr. prime de forma $3k+1$ și cele de forma pq, unde p și q sunt nr. prime de forma $3k+2$.

~~$f(xy) = p \cdot q$ $f(x) \cdot f(y) = p \cdot q$~~

$55^2 = \underbrace{25}_{5\cdot 5} \cdot \underbrace{121}_{11 \cdot 11}$ 55 este atom în M_3

$f(55^2) = f(55) \cdot f(55) = \cancel{f(5) \cdot f(11)} = f(25) \cdot f(121)$.

$f : M_3 \longrightarrow M_2$.

$55, \cancel{5}, \cancel{11}, 25, 121$ atomi $\Rightarrow$ $f(55), f(25), f(121)$ atomi

$A_1^2 = A_2 \cdot A_3$, A_1, A_2, A_3 nr. prime impare $\Rightarrow$

$\Rightarrow A_1 = A_2 = A_3$ $\Rightarrow$ f nu e bijectivă.

25 : $(M_3, \cdot) \not\cong (M_5, \cdot)$ morfismi

atomii lui M_3 : nr prime de forma $3k+1$ și cele $p \cdot q$, cu p, q prime de forma $3k+2$.

atomii lui M_5 : nr. prime de forma $5k+1$, cele $p \cdot q$, cu p, q prime de forma $5k+4$.

analog, vom obține $A_1^2 = A_2 \cdot A_3$, A_1, A_2, A_3 de forma de mai sus.

(23) $H = \{ f \mid f : A \to A \}$

$f \sim g \iff \exists\, u \in H$ bijectivă a.î. $fu = ug$.

$\sim$ rel. de echivalență

$\sim$ reflexivă: $\exists\, 1_H \in H$ bij. a.î. $f = f 1_H = 1_H \circ f = f$.

$\sim$ sim.: $f \sim g \Rightarrow \exists\, u$ bij. a.î. $fu = ug \,/\, u^{-1} \Rightarrow f = ugu^{-1} \Rightarrow$

$\Rightarrow u^{-1} f = g u^{-1}$, u^{-1} bijectivă $\Rightarrow g \sim f$.

$\sim$ tranz.: $f \sim g \Rightarrow \exists\, u$ bij. a.î. $fu = ug$, $g \sim t \Rightarrow \exists\, i$ bij. a.î. $gi = it$ $\Rightarrow$

~~$\Rightarrow f = ugu^{-1} \Rightarrow fi = ugu^{-1}i$~~ $\Rightarrow$

~~$it = ugu^{-1}i \Rightarrow iti^{-1}$~~ $= ugu^{-1} \Rightarrow$

~~$\Rightarrow fui =$~~ $f(ui) = ugi = (ui)t$,

ui bijectivă $\Rightarrow f \sim t \Rightarrow \sim$ rel. de echiv.

$f = ugu^{-1}$ (autom. interior)

$f = \varphi_u(g)$

$\hat{f} = \{ u f u^{-1} \mid u \in S(M) \}$

(24) construcția lui $\mathbb{Z}$: $\sim$ rel. pe $\mathbb{N} \times \mathbb{N}$ a.î. $(a,b) \sim (c,d)$, dacă $a + d = b + c$. $\mathbb{N} \times \mathbb{N} / \sim \;\cong \mathbb{Z}$.

$(a,b) \sim (a,b) \iff a + b = b + a$, adev. $\Rightarrow \sim$ refl.

$\sim$ sim.: $(a,b) \sim (c,d) \Rightarrow a+d = b+c \Rightarrow (c,d) \sim (a,b) \Rightarrow$

$\sim$ tranz.: $(a,b) \sim (c,d) \Rightarrow a + d = b + c$, $(c,d) \sim (e,f) \Rightarrow c + f = d + e$ $\Rightarrow$

$\Rightarrow a + f = a + (d + e - c) = b + e \Rightarrow$

$\Rightarrow (a,b) \sim (e,f)$.

$\mathbb{N} \times \mathbb{N} / \sim$ = mulț. claselor $\widehat{(a,b)} = \{ (c,d) \in \mathbb{N} \times \mathbb{N} \mid (a,b) \sim (c,d) \}$.

$a + d = b + c$

ct. $= a - b = c - d$

Fie $f: \mathbb{N}\times\mathbb{N}/_{\sim} \to \mathbb{Z}$, $f(a,b) = a-b \in \mathbb{Z}$, bine-definită și bijectivă.

(28) $\varphi: \{a_1, a_2, \dots, a_n\} \times \{a_1, \dots, a_n\} \to \{\dots\}$

pt. fiecare ~~d~~ pereche (a_i, a_j) se definește o funcție cu imaginea în $\{a_1, a_2, \dots, a_n\} \Rightarrow n^{n^2}$ operații:

$a * b = b * a$

$$\begin{array}{c|ccccc|} & 1 & 2 & \dots & e & \dots & n \\ \hline 1 & & & & 1 & & \\ 2 & & & & 2 & & \\ \vdots & & & & \vdots & & \\ e & - & - & - & e & - & \\ \vdots & & & & & & \\ n & & & & n & & \\ \hline \end{array}$$

Pt. ca operația să fie comutativă, este necesar și suficient să definim $\varphi(a_i, a_j)$, cu $i \le j$ (inclusiv diagonala)

$\Rightarrow n + \frac{n^2-n}{2} = \frac{n^2+n}{2}$ valori de ales din cele n $\Rightarrow$

$\Rightarrow n^{\frac{n^2+n}{2}}$ operații

Fie $e \in \{a_1, \dots, a_n\}$ el. neutru, fixat. Pt. fiecare (e, a_i) pereche,

$e * a_i = a_i$

~~$\varphi(e, a_i) = \varphi(a_i)$~~. $2n-1$ valori sunt deja fixate de e.

Rămân de luat restul de $n^2 - 2n + 1 = (n-1)^2$ valori, ce pot fi luate în $n^{(n-1)^2}$ (pt. fiec. el. neutru) $\Rightarrow$ în total, $n \cdot n^{(n-1)^2} = n^{(n-1)^2+1}$.

(34) $x * y = x + [y]$ pe $\mathbb{R}$

asociativitate: $x * (y * z) = x + [y * z] = x + [y + [z]] = x + [z] + [y]$.

$(x * y) * z = x + [y] + [z] \Rightarrow *$ asoc.

el. neutru: $x * e = x, \forall x \in \mathbb{R} \Rightarrow x + [e] = x \Rightarrow e = 0$.

$e * x = 0 + [x] = x$ doar pe $\mathbb{Z} \Rightarrow$ fără el. neutru

comutativă: $x * y = y * x \Leftrightarrow x + [y] = y + [x]$, fals. $(x = 0, y = \frac{5}{3})$.

(35) $a, b \neq 0,\ c \in \mathbb{Z}$. $\quad x * y = axy + b(x+y) + c$

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

(A): $x*(y*z) = x*(ayz + b(y+z) + c) =$

$= ax(ayz + b(y+z) + c) + b(x + ayz + b(y+z) + c) +$

$+ c = a^2xyz + abx(y+z) + acx + bx + \cancel{ab}yz + b^2(y+z) +$

$+ bc\cancel{+c}$;

$(x*y)*z = (axy + b(x+y) + c)*z = az(axy + b(\cancel{x+y}) + c) +$

$+ b(\cancel{axy + b(x+y)} \cancel{+c} + z) \cancel{+c}$.

$(x*y)*z - x*(y*z) = acx + bx - b^2x - acz - bz + b^2z =$

$= (x-z)(ac + b - b^2) = 0 \overset{\forall x,y,z \in \mathbb{Z}}{\Leftrightarrow} b = b^2 - ac$.

(N): $\exists e$ a.î. $x * e = x \Leftrightarrow axe + b(x+e) + c = x \Leftrightarrow$

$(ae + b - 1)x + be + c = 0,\ \forall x \in \mathbb{Z} \Rightarrow$

$\Rightarrow \begin{cases} ae + b - 1 = 0 \\ be + c = 0 \end{cases} \Rightarrow ae = 1 + ac - b^2$

$-a \cdot \frac{c}{b} + b - 1 = 0 \Leftrightarrow -ac + b^2 - b = 0$.

$e = -\frac{c}{b} \in \mathbb{Z} \Rightarrow b / c$.

• $a \neq 0$, $\quad M_{a,b,c} \cong M_{a,1,0} \cong K_a = \{am + 1 / m \in \mathbb{Z}\}$.

Fie $d = \frac{c}{b} \in \mathbb{Z}$, $b = 1 - ae = 1 + ad$, $c = \frac{b^2 - b}{a} = \frac{(1+ad)^2 - (1+ad)}{a} =$

$= \frac{\cancel{1} + 2ad + (ad)^2 \cancel{-1} - ad}{a} = d(1 + ad)$.

$x*y = axy + (1+ad)(x+y) + d(1+ad) =$

$= axy + (1+ad)(x + y + d)$.

În $M_{a,1,0}$: $\quad x*y = axy + x + y$.

$f : M_{a,b,c} \longrightarrow M_{a,1,0}$, $f(x) = x + d$.

$$f(x * y) = f(axy + (1+ad)(x+y+d)) =$$
$$= axy + (1+ad)(x+y+d) + d.$$

$$f(x) * f(y) = \cancel{(axy + x + y + d)} (x+d) * (y+d) =$$
$$= a(x+d)(y+d) + x + y + 2d =$$
$$= axy + axd + ayd + ad^2 + x + y + 2d =$$
$$= axy + (1+ad)(x+y+d) + d = f(x*y) \Rightarrow$$

$\Rightarrow f$ morfism. ~~f inj. și f~~ și f, evident, bijectivă.

$g : M_{a,1,0} \longrightarrow K_a$.

$$g(x * y) = g(x) \cdot g(y) \Leftrightarrow$$
$$g(axy + x + y) = g(x) \cdot g(y)$$
$$g(x) = ax + 1$$
$$a(axy + x + y) + 1 = (ax+1)(ay+1)$$
$$a^2xy + ax + ay + 1 = a^2xy + ax + ay + 1$$

(36) $(N, +) \not\cong (N, \text{cmmmc})$

$(N, \max)$

$(N \cup \{\infty\}, \min)$

~~$f(a+a) = \text{cmmmc}(f(a), f(a)) = f(a)$~~

f^{-1} $\quad f(\text{cmmmc}(a,a)) = f(a) + f(a)$

$$f(a) = 2f(a), \ \forall a \in N \text{ n.c. } \Rightarrow f(a) = 0$$
(nu e bij.)

$$\overset{\|}{f(\max(a,a))}$$
$$\|$$
$$f(\min(a,a))$$

$(N, \text{cmmmc}) \not\cong (N, \max)$

$(N \cup \{\infty\}, \min)$

$f(\text{cmmmc}(a,b)) = \max(f(a), f(b))$ $\Big|$ $\Rightarrow$ $\text{cmmmc}(a,b) \in \{a, b\}$

f bij.

$\max(f(a), f(b)) \in \{f(a), f(b)\}$

contraexemplu

cmmmc(a,b)

$(a,b) \neq 1$.

analog pt. min( )

$(N, \max) \not\cong (N \cup \{\infty\}, \min)$

f bij., $f(\min(a,b)) = \max(f(a), f(b)), \in \{f(a), f(b)\} \Rightarrow$

f bij. $\Rightarrow \forall y \in N, \exists \underset{\substack{\text{unic} \\ x \in N \cup \{\infty\}}}{x}$ a.î. $f(x) = y$.

dar $f(y) = f(\min(y, x))$, cu $x \geq y$, care

are o inf. de soluții $\Rightarrow f(y) > f(x)$, $\forall x > y$.

dar $\operatorname{Im} f \subset N$, cu $f(y)$ finită.

(se obține un șir strict descrescător, deci pest un

rang, va fi negativ)

---

t: pg. 18 ex. 5, 19 (pg. 19)

Curs 3

Asociativ. este esențială în unicitatea el. neutru

	e	a	b
e	e	a	b
a	a	e	e
b	b	e	a

a are 2 el. simetrice:

$\mathcal{U}(M) = \{ a \in M \mid a \text{ simetrizabil} \}$.

M monoid $\Rightarrow \mathcal{U}(M)$ grup

$\mathcal{U}(\mathbb{Z}_n) = \{ \hat{a} \in \mathbb{Z}_n \mid \hat{a} \text{ inv.} \} = \{ \hat{a} \in \mathbb{Z}_n \mid (a,n) = 1 \}$

$(\exists)\ \hat{b} \in \mathbb{Z}_n$ a.î. $\hat{a} \cdot \hat{b} = \hat{1}$

dem.: „$\Rightarrow$" $\hat{a} \cdot \hat{b} = 1 \Leftrightarrow \widehat{ab} = \hat{1} \Leftrightarrow n \mid ab - 1$

fie $d \mid (a,n)$ $\qquad$ $\left.\begin{array}{l} n \mid ab-1 \\ d \mid n \end{array}\right| \Rightarrow \left.\begin{array}{l} d \mid ab-1 \\ d \mid ab \end{array}\right| \Rightarrow d \mid 1 \Rightarrow d = 1.$

„$\Leftarrow$" $(a,n) = 1 \Rightarrow \exists k, l \in \mathbb{Z}$ a.î. $ak + nl = 1$ (Euclid)

$\widehat{ak + nl} = \hat{1} \Rightarrow$

$\hat{a} \cdot \hat{k} + \underbrace{\hat{n} \cdot \hat{l}}_{\hat{0}} = \hat{1} \Rightarrow \hat{a} \cdot \hat{k} = \hat{1} \Rightarrow \hat{a}$ inversabil.

$\mathcal{U}(\mathcal{F}(M)) = \{ f : M \to M \mid f \text{ bij.} \}$

Produs direct de monoizi:

$(M_1, \cdot), (M_2, \cdot)$ monoizi

$(M_1 \times M_2, \cdot)$ monoid cu op. alg. $(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_2)$

$e = (e_1, e_2)$

generalizare: $M = \prod_{i \in I} M_i$

$(x_i)_{i \in I} (y_i)_{i \in I} = (x_i y_i)_{i \in I}$

morfism de monoizi: $f : M \to N$, a.î. $\begin{cases} f(xy) = f(x) f(y) \\ f(e) = e' \end{cases}$,

prin inducție, $f(x_1 x_2 \dots x_n) = f(x_1) f(x_2) \dots f(x_n)$

$f(x^n) = (f(x))^n$

$n \in \mathbb{N}$ fixat

$\varphi_n : (\mathbb{N}, +) \to (\mathbb{N}, +)$, $\varphi_n(x) = nx$, $\forall x \in \mathbb{N}$

1) $\underbrace{\varphi_n(x+y)}_{n(x+y)} = \underbrace{\varphi_n(x)}_{nx} + \underbrace{\varphi_n(y)}_{ny}$

2) $\varphi_n(0) = 0$

ex.: ~~Orice~~ $f:(\mathbb{N},+)\to(\mathbb{N},+)$ morfism de monoizi $\overset{\exists\, n\in\mathbb{N}}{\Rightarrow}$ $f=\varphi_n$.

- $g:(\mathcal{P}(M),\cap)\to(\mathcal{P}(M),\cup)$, $g(X)=C_M X$ (izomorfism)

$$g(X\cap Y)=g(X)\cup g(Y)$$
$$\parallel \qquad\qquad \parallel$$
$$C_M(X\cap Y)=C_M X\cup C_M Y \quad \text{(rel. de Morgan)}$$
$$g(M)=C_M M=\emptyset$$

- $p_1: M_1\times M_2\to M_1$

$p_1(x_1,x_2)=x_1$ morf. surj. de monoizi

$p_2: M_1\times M_2\to M_2$

$p_2(x_1,x_2)=x_2$

$s_1: M_1 \to M_1\times M_2$

$s_1(x_1)=(x_1,e_2)$ morf. inj. de monoizi

$s_2: M_2\to M_1\times M_2$

$s_2(x_2)=(x_2,e_2)$

$$\begin{cases} p_1\circ s_1 = \cancel{x}_1 = 1_{M_1}\\ p_2\circ s_2 = 1_{M_2}\end{cases}$$

$f_1: M_1\to N_1$ morf. de mon.

$f_2: M_2\to N_2$

$f_1\times f_2 : M_1\times M_2\to N_1\times N_2$

$(f_1\times f_2)(x_1,x_2)=(f_1(x_1),f_2(x_2))$

$(\mathbb{Z},\cdot)\to(\mathbb{Z},\cdot)\times(\mathbb{Z},\cdot)$

1) $f(x)=(x,0)$

$f(xy)=f(x)\cdot f(y)$

$(xy,0)$

2) $f(n)$!

$f:(\mathcal{P}(M),\cup) \longrightarrow (\mathcal{P}(M),\cap)$

$f(Y) = C_M Y$. (involuție)

$L(A)$: mulț. cuv. din A $\longrightarrow$ monoidul liber generat de mulț. A

$\alpha\beta = a_1 a_2 \dots a_n b_1 b_2 \dots b_n$

$$\begin{tikzcd} A \arrow[r, "i_A"] \arrow[dr, "f"'] & L(A) \arrow[d, dashed, "\exists \bar{f}"] \\ & (M,\cdot) \end{tikzcd}$$

$i_A(a) = a$.

$\exists \bar{f}$ morfism de monoizi unic cu prop. $\bar{f}\circ i_A = f$. $\square$

$\bar{f}(a_1 \dots a_n) = f(a_1)\cdot \ldots \cdot f(a_n)$

$(M,\cdot)$ monoid (comut.) $\Rightarrow$ $(\mathcal{U}(M),\cdot)$ grup (comut.)

$x,y \in \mathcal{U}(M) \Rightarrow xy \in \mathcal{U}(M)$

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

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

$\mathcal{U}(\mathbb{Z}_8) = \{\hat{1},\hat{3},\hat{5},\hat{7}\} \simeq$ gr. lui Klein

$\mathcal{U}((\mathbb{R},\cdot)) = (\mathbb{R}^*,\cdot)$

$(\mathcal{U}(\mathcal{F}(M)),\circ) \overset{not.}{=} (S(M),\circ)$

mulț. funcț. bij.

pt. $M = \{1,2,\dots,n\}$

$(S_n,\cdot)$

$U_n = \{z\in\mathbb{C} \mid z^n = 1,\ n\in\mathbb{N}^*\} \simeq (\mathbb{Z}_n,+)$

$M_{1,2}$ monoizi $\Rightarrow$ $\mathcal{U}(M_1\times M_2) = \mathcal{U}(M_1)\times\mathcal{U}(M_2)$

$f(x^{-1}) = (f(x))^{-1}$, $\forall x\in G$.

$\varphi_n : (\mathbb{Z},+) \to (\mathbb{Z},+)$

$\varphi_n(x) = nx$

endomorfism

$(G,\cdot)$ grup, $a \in G$ fixat

$\varphi_a : G \to G$, $\varphi_a(x) = axa^{-1}$

φ_a automorfism.

$\varphi_a(xy) = \varphi_a(x) \cdot \varphi_a(y)$

$a(xy)a^{-1} = axa^{-1} \cdot aya^{-1}$

$\varphi_a \circ \varphi_{a^{-1}} = 1_G$ $\Rightarrow$ φ_a automorfism.

$\varphi_{a^{-1}} \circ \varphi_a = 1_G$

$(\varphi_a \circ \varphi_b)(x) = \varphi_a(bxb^{-1}) = abxb^{-1}a^{-1} = abx(ab)^{-1} =$

$= \varphi_{ab}(x)$.

$N \subset M$, $F : S(N) \to S(M)$

$$F(f(x)) = \begin{cases} f(x), & x \in N \\ x, & x \in M \setminus N \end{cases}$$

$f \in S(N)$

$f : N \to N$ bij.

Th. Cayley: $\exists$ un morfism inj. de grupuri de la G în $S(G)$.

$G \cong f(G) \subseteq S(G)$

$f : G \to S(G)$ $\quad$ $f(x) : G \to G$

pt. $x \in G$, $f(x) = t_x$, $\quad$ $f(x)(y) = xy$

$t_x(g) = xg, \forall g \in G$ $\quad$ (omotetie de repart.)

(2') $\mathbb{N} \xrightarrow[n \to (n,0)]{i} \mathbb{N}\times\mathbb{N} \xrightarrow{p} \mathbb{N}\times\mathbb{N}/_\sim$

$(a,b) \longrightarrow \widehat{(a,b)}$

$p\circ i(m) = p\circ i(n)$

$\widehat{(m,0)} = \widehat{(n,0)} \Rightarrow m+0 = n+0 \Rightarrow m=n \Rightarrow$

$p\circ i$ injectivă.

$\mathbb{Z} = \mathbb{N}\times\mathbb{N}/_\sim$

$\widehat{(a,b)} + \widehat{(c,d)} = \widehat{(0,0)}$

$\widehat{(n,0)} + \widehat{(0,n)} = \widehat{(n,n)} = \widehat{(0,0)}$

$\widehat{(a,b)} = \begin{cases} \widehat{(n,0)} & a+0 = b+n \quad a \geq b \\ \widehat{(0,n)} & a+n = b+0 \quad b \geq a \end{cases}$

---

(5) $(\mathbb{Z},+), (\mathbb{Q},+), (\mathbb{R},+), (\mathbb{C},+), (\mathbb{Q}^*,\cdot), (\mathbb{R}^*,\cdot), (\mathbb{C}^*,\cdot), (\mathbb{Q}^*_+,\cdot), (\mathbb{R}^*_+,\cdot)$

- pp. că $\exists\, f: \mathbb{Z} \to \mathbb{Q}$, $f(x)+f(y) = f(x+y)$, $\forall\, x,y \in \mathbb{Z}$, f bij.

  $1 \in \mathbb{Z} \Rightarrow f(1) \in \mathbb{Q}$. not. $f(1) = b \Rightarrow f(1) = \frac{b}{2} + \frac{b}{2}$.

  ~~pp. că $\exists$~~ f bij. $\Rightarrow \exists\, a \in \mathbb{Z}$ a.î. $f(a) = \frac{b}{2}$ $\Big| \Rightarrow f(a)+f(a) = f(1) \Rightarrow$

  $\Rightarrow f(a+a) = f(a)+f(a) = f(1) \Rightarrow 2a = 1 \Rightarrow a = \frac{1}{2} \notin \mathbb{Z}$.

- $\mathbb{Z}$ nu poate fi izomorf cu $(\mathbb{R},+), (\mathbb{C},+), (\mathbb{R}^*,\cdot), (\mathbb{C}^*,\cdot), (\mathbb{R}^*_+,\cdot)$, deoarece nu se poate stabili o bijecție între ele, ultimele fiind nenumărabile.

- $\mathbb{Q}$ nu poate fi izomorf cu — // —

- pp. că $(\mathbb{R}^*,\cdot) \simeq (\mathbb{C}^*,\cdot)$. $\varphi: \mathbb{C}^* \to \mathbb{R}^*$, φ izomorfism $\Rightarrow$

  $\Rightarrow \varphi(e_{(\mathbb{C},\cdot)}) = e_{(\mathbb{R},\cdot)} \Rightarrow \varphi(1) = 1$.

  $1 = \varphi(1) = \varphi((-1)\cdot(-1)) = \varphi(-1)\cdot\varphi(-1) = \varphi^2(-1)$, $\varphi(1)=1$, $\varphi(-1) \in \mathbb{R}$, φ bij. $\Big| \Rightarrow \varphi(-1) = -1$.

  $-1 = \varphi(-1) = \varphi(i^2) = \varphi^2(i)$, cu $\varphi(i) \in \mathbb{R}$. m.c.

· pp. $(\mathbb{Q},+) \simeq (\mathbb{Q}^*,\cdot)$

în $(\mathbb{Q}^*,\cdot)$, $\exists$ -1 element de ordinul 2.

în $(\mathbb{Q},+)$, $a+a=0 \Rightarrow a=0$, $\mathrm{ord}(0)=1 \Rightarrow \nexists$ element de ordin 2.

$f(-1)+f(-1)=f(1)=0 \Rightarrow f(-1)=0=f(1)$ .n.c.

$N(t)=N_0\, e^{-\lambda t}$

$t_{1/2}=\frac{\ln 2}{\lambda}$

· pp. $(\mathbb{Q},+) \simeq (\mathbb{Q}_+^*,\cdot)$

fie $\phi:(\mathbb{Q},+)\longrightarrow(\mathbb{Q}_+^*,\cdot)$ izomorfism

f surj. $\Rightarrow \exists\, r\in\mathbb{Q}$ a.î. $\phi(r)=2 \Rightarrow \frac{r}{2}\in\mathbb{Q}$.

$2=\phi(r)=\phi\left(\frac{r}{2}+\frac{r}{2}\right)=\phi\left(\frac{r}{2}\right)\cdot\phi\left(\frac{r}{2}\right)=\phi^2\left(\frac{r}{2}\right)\in\mathbb{Q}_+^* \Rightarrow$

$\Rightarrow \phi\left(\frac{r}{2}\right)=\sqrt{2}\notin\mathbb{Q}_+^*$.

· pp. $(\mathbb{R},+) \simeq (\mathbb{R}_+^*,\cdot)$

$\exp:\mathbb{R}\to\mathbb{R}_+^*$, $\exp(x)=e^x$

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

$e^{x+y}=e^x\cdot e^y$

exp este inj.

surj.: $\forall\, y\in\mathbb{R}_+^*, \exists\, \ln y\in\mathbb{R}$ a.î. $e^{\ln y}=y$.

izomorfism invers este log.

· ~~(R~~

· $(\mathbb{R},+) \simeq (\mathbb{C},+)$

$\cdot\ (\mathbb{R},+) \not\cong (\mathbb{R}^*,\cdot)$

divizibil — nu este divizibil

(Ti 2.)

$(G,+)$ divizibil : $\forall g \in G,\ \forall n \in \mathbb{N}^*,\ \exists x \in G$ a.î. $nx = g$.

$(\mathbb{R},+)$ divizibil ;

$(G,\cdot)$ divizibil : $\forall g \in G,\ \forall n \in \mathbb{N}^*,\ \exists x \in G$ a.î. $x^n = g$.

$(\mathbb{R}^*,\cdot)$ nedivizibil : pt. n par nu

$\cdot\ (\mathbb{C},+) \not\cong (\mathbb{C}^*,\cdot)$

(19) $x^2 = e,\ \forall x \in G$

$x, y \in G \Rightarrow xy \in G$. $(xy)^2 = e \Rightarrow (xy)^{-1} = xy$.

$$(xy)^{-1} = y^{-1}\cdot x^{-1} \underset{x^2, y^2 = e}{=} yx = xy.$$

pp. că ord G nu este o putere a lui 2.

fie p prim, $p \mid \operatorname{ord} G$. Din th. lui Cauchy, $\exists a \in G$, cu $\operatorname{ord}(a) = p$! $(p \geq 3)$

$\left.\begin{matrix} a^p = e \\ a^2 = e \end{matrix}\right| \Rightarrow a^{(p,2)} = a^1 = e$. m.c.

Introducem o structură de spațiu vectorial peste $\mathbb{Z}_2$ corp. Axiomele se verifică: (în rap. cu int. uzuale)

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

$\hat{0}\cdot x = 0$

$\forall \hat{k}, \hat{l} \in \mathbb{Z}_2$: $\hat{k}(a+b) = \hat{k}\cdot a + \hat{k}\cdot b$

$\forall a, b \in G$ $\quad (\hat{k}+\hat{l})\cdot a = \hat{k}\cdot a + \hat{l}\cdot a$

$(\hat{k}\cdot\hat{l})\cdot a = \hat{k}\cdot(\hat{l}\cdot a)$

$\forall$ el. de bază $\in \mathbb{Z}_2$

G spațiu vectorial finit $\Rightarrow$ admite o bază finită. fie $B = \{e_1, \dots, e_n\}$

$\forall x \in G,\ \exists!\ \alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{Z}_2$ a.î. $x = \sum_{i=1}^{n} \alpha_i \cdot e_i$.

Nr. elem. din G = nr. n-upletelor $(\alpha_1, \alpha_2, \dots, \alpha_n)$ care se pot forma cu el. din $\mathbb{Z}_2 \overset{\text{nr}^2}{=}$ nr. fct. $\{\alpha_1, \dots, \alpha_n\} \to \mathbb{Z}_2$ $= 2^n$.

Curs 4

$\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$, $(m,n)=1$

def. $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$

$f(\hat{a}) = (\bar{a}, \bar{\bar{a}})$

$\hat{a} = \hat{b} \Rightarrow (\bar{a}, \bar{\bar{a}}) = (\bar{b}, \bar{\bar{b}})$

$\Updownarrow$ $\Updownarrow$

$mn \mid a-b$ $\bar{a} = \bar{b}$ și $\bar{\bar{a}} = \bar{\bar{b}}$

$\Updownarrow$ $\Updownarrow$

$m \mid a-b$ $n \mid a-b$

$f(\hat{a} + \hat{b}) = f(\hat{a}) + f(\hat{b})$

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

$= (\bar{a}+\bar{b}, \bar{\bar{a}}+\bar{\bar{b}})$

$(\overline{a+b}, \overline{\overline{a+b}}) = (\bar{a}+\bar{b}, \bar{\bar{a}}+\bar{\bar{b}})$

$f(\hat{a} \cdot \hat{b}) = f(\hat{a}) \cdot f(\hat{b})$

f morf. de monoizi

- f inj.

$f(\hat{a}) = f(\hat{b}) \overset{?}{\Rightarrow} \hat{a} = \hat{b}$

$(\bar{a}, \bar{\bar{a}}) = (\bar{b}, \bar{\bar{b}}) \Leftrightarrow \begin{matrix} \bar{a} = \bar{b} \\ \bar{\bar{a}} = \bar{\bar{b}} \end{matrix} \Leftrightarrow \left.\begin{matrix} m \mid a-b \\ n \mid a-b \\ (m,n)=1 \end{matrix}\right| \Rightarrow mn \mid a-b$

Fie $(\bar{x}, \bar{\bar{y}}) \in \mathbb{Z}_m \times \mathbb{Z}_n$; $\exists!\ \hat{a} \in \mathbb{Z}_{mn}$ a.î. $f(\hat{a}) = (\bar{x}, \bar{\bar{y}})$.

$\left.\begin{matrix} \bar{a} = \bar{x} \\ \bar{\bar{a}} = \bar{\bar{y}} \end{matrix}\right| \Rightarrow \begin{cases} a \equiv x \pmod{m} \\ a \equiv y \pmod{n} \end{cases}$

Indicatorul lui Euler: $\varphi : \mathbb{N}\setminus\{0,1\} \longrightarrow \mathbb{N}\setminus\{0,1\}$

$$\varphi(n) = |\mathcal{U}(\mathbb{Z}_n)|$$

$$\| $$

$$\{\hat{a} \mid (a,n)=1\}$$

$$1 \le a \le n$$

f : izomorfism de monoizi $\Rightarrow$ $\mathcal{U}(\mathbb{Z}_{mn}) \simeq \mathcal{U}(\mathbb{Z}_m \times \mathbb{Z}_n)$ izom. de gr.

$$\|$$

$$\mathcal{U}(\mathbb{Z}_m) \times \mathcal{U}(\mathbb{Z}_n)$$

$$\varphi(mn) = |\mathcal{U}(\mathbb{Z}_{mn})| = |\mathcal{U}(\mathbb{Z}_m) \times \mathcal{U}(\mathbb{Z}_n)| = |\mathcal{U}(\mathbb{Z}_m)| \cdot |\mathcal{U}(\mathbb{Z}_n)| = \varphi(m)\cdot\varphi(n).$$

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$$

$$\varphi(n) = \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \cdot \ldots \cdot \varphi(p_r^{k_r})$$

$$\|$$

$$p_1^{k_1} - p_1^{k_1-1}$$

$$\mathcal{U}(\mathbb{Z}_{12}) = \{\hat{1}, \hat{5}, \hat{7}, \hat{11}\} \simeq K$$

Subgrupuri

$$Int(G) \le Aut(G)$$

$$\varphi_a \circ \varphi_b = \varphi_{ab}$$

$$\varphi_e = 1_G$$

$$(\varphi_a)^{-1} = \varphi_{a^{-1}}$$

$H \le (\mathbb{Z},+) \Rightarrow \exists\, n \in \mathbb{N}$ a.î. $H = n\mathbb{Z}$.

„$\Rightarrow$" $H = \{0\}$; $n = 0$

$H = \mathbb{Z}$; $n = 1$

$n := \min\{k \in H \mid k > 0\}$

arăt că $H = n\mathbb{Z}$ „$\supseteq$" $n \in H \Rightarrow nk \in H, \forall k \in \mathbb{Z}$.

„$\subseteq$" $x \in H$; $x = nq + r$, $0 \le r < n$

$r \ne 0$: $0 < r = x - nq \in H$

Subgrupurile gr. lui Klein

Nucleul și imag. unui morfism de grupuri:

$H \leq G, \quad H' \leq G'$

$f(H) = \{ x' \in G' \mid \exists\, x \in H \text{ a.î. } x' = f(x) \}$ = imaginea directă

$f^{-1}(H') = \{ x \in G \mid f(x) \in H' \}$

$x' \cdot (y')^{-1} = f(x)(f(y))^{-1} = f(x) \cdot f^{-1}(y) = f(xy^{-1}) \in f(H)$

$f(G) \leq G'$

$\quad \| $

$\operatorname{Im} f$

$f^{-1}(\{e'\}) \leq G$

$\quad \|$ not.

$\operatorname{Ker} f = \{ x \in G \mid f(x) = e' \}$.

~~f surj <=> Im f c~~

f inj. $\iff \operatorname{Ker} f = \{e\}$

„$\Rightarrow$" $\quad f(x) = e' = f(e) \overset{f \text{ inj}}{\Rightarrow} x = e.$

„$\Leftarrow$" $\quad f(x) = f(y) \;/ \cdot (f(y))^{-1} \Rightarrow \underbrace{f(x) \cdot (f(y))^{-1}}_{f(xy^{-1})} = e' \Rightarrow$

$\Rightarrow xy^{-1} \in \operatorname{Ker} f \Rightarrow xy^{-1} = e \,/\!\cdot y \Rightarrow x = y \Rightarrow f$ inj.

Teorema de corespondență pt. subgrupuri:

$f : G \to G'$ morfism surjectiv de grupuri.

$\{ H \leq G \mid \operatorname{Ker} f \subseteq H \} \longleftrightarrow \{ H' \leq G' \}$

$H \xrightarrow{u} f(H)$

$\operatorname{Ker} f = f^{-1}(\{e'\}) \leq f^{-1}(H') \xleftarrow{v} H'$

$u \circ v = 1,$

$v \circ u = 1$

$f^{-1}(f(H)) = H$

$f(f^{-1}(H')) = H'$

„⊆" $f(x) \in H'$

$x \in f^{-1}(H') \Rightarrow f(x) \in f(f^{-1}(H'))$

„⊇" $x' \in H' \overset{?}{\Rightarrow} x' \in f(f^{-1}(H'))$.

$x' = f(x)$, căci f surj!

$x' \in H' \Rightarrow f(x) \in H'$.

$p: \mathbb{Z} \longrightarrow \mathbb{Z}_n$, $p(k) = \hat{k}$

$\ker p = n\mathbb{Z} \leq d\mathbb{Z} \Leftrightarrow d/n$.

$p(d\mathbb{Z}) = \hat{d}\mathbb{Z}_n$

$\vec{m} = \vec{I} \times \vec{S}$

$\vec{p} = \vec{m} \cdot \vec{d}$

$\vec{B}$

$\vec{B} = nk\hat{z}$.

$\langle X \rangle = \bigcap\limits_{\substack{X \leq K \\ K \in \text{subgrup}}} K$: subgrupul generat de X

$G = (S(\mathbb{R}), \circ)$ $H = \langle f, g \rangle = k$.

$f(x) = x+1$

$g(x) = 2x$

$X = \{x_1, x_2, \dots, x_n\}$, G comutativ

$\langle X \rangle = \{ \sum\limits_{i=1}^{n} k_i x_i \mid k_i \in \mathbb{Z} \}$

$\langle X \rangle$ $X = \{2, 3\} \subseteq \mathbb{Z}$

$\langle X \rangle = \langle 2, 3 \rangle = \langle 2k + 3l \mid k, l \in \mathbb{Z} \} = \mathbb{Z}$

gen. $(\mathbb{Z} \times \mathbb{Z}, +) \to (1,0)$ și $(0,1)$

dar nu este ciclic.

$G = \underbrace{m\mathbb{Z} \times n\mathbb{Z}}_{(m,n)=1} \times$ (... grupuri triviale) $\longrightarrow$ ciclic

$\mathbb{Z} \times \mathbb{Z}_n$ nu e ciclic

Seminar

$f:(\mathbb{Z},+)\to(\mathbb{Z},+)$ morfism de grupuri

$f(0)=0$

$f(1)=n,\ n\in\mathbb{Z}$

$f(a+b)=f(a)+f(b)$

$P_k:\ f(k)=kf(1)$.

$\mathcal{U}(\mathrm{End}(G,\circ))=\mathrm{Aut}(G)$

$(\mathrm{End}(\mathbb{Z}),\circ)$ monoid

$f_n(x)=nx$

$f_m(x)=mx$

$f_n\circ f_m(x)=n\cdot mx$.

$(\mathrm{End}(\mathbb{Z}),\circ)\simeq(\mathbb{Z},\cdot)$ - izom. de monoizi

$g:\mathrm{End}\,\mathbb{Z}\to\mathbb{Z}$

$g(f)=f(1)$

$g(f_1\circ f_2)=g(f_1)\cdot g(f_2)$

$f_1(\underbrace{f_2(1)}_{x})=f_1(1)\cdot f_2(1)$

$f_1(x)=xf_1(1)=f_2(1)\cdot f_1(1)$

$g(f_1)=g(f_2)\Rightarrow f_1=f_2$.

$\Downarrow$

$f_1(1)=f_2(1)\,\big|\cdot x\Rightarrow f_1(x)=f_2(x),\ \forall x\in\mathbb{Z}$.

$\forall n\in\mathbb{Z},\ \exists f\in\mathrm{End}\,\mathbb{Z}$ a.î. $g(f)=n\iff f(1)=n$.

$(\mathrm{Aut}(\mathbb{Z}),\circ)$

$\mathcal{U}(\mathrm{End}\,\mathbb{Z},\circ)\simeq\mathcal{U}(\mathbb{Z},\cdot)$ izom de grupuri

$\{\pm1\}$

$(\mathrm{End}\, \mathbb{Z}_n, \circ) \simeq (\mathbb{Z}_n, \cdot)$

$f: \mathbb{Z}_n \to \mathbb{Z}_n$

$f(\hat{k}) = \hat{a} \cdot k$ autom.

M_1, M_2 monoizi $\Rightarrow \mathcal{U}(M_1 \times M_2) = \mathcal{U}(M_1) \times \mathcal{U}(M_2)$.

$\mathcal{U}(M_1 \times M_2) = \{ (x_1, x_2) \mid x_1 \in M_1,\ x_2 \in M_2,\ (x_1, x_2) \text{ inversabile} \}$

(x_1, x_2) inv. în $M_1 \times M_2 \Leftrightarrow \exists (y_1, y_2) \in M_1 \times M_2$ a.î.

$(x_1, x_2) \times (y_1, y_2) = (e_1, e_2) \Leftrightarrow (x_1 y_1, x_2 y_2) = (y_1 x_1, y_2 x_2) =$

$= (e_1, e_2) \Rightarrow \begin{cases} x_1 y_1 = e_1 \\ x_2 y_2 = e_2 \end{cases}$

ex. de monoid M care are un el. inv. la stânga, cu un nr. finit de inv. (>1) la stânga.

$M = (\mathcal{X}^{\mathcal{X}}, +) \times (\mathbb{Z}_n, +)$

$|\mathcal{U}(M)| = |\mathcal{U}(M, r)| \cdot |\mathcal{U}(\mathbb{Z}_n, +)| = 1 \cdot n = n$.

$\cdot\ (\mathbb{Z}, +) \not\simeq (\mathbb{Q}^*, \cdot)$

în $\mathbb{Z}, +$, ec. $2x = a$ are cel mult o soluție

în $\mathbb{Q}^*$, $(-1) \cdot (-1) = 1 \cdot 1 = 1$

$f(k) = f(1)^k$. $\quad \{ (\frac{a}{b})^k \mid k \in \mathbb{Z} \} = \mathbb{Q}^*$

$(\mathbb{C}, \cdot) \not\simeq (\mathbb{R}, \cdot)$

în $\mathbb{C}$: ec. $x^n = 1$ are n sol. distincte

în $\mathbb{R}$ sunt cel mult 2

$(\mathbb{R}, +) \simeq (\mathbb{C}, +)$

t: 4, 8, 12, 25, 26 pg. 18 ; 4/17

pg. 36 ex. 61, $\to$ Dumitrescu

$\cdot\ f:(\mathbb{Q},+)\longrightarrow(\mathbb{Z},+)$ morfism de grupuri $\Rightarrow f$ morfismul nul.

$f(x)=x f(1)$.

$f(3)=f(\frac{3}{2})+f(\frac{3}{2})=2f(\frac{3}{2})$

Dacă $f(3)=2^k\cdot m$, m impar

$\Rightarrow f(\frac{3}{2})=2^{k-1}\cdot m \Rightarrow f(\frac{3}{2^k})=m \Rightarrow 2f(\frac{3}{2^{k+1}})=m$,

cu m impar, r.c.

~~$f(x)=x\cdot f(1)$~~

$x=1+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{\ }}}}$

~~$f(3)$~~

$f(x)\neq 0$ fie $d\in\mathbb{Z}$. $f(x)\nmid d$

$f(x)=\left(f(\frac{x}{d})+f(\frac{x}{d})+\dots+f(\frac{x}{d})\right)$

4. $\cdot\ f:(\mathbb{Z},+)\longrightarrow(\mathbb{Z},+)$ morfism

$f(0)=0$

$f(n)=f(1+1+\dots+1)=f(1)+f(1)+\dots+f(1)=n f(1)$.

f este unic determinat de $f(1)\overset{\text{not.}}{=}n$.

$\operatorname{Hom}_{gr}(\mathbb{Z},\mathbb{Z})=\{f_n(x)\mid f_n(x)=nx,\ n\in\mathbb{N}\}$.

$\cdot\ f:(\mathbb{Z},+)\longrightarrow(\mathbb{Q},+)$ morfism

$f(1)=f(1+0)=f(1)+f(0)\Rightarrow f(0)=0$

$f(x)=x f(1)$.

~~$f(x)=f(\frac{x}{n}+\frac{x}{n}+\dots+\frac{x}{n})=n\cdot f(\frac{x}{n}),\ \forall n\in\mathbb{N}^*$.~~

$f(x)=x f(1),\ \forall x\in\mathbb{N}\Rightarrow f$ e unic det. de $f(1)\in\mathbb{Q}\Rightarrow$

$\Rightarrow \operatorname{Hom}_{gr}(\mathbb{Z},\mathbb{Q})=\{f_n(x)\mid f_n(x)=nx,\ n\in\mathbb{Q}\}$.

· $\mathbb{Q}$ nu e ciclic: Dacă $a \in \mathbb{Q}$, $a \neq 0$, $\langle a \rangle = \{na \mid n \in \mathbb{Z}\} \neq \mathbb{Q}$,

căci $\frac{a}{m} \notin \langle a \rangle$, cu $m \in \mathbb{N}^*$ $\Rightarrow$ $\mathbb{Q}$ nu are un singur gen. $\Rightarrow$ nu e ciclic

$\langle 0 \rangle = \{0\} \neq \mathbb{Q}$

· $f : (\mathbb{Q}, +) \to (\mathbb{Q}, +)$ morfism

$f(0) = 0$, $f(n) = n f(1)$, $\forall n \in \mathbb{N}$

$$\left.\begin{aligned} & f\left(\frac{m}{n}\right) = f\left(\frac{1}{n} + \dots + \frac{1}{n}\right) = m \cdot f\left(\frac{1}{n}\right) \\ & f(1) = f\left(\frac{1}{n} + \dots + \frac{1}{n}\right) = n \cdot f\left(\frac{1}{n}\right) \Rightarrow f\left(\frac{1}{n}\right) = \frac{f(1)}{n} \end{aligned}\right| \Rightarrow$$

$\Rightarrow f\left(\frac{m}{n}\right) = \frac{m}{n} \cdot f(1) \Rightarrow f(x) = x \cdot f(1), \forall x \in \mathbb{Q}$.

$\mathrm{Hom}_{gr}(\mathbb{Q}, \mathbb{Q}) = \{ f_r(x) \mid f_r(x) = rx, r \in \mathbb{Q} \}$.

· $f : (\mathbb{Z}_n, +) \to (\mathbb{Z}_n, +)$ morfism

$f(\hat{0}) = \hat{0}$, $f(\hat{x}) = f(\hat{1} + \hat{1} + \dots + \hat{1}) = \hat{x} \cdot f(\hat{1})$,

deci f e unic det. de $f(\hat{1})$, care poate lua n valori

· $f(\mathbb{Z}_n, +) \to (\mathbb{Z}_m, +)$ morfism

$f(\hat{x}) = \bar{x} \cdot f(\hat{1})$. Ambele gr. sunt ciclice, cu generatorul 1,

deci, știind $f(\hat{1}) = \bar{a} \in \mathbb{Z}_m$, știm morfismul.

8. $f(\hat{m}) = \bar{m} \cdot f(\hat{1}) = \bar{0} = f(\hat{0})$ ~~$\bar{0} = \overline{am} = f(\hat{0}) = \overline{ma}$~~

~~dar $f(\hat{m}) = m$~~

a.î.

$\bar{0} = f(\hat{n}) = \bar{n} \cdot f(\hat{1}) = \bar{n} \cdot \bar{a} \Rightarrow$ ~~$n \cdot a \mid m$~~ $m \mid na$.

Dacă $d = (m, n) \Rightarrow m = dk_1$, $n = dk_2$, $(k_1, k_2) = 1$ $\Big| \Rightarrow$

$\Rightarrow k_1 = \frac{m}{d} \mid k_2 a \Rightarrow \frac{m}{d} \mid a$.

Dacă $\frac{m}{d} \mid a$, $f_a(\hat{x}) = \overline{x \cdot a}$.

$f_a(\hat{n}) = \overline{n \cdot a} = \bar{0}$.

8. $G = H_1 \cup H_2$ subgrupuri proprii $\Rightarrow$ $H_1 \not\subset H_2$ și $H_2 \not\subset H_1$ (altfel, unul din ele ar fi G. r.c.)

arăt că $H_1 \cup H_2$ nu poate fi subgrup al lui G.

fie $a \in H_1 - H_2$ și $b \in H_2 - H_1$.

Dacă $H_1 \cup H_2$ e grup $\Rightarrow$ $ab \in H_1 \cup H_2$.

i) $ab \in H_1 \Rightarrow$, $a \in H_1 \Rightarrow a^{-1} \in H_1$ $\Big|$ $\Rightarrow a^{-1}(ab) = b \in H_1$. fals.

ii) $ab \in H_2$, $b \in H_2 \Rightarrow b^{-1} \in H_2$ $\Big|$ $\Rightarrow a = ab \cdot (b^{-1}) \in H_2$. fals.

$\Rightarrow$ $H_1 \cup H_2$ nu poate fi un subgrup al lui G, deci nici G.

---

ex. de gr. care pot scrie ca reuniune a 3 subgr. proprii

· orice grup izomorf cu gr. lui Klein $= \{e,a\} \cup \{e,b\} \cup \{e,c\}$

· grupul cuaternionilor de ordin 8 $Q_8 = \{1,-1,i,-i,j,-j,k,-k\}$,

$i^2 = j^2 = k^2 = -1$, $i \cdot j = k$, $i \cdot k = -j$, $j \cdot i = -k$, $j \cdot k = i$, $k \cdot i = j$, $k \cdot j = -i$

$Q_8 = \{1,-1,i,-i\} \cup \{1,-1,j,-j\} \cup \{1,-1,k,-k\}$.

12. grupuri cu exact:

2 subgr.: cele izomorfe cu $\mathbb{Z}_p$, p prim (îl am ca ciclic grup pe oricare nr.)

3 subgr.: −//− $\mathbb{Z}_{p^2}$, p prim

4 subgr.: −//− $\mathbb{Z}_{p_1 \cdot p_2}$, $p_{1,2}$ prime

5 subgr.: −//− $\mathbb{Z}_{p \cdot q \cdot r}$, p, q, r prime.

25. G grup, $H_1 \subset H_2 \subset \ldots \subset H_n \subset \ldots$ șir cresc. de subgr.

i) $H = \bigcup_{n \geq 1} H_n$ subgrup al lui G. (A): din G grup; (N): $e \in H_i$, $i = \overline{1,n}$

(P): fie $a \in H_i$, $b \in H_j$. dacă $i = j$, evident, cum H_i e subgrup $\Rightarrow$ $\Rightarrow ab \in H_i$. pp. $i < j \Rightarrow H_i \subset H_j$. ~~Dacă~~ $a \in H_i \Rightarrow$ $\Rightarrow a \in H_j \Rightarrow ab \in H_j \Rightarrow ab \in H$;

(S): $a \in G \Rightarrow \exists i$ a.î. $a \in H_i$ subgr. $\Rightarrow a^{-1} \in H_i$;

ii) $H_n \neq H_{n+1}$, $\forall n \in \mathbb{N}^* \Rightarrow H$ nu e finit generat.

Dacă $H = \langle h_1, h_2, \dots, h_k \rangle$ finit generat, at. $\exists n_k$ a.î.

H_n nu conține niciun h_i, $\forall n \geq n_k$, iar H_{n-1} are cel puțin un h_i,

~~Dacă H ar fi generat f~~ deci pe toți $h_1, h_2, \dots, h_i$. $\Rightarrow$

H generat finit $\Rightarrow$ toate elem. lui H, deci inclusiv cele din H_n se pot

scrie ca o combinație din $h_1, \dots, h_i$, adică cu el. din H_{n-1}.

cf. def. subgrupului, s-ar ajunge la $H_{n-1} > H_n$ m.c.

~~formarii~~

26. $S(X)$: grupul bij. de la X la X în rap. cu comp. fct.

comp. fct. ...

$f, g \in S(\mathbb{R})$, $f(x) = x+1$, $g(x) = 2x$, $\forall x \in \mathbb{R}$

$f_n = g^{-n} f g^n$. $\qquad g^i(x) = 2^i x$.

$G = \langle f, g \rangle$ $\qquad g^{-i}(x) = \frac{1}{2^i} x$.

$H_n = \langle f_n \rangle$ $\qquad f_i \circ f_i = g^{-n} \circ f g^i$ $\frac{1}{2^i}(2^i x + 1)$

$= g^{-i} \circ f^2 \circ g^i$

$H = \bigcup_{n \geq 1} H_n$ subgrup al lui G.

fie $x \in H_i = \langle f_i \rangle$ grup?

$f_i = g^{-i} \circ f \circ g^i = g^{-i}\left(f\left(\frac{2^i x}{2^i}\right)\right) = \frac{1}{2^i} f(2^i x) =$

~~$f_i \circ f_i = g^{-i}($~~ $= \frac{1}{2^i}(2^i x + 1) = x + \frac{1}{2^i}$.

~~$f_i^{-1} = x - \frac{1}{2^i}$~~.

$\langle f_i \rangle = \{ f(x) = x + \frac{m}{2^i} \mid m \in \mathbb{N}^* \}$.

$x = g^{-i} f g^i$, $y = g^{-j} f g^j \Rightarrow$

$z = x \circ y = g^{-i} \circ f \circ g^i \circ g^{-j} \circ f \circ g^j = x + \frac{1}{2^i} + \frac{1}{2^j} =$

~~$i \to j$: $x \circ y = \left(x + \frac{1}{2^i}\right) \circ ($~~

fie $i > j$: $\qquad z(x) = x + \frac{(2^{i-j}+1)^m}{2^i} \in \langle f_i \rangle$

simetrizabil?

Curs 5

G grup, H subgrup; rel. binare R_H^s, R_H^d

$x, y \in G$: $\quad x R_H^s y \Leftrightarrow x^{-1}y \in H$

$\quad x R_H^d y \Leftrightarrow xy^{-1} \in H$

sau (not.): $\quad x \equiv_s y \pmod H \Leftrightarrow x^{-1}y \in H$

$\quad x \equiv_d y \pmod H \Leftrightarrow xy^{-1} \in H$

generalizare de la: $\quad x \equiv y \pmod n \Leftrightarrow x-y \in n\mathbb{Z}$

$(\hat{x})_s = \{ y \in G / x^{-1}y \in H \} = \{ y \in G / y \in xH \} = xH.$

$(\hat{x})_d = Hx$

$H = \{e\}$

$x \equiv_s y \pmod H \Leftrightarrow x^{-1}y \in \{e\} \Leftrightarrow x^{-1}y = e \Leftrightarrow x = y.$

$(\hat{x})_s = (\hat{x}_d) = \{x\}$

$H = G$: $\quad (\hat{x})_s = (\hat{x})_d = (\hat{e})_s = G.$

G abelian $\Rightarrow$ rel. coincid

$S_3 = \{ e, (12), (13), (23), (123), (132) \}$

$(12) \downarrow$ transpoziție; $(123) \downarrow$ ciclu

$H = \{ e, (12) \} \leq S_3$

$\sigma \equiv_s \tau \pmod H \Leftrightarrow \sigma^{-1}\tau \in H \Leftrightarrow \sigma^{-1}\tau(3) = 3 \Leftrightarrow \sigma(3) = \tau(3)$

I. $\sigma(3) = \tau(3) = 1$

$C_s^1 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}.$

II. $\sigma(3) = 2$

$C_s^2 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$

III. $\sigma(3) = 3$

$C_s^3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} = H$

$\sigma \equiv_d \tau \pmod{H} \Leftrightarrow \quad \sigma^{-1}(3) = \tau^{-1}(3)$

I. $\sigma^{-1}(3) = 1 \Leftrightarrow \sigma(1) = 3.$

$$C_d^1 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right.$$

II. $\sigma^{-1}(3) = 2 \Leftrightarrow \sigma(2) = 3$

$$C_d^2 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}.$$

III. $\sigma^{-1}(3) = 3 \Leftrightarrow \sigma(3) = 3$

$$C_d^3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} = H$$

$S/R_H^s = \{ C_1^s, C_2^s, C_3^s \}$, $S/R_H^d = \{ C_1^d, C_2^d, C_3^d \}$ sunt diferite.

$f: G/R_H^s \longrightarrow G/R_H^d$, $f(xH) = Hx^{-1}$ bijectivă.

f bine definită.

$(\hat{x})_s = (\hat{y})_s \Rightarrow xH = yH \Leftrightarrow x^{-1}y \in H \Rightarrow$

~~$\Rightarrow (x^{-1}y)^{-1} \in H \Rightarrow y^{-1}x \in H$ (nu e nevoie)~~

$Hx^{-1} = Hy^{-1}$

$\alpha \equiv_d \beta \pmod{H} \Leftrightarrow \alpha\beta^{-1} \in H.$

$\alpha = x^{-1}$
$\beta = y^{-1}$

$x^{-1} \cdot \underbrace{(y^{-1})^{-1}}_{y} \in H \Rightarrow x^{-1} \equiv_d y^{-1} \pmod{H} \Rightarrow$

$Hx^{-1} = Hy^{-1}.$

f inj. : $f(xH) = f(yH) \overset{?}{\Rightarrow} xH = yH.$
$Hx^{-1} = Hy^{-1} \Rightarrow xH = yH$ (reciproca de mai sus)

surj. : Fie $Hy \in G/\equiv_d \pmod{H}$ $\quad f(y^{-1}H) = Hy.$

$\Rightarrow f$ bij.

$|G| = [G:H] \cdot |H|$

Lemă: $\varphi : H \to xH$, $\varphi(h) = xh$ bij.

$\varphi(h) = \varphi(h') \Rightarrow xh = xh' \Rightarrow h = h' \Rightarrow \varphi$ inj.

$a \in G$

$\langle a \rangle = \{ a^m \mid m \in \mathbb{Z} \}$ s.n. subgrupul ciclic generat de a

$G = \langle a \rangle \Rightarrow G$ grup ciclic

$G = (\mathbb{Z}, +)$

$\langle 2 \rangle = 2\mathbb{Z}$

$a \in G$ este de ordin finit dc. $\exists\, i \neq j$ a.î. $a^i = a^j \Leftrightarrow \exists k \in \mathbb{N}^*$ a.î. $a^k = e$

$\operatorname{ord} a = \min \{ k \in \mathbb{N}^* \mid a^k = e \}$

$n = \operatorname{ord}(a) \Leftrightarrow$ 1) $a^n = e$

2) $a^k = e \Rightarrow k / n$

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

$\operatorname{ord}(a) = |\langle a \rangle| \mid |G|$

$|G| = n \Rightarrow a^n = e, \forall a \in G.$

(Mica Teoremă a lui Fermat) p prim, $a \in \mathbb{N} \setminus \{0, 1\}$, $(a, p) = 1$

$a^{p-1} \equiv 1 \pmod{p}$ caz particular al:

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

$n =$ prim $\Rightarrow \varphi(p) = p - 1$

dem: $|G| = m \Rightarrow a^m = e, \forall a \in G.$

$G = \mathcal{U}(\mathbb{Z}_n)$; $|G| = \varphi(n)$

$\hat{a} \in \mathcal{U}(\mathbb{Z}_n) \Leftrightarrow (a, n) = 1$

$\hat{a}^{\varphi(n)} = \hat{1} \Leftrightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

$x \in G$, ord $x = n < \infty$

$$\text{ord}(x^k) = \frac{n}{\underset{\text{cmmdc}}{\underbrace{(n,k)}}}$$

dem.: 1) $(x^k)^{\frac{n}{(n,k)}} = e$

2) $(x^k)^l = e \Rightarrow \frac{n}{(n,k)} \Big| l$

$$(x^k)^{\frac{n}{(n,k)}} = e$$

$d = (n,k)$

$n = dn_1$ $\quad (n_1, k_1) = 1$

$k = dk_1$

$$(x^k)^{\frac{n}{(n,k)}} = x^{k \cdot \frac{n}{d}} = x^{k_1 n} = (x^n)^{k_1} = e^{k_1} = e$$

$$(x^k)^l = e \Rightarrow n \mid kl \Rightarrow \cancel{d}n_1 \mid \cancel{d}k_1 l \quad \left.\begin{matrix} \\ (n_1,k_1)=1 \end{matrix}\right| \Rightarrow n_1 \mid l$$

$\Rightarrow n_1 = \text{ord}(x^k)$.

Seminar

$\mathbb{Z} \times \mathbb{Z}$ nu e ciclic, dar e finit generat

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

$\mathbb{Z} \times \mathbb{Z} = \langle (a,b), (c,d) \rangle$

$(1,0) = k(a,b) + l(c,d)$

$(0,1) = k'(a,b) + l'(c,d)$

$$\begin{cases} 1 = ka + lc \\ 0 = kb + ld \end{cases} \qquad k, k', l, l' \in \mathbb{Z}$$

$$\begin{cases} 0 = k'a + l'c \\ 1 = k'b + l'd \end{cases}$$

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm 1$$

$ad - bc = \pm 1$

$\Downarrow$

$(a, c) = 1$

$(b,d) = 1$

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} k \\ l \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \cancel{\begin{pmatrix} k \\ l \end{pmatrix} \cdot \begin{pmatrix} a & c \\ b & d \end{pmatrix}}$$

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \cancel{\begin{pmatrix} k' \\ l' \end{pmatrix}} \begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} k' \\ l' \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} k & k' \\ l & l' \end{pmatrix}$$

$$1 = \underset{\in \{\pm 1\}}{\det \begin{vmatrix} a & c \\ b & d \end{vmatrix}} \cdot \begin{vmatrix} & \end{vmatrix}$$

$\mathbb{Z}\times\mathbb{Z}$ ciclic $\Leftrightarrow$ $\exists\,(x,y)\in\mathbb{Z}\times\mathbb{Z}$ a.î. $\langle (x,y)\rangle=\mathbb{Z}\times\mathbb{Z}$

$$\begin{cases}(1,0)=k\cdot(x,y)\\(0,1)=l\cdot(x,y)\end{cases}\Leftrightarrow\begin{cases}kx=1 & \text{şi } ky=0 \to k\neq 0 \to y=0 \to x=y=0 \Rightarrow\\ lx=0 & \text{şi } ly=1\end{cases}$$

$\Downarrow$ $l=0$ sau $x=0$

$\mathbb{Z}\times\mathbb{Z}=\langle(0,0)\rangle$.

rez. ex. din curs 5:

i) $(\mathbb{Q},+)$ ciclic

$$\left\langle\frac{1}{2},\frac{1}{3}\right\rangle=\left\langle\frac{1}{6}\right\rangle$$

$$\langle x_1,\dots,x_n\rangle=\left\{\sum_{i=1}^{n}k_i x_i \;\middle|\; k_i\in\mathbb{Z}\right\},\ a,b\in\mathbb{Z}$$

G abelian

fie $x=\frac{a}{2}+\frac{b}{3}=\frac{3a+2b}{6}=\frac{1}{6}\underbrace{(3a+2b)}_{\in\mathbb{Z}}\in\left\langle\frac{1}{6}\right\rangle$

$\frac{1}{6}=\frac{1}{2}-\frac{1}{3}\Rightarrow a\cdot\frac{1}{6}=a\left(\frac{1}{2}-\frac{1}{3}\right)=a\cdot\frac{1}{2}-a\cdot\frac{1}{3}$

$\langle x_1,\dots,x_n\rangle=\langle y_1,\dots,y_m\rangle\Leftrightarrow x_i\in\langle y_1,\dots,y_m\rangle,\forall i$
$y_j\in\langle x_1,\dots,x_n\rangle,\forall j$

ii) $(\mathbb{Q},+)$ subgr. finit generat este ciclic

fie $H=\left\langle\frac{a_1}{b_1},\frac{a_2}{b_2},\dots,\frac{a_n}{b_n}\right\rangle$; cu $(a_i,b_i)=1,\forall i$.

$b=\text{cmmmc}(b_1,b_2,\dots,b_n)$

$a=\text{cmmdc}\left(\frac{a_1 b}{b_1},\frac{a_2 b}{b_2},\dots,\frac{a_n b}{b_n}\right)$

$x\in\left\langle\frac{a_1}{b_1},\dots,\frac{a_n}{b_n}\right\rangle$

$$x=k_1\cdot\frac{a_1}{b_1}+\dots+k_n\cdot\frac{a_n}{b_n}=\frac{k_1\cdot\boxed{\frac{a_1 b}{b_1}}+k_2\cdot\boxed{\frac{a_2 b}{b_2}}+\dots+k_n\boxed{\frac{a_n b}{b_n}}}{b}$$

$$=\frac{a}{b}\left(k_1\cdot\frac{a_1 b}{a b_1}+k_2\cdot\frac{a_2 b}{a b_2}+\dots+k_n\frac{a_n b}{a b_n}\right)$$

$$\left(\frac{a_1 b}{a b_1},\dots,\frac{a_n b}{a b_n}\right)=1\Rightarrow$$

$\exists\,k_1,k_2,\dots,k_n$ a.î. $k_1\cdot\frac{a_1 b}{a b_1}+\dots+k_n\cdot\frac{a_n b}{a b_n}=1\Rightarrow$

$\Rightarrow\frac{a}{b}\in\left\langle\frac{a_1}{b_1},\dots,\frac{a_n}{b_n}\right\rangle$.

$bH \leq \mathbb{Z} \Rightarrow bH = a\mathbb{Z} \Rightarrow H = \frac{a}{b}\mathbb{Z} \Rightarrow H$ ciclic.

iii) $(\mathbb{Q},+)$ nu e finit generat.

fie $\frac{a_1}{b_1}, \dots, \frac{a_n}{b_n}$ un sist. finit de gen.

cf. b), $\mathbb{Q} = \langle \frac{a}{b} \rangle$, $a, b = \dots$

$\Rightarrow \exists x \in \mathbb{Z}$ a.î. $\frac{1}{2b} = \frac{xa}{b} \Rightarrow 2ax = 1, a,x \in \mathbb{Z}$ r.c.

t: pg. 57 ex. 69, ~~76~~ $\longrightarrow$ cartea Dumitrescu
(mai bine nu)

(26) $(S(\mathbb{R}), \circ)$, $G = \langle f, g \rangle$ $\quad f(x) = x+1$
$g(x) = 2x$

$H \leq G$, H nu este finit generat.

$H_n = \langle g^{-n} f g^n \rangle$

$H_n \underset{\neq}{\leq} H_{n+1}$

$n=0$: $f \in \langle g^{-1} f g \rangle$

t: + ex. 29, 30,

(69) $G = (\mathbb{C}^*, \cdot)/\mathbb{Q}^*$

a) $x^{-1}y \in \mathbb{Q}^*$ pt $x,y \in \mathbb{C}^* \Leftrightarrow xy^{-1} \in \mathbb{Q}^*$

$\mathbb{Q}^*$ subgrup normal al lui $\mathbb{C}^*$:

$\Leftrightarrow \forall x \in \mathbb{C}^*$, $x\mathbb{Q}^* = \mathbb{Q}^* x$.

$x \cdot \frac{a}{b} = \frac{a}{b} \cdot x$ evident

$G = \mathbb{C}^*/\mathbb{Q}^* = \{\mathbb{Q}^*, x\mathbb{Q}^*, y\mathbb{Q}^*, \dots\}$, $x, y, \dots \in \mathbb{C}^*$

clasele de echivalență

$\mathrm{ord}(\widehat{1+i})$, $\mathrm{ord}(\widehat{2+i}) = ?$

G este grup în rap. cu op. "·" definită astfel:

$x\mathbb{Q}^* \cdot y\mathbb{Q}^* = (xy) \cdot \mathbb{Q}^*$.

$\Updownarrow$

cu clase: $\hat{x} \cdot \hat{y} = \widehat{x \cdot y}$, $\forall x, y \in \mathbb{C}^*$.

Dem.: operația este bine definită;

$x_1, x_2 \in \hat{x}$, $y_1, y_2 \in \hat{y}$ $\Rightarrow$ $x_1 \mathbb{Q}^* = x_2 \mathbb{Q}^*$ și $y_1 \mathbb{Q}^* = y_2 \mathbb{Q}^*$

$$\widehat{x_1 \cdot y_1} = \widehat{x_2 \cdot y_2} = \widehat{x \cdot y}$$

ρ_N : $\frac{x}{y} \in \mathbb{Q}^*$; $(x_1, x_2) \in \rho_n$, $(y_1, y_2) \in \rho_n$.

~~x_1, x~~ $\hat{x} = x_1 N = x_2 N = N x_1 = N x_2$

$\hat{y} = y_1 N = y_2 N = N y_1 = N y_2$

~~$(x_1 y_1) N = h$ a.î.~~

$x \in x_1 y_1 N \Rightarrow \exists n \in N$ a.î. $x = x_1 (y_1 n) \Rightarrow x = x_1 (y_2 n') =$

$= x_1 (n'' y_2) = \cancel{x'''x_1}\ x_2 n''' y_2 = n^{IV} x_2 y_2 \Rightarrow$

$\Rightarrow x \in N \cancel{y_2} x_2 y_2 \Rightarrow x \in x_2 y_2 N.$

Analog și reciproca.

El. neutru: $\hat{x} \cdot N = N \cdot \hat{x} = \widehat{xN} \Rightarrow \hat{e} = N.$

„ · " este asociativă.

Inversul: $\hat{x}^{-1} = \widehat{x^{-1}}$ $\left(\hat{x} \cdot \widehat{x^{-1}} = \widehat{x \cdot x^{-1}} = N \right)$

$N = \mathbb{Q}^*$ de fapt mai sus.

$\Rightarrow (G, \cdot)$ ~~definit~~ grup (gr. factor)

$\left(\widehat{(1+i)}\mathbb{Q}\right)^{ord(\widehat{1+i})} = \mathbb{Q}^*$;

$\widehat{(1+i)}^2 = \widehat{(1+i)^2} = \widehat{2i}$.

$\left(\widehat{(1+i)}\right)^4 = \widehat{(1+i)^4} = \widehat{(2i)^2} = \widehat{-2}\mathbb{Q}^* = \mathbb{Q}$, deoarece $-2 \in \mathbb{Q}^*$.

~~$\widehat{(2+i)}^2$~~

$n = ord\,(\widehat{2+i})$ există dacă $\widehat{(2+i)}^n \overset{?\,\exists n?}{\in} \mathbb{Q}^*$ $\Big($pt. ca $\left((2+i)G\right)^n =$

$= \widehat{(2+i)^n}\,\mathbb{Q}^* = G \Big\} \Rightarrow (2+i)^n \in \mathbb{Q}^* \Big)$

În ex. precedent, 68

$u : (\mathbb{Z}[i], \cdot) \longrightarrow (\mathbb{Z}_5 \times \mathbb{Z}_5, \cdot)$, $u(a+bi) = (\widehat{a+2b}, \widehat{a-2b})$

u morfism de monoizi.

$u((2 \pm i)^n) = ?$ $\qquad u(ab) = u(a)\cdot u(b)$

$u((a+bi)(c+di)) = u(ac-bd+i(ad+bc)) \overset{def}{=} (\widehat{ac-bd+2(ad+bc)}, \widehat{ac-bd-2(ad+bc)})$.

$= u(a+bi)\cdot u(c+di) = (\widehat{a+2b}, \widehat{a-2b}) \cdot (\widehat{c+2d}, \widehat{c-2d}) =$

$= (\widehat{ac+2ad+2bc+4bd}, (\quad \widehat{\ } \quad))$.

$\{u(2+i)^n \mid n \geq 1\} = \{(\hat{4}, \hat{0}), (\hat{4}, \hat{0})\}$.

~~$(\hat{4},0)$~~ $\{ u((2+i)^2 \cdot (2+i)) = (\hat{4}, \hat{0}) \cdot (\quad)$

$u(2+i)^2 = u(3+4i) = ($

$u(2+i)^3 = (\hat{4}, \hat{0}) \cdot (\hat{1}, \hat{0}) = (\hat{4}, \hat{0})$ și se repetă.

analog, $\{u(2-i)^n \mid n \geq 1\} = \{(\hat{0}, \hat{4}), (\hat{0}, \hat{1})\}$.

Revenind, dacă $(2+i)^n \in \mathbb{R}^*$ și cum $(2+i)^n \cdot (2-i)^n = 5^n$ $\Rightarrow \left(\frac{2+i}{2-i}\right)^n \in \mathbb{R}^*$

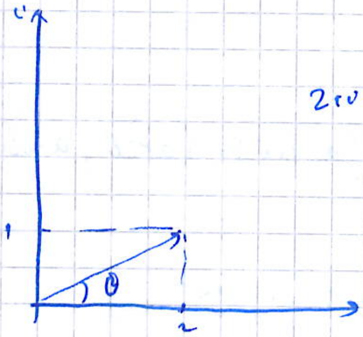
și cum $\left|\frac{2+i}{2-i}\right| = 1 \Rightarrow \left(\frac{2+i}{2-i}\right)^n = 1 \Rightarrow (2+i)^n = (2-i)^n \Rightarrow$

$\Rightarrow \exists n$ a.î. $u(2+i)^n = u(2-i)^n$ n.c.

b) i) $\frac{\operatorname{arctg}\left(\frac{1}{2}\right)}{\pi} \notin \mathbb{Q}^*$;

ii) subgr. generat de $1+i$ și $2+i$ nu e ciclic.

c) G nu e finit generat.



$2+i = \sqrt{5}\,(\cos\theta + i\sin\theta)$, $\theta = \operatorname{arctg}\frac{1}{2}$

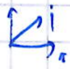
$(2+i)^n \notin \mathbb{R}^* \Rightarrow \sin n\theta \neq 0 \Rightarrow$

$n\theta \neq k\pi,\ k\in\mathbb{Z} \Rightarrow$

$\dfrac{\operatorname{arctg}\frac{1}{2}}{\pi} \neq \dfrac{k}{n},\ \forall k,n\in\mathbb{Z}$.

$\notin \mathbb{Q}$

ord$(\widehat{1+i}) = 4$, ord$(\widehat{2+i}) = \infty \Rightarrow$ dacă subgr. generat de a și b
a, a^2, a^3, e $\quad b, b^2, \dots$



$-1, 1, i, -i, h, \dots$

ar avea un generator, $g = a^i b^k$, ciclic. $\quad$.

$\Rightarrow b^{k+1} = g^t = (a^i b^k)^t \Rightarrow a^{it} = e$ și
$b^{kt} = b^{k+1} \Rightarrow b^{k(t-1)-1} = e$ n.c.,

căci b are ordinul infinit.

c) G finit generat $\Rightarrow \exists\, \hat{g}_1, \hat{g}_2, \dots, \hat{g}_k$ generatori a.î. $\forall\, g\in G$,
$\hat{g} = g_1^{i_1} \cdot g_2^{i_2} \cdot \ldots \cdot g_k^{i_k}$.

def. $f: G \to \mathbb{N}^k$, $f(g) = (i_1, i_2, \dots, i_k)$.

se dem. că f bijectivă.

cum $\mathbb{N}^k$ este numărabilă (se dem. prin inducție)

se fol. că prod. cartezian a 2 mulțimi ~~e mulț.~~ numărabile este o mulț. numărabilă

$\Rightarrow G$ numărabilă.

~~dar, cf. th. Lagrange, $\mathbb{C}^* = G \cdot |\mathbb{C}^* : G|$~~

prin def., $\cancel{\mathbb{C}^* = \bigcup_{x\in\mathbb{C}^*} x\mathbb{Q}^*}$ $\mathbb{C}^* = \bigcup_{x\in\mathbb{R}} x\mathbb{Q}^*$

mulț. claselor este numărabilă $\Rightarrow$

$\Rightarrow \mathbb{C}^*$ este numărabilă. contradicție.

Curs 7

Subgrupuri normale

Def.: $\forall x \in G, h \in N, xhx^{-1} \in N$

$f: G \to G'$ morfism

1) $N \trianglelefteq G \Rightarrow f(N) \trianglelefteq G'$

fie $g' \in G', h \in N$.

$g' \cdot f(h) (g')^{-1} \in f(N)$

f surj. $\Rightarrow \exists\, g \in G$ a.î. $f(g) = g' \Rightarrow$ $\ldots = f(ghg^{-1}) \in f(N)$, deoarece $N \trianglelefteq G$.

2) $N' \trianglelefteq G' \Rightarrow f^{-1}(N') \trianglelefteq G$.

$\operatorname{Ker} f \trianglelefteq G$.

fie $g \in G, h \in f^{-1}(N')$. arăt că $ghg^{-1} \in f^{-1}(N') \Leftrightarrow$

$f(ghg^{-1}) \in N'$.

$f(h) \in N', N' \trianglelefteq G' \Rightarrow f(g) \cdot f(h) \cdot f(g^{-1}) \in N' \Rightarrow \ldots$

$N \trianglelefteq H \trianglelefteq G$ $\qquad p(H) = \{ p(h) \mid h \in H \} = H/N$

$$\begin{tikzcd} A \arrow[r, "p"] \arrow[dr, "f"'] & A/\rho \arrow[d, "\exists! \bar{f}"] \\ & B \end{tikzcd}$$

a.î. $\bar{f} \circ p = f \Leftrightarrow \rho_f \supseteq \rho$

f morf. de grupuri

$$\begin{tikzcd} G \arrow[r, "p"] \arrow[dr, "f"'] & G/N \arrow[d, "(\exists!)\, \bar{f}"] \\ & G' \end{tikzcd}$$

(Prop. de universalitate a grupurilor de factor)

morfism de gr.

$\bar{f} \circ p = f \Leftrightarrow N \subseteq \operatorname{Ker} f$

$G \xrightarrow{f} G'$ surj.

$$G/\mathrm{Ker} f \simeq G'$$

f morf. de gr. $\Rightarrow$ $\underset{f^{-1}(\{e'\})}{\underset{\|}{\mathrm{Ker} f}} \trianglelefteq G$

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

$N \underset{\trianglelefteq}{\subseteq} H \trianglelefteq G$ $\quad \dfrac{G/N}{H/N} \cong G/H$

Folosesc th. fundam. de izo. pt. gr.: $\quad G/N \xrightarrow{f} G/H$, f surj.

$\mathrm{Ker} f = H/N$

$$f(xN) = xH$$

$\left.\begin{array}{l} xN = yN \Leftrightarrow x^{-1}y \in N \\ N \subset H \end{array}\right| \Rightarrow x^{-1}y \in H \Rightarrow xH = yH \Rightarrow f$ bine definită.

$$f(xN \cdot yN) = f(xyN) = xyH = xH \cdot yH = f(xN) \cdot f(yN)$$

$$\mathrm{Ker} f = \{xN \mid \underset{xH}{\underset{\|}{f(xN)}} = H\} = \{xN \mid x \in H\} = H/N.$$

ex.: $G = (\mathbb{C}^*, \cdot)$

$H = S^1 = \{z \in \mathbb{C}^* \mid |z| = 1\}$

$G/H = \mathbb{C}^*/S^1 \simeq (\mathbb{R}_+^*, \cdot)$

$\left.\begin{array}{l} f: \mathbb{C}^* \longrightarrow \mathbb{R}_+^* \text{ morf. surj.} \\ \mathrm{Ker} f = S^1 \end{array}\right| \overset{TFIG}{\Rightarrow} \mathbb{C}^*/S^1 \simeq \mathbb{R}^*$

$f(z) = |z|$

$\mathrm{Ker} f = S^1.$

$H_{1,2} \trianglelefteq G_{1,2} \Rightarrow H_1 \times H_2 \trianglelefteq G_1 \times G_2$

$$(G_1 \times G_2) / (H_1 \times H_2) \simeq G_1/H_1 \times G_2/H_2$$

Seminar

Curs 6. Ex. $k \in \mathbb{Z}_{240}$, $ord(\hat{k}) = 30$ $\quad\varphi(30) = 8$

$$ord(\hat{k}) = \frac{240}{(k, 240)} = 30 \Rightarrow (k, 240) = 8 \qquad 240 = 2^4 \cdot 3 \cdot 5$$

$k \in \{8, 56, 88, 104, 136, 152, 184, 232\}$.

G_1, G_2 grupuri, $x_{1,2} \in G_{1,2}$ el. de ordin finit

$$ord(x_1, x_2) = [ord\, x_1, ord\, x_2].$$

$p = ord(x_1, x_2) \Rightarrow (x_1, x_2)^p = e$

$ord\, x_1 = m_1$

$ord\, x_2 = m_2$

$\begin{cases} x_1^p = e \\ x_2^p = e \end{cases} \Rightarrow \begin{cases} m_1 / p \\ m_2 / p \end{cases} \Rightarrow p = [m_1, m_2]$

$ord(\hat{3}, \bar{\bar{4}})$ în $\mathbb{Z}_{24} \times \mathbb{Z}_{36}$

$$ord(\hat{3}, \bar{\bar{4}}) = [ord(\hat{3}), ord(\bar{\bar{4}})] = [8, 9] = 72.$$

$x \in \mathbb{Z}_{24} \times \mathbb{Z}_{36}$, cu $ord(x) = 72$.

$x = (x_1, x_2) \qquad [ord\, x_1, ord\, x_2] = 72.$

$ord\, x_1 / 24$, $ord\, x_2 / 36$

$ord\, x_1 \in \{1, 2, 3, 4, 6, 8, 12, 24\}$

$ord\, x_2 \in \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$

$x \in \{(8, 9), (8, 18), (8, 36), (24, 9), (24, 18), (24, 36)\}$

$(8, 9)$

$\hat{3}, \hat{9}, \hat{15}, \hat{21}$

$\bar{\bar{4}}, \bar{\bar{8}}, \bar{\bar{16}}, \bar{\bar{20}}, \bar{\bar{28}}, \bar{\bar{32}}$

(26) $f, g : \mathbb{R} \to \mathbb{R}, \quad f(x) = x+1, \quad g(x) = 2x$

$G = \langle f, g \rangle$

$H_n = \langle g^{-n} f g^{n} \rangle$

$$g^{-n} f g^{n}(x) = g^{-n}(2^n x + 1) = x + \frac{1}{2^n}.$$

$\langle f_n \rangle \; H_n \subseteq H_{n+1} \iff f_n \in H_{n+1} = \langle f_{n+1} \rangle$

$$\cancel{f_{n+1} \circ f_{n+1}(x)} = f_{n+1}\left(x + \frac{1}{2^{n+1}}\right) = x + \frac{1}{2^n} = f_n(x).$$

$\cancel{f_{n+1}(x) = x +}$

$$f_{n+1}\left(x + \frac{1}{2^{n+1}}\right) = x + \frac{1}{2^{n+1}} + \frac{1}{2^{n+1}} = x + \frac{1}{2^n}.$$

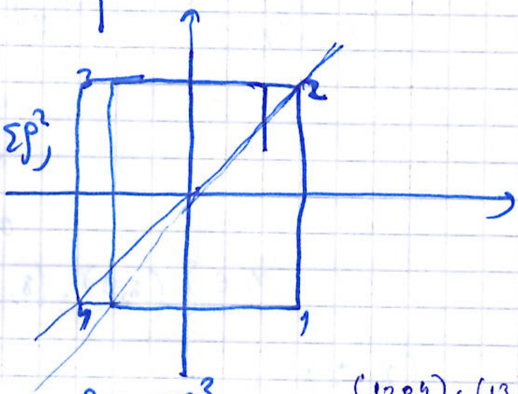
arăt că ~~pp.~~ $H_n \subsetneq H_{n+1}$.

pp. $H_n = H_{n+1} \Rightarrow f_{n+1} \in H_n \Rightarrow f_{n+1} = f_n^{k}, k \in \mathbb{Z}$.

$\Rightarrow x + \frac{1}{2^{n+1}} = x + \frac{k}{2^n} \Rightarrow k = \frac{1}{2} \in \mathbb{Z}$. Abs.

t: 14, 16 / pg. 18-19 cul. de pb. + 76, 78

Grupul diedral



$D_4 = \{ e, \rho, \rho^2, \rho^3, \varepsilon, \varepsilon\rho, \varepsilon\rho^2, \varepsilon\rho^3 \}$

ρ = rot. de $\frac{\pi}{2}$

$\rho \longleftrightarrow (1234)$

$\varepsilon \longleftrightarrow (13)$

ord $\rho = 4$, ord $\varepsilon = 2$

$\rho\varepsilon = \varepsilon\rho^3$

$3 \to 2$, $4 \to 1$, $1 \to 4$, $2 \to 3$

$(1234) \cdot (13) = \cancel{(1432)}$

$(13) \cdot (1432)$

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

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

cuaternioni ca matrice:

$\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\} \simeq \mathbb{C}$

$\left\{ \begin{pmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{pmatrix} \;\middle|\; z_1, z_2 \in \mathbb{C} \right\} = \mathbb{H}$ corp necomutativ

(29) $ord(x) = n \in \mathbb{N}^*$

$ord\, y = m \in \mathbb{N}^*$

$xy = yx, \quad (m,n) = 1 \Rightarrow ord(xy) = ord\, x \cdot ord\, y$.

$x^n = e \Rightarrow x^{n \cdot m} = e$

$y^m = e \Rightarrow y^{n \cdot m} = e$ $\Big| \Rightarrow (xy)^{nm} = e$

fie $p = ord(xy) \Rightarrow (xy)^p = e \Rightarrow p \mid m \cdot n$, $(m,n)=1$

$x^p = y^{-p} \Rightarrow x^{np} = y^{-np} \Rightarrow y^{-np} = e \Rightarrow y^{np} = e$, $m = ord\, y$ $\Big| \Rightarrow m \mid np$, $(m,n)=1$ $\Big| \Rightarrow$

$\Rightarrow m \mid p$

Analog, $n \mid p$, $(m,n)=1$ $\Big| \Rightarrow m \cdot n \mid p$, dar $p \mid mn$ $\Big| \Rightarrow p = mn$

$\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$ $\quad \underbrace{A^2}_{I_2} - (tr A) \cdot A + \underbrace{det A}_{-1} \cdot I_2 = O_2$

$tr A = 0$.

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

$AB = \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \quad (AB)^2 = O_2$

$B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

G un grup cu 6 el. este izomorf cu $\mathbb{Z}_6$ sau cu S_3.

$|G| = 6 \qquad S_3 = \langle \underset{ord\, 2}{(12)}, \underset{ord\, 3}{(123)} \rangle$

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad (12) \cdot (123) = (23)$

$xy =$

fie $x, y \in G$ cu $ord\, x = 2$, $ord\, y = 3$

$\{e, x, y, y^2, xy, xy$

$f(x) = \frac{pq}{ord\, x}$

El. de ordin 4 din $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$; $x = (\overline{x_1}, \overline{\overline{x_2}})$, $ord\, x = [ord\, x_1, ord\, x_2] = 4$,

$ord\, x_1 \in \{1, 2, 3, 4, 6, 12\}$, $ord\, x_2 \in \{1, 3, 5, 15\} \Rightarrow$

$x_1 \in \{3, 9\}$, $x_2 = 0$.

Rel. de congruență : $(x_1, x_2) \in \rho$ și $(y_1, y_2) \in \rho \Rightarrow (x_1 \cdot y_1, x_2 \cdot y_2) \in \rho$

ρ rel. de congr. pe $(G, \cdot)$:

a) $(x, y) \in \rho \Rightarrow (x^{-1}, y^{-1}) \in \rho$

ρ rel. de echivalență $\Rightarrow x^{-1} \rho x^{-1}$

$x \rho y$

ρ rel. de congruență

$\Rightarrow x^{-1} x \,\rho\, x^{-1} y \Rightarrow e \,\rho\, x^{-1} y$; $y^{-1} \rho y^{-1}$ $\Rightarrow$

$\Rightarrow y^{-1} \rho x^{-1} \xrightarrow{\rho \text{ rel. de echiv.}} x^{-1} \rho y^{-1} \Rightarrow (x^{-1}, y^{-1}) \in \rho$

b) $(x_1, x_2) \in \rho$, $(y_1, y_2) \Rightarrow (x_1 y_1^{-1}, x_2 y_2^{-1}) \in \rho$.

$\overset{a)}{\Rightarrow} (y_1^{-1}, y_2^{-1}) \in \rho$

$\rho\langle e \rangle = \{ x \in G \mid (x, e) \in \rho \}$ - subgrup al lui G.

Not.: $N \triangleleft G$ subgrup normal

a) $(N, \cdot)$ subgrup normal al lui $G \Leftrightarrow$

(b) $x N x^{-1} = N$, $\forall x \in G$

$xN = Nx \Leftrightarrow \forall g \in N, \exists g' \in N$ a.î. $xg = g'x \Leftrightarrow x g x^{-1} = g'$,

$\Rightarrow x N x^{-1} \subseteq N$ și analog și invers.

b) $\Rightarrow$ (c) $\rho_N = \rho_N'$

$x \rho_N y \Leftrightarrow x^{-1} y \in N \Leftrightarrow y \in xN$

$x \rho_N' y \Rightarrow \cancel{x} y x^{-1} \in N \Leftrightarrow y \in Nx$

(c) $\Rightarrow$ (d) $G / \rho_N = G / \rho_N'$.

$\rho_N = \rho_N' \Leftrightarrow \forall x \in G, \hat{x} = \overline{x} \Leftrightarrow G/\rho_N = G/\rho_N'$.

$xN = Ny$

$x \in xN \Rightarrow x \in Ny \Rightarrow x R_N^d y$

$x R_N^d y \Rightarrow x y^{-1} \in N \Rightarrow \exists n_1, n_2 \; x n_1 = n_2 y$ $\quad$ $N \cdot x = \{ n x \mid n \in N \}$.

$\Rightarrow Ny = Nx$.

d $\Rightarrow$ c) $x R_N^d y \Rightarrow x R_N^s y \Rightarrow x^{-1} y \in N \Rightarrow y \in xN$.

$xN = Ny$.

$\Rightarrow xN = Nx$.

În $(S_n, \circ)$, subgr. altern. $A_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\}$ este normal.

$$I_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = -1\}.$$

$\varepsilon(\sigma) = (-1)^{m(\sigma)}$ signatura lui σ

$$\varepsilon(\sigma) = \sum_{1\le i<j\le n} \frac{\sigma(j)-\sigma(i)}{j-i}$$

$$S_n = A_n \cup I_n.$$

τ transpoziție $\Rightarrow$ $I_n = A_n \circ \tau = \tau \circ A_n$.

$$\varepsilon(\sigma\cdot\theta) = \varepsilon(\sigma)\cdot\varepsilon(\theta)$$

$(i<j)$

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

$i+1, i+2, \dots, j-1, j$ $\quad (j-1)-i+2$

~~$j-i+1 \quad 1+2+\dots+j-i-1 =$~~ $\frac{(j-i-1)(j-i)}{2}$.

$i+1, \dots, j-1$

$$\varepsilon(\tau_{ij}) = \cancel{(-1)}^{\,j-i+1+\dots} \quad j-i+j-i-1 = -1.$$

- ρ congruență $\Leftrightarrow$ $\exists\, N \trianglelefteq G$ a.î. $\rho = \rho_N$

"$\Rightarrow$" fie $N = \rho\langle e\rangle = \{x\in G \mid x\rho e\} = \{x \in G \mid e\rho x\}$.

$x, y \in N \Rightarrow x\rho e,\ y\rho e \Rightarrow xy\,\rho\, e \Rightarrow xy \in N$.

$x\rho e \Rightarrow x^{-1}\rho e^{-1} = e \Rightarrow x^{-1}\in N \Rightarrow$ $\Big|\Rightarrow (N,\cdot)$ subgrup al lui G.

N normal: $xNx^{-1} = N$. $\forall x\in G$, $\forall g \in N = \rho\langle e\rangle$, $xgx^{-1}\in\rho\langle e\rangle$.

$x\rho x,\ g\rho e,\ x^{-1}\rho x^{-1} \Rightarrow xgx^{-1}\,\rho\, xx^{-1} = e \Rightarrow$

$xNx^{-1} \subset N$.

$\forall g\in N$, $\exists\, g' = x^{-1}gx \in N$ a.î. $g = x\cdot g'\cdot x^{-1} \Rightarrow N \subset xNx^{-1}$

$x\rho_N y \Leftrightarrow x^{-1}y \in N = \rho\langle e\rangle \Leftrightarrow$

$(x^{-1}y)\,\rho\, e \Leftrightarrow x^{-1}y^{-1}y\,\rho\, y \Leftrightarrow x\rho y$.

$\Rightarrow \rho = \rho_N\ (\rho_N')$.

"$\Leftarrow$" $x_1 \rho_N x_2 \Leftrightarrow x_1^{-1}x_2 \in N \Rightarrow x_2 \in x_1 N$.

$y_1 \rho_N y_2 \Leftrightarrow$ $\quad y_2 \in y_1 N$ $\Big|\Rightarrow x_2 y_2 \in (x_1 N)\cdot(y_1 N) =$

$= x_1 (y_1 N) N = (x_1 y_1) N \Rightarrow$

$\Rightarrow x_1 y_1\ \rho_N\ x_2 y_2 \Rightarrow$

$\Rightarrow \rho_N$ rel. de congruență.

$$F : C(G) \longrightarrow S_N(G)$$

$$F(\rho) = \rho\langle e\rangle$$

$$F^{-1} : S_N(G) \longrightarrow C(G)$$

$$F^{-1}(N) = \rho_N$$

~~$x' = f(x) \cdot f(\alpha) \cdot f(y) = \ldots$~~

$f : G \to G'$ morfism, $\operatorname{Ker} f = \{(x,y) \in G \times G \mid f(x) = f(y)\}$

$\downarrow$ relație echiv. pe G

$$\rho_{\ker f} = \ker f.$$

$$(x,y) \in \ker f \Leftrightarrow f(x) = f(y) \Leftrightarrow f(x)\cdot(f(y))^{-1} = e' \Leftrightarrow$$

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

$(x,y) \in \rho'_{\ker f} = \rho_{\ker f}$ ($\ker f$ este subgrup normal în G)

$$\forall x \in G, \forall y \in \ker f,\ x \cdot y \cdot x_G^{-1} \in \ker f.$$

$$f(x y x_G^{-1}) = f(x)\cdot f(y)\cdot f(x_G^{-1}) = f(x)\cdot e_{G'} (f(x))^{-1}_{G'} = e_{G'}.$$

Th. fund. de izom.: $f : G \to G'$ morfism $\Rightarrow G/\ker f \simeq \operatorname{Im} f$

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[dr, "p"'] & \operatorname{Im} f \\
& G/\ker f \arrow[u, "\bar{f}"']
\end{tikzcd}$$

$$p : G \to G/\ker f,\quad p(x) = \hat{x}$$

fie $\bar{f} : G/\ker f \longrightarrow \operatorname{Im} f$, $\bar{f}(\hat{x}) = f(x)$. $\quad f = \bar{f} \circ p$.

$\bar{f}$ bine definită: $\hat{x}_1 = \hat{x}_2 \Rightarrow x_2 \in x_1 \ker f \Rightarrow x_2 = x_1 \cdot \alpha,\ \alpha \in \ker f \Rightarrow$

$$\Rightarrow f(x_2) = f(x_1)\cdot f(\alpha) = f(x_1),\ \text{căci } f(\ker f) = \{e\}$$

$$\Rightarrow f(x_2) = f(x_1) \Rightarrow \bar{f}(\hat{x}_1) = \bar{f}(\hat{x}_2).$$

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

$\Rightarrow \bar{f}$ morfism.

$\hat{x} \in \ker \bar{f} \Leftrightarrow \bar{f}(\hat{x}) = e' \Leftrightarrow f(x) = e' \Leftrightarrow x \in \ker f \Leftrightarrow \hat{x} = \hat{e} \Rightarrow$

$\Rightarrow \ker \bar{f} = \{\hat{e}\}$ (~~ker f~~) $\Rightarrow \bar{f}$ inj.

$\forall y \in \operatorname{Im} f$, $\exists x \in G$ a.î. $y = f(x) \Rightarrow \exists \hat{x} \in G/\ker f$ a.î.

$y = \bar{f}(\hat{x}) \Rightarrow \bar{f}$ surj.

$\Rightarrow \bar{f}$ izomorfism $\Rightarrow G/\ker f \simeq \operatorname{Im} f$.

Th.: $f : G \to G'$ morfism surj. de gr.

$H \triangleleft G$, $\ker f \subset H \Rightarrow f(H) \triangleleft G'$.

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, "p"'] \arrow[dr, "g"] & G' \arrow[d, "p'"] \\
G/H \arrow[r, "\bar{f}"] & G'/f(H)
\end{tikzcd}$$

$p'(y) = y \cdot f(H)$

TIN

Fie $y \in G'$. f surj. $\Rightarrow \exists x \in G$ a.î. $f(x) = y$

$xH = Hx \Rightarrow f(xH) = f(Hx) \Rightarrow$

$f(x) \cdot f(H) = f(H) \cdot f(x)$ | $\Rightarrow yH' = H'y, \forall y \in G'$.

not. $H' = f(H)$

$\Rightarrow f(H)$ normal în G'.

$g = p' \circ f : G \to G'/f(H)$ morfism surjectiv pt care

aplicăm th fund. de izomorfism $\Rightarrow G/\ker g \simeq G'/f(H)$.

arăt că $\ker g = H$.

$x \in \ker g \Leftrightarrow g(x) = \hat{e}' \Leftrightarrow p'(f(x)) = \hat{e}' \Leftrightarrow$

$f(x) \in \ker p' = H' = f(H) \Leftrightarrow x \in H$.

(deoarece $\ker f \subset H$)

$\boxed{\text{Th. de corespondență:}}$ $H \subseteq K$, $H \triangleleft G$, $K \triangleleft G$

$$(G/H)/(K/H) \simeq G/K.$$

(A 3-a th. de izom. din curs)

Fie $f: G/H \to G/K$, $f(xH) = xK$. Se arată că f este bine definită; f morfism, f surj.: $\forall \bar{x} \in G/K, \exists \hat{x} \in G/H$ a.î. $f(\hat{x}) = \bar{x}$

$$\operatorname{Ker} f = \{xH \mid f(xH) = K\} \overset{H \subset K}{=} \{xH \mid x \in K\} = K/H.$$

și se aplică ~~prima th.~~ th. fundamentală de izomorfism.

A 2-a th. de izom.:

G grup, H, K subgr., $K \triangleleft G$ ⇒ 1) HK subgr. al lui G, 2) $H \cap K$ subgr. normal în H și 3) $HK/K \simeq H/H\cap K$.

Dem.: 1) $h_{1,2} \in H$, $k_{1,2} \in K$ ⇒ $h_1k_1, h_2k_2 \in HK$.

$$h_1k_1h_2k_2 = h_1h_2h_2^{-1}k_1h_2k_2 = h_1h_2(h_2^{-1}k_1h_2)k_2$$

$K \triangleleft G$ ⇒ $h_2^{-1}k_1h_2 \in K$ ⇒ $h_1k_1h_2k_2 \in HK$.

$$(hk)^{-1} = k^{-1} \cdot h^{-1} = h^{-1}(\underbrace{h k^{-1} h^{-1}}_{\in K}) \in HK \Rightarrow$$

⇒ HK subgrup al lui G.

2) $H \cap K$ este subgrup ca intersecție a 2 subgr. din G.

$K \triangleleft G$ ⇒ $xK = Kx$, $\forall x \in G$

$g k g^{-1} \in K, \forall g \in G$.

~~$\overset{?}{\Rightarrow}$ $k_H k^{-1} \in H \cap K$.~~

Fie $x \in H \cap K$. $\forall g \in H$, $gxg^{-1} \in H$

$x \in K$ ⇒ $gxg^{-1} \in K$ ⇒

⇒ $gxg^{-1} \in H \cap K$ ⇒ $H \cap K \triangleleft H$.

3) Fie $f : H \longrightarrow HK/K$, $f(h) = hK$.
(K e normal în HK)

$f(h_1)f(h_2) = h_1K \cdot h_2K \overset{K \trianglelefteq HK}{=} (h_1h_2)K = f(h_1h_2) \Rightarrow f$ morfism.

Fie $h_0 k_0 K$ un el. din HK/K. $h_0 \in K \Rightarrow h_0 k_0 K = h_0 K$.

$f(h_0) = h_0K \Rightarrow f$ morfism surjectiv.

$\ker f = \{ h \in H \mid \underbrace{f(h)}_{=hK} = K \} = H \cap K$

Din th fundamentală de izom.: $H / H \cap K \simeq HK/K$, c.c.t.d.

Temă: 76 $G = (\mathbb{Q}, +)/\mathbb{Z}$

a) $(a,b) = 1 \Rightarrow \mathrm{ord}\left(\widehat{\left(\frac{a}{b}\right)}\right) = b$.

$\mathrm{ord}\left(\widehat{\frac{a}{b}}\right) = n$ nr. minim a.î. $\underbrace{\frac{a}{b} + \frac{a}{b} + \dots + \frac{a}{b}}_{n \text{ ori}} \in \mathbb{Z} \Rightarrow n \cdot \frac{a}{b} \in \mathbb{Z} \Rightarrow$

$\Rightarrow b / na$, $(a,b) = 1 \Rightarrow b/n$, n minim $\Rightarrow n = b$.

b) Orice subgrup finit generat este ciclic finit.

$\langle q_1\mathbb{Z}, \dots, q_n\mathbb{Z} \rangle$

Pt. orice generatori $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots, \frac{p_n}{q_n}$, redefine generatorul $\frac{1}{s}$,

$s = [q_1, q_2, \dots, q_n]$, iar subgr. ciclic cu s el. $\langle \widehat{\frac{1}{s}} \rangle$ este finit.

c) Dacă $\mathrm{ord}\, G = n \in \mathbb{N}^*$, cf. th. lui Lagrange, $\mathrm{ord}\left(\widehat{\frac{a}{b}}\right) / n$,

dar cf. a) putem construi o clasă de ordin $n+1$ $\Rightarrow G$ nu e finit.

Dacă G ar fi finit generat, cf b), ar fi ciclic finit r.c.

78) $(\mathbb{R},+)/\mathbb{Z} \not\cong (\mathbb{R},+)/\langle\sqrt{2},\sqrt{3}\rangle \overset{not.}{=} H$

$e = \mathbb{Z}$

pp. c. $\exists f : (\ /\ )_{G_1} \to (\ /\ )_{G_2}$ izomorfism.

$\frac{\sqrt{2}}{2} + \langle\sqrt{2},\sqrt{3}\rangle + \frac{\sqrt{2}}{2} + \langle\sqrt{2},\sqrt{3}\rangle = \langle\sqrt{2},\sqrt{3}\rangle \Rightarrow$

$= (\frac{\sqrt{2}}{2}, \sqrt{3}, \sqrt{3})$ $\sqrt{2} + <$ ...

$ord\left(\widehat{\frac{\sqrt{2}}{2}}\right)_{G_2} = 2.$

$\sqrt{2}, \sqrt{2} + \frac{\sqrt{2}}{2}, \frac{\sqrt{3}+\sqrt{3}}{2} = \sqrt{3}, \sqrt{3} \to \frac{\sqrt{2}+\sqrt{3}}{2}$

$2\sqrt{2}$

$ord\left(\widehat{\frac{\sqrt{3}}{2}}\right) = 2$

$\sqrt{2} + \langle\sqrt{2},\sqrt{3}\rangle = \langle\sqrt{2},\sqrt{3}\rangle$ (?cu coef. reale)

$ord\left(\widehat{\frac{\sqrt{2}+\sqrt{3}}{2}}\right) = 2.$

$(\sqrt{2} + \frac{\sqrt{3}}{2}) + H =$

$\Rightarrow G_2$ are 3 el. de ordin 2.

$(\mathbb{R},+)$ are un el. de ordin 2: $\widehat{\frac{1}{2}}$.

$2\hat{x} + \mathbb{Z} = \mathbb{Z} \Rightarrow 2\hat{x} \in \mathbb{Z}$ și $\hat{x} \notin \mathbb{Z} \Rightarrow$

$\hat{x} = \cancel{\frac{1}{2}} \cancel{\ldots} \widehat{n+\frac{1}{2}} = \widehat{\frac{1}{2}}.$

f morfism $f(x^2) = (f(x))^2 = \langle\sqrt{2},\sqrt{3}\rangle \Rightarrow f(x)$ are 3 posibilități și x unic $\Rightarrow$

$f\left(\left(\widehat{\frac{1}{2}}\right)^2\right) =$

$\Rightarrow f$ ori nu e inj.,

$f(\mathbb{Z}) = \cancel{f(}\langle\sqrt{2},\sqrt{3}\rangle\cancel{)} =$

ori nu e surj.

$\Rightarrow f$ nu e bij.

---

14) $j = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \; k = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ în $GL(2,\mathbb{C})$

$J = \langle j\rangle, \; K = \langle k\rangle, \; Q = \langle j,k\rangle$

i) $j^2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

$j^3 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix}$

$j^4 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$

$\Rightarrow |J| = 4.$

$k^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

$k^3 = \begin{pmatrix} \cancel{0} & \cancel{1} \\ \cancel{-1} & \cancel{0} \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cancel{0} & \cancel{-1} \\ \cancel{1} & \cancel{0} \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

$k^4 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \cancel{0} & \cancel{-1} \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$

$\Rightarrow |k| = 4.$

$|J \cap K| = 2 \; (j^2 = k^2,\ j^4 = k^4 = I_2 = e)$

(L-am rezolvat la iv)

ii) $J, K \triangleleft Q$

$g j g^{-1} \in J,\ \forall g \in Q = \langle j, k \rangle \Rightarrow g = j^a \cdot k^b,\ a, b \in \mathbb{N}.$

$g^{-1} = k^{-b} \cdot j^{-a}.$

$g \cdot j \cdot g^{-1} = j^a \cdot k^b \cdot j \cdot (k^b)^{-1} \cdot (j^a)^{-1} = j^a \cdot k^{b-1} \cdot (-I_2) \cdot (k^b)^{-1} (j^a)^{-1}$

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

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

$k \cdot j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = j \cdot k \cdot (-I_2)$

$g \cdot j \cdot g^{-1} = -I_2 \cdot j^a \cdot k^{-1} \cdot \underbrace{k^b (k^b)^{-1}}_{I_2} (j^a)^{-1}$

$\det k = 1.$ $\quad j^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$ $\quad j^2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = k^2.$

$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\quad k^{-1} = k^3$

$\cancel{g \cdot j \cdot g^{-1} = -I_2 \cdot j^{a-2} \cdot j^2 \cdot k^{-1}}$

$g \cdot j \cdot g^{-1} = j^a \cdot k^{b-1} \cdot j \cdot k \cdot (-I_2) (k^b)^{-1} (j^a)^{-1} = (\dots)$

(reduc toate puterile lui k) $= j^{a+b} \cdot (-I_2)^b \cdot (j^{a+b})^{-1} \in$

$(-I_2)^1 j^a \cdot k^{b-2} \cdot (k \cdot j) \cdot (k^{b-1})^{-1} \cdot (j^a)^{-1} = \cancel{-I_2} (-j)^b \in$

$-I_2 \cdot jk$

$= (-I_2)^b \cdot j^a \cdot j \cdot (j^a)^{-1} = (-I_2)^b \cdot j \in J?$ $\quad = (j^3)$

$|Q| = 8: \quad j,\ j^2 = k^2,\ j^3,\ I_2,\ k,\ k^3,\ j \cdot k,\ k \cdot j.$

iii) $x^2 = I_2$, $x = j^a \cdot k^b$

$$(j^a \cdot k^b)^2 = I_2 \Rightarrow$$

$$j^a \cdot k^b \cdot j^a \cdot k^b = I_2.$$

$j^2 \neq I_2$, $(j^2)^2 = (k^2)^2 = I_2$, $(j^3)^2 = j^2 \neq I_2$, $\text{ord } I_2 = 1$,

$(k^3)^2 = k^2 = j^2 \neq I_2$, $(j \cdot k)^2 = (k \cdot j)^2 = -I_2$.

iv) Q nu este abelian, căci $j \cdot k \neq k \cdot j$

Subgrupurile lui Q: $\{I_2\}$, J, K, $Q = \langle J, K \rangle$

Cf. th. lui Lagrange, $[Q : J] = \frac{|Q|}{|J|} = \frac{8}{4} = 2 \Rightarrow$

$\Rightarrow Q = J \cup xJ$, cu $x \in Q \setminus J = K$, iar

$J \cap xJ = \emptyset$

Dacă $x \in K$, at. $\left.\begin{array}{l} xJ \neq J \\ xJ \in Q = J \cup xJ \end{array}\right\} \Rightarrow xJ = Jx \Rightarrow$

$\Rightarrow J$ este subgrup normal.

Analog, K este subgrup normal.

16 i) $G = \{e, x, y, xy\}$. Cf. th. Lagrange, $\text{ord } x \mid \text{ord } G = 4 \Rightarrow$

- $\text{ord } x = 4 \Rightarrow G = \langle x \rangle \Rightarrow G \simeq \mathbb{Z}_4$, cu $f(x) = 1$

sau

- $\text{ord } x = 2 \Rightarrow x^2 = e$ $\left[\begin{array}{l} y^2 = e \\ y^4 = e \Rightarrow G = \langle y \rangle \text{ analog cazului anterior.} \end{array}\right.$ $\left[\begin{array}{l} (xy)^2 = e \Rightarrow G \text{ abelian} \Rightarrow \\ (xy)^4 = e \ldots \end{array}\right.$

şi $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ (ex. rez. la seminar, $G = \langle x, y \rangle$).

ii)

ii) $|G| = 6 \Rightarrow G \simeq \mathbb{Z}_6$ sau $G \simeq S_3$.

· G ciclic $\Rightarrow G \simeq \mathbb{Z}_6$, cu f izom., $f(x) = \varphi$, unde $\langle x \rangle = G$.

· altfel, cf. th. lui Cauchy, $|G| = 2\cdot 3 \Rightarrow \exists\, b \in G$ cu $ord(b) = 2$,
$\exists\, a \in G$, cu $ord(a) = 3$

iar $ord(x) \in \{1,2,3,6\}$, cf. th. Lagrange. G nu e ciclic $\Rightarrow$

$\Rightarrow ab \neq ba \Rightarrow G = \{e, a, a^2, b, ab, a^2b\}$.

~~$ab = ba \Rightarrow b = a^2ba \Rightarrow$~~ $\Rightarrow \boxed{ba = a^2b}$ $\quad ab = ba^2$

~~$ba = a^2b$~~.

dacă $ab = ba$.
- $ord(ab) = 2 \Rightarrow ab \cdot ba = a^2 = e$ n.c.
- $ord(ab) = 3 \Rightarrow (ba)^3 = b^3a^3 = b \neq e$ n.c.
- G n.c.

$\Rightarrow$

$\cdot$	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b						
ab	ab	b	ab	a	—	
a^2b	a^2b	ab	b	a^2	a	e

fie $\varphi : G \to S_3$, $\varphi(e) = 1$, $\varphi(a) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$,
$ord(\varphi(a)) = 3$

$\varphi(b) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. $ord(\varphi(b)) = 2$.

$\varphi(a^2) \overset{def}{=} \varphi(a)\cdot\varphi(a) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$

$\varphi(ab) = (13)$

$\varphi(a^2b) = (23)$

iii) $|G| = 8 \Rightarrow G \simeq D_4$ sau $G \simeq Q$ sau $G \simeq \mathbb{Z}_8$ sau $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$

sau $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

iv) p prim și $|G| = p \Rightarrow G \simeq \mathbb{Z}_p$.

Fie $x \in G$, $x \neq e$. ~~$\langle g \rangle$ conține mai mult de~~

$|\langle g \rangle| \geq 2$ și $|\langle g \rangle| \leq |G|$.

Cf. th. lui Lagrange, $|\langle g \rangle| \mid |G| = p$ prim $\Rightarrow$

$\Rightarrow |\langle g \rangle| = p = |G| \Rightarrow G = \langle g \rangle$.

iii) $\exists x \in G$ de ordin $8 \Rightarrow G$ ciclic $\Rightarrow G \simeq \mathbb{Z}_8$

Cf. th. Lagrange, el. au ordin 2 sau 4.

caz 1: $\nexists$ el. de ordin 4 $\Rightarrow$ toate el. au ordin 2 $\Rightarrow G$ abelian.

și $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ * ($G = \langle a, b, c \rangle$ și luăm

$f(a) = (1,0,0)$, $f(b) = (0,1,0)$, $f(c) = (0,0,1)$).

caz 2: $\exists a$ de ordin $4 \Rightarrow H = \langle a \rangle = \{e, a, a^2, a^3\}$.

• Dar fie $b \in G \setminus H$ de ordin 2.

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

Curs 8

Grupuri ciclice:

$\varphi: \mathbb{Z} \to G$, $\varphi(n) = a^n$

φ morfism surj. de gr.

I. G infinit $\quad \ker\varphi = \{0\} \Rightarrow \varphi$ izom.

II. $\ker\varphi \neq \{0\} \Rightarrow \ker\varphi = n\mathbb{Z}, n \geq 1 \quad$ TFIG $\Rightarrow \mathbb{Z}/n\mathbb{Z} \simeq G$.

Grupuri de permutări

$S(A) = \{ f: A \to A \mid f \text{ bij.} \}$

$(S(A), \circ)$ grup comutativ $\Leftrightarrow |A| \leq 2$

$A \sim A'$ (adică $\exists\, \varphi: A \to A'$ bij.) $\Rightarrow (S(A), \circ) \simeq (S(A'), \circ)$

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, shift right, "\varphi"'] & S(A) \arrow[d, "\varphi"] \\ A' \arrow[r, "\bar{f}"] \arrow[u, shift right, "\varphi^{-1}"'] & S(A') \end{tikzcd}$$

$$f \longrightarrow \varphi \circ f \circ \varphi^{-1} = \bar{f}$$

$$\varepsilon(\sigma) = \sum_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = (-1)^{\text{inv}(\sigma)}$$

$\varepsilon: S_n \to \{-1, 1\}$ morfism surjectiv

$\ker \varepsilon = A_n$

din TFIG: $\dfrac{S_n}{A_n} \simeq \{\pm 1\} \qquad [S_n : A_n] = 2 \Rightarrow |A_n| = \dfrac{n!}{2}$.

$\sigma = (i_1\ i_2 \dots i_m) \in S_n$, $\sigma^{-1} = (i_m\ i_{m-1} \dots i_1)$

$$\begin{pmatrix} 1\,2 \dots i_1 \dots i_2 \dots i_m \dots \\ 1 \dots i_2 \dots i_3 \dots i_1 \dots \end{pmatrix} \cdot \begin{pmatrix} 1 \dots i_1 & \\ \dots i_m & \end{pmatrix} = e$$

$O_\gamma = \{i_1, \dots, i_m\}$ - orbita ciclului.

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

$O_{\gamma_1} \cap O_{\gamma_2} = \emptyset$ cicli disjuncți

$\gamma_1 \cdot \gamma_2 = \gamma_2 \cdot \gamma_1$

Seminar 8

- Gr. abeliene cu 8 el.

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

$D_4 = \{e, \varepsilon, \rho, \rho^2, \rho^3, \varepsilon\rho, \varepsilon\rho^3, \varepsilon\rho^2\}$

Subgr. cu 2 el.: $H_1 = \{e, \rho^2\}$, $H_2 = \{e, \varepsilon\}$, $H_3 = \{e, \varepsilon\rho\}$

$(\varepsilon\rho)^2 = \varepsilon(\rho\varepsilon)\rho = \varepsilon \cdot \varepsilon\rho \cdot \rho^3 = e \cdot \rho^4 = e$

$(\varepsilon\rho^2)^2 = \varepsilon\rho^2 \cdot \varepsilon\rho^2 = \varepsilon\rho \cdot (\rho\varepsilon) \cdot \rho^2 = \varepsilon\rho \cdot \varepsilon\rho^3 \cdot \rho^2 = \varepsilon\rho \cdot \varepsilon\rho = (\varepsilon\rho)^2 = e$

$H_4 = \{e, \varepsilon\rho^2\}$, $H_5 = \{e, \varepsilon\rho^3\}$

Subgr. cu 4 el.: $H_6 = \langle\rho\rangle = \{e, \rho, \rho^2, \rho^3\}$, $H_7 = \{e, \varepsilon\rho, \rho^2, \varepsilon\rho^3\}$,

$H_8 = \{e, \rho^2, \varepsilon, \varepsilon\rho^2\}$.

$H_6, H_7, H_8 \trianglelefteq D_4$

$H_1 = H_6 \cap H_7 \trianglelefteq D_4$

$\rho H_2 \rho^{-1} = \{e, \rho\varepsilon\rho^{-1}\} \neq H_2$

H_2, H_3, H_4, H_5 nu sunt normale

$\{\hat{e}, \hat{\rho}, \hat{\varepsilon}, \widehat{\varepsilon\rho}\} = D_4 / H_1 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ (de tip Klein)

$\hat{\rho}^2 = \hat{e}$

$\hat{\varepsilon}^2 = \hat{e}$

$\widehat{\varepsilon\rho}^2 = \hat{e}$

$\widehat{\varepsilon\rho^3} = \hat{\varepsilon} \cdot \hat{\rho}^2 \cdot \hat{\rho} = \widehat{\varepsilon\rho}$

$\widehat{\varepsilon\rho^2} = \{\varepsilon\rho^2, \varepsilon\} = \hat{\varepsilon}$

$\widehat{\varepsilon\rho^3} = \{\varepsilon\rho^3, \varepsilon\rho\} = \widehat{\varepsilon\rho}$

$U(\mathbb{Z}_{12}) = \{1, 5, 7, 11\} = K$

$\hat{5} \cdot \hat{7} = \hat{35} = \hat{11}$

0,0 0,1 1,0 1,1

$ij = k = ji^3 = j \cdot (-i) = k$, $i^2 = j^2 = -1$

$Q_8 = \langle i, j \rangle$ ord i = ord j = 4

A

(79) $(\mathbb{Z}^2,+)/\langle 2,3\rangle$ ciclic infinit

$(\mathbb{Z}^2,+)/\langle 2,2\rangle$ nu e ciclic

Fie $(a,b)\in\mathbb{Z}^2$.

I. $a=2k+1 \Rightarrow (\widehat{a,b})=(\widehat{1,b-3k})$

II. $a=2k \Rightarrow (\widehat{a,b})=(\widehat{0,b-3k})$

$(\widehat{0,a})$

$(\widehat{1,a})$

$\mathbb{Z}^2/\langle(2,3)\rangle=\{(\widehat{0,a}),(\widehat{1,b})\mid a,b\in\mathbb{Z}\}$.

$\times t$: cule de pb. pg. 24 : 59, 60, 61, 62, 66, 68 : ~~Demonstrație~~

(59) $\sigma^2=\pi_1^2\ldots\pi_n^2\,\underbrace{(\pi_i\tau_j)^2}_{=e}=(12)(3456)$

lg π_i impară $\Rightarrow$ lg π_i^2 impară (tot ciclu)

lg π_i pară $\Rightarrow$ $\pi_i^2=\gamma_1\gamma_2$ — cicli disjuncți

lg $\gamma_1=$ lg $\gamma_2=\dfrac{\text{lg }\pi_i}{2}$.

(57) $\tau=(i_1\ldots i_n)\in S_n$

τ^k se desc. în produs de $d=(k,n)$ ciclii de lg. n/d.

dem.: $k=dk_1$, $n=dn_1$, $(n_1,k_1)=1$. $\tau^k=(\tau^d)^{k_1}$.

$\tau^d(i_1)=i_{d+1}$, $\tau^d(i_{d+1})=i_{2d+1}$, ..., $\tau^d(i_{(n_1-1)d+1})=i_{n+1}=i_1$

$\tau^d(i_2)=i_{d+2}$, ..., $\tau^d(i_{(n-d)+2})=i_{2n}=i_2$

$0,1,\ldots,n-1$

$\tau\to\tau^d=\tau_1\ldots\tau_d$, $\tau_j=(i_j,i_{d+j},\ldots i_{(n_1-1)d+1})$,

$j=\overline{1,n}$ → ciclii disjuncți de lg. $n_1=\dfrac{n}{d}$.

$\tau^{dk_1}=\tau_1^{k_1}\cdot\ldots\cdot\tau_d^{k_1}$.

? $\tau_1^{k_1},\ldots,\tau_d^{k_1}$ ciclii disjuncți de lg. n_1, cu ac. orbite ca $\tau_1,\ldots,\tau_d$

$\tau=\tau_1\ldots\tau_d$, $\tau^{k_1}=\pi_1\pi_2\ldots\pi_n$.

caz 1: $j \notin O_{\gamma_1} \cup O_{\gamma_2}$ F

caz 2: $j \in O_{\gamma_1}$

$$(\gamma_1 \circ \gamma_2)(j) = \gamma_2(\gamma_1(j)) = \gamma_1(j) \qquad \cancel{(\gamma_2 \circ \gamma_1)(j)} =$$

caz 3: $j \in O_{\gamma_2}$

$$\operatorname{ord}(\gamma_1 \gamma_2) = [\operatorname{ord}\gamma_1, \operatorname{ord}\gamma_2]$$

$$|O_\gamma| = l(\gamma)$$

ex.: pe $(\mathbb{Q}/\mathbb{Z}, +)$ nu se poate defini o str. de inel unitar

Butterfly Curs 9 $(R_i)_{i \in I}$ familie nevidă de inele unitare: $U(\prod R_i) = \prod U(R_i)$

$G = \bigcup_{x \in G} xH$; H normal $\Rightarrow$ $x \cdot h \cdot x^{-1} \in H$ or $xH = Hx$.

Ideal: $\forall a \in R$, $x \in I \Rightarrow ax \in I$
xa

Idealele lui $\mathbb{Z}$: $n\mathbb{Z}$

$\mathbb{Z}_n$: $d\mathbb{Z}_n$, d/n

$\mathbb{Q}$:

K(corp): $\{0\}, K$

$$(x)_s = \{ax \mid a \in R\}$$

$$R = \mathbb{Q}[X] \Rightarrow (X) = \{X \cdot f(X) \mid f(X) \in \mathbb{Q}[X]\}$$

$$(X^2+1) = \{(X^2+1) f(X) \mid f(X) \in \mathbb{Q}[X]\}$$

$$(X, X^2+1) = \{X f(X) + (X^2+1) g(X) \mid f, g \in \mathbb{Q}[X]\} = \mathbb{Q}[X].$$

$$f(X) = -X$$
$$g(X) = 1$$

$$\mathbb{Q} \simeq \mathbb{Q}[X]/(X).$$

Idealele lui R/I : $J \longmapsto p(J)$, J ideal din R care conține pe I.

$$J \supseteq I \qquad p(J) = J/I = \{\hat{a} \mid a \in J\}.$$

$$\frac{R/I}{J/I} \simeq R/J.$$

Seminar 9

(60) $p \mid n$

p prim

$\sigma \in S_n$, $\sigma^p = e \Rightarrow \exists\, i$ a.î. $\sigma(i) = i$

$\sigma = \pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_k$

$\sigma = [\,l(\pi_1), l(\pi_2), \ldots, l(\pi_k)\,] = p \Rightarrow \exists\, j$ a.î. $l(\pi_j) = 1 \Rightarrow \pi(j) = j$.

$l(\pi_i) = p$, $i = \overline{1,k} \Rightarrow p \cdot k = n$! $\alpha\varphi$

(61) i) $S_n = \langle (12), (13), \ldots, (1n) \rangle$

Fie transpoziția $(i_1\ i_2)$, $1 \le i_1 < i_2 \le n$.

$(i_1\ i_2) = (1\ i_2)(1\ i_1)(1\ i_2)$

ii) $(12), (23), \ldots, (n-1, n)$

arăt că $(1\ a) = \cancel{(12)(23)\ldots(a-1,a)}$

$(a-1, a) \cdot (\ldots (2\,3)(1\,2)(2\,3) \ldots (a-1, a)$

iii) $S_n = \langle (12), (12 \ldots n) \rangle$

$\sigma\,(i_1\ i_2 \ldots i_k)\,\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2) \ldots \sigma(i_k))$

$j \notin \{\sigma(i_1), \ldots, \sigma(i_k)\}$

$\sigma^{-1}(j) \notin \{i_1, \ldots, i_k\}$

$j = \sigma(i_1) \to \sigma(i_2)$

$\sigma\,(12)\,\sigma^{-1} = (\sigma(1)\ \sigma(2))$

$\quad 2 \quad 3$

(59) $A_n = \{\sigma^2 \mid \sigma \in S_n\} \Leftrightarrow n \le 5$

$(12)\cdot(3456) \not\exists\, \sigma^2$

$\sigma = \pi_1 \pi_2 \dots \pi_r \longrightarrow$ desc. unică

$lg(\pi_i)$ impară $\Rightarrow \pi_i^2$ ciclu de lungime impară

$lg(\pi_i)$ pară $\Rightarrow \pi_i^2 = \gamma_1 \gamma_2$ – ciclii disjuncți și

$lg(\gamma_1) = lg(\gamma_2) = \frac{1}{2} l(\pi_i)$

(66) $K = \{e, (12)(34), (13)(24), (14)(23)\} \le S_4$.

i) $K \triangleleft S_4 \Leftrightarrow \sigma K \sigma^{-1} \subseteq K, \forall \sigma \in S_4$

$\sigma(12)(34)\sigma^{-1} = \sigma(12)\sigma^{-1}\sigma(34)\sigma^{-1} = (\sigma(1)\ \sigma(2))\cdot(\sigma(3)\ \sigma(4))$

$\Rightarrow K \triangleleft S_4 \Rightarrow K \triangleleft A_4$.

ii) $S_4/K \simeq S_3$

$|S_4/K| = \frac{|S_4|}{|K|} = \frac{4!}{4} = 3! = 6$ A_n

$C_4^2 = \frac{4!}{2!2!}$

$C_4^3 \cdot 2! = 8$

$S_4 = \{e, 2\text{-ciclii}, 3\text{-ciclii}, 4\text{-ciclii}, \text{produse de 2 transpoziții}\}$.

2-ciclii → 6, 3-ciclii → 8, 4-ciclii → 6, produse de 2 transpoziții → 3

S_4/K nu are el. de ordin 6 $\Rightarrow S_4/K \not\simeq \mathbb{Z}_6 \Rightarrow S_4/K \simeq S_3$.

iii) $\not\exists\, H \le A_4$ a.î. $ord(H) = 6$

Pp. că $\exists$ a.î. $ord\, H = 6 \Rightarrow H \simeq \mathbb{Z}_6$ sau $H \simeq S_3$.

nu există $\sigma \in A_4$ a.î. $ord\, \sigma = 6$

El. de ordin 2 din S_3 sunt: $(12), (13), (23)$

$\Rightarrow H$ are exact 3 el. de ordin 2 $\Rightarrow K \le H$

$|K| \mid |H|$ n.c.

$4 \quad 6$

iv) Subgr. normale ale lui A_4 sunt $\{e\}, K$ și A_4.

$\{e\}$

2 el. $\{e, (12)(34)\} \ntriangleleft A_4$

3 el. — analog ~~$\{e, (12), (34), (12)(34)\}$~~.

4 el. K

12 el. A_4

$\sigma \in A_4$

$\sigma = (123)$

$\sigma \cdot (12)(34)\sigma^{-1} = (\sigma(1)\ \sigma(2)) \cdot (\sigma(3)\ \sigma(4)) \notin \{e, (12)(34)\}$

$2 \quad 3 \quad 1 \quad 4$

v) Subgr. normale ale lui S_4 : $\{e\}, K, A_4, S_4$.

H subgr. normal în $S_4 \Rightarrow H \cap A_4 \trianglelefteq A_4 \Rightarrow H \cap A_4 \in \{e, A_4, K\}$.

$H \cap A_4 = A_4 \Rightarrow A_4 \le H \le S_4$ m.c. de th. Lagrange $\Rightarrow$ egalități.

$H \cap A_4 = K \Rightarrow \quad K \le H \le S_4$

$H \cap A_4 = \{e\}$ n.c.

$K \subset H$.

$H \not\subseteq A_4 \Rightarrow \exists\, \tau \in H$, τ impară

$\tau = (ij)$

$H \trianglelefteq S_4$ $\Bigg| \Rightarrow H = S_4$.

$\sigma \tau \sigma^{-1} = (\sigma(i)\ \sigma(j))$

τ : 4-ciclu $\Rightarrow H$ conține toate 4-ciclurile $\Rightarrow H = S_4$.

$\tau = (ijkl) \Rightarrow \tau^2 = (ik)(jl) \in H \Rightarrow K \le X \Rightarrow$

$|K| \ge 6 + 8 = 14$

$(ijkl)(iljk) = (jlk) \Rightarrow$

$\Rightarrow$ conține

$\Rightarrow K = S_4$.

t: pb. de la finele din curs

Curs – Permutări

Lagrange $|S_n| = |S_n : \overline{S_{n-1}}| \cdot |\overline{S_{n-1}}|\ (n-1)!$

$\downarrow$

nr. claselor de echivalență mod $\overline{S_{n-1}}$

$\sigma \underset{s}{\equiv} \tau \,(\mathrm{mod}\, \overline{S_{n-1}})$ ~~$\sigma, \tau \in S_n$~~ $\Leftrightarrow \sigma^{-1}\tau \in \overline{S_{n-1}} \Leftrightarrow \sigma^{-1}\tau(n) = n \Leftrightarrow \tau(n) = \sigma(n) \Rightarrow$

$\Rightarrow n$ clase $\Rightarrow |S_n| = n \cdot (n-1)! = n!$

$\varepsilon(\sigma) = (-1)^{\mathrm{inv}(\sigma)}$ $\qquad \varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}$

$k+1 \ldots \quad (l-k) + (l-k-1) = 2(l-k) - 1$.

$$\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)}; \quad \varepsilon(\sigma \circ \tau) = \prod \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \cdot \frac{\tau(j) - \tau(i)}{j - i}$$

$= \varepsilon(\sigma) \cdot \varepsilon(\tau)$.

$$\sigma = (i_1\ i_2\ \dots\ i_m) = (i_2\ i_3\ \dots\ i_m\ i_1) = \dots = (i_m\ i_1\ \dots\ i_{m-1})$$

nr. ciclurilor de lg. m : $C_n^m \cdot (m-1)!$

$a_1, \longrightarrow a_k$ $\quad (a_1\ a_2\ a_3\ a_4)$

$(a_1\ a_2\ a_4\ a_3)$

$a_1 ? a_i$

$(a_1\ a_{i_1} \dots a_{i_k}\ a_{i_{m-1}})$

$\left(\begin{matrix} i_1 \dots i_2 \dots i_m \\ i_2 \dots i_3 \dots i_1 \end{matrix} \right) \left(\begin{matrix} i_1 \dots i_m \\ \dots i_{m-1} \end{matrix} \right) = (\quad)$

$$\sigma^{-1} = (i_m\ i_{m-1}\ \dots\ i_1)$$

$$\mathrm{ord}(\sigma) = m.$$

$$\sigma^k(i_1) = i_{k+1}$$

$\boxed{\sigma\tau = \tau\sigma}$, $\mathrm{ord}(\overset{m}{\sigma\tau}) \overset{?}{=} \mathrm{cmmmc}(\mathrm{ord}\overset{k}{\sigma}, \mathrm{ord}\overset{l}{\tau}) \overset{not.}{=} u$

$r \in \overline{1,n}$ arbitrar: $r \notin A \cup B \Rightarrow \sigma(r) = r$ și $\tau(r) = r \Rightarrow$

$$\sigma(\tau(r)) = \sigma(r) = r = \tau(\sigma(r)).$$

~~$r \notin A, r \in B \Rightarrow \tau(r) =$~~

$r \in A, r \notin B$: $\quad \tau(r) = r, \quad \sigma(\tau(r)) = \sigma(r).$

$\tau(\sigma(r)) = \tau(\sigma(\tau(r))) \cancel{= \tau(}$

$\sigma(r) \in A \Rightarrow \sigma(r) \notin B \Rightarrow \tau(\sigma(r)) = \sigma(r)$

~~$\sigma(\tau(r)) =$~~

$\mathrm{ord}\,\sigma = k, \mathrm{ord}\,\tau = l.$

$$\mathrm{ord}(\sigma\tau) = m$$

$(\sigma\tau)^m = e$ | $\sigma\tau = \tau\sigma \Rightarrow \sigma^m\tau^m = e$; $\sigma^m = \tau^{-m}$.

$\Rightarrow \begin{matrix} k/m \\ l/m \end{matrix} \Big| \Rightarrow u/m$ $\quad \sigma^m \neq e \Rightarrow \exists r$ a.î. $\sigma^m(r) \neq r \Rightarrow r \in A$ (altfel $\sigma(r)$ $\sigma(\sigma(r)) = r$)

$(\sigma\tau)^u = \sigma^u \tau^u = (\sigma^k)^i (\sigma^l)^j = e \Rightarrow m/u$ $\quad \sigma^m(r) = \tau^{-m}(r) \Rightarrow$

$\tau^{-m}(r) \neq r \Rightarrow \tau^m(r) \neq r \Rightarrow r \in B.$

$\sigma = \tau_1 \tau_2 \dots \tau_t$ → dsc. în cicli disjuncți

$\mathrm{ord}\,\sigma = \cancel{\text{cm}}$ cmmmc$(\mathrm{ord}\,\tau_1, \mathrm{ord}\,\tau_2 \dots \mathrm{ord}\,\tau_t)$

$\sigma\tau = \tau\sigma$

Th.: $n_\sigma = |\{i \mid \sigma(i) \neq i\}|$

$\sigma(i) \neq i \Rightarrow \sigma(\sigma(i)) \neq \sigma(i)$. $n_\sigma \geq 2$.

$\sigma \in S_n \Rightarrow$

$\sigma(i_1) \neq i_1$. not. $i_2 = \sigma(i_1)$, $i_3 = \sigma(i_2)$ ... $i_{k+1} = \sigma(i_k) = \sigma^k(i_1)$

$t = \mathrm{ord}(\sigma) \Rightarrow \sigma^t = e \Rightarrow \sigma^t(i_1) = i_1 \Rightarrow i_{t+1} = i_1$

$i_r = i_s$, $r+1$, $1 \leq r, s \dots \Rightarrow \sigma^{r-1}(i_1) = \sigma^{s-1}(i_1) \Rightarrow \sigma^p(i_1) = i_1 \dots$

fie $\tau = (i_1\ i_2 \dots i_m)$ și $\sigma' = \tau^{-1}\sigma$.

știm că $\sigma(i_1) \neq i_1$.

~~$\sigma(\sigma(i_1)) = \sigma(i_1) = i_2$~~

$\sigma(i_k) = i_k \Leftrightarrow \cancel{\sigma(i_k) = \sigma^{k-1}(i_1)}$

$i_{k+1} = \sigma^k(i_1) = \sigma^{k-1}(i_1) \Rightarrow \sigma(i_1) = i_1$.

$\Rightarrow \tau^{-1}(i) = i \Rightarrow \sigma'(i) = i$.

~~$\sigma'(i) = \tau^{-1}(\sigma(i))$~~

$i_k \in \{i_1, \dots, i_m\} \Rightarrow \sigma(i_k) = i_{k+1}$

$\sigma'(i_k) = \tau^{-1}(\sigma(i_k)) = i_k$.

$\tau^{-1} = (i_m\ i_{m-1}\ i_{m-2} \dots i_1)(\ i_k\ i_{k+1}\ )$

$\sigma(i) = i \Rightarrow \sigma'(i) = i$, $i \neq i_k$

$\sigma'(i_k) = i_k$, $k = \overline{1,m}$

$\Rightarrow n_{\sigma'} < n_\sigma \Rightarrow$

inducție ipotetic

$\sigma' = \tau_2 \dots \tau_t \Rightarrow \sigma^{-1}\sigma = \tau_2 \dots$

$\sigma = \tau_1 \tau_2 \dots \tau_t$

Obs: $\sigma = (i_1\ i_2 \dots i_m) = (i_1\ i_m)(i_1\ i_{m-1}) \dots (i_1\ i_2) = (i_1 i_2) \dots$

$$\begin{array}{ccc} A & \underset{f^{-1}}{\overset{f}{\rightleftarrows}} & A' \\ {\scriptstyle u}\downarrow{\scriptstyle \text{bij.}} & & \\ S(A) & \xrightarrow{\varphi} & S(A') \end{array}$$

$\varphi(u) = f \circ u \circ f^{-1}$

$\varphi(u \circ v) = f \circ (u \circ v) \circ f^{-1} = f \circ u \circ (f^{-1} \circ f) \circ v \circ f^{-1} =$

$= \varphi(u) \circ \varphi(v)$.

29) $(G,\cdot)$ grup, $x, y \in G$

i) $xy = yx$, ord x, ord y finit, $(\text{ord } x, \text{ord } y) = 1 \Rightarrow \text{ord}(xy) = \text{ord } x \cdot \text{ord } y$

$\neq 1 \overset{?}{\Rightarrow}$

$\langle x \rangle \cap \langle y \rangle = \{e\}$

$\forall g \in G_1 \cap \cancel{G_2} \Rightarrow g \cdot h \in G_{\ldots}$

$(xy)^p = e \Rightarrow x^p y^p = e \Rightarrow$

$x^p = y^{-p} \in \langle x \rangle \cap \langle y \rangle = \{e\} \Rightarrow$

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

$(xy)^{\text{ord} x \cdot \text{ord} y} = e \Rightarrow \text{ord}(xy) \mid$

$\Rightarrow \text{ord}(xy) = \text{ord } x \cdot \text{ord } y$

contraex.:

ii) ord x, ord y finite $\overset{?}{\Rightarrow}$ ord(xy) finit

În $GL(2,\mathbb{R})$: $x = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$, $y = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$

ord x = ord y = 2. $\text{Tr} A = 0$; $\det A = -1$.
$x^2 = \ldots$

$xy = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \ldots$

$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cancel{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}}$

iii) ord xy finit $\not\Rightarrow$ ord x, ord y finit

ord(x) infinit, $y = x^{-1}$ ord infinit, ord xy = ord $e = 1$.

iv) $|G| = p_1 \cdots p_n$, prime, G abelian $\Rightarrow$ G ciclic

Inducție: $|G| = p_1 \cdots p_n \cdot p_{n+1}$, $x \in G \setminus \{e\}$

fie ord $x = p_k \cdots p_{n+1}$, $k > 1 \Rightarrow (x^{p_k \cdots p_n})^{p_{n+1}} = e \Rightarrow$

$\Rightarrow$ ord $(x^{p_k \cdots p_n}) \mid p_{n+1}$, p_{n+1} prim

$$\Rightarrow \text{ord}(\underbrace{x^{p_k \cdots p_n}}_{\text{not } y}) = p_{n+1} \Rightarrow$$

$$|G/\langle y\rangle| = \frac{|G|}{|\langle y\rangle|} = \frac{p_1 p_2 \cdots p_{n+1}}{p_{n+1}} = p_1 p_2 \cdots p_n, \text{ deci}$$

cf. ip. de Inducție $G/\langle y\rangle$ este ciclic.

fie $z \in G/\langle y\rangle$ un generator al său. ~~dacă $z \in \langle y\rangle$~~

$$z^{p_1 p_2 \cdots p_n} = e_{G/\langle y\rangle} = \langle y\rangle \Rightarrow z^{p_1 p_2 \cdots p_n} \in \langle y\rangle.$$

• dacă $z^{p_1 p_2 \cdots p_n} = e \Rightarrow$ ord $z = p_1 p_2 \cdots p_n$

ord $y = p_{n+1}$

$(\text{ord } z, \text{ord } y) = 1$ $\Rightarrow$ ord(yz) = ord G $\Rightarrow$ $G = \langle yz\rangle$

• dacă $z^{p_1 p_2 \cdots p_n} \neq e$ ~~$\Rightarrow$ ord $z = p_{n+1}$~~

Și $(z^{p_1 \cdots p_n})^{p_{n+1}} = e \Rightarrow \text{ord}(z^{p_1 \cdots p_n}) = p_{n+1}$

$$\text{ord } z^k = \frac{\text{ord } z}{(\text{ord } z, k)} \Rightarrow p_{n+1} = \frac{\text{ord } z}{(\text{ord } z, p_1 p_2 \cdots p_n)} \Rightarrow$$

$\Rightarrow$ ~~ord $z = p_1 p_2 \cdots p_{n+1}$~~ $p_{i_1} \cdots p_{i_j} \cdot p_{n+1}$.

și

~~ord $(z^{p_{n+1}} \cdots p_{i_1} p_{i_2} \cdots p_{i_k})$~~ $= p_{n+1}$.

$\Rightarrow$ ord $z = p_1 p_2 \cdots p_{n+1} \Rightarrow G = \langle z\rangle$

$\Rightarrow$ G ciclic

(30) i) G, H grupuri, $x = (g, h) \in G \times H$, $\mathrm{ord}\, g$, $\mathrm{ord}\, h$ finite

$\mathrm{ord}\, x = [\mathrm{ord}\, g, \mathrm{ord}\, h]$.

$(g,h)^p = (e_G, e_H) \Leftrightarrow g^p = e_G$ și $h^p = e_H \Rightarrow \mathrm{ord}\, g / p$, $\mathrm{ord}\, h / p$

și p minim — $p = [\ \ ]$.

ii) el. de ordin 8 în $\mathbb{Z}_6 \times \mathbb{Z}_{10}$; $\nexists$

$|\mathbb{Z}_6 \times \mathbb{Z}_{10}| = 60 \not\vdots 8$

$[n, m] = 4$, $n/12$, $m/15 \Rightarrow$ ... $m=1$.

(57) : $\tau_i^{k_1}$ ciclu disj. de lg. n ... $\hat{o}$ ... cu τ_i.

cazul $d = 1$: $(k, n) = 1$.

$\tau^k = \pi_1 \ldots \pi_r$ desc. în produs de cicli disj. $r \geq 2$.

$\pi_1^m(i_1) = i_1$, $m =$ lg. ciclului

$\tau^{km}(i_1) = i_1$ | $\Rightarrow km \equiv 0 \pmod{n} \Rightarrow n / km \Rightarrow$

$\tau^n(i_1) = i_1$ | $\Rightarrow n / m \Rightarrow m \geq n$

τ^k permută doar n el. $\Rightarrow$ fiec. din π_i are lg. minim n

$\Rightarrow r = 1$, π^k ciclu și evident disjuncte.

caz particular: $k = 2$, n par :

π^2 se desc. în produs de 2 cicli disj. de lg $\frac{n}{2}$.

$(3,1)\cdot(1,1) = (1,1)$. ... $(0,1) = (1,0)\cdot(1,0)$ ... $(a,b) = \ldots(a,b)$

$M/\alpha = \{\widehat{(a,b)} \mid \widehat{(a,b)} = \{ b \in M \mid (c,d) \alpha (c,d) \}\}$.

$\| $

$\mathbb{Q}$

$\frac{a}{b} = \frac{c}{d} \Rightarrow$

$\Rightarrow$ ... $M/\alpha = \{\{(a,b) \mid (a,b) = 1\}\}$. doar pt că gen.

$(a,b) = 1$ și ~~...~~ $(c,d) = 1$ nu pot fi în rel. α cu $(a,b) \Rightarrow$ ...

68) i) $Hom_{gr}(S_n, \mathbb{Z}_2\times\mathbb{Z}_2)$

$f: S_n \longrightarrow \mathbb{Z}_2\times\mathbb{Z}_2$ morfism

σ – ciclu de lg. 3 $\Rightarrow \sigma^3 = e$.

$$f(\sigma^3) = 3f(\sigma)$$
$$\| $$
$$f(e) = (\hat{0};\hat{0})$$

63) $A_n = \langle \sigma \mid \sigma \text{ ciclu de lungime } 3\rangle$, $n\geq 3$

Orice permutare se poate scrie ca produs de transpoziții

$\varepsilon(\tau_{ij}) = -1 \Rightarrow$ nr. par de transpoziții.

arăt că produsul a 2 $\tau_{ij} \in \langle \sigma \mid lg\,\sigma = 3\rangle$

distincte: $(i\ j)(k\ l) = (i\ j\ k)(i\ k\ l)$

$(i\ j)(i\ l) = (i\ l\ j)$ $\quad i\to l,\ l\to j$ $\quad k\to j,\ k\to l,\ i\to$

$\begin{pmatrix} i & j & k \\ j & k & i\end{pmatrix}\begin{pmatrix} - & j & - & k & - & l & - \\ - & k & - & l & - & j & -\end{pmatrix} = (j\ i\ l)$

$f(\sigma) = (\hat{0},\hat{0}) = e_{\mathbb{Z}_2\times\mathbb{Z}_2}$, σ ciclu de lg. 3.

dar σ generează $A_n \Rightarrow A_n \subseteq Ker(f)$.
dar $ker f$ subgrup normal al lui S_n $\Big| \Rightarrow Ker f \in \{A_n, S_n\}$

- $Ker f = S_n \Rightarrow f$ morfismul nul.
- $Ker f = A_n$. Fie $\sigma, \tau \in S_n \setminus A_n$.

$$f(\sigma) + f(\tau) = f(\underbrace{\sigma\tau}_{\text{permutare pară}}) = (\hat{0},\hat{0}) \Rightarrow$$

$\Rightarrow f(\sigma) = f(\tau) \overset{not}{=} a \in \mathbb{Z}_2\times\mathbb{Z}_2 \Rightarrow 4$ morfisme.

ii) $Hom_{gr}(S_3, \mathbb{Z}_3)$

fie $f: S_3 \to \mathbb{Z}_3$

Ker f subgrup normal al lui S_3

$xN = Nx, \ \forall\, x \in S_3$.

$S_3 = \{ e, (12), (13), (23), (123), (132) \}$.

$[S_n : A_n] = \dfrac{n!}{\frac{n!}{2}} = 2 \Rightarrow A_n$ subgrup normal în S_n.

$A_n = \mathrm{Ker}\ \varepsilon$ (inversiunea) $\Rightarrow$ din TFIG $\underbrace{S_n / A_n}_{\text{grupul factor}} \simeq \{-1, 1\} \Rightarrow$

$\mathrm{Ker} f \in \{ \{e\}, A_3, S_3 \}$.

$(13)(23) = (12)$

$(12)(13) = (321) = (132)$

$\cdot$ $\mathrm{Ker} f = \{e\} \Rightarrow f$ morfism injectiv n.c.

$\cdot$ $\mathrm{Ker} f = A_3 \xrightarrow{TFIG} S_3 / A_3 \simeq \underbrace{\mathrm{Im} f}_{\text{grup}} \leq \mathbb{Z}_3 \Rightarrow$

$\Rightarrow \mathbb{Z}_3$ are un subgrup cu 2 el. n.c.

$\cdot$ $\mathrm{Ker} f = S_3 \Rightarrow f$ morfismul nul.

iii) $Hom_{gr}(\mathbb{Z}_3, S_3)$

$f: \mathbb{Z}_3 \to S_3$ morfism.

Ker f subgrup normal în $\mathbb{Z}_3 \Rightarrow \mathrm{Ker} f \in \{ \mathbb{Z}_3, \hat{0} \}$.

$\mathrm{Ker} f = \{\hat{0}\} \Rightarrow f$ morfism injectiv $\Rightarrow f(\hat{0}) = e$,

$f(\hat{1}) = \sigma, \ f(\hat{2}) = \sigma^2, \ \sigma^3 = e \Rightarrow \sigma$ ciclu de $\underset{2\text{ pos}}{3}$

$\Rightarrow 3$ morfisme.

(58) $\operatorname{ord}\sigma = [\operatorname{ord}\pi_1, \dots, \operatorname{ord}\pi_r]$ în alt mod

$n_i = \operatorname{ord}(\pi_i)$ $\quad \vert m$

$(\pi_1 \dots \pi_r)^m = \pi_1^m \cdot \pi_r \dots = e$

$\operatorname{ord}\sigma / m$.

$\sigma^k = e \Rightarrow \pi_1^k \cdot \dots \cdot \pi_r^k = e$

cf (57) : $\pi_i^k = \tau_{i_1} \dots \tau_{i_{s_i}}$ produs de cicli disjuncți de lg. $\frac{l_g(\pi_i)}{(k, l_g \pi_i)}$

cu aceleași orbite ca orbitele ciclului π_i, $i = \overline{1,r}$

$\Rightarrow \pi_{ij}$, $1 \le j \le s_i$, $1 \le i \le r$ cicli disjuncți, ~~dar~~ care

dau ca produs permutarea identică $\Rightarrow \tau_{ij} = e \Rightarrow \pi_i^k = e \Rightarrow n_i \mid k, i = \overline{1,r} \Rightarrow$

$\Rightarrow m \mid k$ ~~$\Rightarrow \operatorname{ord}\sigma / m / k$~~

$\sigma^k = e \Rightarrow m = \operatorname{ord}\sigma$.

(79) $(\mathbb{Z}^2, +) / \langle (2,3) \rangle$ ciclic infinit

$(\mathbb{Z}^2, +) / \langle (2,2) \rangle$ nu este ciclic

$f : \mathbb{Z} \to (\mathbb{Z}^2, +) / \langle (2,3) \rangle$, $f(m) = \widehat{(m, m)}$.

$\widehat{(m, m)} \notin \langle (2,3) \rangle$, $\forall m \neq 0$. $\Rightarrow$ e infinit ~~$a + \langle 2,3 \rangle$~~ $(1,1)$

$\widehat{(m,m)} = (m, m) + \langle (2,3) \rangle$

$(a, b) = (b - a) \cdot (2,3) + (3a - 2b) \cdot (1,1)$, $\forall a, b \in \mathbb{Z}$.
$\quad \in \mathbb{Z} \qquad \in \mathbb{Z}$

$- m(3a - 2b) \quad (m, m)$

fiecare clasă $\widehat{(a,b)} = (3a - 2b) \cdot \widehat{(1,1)} \Rightarrow \widehat{(1,1)}$ e generator

~~$(\quad)(2,3) + (3a-2b)(2,2)$~~

În $(\mathbb{Z}^2, +) / \langle 2,2 \rangle$: $\quad (\widehat{1,1}) + \langle 2,2 \rangle$ ~~$+$~~ $(1, 1 + 2a, 2)) =$

$-2n, -2n, \dots = (0,0)$

$\operatorname{ord}(\widehat{1,1}) = 2$,

$\operatorname{ord}(\widehat{1,0}) = \infty$

Dacă gr. ar avea un generator $\Rightarrow \widehat{1,1} = g^h \Rightarrow g^{2h} = e = \langle 2,2 \rangle$ fals

dar $g^m = \widehat{1,0} \Rightarrow \operatorname{ord} g = \infty$.

(69) $f : S_4 \to S_3$ morfism

$\operatorname{Ker} f \trianglelefteq S_4 \Rightarrow \operatorname{Ker} f \in \{\{e\}, K, A_4, S_4\}$

$\{e\}$: morfism injectiv; S_4: morfismul trivial

$\operatorname{Ker} f = A_4 \Rightarrow f((12)(34)) = e \Rightarrow f((12)) \circ f((34)) = e$.

$f((12)(12)) = e \Rightarrow f((34)) = f((12)) = \tau_{ij} \in S_3$

$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ $f(\sigma) = \tau_{\in S_3}$, $\forall \sigma \in S_4 - A_4$

$\Rightarrow$ 3 morfisme

$\operatorname{Ker} f = K \Rightarrow f((12)) = f((34)) = r_1$

$f((13)) = f((24)) = r_2$

$f((14)) = f((23)) = r_3$

dacă $r_1 = (ij)$, $r_2 = (ik) \Rightarrow f((12)(13)) = (j\,i\,k)$

$\operatorname{Ker} f \trianglelefteq S_4 \Rightarrow$: $\tau_1, \tau_2 \in K \Rightarrow (j\,i\,k) \in K$ n.c.

~~$\operatorname{Ker} f = K$; f~~

$\Rightarrow$ 6 morfisme

Inele

Ex. 13: 1) nr. structuri neizomorfe de inel pe $(\mathbb{Z}_p, +)$, p prim

Dacă $R = (\mathbb{Z}_p, +, \cdot)$ este unitar, at. $\langle 1 \rangle = R$ și cf. TFIG

$\mathbb{Z}/p\mathbb{Z} \simeq R = \operatorname{Im} f$, cu $f(k) = k \cdot 1$ surjectivă.

$\boxed{\text{str. de inel neunitar: } a \cdot b = 0, \forall a, b \in G}$ singura

Altă str.: dacă $\exists\, a, b$ cu $a b \neq 0 \Rightarrow S = (\{ac, c \in R\}, +)$ subgrup

Din th. lui Lagrange, ord $S \mid \operatorname{ord}(\mathbb{Z}_p, +) = p \Rightarrow |S| = p \Rightarrow$

$\Rightarrow f(c) = ac$ este bijectivă $\Rightarrow$

$\exists\, d \in R$ a.î. $ad = a$. Arăt că d este unitatea.

$\forall c \in R$, $c \neq 0 \Rightarrow ac \neq 0 \overset{\text{fixez } c}{\Rightarrow} f(e) = ce$ este bijectivă, analog $\Rightarrow$

$\Rightarrow \exists\, k_c$ a.î. $k_c a = c$; $cd = k_c ad = k_c a = c \Rightarrow$

$\Rightarrow d$ unitate, $\forall c \in R$

Ex. 1.4: pe $(\mathbb{Q}/\mathbb{Z}, +)$ nu se poate defini o str. de inel unitar

fie $u = \left(\widehat{\frac{a}{b}}\right) = \frac{a}{b} + \mathbb{Z}$ - el. unitate $(a,b)=1$

știm că $\cancel{\frac{a}{b} + \dots + a}$ $ord\left(\widehat{\frac{a}{b}}\right) = b \Rightarrow$

$$\hat{0} = \underbrace{\hat{u} + \dots + \hat{u}}_{b \text{ ori}} = \underbrace{(u + \dots + u)}_{b \text{ ori}} \cdot x = u(\cancel{x + x} + \dots \quad u(\underbrace{1 + \dots + 1}_{b \text{ ori}}) u =$$

$$= \underbrace{x + \dots + x}_{b \text{ ori}} \Rightarrow b \cdot x = 0, \forall \hat{x} \in R$$

$$\hat{x} \leftarrow \left(\widehat{\frac{1}{b+1}}\right) \Rightarrow \left(\widehat{\frac{b}{b+1}}\right) = \hat{0} \Rightarrow \left(1 - \widehat{\frac{1}{b+1}}\right) = 0 \Rightarrow \frac{1}{b+1} = 1 \Rightarrow b = 0 \text{ n.c.}$$

Ex. 1.6: $(\mathbb{R}^{\mathbb{R}}, +, \circ)$ nu e inel unitar

nu verif. prop 3): $f \circ (g+h) = f \circ g + f \circ h$

ex: $f(x) = x+1$, $g(x) = h(x) = x$.

$2x+1 \qquad x+1 \qquad x+1$

Ex. 1.10: $\exists\, a, b \neq 0$ a.î. $ab = 0$
$a \neq 0$

Ex. 1.11: în $M_n(\mathbb{R})$, $\exists A, B \neq O_n$ a.î. $A \cdot B = O_n$

dacă $\det B \neq 0$ $\Big| \Rightarrow A \cdot B \cdot B^{-1} = O_n \Rightarrow A = O_n$.

dacă $\det B = 0$, $rang(AB) \leq n-1$

$rang(BA) \leq \min(rang\, A, rang\, B) \leq rang\, B \leq n-1 \Rightarrow$

$\Rightarrow BA = O_n \Rightarrow A$ are divizor la stg.

R inel integru $\Rightarrow \forall a, b \in R$, $ab = 0 \Rightarrow a = 0$ sau $b = 0$.

$(x_1, \dots, x_n) A = O_n$ sistem omogen liniar cu $\det A = 0$

$\exists\, v \neq (0, \dots, 0) =$

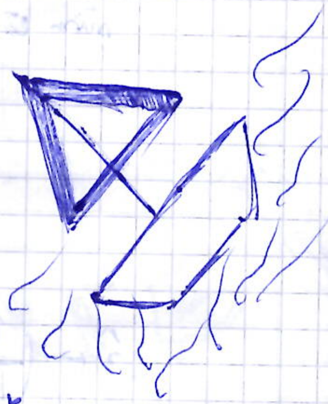
$$C = \begin{pmatrix} x_1 & \dots & x_n \\ \hline x_1 & \dots & x_n \end{pmatrix}$$

Curs 10 – Inele cont.

Prop. de universalitate a inelelor factor

$$\begin{array}{l} R \xrightarrow{f} R/I \\ f \searrow_{R'} \swarrow (\exists!)\ \bar{f} \text{ a.î. } \bar{f}\circ p = f \iff I \subseteq \operatorname{Ker} f \end{array}$$

$$\bar{f}(\hat{a}) = f(a)$$



$\operatorname{Ker} f \trianglelefteq R$

$R/\operatorname{Ker} f \simeq \operatorname{Im} f$ – ~~TI~~ FII

$I \trianglelefteq R_1 \times R_2 \iff I = I_1 \times I_2,\ I_1 \trianglelefteq R_1,\ I_2 \trianglelefteq R_2.$

$$\frac{R_1 \times R_2}{I_1 \times I_2} \simeq \frac{R_1}{I_1} \times \frac{R_2}{I_2}. \quad (\text{Ex. } 4.8)$$

$$\frac{\mathbb{Z}\times\mathbb{Z}}{2\mathbb{Z}\times 3\mathbb{Z}} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}.$$

Th. chineză a resturilor:

$\mathbb{Z}_{n_1 n_2} \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2},\ (n_1, n_2) = 1.$

$\hat{k} \longrightarrow (\bar{k}, \bar{\bar{k}})$ surjectivă

$(n_1, n_2) = 1 \Rightarrow n_1\mathbb{Z} + n_2\mathbb{Z} = \mathbb{Z}$

$I_1 + I_2 = R \Rightarrow I_1 \cap I_2 = I_1 I_2.$

$I_1 + I_2 = \{ a_1 + a_2 \mid a_i \in I_i \}$

$I_1 I_2 = \left\{ \sum_{i=1}^{n} a_1^{(i)} a_2^{(i)} \mid n \in \mathbb{N},\ a_1^{(i)} \in I_1,\ a_2^{(i)} \in I_2 \right\}.$

$1 = x_1 + x_2,\quad x_1 \in I_1,\ x_2 \in I_2$

$a \in I_1 \cap I_2 \Rightarrow a = \underbrace{ax_1}_{\in I_1} + \underbrace{ax_2}_{\in I_2} \in I_1 I_2.$

$(n_1, n_2) = 1$: $\mathbb{Z}_{n_1 n_2} \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$

$\mathbb{Z}_4 \times \mathbb{Z}_6 \not\simeq \mathbb{Z}_{24}.$

$$R/_{I_1 \cap I_2} \simeq R/I_1 \times R/I_2.$$

Teoremă. $f : R/I_1 \cap I_2 \longrightarrow R_1/I_1 \times R_2/I_2$, $f(\hat{x}) = (\overline{x}, \overline{\overline{x}})$.

$$\mathbb{Z}[X]/_{(X^2-1)} = \{ \hat{f} \mid f \in \mathbb{Z}[X] \} = \{ a\widehat{X+b} \mid a, b \in \mathbb{Z} \}.$$

$$\hat{f} = \widehat{(X^2-1)\, q + r}.$$

$$= \widehat{(X^2-1)\, q + aX + b}.$$

$$\widehat{aX+b} \text{ idempotent} \Rightarrow \widehat{2abX + a^2+b^2} = \widehat{aX+b}.$$

$$\widehat{aX+b} = \widehat{cX+d} \Leftrightarrow a=c \text{ și } b=d.$$

$$\text{Idemp.}(\mathbb{Z}_{36}) = \{\hat{0}, \hat{1}, \hat{9}, \widehat{28}\}.$$

$$\mathbb{Z}_{36} \simeq \mathbb{Z}_6 \times \mathbb{Z}_9$$

$$\hat{0} \leftarrow (\overline{0}, \overline{\overline{0}})$$

$$\hat{1} \leftarrow (\overline{1}, \overline{\overline{1}})$$

$$\widehat{28} \leftarrow (\overline{0}, \overline{\overline{1}})$$

$$\hat{9} \leftarrow (\overline{1}, \overline{\overline{0}})$$

I ideal în R inel
$x, y \in I \Rightarrow x - y \in I$
$x \in I$, $\forall a \in R$, $ax \in I$.

Corpuri

Seminar: f cont., $f \in C(\mathbb{R})$ divizor al lui zero $\Leftrightarrow \exists (a,b) \subset \mathbb{R}$ a.î. $f(x) = 0$, $\forall x \in (a,b)$

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$$

„$\Rightarrow$" $\hat{a} \in \mathbb{Z}_n$ nilpotent $\Leftrightarrow p_1 p_2 \cdots p_m \mid a$

$\hat{a}$ nilpotent $\Leftrightarrow \hat{a}^t = \hat{0} \Leftrightarrow n \mid a^t \Leftrightarrow p_i \mid a^t$, $i = \overline{1,m}$

$$\Rightarrow p_i \mid a \Rightarrow p_1 \cdots p_m \mid a.$$

„$\Leftarrow$" $a = (p_1 \cdots p_m) b$, $k = \max(k_1, \ldots, k_m)$ $\Rightarrow a^k \vdots n \Rightarrow \hat{a}^k = \hat{0}$.

$N(R) = \{ a \in R \mid a \text{ nilpotent} \}$, R comutativ.

$N(R)$ ideal $\Leftrightarrow$ $\forall x \in N(R)$ şi $y \in N(R) \Rightarrow x - y \in R$.

$\forall x \in N(R)$, $\forall r \in R \Rightarrow xr \in N(R)$

$x^k = 0 \Rightarrow (xr)^k = 0$.

$$\left.\begin{matrix} x^{n_1} = 0 \\ y^{n_2} = 0 \end{matrix}\right| \Rightarrow (x - y)^{n_1 + n_2 + 1} = 0$$

$$\sum_{i=0}^{n_1+n_2-1} C_{n_1+n_2-1}^{i} x^i \cdot y^{n_1+n_2-1-i} = 0.$$

$N(\mathbb{Z}_n) = \hat{d}\mathbb{Z}_n$, $d = K\{p_1, \ldots, p_m\}$

$= \widehat{p_1 \cdots p_m} \mathbb{Z}_n$

$N(\mathbb{Z}_n) = \widehat{p_1 p_2 \cdots p_m} \mathbb{Z}_n$.

$$|N(\mathbb{Z}_n)| = \frac{n}{p_1 p_2 \cdots p_m}.$$

$$|N(\mathbb{Z}_{36})| = \frac{36}{2 \cdot 3} = 6$$

$N(\mathbb{Z}_{36}) = \hat{6}\mathbb{Z}_{36}$

$\mathrm{Idemp}(\mathbb{Z}_{p^k}) = \{\hat{0}, \hat{1}\}$

p prim, $k \geq 1$

$\hat{a}^2 = \hat{a} \Rightarrow p^k \mid a^2 - a = a(a-1) \Rightarrow p^k \mid a$ sau $p^k \mid a - 1 \Rightarrow$

$\Rightarrow \hat{a} = 0$ sau $\hat{a} = \hat{1}$.

$$\mathbb{Z}_n = \mathbb{Z}_{p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}} \simeq \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}.$$

$$(\hat{a}_1, \ldots, \hat{a}_m)^2 = (\hat{a}_1, \ldots, \hat{a}_m).$$

$$|\mathrm{Idemp}(\mathbb{Z}_n)| = 2^m.$$

$\mathbb{Z}_{72} \simeq \mathbb{Z}_8 \times \mathbb{Z}_9$

$\hat{a} \mapsto (\bar{a}, \bar{\bar{a}})$

$\hat{0} \to (\bar{0}, \bar{\bar{0}})$

$\hat{1} \to (\bar{1}, \bar{\bar{1}})$

$\widehat{64} \to (\bar{0}, \bar{\bar{1}})$

$\hat{9} \to (\bar{1}, \bar{\bar{0}})$

$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $\cancel{1}0 \to 1$, $\to 4$

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

$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

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

$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ 2.7

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

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

3.11: $f : \mathbb{Z}_m \to \mathbb{Z}_n$ morfism de inele

$f(\hat{1}) = \bar{a}$

$f(\hat{0}) = f(\hat{m}) = m \cdot \bar{a}$

$$f(\hat{1} \cdot \hat{1}) = f(\hat{1}) \cdot f(\hat{1})$$
$$\parallel$$
$$f(\hat{1})$$

$\begin{cases} \bar{a}^2 = \bar{a} \\ m\bar{a} = \bar{0} \end{cases}$

$f(\hat{k}) = k\bar{a}$.

inele unitare $\Rightarrow$ $\bar{a} = 1 \Rightarrow m \cdot \bar{1} = \bar{0} \Leftrightarrow \bar{m} = \bar{0} \Leftrightarrow n / m$.

$f : \mathbb{Z}_{12} \to \mathbb{Z}_{28}$ $\bar{a} \in \mathbb{Z}_{28}$ $\left| \begin{array}{l} \bar{a}^2 = \bar{a} \\ 12\,\bar{a} = \bar{0} \end{array} \right.$

$\bar{a} < \begin{array}{l} \bar{0} \to \text{morfismul nul} \\ \overline{21} \end{array}$

Curs 11

Corpul de fracții al unui domeniu de integritate

$(R,+,\cdot)$ inel integru comutativ

$$Q(R) = \frac{R \times (R\setminus\{0\})}{\sim}$$

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc$$

$$\frac{a}{b} := \widehat{(a,b)}$$

$R = \mathbb{Z}$ $\quad \frac{1}{2} = \widehat{(1,2)} = \frac{2}{4} = \langle \widehat{2,4} \rangle$

$$\begin{cases} \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \\ \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \end{cases} \qquad \left.\begin{matrix} \frac{a}{b} = \frac{a'}{b'} \\ \frac{c}{d} = \frac{c'}{d'} \end{matrix}\right\} \Rightarrow \frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$$

$$\frac{a}{b} \neq \frac{0}{1} \Rightarrow a \neq 0, \ \exists \frac{b}{a} \in Q(R) \quad \frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1}$$

$$R = \mathbb{Z}[\sqrt{2}] = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Z} \}$$

$$x \in Q(R), \ x = \frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{(a+b\sqrt{2})(c-d\sqrt{2})}{c^2-2d^2} =$$

$$= \underbrace{\frac{ac-2bd}{c^2-2d^2}}_{\in \mathbb{Q}} + \underbrace{\frac{bc-ad}{c^2-2d^2}}_{\in \mathbb{Q}} \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

$$\left.\begin{matrix} R \subset Q(R) \\ R \subset K \end{matrix}\right| \Rightarrow R \subset Q(R) \subset K$$

$$x \in Q(R) : x = \frac{a}{b} \rightsquigarrow ab^{-1} \in K$$

$R = \mathbb{Z}[i] = \{ a+bi \mid a, b \in \mathbb{Z} \}$

$$Q(\mathbb{Z}[i]) = \mathbb{Q}(i) = \{ p+qi \mid p,q \in \mathbb{Q} \}$$

Inele de polinoame

R inel comutativ unitar

$(a_n)_{n\geq 0}$; $\exists (n_0) \geq 0$ a.î. $a_n = 0, \forall n \geq n_0$

$\parallel$

$R^{(\mathbb{N})}$

$$(a_n)_{n\geq 0} + (b_n)_{n\geq 0} = (a_n + b_n)_{n\geq 0}$$

$$(a_n)_{n\geq 0} \cdot (b_n)_{n\geq 0} = (a_n \cdot b_n)_{n\geq 0}$$

$$c_n = \sum_{i+j=n} a_i \cdot b_j$$

$R[X] = (R^{\mathbb{N}}, +, \cdot)$ inel comutativ unitar

$\downarrow$

inelul de polinoame

$$0 = (0, 0, \dots, 0)$$

$$1 = (1, 0, \dots, 0)$$

$\varepsilon : R \longrightarrow R^{(\mathbb{N})}$ morf. inj. de inele

$$\varepsilon(a) = (a, 0, \dots, 0)$$

$$X = (0, 1, 0, \dots, 0)$$

$$X^2 = (0, 0, 1, 0, \dots, 0)$$

$$X^n = (0, 0, \dots, \underset{\text{poz. } n}{1}, 0, \dots, 0)$$

$$(a_0, a_1, \dots, a_n, 0, 0, \dots) = (a_0, 0, 0, \dots) + (0, a_1, 0, \dots 0) + \dots +$$

$$+ (0, \dots 0, a_n, 0, \dots 0) = \varepsilon(a_0) + \varepsilon(a_1)X + \dots + \varepsilon(a_n)X^n$$

$f = a_0 + a_1 X + \dots + a_n X^n$, $\deg f = n$.

$\deg 0 = -\infty$

R integru $\Rightarrow \deg(fg) = \deg f + \deg g$.

$\Rightarrow U(R[X]) = U(R)$

$fg=0 \Rightarrow \deg fg = -\infty \Rightarrow \deg f + \deg g = -\infty \Rightarrow f=0$ sau $g=0$.

$$\begin{array}{ccc} R & \xrightarrow{\varepsilon} & R[X] \\ & \searrow^{\varphi} & \downarrow \bar{\varphi} \\ & & S \ni s \end{array}$$

$\varepsilon(a)=a$

$\bar{\varphi}\circ\varepsilon=\varphi$

$\bar{\varphi}(X)=s$

$\bar{\varphi}(a_0+a_1X+\dots+a_nX^n)=\varphi(a_0)+\varphi(a_1)s+\dots+\varphi(a_n)s^n$

$R\subset S$

$f\in R[X]$, $f=a_0+a_1X+a_2X^2+\dots+a_nX^n$

$\tilde{f}: S\to S$, $\tilde{f}(s)=f(s)$
$\qquad\qquad\qquad\qquad \| $
$\qquad\qquad a_0+a_1s+\dots+a_ns^n$.

R_1, R_2
$\triangleleft\ \ \triangleleft$
I_1, I_2

$I_1\times I_2 \triangleleft R_1\times R_2$

$f\in R[X]$, R integru infinit; $\tilde{f}=0 \Leftrightarrow f=0$.

Th. împ. cu rest: $f,g\in R[X]$, $g\neq 0$, coef. dom. al lui g inversabil:
$\Rightarrow \exists!\, q, r\in R[X]$ a.î. $f=g\cdot q+r$, $\deg r<\deg g$.

Dem.: $f=a_0+\dots+a_nX^n$
$g=b_0+b_1X+\dots+b_mX^m$, $b_m\neq 0$ inv.

Ind. după n

$n<m$: $q=0$, $r=f$

$n\geq m$: $f_1=f-b_m^{-1}a_nX^{n-m}g$

$\deg f_1<\deg f$

Ip. Ind $\Rightarrow f_1=g\cdot q_1+r_1$, $\deg r_1<\deg g$

$\Rightarrow f=g\cdot q_1+r_1+b_m^{-1}a_nX^{n-m}g=g\underbrace{(b_m^{-1}a_nX^{n-m}+q_1)}_{q}+r_1$.

$$\frac{\mathbb{Q}[X]}{X^2-1} \simeq \mathbb{Q}\times\mathbb{Q}$$

$$R/_{IJ} = R/_{I\cap J} \simeq R/_I \times R/_J$$

$I+J=R$

$$\frac{\mathbb{Q}[X]}{X^2-1} \simeq \mathbb{Q}[X]/_{(X-1)} \times \mathbb{Q}[X]/_{X+1}$$

$\simeq \mathbb{Q}$ $\quad\quad$ $\simeq \mathbb{Q}$

$$\frac{\mathbb{Q}[X]}{X-1} = \{\hat{f} \mid f\in\mathbb{Q}[X],$$

$$f=(X-1)\,q(X)+r, \quad r\in\mathbb{Q}$$

$$\hat{f} = \widehat{(X-1)}\,\widehat{q(X)} + \hat{r}$$

$$\varphi:\mathbb{Q}[X]\longrightarrow\mathbb{Q}$$

$$\varphi(f) = f(1)$$

$$\ker\varphi = \{f\in\mathbb{Q}[X] \mid f(1)=0\} = \widehat{(X-1)}$$

IT'S THAT
THE WAY WE
STAND ?
IT'S TEARING ME
APAAAART

Seminar:

$A=\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}$, $B=\begin{pmatrix} 0 & b\\ 0 & 0\end{pmatrix}\cdot\begin{pmatrix} \cdot & \cdot\\ \cdot & \cdot\end{pmatrix}$

$AB=\begin{pmatrix} 0 & ab\\ 0 & 0\end{pmatrix} \Rightarrow ab=0.$

$BA=\begin{pmatrix} 0 & 0\\ 0 & 0\end{pmatrix}$

$I\le R_1\times R_2 \Rightarrow I=I_1\times I_2,\ I_1\le R_1$
$I_2\le R_2$

$c\cdot p_1(I)\in p_1(I)\ \forall c\in R.$

$c\cdot a_1 = p_1(a_1c)$

$a_1c\in I \cap a_1$ ...

$p_1: R_1\times R_2\to R_1,\ p_1(a_1,a_2)=a_1$

$p_2: R_1\times R_2\to R_2,\ p_2(a_1,a_2)=a_2$

$$I=p_1(I)\times p_2(I)$$

"⊇" $a_1 = p_1((a_1, *))$ $\in I$

$a_2 = p_2((*, a_2))$ $\in J$

"⊆" Evident

$I = p_1(I) \times p_2(I) = I_1 \times I_2$

$p_i(I) = I_i$

$(a_1, a_2) \in I$

$= (a_1, 0) + (0, a_2) = (a_1, *) \cdot (1, 0) + (*, a_2)(0, 1)$.

$R = R_1 \times R_2 \times \dots \times R_n$

$p_i(I) \trianglelefteq R_i$

$$\frac{R_1 \times R_2}{J_1 \times J_2} \simeq \frac{R_1}{J_1} \times \frac{R_2}{J_2}$$

$R_1 \times R_2 \longrightarrow R_1/J_1 \times R_2/J_2$

$(a_1, a_2) \longmapsto (\overline{a_1}, \overline{\overline{a_2}})$

$\operatorname{Ker} \varphi = I_1 \times I_2$

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

$X^2 - X = X(X-1)$

$I = (X)$

$J = (X-1)$

$I + J = \mathbb{Z}[X]$

$1 = \underset{\in I}{X} + \underset{\in J}{(1 - X)} \in I + J$

Din th. chineză a resturilor pt. ideale, $\mathbb{Z}[X]/(X^2-X) \simeq \mathbb{Z}[X]/X \times \mathbb{Z}[X]/(X-1) \simeq \mathbb{Z} \times \mathbb{Z}$.

$\mathbb{Z}[X]/(X^2-1) \not\simeq \mathbb{Z} \times \mathbb{Z}$.

Obs. $I = (X-1)$

$J = (X+1)$

$I + J \neq \mathbb{Z}[X]$

Pp. că $1 \in I + J \Leftrightarrow 1 \in \underbrace{(X-1) + (X+1)}$

$(X-1, X+1) = (2, X-1)$

$1 = (X-1)u(X) + (X+1)v(X)$, $u(X), v(X) \in \mathbb{Z}[X]$

$X \to 1$ $\quad 1 = 2\underset{\in \mathbb{Z}}{v(1)}$. n.c.

$(2, X)$ nu este ideal principal

Pp. $(2,X) = (p(X)) \Rightarrow 2 = p(X)\cdot g(X) \Rightarrow \deg p(X) = 0$

$p = \pm 1, \cancel{\pm 2}$

$X = p \cdot r(X)$

$\Rightarrow (2, X) = (\pm 1) = \mathbb{Z}[X]$.

$1 \in (2,X) \Rightarrow 1 = 2u(X) + Xv(X)$ | m.c.

$X \longrightarrow 0$

$\mathbb{Z}[X]/(X^2-1) = \{ \widehat{a+bX} \mid a, b \in \mathbb{Z} \}$.

El. idemp. $(\mathbb{Z}[X]/(X^2-1)) = ?$

$\widehat{a+bX}^2 = \widehat{a+bX} \Leftrightarrow \widehat{a^2+2abX+b^2X^2} = \widehat{a+bX} \Leftrightarrow$

$\widehat{a^2+2abX+b^2} = \widehat{a+bX}$

$\widehat{a+bX} = \widehat{c+dX} \Leftrightarrow a = c$ și $b = d$

$\widehat{a-c+(b-d)X} = \hat{0}$

$a-c+(b-d)X \in (X^2-1)$

$\Vert$

$(X^2-1)\, p(X) \Rightarrow p(X) = 0$

2.

$\Rightarrow a^2+b^2 = a$ și $2ab = b \Rightarrow \begin{cases} a^2+b^2 = a \\ b(2a-1) = 0 \end{cases}$ $\xrightarrow{b=0}$ $\cancel{a^2=a} \; a \in \{0,1\} \Rightarrow 2$ idem

$\rightarrow 2a-1 \Rightarrow a = \frac{1}{2} \notin \mathbb{Z}$ fals

$\mathrm{Idemp}(\mathbb{Z}\times\mathbb{Z}) = \{(0,0), (1,1), (0,1), (1,0)\}$.

$N\left(\mathbb{Z}[X]/(X^2-1)\right) = ?$

$(\widehat{a+bX}) = \hat{0}$

$(\widehat{a+bX})^n = \hat{0} \Leftrightarrow (a+bX)^n \in (X^2-1)$

$(a+bX)^n = (X^2-1) f(X)$

$(X-1)(X+1)$

$$\begin{cases} X-1 \mid (a+bX)^n \\ X+1 \mid (a+bX)^n \end{cases} \Rightarrow \begin{cases} X-1 \mid a+bX \\ X+1 \mid a+bX \end{cases} \Rightarrow$$

$$(X^2-1) \mid a+bX \Rightarrow a+bX=0 \Rightarrow a=b=0.$$

$$N(\mathbb{Z}\times\mathbb{Z}) = \{(0,0)\}.$$

$$\left|U\left(\mathbb{Z}[X]/(X^2-1)\right)\right| = 4 \qquad U\left(\mathbb{Z}[X]/(X^2-1)\right) = \{\hat{X}, -\hat{X}, 1, -1\}.$$

$$\widehat{a+bX}\cdot\widehat{c+dX} = 1 \Leftrightarrow \widehat{ac+(ad+bc)X+bdX^2} = \hat{1} \Leftrightarrow$$

$$\widehat{ac+bd+(ad+bc)X} = \hat{1} \Leftrightarrow \begin{cases} ac+bd=1 \\ ad+bc=0 \end{cases} \Rightarrow (c,d)=1$$

$$\boxed{a = -\frac{bc}{d}}$$

$$-\frac{bc^2}{d} + bd = 1 \Rightarrow -bc^2+bd^2=d \Rightarrow b \mid d$$

$$d = bd_1 = b(d^2-c^2)$$

$$\left.\begin{array}{l} d \mid bc \\ (d,c)=1 \end{array}\right| \Rightarrow d \mid b.$$

$$\Rightarrow b = \pm d$$

I) $b=d$:

$a=-c$

$-a^2+b^2=1$

$(b-a)(b+a)=1$

$$\begin{cases} b-a=1 \\ b+a=1 \end{cases} \Rightarrow \begin{cases} a=0 \\ b=1 \end{cases}$$

$$\begin{cases} b-a=-1 \\ b+a=-1 \end{cases} \Leftrightarrow \begin{cases} a=0 \\ b=-1 \end{cases}$$

II) $b=-d$:

$a=c$

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

$(a-b)(a+b)=1$

$$\begin{cases} a-b=1 \\ a+b=1 \end{cases} \Leftrightarrow \begin{cases} a=1 \\ b=0 \end{cases}$$

$$\begin{cases} a-b=-1 \\ a+b=-1 \end{cases} \Leftrightarrow \begin{cases} a=-1 \\ b=0 \end{cases}$$

$$I = (3, X^3 - 3X^2 + 2X + 1)$$

I nu este ideal principal

$\mathbb{Z}[X]/I$ nu este inel integru

$$\frac{R/J}{J/J} \simeq R/J$$

$$\neq \mathbb{Z}_2 + \mathbb{Z}_2 \quad \neq \mathbb{Z}_3 + \mathbb{Z}_3 + \mathbb{Z}_3 \quad \neq \mathbb{Z}_3 \times \mathbb{Z}_3$$

$$\mathbb{Z}[X]/(3, X^3 - 3X^2 + 2X + 1) \simeq \frac{\overset{\mathbb{Z}_3[X]}{\mathbb{Z}[X]/(3)}}{(3, X^3 - X^2 + 2X + 1)/(3)} = \mathbb{Z}_3[X]/\left((X + \hat{1})(X - \hat{1})^2\right)$$

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

$$\Rightarrow \underset{\neq \bar{0}}{\overline{(X + \hat{1})}} \cdot \underset{\neq \bar{0}}{\overline{(X - \hat{1})^2}} = \bar{0}$$

$$\left[\underset{\neq 0}{(X + \hat{1})}\ \underset{\neq 0}{(X - \hat{1})}\right]^2 = 0$$

t: Det. toate inele comutative unitare cu 4 el.

$$\frac{\mathbb{Z}_2[X]}{(X^2 + X + 1)}, \quad \frac{\mathbb{Z}_2[X]}{(X + 1)^2}.$$

$$\frac{K[X]}{(f)}$$ corp, f ireductibil.