

Algebra #1

2 p maxим pt "prezentă" la seminare

0,5 pts

1,5 < 3 teme
3 lucrări

Căntă: 1. Ion D. Ioan, N Radu, "Algebra" 1991 BUC

2. T Dumitrescu, "Algebra" 2006 BUC

Culegeri 3. Dăncălescu, Băilescu, Mănescu

Def 1. Operație algebraică (lege de compoziție) pe
o mulțime: o funcție $f: G \times G \rightarrow G$

$$f(x, y) = x \circ f y$$

2. Operația se numește asociativă $\Leftrightarrow x \circ (y \circ z) = (x \circ y) \circ z$

$$= (x \circ y) \circ z, \forall x, y, z \in G$$

3. Existe numărul element neutru (\Leftarrow)

$$\rightsquigarrow x \circ e = pox = x \quad \forall x \in G$$

• Remarcă: elementul neutru este unic

- Ppcă f, l sunt elemente neutre $e \neq f$

$$e \circ f = e = f \circ e$$

$$f \circ e = f$$

$$x \circ f = f$$

$$x \circ f = f \circ x = x$$

$$e \circ f = e \quad \Rightarrow \quad e = f \text{ (contradicție)}$$

$$f \circ e = f$$

4. Să se demonstreze că $g \in G$ este inversabil dacă există g'

$$g \circ g' = g' \circ g = e$$

g' = element

g' este inversul lui g

operările asociative, și element neutru

Remarcă: Dacă $\exists g'$, atunci este unică

$$g, g', g'' \in G$$

$$g \circ g' = e \quad \Rightarrow \quad g' = g^{-1}$$

$$g \circ g'' = e \quad \Rightarrow \quad g' \circ g \circ g'' = g' \quad \text{2/4}$$

$$\circ \quad e^0 g'' = g'(0) \quad g'' = g'$$

5. (G, \circ) se numește grup dacă

+ defnimbolică

$\forall x \in G, x^{-1}$ inversul

Există o formulă folosind $+, -, \cdot, /, \sqrt{}$ pentru
a rezolva

Th (Abel - Ruffini)

Ecuația generală de grad ≥ 5 nu poate fi rezolvată
doar cu ajutorul operatiilor $+, -, \cdot, /, \sqrt{}$

Th (Galois)

În ce condiții, ecuația $x^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0 = 0$
se rezolvă prin cele 5 operații?

Curs 2

Definitie: G multime, \circ operatie pe G , G s.m. grupa dacă

$$1) (x \circ y) \circ z = x \circ (y \circ z), \forall x, y, z \in G$$

$$2) \exists e \in G \text{ a.i. } x \circ e = e \circ x = x$$

$$3) \forall g \in G \Rightarrow \exists g^{-1} \in G \text{ a.i. } g \circ g^{-1} = g^{-1} \circ g = e \text{ (g, unic)}$$

Df: (G, \circ) grup

G s.m. comutativa dacă $x \circ y = y \circ x, \forall x, y \in G$

SCOPUL CURSULUI: Teorema (Lagrange) (G, \circ) grup finit, \exists elem. neutru $e \in G$

$$\Rightarrow |G| = q$$

$|G| =$ cardinalul multimi G

Notatie: $g^m = \underbrace{g \circ g \circ \dots \circ g}_{\text{de } m \text{ ori}}$

As: dem în cadrul în care G este comutativă

Lemă: Dacă există o funcție $f: A \rightarrow B$, A, B multimi finite $|A| = |B|$

Sunt echivalente: 1) f bij

2) f inj

3) f surj

Dem: 1 \Rightarrow 2 evidentă

$\begin{matrix} \downarrow \\ 2 \Rightarrow 3 \end{matrix}$

$$A = \{a_1, a_2, \dots, a_m\}$$

$$\begin{aligned} & a_i \neq a_j \wedge i \neq j \\ & \{f(a_1), f(a_2), \dots, f(a_m)\} \subseteq B \quad \Rightarrow |A| = |B| \Rightarrow \exists a_i \in A \text{ a.i. } f(a_i) = \end{aligned}$$

m elemente

$\exists \Rightarrow 1$

(\Leftarrow suficient să există o inj)

Prezumem că f nu este inj.

$\Rightarrow \exists i \neq j \text{ s.t. } f(a_i) = f(a_j) \Rightarrow \{f(a_1), f(a_2), \dots, f(a_m)\} \subseteq m+1$

$1 \leq i \leq m$

Dacă surj. lui f rezultă ca $\{f(a_1), \dots, f(a_m)\} \subseteq m+1$

" B (m elem)

contradictie

ct: pt. \Rightarrow card A și B au aceeași cardinal, inf.

$f: N \rightarrow N$

$f(m) = m+1$

1 - inj

f + surj (0 nu este cuprins)

A - multime

A este infinită dacă există $(f, l): A \rightarrow A$, f inj. care nu e biy.

Obs: (G, \circ) grup $\left\{ \begin{array}{l} g_1 = g_2 \\ g_1 \circ g_2 = g_2 \circ g_1 \end{array} \right. \Rightarrow g_1 = g_2$

Dacă $\exists h \in G$. $h \circ g = g \circ h = \emptyset$

$g_1 = e \circ g_1 = (h \circ g) \circ g_1 = h \circ (g_1 \circ g_1) = h \circ g_1 = (h \circ g) \circ g_2 = (h \circ g) \circ g_2 = e \circ g_2 = g_2$

Analog: $g_1 \circ g = g_2 \circ g = g_1 = g_2$

Dacă G comutativă $g_1 \circ g = g \circ g_2 \Rightarrow g_1 = g_2$ atfel ar negația

Durch Lagrange (G kommutativ)

$g \in G$

$$G = \{g_1, g_2, g, \dots, g_m\} \quad |G| = m$$

\Downarrow
 $g^m = e$

$$l: G \rightarrow G$$

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

\rightarrow Acht $\Leftrightarrow l$. inj ($l(h_1) = l(h_2) \Rightarrow h_1 = h_2$)

$$h_1 \circ g = h_2 \circ g \stackrel{\text{obs}}{\Rightarrow} h_1 = h_2$$

G finitär, l inj $\xrightarrow{\text{Lemma}}$ l . bij

$$\{l(g_1), l(g_2), \dots, l(g_m)\} = \{g_1, g_2, \dots, g_m\}$$

$G \text{ com}$

$$\Rightarrow l(g_1) \circ l(g_2) \circ \dots \circ l(g_m) = g_1 \circ g_2 \circ \dots \circ g_m$$

$$(g_1 \circ g) \circ (g_2 \circ g) \circ \dots \circ (g_m \circ g) = g_1 \circ g_2 \circ \dots \circ g_m$$

$$(g_1 \circ g_2 \circ \dots \circ g_m) \circ \overbrace{g}^{\text{in grey pattern simplifies}} = g_1 \circ g_2 \circ \dots \circ g_m$$

$$\boxed{g^m = e}$$

Abs 2017 ²⁰¹⁷, ultimale 2. cipe : NY

Examen

Nach: o. operatice pe multimea M

(M, \circ) se numeste monoid deci:

$$1) x \circ (y \circ z) = (x \circ y) \circ z, \quad (\forall) x, y, z \in M$$

$$2) \exists e \in M \text{ s.t. } e \circ x = x \circ e = x, \quad \forall x \in M$$

(def. e, neutral)
e-unit

Exemplu:

$$(\mathbb{Z}, \circ) \quad x \circ y = x \cdot y + x + y$$

memorial 1. $((x \circ y) \circ z) = x \circ (y \circ z)$

are. $(x \cdot y + x + y) \circ z = a \cdot z + a + z$
not a

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

$$x \circ (y \circ z) = x \circ (y \cdot z + y + z) = x \cdot (y \cdot z + y + z) =$$

$$= x \cdot y \cdot z + x \cdot y + x \cdot z + x \cdot y + z + y + z$$

2. ②

$$x \circ e = e \circ x = x$$

$$x \cdot e + x + e = x$$

$$e(x+1) = 0 \Rightarrow e = 0$$

$$x \circ 0 = 0 \circ x = x \cdot 0 + x + 0 = x$$

3. este \mathbb{Z} comutativă

$$x \circ y = y \circ x, \forall x, y \in \mathbb{Z}$$

Cine sunt elementele inversibile?

$$x \in \mathbb{Z}, \exists y \in \mathbb{Z} \text{ a.t.}$$

$$1 \quad x \circ y = 0 = x \cdot y + x + y + 1$$

$$1 = x \cdot y + x + y + 1 = (x+1)(y+1)$$

$$\Leftrightarrow x+1 = y+1 = 1 \quad \text{ sau } x+1 = y+1 = -1$$

$$(x=0)$$

$$(x=-2)$$

Elemente:

$$G = \{ \bar{a} \mid a \in \{0, 1, \dots, g_0\} \}$$

$$(a, 100) = 1 \}$$

$a, b \in \mathbb{Z}$

$$\bar{a} = \bar{b} \stackrel{\text{def}}{\Rightarrow} 100 | a - b$$

$$\bar{a} \cdot \bar{b} \stackrel{\text{def}}{=} \overline{a \cdot b} \quad (\text{Ex. op.})$$

cu lumen def

$$\begin{aligned} \bar{a} &= \bar{a}_1 \\ b &= \bar{b}_1 \end{aligned} \quad \left\{ \begin{array}{l} \bar{a} = \bar{a}_1 \\ b = \bar{b}_1 \end{array} \right. \Rightarrow \bar{a} \cdot \bar{b} = \bar{a}_1 \cdot \bar{b}_1$$

Alt-exercitiu:

Propozitie: (M, \circ) monoid finit, comutativ cu proprietatea:

$$\textcircled{3} \quad m \circ m_1 = m \circ m_2 \Rightarrow m_1 = m_2$$

Atunci (M, \circ) grup.

$$g \in M$$

$$f: M \rightarrow M$$

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

$$f(m_1) = f(m_2)$$

$$g \circ m_1 = g \circ m_2 \stackrel{\textcircled{3}}{\Rightarrow} m_1 = m_2 \quad \text{deci } \begin{cases} f \text{ inj.} \\ M \text{ finita} \end{cases} \stackrel{\text{Lema}}{\Rightarrow} f \text{ surj.}$$

$$\begin{matrix} g \in M \\ \text{surj.} \end{matrix} \Rightarrow \exists g_1 \in M \text{ s.t. } f(g_1) = e$$

(N^+, \cdot) → monoid

1-②

(G, \cdot) monoid

$$\bar{a} \cdot (\bar{b} \cdot \bar{c}) = (\bar{a} \cdot \bar{b}) \cdot \bar{c}$$

$$\bar{a} = \bar{a} \cdot 1 = 1 \cdot \bar{a}$$

$$|G|=50$$

(G, \cdot) are prop de simplificare

$$\bar{m} \cdot \bar{m}_1 = \bar{m} \cdot \bar{m}_2 \Rightarrow \bar{m}_1 = \bar{m}_2$$

$$\bar{m}, \bar{m}_1, \bar{m}_2 \in \{0, 1, \dots, 49\}$$

$$(m, 100) = (\bar{m}_1, 100) = (\bar{m}_2, 100)$$

$$\overline{m \cdot m_1} = \overline{m \cdot m_2}$$

$$100 | m(m_1 - m_2)$$

$$(m, 100) = 1$$

$$\Rightarrow 100 | m_1 - m_2$$

$$\overline{m_1} = \overline{m_2}$$

$$\Rightarrow m_1 = m_2$$

$$\overline{2017^{2017}} = \overline{17^{2017}} =$$

$$17 \in G \Rightarrow 17^{|G|} = \overline{1}$$

$$\overline{17^{40}} = \overline{1}$$

$$= (\overline{17^{40}})^{50} \cdot \overline{17} = \overline{1}^{50} \cdot \overline{17} = \overline{17^{17}}$$

$$\overline{17^2} = \overline{289} = \overline{11}$$

$$\overline{17^9} = \overline{121} = \overline{21}$$

$$\overline{17^{-8}} = \overline{21^{-2}} = \overline{41}$$

$$\overline{17^{16}} = \overline{41^{-2}} = \overline{81}$$

$$\overline{17^{17}} = \overline{81} \cdot \overline{17} = \overline{99} \text{ (ul. 2 cifre)} 2017^{2017}$$

la curs 3: modulul celor două de numere

$m \in \mathbb{N}^*$

$$G = \{ \bar{a} \mid a \in \mathbb{Z}, (a, m) = 1 \}$$

$a_i \neq a_j \text{ pt } i \neq j$

2^{23}

$\overline{a_0 a_1 a_2 \dots a_{22}}$

Cifra lipse

$$\bar{a} = \bar{b} \stackrel{\text{def}}{\iff} g(a - b)$$

$$\bar{2}^6 = \bar{64} = \bar{1}$$

$$2^{-23} = (\bar{2}^6)^4 \cdot \bar{2}^5 = \bar{32} = \bar{5}$$

$$\leftarrow = \overline{0 + 1 + 2 + \dots + 5} + 0 \cdot \bar{2}^2$$

$$a_i = 5$$

$$2^{23} = 536\ 840\ 912$$

Grupuri de clase de resturi #3

$m \in \mathbb{N}^*$

$a, b \in \mathbb{Z}$

$$\text{Scriem } \bar{a} \geq \bar{b} (\Leftrightarrow) m | (a - b)$$

\equiv Relație de echivalență

a) reflexivă $a \equiv a \pmod{m}$

$$\text{Dacă } m | (a - a) \Leftrightarrow m | 0 \text{ adeastă}$$

b) simetrică

$$a \geq b \pmod{m} \Leftrightarrow b \equiv a \pmod{m}$$

c) transițivă

$$\begin{aligned} a &\geq b \pmod{m} \\ b &\geq c \pmod{m} \end{aligned} \quad \left\{ \Rightarrow a \geq c \pmod{m} \right.$$

$$\begin{aligned} \text{Dem} \quad m &| (a - b) \\ m &| (b - c) \end{aligned} \quad \left\{ \begin{array}{l} (+) \\ (-) \end{array} \right. \quad m \mid ((a - b) - (b - c)) \Rightarrow a \equiv c \pmod{m}$$

$$a) \bar{a} = \bar{a}$$

$$b) \bar{a} = \bar{b} \Leftrightarrow \bar{b} = \bar{a}$$

$$c) \begin{cases} \bar{a} = \bar{b} \\ \bar{b} = \bar{c} \end{cases} \quad \Rightarrow \quad \bar{a} = \bar{c}$$

Notation $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \bar{m-1}\}$

$$0 \leq i < j \leq m-1 \Rightarrow \bar{i} \neq \bar{j}$$

~~Def~~

Da es $\bar{i} = \bar{j} \Leftrightarrow m|(j-i)$, $m \in \mathbb{Z}_{\geq 2} \quad (\cancel{j-i}) \neq 0$
 $|j-i| \leq m$ a
wegen

$$2) |j-i| = |m| \cdot u \leq m-1 \Rightarrow m \leq m-1 \text{ contradiction}$$

Obs 1)

$$0 \leq i < j \leq m-1$$

~~Def~~ $i, j \in \mathbb{N}$ $\Rightarrow \bar{i} \neq \bar{j}$

$$2) a \in \mathbb{Q} \Rightarrow \exists i \in \{\bar{0}, \bar{1}, \dots, \bar{m-1}\} \text{ s.t. } \bar{a} = \bar{i}$$

Denn Th Impartition au rest $\Rightarrow a_2 \cdot q + r$

$$(2) m \mid (a - i) \Leftrightarrow \bar{a} = \bar{i}$$

$2 \in \mathbb{Q}$

Structura de grup pe \mathbb{Z}_m

$a, b \in \mathbb{Z}$

Definim $\bar{a} + \bar{b} = \overline{a+b}$

Este corectă definiția?

$$\left. \begin{array}{l} \bar{a} = \overline{a_1} \\ \bar{b} = \overline{b_1} \end{array} \right\} \Rightarrow \bar{a} + \bar{b} = \overline{a_1 + b_1} \quad \bar{a} + \bar{b} = \overline{\bar{a}_1 + \bar{b}_1}$$

$$\Rightarrow \bar{a} - \bar{a}_1 = \bar{0} \Rightarrow m \mid (a - a_1) \quad \left(\begin{array}{l} m \mid (a - a_1 + b - b_1) \\ \Rightarrow m \mid (b - b_1) \end{array} \right) \Rightarrow$$

$$\Rightarrow \bar{a} - \bar{a}_1 + \bar{b} - \bar{b}_1 = \bar{0} \quad \Rightarrow \bar{a} + \bar{b} = \bar{b}_1 + \bar{a}_1$$

Prop: $(\mathbb{Z}_m, +)$ grup comutativ cu m elemente

- relativ pe \mathbb{Z}_m

$$\bar{a} + (\bar{b} + \bar{c}) = \bar{a} + \bar{b} + \bar{c} \quad \text{(associativitatea este)} \quad \text{pe } \mathbb{Z}_m$$

$$\bar{a} + \bar{0} = \bar{a}, \forall \bar{a} \in \mathbb{Z}_m$$

$a \in \mathbb{Z}$

$$a + \overline{-a} = \overline{-a} + \overline{a} = \overline{0}$$

$$\begin{aligned}\overline{a+b} &= \overline{a+b} \\ \overline{b+a} &= \overline{b+a}\end{aligned} \quad \left. \begin{array}{l} \Rightarrow \overline{a+b} = \overline{b+a} \end{array} \right.$$

$\Rightarrow (\mathbb{Z}_m, +)$ grup abelian

Teorema $(G, +)$ grup comutativ $\Rightarrow (\mathbb{G}, +) \cong (\mathbb{Z}_m, +)$

$$\cancel{(\mathbb{G}, +) \cong (\mathbb{Z}_m^+, +)} \times \cancel{(\mathbb{Z}_n^+, +)}$$

$$G \cong (\mathbb{Z}_{m_1}, +) \times (\mathbb{Z}_{m_2}, +) \times \dots \times (\mathbb{Z}_{m_k}, +) \times (\mathbb{Z}, +)$$

Explicatia termenilor

1). $(G, +)$ grup

Suntem că $(G, +)$ este liniță generat, dacă există multime finită $\{g_1, g_2, \dots, g_m\} \subseteq G$, (a.i.) să se poată scrie el în poate formă $g = h_1 \cdot h_2 \cdots h_n$, unde $h_i \in \mathcal{G}$ și pt $i, j \in \overline{1, m}$

$(G_1, *)$, (G_2, \perp) - grupuri

Suntem că G_1 este izomorf cu G_2 ($G_1 \cong G_2$)

dacă $\exists f: G_1 \rightarrow G_2$, f bijectivă

$$f(g_1 \perp g_2) = f(g_1) \perp f(g_2)$$

Construcție: $(G_1, *)$, (G_2, \perp) și

$(G_1 \times G_2, \circ)$ - grup

Definim $(g_1, g_2) \circ (h_1, h_2) = (g_1 * h_1, g_2 \perp h_2)$

(e_1, e_2) - elemente neutre

$(g_1, g_2) \circ (h_1^{-1}, h_2^{-1}) = (e_1, e_2)$

Definim o altă operare pe \mathbb{Z}_m

$$\bar{a} \cdot \bar{b} = \bar{a \cdot b} \quad - demonstrație similară$$

elementul neutru este $\bar{1}$

Obs $\bar{0}$ nu este invers

$$\bar{a} = a \bar{0} = \bar{0} \cdot \bar{a}, \forall a \in \mathbb{Z}_m$$

Q) (\mathbb{Z}_m, \cdot) - monoid

$$U(\mathbb{Z}_m) = \{ \bar{a} \mid a \in \mathbb{Z}, (a, m) = 1 \}$$

$$\text{Ex } U(\mathbb{Z}_{12}) = \{ \bar{1}, \bar{5}, \bar{7}, \bar{11} \} \quad \bar{1} \cdot \bar{1} = \bar{1}$$

$$\bar{5} \cdot \bar{5} = \bar{1}$$

$$\bar{7} \cdot \bar{7} = \bar{1}$$

$$\bar{11} \cdot \bar{11} = \bar{1}$$

$$\prod_{i=1}^n (\mathbb{Z}_{m_i}, +) \quad | \quad |(A \times B)| = |A| \cdot |B|$$

$$(\mathbb{Z}_4, +) \times$$

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

Proprieta $(U(\mathbb{Z}_m), \cdot)$ grup

// teorema lemea dedata treanta

$$\bar{a} \in U(\mathbb{Z}_m)$$

$$\bar{b} \in U(\mathbb{Z}_m) \quad | \quad | \quad \bar{a} \cdot \bar{b} \in U(\mathbb{Z}_m)$$

$$\Rightarrow (a; m) = 1$$

$$\Rightarrow (b; m) = 1 \quad | \quad | \quad (a \cdot b; m) = 1$$

Demonstra

$$\bar{m} \cdot \bar{a} = \bar{m} \cdot \bar{b} \quad (=)$$

$$\bar{a} = \bar{b}, m, q, b \text{ sunt}$$

$$\Rightarrow \begin{cases} (m, a) = 1 \\ (m, b) = 1 \end{cases}$$

$$m \mid (ma - mb) \quad (=) \quad m \mid m(a - b) \quad (=)$$

$$(a, m) = 1$$

$$\Rightarrow m \mid (a - b) \quad (=) \quad \bar{a} = \bar{b} \quad (m, m) = 1 \quad (=)$$

Principul inclusivului și exclusivului (P_i & P_e)

A_1, A_2, \dots, A_m multimi mănuște

$$\left| \bigcup_{i=1}^m A_i \right| = \sum_{j=1}^m |A_j| - \sum_{1 \leq i < j \leq m} (A_i \cap A_j) + \dots + (-1)^{m+1} \left| \bigcap_{j=1}^m A_j \right|$$

Câte elemente are $P(m)$

$$P(m) = \{ n \in \mathbb{N} \mid 0 \leq n \leq m-1, (m, n) = 1 \} \subset \phi(m)$$

$$2 \leq m = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}, p_i \neq p_j \forall i \neq j, 1 \leq i, j \leq r$$

$$|A-B| = |A|-|B|$$

$$A = \{ k \mid 0 \leq k \leq m-1, (k, m) \neq 1 \} \Rightarrow \{ p_i \mid k \}$$

$$A' = \{ k \in \mathbb{N} \mid 0 \leq k \leq m-1, p_i \nmid k \}_{i=1, 2, \dots, r}$$

$$A = \bigcup_{j=1}^r A'_j \text{ aplicăm formula } (P_i \& P_e)$$

$$\phi(m) = m - \sum_{j=1}^r \frac{m}{p_j} + \sum_{i,j} \frac{m}{p_i p_j} - \sum_{i=1}^m \frac{1}{p_1 p_2 \cdots p_k \cdots p_{i-1} p_{i+1} \cdots p_r}$$

Principiul includerii si excluderii

 A_1, A_2, \dots, A_n multimi finite

$$\text{Atunci } |\bigcup_{i=1}^n A_i| = \sum_{i=1}^n |A_i| - \sum_{0 \leq i < j \leq n} |A_i \cap A_j| + \\ + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n|$$

Dem- inducție după n Inducție $n=1$: $|A_1| = |A_1|$ evident

$n=2$: $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

$A_1 \cap A_2 = \{x_1, x_2\}$

$A_1 \setminus A_2 = \{x_1\}$

$A_2 \setminus A_1 = \{x_2\}$



$t+h+x = |A_1 \cup A_2|$

$$|A_1| + |A_2| - |A_1 \cap A_2| = (t+h) + (x+h) - t \cancel{+ h \cancel{- t}} \\ = h + x = |A_1 \cup A_2|$$

- D.P Aden pt n dem pt $n+1$ A_1, A_2, \dots, A_n multimi finite

$$|\bigcup_{j=1}^{n+1} A_j| = |x \cup A_{n+1}| = |x| + |A_{n+1}| - |x \cap A_{n+1}| \xrightarrow{\text{carac } n+2} \text{aplic ipoteza}$$

$x = A_1 \cup A_2 \cup \dots \cup A_n$

A_{n+1}

de inducție pt
e calculat $|x|$

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

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

$$A_{n+1} \cap X = A_{n+1} \cap (A_1 \cup A_2 \cup \dots \cup A_n) = (A_{n+1} \cap A_1) \cup (A_{n+1} \cap A_2) \cup \dots \cup (A_{n+1} \cap A_n)$$

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

$$|A_{n+1} \cap X| = |A_{n+1} \cap A_1| + |A_{n+1} \cap A_2| + \dots + |A_{n+1} \cap A_n|$$

*ipoteza
ind*

$$|A_1| - |A_1 \cap A_2 \cap A_3 \cap \dots \cap A_n| - |A_1 \cap A_2 \cap A_3 \cap \dots \cap A_{n-1}| = \dots + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n \cap A_{n+1}|$$

$$(A_{n+1} \cap A_1) \cap (A_{n+1} \cap A_2) = A_1 \cap A_2 \cap A_{n+1}$$

$(\cup(\mathbb{Z}_n), \cdot)$ grup ^{comutativ} cu $\varphi(n)$ elemente
 $n \in \mathbb{N}, n \geq 2$

$$a, b \in \mathbb{Z} \quad \text{def} \quad \bar{a} = \bar{b} \Leftrightarrow n \mid a - b$$

$(\mathbb{Z}_n, +)$ grup comutativ cu n elem

$$\bar{a} + \bar{b} = \overline{a+b}$$

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

$$a \in U(\mathbb{Z}_n)$$

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

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

$$\varphi(n) = |\{a \in \mathbb{Z} \mid 0 \leq a \leq n-1, (a, n) = 1\}|$$

$$\varphi(n) = n \cdot \prod_{p \mid n} (1 - \frac{1}{p})$$

p.prim

$$p \mid n$$

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

$$p_1 < p_2 < \dots < p_k$$

$$\begin{aligned} p_j &\text{ prim, } \alpha_j \in \mathbb{N}^* \\ b_j &= \bar{a} \end{aligned}$$

$$D(a) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1})$$

Teorema lui Lagrange:

(G, \cdot) grup comutativ finit
2-élément neutru

$$g \in G$$

$$|G|$$

$$\Rightarrow g = e$$

Astăzi Lagrange pentru $(G, \cdot) = (\mathbb{U}(\mathbb{Z}_n), \cdot)$
 $a \in \mathbb{Z}, (a, n) = 1 \Rightarrow |a|_{\mathbb{U}(\mathbb{Z}_n)} = \bar{n}$

Teorema (Euler)

$$\begin{aligned} a \in \mathbb{Z} \quad (a, n) = 1 \\ n \in \mathbb{N}, n \geq 2 \end{aligned} \Rightarrow \begin{cases} \bar{a}^{\varphi(n)} = \bar{1} \\ n \mid a^{\varphi(n)} - 1 \end{cases}$$

Caz particular al teoremei lui Euler

$$\underbrace{n \text{ prim}}_{\text{rezultat}} \Rightarrow \varphi(n) = n - 1 \quad \begin{cases} a \in \mathbb{Z} \\ (a, n) = 1 \end{cases} \Rightarrow \begin{cases} \bar{a}^{n-1} = \bar{1} \\ n \mid a^{n-1} - 1 \end{cases}$$

$$n \text{ prim } \bar{n} = 1$$

$$a \bar{=} 1$$

$$n = p_1$$

$$\varphi(n) = p_1 - p_1^2 = p_1 - 1 = n - 1$$

Mica Teoremă a lui Fermat

Ex: p prim $\Rightarrow 7p + 3^p - 4$ nu este patrat perfect.

$$k_2 = 14 + 9 - 4 = 19 \text{ nu e pp}$$

$$k_3 = 21 + 27 - 4 = 44 \text{ nu e pp}$$

$$k_4 = 35 + 243 - 4 = 274 \text{ nu e pp}$$

șapte

Dam

$$p=4K+1$$

$$\textcircled{Z_4} \quad \overline{x_p} = \overline{2p+3}^T - \overline{4} \quad p=\overline{1} \quad \overline{3} = \overline{6}^T = \overline{-2} = \overline{3}$$
$$= \overline{2} + \overline{3} = \overline{1}$$

$$4k+2+u^2$$

$$\text{Fact. cases: } u^2 \Rightarrow \begin{cases} u \text{ odd} \\ u \text{ even} \end{cases}$$

$$4k+2+4n^2$$

$$\Rightarrow 4|2$$

$$2=0, Z_4 \text{ } \cancel{\propto}$$

$$\begin{array}{l} p \text{ prim} \\ p \neq 2 \end{array} \quad \left. \begin{array}{l} p=4K+1 \\ p=4K+3 \end{array} \right\} \Rightarrow \begin{array}{l} p=4K+1 \\ p=4K+3 \end{array}$$

$$p=4K+3, K \in \mathbb{N}, p \text{ prim}$$

$$\text{Fact. } \overline{2p+3}^T - \overline{4} = \overline{u}^2 \quad u \in \mathbb{Z}$$

$$\overline{Z_2}$$

$$\overline{3} - \overline{u} = \overline{2p+3}^T - \overline{4} = \overline{u}^2$$

$$\text{DX3} \Rightarrow 3^{p+1} = \overline{7} \Rightarrow \overline{3}^p = \overline{7} \quad p \mid u^2 \Rightarrow$$

Par. L Fermat

$$\textcircled{7} = (\textcircled{7})^{\frac{p-1}{2}} = (\overline{2}^2)^{\frac{p-1}{2}} = \overline{2}^{\frac{p-1}{2}} = \textcircled{7}$$

$$\frac{p-1}{2} = 2K+1$$

$$\Rightarrow 1 = (-1)^{2K+1} = -1$$

$$\text{DX40}$$

$$\overline{u}^{\frac{p-1}{2}} = \overline{7}$$

$$\Rightarrow p \mid 2$$

$$p=2 \cancel{\propto}$$

Algoritmul de criptare RSA (Rivest, Shamir, Adleman)

• CESAR

ABCD : XYZ
0 1 2 3 23 24 25

ZARURILE AU FOST ARUNCATE

CDU...

(n, e) \rightarrow publice

$n = p \cdot q$ p, q prime destinate, mari

p, q secrete $\varphi(p \cdot q) = (p-1)(q-1)$

$\text{lcm}(e, \varphi(n)) = 1$

"Alfabet" 26^k $k \in \mathbb{N}$

26-lungimea alfabetului

STEAVĂ ECSB

o secvență de k simboluri

$a_{k-1}, a_{k-2}, \dots, a_1, a_0$

se transformă într-o secvență de
 $k+1$ simboluri

$a_j \leftrightarrow m$

$P = a_{k-1} \cdot 26^{k-1} + a_{k-2} \cdot 26^{k-2} + \dots + a_1 \cdot 26 + a_0$

mesajul criptat este $P^e = \overline{Q}$

z_n

$0 \leq Q \leq 2^n - 1$

$Q = b_k \cdot 26^k + \dots + b_1 \cdot 26 + b_0$

Ex

$n = 213 \quad e = 89$

$26^2 = 676$

$N \cup \frac{13}{20} \rightarrow 13 \cdot 26 + 20 = 358$

$26^3 > 713$

$$NU \rightarrow \overline{358}^{89}$$

$$f_{23} = 2 \cdot 7^2 - 6^2 = 2 \cdot 49 - 36$$

$$Z_{23} \cdot 358 \cdot 23 = 13 \cdot 915$$

$$\overline{73} = \overline{1}$$

Nach Einsetzen

$$\overline{358}^{89} = \overline{13}^{89} = (\overline{13}^{23})^6, \overline{13} = \overline{13}$$

$$Z_{23} \cdot \overline{358}^{89} = \overline{13}^{89} = \overline{13}^{23}$$

$$\overline{13} \cdot x = \overline{7}^{30} = \frac{1}{\sqrt{2}}$$

$$\overline{3}x = \overline{6} \cdot x = \overline{2} = \overline{33} \quad x = \overline{m}$$

$$x = 23 \text{ u.t. 11}$$

$$(x = 31 \text{ u.t. 11})$$

$$Z_{23} \cdot \overline{310644} = \overline{23} \text{ u.t. 13} = \overline{13}$$

$$\overline{52} = \overline{13}^{-1} = \overline{2}$$

$$\overline{52} \cdot \overline{13} = \overline{1} = \overline{24}$$

$$v = \overline{6}$$

$$= \overline{713} \text{ t. } \overline{310644} = \overline{197}$$

$$NU \rightarrow \overline{358}^{89} = \overline{197} = \overline{26 \cdot 7 + 15} = 0 \cdot 26^2 + 7 \cdot 26 + 15$$

$$NU \rightarrow 0, 7, 15 \\ A \text{ H P}$$

Descriptare casul general

1) baza $\underline{P, Q}$

2) $\overline{\epsilon} \cdot f = \overline{f} \in U(Z_n)$

3) $\overline{Q} \cdot f \in Z_n$

Theorema lui Wilson

Dacă p prim, atunci $p \mid ((p-1)! + 1)$

$$p = 7$$

$$6! + 1 = 720 + 1 = 721 \quad \left| \begin{array}{l} \\ \end{array} \right. \quad 7 \mid 721$$

$$p = 23 \quad \cancel{223}$$

$$22! = (2 \cdot 12) \cdot (3 \cdot 8) \cdot (5 \cdot 14) \cdot (7 \cdot 10) \cdot (9 \cdot 18) \cdot$$

$$\cancel{(15 \cdot 20)} \quad (16 \cdot 13) \cdot (21 \cdot 11) \cdot (17 \cdot 19) \cdot (1 \cdot 1)$$

$$\cancel{(22)}$$

$$\overline{22} \cdot \overline{22} = 1$$

Demonstratie

(G, \cdot) grup comutativ finit

$$g_1 \cdot g_2 \cdots g_n = a_1 a_2 \cdots a_j =$$

Dacă $g \neq g'$ diferență \Rightarrow unde $a_i^2 \neq 0$

$$g = g'^{-1} \quad g^2 = e$$

$$= \prod_{\substack{g \in G \\ g^2 \neq e}}$$

11

$$G = U(\mathbb{Z}_p)$$

grupuri $\varphi(p) = p-1$

Cate elemente dim G , $g^2 = p$?

$$\Rightarrow p \mid (x^2 - 1) \Leftrightarrow p \mid (x+1)(x-1),$$

$$\Rightarrow p \mid (x+1) \text{ sau } p \mid (x-1)$$

$$x \in \overline{1, p-1} \quad \left| \begin{array}{l} \Rightarrow x = p-1 \\ \text{sau} \\ x = 1 \end{array} \right.$$

$$\prod_{g \in G} g = (\overline{p-1}) \cdot \overline{1} = \overline{p-1}$$

$$\begin{array}{c} 2014 \\ \overline{16} \end{array} \Big| \begin{array}{c} 9 \\ 8\overline{15,1} \end{array}$$

$$2014^2 = 9 \cdot 9^2 + 9^2$$

$$p \text{ prim}, p = qk+l \Rightarrow p = a^2 + b^2$$

Negi criptografă numerele

A B C D E F ...

1 2 3 ...

$X = \text{produsul literelor}$

F, ...,

28

- | |
|------------------------|
| 1. restul împărțirii |
| 2. " la 2011 |
| 3. $x = a^2 + b^2$ |
| Dacă \exists soluții |

Demonstração

$$p \text{ primo} \quad p = 4k+1, \quad m = \left(\frac{p-1}{2}\right)! \Rightarrow \overline{m}^2 = -1$$

$$p=3$$

$$\overline{1} = \overline{1}$$

$$\overline{2} = \overline{2}$$

$$\vdots$$

$$\overline{6} = \overline{6}$$

$$\overline{7} = -\overline{6}$$

$$\vdots$$

$$\overline{12} = -1$$

$$\overline{\frac{1}{2}} = \overline{\frac{1}{2}}$$

$$\vdots$$

$$\overline{\frac{p-1}{2}} = \overline{\frac{p-1}{2}}$$

$$\overline{\frac{p+1}{2}} = \overline{\frac{p-1}{2}}$$

$$\vdots$$

$$\overline{p-1} = -1$$

$$(p-1)! = \overline{\left((-1)^{\frac{p-1}{2}}\right)} \cdot \overline{\left[\left(\frac{p-1}{2}\right)!\right]}^2$$

$$\therefore \overline{m}^2 = -1$$

$p = qk + 1$, $k \in \mathbb{N}$, $m = \left(\frac{p-1}{2}\right)!!$. Atunci $m^2 \equiv 1$
în \mathbb{Z}_p

Demonstrare

$$x \leq [x] \leq x+1$$

$$[\sqrt{p}] < [\sqrt{p+1}] < [\sqrt{p}]+1$$

$$\sqrt{p} < \sqrt{x^2} < p$$

căputăm $p+1$ nr

$\exists x, y$ care au același rest - principiu căutări

STOP

Fie grup (G, \cdot) , $H \subseteq G$

(H, \cdot) subgrup \rightarrow parte stabilă

$\rightarrow \forall x \in H$, atunci $x^{-1} \in H$.

Teorema Lagrangei pentru grupuri

$$\text{Dann - also: } \bar{i} = \bar{j}$$

$$\bar{2} = \frac{\bar{1}}{2}$$

:

$$\frac{\bar{1}-\bar{i}}{2} = \frac{\bar{n}-\bar{i}}{2}$$

$$\frac{\bar{n}+\bar{i}}{2} = -\left(\frac{\bar{n}-\bar{i}}{2}\right)$$

$$\frac{\bar{n}+3}{2} = -\left(\frac{\bar{i}-\bar{3}}{2}\right)$$

$$\therefore \bar{i}-\bar{i} = -1$$

$$|\bar{(n-i)}| = (-1)^{\frac{n-1}{2}} \frac{m!}{(n-i)!}$$

$$(-1)^3 = (-1)^2$$

$$\bar{m}^2 = -1$$

$$m = \frac{\bar{n}-1}{2}$$

$$\bar{m}^2 = -1 \quad (\bar{Z}_p)$$

Def my $x, y \in \{0, 1, 2, \dots, [\sqrt{p}]^2\}$
 $([\sqrt{p}] + 1)^2$ zahl > p

$$x-1 < [\bar{z}] \leq z$$

$$([\bar{z}] + 1) > z \Rightarrow [\sqrt{p}] + 1 > \sqrt{p}$$

$$([\sqrt{p}] + 1)^2 > p$$

$$a_1, a_2, \dots, a_{p+1}$$

Partial Emp. Law: $a_1, a_2, \dots, a_{p-1} \quad \left\{ \begin{array}{l} 1 \leq i \leq p+1 \\ \text{a.i. } \bar{x}_i \bar{y}_i \in \bar{Z}_p \end{array} \right.$

$$\Rightarrow \exists (x_1, y_1) f(x_2, y_2) \text{ a.s. s.t. } my_1 = x_2 + m y_2 \text{ in } \bar{Z}_p$$

$$\text{Relation } a = \frac{x_1 - x_2}{y_1 - y_2}$$

$$b = \frac{y_1 - y_2}{x_1 - x_2}$$

$$|a| \leq |\sqrt{a^2 + b^2}| < \sqrt{a^2 + b^2}$$

$$x_1 - x_2 + m(y_1 - y_2) = 0$$

$$|b| \leq |\sqrt{a^2 + b^2}| < \sqrt{a^2 + b^2}$$

$$a + b m = 0$$

$$(a + b m) \cdot (a - b m) = 0$$

$$\frac{a^2 - b^2 - m^2}{a^2 + b^2} = 0, m^2 = -1$$

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

$$\Rightarrow n/a^2 + b^2 = 0$$

$$\text{Dek. } a^2 + b^2 = 0 \Rightarrow a = b = 0 \Rightarrow x_1 = x_2 \wedge y_1 = y_2 \quad \checkmark$$

$$0 < a^2 + b^2 \leq r^2 \quad | \quad \rho/a^2 + b^2 = r$$

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

Definitie:

(G, \cdot) grup

Ist $H \subseteq G$

H = subgrup dari:

$$1) \forall x, y \in H \Rightarrow x \cdot y \in H$$

$$2) \forall x \in H \Rightarrow x^{-1} \in H$$

$$(H, \cdot) \leq (G, \cdot)$$

\hookrightarrow subgrup

È possibile să există $(H, \cdot) \leq (G, \cdot)$?

$$|H|=2$$

$$|G|=0$$

M

CURS 6

Definizio: (G, \cdot) grup. $H \subseteq G$.
 $\underset{H \neq \emptyset}{}$

H s.m. subgroup al lui G (se măsoară $H \leq G$) dacă

- 1) $\forall x, y \in H \Rightarrow x \cdot y \in H$
- 2) $\forall x \in H \Rightarrow x^{-1} \in H$

Scop Teorema Lagrange: (G, \cdot) grup finit, $H \leq G$. Să se arate că $|H| / |G|$ (cardinalul H față de cardinalul lui G)

Demonstrare: Dacă $H = G$ enunțul este evident așa

Pp. ca $H \leq G$. Aleg $x \in G \setminus H$.
 $\hookrightarrow G \setminus H \neq \emptyset$

Consider multimea $x_1 H = \{x_1 \cdot h \mid h \in H\}$

Demonstrație că: 1) $|x_1 H| = |H|$
 2) $x_1 H \cap H = \emptyset$

Dem 1): $f: H \rightarrow x_1 H$, $f(h) = x_1 \cdot h$

f surjectivă.

Această f este inj.

$$h_1, h_2 \in H \text{ și } f(h_1) = f(h_2) \Rightarrow h_1 = h_2$$

$$x_1 \cdot h_1 = x_1 \cdot h_2$$

$$(3) x_1^{-1} \in G$$

$$h_1 = \underbrace{x_1^{-1} \cdot (x_1 \cdot h_1)}_{\text{orice}} = x_1^{-1} \cdot (x_1 \cdot h_2) = e \cdot h_2 = h_2$$

$$e \cdot h_1 = (x_1^{-1} \cdot x_1) \cdot h_1$$

$$e - @$$

$$\Rightarrow f \text{ inj} \Rightarrow f \text{ bijecție} \Rightarrow |H| = |x_1 H|$$

Dem 2): reducere la absurd

Pp. că $(\exists) g \in x_1 H \cap H$

$$g = x_1 \cdot h_1 = h_2 \quad h_1, h_2 \in H$$
$$1 \cdot h_1^{-1}$$

$$x_1 = x_1 \cdot h_1 \cdot h_1^{-1} = h_2 \cdot h_1^{-1}$$

$$x_1 \cdot e = h_2 \cdot h_1^{-1} \in H$$

$$h_1 \in H \Rightarrow h_1^{-1} \in H$$

\rightarrow \exists diverse $x_1 \notin H$

$$|H \cup x_1 H| = |H| + |x_1 H| = 2|H|$$

$$H \cap x_1 H = \emptyset$$

Cazul $H \cup x_1 H = G \Rightarrow |G| = 2|H|$ este multiplu de $|H|$

Cazul $H \cup x_1 H \subsetneq G$. Sun acizi că $x_2 \in G \setminus (H \cup x_1 H)$

$$H \cup x_1 H \cup x_2 H \subseteq G$$

Dem că $|x_2 H| = |H|$ analog (1)

Dem: $x_2 H \cap (H \cup x_1 H) = \emptyset$

Pp că: $x_2 H \cap (H \cup x_1 H) \neq \emptyset$

pt. asemenea \Rightarrow $x_2 h_1 = h_1$

$$h_1, h_2 \in H$$

$$\text{ sau } x_2 h_1 = x_1 h_2$$

$$x_2 = h_2 h_1^{-1} \in x_1$$

\exists

$$x_2 = x_1 \cdot h_2 \cdot h_1^{-1} \in x_1$$

\exists

$$|H \cup x_1 H \cup x_2 H| = 3|H|$$

$$|H \cup x_1 H| + |x_2 H| = 2|H| + |H| = 3|H|$$

$\Rightarrow |G| = 3|H|$ este multiplu de $|H|$

Cazul $HU \times_1 HU \times_2 H \not\in G$

Aleg $\frac{x_3 \in G}{x_2 \in G} (HU \times_1 HU \times_2 H) \dots$

Ve se întâlnește un moment în care nu se obține:

$$G = HU \times_1 HU \times_2 HU \dots U \times_n H$$

Dacă nu se obține egalitatea menită $\Rightarrow |G| \geq (n+1) \cdot |H| \geq n+1, \forall n \in \mathbb{N}$

Doar că G este finită.

Cazul II): (G, \cdot) grup finit comutativ, $g \in G$

T. George

$$\text{Atunci } g^{|G|} = e, \quad e = \text{id}$$

Azi: Dăm p. necomutativă

G grup finit $g \in G$

ord $g = \min \{ k \in \mathbb{N}^* \mid g^k = e \}$
ordinalul lui g ↓ ordinul

Justificare: $\{ g, g^2, g^3, \dots, g^{[G]}, g^{[G]+1} \} \subseteq G$ \rightarrow sunt $|G|$ elem.

$$\Rightarrow 1 \leq i \leq j \leq |G| + 1$$

$$\text{arătă: } g^i = g^j$$

$$g^{j-i} = e$$

$$1 \leq j-i \leq |G| \Rightarrow$$

T Lagrange: (G, \cdot) gr. Ringe, $H \leq G$ - So se erzählt es $|H|/|G|$ ^{ausdrückt}

Denn. $g \in G$ $H = \{e, g, g^2, \dots, g^{d-i}\}$
 $; \quad d-i = d$
 $g \cdot g = g = e$
 $0 \leq i \leq d-1$

1) $H \leq G$
 2) $|H| = d$

$$g^x = g^i \cdot g^j = g^{i+j} \in H$$
 $i+j = d \Rightarrow i = d-j$
 $n = \{0, 1, \dots, d-1\}, g \in \mathbb{Z}$
 $g^0 = e$
 $0 \leq i \leq d-1 \Rightarrow g^i \neq g^j$
 $\text{Denn. } g^i = g^j \Rightarrow g^{i-j} = e$
 $d \geq i-j \geq 0$
 def. lini. f.

aus - folgern T. Lag $\Rightarrow \text{el. } |H|/|G|$
 $|G| = dl - m$

$$g^l = g^{dl} = (g^d)^m = e^m = e$$
 $m \in \mathbb{N}^*$

Example:

$$G = (\mathbb{Z}_{100}, +)$$

$$\text{ord } \overline{56} = ?$$

def: ord einer Klasse $d \in \mathbb{N}^k$ s.t.

$$\overline{56d} = d \cdot \overline{56} = \overline{0}$$

$$100 | 56d$$

$$25 | 14d \Rightarrow 25 | d$$

$$\text{ord } \overline{56} = 25$$

$$\overline{G_1} = \cup (\mathbb{Z}_{100}) \rightarrow \text{gruppe mit 40 elementen}$$

$$\overline{3} \in G \quad \text{und } \overline{3} \text{ im } G_1$$

• Cum se calcula ord $\bar{V}, \bar{V} \in S_n$? (ordine unei permutări)

1) Se decompune \bar{V} în produs de cicluri disjuncte.

(a_1, a_2, \dots, a_k) este un ciclu al lui \bar{V} .

Def - h.s.m. lungimile ciclului (a_1, a_2, \dots, a_h)

$$\bar{V}(a_j) = \begin{cases} a_{j+1} & \forall j = 1, h-1 \\ a_1 & j = h \end{cases}$$

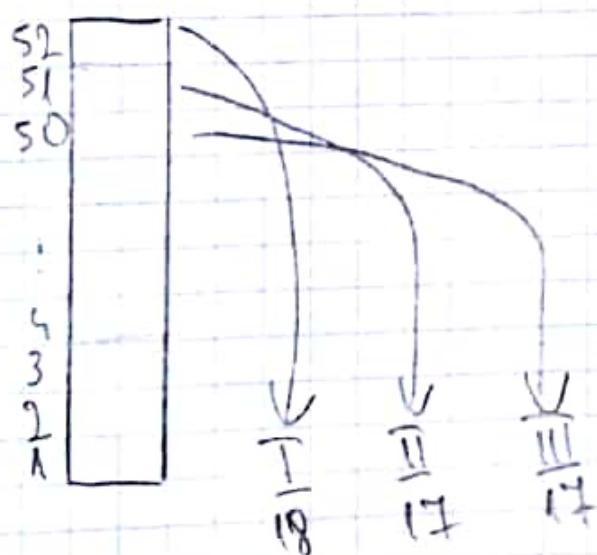
$$\text{ord } (a_1, a_2, \dots, a_h) = h$$

$$\text{in } S_n \quad a_i \neq a_j \quad \forall i \neq j$$

$$a_j \in \{1, 2, \dots, n\} \quad \forall j = 1, h$$

2) ord $\bar{V} = \text{c.m.m. m.c. al lungimilor ciclilor care apar în decompunerea lui } \bar{V}$

↓ problema cu permutări de curs (C1?)



Noi! Pachet



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	18	52	35	17	51	34	16	50	33	15	49	32	14	48	31	13	47	30	12	46	29	11	45	28	10	44

	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
	27	9	43	26	8	42	25	7	41	24	6	40	23	5	39	22	4	38	21	3	37	20	2	36	19	1

Dificil halfman ≈ 1975 (-D+E)

Ax_0 \rightarrow cyclic group

Dacă $p \mid p^k - 1$.

$(\mathbb{Z}/2^p)^\times$ - grup ciclic

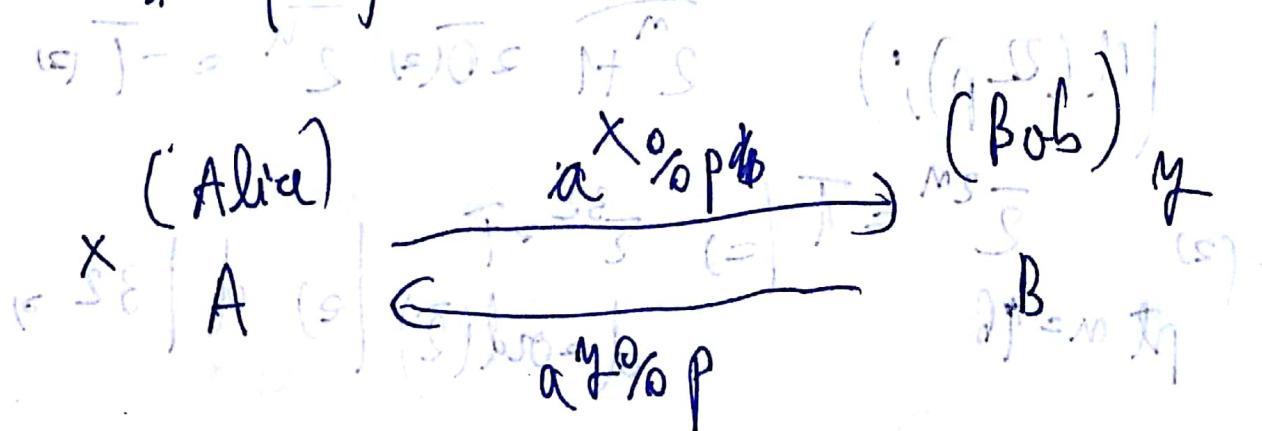
$$|\mathbb{Z}/2^p| = \{1, \bar{a}, \bar{a}^2, \dots, \bar{a}^{p-1}\}$$

$$|\mathbb{Z}/2^p| \cong \varphi(p)^2 \cdot p^{-1}$$

(5) $\text{deoarece } \text{ord } \bar{a} \text{ este impar} \Rightarrow (\text{ord } \bar{a}) \mid p-1 \Rightarrow \text{ord } \bar{a} = p.$

(1-4) $\text{I. b. } \text{ord } \bar{a} \text{ este impar} \Rightarrow (\text{ord } \bar{a}) \mid p-1 \Rightarrow \text{ord } \bar{a} = p.$

// definiția ordinului



$\rightarrow S = T \oplus T \cap S$ $\rightarrow (T, T \cap S) = 1$ $(p, q) \text{ publice}$

(oneară)

$T \oplus S \cong T \oplus (T \cap S) \cong T$

11

$(\exists x)(\frac{1}{a}x = b) \Leftrightarrow b \in \overline{O, p-1}$ și $a^x \equiv b \pmod{p}$

cheia comună $a^{x,y}$

Numele prime mari

$2^{\frac{p-1}{2}} + 1$ este

$\left(2^{\frac{p-1}{2}} - 1\right)N$

Ex. $\frac{2^m + 1}{p}$ prim atunci $p = 2^m + 1$ nu

Dacă $2^{16} + 1$ prim

$\Rightarrow p$ prim $\Leftrightarrow (p-1)$ este divizibil cu $2^m + 1$ $\Rightarrow \text{ord}(2) \mid (p-1)$

$(d(2, p);)$ $2^m + 1 \equiv 0 \pmod{2^m} \Rightarrow -1 \mid 2^m$

$\Rightarrow \frac{2^m}{2} = 1 \Leftrightarrow \frac{32}{2} = 1$ (corect)

pt $m=16$ $d \mid 32 \Rightarrow d \mid \text{ord}(2)$

$d \mid 32$ $\Rightarrow d \mid \text{ord}(2) = 32$

$\text{ord}(2) + 1 \mid 32$

$\text{ord}(2) \mid 32 \Rightarrow -1 \mid 32$

$\Rightarrow 32 \mid (p-1) \Rightarrow p \neq 32 + 1 = 33$

21

$$t=1 \Rightarrow p=33 \quad X$$

$$t=2 \Rightarrow p=65 \quad X$$

$$t=3 \Rightarrow \boxed{p=97} \quad X$$

$$t=4 \Rightarrow \boxed{p=161} \quad X$$

$$t=5 \Rightarrow \boxed{p=193} = 9 \quad \text{X}$$

principiu de inducție matematică

$$2^{2^m} + 1 - \text{prim pentru } \{0, 1, 2, 3, 5, 7, 17\}$$

Categorie $2^m - 1$

$$2^{420428} - 1 - \text{(exemplu zilei)}$$

Ex: dacă $2^u - 1$ - prim \Rightarrow u prim

Cele mai mari sur prime explicate

n par

$$(2^u - 1) \text{ perfect patrat} \Leftrightarrow 2^u - 1 \mid (2^u - 1)^2$$

deci $2^u - 1 = d_1 \cdot d_2 \cdots d_k$

Denum: 2^{u-1} prim (cel mai mare din antichitate)

$$2^{13} - 1 = 281 \cdot 31$$

281 este prim, deci 281 este prim

$\text{im}(\alpha(2\varphi))$

$$\overline{2}^{13} = \overline{1}, \quad \text{ord}(\overline{2}) = 13$$

$$13|(p-1) \quad p = 1 + 13t, \quad 13|p-1$$

$$t = 2, 4, 6$$

$$\hookrightarrow p = 2^4 t$$

$$\hookrightarrow p = 53$$

$$\hookrightarrow p = 179$$

impăriție 8191 la p

$$\text{ord } \overline{2} = 179$$

$$2^{13} - 1 \text{ este prim}$$

la fel se poate demonstra și pentru $2^{11}-1$

$$4) \quad \text{ord } g^K = \frac{\text{ord } g}{\text{gcd}(K, \text{ord } g)}$$

(5) (G, \cdot) grup comutativ $\text{gcd}(a, b)$

$$\text{gcd}(\text{ord } a, \text{ord } b) = 1 \Rightarrow \text{ord}(ab) = \text{ord } a = \text{ord } b$$

de demonstrat la exercițiu nr. 5

91.

Grupuri de permutări

$n \in \mathbb{N}^*$

$S_n = \{ f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\} \text{ fără fix}\}$

$(S_n, \circ) \sim \text{grup}$

$f, g \in S_n$ înțelesă ca permutări

$f \circ g : \{1, 2, 3, \dots, n\} \rightarrow \{1, 2, \dots, n\}$

$(f \circ g)(j) = f(g(j)) \quad \forall j = 1, n$

Ex: grup comutativ. De ce? există 2 elemente care
nu comută.

$\text{Obs } |S_n| = n!$

Se numește semnătura unei permutări

$\tau = (\tau_1, \tau_2, \dots, \tau_m) \in \prod_{1 \leq i < j \leq m} \frac{\tau(i) - \sigma(i)}{j-i} \in \{-1, 1\}$

// Definiția inversă a lui τ

$(i, j) \sim \text{inversie} \quad (i < j)$

$\tau(i) > \sigma(j)$

5/

Prop:

$$\mathcal{E}(\sigma \circ \tau) = \mathcal{E}(\sigma) \cdot \mathcal{E}(\tau)$$

- urm de demonstrat folosind formula

fie $\sigma, \tau \in S_n$ și $f: X \rightarrow Y$ funcție

ordinele unei permutări $\sigma^k = \sigma \circ \sigma \circ \dots \circ \sigma$ identică

Cidrul unei permutări

$a_1, a_2, \dots, a_k \in f^{-1}(x)$

$$N_f = \{j \mid \sigma(a_k) = \sigma(a_1), \dots, \sigma(a_j) = \sigma(a_{j+1})\}$$

trebuie să fie $j < k$

Nolâncidul ca o permutare determinată

Spunem că

$(a_1, a_2, \dots, a_m) \in (b_1, b_2, \dots, b_n)$ sunt disjuncții

dacă $\{a_1, a_2, \dots, a_m\} \cap \{b_1, b_2, \dots, b_n\} = \emptyset$

dacă nu, atunci cei doi ciclici comună

ord(ciclu) $\geq K$

$(f) \rightarrow \langle 0 \rangle$

E/

$\tau = (a_1, a_2, \dots, a_k)$

~~$\tau^2 = (a_1, a_2, \dots, a_k)$~~

$$\tau^k(a_1) + \tau^{k-1}(\tau(a_1)) + \tau^{k-1}(a_2) =$$

$= \dots = a_1$ - inducțiv

că k este cel mai mic număr care are această proprietate

2 cicli disjuncti

$$\text{ord}((a_1, a_2, \dots, a_k) \cdot (b_1, b_2, \dots, b_t)) = [k, t]$$

cel mai mare multiplu
 comun

$$\sigma = (a_1, a_2, \dots, a_k)^0 \cdot (b_1, b_2, \dots, b_t)^0 \dots$$

~~τ^k~~

cicli disjuncti

$$\text{ord } \sigma = [k, t, \dots]$$

lungimile adiutorii

Problema bonus

A, B, C, D, ...

?

$$\sigma \in S_{26}$$

rezolvă în context ca o permutare

YY

-y K, Q, X, Y, W}

B M H A B C P I O C B P H Z A R G N I Z B P H D M
N M B P G H A N O H I M A Z O P D E L O M O P S E F
M I H E M N M O P D I Z A R V O R B P O H I

Algebra

- alt test de așteptăt

există diferență: $\sigma_1, \sigma_2 \Rightarrow \sigma_1^0 \sigma_2 = \sigma_2^0 \sigma_1$

$$(a_1, a_2, \dots, a_k)^k = e \quad e \text{ este un element identic}$$

- ordinul unei cicluri lungimea este k

$\sigma = (a_1, a_2, \dots, a_k)$ ciclul lungimea k
 $a_k = e$
 $\sigma^m(a_1) = ?$

$$m = kq + r, q, r \in \mathbb{N}, r < k$$

$$\sigma^m(a_1) = \sigma^r(a_1) = \sigma(a_{r+1})$$

Demonstrare

Formula pt ordinul unei permutări

Fie $m \in \mathbb{N}$, astfel că $\sigma^m = e$

$$\Rightarrow \sigma^m(a_1) = a_1 = a_{r+1} \Rightarrow r = 0$$

$\sigma^m = (a_1, a_2, \dots, a_{k_1})^0 (b_1, b_2, \dots, b_{k_2})^0 \dots$
cicluri diferență comută

$$m = k_1 q_1 + r (=) K_1 / m$$

Repet argumentul pentru fiecare cule care apare în descompunerea lui σ , $K_j \mid M \Rightarrow [K_1, K_2, \dots, K_t] \mid M$

$$\Rightarrow [K_1, K_2, \dots, K_t] \leq M$$

Trebuie să demonstrezi că $\sigma^{[K_1, K_2, \dots, K_t]} = e$

$$[\sigma^{K_1}, \sigma^{K_2}, \dots, \sigma^{K_t}] = K_1 \cdot e, \quad e \in N^F$$

$$\sigma^{[K_1, K_2, \dots, K_t]}(a_1) = (\sigma^{K_1})^{a_1}(a_1) = a_1$$

Că fel pentru toate K_1, K_2, \dots, K_t

(G, \circ) grup

$H \leq G$ subgrup al lui G

Să numește subgrup normal al lui G ($H \trianglelefteq G$)

Dacă $x^{-1}hx \in H, \forall x \in G, h \in H$

Termen 1. - alegem doar anume nume

NUME PRENUME

NUME	PRENUME	
A B C D E F G H I J K L M N O P Q R S T U V X Y Z		- pe m
G I C A L E X N D R U V B F ...		

Scriem literele rămase (lexicografic)

B F H ...

Notăm cu $\langle \tau \rangle$ subgrupul generat de τ . Cercetăți dacă H este subgrup normal.

2. τ permutarea asociată - PRENUME Nume

Cercetăți dacă se întâmplă următorul lucru:

$$\forall x \in S_{26} \text{ a.i. } x\tau x^{-1} = \tau$$

3. Găsești toate cele prime p, q , astfel încât $p \nmid q | (q^p - 1)$

$$(p \cdot q) \mid (q^p - 1)(q^q - 1)$$

Demonstrare

Obs (G, \circ) grup comutativ, atunci orice subgrup H , este subgrup normal. (Evident)

$$(f \circ f^{-1}) \triangleq (G, \circ)$$

$$(G, \circ) \triangleq (G, \circ)$$

Fie H

H necomutativ $\neq f \circ f^{-1} \neq G$

Exemplu $G = S_3$ subgrup grup necomutativ cu 6 elemente

Subgrupurile lui S_3 - $H \Rightarrow |H| \in \{1, 2, 3, 6\}$

$$|H|=1 \Leftrightarrow H = \{\text{id}\} \quad |H|=6 \Leftrightarrow H = G$$

$$f\#| = 2 \quad P_2 = \begin{pmatrix} 1 & e^3 \\ 1 & 2e^3 \end{pmatrix}$$

Se numește transpozitie un ciclu de lungime 2, adică

$$H = \left\{ e, \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \right\} \quad NV \text{ este normal}$$

$$H_2 \neq e, \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$$

$$H = \left\{ e, \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} \right\} \quad NV \text{ este normal}$$

$$|A|^2 = 3 |H_2| \{ e, (1, 2, 3), (1, 3, 2) \}$$

$$H = \{ e \}, H_2 = \{ g \} \text{ normal}$$

Verificăm pe celelalte

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

(G, \circ) grup finit

(H, \circ) subgrup al lui G

nu există alt subgrup al lui H , care să aibă același număr de elemente ca H .

Atunci $|H| \geq 6$

$\{e, g\} : |H| = 2$ nu este un grup finit.

$\{e, g, h\} : |H| = 3$ nu este un grup finit.

$$H_1 = \{x h x^{-1} \mid h \in H\} = H x H^{-1}$$

Prengem $H_1 \subseteq H$

$$(x_1 h_1 x_1^{-1})(x_2 h_2 x_2^{-1}) = x_1 h_1 x_1^{-1} x_2 h_2 x_2^{-1} = h_1 h_2 \in H$$

$h \in H \quad h^{-1} \in H$

$$\text{fie } g(h) = x h x^{-1}, \forall h \in H$$

f injectivă

$$g(h_1) = g(h_2) \Rightarrow x h_1 x^{-1} = x h_2 x^{-1}$$

$\Rightarrow h_1 = h_2 \Rightarrow f$ injectivă

$\Rightarrow f$ bijecțivă $\Rightarrow |H| = |H_1|$

$\Rightarrow H_1 = H \Rightarrow H$ subgrup normal

Proprietate (6) grup $g(H)$ subgrup \Rightarrow

$\Rightarrow (H, \circ) \quad H \trianglelefteq G \Leftrightarrow$ dacă sunt adele în numărădăcă
multe echivalente cumătoare afirmație

$$1) \quad H \trianglelefteq G$$

$$2) \quad x H x^{-1} = H, \forall x \in G$$

$$3) \quad x H = H x, \forall x \in G$$

Notatii $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$

$Hx = \{xh \mid h \in H\}$

$hx = \{hx \mid h \in H\}$

Demonstram că $(1) \Rightarrow (2) \Leftarrow (3) \Rightarrow (1)$

$(1) \Rightarrow (2) \quad H \triangleq G$

$xHx^{-1} \subseteq H \cdot (a)$

$(x^{-1}x)H(x^{-1}) \subseteq x'Hx \quad H \subseteq x'Hx \quad \forall x \in G$
 $\cancel{x \in x^{-1}} \quad |^2$

$\Rightarrow H \subseteq xHx^{-1} \quad (b)$

$(a), (b) \Rightarrow H = xHx^{-1}$

$(2) \Rightarrow (3)$ evident

~~$xH \subseteq H$~~

$(3) \Rightarrow (1)$

$xH = Hx \quad xHx^{-1} = H$

consider $xh \in xH \Rightarrow xh \in Hx \quad (2) \quad xh \in Hx \Rightarrow h \in x^{-1}x \quad h \in G$

$(2) \quad h \in xhx^{-1}, \quad \forall x \in G \quad |^2 \quad H \triangleq G$

Rez fundamental în grupă factor

61

Subgroup normal. Grup factor.

Ex: $H_m = \frac{G}{mH}$ (de grup factor) ($H \trianglelefteq G$)

Def Subgrupul normal ($xhx^{-1} \in H, h \in H, x \in G$)
extrivial

Sunt echivalente afirmațiile

- a) $H \trianglelefteq G$
- b) $xHx^{-1} = H, \forall x \in G$
- c) $xhx^{-1} \in H, \forall h \in H, x \in G$

Observație

(G, ·) grup, $H \subseteq G$

$x_1, x_2 \in G$ Atunci

$x_1H = x_2H$ sau $x_1H \cap x_2H = \emptyset$

Demonstrare

Dacă sunt disjuncte

Pentru $x_1H \cap x_2H \neq \emptyset$

$\exists h_1, h_2 \in H \text{ s.t. } x_1h_1 = x_2h_2$

Doresc să arăt că $x_1H = x_2H$

11

$$1) X_1 H \subset X_2 H$$

$$x_1 h = (x_1 h_1) h_1^{-1} \cdot h \in X_1 H \quad \text{and} \quad x_1 h_1 \in X_2 (h_2 h_1^{-1} h) \in X_2 H$$

$$\Rightarrow X_1 H \subset X_2 H$$

$$2) X_2 H \subset X_1 H$$

$$x_2 h_2 = (x_2 h_2) h_2^{-1} \cdot h = x_1 (h_1 h_2^{-1} h) \in X_1 H, \forall h \in H$$

$$\Rightarrow X_2 H \subset X_1 H$$

$$(1)(2) \Rightarrow X_1 H = X_2 H$$

(G, ·) grup, H ⊆ G

$\frac{G}{H}$ grup factor

$$\frac{G}{H} = \left\{ xH \mid x \in G \right\}$$

Notatie: $x, y \in G$

$\hat{x} = \begin{cases} y & \text{daca } xH = yH \\ \emptyset & \text{altele} \end{cases}$

Ex: $H = m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$

$$0H = \{0, m, 2m, \dots, -m, -2m, \dots\}$$

$$\frac{G}{H} = \left\{ \hat{x} \mid x \in G \right\}$$

Notatii $\frac{G}{H} = \{ \hat{x} \mid x \in G \}$

introducem o operatie

x, y

$$\hat{x} * \hat{y} = \hat{x \cdot y}$$

Definitia este buna

Trebui sa arat

$$\hat{x}_1 * \hat{y}_1 = \hat{x_1 \cdot y_1}$$

Trebui sa arat ca $\hat{x} * \hat{y} = x y H = x_1 y_1 H$

$$\boxed{\begin{aligned}\hat{x} &= \hat{x}_1, \quad x = h_1^{-1} x_1 h_2 \\ \hat{y} &= \hat{y}_1, \quad y = h_3^{-1} y_1 h_4\end{aligned}}$$

$h_1, h_2, h_3, h_4 \in H$

$$\hat{x} * \hat{y} \stackrel{(1)}{=} x_1 h_2 \cdot h_1^{-1}$$

$$x_1 h_2 \cdot h_1^{-1} \stackrel{(2)}{=} x_1 h_2 h_1^{-1}$$

$$\hat{x} * \hat{y} \stackrel{(1)}{=} x_1 h_2 h_1^{-1} y_1 h_4^{-1}$$

$$x y = x_1 (h_1 \cdot y_1) h_2$$

Subgrupul normal $y_1 H = H y_1$

$$x_1 h_2 h_1^{-1} y_1 h_4^{-1} = x_1 h_2 h_1 h_4^{-1}$$

$$x y = x_1 h_2 h_1 h_4^{-1}$$

Un grupul finit are sens doar pentru subgrupurile normale.

Teorema $(\frac{G}{H}, +)$ grup

Demonstratie

1) Asociativitate

$$(\hat{x} * \hat{y}) * \hat{z} = \hat{x} * (\hat{y} * \hat{z})$$

$$(\hat{x} * \hat{y}) * \hat{z} = \hat{x} \hat{y} * \hat{z} = (\hat{x} \hat{y}) \hat{z}$$

$$\hat{x} * (\hat{y} * \hat{z}) = \hat{x} * \hat{y} \hat{z} = \hat{x} (\hat{y} \hat{z})$$

Asociativitatea din $G \Rightarrow$ asociativitatea din $\frac{G}{H}$

2) Element neutru

$$\hat{x} * \hat{e} = \hat{e} * \hat{x} = \hat{x}$$

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

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

3) Existenta inversului

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

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

Observabil $(6, +)$ grup finit, $H \trianglelefteq G$

Atunci $\left| \frac{G}{H} \right|^2 = \frac{|G|}{|H|} = \left(\left| H \right| / |6| \right)$

$$\frac{6}{m} = \left\{ xH \mid x \in G \right\}$$

$$P_{\text{per}} \left| \frac{G}{H} \right| \approx r$$

$x_1, x_2, \dots, x_r \in G$ a.i. $\frac{G}{H} = \{x_1 H, x_2 H, \dots, x_r H\}$

$x_i H + x_j H \quad (2) \quad x_1 H \cap x_2 H = \emptyset, \forall i, j$
pt $i \neq j$

$$x_1 H \cup x_2 H \cup \dots \cup x_r H = G \quad (2) \quad |G| = \sum_{i=1}^r |x_i H| =$$

$|x_1 H| = |H|$ (demonstrat in cursul anterior)

$$2) |H| \Rightarrow r = \frac{|G|}{|H|}$$

Definitie Morfism de grupuri
 (G_1, \cdot) $(G_2, *)$
+ izomorfism

Observati - f morfism de grupuri

- 1) $f(e_1) = p_1$
- 2) $f(x) = f(x')$

Demonstrare

$$\overbrace{f(e_1)}^{} = f(e_1 \cdot e_1) = f(e_1) * f(e_1) = e_2$$

$$f(\tilde{x}) * f(x) = f(x \cdot \tilde{x}^{-1}) = f(e_1) \Leftrightarrow f(\tilde{x}) * f(x) = e_2$$

$$\therefore f^*(\tilde{x}) = f(\tilde{x}^{-1})$$

$$\text{Ker } f = \{g \in G \mid f(g) = e_2\}$$

$$\text{Im } f = \{f(g) \mid g \in G\}$$

$$\text{Im } f \subseteq G_2$$

$$\text{Scopul este de a demonstra ca } \frac{G_1}{\text{Ker } f} \cong \text{Im } f$$

$$\text{Im } f \subseteq G_2$$

$$e_2 \in \text{Im } f$$

$$x, y \in \text{Im } f \Rightarrow x * y \in \text{Im } f$$

$$x = f(g_1)$$

$$y = f(g_2)$$

$$x * y = f(g_1 * g_2) \in \text{Im } f, g_1, g_2 \in G_1$$

Inversul neutral $e \in \text{Im } f$ -

~~$$f^{-1}(x) = f^{-1}(f(x))$$~~

Sei $x, y \in \ker f$, $x, y \in G$

$$f(xy) = f(x) * f(y)$$

$$\text{pt } f(x) = e_2$$

$$f(y) = e_2$$

$$f(\bar{x}) = f(\bar{x}^{-1}) \Rightarrow \bar{x}^{-1} \in \ker f$$

Sei $y \in G$, $x \in \ker f$

$$gy\bar{y}^{-1} \in \ker f?$$

$$f(gx\bar{y}^{-1}) \stackrel{\text{det morphism}}{=} f(g) * f(x) * f(\bar{y}^{-1}) =$$

Idee pt adematra rä $\frac{G_1}{\ker f} \cong \text{Im } f$

Th Teorema fundamentală de izomorfism pentru
grupuri. $f: G_1 \rightarrow G_2$

Astură $\frac{G_1}{\text{Ker } f} \cong \text{Im } f$

$\text{Im } f \leq G_2$ (demonstrat în cursul precedent)

$$\text{Ker } f = \{x \in G_1 \mid f(x) = e_2\} \quad e_2 - \text{el. neutru } G_2$$
$$\text{Ker } f \leq G_1 \quad e_1 - \text{el. neutru } G_1$$

Demonstrare TFIG

Def $\varphi: \frac{G_1}{\text{Ker } f} \rightarrow \text{Im } f$ prin formula $\varphi(\tilde{g}) = f(g)$

Trebuie să demonstreăm că φ este definită, morfism
de grupuri, și este bijecție.

$f: G_1 \rightarrow G_2$ morfism de grupuri

$$g_1 \circ g_2 \stackrel{?}{\Rightarrow} \varphi(f(g_1)) = \varphi(f(g_2))$$

$$\tilde{g}_1 \circ \tilde{g}_2 \stackrel{?}{\Rightarrow} f(h) = e$$

$h \in \text{Ker } f \Rightarrow f(h) = e$

$$\varphi(f(g_1)) = f(g_1) = f(h \circ g_2) = f(h) * f(g_2) = e * f(g_2) = f(g_2)$$

$$\varphi(g_1) = f(g_2) \stackrel{?}{\Rightarrow} \varphi(g_1) = \varphi(g_2)$$

11

$$\varphi(g_1 \cdot g_2) = \left(\frac{g_1}{\ker f}, f \right)$$

$$\varphi(\widehat{g_1 + g_2}) = \varphi(\widehat{g_1} + \widehat{g_2}) \stackrel{\text{def}}{=} f(g_1, g_2) = f(g_1) * f(g_2)$$

$\Rightarrow \varphi(\widehat{g_1}) * \varphi(\widehat{g_2})$ - decescă morfism

a). Fie φ este surjectivă

Dacă $x \in \text{Im } f \Leftrightarrow x = f(g)$

b). injectivitate

$$\varphi(g_1) = \varphi(g_2) \Rightarrow \widehat{g_1} = \widehat{g_2}$$

$$\varphi(\widehat{g_1} \cdot \widehat{g_2^{-1}}) = \varphi(\widehat{g_1}) * \varphi(\widehat{g_2}) = \varphi(\widehat{g_1}) * \cancel{\varphi(\widehat{g_2^{-1}})} = \varphi(\widehat{g_1})$$

$$\Rightarrow \varphi(\widehat{g_1}) * \varphi(\widehat{g_2}) = e_2$$

$$\varphi(g_1 \cdot g_2^{-1}) = f(g_1 g_2^{-1}) \stackrel{(2)}{=} f(g_1) \widehat{g_2} = e_2,$$

$$\Rightarrow g_1 \cdot g_2^{-1} \in \text{Ker } f \Leftrightarrow g_1 = h g_2 \Leftrightarrow \widehat{g_1} = \widehat{g_2}$$

$$\text{Atunci } \frac{\text{Im } f}{\text{Ker } f} \cong \text{Im } f$$

Obs. (G_1, \cdot) , $(G_2, *)$ grupe. $f: G_1 \rightarrow G_2$ morfism
de grupuri, nu adăugăte unatocare astăzi

a) f este injectivă

b) $\text{Ker } f \subseteq \text{Im } f$

\Rightarrow

$x \in \text{Im } f \Rightarrow f(x) = p$

f este injectivă.

$\Rightarrow x \in E_1$

\Leftarrow

$\text{ker } f = \{e\}$

$g_1 g_2 \in G_1$

$$f(g_1) = f(g_2)$$

$$\cancel{f(g_1) = f(g_2)}$$

$$f(g_1 \cdot g_2^{-1}) = f(g_1) \circ f(g_2^{-1}) = f(g_1) * f(g_2)^{-1} =$$

$$f(g_1) \cdot f(g_1)^{-1} = e_2 \Leftrightarrow g_1 \cdot g_2^{-1} = e_1 \Leftrightarrow g_1 = g_2$$

f injectivă

Tema devință numărul primelor

$m_2 \quad p$

1) Cate morfisme de grupuri $(\mathbb{Z}_m, +) \rightleftarrows (\mathbb{Z}_p, +)$

2) Este adverbat că $|\mathcal{M}_{mp}| \approx |\mathbb{Z}_m| \times |\mathbb{Z}_p|$
 justificare: $(+)(+)(+)$

3)

Aplicații Teorema

(G, \cdot) grup ciclic $\Rightarrow (G, \cdot) \cong (\mathbb{Z}, +)$ sau

Demonstratie $(G, \cdot) \cong (\mathbb{Z}_n, +)$ pt $n \in \mathbb{N}^*$

$$G = \{h^n \mid n \in \mathbb{Z}\}$$

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

$$f: \mathbb{Z} \rightarrow G, f(n) = h^n, h \in G$$

a) f este surjectivă, deoarece G este ciclic

b) f este injectivă morfism de grupe

$$f(m+n) = f(m) \cdot f(n) \Leftrightarrow$$

$$(\Leftarrow) h^{m+n} = h^m \cdot h^n \Rightarrow f$$
 este morfism de grupe

$$\text{TF}(G) \xrightarrow[\text{Ker } f]{} \frac{\mathbb{Z}}{m\mathbb{Z}} \cong \text{Im } f \cong G$$

Dacă $H \leq (\mathbb{Z}, +)$ atunci $H = m\mathbb{Z}$ (demonstrată la următoare)

$$\Rightarrow \text{Ker } f = m\mathbb{Z}$$

$$\frac{\mathbb{Z}}{m\mathbb{Z}} \cong \text{Im } f$$

Dacă $m=0 \Rightarrow \text{Ker } f = \emptyset \Rightarrow$ f injectivă }
f surjectivă } $\Rightarrow G \cong (\mathbb{Z}, +)$

$$\text{Dacă } m > 0 \Rightarrow \frac{\mathbb{Z}}{m\mathbb{Z}} \cong \mathbb{Z}_m$$

Problema bonus

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Caesar shift

C E R = U W Y

$$C + 18 \rightarrow 3 + 18 = 21$$

$$E + 18 =$$

$$R + 18 =$$

R E G E
+ 17 + 17 + 6 + 17

| R E P U | B L I C A
| + + + + + + + + +
| P V Y | S P O O R

$$\begin{array}{c} \cancel{P} + \cancel{V} + \cancel{Y} = 3 + 2 + 8 \\ \cancel{G} + \cancel{L} + \cancel{I} = 2 + 1 + 8 \end{array}$$

O U D Y . D Q Y I Y O C A | X F C Y (K M | O O i H F M)

V T S Y

Imagine current = 6 (A beautiful mind)

(6, 1) group $\{6\} \cong \mathbb{Z}_6 - \text{primes}$

$$G \cong (\mathbb{Z}_6)^t$$

Find $x \in G - \{e\}$ $\left\{ \begin{array}{l} \text{ord}(x) \mid p \\ \text{ord}(x) \geq p \end{array} \right\} \text{and } (x) \cong p$

$$x, x^p, x^{p^2}, \dots, x^{p^{n-1}}$$

elemente distincte, dacă $\text{ord}(x) = p$

$$\begin{aligned} & x \neq x^j \\ & 1 \leq i < j \leq n \quad \left\{ \begin{array}{l} \Rightarrow x^{j-i} \neq e \\ \text{ord}(x) \geq p \end{array} \right. \quad \left\{ \begin{array}{l} \Rightarrow p \mid j-i \Rightarrow p = j-i \\ i+j \end{array} \right. \end{aligned}$$

\Rightarrow contradicție $\Rightarrow x \neq x^p \neq \dots \neq x^{p^{n-1}}$

$g \in G \Rightarrow \exists i \in \{0, 1, \dots, p-1\}$ astfel încât $g = x^i$

$$f(g) = i \quad \text{f. c.: } (G, \cdot) \rightarrow (\mathbb{Z}_p^+, \cdot)$$

Exercițiul funcția este izomorfism de grupuri.

Seminar

grup cu 4 elemente $|G| = 4 \Leftrightarrow G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

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

Intre - grupuri (G, \cdot) $x, y \in G$ $(xy)^{-1} = y^{-1}x^{-1}$

Algebra #12

- criptose Vigenere (alta temă)

- engleză

- franceză

- germană

- italiana

- spaniolă

- lungime cuw ≤ 4

- cheia poate avea sens (ex. XYZ)

Grupul de permutări

$\tau, \tau \in S_m \quad Ax \in S_n$

În ce condiție există alte permutări α s.t. $X \circ \alpha^{-1} = \tau$?

Există α , dacă și numai dacă τ și α au același tip de descompunere:

Stim că orice permutare se descompune în produs de cicluri disjointe

$$\tau = (a_1, a_2, \dots, a_{k_1}) (b_1, b_2, \dots, b_{k_2}) \dots (x_1, x_2, \dots, x_{k_g})$$

Tipuri de descompunere = lista lungimilor ciclilor =

$$= (k_1, k_2, \dots, k_g) \quad \left(\sum_{i=1}^g k_i = m \right)$$

$$\text{Ex: } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 9 & 1 & 6 & 8 \end{pmatrix} = (1, 2, 3) (4, 5) (6, 7) (8)$$

$$\alpha \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 7 & 1 & 2 & 6 & 4 & 8 \end{pmatrix} = (1, 3, 4) (2, 5) (6, 7) (8)$$

Cele 2 liste nu coincid, dacă urmărește oarecum
 $T \circ \sigma$ sunt permutările conjugate

$$\Rightarrow X \circ X^{-1} = I \in C \Rightarrow C \text{ este } G \text{ în același desuprave}$$

$$C = (a_1, a_2, \dots, a_{K_1}) (b_1, b_2, \dots, b_{K_2}) \dots (x_1, x_2, \dots, x_{K_M})$$

$$X \circ X^{-1} = \underbrace{X(a_1, a_2, \dots, a_{K_1}) X^{-1}}_{\text{permutare }} (b_1, b_2, \dots, b_{K_2}) \dots$$

$$X^{-1} X (x_1, x_2, \dots, x_{K_M}) X^{-1}$$

$$X = \begin{pmatrix} 1 & 2 & 3 & \dots & n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_{K_1} & \dots \\ m_1 & m_2 & \dots & m_{K_1} & \dots \end{pmatrix}$$

// multe schimbări de ordine

$$\text{Calculați } X(a_1, a_2, \dots, a_{K_1}) X^{-1} = (m_1, m_2, \dots, m_{K_1})$$

$$(X(a_1, a_2, \dots, a_{K_1}) X^{-1})(m_1) = (X(a_1, a_2, \dots, a_{K_1}))(a_1)$$

$$= (X)(a_2) = m_2$$

$$(X(a_1, a_2, \dots, a_{K_1}) X^{-1})(f) = (X(a_1, a_2, \dots, a_{K_1}))(X(f))$$

$$\text{daca } f \in \{m_1, m_2, \dots, m_{K_1}\} \text{ atunci } X^{-1}(f) = X(f) = f$$

Reciproca: $C \in S_n$ an arestă descompunere $\Rightarrow \exists X \in S_n$

$$\text{dñ. } X \circ \sigma X^{-1} = C$$

$$\sigma = (\dots)$$

$$C = (a_1, a_2, \dots, c_{k_1}) (d_1, d_2, \dots, d_{k_2}) \dots$$

$$\text{Aleg } X_2 = \left(\begin{array}{c} a_1, a_2, \dots, a_{k_1} \\ b_1, b_2, \dots, b_{k_2}, \dots \end{array} \right)$$
$$\quad \quad \quad \left(\begin{array}{c} c_1, c_2, \dots, c_{k_1}, d_1, d_2, \dots, d_{k_2}, \dots \end{array} \right)$$

$$\text{Calculați } (X \circ \sigma X^{-1})(C_1) = X \circ (a_1) = X(a_1) = c_2$$

$$\sigma = \left(\begin{array}{c} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{array} \right) \Rightarrow C = \left(\begin{array}{c} 1 & 2 & 3 & 4 & 6 \\ 3 & 4 & 5 & 2 & 1 \end{array} \right) = (24)(135)$$

$$= (12)(3,4,5)$$

$$X_2 = \left(\begin{array}{c} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{array} \right)$$

$$X \circ \sigma X^{-1} = \left(\begin{array}{c} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{array} \right) \left(\begin{array}{c} 1 & 2 & 3 & 4 & 6 \\ 2 & 1 & 4 & 5 & 3 \end{array} \right) \left(\begin{array}{c} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{array} \right) =$$

$$= \left(\begin{array}{c} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{array} \right) \left(\begin{array}{c} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{array} \right) = \left(\begin{array}{c} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{array} \right)$$

Spre deosebire de $x, y \in G$, mult conjugate (\sim) \tilde{f}_G

$$g \in G^{-1} = g, (G, \cdot) \text{ grup}$$

Natura interesantă în cazul grupelor recombinate

$$C_x = \left\{ \begin{array}{l} g \in G \mid xg \in G^{-1} \\ g \in G \end{array} \right\} \text{ orbită lui } x$$

- multimea elementelor conjugate lui x

$$\text{obs. } C_x = C_y \text{ sau } C_x \cap C_y = \emptyset$$

$$\text{Pp că } C_x \cap C_y \neq \emptyset$$

$$g_1, g_2 \in G \text{ ac. } g_1 x g_1^{-1} = g_2 x g_2^{-1} \quad (2)$$

$$(2) \quad x = g_1^{-1} g_2 \cancel{x} g_2^{-1} g_1 = h y h^{-1}$$

$$(ab)^{-1} = b^{-1} a^{-1} \quad (g_1^{-1} g_2)^{-1} = g_2^{-1} g_1$$

$$x \in C_x \quad (2) \quad g_2 x g_2^{-1} \quad \tilde{f} = g_2 \cancel{h y h^{-1}} g_1^{-1}$$

$$(2) \quad y = (g_2 h) y (h^{-1} g_1^{-1}) \in C_y \quad C_x = C_y$$

$$t \in C_y \quad t = g_2 y g_2^{-1} = g_2 (h^{-1} x h) g_2^{-1} = g_2 h^{-1} \cancel{x} h g_2^{-1}$$

$$(2) \quad C_x = C_y$$

$\in C_x$
5/

Ecuatia claselor de conjugare

Dacă $x_1, x_2, \dots, x_n \in G$ ai $G = \bigcup_{i=1}^n Cx_i$.

Ințilbou

$x \in Gx_i$ (dintotdeauna)

când $|Cx| = 1$ (z), $Cx = f(x)$

$$fxg^{-1} = x \quad (\text{z}) \quad g^{-1}gx = xg + g_0$$

Dacă $Z(G)$ - centrul grupului

$$Z(G) = \{x \mid \forall y \in G \quad xy = yx\}$$

- toate elementele grupului care comută cu toate

$$\exists x \quad Z(G) \trianglelefteq G$$

$$\text{Rică } y \in Z(G) \quad y \in xZ(G)x^{-1} \quad (\text{z})$$

$$\Leftrightarrow y \in xZ(G)x^{-1} \subseteq Z$$

$$|G| = |Z(G)| + \sum_{|Cx_i|=1} |Cx_i|$$

$$G_x = \{g \in G \mid gxg^{-1} = x\}$$

$$|Cx| = \frac{|G|}{|G_x|}$$

$$Ex: G_x \leq G$$

5/

$$(G, \cdot) = (\mathbb{S}_{n+1}^0)$$

$$|S_4| = 12! \quad 4! = 24$$

$$\tau(S_4) = ? = \{ e \}$$

$$1 - - -$$

$$\cancel{3!}$$

$$(4)$$

$$(3,1)$$

$$(2,2)$$

$$(2,1,1)$$

$$(1,1,1,1)$$

Câte cicluri de lungime 4 = 5!

$$|S_4| = 12! / (6 + 8 + 3 + 6) = 1$$

Câte cicluri de lungime 3 = 8

Câte cicluri de lungime 2

Pentru prim \$(\mathbb{Z}, \cdot)\$ grup \$(\mathbb{Z}) \in p^2 \Rightarrow G\$ comunitativ
 $(\mathbb{Z}, \cdot) \cong (\mathbb{Z}_{p^2})$

$$G \cong \mathbb{Z}_p \times \mathbb{Z}_p$$

$$|G| = \sum_{X \in \mathcal{P}(G)} \frac{|G|}{|GX|} = p^2$$

$$G \text{ comunitativ} \Rightarrow \tau(G) = |G|$$

$$\tau(\mathbb{Z}) \leq G \quad |\tau(G)| \leq p^{2k} \quad \tau(\mathbb{Z}) \in \{1, p, p^2\}$$

$$6/$$

$$\frac{|G|}{(6x_i)} \geq \frac{p^2}{|G_{X_i}|} e^{\{p\}p^2} \Rightarrow (x_i \in \{p, p^2\})$$

Orește grup în elemente ciclice
 $A \leq (\mathbb{Z}_p, +)$

$$z(G) \mid_{2p} \Rightarrow z(G) = \{b^i \mid i \in \overline{0, p-1}\} \text{ ord } b = p$$

$$z(G) \leq 6$$

$$\left| \frac{6}{z(G)} \right| \geq \frac{|G|}{|z(G)|} = \frac{p^2}{p} = p \Rightarrow \frac{6}{z(G)} \leq (2p, +)$$

$$\Rightarrow \exists b \in G \text{ s.t. } \frac{6}{z(G)} = b^i \mid i \in \overline{0, p-1}$$

$$\forall x, X \in G \quad \bar{x} \in \frac{6}{z(G)} \Rightarrow \bar{x} = b^i \Rightarrow x = b^i u$$

$$\bar{y} \in \frac{6}{z(G)} \Rightarrow \bar{y} = b^j \Rightarrow y = b^j u$$

$$xy = b^i u b^j u = b^{i+j} u^2$$

Teorema lui Cauchy (G, \circ) grup finit, p prim $p \mid |G| \Rightarrow$

$\exists g \in G$, $u \in \text{ord } g = p$

ff

Cea de-a doua

profil NU SIMTE ROSTUL ceea ce acela

⇒ Algebra universală

⇒ "universal" (nu va fi de seamă)

A multime

 $(A, f_1, f_2, \dots, f_k)$

convenție:

 $(n_1 \geq n_2 \geq \dots \geq n_k \geq 0)$

semnificația algebraică

 $f_j : A^{n_j} \rightarrow A, n_j \in \mathbb{N}$ $(A^n = A \times A \times \dots \times A)$ $(x \in A^n = A \times A \times \dots \times A)$ $x = (a_1, a_2, \dots, a_n)$ $f_j = operația n_j-ată$ $n_j = 1 \Rightarrow f = operație unică$ $n_j = 2 \Rightarrow f = operație binară$ $n_j = 0, A = \emptyset$ Operație 0-ată: $f : \emptyset \rightarrow A$ $f(\emptyset) \in A$

⇒ algebras a univ. din t

Convenție de lucru înainte:

- monoid (A, f_1, f_2) $n_1 = 2$ $f_1 : A^2 \rightarrow A$ operație⇒ $f_1(f_1(x, y), z) = f_1(x, f_1(y, z))$ $f_1(\emptyset) = x$, elem.

Pentru analogii se numește legă ecuațională

- (G, \cdot) grup $(G, f_1, f_2, f_3, \cdot)$ $m_1 = 2, m_2 = 1, m_3 = 0$

$$f_2: G \rightarrow G$$

$$f_2(g) = g^t \quad (\text{functie care asociază fiecărui element } g \text{ din } G \text{ său})$$

$$f_3(\emptyset) = e$$

$$(x) f_1(f_1(x, y), z) = f_1(x, f_1(y, z)), \forall x, y, z \in G$$

$$(y) f_1(f_1(y, g), f_2(g)) = f_1(f_2(g), f_2(g)) = g$$

$$(z) f_1(e, g) = f_1(g, e) = g, \forall g \in G$$

- R înst

$$(R, f_1, f_2, f_3, f_4, f_5)$$

$$\begin{array}{cccccc} & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ f_1 & 2 & 1 & 0 & 0 & 0 \end{array}$$

$$f_2(\emptyset) = 0$$

$$f_3(\emptyset) = 1$$

+

$$1) f_1(x, f_1(y, z)) = f_1(f_1(x, y), z), \forall x, y, z \in R$$

associativitatea față de I - a operări

$$2) f_2(x, f_2(y, z)) = f_2(f_2(x, y), z), \forall x, y, z \in R$$

associativitatea celei de-a II - a operări

$$3) f_1(f_1(x, f_3(z))) = f_1(f_3(f_1(x)), z) = 0$$

$$4) f_1(0, 0) = f_1(0, 1) = 0$$

$$5) f_2(0, 1) = f_2(1, 0) = 0$$

$$6) f_2(x, f_1(y, z)) = f_2(f_2(x, y), f_2(x, z))$$

$(A, f_1, f_2, \dots, f_n)$

$B \subseteq A$

Subalgebra universală

$f_j : a_i, b_1, \dots, b_j \in B$

$\forall a_1, \dots, b_j \in B$

nu stiu de ce ar par

~~Subasta asta~~

(A, f_1, \dots, f_n)

$\downarrow n$

$(B, g_1, g_2, \dots, g_m)$

$\downarrow m$

$h : A \rightarrow B$ morfism de algebre

$$h(f_j(a_1, \dots, a_n)) = g_j(h(a_1), \dots, h(a_n)) \quad j = 1, \dots, n$$

Principiile de inexistență

Kurt Gödel: — există afirmații indecibile

• Greșeală în rezultat a matematicienilor din cîteva

D)

Multimi.

Funcții.

Convenție: ~~sunt~~

George Pólya - Comisian una apără de la litere

A, B multimi

$|A| = |B| \Leftrightarrow \exists f : A \rightarrow B$ bijectivă

ex: $\{0, 1\} = \mathbb{R}$

Exemplu: $(-\frac{\pi}{2}, \frac{\pi}{2}) \rightarrow \mathbb{R}$

$f(x) = \lg(x)$ bijección

$$(0, 1) \xrightarrow{f} (-\frac{\pi}{2}, \frac{\pi}{2})$$

$$g(x) = ax + b$$

$$g(0) = -\frac{\pi}{2}$$

$$g(1) = \frac{\pi}{2}$$

o

$$x: 0 \rightarrow 1: -\frac{\pi}{2}$$

$$g(0) = -\frac{\pi}{2}$$

$$g(1) = a - \frac{\pi}{2} = \frac{\pi}{2} \Rightarrow a = \pi \Rightarrow g(x) = \pi x - \frac{\pi}{2}$$

A multime

Def: A infinita dc $\exists A, \subsetneq A$ pot fi si,

bijecțivă

Hotelul lui Hilbert.

0, 1, 2, 3, ...

$$|Z| = |N|$$

$$f(x) = \begin{cases} 2^x & x \in N \\ -2^{x-1} & \begin{cases} x \in Z \\ x \neq 0 \end{cases} \end{cases}$$

$$|N \times N| = |N|$$

$$f: N \times N \rightarrow N$$

$$f(x, y) = \underline{\underline{\frac{(x+y+1)}{2}}} + x$$

$$|N| < |\mathbb{R}| = (0, 1)$$

Definim că $|A| < |B|$ d.e. $\exists f: A \rightarrow B$, f inj.

$\times \forall g: A \rightarrow B$ inj.

$$f: N \rightarrow R$$

$$f(x) \neq x \text{ inj.}$$

Este suficient să există o f bijecție

$\exists f$ bijecție

$$f: N^* \rightarrow (0, 1) \quad (|N| = |N^*|)$$

$$f(1) = 0, a_1, a_{12}, a_{123}, \dots$$

$$f(2) = 0, a_2, a_{23}, a_{234}, \dots$$

$$f(n) = 0, a_n, a_{n1}, a_{n2}, \dots$$

Bz. diagonalizare lui Cantor:

$$x \in (0, 1)$$

$$x = a_1, a_2, a_3$$

$$\text{d.e. } f(\{a_1, a_2, a_3\}) \Rightarrow x \notin f$$

$$a_4, a_5, a_6$$

:

$x \notin f(n) \forall n \in N^* \Rightarrow f$ nu e surjectivă

$\exists A$ a. z. $|N| < |A| \leq |\mathbb{R}|$?

Răsonare: imposibilă

✓ 4 probleme

Algebra #13

2 standard 1 media 1 grea

➤ Multimi. Functii. Cardinalul unei multimi

➤ Inductie

Daca $n \in \mathbb{N}$, $n \geq 3$ se arata ca $\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_n} = 1$ unde $a_1 < a_2 < \dots < a_n$
 $a_j \in \mathbb{N}^*$

$$\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_n} = 1 \quad \forall n \in \mathbb{N}$$

1) Verificarea $n=3$

$$\frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} = 1$$

~~"~~ ~~/6~~ $a_1 = 2 < 3 < 6$
 ~~2, 4, 5~~

2) Pasul de inductie

$$\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_n} = 1 \quad , \quad a_1 < a_2 < \dots < a_m$$

$$\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_m} \left(\frac{1}{2} + \frac{1}{3} + \frac{1}{6} \right) = 1 \quad (2)$$

$$(2) \quad \underbrace{\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_{m-1}}}_{\leq m-1} + \frac{1}{2am} + \frac{1}{3am} + \frac{1}{6am} = 1$$

$a_{m-1} < 2am < 3am < 6am$

11

$P(n) \Rightarrow P(n+2)$, $\forall n \in \mathbb{N}$

Verificare pt $n=4$

$$\frac{1}{2} + \frac{1}{2} = 1 \quad \text{(P)} \quad \frac{1}{2} \left(\frac{1}{2} + \frac{1}{3} + \frac{1}{6} \right) + \frac{1}{2} \quad ?$$

$$\text{(P)} \quad \frac{1}{2} + \frac{1}{3} + \frac{1}{6} + \frac{1}{12} = 1$$

$P(3)$ aderast

$P(4)$ aderast

$P(n) \Rightarrow P(n+2)$ aderast

> Struktur $\begin{cases} \text{Monoid} \\ \text{Grup} \end{cases}$

$f: G \rightarrow G$

- operatiunea
- element neutru
- inversul unui element (calcul)

$M = \{ \text{elemente} \mid k \in \mathbb{N} \}$

(M, \cdot) $\xrightarrow{\text{compatibil cu operatiunea}}$ monoid

$$(\mathbb{R}, *) \quad x * y = xy + x + y = xy + x + y + 1 + 1 - 1$$

$$= x(y+1) + y + 1 - 1 = (x+1)(y+1) - 1$$

$$\begin{aligned} & \stackrel{x=0}{(x+1)(y+1)-1=0 \Leftrightarrow} x \neq \overline{\frac{1}{y+1}} - 1 \\ & y \in \mathbb{R} \setminus \{-1\} \end{aligned}$$

$\Rightarrow (\mathbb{R}, *)$ monoid

Gruppen

$$1) (\mathbb{Z}_m, +) \quad m \in \mathbb{N}^*$$

$$U(\mathbb{Z}_m) = \{ \bar{a} \mid a \in \mathbb{Z}, (a, m) = 1 \}$$

2) (\mathbb{Z}_m, \cdot)
 $\downarrow = q_m$ - fund. achar

$$3) (\mathbb{F}_m, \circ)$$

$$4) (G_1, \cdot), (G_2, *)$$

$$((G_1 \times G_2), \perp) \quad (a_1, b_1) \perp (a_2, b_2) \Leftrightarrow (a_1, b_2) \perp (a_2, b_1)$$

grup

$$(U(\mathbb{Z}_{37}), \cdot)$$

$$\begin{aligned} & \overline{11}x = \overline{1} \quad | \cdot (-4)_{(2)} \quad -\overline{4}x = \overline{1} \quad \overline{30}x = \overline{33}x \\ & \overline{33}x = \overline{3} \end{aligned}$$

Cu algoritmul lui Euclid

$$\frac{111}{111} \text{ in } (\mathbb{U}(2014), +)$$

$$\begin{array}{r} 2014 \\ 111 \\ \hline 888 \\ 111 \\ \hline 18 \\ 111 \\ \hline 18 \\ 18 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 111 \mid 19 \\ 16 \mid 5 \\ 16 \\ \hline 5 \\ 16 \\ \hline 0 \end{array}$$

$$2014 = 111 \cdot 18 + 19$$

$$111 = 5 \cdot 19 + 16$$

$$19 = 1 \cdot 16 + 3$$

$$16 = 5 \cdot 3 + 1$$

$$3 = 3 \cdot 1 + 0$$

Se observă că exceptă ultimul

$$18 + \frac{1}{5 + \frac{1}{1 + \frac{1}{5}}} = 18 + \frac{1}{5 + \frac{1}{\frac{18+1}{18}}} = 18 + \frac{1}{5 + \frac{1}{\frac{19}{18}}} = 18 + \frac{1}{5 + \frac{1}{\frac{19}{35}}} = 18 + \frac{1}{5 + \frac{35}{63}} = \frac{636}{35}$$

$$\frac{2014}{111} = \frac{636}{35} = \frac{(-1)}{111 \cdot 35} \stackrel{\text{mărește cu }}{\rightarrow} \frac{-1}{111 \cdot 35} \quad (2)$$

$$(1) \quad 2014 - 636 \cdot 111 = -1$$

$$\text{Trecem în } 2014 \quad \frac{2014 - 636 \cdot 111}{111 \cdot 636} = \frac{-1}{111 \cdot 636} = \frac{-1}{63636} = \frac{1}{-63636}$$

Teoreme - Teorema lui Euler

$$(a, n) = 1, \quad n \in \mathbb{N}^*, \quad a \in \mathbb{Z} \Rightarrow n \mid (a^{\varphi(n)} - 1)$$

- Mică Teoremă a lui Fermat

$$p \text{ prim}, \quad a \in \mathbb{Z}, \quad p \nmid a, \quad p \mid a^{p-1} - 1$$

- Th lui Wilson

$$p \text{ prim} \Rightarrow p \mid ((p-1)! + 1)$$

$$35! = 36 \cdot 35 \cdots 2 \cdot 1 = (-1)(-2) \cdot 18 \cdot (2 \cdot 1) =$$

// lără centru, orbită, clase conjugate

Subgrup normal. Grup factor

- Th lui Lagrange $\lvert \frac{G}{H} \rvert = e$

dacă (G, \cdot) grup, $H \leq G$ (\Rightarrow)
 $\lvert H \rvert \mid \lvert G \rvert$

Ordenul unui element (măsoară)

Ex: $2^{16} + 1$ nr prim

$$1) g^{\text{ord } g} = 1$$

$$2) \underset{m \in \mathbb{Z}}{g^m = 0} \Rightarrow \text{ord } g | m$$

$$3) \text{ord}(g) \mid |G|$$

$$4) \text{ord } g^k = \frac{\text{ord } g}{(\text{ord } g, k)}$$

$$5) \text{ord}(g_1 g_2) = \text{lcm}(\text{ord } g_1, \text{ord } g_2)$$

Given two prime numbers p, q prime

$$\frac{pq}{\cancel{p} \cancel{q}} \mid p^k (5^p - 2^p) (5^q - 2^q)$$

$$(\text{as } p \mid (5^p - 2^p) \quad q \mid b)$$

$$q \mid (5^q - 2^q)$$

8/

fundamentala

Teorema de clasificare a grupurilor $(G_1, \cdot), (G_2, \cdot)$

Exemplu de subgrup normal trivial în S_m

$$\rho_{g, \alpha} : S_m \rightarrow \{ \pm 1 \}$$

$G_1 = (S_m, \cdot), G_2 = \{ \pm 1 \}, \alpha$

$\text{sgn}(\sigma) = -1 \quad \Rightarrow \text{injektivă}$

fiecare ar trebui

$$A_m = \{ \sigma \in S_m \mid \text{sgn}(\sigma) = 1 \} \subset \text{ker } \rho$$

$$|A_m| = \frac{|S_m|}{|\{ \pm 1 \}|} = \frac{m!}{2}$$

Problema generală

$$G \leq (Sp, \cdot)$$

strangele grupuri cu cicluri de lungime pătrată, $G = Sp$

$$(1, 2, \dots, p) \in G$$

$$(1, a) \in G, \sigma \in G \Rightarrow \sigma^{ta^{-1}} \in G$$

Exercițiu

$\prod_{m \in N} (p, m)^n = 1 \Rightarrow \sigma^M = \text{ciclu de lungime pătrată}$

ciclul lui

Să arătăm că o lăție ciclă este produs de transpozitii

77