Curs 5

3.11.2020

① Operații algebrice (legi de compoziție)

Def 1 Fie A mulțime nevidă. ① operație algebrică (lege de compoziție) "$*$" pe mulțimea A este o funcție $*: A \times A \longrightarrow A$.

Notație În loc de $*(a,b)$ vom scrie $a*b$.

Def 2 Fie $*$ o lege de compoziție pe mulțimea A. Atunci legea se numește:

1) asociativă dc $a*(b*c) = (a*b)*c$ $(\forall)\, a,b,c \in A$

2) comutativă dc $a*b = b*a$ $(\forall)\, a,b \in A$.

Legea "$*$" are element neutru $e \in A$ ("notat" cu e) dacă:

$$a*e = e*a = a \quad (\forall)\, a \in A$$

Obs 1) Dacă există, elementul neutru este unic (Dem e, f elem. neutre $e = e*f = f$)

Def 3 ① submulțime nevidă H a lui A s.n. parte stabilă a lui A (în raport cu $*$) dacă $x*y \in H$ $(\forall)\, x,y \in H$.

Def 4 Fie M o mulțime nevidă și "$*$" o lege de compoziție pe M. Atunci perechea $(M,*)$ s.n. monoid dacă $*$ este asociativă și are element neutru;

$(M,*)$ s.n. monoid comutativ dacă $(M,*)$ e monoid și "$*$" este comutativă.

Exemple: ① Fie "+" pe $\mathbb{N}$: "+" este asoc, com, are element neutru (0);
$(\mathbb{N},+)$ este monoid comutativ

② $(\mathbb{N},+)$ $(\mathbb{N},\cdot)$ $(\mathbb{Z},+)$ $(\mathbb{Z},\cdot)$ $(\mathbb{Q},+)$ $(\mathbb{Q},\cdot)$ $(\mathbb{R},+)$ $(\mathbb{R},\cdot)$, $(\mathbb{C},+)$, $(\mathbb{C},\cdot)$
sunt monoizi comutativi

③ Fie A o mulțime nevidă. $(\mathcal{P}(A),\cup)$; $(\mathcal{P}(A),\cap)$ → monoizi comutativi

④ Fie A o mulțime nevidă. $(\{f:A\to A \mid f \text{ funcție}\},\circ)$ este un monoid
(1_A este elementul neutru) compunerea funcțiilor

Def Fie $(M,*)$ un monoid cu elementul neutru e. Un element $a\in M$ s.n. element inversabil (sau simetrizabil) dacă există $a'\in M$ cu
$a*a'=a'*a=e$.

Elementul a' s.n. inversul lui a (sau simetricul lui a).

Obs 1) $(M,*)$ monoid; $a\in M$. Dc. a este inversabil atunci a' este unic.

(Dem Dc a', b sunt 2 "inversi" ai lui A atunci $a'=a'*e=a'*(a*b)=(a'*a)*b=e*b=b$)

Exemple Fie $M=(\{f:\mathbb{N}\to\mathbb{N}\mid f \text{ funcție}\},\circ)$ monoid (necomutativ).
1) Să se arate că $f:\mathbb{N}\to\mathbb{N}$ $f(n)=n+1$ (are "invers la stânga") nu este inversabil ca element al lui M.

· f e inj, nu e surj. $\Rightarrow$ f nu e inversabilă.

f e inj $\xRightarrow[\text{cursul}]{\text{vezi}}$ $(\exists)\ g: \mathbb{N} \to \mathbb{N}$ a.î. $g \circ f = 1_{\mathbb{N}}$.

$(g \circ f)(n) = n$ $(\forall)\ n \in \mathbb{N}$

$g(f(n)) = n$

$\overset{\shortparallel}{g(n+1)}$

Constr. $g: \mathbb{N} \to \mathbb{N}$ $\quad g(n) = \begin{cases} n-1 & , \text{dc } n \geq 1 \\ k & , \text{dc } n = 0 \end{cases}$,

unde $k \in \mathbb{N}$ poate fi ales arbitrar

2) Fie $k \geq 1$. și $f: \mathbb{N} \to \mathbb{N}$ $f(n) = \begin{cases} 0 & , n \in \{0, \ldots, k\} \\ n-k, & n > k \end{cases}$. Arătați că există o mulțime finită de funcții $g: \mathbb{N} \to \mathbb{N}$ a.î. $f \circ g = 1_{\mathbb{N}}$ și nu există nicio funcție $h: \mathbb{N} \to \mathbb{N}$ a.î. $h \circ f = 1_{\mathbb{N}}$. (Exc!)

Def Un monoid $(M, *)$ s.n. grup dacă $(\forall)\ a \in M$ este inversabil.

Notație $(M, *)$ monoid $\rightsquigarrow$ $U(M) \overset{\text{def}}{=}$ mult. elem. inversabile ale lui M în raport cu "$*$"

($e \to$ elem. neutru) $\left(\overset{\text{sau}}{U(M,*)}\right) = \{a \in M \mid (\exists)\ a' \in M \text{ a.î. } a * a' = a' * a = e\}$.

Obs monoidul $(M, *)$ s.n. grup $\Leftrightarrow$ $U(M) = M$.

Exemple 1) $U(\mathbb{N}, +) = \{0\}$, $U(\mathbb{N}, \cdot) = \{1\}$, $U(\mathbb{Z}, \cdot) = \{-1, 1\}$, $U(\mathbb{Q}, \cdot) = \mathbb{Q}^*$

2) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ $\to$ gr. com. ; $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$

3) $(M, *)$ - monoid $\longrightarrow$ $(U(M), *)$ $\to$ grup.

Notații Dacă $(M,*)$ monoid $\rightsquigarrow$ elem. neutru se notează cu e, elem. inv. al lui a se notează cu a'

$(M,+)$ monoid $\rightsquigarrow$ —"— 0, —"— $-a$

$(M,\cdot)$ monoid $\rightsquigarrow$ —"— 1, —"— a^{-1}.

De acum înainte voi folosi notația multiplicativă.

Reguli de calcul în monoid

① $(M,\cdot)$ monoid și $a_1,\dots,a_n\in M$ atunci valoarea produsului $a_1\cdot a_2\cdots a_n$ nu depinde de modul în care s-au pus parantezele. ($n=3$ $(a_1a_2)\cdot a_3=a_1(a_2a_3)$ $= a_1a_2a_3$)
(ind. după n)

② $(M,\cdot)$ monoid și $a_1,a_2,\dots,a_n\in U(M)$ atunci $a_1\cdot a_2\cdot\ldots\cdot a_n\in U(M)$ și

$$(a_1\cdot a_2\cdot\ldots\cdot a_n)^{-1}=a_n^{-1}\cdot a_{n-1}^{-1}\cdot\ldots\cdot a_2^{-1}a_1^{-1}.$$

(**Dem** arăt doar egalitatea $(a_1\cdot a_2\cdot\ldots\cdot a_n)\cdot(a_n^{-1}\cdot a_{n-1}^{-1}\cdot\ldots\cdot a_1^{-1})\overset{①}{=}(a_1\cdots a_{n-1})\cdot(\underbrace{a_na_n^{-1}}_{=1})\cdot$
$\cdot(a_{n-1}^{-1}\cdots a_1^{-1})=(a_1\cdots a_{n-1})\cdot(a_{n-1}^{-1}\cdots a_1^{-1})\overset{ind}{=}1.$)

③ $(M,\cdot)$ monoid și $a,b\in M$. Atunci:

$a^m\cdot a^n=a^{m+n}$; $(a^m)^n=a^{mn}$ $(\forall)\ m,n\geq 0$ (e valabil și pentru $(\forall)\ m,n\in\mathbb{Z}$ dacă a e inversabil)

$ab=ba \Rightarrow (ab)^n=a^nb^n$ $(\forall)\ n\geq 0$ (e valabil și pentru $(\forall)\ n\in\mathbb{Z}$ dacă a,b sunt inversabile)

$\mathbb{Z}_n = \{\hat{0}, \hat{1}, \dots, \widehat{n-1}\}$, $n \geq 2$, $n \in \mathbb{N}$. $\mathbb{Z}_n = \mathbb{Z}/_{\equiv \bmod n}$

Definim "+" pe $\mathbb{Z}_n$: $\hat{a} + \hat{b} \overset{def}{=} \widehat{a+b}$

"$\cdot$" pe $\mathbb{Z}_n$: $\hat{a} \cdot \hat{b} \overset{def}{=} \widehat{ab}$

Cele 2 operații sunt bine definite (nu depind de reprezentantul clasei). Vreau să arăt că $\widehat{a+b} = \widehat{a'+b'}$, $\widehat{ab} = \widehat{a'b'}$

Fie $a', b' \in \mathbb{Z}$ a.î. $\hat{a} = \hat{a'}$, $\hat{b} = \hat{b'}$.

$n \mid a - a'$ $\quad$ $n \mid b - b'$ $\Rightarrow n \mid (a-a') + (b-b') \Rightarrow n \mid (a+b) - (a'+b')$

$n \mid (a-a') \cdot (b'-b) \Rightarrow n \mid -ab + ab' - a'b' \dots$

$\Rightarrow a'b' - ab = \underbrace{(a'-a)b'} + \underbrace{a(b'-b)} \Rightarrow n \mid a'b' - ab. \Rightarrow \widehat{ab} = \widehat{a'b'}$.

Exc $(\mathbb{Z}_n, +) \to$ grup comutativ ($\hat{0} \to$ elem. neutru, inversul lui $\hat{k}$ este $\widehat{-k}$)

$(\mathbb{Z}_n, \cdot) \to$ monoid comutativ ($\hat{1} \to$ elem. neutru)

$U(\mathbb{Z}_n, \cdot) = \{\hat{k} \mid (\exists)\, \hat{l}$ a.î. $\hat{k} \cdot \hat{l} = \hat{1}\}$

$= \{\hat{k} \mid 1 \leq k \leq n$ și $(k, n) = 1\}$

$\hat{k} \cdot \hat{l} = \hat{1} \overset{def}{\Leftrightarrow} n \mid k \cdot l - 1 \Leftrightarrow k \cdot l - 1 = n \cdot a \Leftrightarrow k \cdot l - n \cdot a = 1 \boxed{\Leftrightarrow} (k, n) = 1$

$|U(\mathbb{Z}_n)| = \varphi(n) \leftarrow$ fct. indicatorul lui Euler.