13.10.2017

Curs 2

Definiție G mulțime, $\circ$ operație pe G, G s.n. grup dacă

1) $x\circ(y\circ z)=(x\circ y)\circ z$, $\forall\, x,y,z\in G$
2) $\exists\, e\in G$ a.î. $x\circ e=e\circ x=x$
3) $\forall\, g\in G \Rightarrow \exists\, g_1\in G$ a.î. $g\circ g_1=g_1\circ g=e$ (g_1 unic)

Def: $(G,\circ)$ grup

G s.n. comutativ dacă $x\circ y=y\circ x$, $\forall\, x,y\in G$

SCOPUL CURSULUI **Teorema (Lagrange)** $(G,\circ)$ grup finit, $g\in G$ (cu elem. neutru e)

$\Rightarrow g^{|G|}=e$

$|G|$ = cardinalul mulțimii G

Notație: $g^m \overset{not}{=} \underbrace{g\circ g\circ \dots \circ g}_{\text{de } m \text{ ori}}$

Obs: dem în cazul în care G este comutativ

Lemă: f funcție $f:A\to B$, A,B mulțimi finite $|A|=|B|$

Sunt echivalente: 1) f bij
2) f inj
3) f surj

Dem: $1\Rightarrow 2$ evidentă

$\downarrow$ $\quad 2\Rightarrow 3$

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

$a_i\neq a_j$ pt $i\neq j$

$\{f(1),f(2),\dots,f(m)\}\subseteq B$ $\Rightarrow$ (m elemente) $\Rightarrow (\forall)\, a\in B \Rightarrow \exists\, a_i\in A$ a.î. $f(a_i)=$

$=$ mulțime de

3 => 1

(i suficient să arăt că f inj)

Presupunem că f nu este inj.

$\Rightarrow (\exists)\ i \neq j$ a.î. $f(a_i) = f(a_j) \Rightarrow |\{f(a_1), f(a_2), \dots, f(a_m)\}| \leq m-1$

$1 \leq i \leq m$

Dem surj lui f rezultă că $\{\underbrace{f(a_1), \dots, f(a_m)}_{B(m \text{ elem})}\}$ contradicție

ex: $\mathbb{N}$ cardinal A și B au același cardinal, inf.

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

$f(n) = n+1$

f. inj

f + surj (0 nu este cuprins)

A - mulțime

A este infinită dacă există $(\exists) f: A \to A$, f inj care nu e surj

Obs: $(G, \circ)$ grup, $g \circ g_1 = g \circ g_2 \Rightarrow g_1 = g_2$

Dem: $\exists h$ a.î. $h \circ g = g \circ h = e$

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

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

Dacă G comutativ $g_1 \circ g = g \circ g_2 \Rightarrow g_1 = g_2$ atât cu stânga

Dem Lagrange (G comutativ)

$G = \{g_1, g_2, g \cdots, g_n\}$ $|G| = n$ $g \in G$ $g^m = e$

$f: G \to G$

$f(h) = h \circ g$

→ Arat că f inj ($f(h_1) = f(h_2) \Rightarrow h_1 = h_2$)

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

G finită, f inj $\overset{\text{Lema}}{\Rightarrow}$ f bij

$\{f(g_1), f(g_2) \cdots, f(g_n)\} = \{g_1, g_2, \cdots, g_n\}$

G com $\Rightarrow$ $f(g_1) \circ f(g_2) \circ \cdots \circ f(g_n) = g_1 \circ g_2 \circ \cdots \circ g_n$

$(g_1 \circ g) \circ (g_2 \circ g) \circ \cdots \circ (g_n \circ g) = g_1 \circ g_2 \circ \cdots \circ g_n$

comutativitate

$(g_1 \circ g_2 \circ \cdots \circ g_n) \circ g^n = g_1 \circ g_2 \circ \cdots \circ g_n$ În grup putem simplifica

$g^n = e$

Obs 2017^{2017}, ultimele 2 cifre : ??

Examen

Def: o operație pe mulțimea M

$(M, \circ)$ se numește monoid dacă:

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

2) $\exists e \in M$ a.î. $e \circ x = x \circ e = x$, $\forall x \in M$

(el. s. neutru)

e - unic

Exemplu:

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

↓ monoid l. $((x \circ y) \circ z) = x \circ (y \circ z)$

asoc. $(x \cdot y + x + y) \circ z = a \cdot z + a + z$

unde $a = x \cdot y + x + y$

$= (xy + x + y) \cdot z + xy + x + y + z = xyz + xz + yz + xy + x + y + z$

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

unde $b = yz + y + z$

$= xyz + xy + xz + x + yz + y + z$

2. e

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

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

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

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

3. este și comutativ

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

Cine sunt elementele inversabile?

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

$x \circ y = 0 = xy + x + y \mid +1$

$1 = xy + x + y + 1 = (x+1)(y+1)$

$\Leftrightarrow x + 1 = y + 1 = 1$ sau $x + 1 = y + 1 = -1$

$x = 0$ $x = -2$

Reluăm - inv -

$G = \{ \bar{a} \mid a \in \{0, 1, \dots, 99\} \}$

$(a, 100) = 1 \}$

↓ cel mai mare div. comun

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

$\bar{a} = \bar{b} \overset{def}{\Leftrightarrow} 100 \mid a - b$

$\bar{a} \cdot \bar{b} \overset{def}{=} \overline{a \cdot b}$ (Ex op $\cdot$ e bine def)

$\left.\begin{matrix} \bar{a} = \bar{a}_1 \\ \bar{b} = \bar{b}_1 \end{matrix}\right\} \overset{?}{\Rightarrow} \bar{a} \cdot \bar{b} = \bar{a}_1 \cdot \bar{b}_1$

Alt exercițiu

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

① $m \circ m_1 = m \circ m_2 \Rightarrow m_1 = m_2$

Atunci $(M, \circ)$ grup.

$g \in M$

$l: M \to M$

$l(m) = g \circ m$

$l(m_1) = l(m_2)$

$g \circ m_1 = g \circ m_2 \overset{①}{\Rightarrow} m_1 = m_2$ deci $\left\{\begin{matrix} l. \text{ inj} \\ M \text{ finită} \end{matrix}\right. \overset{\text{Lemă}}{\Rightarrow} l.$ surj

$\left.\begin{matrix} g \in M \\ l \text{ surj} \end{matrix}\right\} \Rightarrow \exists g_1 \in M$ a. î. $l(g_1) = e$

$(N^*, \cdot)$ → monoid

1 - ②

$(G, \cdot)$ monoid

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

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

$|G| = 40$

$(G, \cdot)$ are prop. de simplificare

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

$m, m_1, m_2 \in \{0, 1, \ldots, 99\}$

$(m, 100) = (m_1, 100) = (m_2, 100)$

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

$100 \mid m(m_1 - m_2)$

$(m, 100) = 1$

$\Rightarrow 100 \mid m_1 - m_2$

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

$\Rightarrow m_1 = m_2$

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

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

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

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

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

$\bar{17}^4 = \bar{121} = \bar{21}$

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

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

$\bar{17}^{17} = \bar{81} \cdot 17 = \bar{77}$ (ult. 2 cifre) 2017^{2017}

La curs 9: modulul ~~set~~ claselor de resturi

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

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

$a_i \neq a_j \pmod{n}$ pt $i \neq j$

$2^{29} = \overline{a_9 a_8 a_7 \ldots a_1}$

Cifra bipară

$\bar{a} = \bar{k} \overset{\text{def}}{\iff} n \mid a - k$

$\bar{2}^6 = \bar{6}^4 = \hat{1}$

$2^{-29} = (\bar{2}^{-6})^4 \cdot \bar{2}^5 = \bar{32} = \bar{5}$

$= \overline{0+1+2+\ldots+9+0+\ldots+2}$

$n = 4$

$2^{29} = 536870912$