

C6: monoidi (reguli de calcul fără un monoid)  
grupuri (def)

Exemplu

$\mathbb{Z}_m$

$\frac{m \geq 2}{m \in \mathbb{N}}$

$\mathbb{Z}_m^{\text{not}} = \mathbb{Z}_{\substack{\text{mod}(m)}}^{\text{not}}$

Definiția "+" pe  $\mathbb{Z}_m$ :

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

$$\hat{a} \cdot \hat{b} \stackrel{\text{def}}{=} \hat{ab}$$

"." pe  $\mathbb{Z}_m$ :

Care 2 operații sunt bine definite (nu depind de reprezentarea clasei)

Fie  $a, b \in \mathbb{Z}$  a.t.  $\hat{a} = a'$ ,  $\hat{b} = b'$

$$\begin{array}{c} \hat{a} = a' \\ \hat{b} = b' \\ \hline m | a - a' \\ m | b - b' \end{array}$$

$$\begin{array}{c} \hat{a+b} = \hat{a'} + \hat{b'} \\ \hat{ab} = \hat{a'} \hat{b'} \end{array}$$

$$\Rightarrow m | (a - a') + (b - b') \Rightarrow$$

$$\Rightarrow m | (a + b) - (a' + b') \Rightarrow a + b \equiv a' + b' \pmod{m} \Rightarrow \hat{a+b} = \hat{a'} + \hat{b'} \quad (1)$$

$$\begin{aligned} a'b' - ab &= (a' - a)b' + ab' - ab = (a' - a)b' + a(b' - b) = \\ &= (a' - a)b' - a(b - b') \\ m | a - a' &\Rightarrow m | a' - a \\ m | b - b' &\Rightarrow m | b' - b \end{aligned}$$

$$\begin{aligned} \Rightarrow m | (a' - a)b' - a(b - b') \\ \Rightarrow m | a'b' - ab \Rightarrow \hat{a'b'} = \hat{ab} \quad (2). \end{aligned}$$

$$\Rightarrow a'b' \equiv ab \pmod{m}$$

Exe  $(\mathbb{Z}_m, +) \rightarrow$  grup abelian (comutativ) ( $\hat{0} \rightarrow$  elem. neutru  
inversul lui  $\hat{k}$  este  $\hat{-k}$ )

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

$$U(\mathbb{Z}_m, \cdot) = \left\{ \hat{k} \mid (\exists) \hat{l} \text{ a.i. } \hat{k} \cdot \hat{l} = \hat{1} \right\}$$

$$\hat{k} \cdot \hat{l} = \hat{1} \stackrel{\text{def}}{=} m | k \cdot l - 1$$

$$(1) \quad U(\mathbb{Z}_m, \cdot) = \left\{ \hat{k} \mid 1 \leq k \leq m \text{ și } (k, m) = 1 \right\}$$

$$\Leftrightarrow k \cdot l - 1 = m \cdot a$$

$$\Leftrightarrow k \cdot l - m \cdot a = 1$$

$$\boxed{\Leftrightarrow} \quad (k, m) = 1$$

$$\Rightarrow \text{Fie } d = (k, m) \Rightarrow k = d \hat{k}' \quad (k', m) = 1$$

$$d \cdot (k \cdot l - m \cdot a) = 1 \Rightarrow d | 1 \Rightarrow d = 1 \Rightarrow \boxed{(k, m) = 1}$$

$$k \cdot l - m \cdot a = 1 \Rightarrow d \cdot (d \hat{k}' \cdot l - m \cdot a) = 1 \Rightarrow d | 1 \Rightarrow d = 1 \Rightarrow \boxed{(k, m) = 1}$$

" $\Leftarrow$ " Algoritm Euclid

Dc  $(k, m) = d$  Euclid

$d = k \cdot x + m \cdot y$  pt  $x, y \in \mathbb{Z}$

Exemplu  $(24, 40) = 8$

$$\begin{aligned} 40 &= 24 \cdot 1 + 16 \\ 24 &= 16 \cdot 1 + 8 \end{aligned}$$

$$\begin{aligned} \Rightarrow 16 &= 40 \cdot 1 - 24 \cdot 1 \\ \Rightarrow 8 &= 24 \cdot 1 - (40 \cdot 1 - 24 \cdot 1) = 24 \cdot 2 - 40 \cdot 1 \end{aligned}$$

$$16 = 8 \cdot 2 + 0$$

In general:  $(k, n) = d$

$$\begin{aligned} m &= k \cdot g_1 + r_1 \Rightarrow r_1 = m \cdot 1 - k \cdot g_1 \\ k &= r_1 \cdot g_2 + r_2 \Rightarrow r_2 = k - r_1 \cdot g_2 = \\ &\vdots \\ &= k - (m \cdot 1 - k \cdot g_1) \cdot g_2 \\ &= m \cdot g_2 + k \cdot (1 + g_1 \cdot g_2) \\ R_{t-3} &= r_{t-2} \cdot g_t + R_{t-1} \\ r_{t-1} &= r_t \cdot g_{t+1} + 0 \end{aligned}$$

$$(1) U(Z_{n_1}) = \left\{ \hat{k} \mid 1 \leq k \leq n_1 \text{ și } (k, n_1) = 1 \right\} \Rightarrow |U(Z_n)| = f(n)$$

fct. indică  
torul lui Euler

$$U(Z_{n_1}) = \left\{ \hat{k} \mid 1 \leq k \leq 4 \text{ și } (k, n_1) = 1 \right\} = \{1, 3\}$$

Def ① Fie  $(M_1, \cdot), (M_2, \cdot)$  2 monoizi. O funcție  $f: M_1 \rightarrow M_2$  s.m. morfism de monoizi dacă sunt îndeplinite simultan condițiile: ①  $f(x \cdot y) = f(x) \cdot f(y) \forall x, y \in M_1$ , ②  $f(1_{M_1}) = 1_{M_2}$ . Notație De acord cu  
înainte vom folosi pt monoizi op. multiplicativă

② Un morfism de monoizi bijectiv s.m. izomorfism de mozi.

Proprietățile morfismelor de monoizi

① Compozierea a 2 morfisme de monoizi este tot un morfism de monoizi.

② Inversul unui izomorfism de monoizi este tot un izomorfism.

③ Dacă  $f: M_1 \rightarrow M_2$  este un morfism de monoizi și  $a \in M_1$ , atunci

$$(i) f(a^n) = (f(a))^n \quad (\forall n \geq 1). \quad (\text{Ind după } n \text{ folosind } ① \text{ def. morf.})$$

(ii) Dc.  $a \in U(M_1) \Rightarrow f(a) \in U(M_2)$  și  $f(a^{-1}) = f(a)^{-1}$ ; în particular avem  $f(a^n) = (f(a))^n \quad (\forall n \in \mathbb{Z})$ .

Exemplu ①  $(M, \cdot)$  monoïd  $1_M: M \rightarrow M$  izom. de monoizi

② Să se arate că  $(P(B), \cup)$  și  $(P(B), \cap)$  sunt 2 monoizi izomorfi, cu el. neutru al lui  $(P(B), \cup)$  este  $\emptyset$   
 $f: (P(B), \cup) \rightarrow (P(B), \cap)$   $f(x) = L_B^x$   
 $\Rightarrow f(\emptyset) = L_B^\emptyset = B$   $\Rightarrow f$  satisfacă ②

① Fie  $x, y \in P(B)$  ( $\Rightarrow x, y \subseteq B$ )  
 $f(x \cup y) \stackrel{\text{def}}{=} L_B^{x \cup y} = L_B^x \cap L_B^y \stackrel{\text{def}}{=} f(x) \cap f(y)$   
 $\Rightarrow f$  satisfacă ①, prin urmare (din ① și ②)  $f$  e morfism de monoizi.

Exc Arătati că  $f$  e bijectie!  
③ Sunt monoizi  $(N, +)$  și  $(N^*, \cdot)$  izomorfi? NU  
Pp red. la abs. că  $\exists f: (N, +) \rightarrow (N^*, \cdot)$  un izomorfism de monoizi  
 $f(m) = f(\underbrace{1+1+\dots+1}_m) \stackrel{\text{Propri} \ ③}{=} f(1) \cdot f(1) \cdot \dots \cdot f(1) = f(1)^m$   
 $\Rightarrow \forall m \geq 1 \quad f(m) = f(1)^m$   
(f(1) \neq 1, altfel f nu ar fi bij.)  
Xo (exists prime p, p \neq f(1) \neq 1)  
f. Euclid (sunt nr-prime infinit)  
Pp e falsă

Grupuri. Morfisme de grupuri. Subgrupuri

- Exemple (grupuri):
- ①  $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$  grupuri abeliene
  - ②  $(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$  grupuri abeliene
  - ③  $(\mathbb{Z}_n, +) \rightarrow$  grup abelian m > 2
  - ④  $(S_m, \circ) \rightarrow$  grup m > 1  $S_m = \{f \mid f: \{1, \dots, m\} \rightarrow \{1, \dots, m\} \text{ f bij}\}$
  - ⑤  $m > 1, n \in \mathbb{N} \quad (U_n, \cdot) \rightarrow$  grup abelian  $U_n = \{z \in \mathbb{C} \mid z^m = 1\}$ .
  - ⑥  $(U, \cdot) \rightarrow$  grup abelian  $U = \{z \in \mathbb{C} \mid |z| = 1\}$

⑦ Def Fie  $(G_1, *) \subset (G_2, \cdot)$  2 grupuri. Definim produsul direct al celor 2 grupuri ca fiind:  $(G_1 \times G_2, \square)$

Def Fie  $(G_1)_i, (G_2)_i$  2 grupuri. O functie  $f: G_1 \rightarrow G_2$  s.m. morfism de grupuri daca  $f(x * y) = f(x) * f(y)$   $\forall x, y \in G_1$ . Un morfism de grupuri bijectiv s.m. numit izomorfism de grupuri.

Un morfism de grupuri bijectiv este un morfism de grupuri atunci  $f(1_{G_1}) = 1_{G_2}$ .

Obs ① Dc.  $f: G_1 \rightarrow G_2$  s.t.  $\forall g_1 \in G_1 \quad f(g_1) *_{G_2} f(g_1) = {}^1_{G_2}$

(Dem: Fie  $f(\iota_{G_1}) = a$ )

$\iota_{G_1} \circ \iota_{G_1} = \iota_{G_1}$

$f(\iota_{G_1} * \iota_{G_1}) = f(\iota_{G_1}) \Rightarrow a = a^2$

$\Downarrow$

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

$a \cdot \bar{a} = a \cdot (a \cdot \bar{a})^{G_2 \rightarrow G_1}$

$\iota_{G_2} = a \cdot \iota_{G_2} = a \Rightarrow$

$\Rightarrow f(\iota_{G_1}) = \iota_{G_2}.$

D. morphisme de monoizi au loc  
l'ord

⇒  $f(\theta_1) = \theta_2$  ,  
 ② Propz. ① → ③ de la morfisme de monoizi au xz  
 si pentru morfismele de grupuri (clar un morfism de gr.)  
 e morfism de monoizi  
 $\theta(zt) = (zt)^{-1} f(z)f(t)$

Exemplu ① Fie  $f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$  și  $g: (\mathbb{R}^*, \cdot) \rightarrow (\mathbb{R}^*, \cdot)$  unde  $f(x) = x$  și  $g(x) = e^x$ . Arăta că  $f$  și  $g$  sunt izomorfii de grupuri.

② Fie  $g: (R, +) \rightarrow (R_+, \circ)$  și  $x \cdot y = g(x) \cdot g(y) \Rightarrow g$  surjectiv;  $g$  bij.

③ Este  $h: (\mathbb{Z}_{21}^+) \rightarrow (\mathbb{Z}_{41}^+)$  un morfism de grupuri? E

$h(\hat{0}) = \bar{0}$  incorrect

$h$  non e bina definita

$\hat{1} = \hat{3}$   $h(\hat{1}) = \bar{1}$   $\bar{1} \neq \bar{3}$  in  $\mathbb{Z}_4 \Rightarrow$

~~$h(\hat{3}) = \bar{3}$~~   $h(\hat{3}) = h(\hat{1}) = \bar{1}$

$h$  e bine definită!  
 $h$  nu e morfism  
de grupuri

Dacă  
 $h$   
e  
morfism

$$h(\bar{1} + \bar{1}) = h(\bar{0}) = \bar{0}$$

$$\text{II}$$

$$h(\bar{1}) + h(\bar{1}) = \bar{1} + \bar{1} = \bar{2} \neq \bar{0} \text{ în } \mathbb{Z}_4$$

$\Rightarrow h$  nu e morfism de gr.

$$\Rightarrow h \text{ nu e morfism de gr.} \quad f(\bar{0}) = \bar{0} \text{ și } f(\bar{1}) = \bar{2}$$

(4) Să se arate că  $f: (\mathbb{Z}_{2,1}^+) \rightarrow (\mathbb{Z}_{4,1}^+)$  este un morfism de grupuri. (Exc!)