Este rog? NU DE Inel

25.10.2022

Curs 4.

Monoizi, grupuri

Def. $(M,\cdot)$ monoid $\begin{cases} \text{"}\cdot\text{" asociativă} \\ (\exists)\ e_M = e_M \cdot x = x, \forall x \in M \end{cases}$

Exemple $(\mathbb{N},+) \subseteq (\mathbb{Z},+) \subseteq (\mathbb{Q},+) \subseteq (\mathbb{R},+) \subseteq (\mathbb{C},+)$

Def. Element inversabil $x \in M$ a.î. $(\exists)\ x' \in M$ a.î. $x \cdot x' = x' \cdot x = e_M$

↳ monoid

OBS. Dc. $(\exists)\ x'$, inversul lui x atunci acesta este unic!

Dem. P.p. $(\exists)\ x''$ invers pt. x

$$x' = e_M \cdot x' = (x'' \cdot x) \cdot x' = x'' \cdot (x \cdot x') = x'' \cdot e_M = x''$$

Exemple

$(\mathbb{N},\cdot)\subseteq(\mathbb{Z},\cdot)\subseteq(\mathbb{Q},\cdot)\subseteq(\mathbb{R},\cdot)\subseteq(\mathbb{C},\cdot)$

NOTAȚIE

$\underbrace{U(M)}_{\text{monoid}}=\{x\in M \mid (\exists)\, x' \text{ a.î. } x\cdot x'=x'\cdot x=e_M\}$

PROP U(M) este parte stabilă rel. "·"

Dem. Fie $x,y\in U(M)$. Vrem să arătăm că $x\cdot y\in U(M)$

Arătăm că $y'x'$ este inversul lui xy

$(xy)(y'x')=x\cdot y\cdot y'\cdot x'=x(y\cdot y')x'$
$=x\cdot e_M\cdot x'=x\cdot x'=e_M$

Temă: $(y'x')(xy)=\ldots=e_M$

Am dem. $\forall\, x,y\in U(M)\to x\cdot y\in U(M)$

Similar $yx\in U(M)$
(inversul este $x'y'$). Deci U(M) este parte stabilă față de M

$(M,\cdot)$ grup — monoid
$(\forall)x\in M$, x este inversabil

$\Updownarrow$

$M=U(M)$

$H\subseteq M$, unde M este grup
s.n. subgr. de H (este parte stabilă față de "·"
$e_M\in H$
$\forall x\in H$, x inv. $\Rightarrow x'\in H$

$(1,\cdot)\subset(\mathbb{N},\cdot)$

$\underbrace{(\{\pm1\},\cdot)}_{\text{subgrup}}\subset(\mathbb{Z},\cdot)$

PROP. Dc. $x_1, \dots, x_n \in U(M)$ at. $x_1, \dots, x_n \in U(M)$ și inversul este $x_n' x_{n-1}' \dots x_2' x_1'$ unde x_i' este inv. lui x_i $\forall i = \overline{1,n}$

NOTAȚIE Ptc. $x \in U(M)$ $x^{-1} = x'$ - inv lui x

$x^{-n} = (x^{-1})^n$

PROP. Fie $(M, \cdot)$ monoid. Atunci: ⓪ $a^0 = 1_M$

① $(a^m)^n = a^{mn}$ $(\forall) a \in M, m, n \in \mathbb{N}$
(dc. $a \in U(M)$, $(\forall) m, n \in \mathbb{Z}$)

② $a^m \cdot a^n = a^{m+n}$ $\forall a \in M, m, n \in \mathbb{N}$

Exemplu

Fie $A \neq \emptyset$

$(\mathcal{P}(A), \cup)$ monoid

$\cup$ "asociativă"

$e_{\mathcal{P}(A)} = \emptyset$

$A \neq \emptyset$

$(\mathcal{P}(A), \cap)$

$\cap$ "asociativă"

$e = A$

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

$a, \cancel{b} \in \hat{r}$ $\quad 0 \le r \le n-1$

$\in \mathbb{Z}$ $\Leftrightarrow$ $a = nq + r, q \in \mathbb{Z}$ $n \in \mathbb{N}, n \ge 2$

$(\mathbb{Z}_n, \hat{+})$

$\hat{a} + \hat{b} \stackrel{def}{=} \widehat{a+b}$

Exemple. Reprezentanți pentru clase de echivalență

$\sim$ pe A

↳ echivalența $(\forall)\, x \in [a]$ este reprezentant pentru $[a]$

Considerăm $\mathbb{Z}_3 = \{\hat{0}, \hat{1}, \hat{2}\}$

Reprezentanți pentru $\hat{0} = 3, 0, 3, 6, 9, \ldots$

Repr. pentru $\hat{1}$: $-2, 1, 4, 7, 10, \ldots$

OBS Def. "+" nu depinde de repr.

Fie a', b' repr. pentru $\hat{a}, \hat{b} \Leftrightarrow \hat{a} = \hat{a'}$

$\Leftrightarrow n \mid (a' - a)$

$n \mid (b' - b)$

$a' = np + r$ $\qquad$ Vrem $\hat{a'} + \hat{b'} = \widehat{a' + b'}$

$a = nq + r$ $\qquad = \widehat{a + b} = \hat{a} + \hat{b}$

$b = nk + s$

$b' = nl + s$

$a - a' = nq - np = n(q - p)$
$b - b' = nk - nl = n(k - l)$ $\Rightarrow a - a' + b - b' = n(q - p) + n(k - l)$

$\Rightarrow a - a' + b - b' = 0$

$\Rightarrow a + b = a' + b' + n[\underbrace{q - p + k - l}_{\in \mathbb{Z}}]$

$\Leftrightarrow \widehat{a + b} = \widehat{a' + b'}$

$(\mathbb{Z}_n, +)$ grup

$(\forall)\, \hat{a} \in \mathbb{Z}_n\, (\exists)$ "$-\hat{a}$" $\in \mathbb{Z}_n$ a.î.

$\hat{a} + (-\hat{a}) = \hat{0}$

Exemplu $(\mathbb{Z}_3, +)$ grup abelian

+	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{0}$	$\hat{1}$

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

$(\mathbb{Z}_n, \cdot)$; $\hat{a} \cdot \hat{b} \overset{def}{=} \widehat{ab}$

Operație bine definită

Fie $a' \in \hat{a}$ $(\hat{a'} = \hat{a})$

$b' \in \hat{b}$ $(\hat{b'} = \hat{b})$

Dem. că $\hat{a'} \cdot \hat{b'} = \widehat{ab} = \hat{a} \cdot \hat{b}$

$a'b' = (a + nk)(b + nl)$

$= ab + n\underbrace{(al + bk + nkl)}_{\in \mathbb{Z}}$

$\widehat{a'b'} = \widehat{ab}$

$(\mathbb{Z}_4, \cdot)$ monoid comutativ

$\cdot$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{2}$	$\hat{0}$	$\hat{2}$	$\hat{0}$	$\hat{2}$
$\hat{3}$	$\hat{0}$	$\hat{3}$	$\hat{2}$	$\hat{1}$

$\hat{a} \cdot \hat{b} = \hat{b} \cdot \hat{a}$

$U((\mathbb{Z}_4, \cdot)) = \{\hat{1}, \hat{3}\}$

$U(M) \subsetneq M$

$(\mathbb{Z}_3, \cdot)$

$\cdot$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{2}$	$\hat{0}$	$\hat{2}$	$\hat{1}$

$U(\mathbb{Z}_3) = \{\hat{1}, \hat{2}\}$

În general

<u>Teoremă</u> Fie $n \in \mathbb{N}$, $n \geq 2$. Atunci $(U(\mathbb{Z}_n), \cdot)$ este subgr. în $(\mathbb{Z}_n, \cdot)$ (monoid) $U(\mathbb{Z}_n)$

$= \{\hat{x} \in \mathbb{Z}_n \mid (x, n) = 1\}$

Dc $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_s^{e_s}$ cu $p_1, \dots, p_s$ nr. prime dist.

$e_i \geq 1$; $|U(\mathbb{Z}_n)| = \varphi(n)$ indicatorul lui Euler

nr. numerelor $1 \leq x \leq n$ coprime cu n

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_s}\right)$$

$\varphi(4) = 2$

$\varphi(6) = 2 = 6\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)$

$12 = 2^2 \cdot 3$

$\varphi(12) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$

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

<u>Temă</u> Tabla " $\cdot$ " pt. $(U(\mathbb{Z}_6), \cdot)$

$\cdot$	$\hat{1}$	$\hat{5}$
$\hat{1}$	$\hat{1}$	$\hat{5}$
$\hat{5}$	$\hat{5}$	$\hat{1}$

<u>Morfisme</u>

Fie $(M_1, \circ)$, $(M_2, *)$ monoizi

Se numește morfism de monoizi o funcție $f: M_1 \to M_2$ a.î. $\begin{cases} f(e_{M_1}) = f(e_{M_2}) \\ f(x \circ y) = f(x) * f(y) \\ \forall x, y \in M_1 \end{cases}$

<u>Def</u>: Un morfism s.n. izomorfism dacă este funcție bijectivă

izomorfism $\begin{cases} \text{— bijectivă} \\ \text{— morfism} \end{cases}$

Considerăm : $(\{\hat{0}, \hat{1}, \hat{3}, \hat{4}\}, \cdot) \leq (\mathbb{Z}_6, \cdot)$

$\cdot$	$\hat{1}$	$\hat{3}$	$\hat{4}$	$\hat{0}$
$\hat{1}$	$\hat{1}$	$\hat{3}$	$\hat{4}$	$\hat{0}$
$\hat{3}$	$\hat{3}$	$\hat{3}$	$\hat{0}$	$\hat{0}$
$\hat{4}$	$\hat{4}$	$\hat{0}$	$\hat{4}$	$\hat{0}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$

$\big\downarrow$ f morfism

$(\mathcal{P}(\{1,2\}), \cup) \xrightarrow{g} (\mathcal{P}(\{1,2\}), \cap)$

Considerăm $A = \{1, 2\}$ $\quad (\mathcal{P}(A), \cup)$

$\hat{1} \to \emptyset \quad \hat{3} \to 1 \quad \hat{4} \to 2 \quad \hat{0} \to 12$

$\cup$	$\emptyset$	1	2	12
$\emptyset$	$\emptyset$	1	2	12
1	1	1	12	12
2	2	12	2	12
12	12	12	12	12

$(\mathcal{P}(A), \cap)$

$\cap$	12	2	1	$\emptyset$
12	12	2	1	$\emptyset$
2	2	2	$\emptyset$	$\emptyset$
1	1	$\emptyset$	1	$\emptyset$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$

OBS: Pt. orice mulțime X $(\mathcal{P}(X), \cup) \underset{\text{izomorfe}}{\simeq} (\mathcal{P}(X), \cap)$

$g : \mathcal{P}(X) \to \mathcal{P}(X)$

$g(Y) = X \setminus Y = \overline{Y}$

$g^{-1}(Y) = X \setminus Y$

$g(Y \cup Z) = \overline{Y \cup Z} \underset{\text{de Morgan}}{=} \overline{Y} \cap \overline{Z} = g(Y) \cap g(Z)$

PROP. Fie A, B, C monoizi

1) $A \xrightarrow{f} B \xrightarrow{g} C$, f, g morfisme atunci $g \circ f$ morfism

2) Dc. $f : A \to B$ izomorfism $\Rightarrow f^{-1} : B \to A$ este izomorfism

Dem 1) Fie $x, y \in A$ $\quad (g \circ f)(x \cdot y)$
$= g(f(x \cdot y)) = g(f(x) f(y)) = g(x) f(y)$