

Exemplu:

- 1 teorie

- 1 problemă

• Ex: un demonstrație (fără teoreme)

• Notă: Soluții

• Total: - Reputat 70%.

- scăzut de temă (probleme din sesiunea viitoare) 10%.

- lauare (meniu) 10%.

- activitate la reuniune 20% (fără prezentă)

• Reputat: parte teoretică (definiții și exemple) + practică.

- partea 3 - nu face o problemă / program. + Monografie

• Ex: 1. Operații cu mulțimi

2. Relații Binare

3. Relații de echivalență

4. Relații funcționale

5. Funcții injecțive

6. Funcții surjective

7. Funcții surjective și aplicații

8. Monotone, etc.

9. Subgrupuri unei grupă de ordin  $\leq 20 \cdot 6$

10. Elemente fixe de ordin  $\leq 8$

11. Relații de echivalență modulo un subgrup.

12. Subgrupuri normale. Aplicații

13. Teoria fund. de izomorfism la grupuri. Aplicații

14. Teorema de structură a grupurilor finite. Aplicații

15. Teorema lui La-Grange

16. Teorema lui Coset. Aplicații

17. Ordinalul unui element întreacă grup. Aplicații

78. Teorema de supradominanță lui Lagrange a grup. de reprezentări

79. Galoisel. Aplicații

80. Ideal. Aplicații

81. Morfisme de inele

82. Teorema fundamentală de izomorfism la inele. Aplicații.

83. Teorema chineză a resturilor

84. Caracteristice unui corp. Aplicații

85. Corpuri finite

86. Inele de puteri. Supradominanță

87.  $\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}$

$$\phi(a) = \frac{a^3}{7}$$


88. Polinoame monice (coefficient dominant 1)

$$m = a_0 + a_1 x + \dots + a_n x^n, \quad a_n - \text{coefficient dominant.}$$

89. Divizibilitatea polinoomelor

90. Rădăcini ale polinoomelor ( $\mathbb{Q}[x]$ )

91. Rădăcini ale polinoomelor ( $\mathbb{R}[x]$ ), Rădăcini.

92. Teorema fund. a algebrei.

93. Polinoame ireductibile

Teoremele și rezolvările: Teoreme ale teoriei.

Exemple subiect examen:

i) a) Definiții și clasificare multimi de subgrup al unui grup.

Def: Fie  $(G, \cdot)$  un grup și  $H \subseteq G$  subgrup,  $H = \emptyset$ .  
 $(H \subseteq G)$

$H \subseteq G$  dacă 1.  $(\forall)x, y \in H \Rightarrow x \cdot y \in H$

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

Ex:  $G : \mathbb{S}_7$ ,  $G \subseteq G$

b) Enunțat teoremei lui Lagrange la grup.

- Bibliografie: - De platformă: Demitrescu Algebra 7.

- Algebra carte

- Probleme de Algebra Racine, Minus, ... (4 autori)

## 7. Elemente de teorie a mulțimilor

### 1. Multimi

$x, A, B \dots$  (multimi)  $a \in x, a \notin x$

$a, b, c \dots$  (elemente)

Mulțimi formate dintr-un element — „singleton”

$\{x\}$  singletonul definit de  $x$ .

$\{x, y\}$  parțialordonat (dubletul)

$(x, y) = \{x\}, \{x, y\}$  permutația ordonată

$(x, y, z) \neq ((x, y), z)$

N-seturi

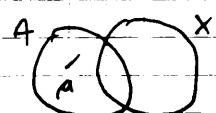
$X = \{x \mid x \text{ are proprietate } n\}$

•  $A, B \subseteq X, ACX \Rightarrow (A) \subseteq A \Rightarrow a \in X$ .

$A \not\subseteq X$

•  $A \not\subseteq X \Rightarrow (\exists) a \in A, a \notin X$

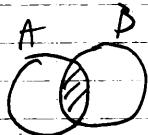
$A = B \Rightarrow A \subseteq B \text{ și } B \subseteq A$ .



$A \cup B = \{x \in X \mid x \in A \text{ sau } x \in B\}$

$A \cap B = \{x \in X \mid x \in A \text{ și } x \in B\}$

$A \setminus B = \{x \in X \mid x \in A \text{ și } x \notin B\}$

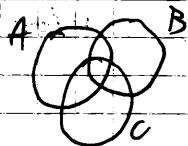


•  $X$  multimi finite.

$A, B$  multimi finite

• Dimensiunea inclusării de subordine:

$$A, B, C \subset X \quad |A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C|$$



$$\bullet \emptyset_X = \{x \in X \mid x \neq x\}$$

Zie  $X$  o mulțime și  $\emptyset_X$  nu este vidă și nici  $X$ .

- Atunci: a)  $\emptyset_X$  nu conține nici un element. (i)
- b) Dă oare  $Y$  (mult.) :  $\emptyset_X \subset Y$  (ii)
- c) Dă oare mult  $Y$ ,  $\emptyset_X = \emptyset_Y$  (iii)

Denumire

- i) Dñ. nu (i)  $x_0 \in \emptyset_X \Rightarrow x_0 \in X$ , nu  $x_0 \in \emptyset_X \Leftrightarrow x_0 \neq x_0$ , contradicție.
- ii) Dñ. nu există  $Y : \emptyset_X \not\subset Y \Rightarrow (\exists) x_0 \in \emptyset_X \text{ și } x_0 \notin Y$ , contradicție.  
(\*)  $Y : \emptyset_X \subset Y$
- iii) Fără răsonare ii) (\*)  $Y : (\emptyset_X \subset \emptyset_Y) \Rightarrow \emptyset_X = \emptyset_Y = \emptyset$ .  $\emptyset = \{x \mid x \neq x\}$   
 $\emptyset_Y \subset \emptyset_X$

$$A \cup \emptyset = A$$

$$A \cap \emptyset = \emptyset$$

$$P(X) = \{A \mid A \subset X\} \text{ mulțimea partilor lui } X$$

$$|X| = n, \quad |P(X)| = 2^n.$$

$$X = \{1, 2, 3\}, \quad P(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

$$X = \emptyset, \quad P(X) = \{\emptyset\}, \quad P(P(\emptyset)) = P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}.$$

Ex) Datei exemple de 3 mulțimi  $X, Y, Z$ , a.t.  $x \in Y \in Z$  și  $x \in Y \subset Z$ .

$$X = \emptyset, \quad Y = \{\emptyset\}, \quad Z = \{\emptyset, \{\emptyset\}\}$$

$$\text{Ex)} P(A) \cap P(B) = P(A \cap B)$$

$A, B \subset X$ .

$$P(A) \cup P(B) \subset P(A \cup B)$$

$$X = \{1, 2, 3, 4\}$$

$$A = \{1, 2, 3\}$$

$$\{3, 4\} \notin P(A) \cup P(B)$$

$$B = \{1, 2, 4\}$$

$$A \cup B = X$$

---

$$A \subset X, X \setminus A = C_A = {}_x^C A \quad (\text{komplement des } A \text{ im rapport zu } X)$$

$$(A = \{x \mid x \in X, x \notin A\}).$$

$$A, B \subset X$$

$$\begin{aligned} C(A \cup B) &= (A \cap C_B) \\ C(A \cap B) &= (A \cup C_B) \end{aligned} \quad \text{Legile der De Morgan'sche Regel}$$

---

$$\text{Ex)} \text{ Zil } A = \{1, 2, \dots, 2015\}$$

Echte subset. BC A,  $\{1, 2\} \subset B$ ?

$$R: 2^{2^{2017}}$$

---

$$B \subset A, \{1, 2\} \subset B, |B| = 5.$$

$$|A| = m, m \geq 2.$$

$$A_1 \subset A, |A_1| = 2, C_X^2 = \frac{x(x-1)}{2}.$$

$$A_1 = K$$

---

$$A = \{3, 4\}$$

$$|A| = 2^{2017}.$$

---

$$B = \{1, 2, 4, 6, 12\}$$

---

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

produced cartesian

---

$$A \times B \times C = (A \times B) \times C$$

---

$$A \times B \times C = \{$$

Dacă  $x=y$ , atunci  $x=x$

O astă se aplică lejeră pe mult.  $X$ .

$\cap \subset X \times Y$

Dacă  $n = \{(x \in X, y \in Y)$ ,

(-ordine)

atunci  $n = \{(y \in Y \mid (\exists) x \in X, x \cap y\})$

$n^{-1} = \{(x, y) \mid (x, y) \in R\}$

Ex:  $X = \{1, 2, 3, 4\}$

$n = \{(1, 1), (1, 2), (2, 3), (2, 4)\}$

## 7. Elemente și operații a mulțimilor

### 1.1. Mulțimi

$\{x\}$  - singulare și def. de  $x$

$(x, y)$  - perechea neordonată def de  $x \neq y$

$(x, y) : \{x\}, \{x, y\}$  pereche ordonată

$(x, y, z) = ((x, y), z)$

$X_m \quad X = \{x \mid x \text{ are prop. } n\}$

$A, B \subset X, A \subset X$

$A = B \Leftrightarrow A \subset B \text{ și } B \subset A$

$A \cup B = \{x \mid x \in A \text{ sau } x \in B\}$

$A \cap B = \{x \mid x \in A \text{ și } x \in B\}$

$A \setminus B = \{x \mid x \in A \text{ și } x \notin B\}$

$! (A \setminus B) \cup (B \setminus A) = A \Delta B$

$|A \cup B| = |A| + |B| - |A \cap B|$  (principiul incluziunii)

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

$X, \emptyset_X = \{x \in X \mid x \neq x\}$

[T] Fie  $X = \{a\}$  mult. și  $\emptyset_X =$  punctul vidă al lui  $X$

Asterni : i)  $\emptyset_X$  nu conține niciun element

ii) ( $\forall$ )  $y \in \text{mult}_Y$ ,  $\emptyset_X \subset Y$

iii) ( $\forall$ )  $Y = \text{mult}_Y$ ,  $\emptyset_X = \emptyset_Y = \emptyset$

Demonstratie :

i) Pentru ( $\exists$ )  $x_0 \in \emptyset_X \Leftrightarrow x_0 \in X$ ,  $x_0 + x_0 \Rightarrow 0 \neq 0 \Rightarrow$  contrad.

$\Rightarrow$  conclusie

ii) St. că ( $\exists$ )  $y \in \text{mult}_Y \Rightarrow (\exists) x_0 \in \emptyset_X, x_0 \neq y$  contr. cu ii)

$\Rightarrow (\forall) y, \emptyset_X \subset Y$

iii) dоказ. ii)  $(\forall) y, \emptyset_X \subset \emptyset_Y \Rightarrow \emptyset_X = \emptyset_Y = \emptyset$ ;  $\emptyset \subset \{x | x \neq x\}$   
 $\emptyset_Y \subset \emptyset_X$

$$A \cup \emptyset = A; A \cap \emptyset = \emptyset$$

$$X = \text{mult}_X$$

$$P(X) = \{A | A \subset X\} - \text{mult multilor lui } X$$

$$|X| = n \in N \Rightarrow |P(X)| = 2^n$$

$$\text{Ex: } X = \emptyset \Rightarrow P(X) = \{\emptyset\}; P(\{\emptyset\}) = P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$$

Ex: Date 3 mult. de mult,  $X, Y, Z$  s.t.  $x \in Y \in Z$  și  $x \in Y \in Z$

$$x = \emptyset, y = \{\emptyset\}, z = \{\emptyset, \{\emptyset\}\}$$

$$A, B \subset X; P(A) \cap P(B) = P(A \cap B)$$

$$P(A) \cup P(B) \subset P(A \cup B)$$

$$A \subset X, X \setminus A = CA = C_X A - \text{comp. lui } A \text{ în rap. cu } X$$

$$AB \subset X; C(A \cup B) = CA \cap CB$$

$$C(A \cap B) = CA \cup CB$$

legile lui de Morgan

Ex: Fie  $A = \{1, 2, \dots, 2019\}$ . Este subm.  $B \subset A$ ,  $\{1, 2\} \subset B$ ? R:  $2^{2017}$ .

$$A \times B = \{(a, b) | a \in A \text{ și } b \in B\}$$

$$A \times B \times C = \{(a, b, c) | a \in A \text{ și } b \in B \text{ și } c \in C\}$$

$x, y \neq \emptyset$ ;  $n \subset X \times Y$  relație binară de la  $X$  la  $Y$ .

$$n = \{(x, y) \in X \times Y | x \in y\}; (x, y) \in n \Leftrightarrow x \in y.$$

Dacă  $X = Y$ ,  $n \subset X \times X$ ;  $n$  = rel. binară pe mult.  $X$ .

$n \subset X \times Y$ : Dom.  $n = \{(x \in X, y \in Y) \text{ s.t. } xny\}$

Ran.  $n = \{y \in Y \mid \exists x \in X \text{ s.t. } xny\}$

$n^{-1} = \{(y, x) \mid (x, y) \in n\}$

Ex:  $X = \{1, 2, 3, 4\}$ ,  $n \subset X \times X$ ,  $n = \{(1, 1); (1, 2); (2, 3); (2, 4); (3, 4)\}$ .

07.10.2019

Date  $X, Y$  și relație.

$n \subset X \times Y$ ,  $n = \{(x, y) \in X \times Y \mid x \in X, y \in Y\}$

Dom.  $n = \{x \in X \mid \exists y \in Y \text{ s.t. } xny\}$

$\boxed{(x, y) \in n \Leftrightarrow xny}$

Ran.  $n = \{y \in Y \mid \exists x \in X \text{ s.t. } xny\}$ ,  $n^{-1} = \{(y, x) \in Y \times X \mid xny\}$

$n \subset X \times Y$ ,  $n \subset Y \times Z$ :  $n \circ n \subset X \times Z$  !  $x = y$ ;  $n \subset X \times X$   
 $\text{rel. binară}$

$n \circ n = \{(x, z) \in X \times Z \mid \exists y \in Y \text{ s.t. } xny \text{ și } nyz\}$

[Ex.] Fie  $X = \{1, 2, 3, 4\}$  și  $n = \{(1, 2); (2, 1); (2, 3); (3, 4)\}$ ,  $n \circ n = \{(1, 4); (3, 4); (2, 1)\}$

Def: Dom.  $n$ , Dom.  $n$ , Ran.  $n$ ;  $n^{-1}$ ,  $n^2$  și  $n \circ n$  (Prop.).

$n \subset X \times X$  ✓

(1)  $n$  reflexivă:  $x \in X$ ,  $(x, x) \in n$ ;  $((x, x) \in n, (y, y) \in n)$

(2)  $n$  simetrică:  $xny \Rightarrow ynx$ .  $((x, y) \in n, (y, x) \in n)$

(3)  $n$  transițivă:  $xny, ynz \Rightarrow xnz$ .  $((x, y) \in n, (y, z) \in n \Rightarrow (x, z) \in n)$

$n$  rel.  $n$  este reflexivă, simetrică și transițivă. rel. de echivalență

• Fie  $n \subset X \times X$  rel. de echivalență.  $x_0 \in X$ .

$\hat{x}_0 \stackrel{\text{def}}{=} \{x \in X \mid (x, x_0) \in n\}$  clasa de echivalență a elementului  $x_0$  reportată la rel.  $n$ .

$\hat{x}_0 \stackrel{\text{def}}{=} \{x \in X \mid x_0 \in X\}$  mult factor (nu mult. nat) a lui  $X$  în rap. cu  $n$ .

Ex<sub>2</sub>) Dacă  $\gamma_1$  și  $\gamma_2$  sunt două relații de echivalență pe mulțimea  $X$ , arătați că  $\gamma_1 \cap \gamma_2$  este o relație de echivalență pe  $X$ .

Ex<sub>3</sub>)  $x = \{1, 2, 3\}$  — Exemplu Ex<sub>2</sub>.

$$\gamma_1 = \{(3, 1); (2, 2); (3, 3)\}, (1, 2), (2, 1) \quad (1, 3) \notin \gamma_1 \cup \gamma_2.$$

$$\gamma_2 = \{(1, 1); (2, 2); (3, 3)\}, (2, 3), (3, 2).$$

$$\gamma_1 \cup \gamma_2 = \{(1, 1); (2, 2); (3, 3); (1, 2); (2, 1); (2, 3); (3, 2)\}.$$

$\forall x \in \text{dom } \gamma_1: (x, x) \in \gamma_1 \cup \gamma_2$ $(x, x) \in \gamma_1 \cup \gamma_2$ $(x, x) \notin \gamma_1 \cup \gamma_2.$	$(1, 2), (3, 3) \in \gamma_1 \cup \gamma_2$ $(1, 3) \notin \gamma_1 \cup \gamma_2.$
---	--

$\rightarrow \gamma_1 \cup \gamma_2$  nu este o relație de echivalență.

$$a, b \in \mathbb{Z}, m \geq 2, n \in \mathbb{N}^*$$

$$a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b)$$

$$|x|_n \Leftrightarrow (\exists k \in \mathbb{Z}) : n \mid x \cdot k.$$

$$m = n: a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b)$$

$$m = 0: a \equiv b \pmod{0} \Leftrightarrow 0 \mid (a - b) \Leftrightarrow a = b.$$

$$(-n):$$

Ex<sub>2</sub>):  $\equiv$  este o relație de echivalență.

$$\mathcal{R} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{m}\}.$$

$\mathbb{Z}_m = \mathbb{Z}/m = \{0, 1, \dots, m-1\}$  mulțimea restelor de resturi mod  $m$ .

$$\mathbb{Z}_m + \mathbb{Z}_m = \mathbb{Z}_m \quad (\mathbb{Z}_m, +, \cdot) \text{ este un grup comutativ.}$$

$$\mathbb{Z}_m \cdot \mathbb{Z}_m = \mathbb{Z}_m$$

$$10: \mathbb{Z}_4, \mathbb{Z}_4 = \{0, 1, 2, 3\}.$$

$$\downarrow \mathbb{Z}_4 = \{4k + 2 \mid k \in \mathbb{Z}\} = \text{mulțimea } \mathbb{Z}_4.$$

$$\mathbb{Z} = \{\dots, -6, -2, 2, 6, \dots\}.$$

$$m = 7 \text{, } 17 = 90, 7, 8, 3, 9, 3, 7).$$

$$L \supseteq \{z | k+2) | k \in \mathbb{Z}\}.$$

(P) mult. unitate:  $U(z_m) = \{x e^{z_m^*} + (y) \} e^{z_m^*} \text{ cu } \bar{n}. x - y = 2\}$

$(\begin{smallmatrix} 2 & * \\ 3 & \end{smallmatrix}, \cdot)$  monoid rapport.

$(U(z_m), \cdot)$  grass. mount.

$$\text{Für } x \in U(z) \Rightarrow (\exists) \gamma \in \mathbb{Z}^+ = x \gamma = z \Leftrightarrow x \gamma = 3 \Rightarrow |(x \gamma - z)| <$$

$$x \equiv y \pmod{m} \Leftrightarrow m \mid (x-y) \Leftrightarrow x = y$$

$$\Leftrightarrow \exists k \in \mathbb{Z} : x_3 - 1 = nk \quad (\Rightarrow x_3 + n(-k) = 1. \quad \Leftrightarrow (x_3, n) = 1.$$

$$d = (a_1, b_1) \Rightarrow (\exists) \alpha, \gamma : d = a\alpha + b\gamma$$

$$U(z_k) = \{x \in \mathbb{R}_+^n \mid (x, n) = \gamma\}.$$

$$U(7_8) = \{7, 8, 3, 7\}$$

$$z_m^* - \text{min}_{\mathbb{R}^n} V(z) \Rightarrow z \text{ ist m. Min.}$$

(2)  $\vec{z}_2, \vec{z}_3, \vec{z}_5, \vec{z}_7$  converge.

$$|U(z_m)| = |\{x \mid z \leq x < z_m, (x_{\infty})=z\}| = \varphi(m)$$

→ r. de ale

↓  
fit für Fehler.

Ex) 두 번째 예제. 예.  $3x^2 - 4x + 7 = 0$  를 푸시고  $\boxed{397}$ .

$$Z_6 = \{0, 1, 2, 3, 4, 5\}$$

Kunnskap,  $ax^2 + bx + c = 0$ ,  $a \neq 0$

$$\Delta = b^2 - 4ac = m^2, \text{ нек.}$$

$$x_{1,2} = \frac{(-b \pm \sqrt{\Delta})}{2a}$$

$$3x^2 + 4x - 7 = 0 \text{ en } \mathbb{R}$$

$$D = (-4)^2 - 4 \cdot 3 \cdot 7 \Rightarrow D = 16 - 84 \Rightarrow D = -68.$$

$$x_{1,2} = \frac{-b \pm \sqrt{\Delta}}{2a} = \begin{cases} x_1 = 1 \\ x_2 = 3 \end{cases}$$

Tarea: Ex en  $\mathbb{Z}_{17}$ .

$$\cap \subset X \times X$$

$\cap$  e antisimétrico daco  $x \cap y \text{ si } y \cap x \Rightarrow x = y$ .

rel. de ordenare: reflexivo și transițivă.

" $\leq$ "

$\cap$  reflex. și trans. renum. relatii de ordonare, daco în mult. este și  
antisimetrică rel. de ordine.

$$\leq, x \leq y \text{ și } x < y : x \leq y \text{ și } x \neq y.$$

$(X, \leq)$  mult. ordonat,  $\cap$ . de ordine  $\Rightarrow \cap$ . de ordonare

$$N, x \mid y \Leftrightarrow \exists z \in N : y = xz.$$

$$(n) x \mid x, (\forall) x \in N. \quad (\text{ex!})$$

$$(\text{as}) x \mid y \text{ și } y \mid z \Rightarrow x \mid z$$

$$(\text{if}) x \mid y, y \mid z \Rightarrow x \mid z.$$

$$P \models \vdash ; 2 \mid (-2), -2 \mid 2 \ni \text{dos } 2 + -2$$

$(\mathbb{Z}, \mid)$  e o mult. ordon. dos nu e o mult. ordonata.

• Ești. mult. ordonata  $(X, \leq)$ .

Daco  $x \leq y$  sau  $y \leq x$ , ( $\forall x, y \in X$ , mult. " $\leq$ " este total ordonata).

$(X, \leq)$  e o mult. total. ordonata.

-  $x_0 \in X$  re num. prim element (element initial al mult.) daco

$$x_0 \leq x, (\forall) x \in X$$

-  $x_0 \in X$  - n- ultimul el (el. final al mult.) daco  $x_0 \geq x, (\forall) x \in X$ .

$(X; S)$ , ( $\forall$ )  $A \subset X$ ,  $A = \emptyset$  există un un element  $x_0$  în  $A$ .

! Obs! Cazul binde ordonată este dublu de cauza trivii.

(mat. it. Peano)  $N$  def, rel. și construcție.

Def: Mat. m. nat este un triplet  $(0, N, S)$  c. n. sunt verificate axiomele Peano:

axiome Peano:  $(P_1) 0 \in N$ .

$(P_2) S: N \rightarrow N^*$  este o fct injectivă.

(Prop. de inducție matematică  $\rightarrow$ )  $(P_3)$  Dacă  $P \subset N$  a. n. i)  $0 \in P$

(inductie)

ii') ( $\forall$ )  $n \in N \Rightarrow S(n) \in P$  at  $P = N$

• Dacă  $n$ , "element initial"

•  $S: N \rightarrow N^*$ ,  $S(n) = n'$  reprezintă fct numărător

$0=1; 1=2; 2=3; \dots$

$S(n) = n^*$  — orice a menținut numărător.

$(P_3)$  principiu de inducție matematică, nu este inducție

Ex) Răspunsul astăzi? Fie Peano unde e?

$(P_1) N \subset \mathbb{Z}$ ,  $n, i \in N$

( $\neq$ )

ii) ( $\forall$ )  $n \in N \Rightarrow S(n) \in N$ .

Def. Regula de comp:  $\varphi: N \times N \rightarrow N$ ,  $\varphi(n, m) = n + m$  a. j.

$(A_1) n + 0 = n$ , ( $\forall$ )  $n \in N$ .

$(A_2) n + m' = (n + m)'$ , ( $\forall$ )  $n, m \in N$ .

$n + (m + 1) = (n + m) + 1$

Ex)  $2+2$  este  $2+1+1 = 2+1 = 3$ .

$2+2 = 2+1+1 = (2+1) + 1 = [2+0] + 1 = ((2+0) + 1) + 1 = 2 + 1 + 1 = 3 = 4$ .

$P_n : N \times N \rightarrow N$ ,  $P_n(z_1, z_2) = z_1 \cdot z_2$  p.r. I<sub>1</sub>:  $z \cdot 0 = 0$ ,  $\forall n \in N$ .

I<sub>2</sub>:  $n \cdot n = n^2$   $\forall n \in N$ .

$$I_3 : z \cdot (m+n) = (z \cdot m) + z$$

$a, b \in N$ ,  $a \leq b \stackrel{d}{\Rightarrow} (\exists) c \in N$  s.t.  $a+c=b$ .

$b \geq a \Leftrightarrow a < b \Leftrightarrow a \leq b \wedge \nexists c \neq 0$

$(N, \leq)$  e bină-ordonată și total-ordonată

C: Nu există siruri strict divergente de nr. naturale.

(concretă bină-ordonare - Fermat a elaborat-o).

$x^4 + y^4 = z^4 \Rightarrow x^4 + y^4 = z^4$  nu are soluții non-nule (Fermat)

(metoda reductio ad absurdum)

Marea Teoremă a lui Fermat: Ex.  $x^n + y^n = z^n$  nu are soluții non-nule întregi

$n \geq 3$  (Euler)

1794 Andrew Wiles - Carlo Ramanujan / Marea Teoremă - m.

18.10.2019

• Relații funcționale

$X = \emptyset$ ,  $Y = \emptyset$

$f \subset X \times Y$  o nr. rel. funcț. dacă  $(\forall)(x \in \text{Dom } f, (f') \ni y \in \text{ran } x) \wedge y \in f(x)$

$\text{Dom } f = \{(x \in X | (f') \ni y \in Y \wedge x \in f(y))\}$

• Dacă am plus  $\text{Dom } f = X$ , atunci  $f$  este o funcție

$x \in f, \text{not } y = f(x)$ .

Obs:  $f$  funcț.  $\Rightarrow f$ . nr. funcț.

$\Leftarrow$

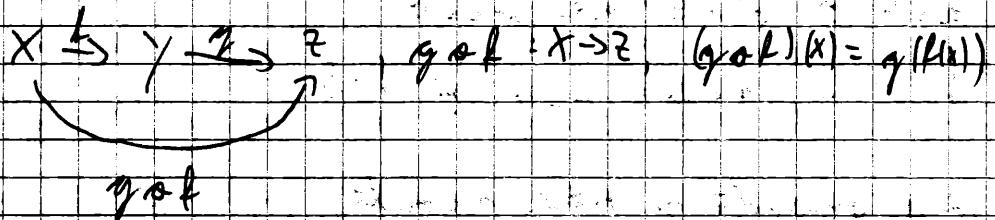
Ex:  $X = \{1, 2, 3\}$ ,  $f \subset X \times X$ ,  $f = \{(1, 1), (2, 3)\}$  nr. funcț.

$\text{Dom } f = \{1, 2\} \subsetneq X$  nu  $f$  este o funcț.

$f: X \rightarrow Y$ ,  $F(X, Y) = Y^X = \{f | f: X \rightarrow Y\}$  (Funktionen)

$A \subset X$ ,  $A \neq \emptyset$ ,  $f_A: A \rightarrow Y$ ,  $f_A(x) = f(x)$ ,  $\forall x \in A$ , Verknüpfung einer Funktion mit einer Menge

Ex:  $\Delta_X: X \rightarrow X$ ,  $\Delta_X \stackrel{\text{def}}{=} \gamma_X$ ,  $\gamma_X(x) = x$ ,  $\forall x \in X$ , ist die Identität



① •  $f: X \rightarrow Y$  injektiv:  $\forall x_1, x_2 \in X$ ,  $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$  (2)  $x_1 \neq x_2 \Rightarrow$

•  $f(x_1) \neq f(x_2)$

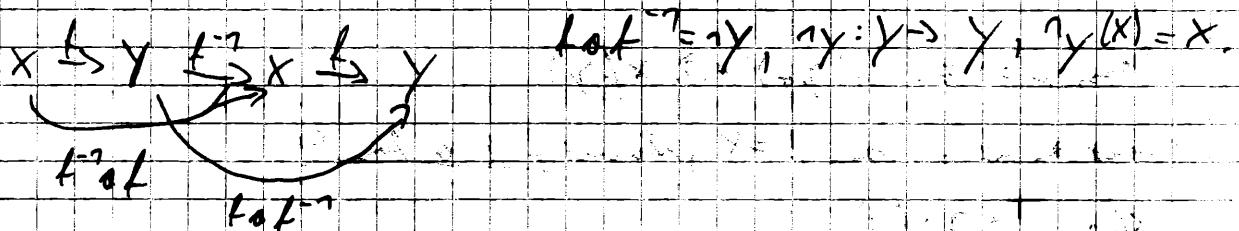
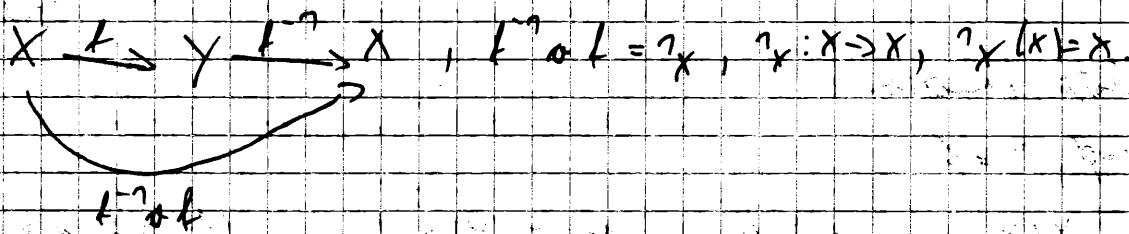
$(\neg \Rightarrow \neg) \Leftrightarrow (\neg \neg \Rightarrow \neg \neg)$

② •  $f$  surjektiv:  $\forall y \in Y, \exists x \in X, f(x) = y$ .

•  $f$  bijektiv sind ①  $\wedge$  ②

Über  $f$  bijektiv  $\Leftrightarrow$  Invertierbar ( $f^{-1}: Y \rightarrow X$ ,  $f^{-1}(y) = x$   $\forall y \in Y$ )

Invertierbar

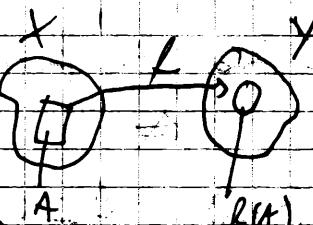


$f: X \rightarrow X$ ,  $f \circ \gamma_X = f = \gamma_X \circ f$ .

Ex:  $f: X \rightarrow Y$ ,  $A \subset X$

$f(A) = \{f(x) | x \in A\} = \{y \in Y | \exists x \in A: f(x) = y\}$

$f(x) = \{y | f(x) = y\}, I \subset f(C)$  (invg. direkt aus der A mit f)



Obs:  $f_{\text{unig}} \Rightarrow f^{-1} = f$ .

$$|X| = m.$$

$n, m \in \mathbb{N}^*$  (finito)

$$|Y| = n$$

$$F(x, y) =$$

$$F(x, y) = y^x ; |y^x| = |y|^{|x|} = n^m$$

$A_1, A_2 \subset X$ ,  $f: X \rightarrow Y$ ,  $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ ? NO.

Ex:  $f: \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}$ ,  $f(x) = \begin{cases} 1, & x \in \{1, 2, 3\} \\ 2, & x = 4 \end{cases}$

$$A_1 = \{1, 4\}$$

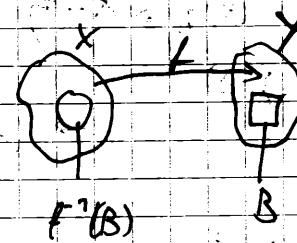
$$A_1 \cap A_2 = \emptyset$$

$$A_2 = \{2, 4\}$$

$$f(A_1 \cap A_2) = f(\emptyset) = \emptyset$$

$$f(A_1) = \{1, 2\}$$

$$f(A_2) = \{1, 2\}$$



$f: X \rightarrow Y$ ,  $B \subset Y$

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}$$

immagine inversa (o inversa) a una B sotto f

$f^{-1}y \rightarrow x$ ,  $f^{-1}(y) = x$ .

T (Ex) Dati due dati fct:  $f: X \rightarrow X$ ,  $B \subset X$  s.t.  $f^{-1}(f(B)) \neq B$ .

## CAP 2. Legi de comp. binară. Monotoni

$A \neq \emptyset$ , ( $\forall$ )  $f: A \times A \rightarrow A$ ,  $(x, y) \mapsto f(x, y)$  c.m.n. op. agraresc intern  
(sau legătura de comp. internă)

$$f(x, y) \xrightarrow{\text{not}} x * y$$

Ex:  $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $(x, y) \mapsto c.m.m.d.c(x, y)$ . E o legăt. de comp. (int.)?

$$(4, -6) = \pm 2$$

$$\text{convențional: } (4, -6) = (|4|, |6|) = 2$$

NUELEGE DE COMPOZITIE.

Obs:  $|A| = n$ ,  $n \geq 1$  nr. finit.  $\rightarrow |A|^{A \times A} = n^{n^2}$

$$\text{!! } |Y^X| = |\{(f: X \rightarrow Y)\}| = n^{n^2}$$

③ "\* e associativă:  $(x * y) * z = x * (y * z)$ ,  $\forall x, y, z \in A$ .

Ex: "+" este associativă;  $+: N \times N \rightarrow N$ ,  $(x, y) \mapsto x + y$ .

Ex:  $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $(x, y) \mapsto x - y$  este associativă?

$$(x - y) - z = x - (y - z)$$

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

$$2 - (1 - 3) = 2 + 2 = 4$$

$\Rightarrow$  "- este associativă pe  $\mathbb{Z}$ .

④ "\* e comutativă:  $x * y = y * x$ ,  $\forall x, y \in A$ .

$x \neq y \neq 0$ .

⑤ 1  $\in A$  este elem. neutru:  $(\forall) x \in A$ ,  $x * 1 = 1 * x = x$ .

Obs: Dacă există, elem. neutru este unic.

⑥  $x \in A$  este invertibil (inversabil):  $(\exists) x' \in A$  s.t.  $x * x' = x' * x = 1$ ,

(unde  $1 \in A$  el. neutru)

•  $M(\mathbb{N}, *)$  o.m. monigru (",\*" este asociativă)

• Un monigru cu el. neutru se numește monoid

Ex:  $(\mathbb{N}^*, +)$  monoid  $\Rightarrow$  monigru  
 $\hookrightarrow (\mathbb{N}^*, +)$

• Un monoid l-a tot oarec elem. de inversabil numește grup

Ex:  $(\mathbb{N}, +)$  l-a monoid dar nu și grup.

, "  $(M, \cdot)$  un monoid ,  $U(M) = \{x \in M \mid (\exists) x' \in M \text{ a.s. } x \cdot x' = x \cdot x' = 1\}$

L mult elem. inversabile (mult stabilă)

$H \neq \emptyset$  ,  $H \subseteq M$  este parte stabilită :  $(\forall) x, y \in H \Rightarrow x \cdot y \in H$ .

\*  $H: (H \times H \rightarrow H)$  , legătură compozită inducă)

P  $\exists_{\exists}(M, \cdot)$  un monoid și  $a_1, a_2, \dots, a_n \in U(M)$  astfel încât  $a_1 \cdot a_2 \cdot \dots \cdot a_k \in U(M)$  și  $(a_1 \cdot a_2 \cdot \dots \cdot a_n)^{-1} = a_k^{-1} \cdot a_{k-1}^{-1} \cdot \dots \cdot a_2^{-1} \cdot a_1^{-1}$  în plus  $(U(M), \cdot)$  este totuși grup.

H

$$(a_1 \cdot a_2 \cdot \dots \cdot a_{k-1} \cdot a_k) (a_k^{-1} \cdot a_{k-1}^{-1} \cdot \dots \cdot a_2^{-1} \cdot a_1^{-1}) = (a_1 \cdot a_2 \cdot \dots \cdot a_{k-1}) (a_k \cdot a_k^{-1})$$

$$\cdot (a_{k-1}^{-1} \cdot \dots \cdot a_2^{-1} \cdot a_1^{-1})$$

$$\text{similar} = (a_1 \cdot a_2 \cdot \dots \cdot a_{k-2}) \cdot (a_{k-1} \cdot a_{k-1}^{-1}) (a_{k-2}^{-1} \cdot a_{k-3}^{-1} \cdot \dots \cdot a_1^{-1}) \quad ?? = ?$$

Ex)  $a, b \in \mathbb{Z}$  ,  $n \geq 2$  ,  $a = b$  (ad n)  $\Rightarrow n | (a \cdot b)$  ( $\Rightarrow a = b$ )

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

$$\therefore : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n , (x, y) \rightarrow xy , xy = yx$$

$(\mathbb{Z}_n, \cdot)$  monoid comutativ  $x \cdot y = y \cdot x$

$(U(\mathbb{Z}_n), \cdot)$  grup ;  $U(\mathbb{Z}_n) = \{x \mid (x, n) = 1\}$

$(\mathbb{Z}_n^*, \cdot)$  grup :  $U(\mathbb{Z}_n^*) = \mathbb{Z}_n^*$  ( $\Rightarrow$  nu este un grup)

$(\mathbb{N}, +)$  monoid

$(\mathbb{N}^*, +)$  grup ( $\Rightarrow$ )

$\Rightarrow U(\mathbb{N}) = \mathbb{N}^*$

$\exists i \in \{1, \dots\}$ ,  $a \in M$ ,  $a^0 = \gamma_0$ ,  $a^i \neq \gamma_i$

$$a^m = \underbrace{a \cdot a \cdot \dots \cdot a}_{m \text{ fact}} \geq i, \text{ natural}$$

$$a^{-m} = (a^{-1})^m, m \in \mathbb{Z} \text{ and } a \in U(M)$$

$$[1] a^m \cdot a^{-m} = a^{m-m}, \forall m, n \in \mathbb{N}^*, (a \in U(M), m, n \in \mathbb{Z}^*)$$

$$[2] (a^m)^{-n} = a^{-m \cdot n}, \forall m, n \in \mathbb{N}^* (a \in U(M), m, n \in \mathbb{Z}^*)$$

$$[3] a, b \in M, a^m \cdot b^{-n} = (a \cdot b)^{-n} \text{ and } ab = ba$$

$$|a|^2 |b|^2 = (ab)^2$$

$$a \cdot a \cdot b \cdot b = ab \cdot ab$$

$$\text{"+": } \gamma a = a + a + \dots + a$$

[1] Ex: Berechne  $\gamma_2 \gamma_3 \gamma_4$  mit "+"

$$(M, +), (M_1, +) \text{ monoid}$$

Def:  $f: M \rightarrow M_1$ ,  $f(x+y) = f(x) \cdot f(y)$   $\forall f(\gamma_m) = \gamma_{m_1}$   $\gamma_m$  monoid de monoid

Ex)  $M \neq \emptyset$ ,  $P(M) = \{A \mid A \subseteq M\}$

$$(P(M), \cap), (A, B) \rightarrow A \cap B$$

$$(P(M), \cup), (A, B) \rightarrow A \cup B.$$

•  $(P(M), \cap)$  monoid:  $(A \cap B) \cap C = A \cap (B \cap C)$ ,  $\forall A, B, C \in P(M)$ .

$$\text{komut: } A \cap B = B \cap A$$

$$3. A \cap \emptyset = A, (\forall) A \in P(M), \emptyset = \emptyset$$

•  $(P(M), \cup)$  monoid:  $(A \cup B) \cup C = A \cup (B \cup C)$ ,  $\forall A, B, C \in P(M)$

$$\text{komut: }$$

$$1. A \cup B = B \cup A$$

$$3. A \cup \emptyset = A, (\forall) A \in P(M), \emptyset = \emptyset$$

$$f: (\mathcal{P}(M), \cup) \rightarrow (\mathcal{P}(M), \cap), f(X) = CX.$$

$$! C(A \cup B) = CA \cap CB$$

$CX = M \setminus X$

$$1. f(X \cup Y) = C(X \cup Y) = (X \cap CY = f(X) \cap f(Y)), \forall x, y \in \mathcal{P}(M)$$

$$2. f(\emptyset) = C\emptyset = M.$$

Nei avem o grupă  $(M, \cdot)$  cu totale elem. inversabile și cu grupă  $(G)$

în  $G$ -uri grupă:  $(G, \cdot)$ . Ex:  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(C, +)$ .

$(\mathbb{Z}^*, \cdot)$  grupă?  $\forall n \in \mathbb{Z}, 4^n \neq 0 \neq 2$

$\cup(z) = \{z^{-1}\}$ ,  $(\{z^{-1}\}, \cdot)$  grupă.

$-(\mathbb{Q}^*, \cdot)$ ,  $(\mathbb{R}^*, \cdot)$ ,  $(C^*, \cdot)$ .

$G$  p.m. grup finit, deci  $|G| < +\infty$

$|G| = 4 : (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ ;  $(\mathbb{Z}_4, +)$

$G, G_1$  grupuri;  $(G \times G_1, \cdot)$  produsul direct al grupelor  $G, G_1$ ; mul.

$$G \times G_1 = \{(a, b) \mid a \in G, b \in G_1\}$$

$$(a, b) \cdot (a_1, b_1) = (aa_1, bb_1)$$

$$(\gamma_G, \gamma_{G_1}) \cdot \gamma_G = \gamma, \gamma_{G_1} = ?$$

$$(a, b)^{-1} = (a^{-1}, b^{-1})$$

Teorema: Există o tablă de adunare în grupuri  $(+, \cdot)$

$$\mathbb{G}^2 \cong G \times G ; (\gamma \pm \gamma)^2, \cdot : (\gamma, \gamma), (\gamma, -\gamma), (-\gamma, \gamma), (-\gamma, -\gamma).$$

$G \text{ grup } (G, \cdot)$ Ex: 1)  $\mathbb{Z}, Q, R, C$       2)  $Q^*, R^*, C^*$ . $A \neq \emptyset, A^* = \{f \mid f: A \rightarrow A\}$ ,  $(f, g) \rightarrow f \circ g$  $(A^*, \circ)$  monoid comutativ,  $\gamma_A \stackrel{\text{not}}{=} I_A: A \rightarrow A$ . $f \circ g = g \circ f$  $\gamma_A(\gamma) = \gamma$  elerzi $(U(A^A), \cdot)$  grup,  $U(A^A) \stackrel{\text{not}}{=} S_A$  grupul num. mult.  $A$ . $A = \{1, 2, \dots, n\}$ ,  $S_A \stackrel{\text{not}}{=} S_n$  grupul permutatiilor de gradul  $n$ . $G, H \quad ((G, \cdot) \times (H, \cdot))$ ,  $(G \times H, \cdot)$  $G \times H = \{(a, b) \mid a \in G, b \in H\}$  $(a, b)(a_1, b_1) = (aa_1, bb_1)$  produs direct al grupurilor  $G, H$ . $(\gamma_G, \gamma_H); (a, b)^{-1} = (a^{-1}, b^{-1})$  $G = H, G^2 \stackrel{\text{not}}{=} G \times G$  $f(\gamma(\gamma))$ Ex:  $(\mathbb{F}^{\pm 1})^2, \cdot)$  grupul lui KleinEl. neutru Ex:  $(\mathbb{Z}^N, +)$ ,  $\mathbb{Z}^N = \{f \mid f: N \rightarrow \mathbb{Z}, f(n) = a_n\}$  $(a_n) = a_0, a_1, \dots$ 

## 2. Morfisme de grupuri

Def:  $f: G \rightarrow G$ , o.m. morfism de grupuri dacă  $f(x, y) = f(x) \cdot f(y), \forall x, y \in G$ Obs: 1.  $(G, \cdot) \xrightarrow{f} (G, +)$ ,  $f(x, y) = f(x) + f(y)$ ,  $(\forall) x, y \in G$ .2.  $f(\gamma_G) = \gamma_{G'}$ ,  $\gamma_{G'}$  elerz. neutru.Ex) 1.  $f: G \rightarrow G$ ,  $f(x) = \gamma_G$ 2.  $I_G: G \rightarrow G$ ,  $I_G(x) = x$ 3.  $f_a: G \rightarrow G$ ,  $f_a(x) = ax^{-1}$ 

(morfismul interior definit de un automorphism - m -)

Homomorfism bijectiv, deci opera și este un izomorfism  $G \cong G$ .

$f: G \rightarrow G$  izomorfism  $\Leftrightarrow$  automorfism.

Ex:  $(\mathbb{R}, +) \xrightarrow{f} (\mathbb{R}_+^*, \cdot)$ ,  $f(x) = 3^x$

$$f(x+y) = 3^{x+y} = 3^x \cdot 3^y = f(x) \cdot f(y)$$

Ex:  $(\mathbb{R}, +) \not\cong (\mathbb{R}_+^*, \cdot)$  În general, dacă  $K$  este un corp comutativ.

$(K, +) \not\cong (K^*, \cdot)$

Obl) 1. Dacă  $a$  este morfism de grupuri este un morfism de grupuri.

2. Rel. „izomorfism de grupuri” este o rel. de echivalență.

$((\mathbb{Z}/7\mathbb{Z})^2, \cdot)$ ;  $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ ,  $K \models \{1, a, b, c \mid a^2 = b^2 = c^2 = 1\}$ .

### 3. Subgrupuri

Ei și  $G$  un grup și  $H \subseteq G$ ,  $H \neq \emptyset$

Def: Spunem că  $H$  este un subgrup al lui  $G$  ( $H \subseteq G$ ) dacă  $\forall x, y \in H$  avem  $x, y \in H$  și  $y^{-1} \in H$ .

Obl: 1.  $\forall x, y \in H \Rightarrow x \cdot y \in H$  și  $y^{-1} \in H \Leftrightarrow \forall x, y \in H$ , avem  $x \cdot y^{-1} \in H$ ,  $H \subseteq G \Rightarrow \forall x, y \in H \Rightarrow x \cdot y^{-1} \in H$ .

2.  $H \subseteq G \Rightarrow (H, \cdot)$  este un grup.

$G \neq \{1\}$

$\{1\}$  subgrupul trivial,  $G$  subgrupul improporțional,  $H \subseteq G$ ,  $H \neq \{1\}$ ,

$H \neq G$   $\Leftrightarrow$  subgrup propriu

Ei și  $H \subseteq G$

1. Atunci  $H \cap K \subseteq G$  ( $\forall x, y \in H \cap K \Rightarrow x, y \in H$  și  $x, y \in K \Rightarrow x^{-1} y \in H$  și  $x^{-1} y \in K \Rightarrow x^{-1} y \in H \cap K$ ).

$H_i \subseteq G$

2.  $H \cup K \not\subseteq G$  ( $H \cup K \subseteq G \Leftrightarrow H \cap K$  nu este subgrup generalizat)

(1)  $f: G \rightarrow G_1$  morfism de grupuri

1.  $H \subseteq G \Rightarrow f(H) = G_1$

2.  $H_1 \subseteq G_1 \Rightarrow f^{-1}(H_1) \subseteq G$ .

Prop. Fie  $f: G \rightarrow G_1$  morfism de grupuri.

a) Dacă  $H \subseteq G$  astfel încât  $f(H) \subseteq G_1$ ,  $f(H) = \{f(x) | x \in H\}$ .

$$\text{Dacă } x, y \in H : f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) = f(h)$$

b) Dacă  $H_1 \subseteq G_1$ , astfel încât  $f^{-1}(H_1) \subseteq G$ .

$$f^{-1}(H_1) = \{x \in G | f(x) \in H_1\}$$

$K \cap f = f^{-1}(G_1)$  nucleu morfismului  $f$ .

$$K \cap f = \{x \in G | f(x) = e_{G_1}\}, K \cap f \subseteq G.$$

Prop. Fie  $f: G \rightarrow G_1$  morfism de grupuri și  $x \in K \cap f = f^{-1}(e_{G_1})$ .

$\Rightarrow$  Adăugăm la  $f$  & injecțivă și fix  $x \in K \cap f$ .

$$\begin{aligned} f(x) &= e_{G_1} \\ f(f(x)) &= f(e_{G_1}) \end{aligned} \Rightarrow x = e_G \Rightarrow K \cap f = \{e_G\}$$

$\Rightarrow$  Adăugăm la  $K \cap f = \{e_G\}$  și fix  $x, y \in G$  astă  $f(x) = f(y)$ .

$$\text{Ex: } f: \mathbb{R} \setminus \{0, 1, 2\} \rightarrow \mathbb{R} \setminus \{0, 1\}$$

$$f: \mathbb{R} \setminus \{0, 1, 2\} \rightarrow \mathbb{R} \setminus \{0, 1\}, f(x) = x^{-2}, f(x \cdot y) = \frac{1}{x^2 y^2} = x^{-2} y^{-2} = f(x) \cdot f(y)$$

de morfism

$K \cap f = \{1\} \Leftrightarrow$  injecțivă;  $f^{-1}(e) \neq \emptyset$  și inj.

$(\mathbb{Z}, +)$  și fizice  $n \in \mathbb{N}^*$ ,  $n \geq 3 \Leftrightarrow k \mid k$  ( $k \in \mathbb{Z}$ ).

Prop)  $H$  este subgrup.

Eins. - Zinsen $(G, \cdot)$  grupp.  $\Leftrightarrow H \subseteq G$ 

$$x, y \in G \quad x \leq y \text{ (mod) } H \Leftrightarrow x^{-1}y \in H \Leftrightarrow y \in xH$$

$$x < y \text{ (mod) } H \Leftrightarrow xy^{-1} \in H \Leftrightarrow x \in Hy$$

$$(G/H)_S = \{x - xH \mid x \in G\}$$

$$(G/H)_D = \{x - Hx \mid x \in G\}$$

(Idee ist: grupp.  $G$ )

$$x \leq y \text{ (mod) } H \text{ bedeutet } y \in xH \Leftrightarrow y \in x^{-1}yH \Leftrightarrow x = y$$

$$|(G/H)_S| = |(G/H)_D| \stackrel{\text{not}}{=} |G:H| \text{ (indirekt bei } G \text{ ein } H)$$

$$f: G \rightarrow G, f(x) = x^{-1} \text{ bijektiv } (f \cdot f^{-1} = \text{id}_G)$$

$$x \leq G$$

$$f(xH) \leq (xH)^{-1} = H^{-1} \cdot x^{-1}; f(xH) = Hx^{-1}$$

$$(G/H)_S = (G/H)_D \Leftrightarrow xH = Hx \Leftrightarrow xHx^{-1} \subseteq H \Leftrightarrow H \subseteq G \text{ (H rechts normal)}$$

Th. von LagrangeSei  $G$  von großer Gruppe mit  $H \subseteq G$ . Atmen ordnen grupp.  $|G| = |H| \cdot |G:H|$ 

In partiell  $|H| / |G|$

Bedenken man. weiter, & aufgibt es keinen anderen als der da stehende modul.  $H$ . $C_1 = x_1H, C_2 = x_2H, \dots, C_s = x_sH$  (diese da steh. modul.  $H$ ).

$$C_i \subset (G/H)_S$$

$$G = \bigcup_{i=1}^s C_i \Leftrightarrow |G| = \sum_{i=1}^s |C_i|$$

$$x \in H, f: H \rightarrow H, x \mapsto x^{-1}, \text{ bijektiv} \quad \text{①} \quad p \Rightarrow |G| = \sum_{i=1}^s |H| = s|H| = |H| \geq |C_i| \quad \text{②}$$

$$= |G \cdot H| |H| \quad |H| / |G| \Leftrightarrow |G \cdot H| / |G|$$

(Indirekte  
Zubij.)

Ex:  $(\mathbb{Z}_m, +)$ ,  $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ ,  $2+3 = \hat{x+y}$

Subgrupurile lui  $\mathbb{Z}_4$

Ei:  $H \leq \mathbb{Z}_4$  T. Lagrange  $|H|/|\mathbb{Z}| \rightarrow |H| = \{1, 2, 4\}$

Dacă  $|H|=1 \rightarrow H=\{0\}$

(Subgrup trivial)

Dacă  $|H|=2 \rightarrow H=\{0, \frac{1}{2} | 2+2=0\} \rightarrow H=\{0, 2\}$  (Subgrup. nulic. general)  
 $\frac{1}{2}+2=0$  (de la urmă 2)

Dacă  $|H|=4 \rightarrow H=\mathbb{Z}_4$ .

Ex: Det. subgrupurile grupului

$$K=\{1, a, b, c\}, a^2=b^2=c^2=1$$

sol.  $H \leq G \rightarrow |H|/|G|=4, |H|=\{1, 2, 4\}$

$\mathbb{Z}_4$

$\frac{1}{2}$

(etajat)

$\downarrow$

0

$$(G, \cdot) \text{ ord}(x) = \begin{cases} +\infty, & x^n \neq 1 \forall n \in \mathbb{N} \\ n, & x^n = 1 \end{cases}$$

$$x \in G, \quad \min(n), x^n = 1, \text{ dacă } (\exists) n \in \mathbb{N}^*, \text{ s.t. } x^n = 1.$$

$$|1|=1$$

$$(\mathbb{Z}, +) \text{ ord}(0)=1$$

$$\text{ord}(x) \geq ?$$

$$\text{Iatăcum dacă } (\exists) n \in \mathbb{N}^*, \text{ s.t. } \underbrace{x+x+\dots+x}_{\text{de } n \text{ ori}} = 0$$

$$\neg x=0 \text{ (Nu există)} \Rightarrow \text{Ordinul oricărui element}$$

diff de ordinul tot  $\mathbb{Z}$  ( $\mathbb{Z}, +$ )

$$\Leftrightarrow x=\{x^k | x \in \mathbb{Z}\}$$

(B): Dacă  $G$  grup. finit,  $|G|=n$ ,  $n \in \mathbb{N}^*$ ,  $x \in G$ , atunci  $\text{ord}(x) | n$ .

$$\text{ord}(x) = \text{ord}(|\langle x \rangle| \Leftrightarrow |\langle x \rangle| \leq G \text{ și Th. Lagrange} \Rightarrow \boxed{\text{ord}(x) | n})$$

$$\text{ord}(x) \leq n \rightarrow n \leq k \cdot q - q \leq n \rightarrow n^2 \leq (x^k)^2 - x^q = 1$$

Eil G este grup finit și număr. ordin  $n \mid |G|$

Astăzi (7) un element  $x \in G$  o.n. ord  $(x) = n$ .

$|G| = n, x \in G, \text{ord}(x) \mid |G|, x^n = 1$ .

$(\mathbb{Z}, +), (\mathbb{U}(\mathbb{Z}_n), \cdot)$  grup.  $|\mathbb{U}(\mathbb{Z}_n)| = \{x \in \mathbb{Z}^* \}$

$|\mathbb{U}(\mathbb{Z}_n)| = \phi(n)$  (functia lui Euler)

$\phi(n) \geq n^*, \phi(m) \geq \lfloor \frac{m}{k} \rfloor$  cu  $k \leq K$ ,  $\min(m, k)^2$

Dnm. T. lui Euler (...)

Nr. T. a. lui Fermat  $p(p) = p - 1$ ;  $a^{p-1} \equiv 1 \pmod{p}$

$(G/H)_S = (G/H)_d$ ,  $xH = Hx \Leftrightarrow xHx^{-1} \subset H \Rightarrow H$  subgrup normal al lui G dacă

$H \subseteq G$   $(\forall x \in G, h \in H) \Rightarrow xHx^{-1} \subseteq H$ .

• G grup. Subgrupurile triviale și subgrupul.

Dacă G abelian,  $\forall x \mid x \in G$ , există alt subgrup. normal.

$|G:H| \geq 2 \Rightarrow H \trianglelefteq G$ ,  $\forall h \in H \quad h \in (G/H)_S$ .

$(G/H)_S = \{H, G/H \Leftrightarrow (G/H)_d\} \cdot H \cdot 1 = H$

$(G/H)_S = (G/H)_d \Leftrightarrow H \trianglelefteq G$ .

### Morfisme de grupe

Numărul, Imaginea

Dacă  $G, G'$  două grupe și  $f: G \rightarrow G'$  un morfism de grupe și at.  $[ker f \trianglelefteq G]$

(Num. lui f este D al lui G)

$H \trianglelefteq G \Rightarrow G/H = \{xH \mid x \in G\}$

$\tilde{x} = \bar{x} \in xH, \tilde{x}' \tilde{y} = \tilde{x'y}$

$(G/H)_i$  grup. Numește grup. factor al lui G în raport cu H. (subj. canonice)

$\tilde{x}\tilde{x}^{-1} = \tilde{x} = \tilde{x} = \tilde{x}x^{-1}$

$\tilde{x} \cdot \tilde{x}^{-1} = \tilde{x}x^{-1} = \tilde{x} = \tilde{x}^{-1} \cdot \tilde{x} = \tilde{x}^{-1} \tilde{x}$

$(G/H)$  nr. factor ( $H \subseteq G$ )

$G/H$ , G abelian  $\Rightarrow$  Orice subgrup  $H \subseteq G$  este subgrup. normal.

Ex:  $(\mathbb{Z}, +), H \subseteq \mathbb{Z}$ .

## T. Fundamentals de izomorfismos al grupos finitos

Si  $f: G \rightarrow G'$ , un morfismo de grupos. Atendiendo a ( $\gamma$ ) un isomorfismo  $I: G/\text{Im } f \rightarrow G'/\text{Im } f$

$$\Rightarrow I = 1, x \equiv y \pmod{\text{Ker } f} \Leftrightarrow x^{-1}y \in \text{Ker } f$$

$$f(x^{-1}y) = 1 \Leftrightarrow x = y.$$

$$G, H \subseteq G, G/H \quad \text{Ker } f \subseteq G \Rightarrow G/\text{Ker } f \cong G/H.$$

$G \rightarrow G'$ -morfismo  $\Rightarrow G/\text{Ker } f \cong G'$ .

$$\text{Función } F(\gamma) = F(\gamma) \Rightarrow x \cdot y$$

$$F(\gamma) = f(\gamma) +$$

$$f^{-1}(x^{-1}) = f(y^{-1}) \Rightarrow x^{-1}y \in \text{Ran } f.$$

$f: G \rightarrow G'$  (función inyectiva)  $\Rightarrow G \cong G'$ .

Amb

$$\exists (G, \cdot) \cong (\mathbb{R}_+^*, \cdot), T = \{x \in \mathbb{R}^* \mid n = x\}.$$

$G/T$  sea isomorfismo con  $\mathbb{R}^*$ .

$$f: G^* \rightarrow \mathbb{R}^*$$

$f: G \rightarrow G^*$ , isomorfismo de grupos  $\Rightarrow G \cong G^*$ ,  $f(n) = n$ .

$T$  fiel de isomorfismo  $\Rightarrow G/\text{Ker } f$  isomorfismo.  $\text{Im } f$ .

$$G = \text{Im } f, \text{Im } f \leq G$$

$$G \cong G' (\Rightarrow G \leq G')$$
 (enfóndar)

Euroz 15.11.2019

### Teorema de monomorfism

$f: G \rightarrow G'$  un izomorfism de grupuri, astfel încât  $f: G/\text{ker } f \rightarrow \text{Im } f$  este monomorfism.

$$\text{ker } f = \{x \in G \mid f(x) = \text{id}_{G'}\} \triangleq G, \text{Im } f = \{f(x) \mid x \in G'\} \triangleq G.$$

$$G/\text{ker } f = \{\bar{x} = x \text{ker } f \mid x \in G\}$$

Astăzi  $f: G \rightarrow G'$  este surjectiv (morfism surjectiv)

$$\text{ker } f = \{\text{id}_{G'}\}, G/\{\text{id}_{G'}\} \cong \text{Im } f, G \cong \text{Im } f; \text{Im } f \leq G.$$

Ex Fie  $(G, \cdot)$  un grup și  $\gamma$  un element de  $G$ ,  $f: g(x)^\gamma = \gamma x \gamma^{-1}; \text{Im } f(G) = \langle \gamma \rangle_{G'}$ .  
Văd că  $G/\langle \gamma \rangle \cong \text{Im } f$ .

T1 (Teorema de izomorfism): Fie  $G$  un grup și  $H$  un subgrupuri normali ale lui  $G$ , astfel încât  $H \subset N$ . Atunci  $N/H \cong G/H$  și  $G/H$

Fie  $f: G/H \rightarrow H/H, f(\bar{x}) = x$  ( $N/H \cong G/N$ )  $G/H = \{xH \mid x \in G\}$ .

$$G/N = \{\bar{x} = xN \mid x \in G\}$$

•  $f$  este bine definită  $\bar{x} = \bar{y} \Rightarrow x^{-1}y \in H, H \subset N \Rightarrow \bar{x} = \bar{y} \Rightarrow f(\bar{x}) = f(\bar{y})$

$f$  este surjectivă  $\bar{x} = xN \not\exists \bar{x} = xH$  a. n.  $f$  este morfism  $f(\bar{x}\bar{y}) = f(\bar{x}\bar{y}) = x\cdot y = f(\bar{x}) \cdot f(\bar{y})$ , (b)  $\bar{x}, \bar{y} \in G/H$ .

$G/H/\text{ker } f \cong \text{Im } f = G/N$  (f este surjectiv). Astăzi că  $\text{ker } f = N/H$ .

$$\text{ker } f = \{x \in G \mid f(x) = \text{id}_H\}$$

Fie  $\bar{x} \in \text{ker } f \Rightarrow f(\bar{x}) = \bar{1} \Rightarrow \bar{x} = \bar{1} \Rightarrow x \in N$  (1).

Fie  $\bar{x} \in N/H \Rightarrow x \in N \Rightarrow \bar{x} = \bar{1} \Rightarrow f(\bar{x}) = \bar{1} \Rightarrow \bar{x} = \text{ker } f$  (2)  $\text{ker } f = N/H$  (2)

$$\text{Din 1 și 2 } \Rightarrow \frac{G/H}{N/H} \cong G/N.$$

$G$ -grup  $b = k_a > 0 \in G$ ;  $G$  este ciclic.

$$G \subset a > \langle a^k \mid k \in \mathbb{Z} \rangle$$

$$\langle z, + \rangle = \langle \gamma \rangle = \langle -\gamma \rangle$$

$$\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}, \gamma + \bar{\gamma} = \overline{\gamma + \bar{\gamma}}$$

$$\langle \mathbb{Z}_m, + \rangle = \langle \gamma \rangle$$

$$\underline{\text{Ex:}} \quad (z_1, t) = \langle a \rangle \Leftrightarrow (a, a) = t$$

I: Orice grup ciclic este izomorf cu  $\mathbb{Z}$  sau cu un grup cu mulțime  $\mathbb{Z}_{n+1}, n \geq 0$

$$\text{Dacă } G = \langle a^k \mid k \in \mathbb{Z} \rangle, \quad f: (\mathbb{Z}, +) \rightarrow (G, \cdot)$$

$$\text{Ești } f: \mathbb{Z} \rightarrow G, \quad f(k) = a^k.$$

$$f \text{ este o aplicație surjectivă: } f(k+l) = a^{k+l} = a^k \cdot a^l = f(k) \cdot f(l)$$

$$\text{Aplicația "I. fund de izomorfi" } \Rightarrow \mathbb{Z}/\ker f \cong \mathbb{Z}, \quad \cong_{\text{grupuri}}, \quad \exists I, \quad I = \{l \mid l \in \mathbb{Z}, \quad \ker f \leq \mathbb{Z} \rightarrow \ker f = \mathbb{Z}, \quad \mathbb{Z} \in N\}.$$

$$\text{I) } \ker f = \{0\} \quad (\text{pt } m=0 \Rightarrow \mathbb{Z}/\{0\}) \Rightarrow G \cong \mathbb{Z}.$$

$$\text{II) } \ker f = \mathbb{Z}, \quad m > 0 \Rightarrow \mathbb{Z}/m\mathbb{Z} \cong G \cong \mathbb{Z}_m \cong G \quad (\text{Teorema de structură a } V)$$

$$\text{III) } \text{Dacă } a \in G \text{ este un operator al lui } G \cdot G = \langle a \rangle$$

$$\text{I) } \text{ord}(a) = +\infty \Rightarrow G \cong \mathbb{Z}$$

$$\text{II) } \text{ord}(a) < +\infty \Rightarrow G \cong \mathbb{Z}_n$$

(Ob.) Orice subgroup într-un factor al unui grup ciclic este ciclic.

$$\underline{\text{Ex:}} \quad \text{Det. subgrupurile factorului } \mathbb{Z}/\mathbb{Z}_{12}$$

$$\text{Det } H \leq \mathbb{Z}_{12}, \quad |H| / |\mathbb{Z}_{12}|$$

$$(\text{--}) \text{ Lui Lagrange } \Rightarrow H \in \{1, 2, 3, 4, 6, 12\}$$

$$|H|=1 \Rightarrow H = \{0\}$$

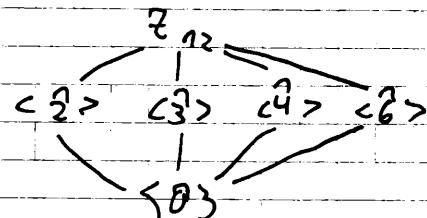
$$|H|=2 \Rightarrow H = \{0, x\} \quad x+x=0 \Rightarrow \{0, 6\}$$

$$|H|=3 \Rightarrow H = \{0, x, x+x\} \quad x+x+x=0 \Rightarrow \{0, 4, 8\}$$

$$|H|=4 \Rightarrow H = \{0, 3, 6, 9\}$$

$$|H|=6 \Rightarrow H = \{0, 2, 4, 8, 10, 12\} = \{12\}$$

$$H=12 \Rightarrow H = \mathbb{Z}_6$$



$$\mathbb{Z}_{12}/\mathbb{Z}_{12} = \{0\}$$

$$\mathbb{Z}_6/\mathbb{Z}_{12} = \left\{ \frac{\mathbb{Z}_{12}}{\mathbb{Z}_2} = 2 \right\} \Rightarrow \mathbb{Z}_{12}/\mathbb{Z}_2 = \mathbb{Z}_2$$

$$\mathbb{Z}_{12}/\langle 3 \rangle = \mathbb{Z}_3, \quad \mathbb{Z}_{12}/\langle 4 \rangle = \mathbb{Z}_4, \quad \mathbb{Z}_{12}/\langle 6 \rangle = \mathbb{Z}_6.$$

$H \leq S_m \Rightarrow H = \langle d \rangle$ . d |  $z_m$  und  $d \mid m$ .

Eigenschaften der Permutationen.

Zie  $M \models d$ ,  $S(m) = \{f(m) = \{f: m \rightarrow m \mid f \text{ bijektiv}\}\}$ .

$(S(m), \circ)$   $\cong$   $S_m$  gruppal mult  $M$ .

$(f, g) \mapsto f \circ g$ ,  $(f \circ g)(x) = f(g(x))$ .

P. Dass  $f: M \rightarrow M'$  o. mult bijektiv, dann ist  $SM \cong S_{M'}$  mit isomorphismus  $S_m \cong S_{m'}$ .

Dass  $\theta: S_m \rightarrow S_m$  o. fij bij, dann  $S_m = S_m'$ .

$$\theta(f) = f \circ f \circ f^{-1}; M \xrightarrow{f} M \xrightarrow{f} M$$
  
$$f \circ f \circ f^{-1}$$

Modifiziere für  $f, f \in S_m$ .

$$\theta(f \circ f_1) = f \circ f \circ f^{-1} \circ f_1^{-1}$$

$$f \circ f_1 = f = f_m \circ f$$

$$f_m = f \circ f^{-1}$$

$f \circ (f \circ f_1) \circ f^{-1} = (f \circ f) \circ (f^{-1} \circ f) \circ (f_1 \circ f^{-1}) = (f \circ f \circ f^{-1}) \circ (f \circ f_1 \circ f^{-1}) = \theta(f) \theta(f_1) \theta(f_1)$  injektivität von  $\theta$ .

$$\theta(f) = \theta(f_1) \Rightarrow f \circ f \circ f^{-1} = f \circ f_1 \circ f^{-1} \Rightarrow f = f_1$$

$\theta$  surjektiv,  $g \in S_m$ ,  $\exists h \in S_m$  s.t.  $\theta(h) = g$ .

$$M \xrightarrow{f} M \xrightarrow{f} M \xrightarrow{f} M, h = g \circ f \circ f^{-1}$$

$$g \circ f \circ f^{-1} \quad \theta(g \circ f \circ f^{-1}) = f \circ g \circ f^{-1}$$

$|M| = n$ ,  $M = \{1, 2, \dots, n\}$ ,  $S_m = S_n$ , gruppal nach d. ordnung

$n \geq 1$  finit

$$\tau \in S_n, \tau = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & & f(n) \end{pmatrix}, \tau^{(1)} \tau^{(2)}$$

$$|S_n| = n!$$

(Ans.)  $S_n$  ist ungrup abelian ( $\Rightarrow n \leq 2, n \leq 1$ )  $S_1, S_2$ .

$$S_3 = \{1, f, f^2, \tau \quad 0/f^3 = 1 = \tau^2, f^2 \tau =$$

9. rezidual probability =  $\prod_{i=1}^n \overline{P(i)} \cdot P(i)$ . m. probability

$$(i,j) \quad 1 \leq i < j \leq n \\ (\text{amazing}) \quad \overline{P(i)} > P(j) \quad \overline{P} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad (3, 1) (3, 2) \\ \rightarrow \overline{P} \cdot P = I \Rightarrow \det(P) = 2$$

then  $V(P) = \text{m. involution}$  I  $\rightarrow V(P)$  and  $\{S\} = \{-2\} \in S_3$ ,

$$\Delta: S_m \rightarrow S_n$$

$$S_n: A \mapsto \{1, 2\} = \{1, 2\}; \quad (A, \dots) \mapsto \frac{A+1}{2}$$

$$D) f: m \rightarrow m' \text{ big } \Rightarrow S_m \cong S_{m'}^{(2)}$$

T. ord. gen. G aus derselben  
(Körper)

$$G \rightarrow S_m \quad ((\gamma) \text{ NSB}_m, G \cong H)$$

$S_m \cong S_n \Rightarrow T_G \rightarrow S_n$  un. morphismus injektiv

$$t(\gamma) = \overline{\gamma} \quad t_\gamma(A) = \gamma^A$$

P. kann anderes (perfekteideale?) Element, mit gleicher Fm. kein?

$$(K \neq \mathbb{F}_1, \mathbb{F}_4, \mathbb{F}_{16}, \text{ct } \alpha^2 = \alpha^2 - \alpha = 17^\circ)$$

Idele și Corpuri

$(A, +, \cdot)$  ideal (ideal unitar)

- $\left\{ \begin{array}{l} B \subset A \text{ subînsemnat, doar: } \\ 1) (B, +) \subseteq (A, +) : (t) x, y \in B \Rightarrow x-y \in B \\ 2) B \text{ nu este subînsemnat cu } \cdot : (t) x, y \in B \Rightarrow xy \in B \\ 3) 1 \in B \end{array} \right.$

$(1) \cap (2) \cap (3) \Rightarrow (B, +, \cdot)$  ideal

---

1)  $\bigcap_{d \in T} B_d$  subînsemnat cu  $\cdot$   $\Rightarrow \bigcap_{d \in T} B_d$  subînsemnat cu  $A$ .

2) De la ipoteza:  $\forall d \in T \quad B_d \subseteq (A, +)$

$\exists (t) x, y \in B_d \Rightarrow x-y \in B_d, (t) x \in T \Rightarrow x \in \bigcap_{d \in T} B_d$

3)  $\forall d \in T \quad 1 \in B_d$ .

2)  $B, C$  subînsemnări ale lui  $A \not\Rightarrow B \cup C$  subînsemnat cu  $A$ .

Ex)  $(\mathbb{Z}, +, \cdot)$

$$\left[ \begin{array}{l} H \subseteq (\mathbb{Z}, +) \Rightarrow H = \mathbb{Z}, \mathbb{Z} \neq 0. \\ 27, 32 : 27 \cup 32 \\ | \quad \quad \quad 3-2 = 1 \notin 27 \cup 32 \end{array} \right]$$

Notare:  $I \neq \emptyset, I \subset A$  și m. ideal liniștit (nu nuanță) / doar doar

1)  $\forall x, y \in I \Rightarrow x-y \in I$

2)  $\forall a \in A$  cu  $x \in I \Rightarrow ax \in I$  (numai  $x \in I$ )

---

$a \in I, x \in I$ : ideal bilateral

$\bar{A} ; \langle 0 \rangle, A$  ideal bilateral

I ideal  $\Rightarrow$  nulul

$\lambda \in I$

$$\text{Ex: } \mathbb{R} \subset \mathbb{R} \quad (2 \cdot \frac{2}{5} = \frac{4}{5} \neq 0)$$

• Dacă ideal în corp  $U(A) = A^*$  nu. corp.

"•" este comutativ, vă spune că este un corp comutativ

{A ideal}

I ideal număr (num. drept) al lui A

Obs: Dacă I conține un element invertibil, atunci  $I = A$ .

$$\exists x \in I \cap U(A)$$

$$I \subset A; A \subseteq I$$

$$\text{Fie } a \in A; a = a(x^*x)a \Rightarrow a \in I.$$

A corp: fie I un ideal număr (num. drept) al lui A,  $I \neq \{0\}$ .

$$\forall x \in I \cap A^* \Rightarrow I = A.$$

! A corp:  $\{0\}$ , A - singular ideal.

$\uparrow$   
ideal, ideal nul

E) Final,  $M_n(A)$  este mult. mulțime cu elem. dim. A ( $A = \mathbb{R}, A = \mathbb{Q}$ ).

$(M_n(A), +, \cdot)$  împreună cu divizori ai lui zero,  $n \geq 2$

$$U(M_n(A)) = GL_n(A)$$

L grup linișit general.

$GL_n(A)$  - grupul general linișit de ordinul n.

$M_2(\mathbb{R})$

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}; AB = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}; BA = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

A ideal, X submultime rezidua la leia A.

$Ax = \{a_1x_1 + a_2x_2 + \dots + a_nx_n \mid a_1, a_2, \dots, a_n \in A; x_1, x_2, \dots, x_n \in X\}$  ideal

ideal stang, generat de X (ex) ?!?

$XA = \{x_1a_1 + x_2a_2 + \dots + x_na_n \mid a_1, a_2, \dots, a_n \in A; x_1, x_2, \dots, x_n \in X\}$ .

idealul drept generat de X

$AxA = \{a_1x_1b_1 + a_2x_1b_2 + \dots + a_nx_1b_n \mid a_1, a_2, \dots, a_n \in A; b_1, b_2, \dots, b_n \in A; x_1, x_2, \dots, x_n \in X\}$

idealul bilateral generat de X

A este comutativ:  $Ax = XA = AxA$ .

$X = \{X\}$ ,  $Ax = \{ax \mid a \in A\}$  idealul generat de X.

Ex)  $(\mathbb{Z}, +)$  și  $\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$   $\rightsquigarrow$  a.

idealul principal al lui  $\mathbb{Z}$

A este corect;  $I \subseteq A$  ideal

1.  $x - y \in I$ ,  $(A)x, y \in I$ .  $I \triangleq (A, +)$ .
2.  $a \in I$ ,  $a \in A, x \in I$   
 $xa = ax$

A este corect

! Construcția inclusiv  $t = \text{ord}(A)$ !

$\text{ord}(A) = \begin{cases} \text{ord}(1), \text{ dacă } \text{ord}(1) < +\infty \\ 0, \text{ dacă } \text{ord}(1) = +\infty \end{cases}$

$\text{ord}(1) \in (A, +)$

$$(\underbrace{1+1+\dots+1}_n = 0, n \geq 1)$$

$\mathbb{Z}_5$

$$1+1+1+1+1=0$$

$$\text{ord}(1) = 5.$$

$\text{ord}(A) = 0$ , A este un ideal maximal cu  $\mathbb{Z}$ ,  $P = \{k \cdot 1_A \mid k \in A\}$

$P \subseteq A$ .

$$1_A = 1.$$

$\text{cor}(A) = \text{ord}(1) \Rightarrow A$  contient  $\alpha$  coprime isomorphes zu  $\mathbb{Z}_n$ :  $\text{Pof}(K, \mathbb{Z}_A)$  (d.h.  $\forall k \in K \exists n \in \mathbb{N}$ )

$\Rightarrow \text{cor}(A) = \langle 0, n \rangle$   $n$ -min. prim.

$0 \leq k \leq n-1$ .

A integre ; kompositum  $K$ :  $\text{cor}(k) = 0$ ,  $k \in K$

(1) subgruppen min. al kein  $A$

$Q, R, C$

$\text{cor}(K) = n$ ;  $\mathbb{Z}_n \subset K$ .

$\Rightarrow$  kompositum  $K$  ist der Rest der  $n$

$\mathbb{Z}_n \subset K$ ,  $|k| = n$  el. miteinander;  $n = |\text{Ker } \mathbb{Z}_n| = \text{dim}_{\mathbb{Z}_n} K$ .

$|K| = n$ ,  $n$ -min.

$|K| = 6$  ?;  $2 \cdot 3$

! T. (Wedderburn): Eine von  $n$  min. gte. non-abelian

$A, B$  integre

Def:  $f: A \rightarrow B$  Homomorphismus de integre: 1.  $f(x+y) = f(x) + f(y)$

2.  $f(x \cdot y) = f(x) \cdot f(y)$ ,  $\forall x, y \in A$

3.  $f(1_A) = 1_B$  ( $1 \equiv 1_A = 1_B$ )

(Or) 1)  $A \xrightarrow{f} B \xrightarrow{g} C$ ;  $A, B, C$  integre;  $f$  &  $g$  morphismus de integre  $\Rightarrow$

$\Rightarrow g \circ f: A \rightarrow C$  morphismus de integre.

$$(g \circ f)(x) = g(f(x)).$$

morphismus injektiv = isomorphismus  $A \not\subseteq B$ ;  $f: A \rightarrow A$  morphismus automorph

$$f: A \rightarrow A, f(x) = x \quad (\text{et!})$$

2)  $f$  isomorphismus  $\Rightarrow f^{-1}: B \rightarrow A$  isomorphismus

3)  $f: A \rightarrow B$  morphismus de integre

(P) a) Dacă  $G$  este un subinel al lui  $A \Rightarrow f(G)$  este un subinel al lui  $B$

În particular:  $f(A) = \text{Im } f$  este subinel al lui  $B$ .

De la proprietate  $f(C) \subseteq (B, +)$  ( $\forall a, b \in f(C) \Rightarrow a - b \in f(C)$ )

$$f(C) = \{f(x) \mid x \in C\} = \{\gamma \in B \mid (\exists x \in C : f(x) = \gamma)\}.$$

$$f(x+y) = f(x) + f(y) \in f(C). \quad (x = f(x), y \in f(y))$$

$$f(1_A) = 1_B$$

$f(c)$  subiectul al lui  $B$

$$f: G \rightarrow G_1$$

a) Dacă  $I$  este un ideal în  $(G, +)$  (num. ideal, lăr. lăr., bilater)  $H \subseteq I \Rightarrow f(H) \subseteq G_1$ ,

subiectul al lui  $B$  este și  $f^{-1}(I)$  este un  $H_n \trianglelefteq G_1 \Rightarrow f(H_n) \trianglelefteq G$

ideal în  $G$  (num. ideal, lăr. lăr.) subiectul lui  $I_{n+1} = f(G) \subseteq G_1$

A  
în

De la proprietate  $f^{-1}(I) \trianglelefteq A$  ( $\forall x$ )

$$\text{Ker } f = f^{-1}(\{0\}) \trianglelefteq G.$$

La proprietate

La înțeles

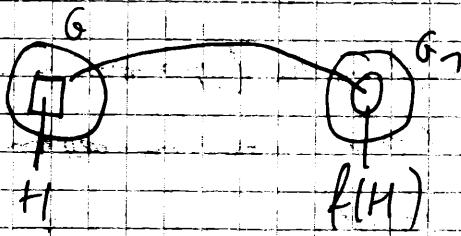
$G, G_1$  grupuri

$A, B$  inele

$f: G \rightarrow G_1$  morfism

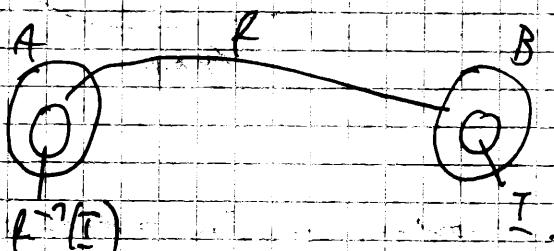
$f: A \rightarrow B$  morfism

①  $H \subseteq G \rightarrow f(H) \subseteq G_1$  (in fSG) ②  $C$  subiectul al lui  $A \Rightarrow f(C)$  subiectul al lui  $B$



(In f este subiectul al lui B)

③  $H_1 \trianglelefteq G_1 \Rightarrow f^{-1}(H_1) \trianglelefteq G$



(Ker f \trianglelefteq G)

④  $I$  ideal s. (d., lăr.)  $\Rightarrow f^{-1}(I)$  ideal s. (d., lăr.) al lui A

Ker f ideal lărât al lui A

Obs: [Morfism de corp: morfism de inel între 2 corpuri]

(P)  $K$ -cor, + ideal

$f: K \rightarrow A$  morfism injectiv?

$\ker f$  ideal al lui  $K$ .

$$f(\gamma) = \gamma \neq 0 \Rightarrow \ker f \cong \{0\} \Rightarrow f \text{ e injectiv.}$$

(P) Fil  $A$  un ideal cointurat de corat  $\gamma$  ( $\gamma$  nesc). Atunci:

$f: A \rightarrow A$ ,  $f(x) = x^\gamma$  morfism de inele (endomorfismul lui Frobenius)

$$f(x\gamma) = (x\gamma)^\gamma = x^\gamma \cdot \gamma^\gamma = f(x) \cdot f(\gamma) \quad (\forall) x, \gamma \in A$$

$$f(\gamma) = \gamma^\gamma = \gamma = \gamma^\gamma = \gamma.$$

$$\begin{aligned} f(x+\gamma) &= (x+\gamma)^\gamma = x^\gamma + C_\gamma^n x^{n-\gamma} \gamma + \dots + C_{n-\gamma}^n x^\gamma \gamma^{n-\gamma} + \gamma^\gamma \quad | \quad n \leq k \leq n-1 \\ &= x^\gamma + \gamma^\gamma = f(x) + f(\gamma). \end{aligned}$$

$$C_n^k = \frac{n!}{k!(n-k)!}$$

$G$  grup,  $H \trianglelefteq G$  ( $\forall x \in G, h \in H \rightarrow x^{-1}x^\gamma h \in H, xH = Hx$ )

$$x \equiv \gamma \pmod{H} \Leftrightarrow x^{-1}\gamma \in H; (G/H) \circ \gamma (G/H) \in [G/H]$$

Alinel  $\gamma$  îl ideal bilateral al lui  $A$ :  $(A/\gamma, +, -)$

$I$  ideal bilateral  $\Rightarrow I \trianglelefteq (A, +) \Rightarrow (A/I, +)$

$$A/I = \{x = x + I \mid x \in A\}.$$

Introducem  $\overline{x}, \overline{\gamma} = \overline{x\gamma}$  (binar definite)

$$\overline{x} = \overline{x'} + i \quad \overline{\gamma} = \overline{\gamma'} + j \Rightarrow x = x' + I, \gamma = \gamma' + I$$

$$\Rightarrow x\gamma = (x' + i)(\gamma' + j) = x'\gamma' + \underbrace{x'i + \gamma'i + ij}_{I} \Rightarrow \overline{x\gamma} = \overline{x'\gamma'}$$

$(A/I, +, -)$  idealul factor (nu ideal cît) al lui  $A$  în raport cu  $I$ .

$\pi: A \rightarrow A/I, \pi(x) = \overline{x}$  (surjectia canonica).

Teorema fundamental de morfism de inele

(izomorf.)

T) Fie  $f: A \rightarrow B$  un morfism de inele. Atunci există un izomorfism  $F: A/\ker f \rightarrow \text{Im } f$ ,  $F(x) = f(x)$ .

(A nu este nicio inel)

Denumire:  $F$  este izomorfism de grupuri ( $A/\ker f \cong \text{Im } f$ )

$$\forall a, b \in A, F(a \cdot b) = F(\bar{a} \bar{b}) = f(a \cdot b) = f(a) \cdot f(b) = F(a) \cdot F(b).$$

$$F(1) = f(1) = 1$$

Expoziție

Învel.

$f: G \rightarrow G_1$  morf. injectivă  
(surjectivă)

$$G/\ker f \cong \text{Im } f \subset G_1$$

$$G \cong \text{Im } f$$

$f: A \rightarrow B$  morf. inj de inele.

$$\xrightarrow{\text{T. fundamental}} A/\ker f \cong \text{Im } f$$

$A \cong \text{Im } f$ ,  $\text{Im } f$  subinel al lui  $B$

$$G \hookrightarrow G_1 (G \subseteq G_1)$$

$$A \hookrightarrow B \quad \begin{cases} A \text{ este fi orientat} \\ \text{nu subinel al lui } B \end{cases}$$

Prima noite - până la inele (particular) (Data: 0.2.2018)

- fără denumire - inventari - pf: rel de ordine  
- surjectivă și bijecțională  
- și simplificări

I - Def și ex:

II - Th. importanță (boundary, Zgrupăj, Teoreme)

Laboratory

## I. MULTIMI și FUNCȚII

- $f: A \rightarrow B$
- $f: A \rightarrow B$ ,  $f$  injectivă ( $\Rightarrow \forall x_1, x_2 \in A$

Aplicații:

1. Exerc. Iată def. respectiv prin formulă următoare:

a)  $f: N \rightarrow N$ ,  $f(n) = n+5$

b)  $g: N \rightarrow N$ ,  $g(n) = n^2 + 7$

c)  $h: Z \rightarrow Z$ ,  $h(x) = 3x + 7$ .

d)  $K: N \rightarrow Z$ ,  $K(x) = \begin{cases} \frac{x}{2}, & x \text{ par} \\ -\frac{(x+1)}{2}, & x \text{ impar} \end{cases}$

e)  $l: R \rightarrow R$ ,  $l(x) = x^3 - 2$ .

f)  $m: R \rightarrow R$ ,  $m(x) = \begin{cases} x^2, & x \leq 0 \\ -x, & x > 0 \end{cases}$

•  $f, g, h$ , injective, dar nu surjective•  $K, l, m, n$  sunt bijective

a) Iată  $n_1, n_2 \in N$  cu  $f(n_1) = f(n_2) \Rightarrow n_1 + 5 = n_2 + 5 \Leftrightarrow n_1 = n_2 \Rightarrow f$  injectivă

Ez.  $f$  nu e surjectiv deoarece  $1 \notin N$  sau  $\exists z \in N$  s.t.  $f(z) = 7$ (deoarece nu există  $n_1 + 5 = 7$ ,  $n_1 = -9 \notin N$ )

b) Iată  $n_1, n_2 \in N$  a.s.  $f(n_1) = f(n_2) \Rightarrow n_1^2 + 7 = n_2^2 + 7 \Leftrightarrow n_1^2 = n_2^2 \Leftrightarrow n_1 = n_2$  (n)

 $\exists x, y \in N$ .  $\rightarrow f$  injectivă• Ez.  $g$  nu e surjectivă deoarece există  $0 \in N$  nu împarte $\exists x \in N$  a.s.  $g(x) = 0$ . (altfel  $x^2 + 7 = 0 \Leftrightarrow x^2 = -7 \notin N$ )

c) Iată  $x_1, x_2 \in Z$  a.s.  $h(x_1) = h(x_2) \Rightarrow 3x_1 + 7 = 3x_2 + 7 \Leftrightarrow$

$3x_1 = 3x_2 \Leftrightarrow$

 $x_1 = x_2 \Rightarrow h$  injectivă.

• Es ist  $k$  eine surjektive, genauer die  $\exists$  nur  $\exists$  ein  $x \in \mathbb{Z}$  s.d.  $k(x) = 0$   
 (falls  $3x+1=0 \Leftrightarrow x = -\frac{1}{3} \notin \mathbb{Z}$ )

d) Es sei  $x, y \in \mathbb{N}$ . o.d.  $k(x) = k(y)$ .

$$\cdot x, y \text{ paar } \Rightarrow \frac{x+y}{2} = \frac{y}{2} \Rightarrow x = y$$

$$\cdot x, y \text{ unpaar } \Rightarrow -\frac{x+y}{2} = -\frac{y+1}{2} \Rightarrow x = y$$

$$\cdot x, y \text{ unpaar, relativist imn } \Rightarrow k(x) \in \mathbb{N}, k(y) \in \mathbb{Z}$$

unmöglich

$$\cdot \text{Für } y \in \mathbb{Z}, \text{ da } y \geq 0 \Rightarrow k(y) = \frac{2y}{2} = y$$

$$y < 0 \Rightarrow k(y) = \frac{-2(y+1)}{2} = y$$

$$2) \text{ Es seien } x_1, x_2 \in \mathbb{R}, x_1 = x_2 \Rightarrow l(x_1) = l(x_2) \Leftrightarrow x_1^3 + 2 = x_2^3 + 2 \quad (\Rightarrow x_1^3 = x_2^3)$$

$$x_1^3 - x_2^3 = 0 \Leftrightarrow (x_1 - x_2)(x_1^2 + x_1 x_2 + x_2^2) = 0 \Leftrightarrow \begin{cases} x_1 - x_2 = 0 \\ x_1^2 + x_1 x_2 + x_2^2 = 0 \end{cases}$$

$$x_1^2 + x_1 x_2 + x_2^2 = 0$$

$\Rightarrow$  feste  $l$  & injektiv ①

$$\text{Es sei } y \in \mathbb{R}, \Rightarrow x^3 - 2 = y \Leftrightarrow x^3 = y + 2 \Leftrightarrow x = \sqrt[3]{y+2} \in \mathbb{R}$$

sowie  $l(\sqrt[3]{y+2}) = y \Rightarrow l$  & injektiv. ②

zu 2

$\Rightarrow l$  & bijektiv

$$f) \text{ auf } \mathbb{R}, \text{ } m(x) = \begin{cases} x^2, x \leq 0 \\ -x, x > 0 \end{cases}$$

Es seien  $x, y \in \mathbb{R}$ ,  $m(x) = m(y)$

$$\cdot \text{Dazu } x, y \leq 0 \Rightarrow m(x) = m(y) \Leftrightarrow x^2 = y^2 \Leftrightarrow (x+y)(x-y) = 0 \Rightarrow x = y.$$

$$\cdot \text{Dazu } x, y > 0 \Rightarrow -x = -y \Leftrightarrow x = y.$$

$$\cdot \text{Dazu } x \leq 0 \text{ & } y > 0 \Rightarrow -x = y^2 \quad (\text{unmöglich})$$

$\Rightarrow m$  bij.

$\Rightarrow m$  injektiv ①

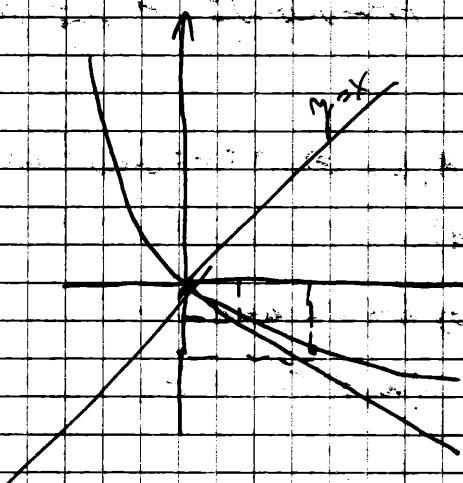
• Es sei  $y \in \mathbb{R}$

$$\cdot y \leq 0, x = -y \geq 0 \Rightarrow m(-y) = -(-y) = y$$

$\Rightarrow y$  min

$$\cdot y > 0, x = -y \not\geq 0 \Rightarrow x = -\sqrt{y} \leq 0 \Rightarrow m(-\sqrt{y}) = y$$

$$\text{Met 2} \quad \begin{array}{c} x \\ \hline -2 & -1 & 0 & 1 & 2 \end{array}$$



Obs: cardinal  $\aleph_0$  durch die  $\mathbb{Q} \cap \mathbb{R}$  auf  $\mathbb{R}$  abstrahieren  
ringen nach  $\rightarrow$  in bijektiv  $\rightarrow$

$$f: \mathbb{R} \rightarrow \mathbb{R}, f(x) = \begin{cases} -\sqrt{x}, & x \geq 0 \\ -x, & x < 0 \end{cases}$$

② Es existiert  $f: \mathbb{R} \rightarrow \mathbb{R}$ ,  $f(x) = \begin{cases} x+3, & x \neq 0 \\ x-3, & x=0 \end{cases}$

Ansatz:  $f$  bijig  $\Leftrightarrow$  det  $f^{-1}$ .

• Es seien  $x, y \in \mathbb{R}$  a.R.  $f(x) = f(y)$ .

$$-x, y \neq 0 \Rightarrow x+3 = y+3 \Rightarrow x = y$$

$$-x, y \neq 0 \Rightarrow x-3 = y-3 \Rightarrow x = y$$

$$-x, y \neq 0 \text{ dif } \Rightarrow x+3 = y-3 \Rightarrow x+6 = y \text{ (impossibilität)}$$

$(x \neq 0, y \neq 0)$

$\Rightarrow$  Fmng. ②

$$\begin{aligned} \bullet \text{ Es seien } y \in \mathbb{R} \text{ a.R. } \Rightarrow x-3 = y \Rightarrow x = y+3 \text{ a.R. } f(y+3) = y. & \Rightarrow \text{ Fmng. ③} \\ y \neq 0 \Rightarrow x+3 = y \Rightarrow x = y-3 \text{ a.R. } f(y-3) = y. & \end{aligned}$$

dim  $\rightarrow$   $\mathbb{R} \rightarrow \mathbb{R}$  bijig  $\Rightarrow$   $f$  und  $f^{-1}$  injektiv.

$$f^{-1}: \mathbb{R} \rightarrow \mathbb{R}, f^{-1}(x) = \begin{cases} x-3, & x \neq 0 \\ x+3, & x=0 \end{cases}$$

$$f = f^{-1}$$

TEMA: ① Es existiert  $f: \mathbb{R} \rightarrow \mathbb{R}$ ,  $f(x) = \begin{cases} x^2, & x \leq 0 \\ -2x, & x > 0 \end{cases}$

Ansatz:  $f$  bijig,  $\Leftrightarrow$  det  $f^{-1}$

$$\begin{aligned} \bullet \quad f: \mathbb{R} \rightarrow \mathbb{R}, f(x) = \begin{cases} 2x^2 + 7, & x \leq 0 \\ -x+7, & x > 0 \end{cases} \end{aligned}$$

• Construcția lui  $\tilde{\sim}$ . Fie  $\sim$  re.  $M \times N$   $\min(a,b) \cap (a,d)$  dorește  $a+d=b+c$ . Astăzi  $\sim$  este o rel. de echivalență și nu  $|N \times N|/n$  și identifică în mod natural  $\tilde{\sim}$ .

Pat: 1)  $\sim$  este reflexivă ( $\Rightarrow (a,b) \sim (a,b)$ ) ( $\Rightarrow a+b=a+b$ )  $\text{adm. b)$ , 1.1.1.

2)  $\sim$  este simetrică ( $\Rightarrow (a,b) \sim (c,d)$ )

$$a+d=b+c \Rightarrow b+c=a+d$$

$$(c,d) \sim (a,b)$$

3)  $\sim$  este transițivă:  $a+d=b+c \quad | \Rightarrow a+f=b+l$   
 $a+f=c+l$

1,2,3  $\rightarrow$   $\sim$  rel. de echivalență  $\Rightarrow$  Agenția bijectivă  $[(a,b)] \rightarrow a,b$

### • Construcția lui $\tilde{Q}$

Fie  $\sim$  rel. pe  $\mathbb{Z} \times \mathbb{N}^*$  definită  $(a,b) \sim (c,d)$  dorește  $a \cdot b = c \cdot d$

Astăzi  $\sim$  este o rel. de echivalență și nu  $\mathbb{Z} \times \mathbb{N}^*$  în același mod natural ca  $\tilde{\sim}$ .

### • Soluții:

1)  $\sim$  reflexivă:  $(a,b) \sim (a,b)$  ( $\Rightarrow a \cdot b = b \cdot a$ , adm. b)  $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$

2)  $\sim$  simetrică:  $(a,b) \sim (c,d) \Rightarrow a \cdot d = b \cdot c$  ( $\Rightarrow b \cdot c = a \cdot d \Rightarrow$ )

$$\Rightarrow (c,d) \sim (a,b)$$

3)  $\sim$  transițivă:  $(a,b) \sim (c,d) \quad | \quad a \cdot d = b \cdot c$   
 $(c,d) \sim (e,f) \quad | \quad c \cdot f = d \cdot e \quad | \Rightarrow a \cdot f = b \cdot e$

1,2,3  $\rightarrow$  rel. de echivalență  $\rightarrow$  Agenția bijectivă  $[(a,b)] \xrightarrow{f} \frac{a}{b} : \mathbb{Z} \times \mathbb{N}^* \rightarrow Q$

### • Construcția lui $R$

Fie  $C$  mult. cont.

Ie  $C$  nu este rel.  $\sim$  definită  $(a_n)_{n \geq 1} \sim (b_n)_{n \geq 1} \quad (\Rightarrow a_n - b_n \geq 1)$

$$(a_n - b_n) = 0.$$

A.  $\sim$  este o rel. de echivalență și  $\sim C_{(n)}$  reprezintă o mod naturală ca  $R$ . ( $a_n \sim b_n \Leftrightarrow \lim_{n \rightarrow \infty} (a_n - b_n) = 0$ ) Cauchy dicit.  $\forall K \geq 1$ ,

$$(7) N \in \mathbb{N}, N = N(K) > 1$$

• Soluție:

1)  $\sim$  reflexivă ( $\exists \lim_{n \rightarrow \infty} (a_n - a_n) = 0$ , A.)

2)  $\sim$  simetrică ( $\Rightarrow \lim_{n \rightarrow \infty} (a_n - b_n) = \lim_{n \rightarrow \infty} (b_n - a_n) = 0$ )

$$\lim_{n \rightarrow \infty} (a_n - b_n) = 0 \Rightarrow \lim_{n \rightarrow \infty} (b_n - a_n) = 0.$$

3)  $\sim$  transițivă  $\Rightarrow \lim_{n \rightarrow \infty} (a_n - b_n) = 0 \quad \Rightarrow \lim_{n \rightarrow \infty} (a_n - c_n) = 0$

$$\lim_{n \rightarrow \infty} (b_n - c_n) = 0$$

7, 2, 3  $\rightarrow$  rel. de echiv.  $\rightarrow$  avem bij  $[a_n]_{n \in \mathbb{N}} \rightarrow \lim_{n \rightarrow \infty} a_n : C_{(n)} \rightarrow R$ .

(-multimi primite Cauchy).

5.  $\ell_1 \cap \ell_2$  este că, doar că,  $\ell_1 \cap \ell_2$  sunt  $\sim$  rel. de echivalență pe  $X$ , atunci  $\ell_1 \cap \ell_2$  este o rel. de echivalență pe  $X$ .

• Sol:  $\ell_1 \cap \ell_2$  este reflexivă, simetrică, transițivă.

1) reflexivitate:  $\forall x \in X$ , avem  $\ell_1, \ell_2$  sunt reflexive  $\Rightarrow (x, x) \in \ell_1 \text{ și } (x, x) \in \ell_2$   
 $\Rightarrow (x, x) \in \ell_1 \cap \ell_2$ .

2) simetria: Fie  $x, y \in X$ , cu  $(x, y) \in \ell_1 \cap \ell_2 \Rightarrow \begin{cases} (x, y) \in \ell_1 \\ (x, y) \in \ell_2 \end{cases}$  simet.  
 $\Rightarrow (x, y) \in \ell_2$

$\Rightarrow \begin{cases} (y, x) \in \ell_1 \\ (y, x) \in \ell_2 \end{cases} \Rightarrow (y, x) \in \ell_1 \cap \ell_2$ .

3) transițivitate: Fie  $(x, y, z) \in \mathbb{Z}$  cu  $(x, y) \in \ell_1 \cap \ell_2$  și  $(y, z) \in \ell_1 \cap \ell_2 \Rightarrow$

$\Rightarrow \begin{cases} (x, y) \in \ell_1 & (y, z) \in \ell_1 \Rightarrow (x, z) \in \ell_1 \\ (x, y) \in \ell_2 & (y, z) \in \ell_2 \Rightarrow (x, z) \in \ell_2 \end{cases} \Rightarrow (x, z) \in \ell_1 \cap \ell_2$

Din 1, 2, 3  $\rightarrow$  liniile sunt de echivalență.

## LECTIA DIN 15.10.2019

### Relații binare - Aplicații

1. Fie  $x = \{1, 2, 3, 4\}$  și relația binară  $R = \{(2, 1), (2, 4), (3, 4)\}; 2 \neq \{(1, 2), (2, 2), (2, 3), (3, 4)\}$

Să se determine  $\text{Dom } R, \text{Dom } R^T, \text{Ran } R, \text{Ran } R^T, R^{-1}, R^{-1} \circ R^T, (R \circ R^T)^{-1}, (R^T \circ R)^{-1}$

$$\text{Dom } R = \{2, 3\}$$

$$\text{Ran } R = \{(1, 1), (2, 1), (2, 4), (3, 4)\}$$

$$\text{Dom } R^T = \{1, 2, 3\}$$

$$R^{-1} = \{(2, 1), (2, 2), (3, 2), (4, 3)\}$$

$$R^{-1} \circ R^T = \{(1, 1), (1, 2), (2, 2), (4, 1)\}$$

$$(R \circ R^T)^{-1} = \{(1, 1), (1, 2), (4, 2), (4, 1)\}$$

2. Fie  $E = \{1, 2, 3, 4, 5\}$  def. rel. binară  $R = \{(x, y) \mid x \in E, y \in E, x \neq y\}$ .

Soluție:

$$R = \{(1, 2), (1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)\}$$

$$R^{-1} = \{(2, 1), (3, 1), (4, 1), (5, 1), (3, 2), (4, 2), (5, 2), (4, 3), (5, 3), (5, 4)\}$$

### Relații de echivalență

Fie „ $\sim$ ” o relație de echivalență pe mulțimea  $A$ .

Dacă  $a \in A$  mult.  $[a] = \{b \in A \mid b \sim a\}$  numită clasa de echivalență a elementelor  $A$ .

Mulțimea claselor de echivalență se numește mulțimea factorilor  $G$  sau  $A/N$ . și se notează  $A/N$ .

Dacă  $A/N = \{[a] \mid a \in A\}$ , subiectia  $\pi(A) = [a]$  se numește subiectul canonice.

Analog nu relația con-

## Aplicații. Relații de ordine

- O rel. binară ( $\text{rel } X$ ) se numește rel. de ordine ( $\text{rel } X$ ) dacă are următoarele proprietăți:

i) reflexivă ( $\Rightarrow x \sim x$ ,  $\forall x \in X$ ).

ii) transițivă ( $\Rightarrow x \sim y \wedge y \sim z \Rightarrow x \sim z$ ,  $\forall x, y, z \in X$ ).

iii) antisimetrică ( $\Rightarrow x \sim y \wedge y \sim x \Rightarrow x = y$ ).

- O mulțime  $X$  se numește def. o rel. de ordine  $\leq$  nu este altă decât  $(X, \leq)$  și este numită mulțime ordonată.

- În  $(X, \leq)$  o mulțime ordonată, un element  $x_0$  se zice:

- cel mai scurt (mai trivial) el. al mulțimii  $X$ , dacă  $x_0 \leq x$ ,  $\forall x \in X$ .

- elem. maximul al mulțimii  $X$ , dacă s.t.  $(\forall x \in X) x \leq x_0$ , atunci

$$x = x_0$$

- cel mai mare (ulterior) elem. al mulțimii  $X$ , dacă  $x \leq x_0$ ,  $\forall x \in X$ .

- elem. minimul al mulțimii  $X$ , dacă s.t.  $(\forall x \in X) x \leq x_0$  și  $x_0 \leq x$  atunci  $x = x_0$ .

## Aplicații

- În  $X = \{\langle 1 \rangle, \langle 1, 2 \rangle, \langle 2, 3, 4 \rangle, \langle 6 \rangle\}$  ord. nu este inclusivă. De ce? Este mulțimea maximală și/ sau minimală?

Sol: - El. minimal:  $\{\langle 1 \rangle, \langle 2, 3, 4 \rangle, \langle 6 \rangle\}$ .

$\{\langle 1 \rangle\}$  este el. minimal al lui  $X$  deoarece nu poate fi superset al altui element  $A \in X$  (d.e.  $A \subset \{\langle 1 \rangle\}$  este chiar  $A = \{\langle 1 \rangle\}$ ).

- El. maximal:  $\{\langle 1, 2 \rangle, \langle 2, 3, 4 \rangle, \langle 6 \rangle\}$ .

- Dacă  $X$  ar avea un element maximal, acesta ar trebui să fie și  $\{\langle 1, 2, 3, 4, 6 \rangle\} \subset A$  (reacum nu ar fi tot  $\{\langle 1 \rangle\} \subset X$ ).

(2) Dati exemplu de o mult. ordonată care are elemente minimale  
dorim să arătăm că este fals.

Sol: Fie  $X = \{\langle 1 \rangle; \langle 2 \rangle; \langle 1, 3 \rangle; \langle 1, 4 \rangle\}$  o mult. ordonată prin inclusiune.  
- El. minimal:  $\langle 1 \rangle$

$A \langle 1 \rangle$  este el. minimal al. mult.  $X$ , dacă  $X$  are un c. min. element. Intr-adevăr, dacă  $B \in X$  este c. min. element, at.

$B \subset A \Rightarrow \emptyset$  și  $B \in X \Rightarrow B \neq \emptyset \in X$  contradicție!  
 $A \in X$

(3) Dati exemplu de o mult. ordonată care nu este el. mult. dorim  
să arătăm că nu există.

Fie  $X = \{\langle 1, 3 \rangle; \langle 2 \rangle; \langle 2, 5 \rangle; \langle 1, 6 \rangle\}$  nu este o mult. ord. min. inclusiune.  
 $A = \langle 2, 5 \rangle$  este un el. maximal, dacă  $X$  nu ar fi un c. max. el.  
Intr-adevăr, dacă  $B \in X$  este c. max. el., at.  $B \supset \bigcup_{A \in X} A =$   
 $= \langle 1, 2, 5, 6 \rangle$  și  $B \in X \rightarrow$  contradicție!

(4) Dati ex. de o rel. de ordinare  $\mathcal{S}$  pe  $N$  a.s.  $(N, \mathcal{S})$  este o latire  
care nu este completă.

Sol: ! Def: O mult. ord.  $(A, \leq)$  se numește "latice" dacă  $\forall a, b \in A$

$(\exists)$  superiorul și inferiorul.

Notă:  $a \vee b$ , num  $\text{sg}(a, b)$

$a \wedge b$ , inf  $\{a, b\}$

Evident: O mult. total. ord. este o latire

$\mathcal{S}$  total ( $\Rightarrow \forall x, y \in \mathcal{S}$  avem  $x \leq y$  sau  $y \leq x$ ).

O latire  $A$  se numește completă, dacă dizează mult. nereido  
a lui  $A$  ord. imp. și inf. în  $A$ .

Eex. rel. de divizibilitate pe  $N$ :  $"|"$  (este r. de ordinare pe  
 $N$  nu verif. imediat)

$(N, \leq)$  este o latire ( $\Leftrightarrow$  pt.  $a, b \in N$  există:

$$(\text{num}): a \vee b = (a, b) \quad (\text{c. s. m. d. c.})$$

$$(\text{inf}): a \wedge b = [a, b] \quad (\text{c. m. m. d. c.})$$

Incompletitudini  $(N, \leq)$  rezultă, de exemplu, din următoarele:

$2, 3, \dots, 2^n, \dots$  nu au număr maxim. Acestea sunt bune și nu există decât totale, deci contradicție.

Teorema

① Se  $R$ , def. rel. binară  $\varnothing \neq R \subseteq X \times Y$  și  $x, y \in X$ .

$\Rightarrow$   $\exists x$  astfel încât  $R$  este o rel. de ordine totală.

② Se vrea stabili o fct.  $f$  def. pe  $A = \{4, 5, 6, 7\}$  cu valori în  $B = \{2, 3, 5, 7\}$  date de figura,  $f(x)$  nu dă o liniă  $x^f$ ?

③ Dati exemple de o rel. de ordine pe  $\mathbb{R}^+$  care nu este totală și nu este ordonată.

### B) Aplicații. Legi de compozitie

④ Se vrea să se studieze dacă urm. operații sunt operații algebrice (= legi de comp.).

a)  $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $(x, y) \rightarrow \text{c.m.m. d.c. } (x, y)$

b)  $N \times N \rightarrow N$ ,  $(x, y) \rightarrow \text{c.m.m. d.c. } (x, y)$

c)  $n^{\frac{m}{n}} : Q \times Q \rightarrow Q$ ,  $(\frac{m}{n}, \frac{p}{q}) \rightarrow \frac{m \cdot p}{n \cdot q}$

d)  $Q \times Q \rightarrow Q$ ,  $(\frac{m}{n}, \frac{p}{q}) \rightarrow \frac{m \cdot p}{n \cdot q}$

e)  $n^{\frac{m+p}{n}} : Q \times Q \rightarrow Q$ ,  $(\frac{m}{n}, \frac{p}{q}) \rightarrow \frac{m+q}{n \cdot q}$

a) Nu e o fct. ( $\Rightarrow$  nu sunt o op. algebrică și nu este c.m.m.d.c. și c.m.m.). Dintre legi care sunt bine determinate. Astfel,  $n^{\frac{m}{n}} \in \{-1, 0\}$  și astăzi  $n \in \mathbb{Z} \setminus \{-1, 0\}$ .

b) Este o op. algebraică în  $\mathbb{N}$  deoarece c.m.m.d. al oricărui  
paire și un număr este un număr natural. Vînă determinat

c) Este o op. algebraică în  $\mathbb{Q}$  și o operare de înmulțire a nr.  
rationale

d) nu este o op. deoarece  $(\frac{2}{3}, \frac{9}{7})$  din  $\mathbb{Q} \times \mathbb{Q}$  nu are reciproc.

$$\frac{2}{3} \text{ nu este } q.$$

e) Nu este o op. algebraică în  $\mathbb{Q}$ .

Indată că, fie  $\frac{7}{2} * \frac{3}{4} = \frac{7+3}{2 \cdot 4} = \frac{4}{8} = \frac{7}{2}$ .

Dar  $\frac{7}{2} = \frac{3}{4} \Rightarrow \frac{7}{2} * \frac{3}{4} = \frac{3}{4} * \frac{3}{4} = \frac{2+3}{4 \cdot 4} = \frac{5}{16}$ .

$\Rightarrow \frac{7}{2} \neq \frac{5}{16}$  (contradicție)

! Există astfel de situații greșite din faptul că elev. lui  
 $q$  sunt slabe de echivalență, iar operația „\*” care a fost  
def. ca fiind o mulțime reg., algebraică și, în loc să aibă de  
echivalență, trebuie să verifice  $(1,2) \in \mathbb{Q} \times \mathbb{Q}$ , deoarece de  
algebrele sunt reprezentante.

Teorema

✓ ① Num. nr. nr. op. algebraice în  $\mathbb{N}$ .

a)  $x * y = x + y$

b)  $x * y = x$

c)  $x * y = xy + 7$

d)  $-m - = 0$

e)  $-m - = \min(x, y)$

Ieziile deasupra sunt asociative, comutative, sau elev. neutru.

☒ ② Dati ex. de op. algebraice care nu sunt nici unele dintre  
aceste, și de ex. o cl. neutră nu independentă (Indicați răspuns)  
1)

7. a) - asociativitate:  $(x * y) * z = x * (y * z)$ ,  $\forall x, y \in N$ .

$$(x * y) * z = (x + y) * z = x + y + z = x + z \quad \Rightarrow x * (y * z) \neq (x * y) * z$$

$$x * (y * z) = x + y + z$$

"\*" nu este asociativă

- comutativitate:  $x * y = y * x$ ,  $\forall x, y \in N$

$$x * y = x + y$$

$$y * x = y + x$$

$$\Rightarrow x * y \neq y * x, \forall x, y \in N.$$

"\*" nu este comutativă

- el. neutru:  $\ell * x = x * \ell = x$ ,  $\forall x \in N$ ,  $(\exists) \ell \in N$  unic.

$$\ell * x = \ell + x$$

$$x * \ell = x + \ell$$

$\Rightarrow$  "\*" nu are el. neutru.

29.10.2019.

### Aplikatii - legi de compozitie

1. Fie  $M$  o multime cu  $m$  el.,  $\forall x \in M$  sunt det m. legile de compozitie care sunt fi det pe  $N$ .

$$\text{sol: } |M| = m, m \in \mathbb{N}^*$$

A def o l.c. pe  $M$  astfel incat lucru pe o combinație funcțională.

$$f: M \times M \rightarrow M$$

$$\text{Avem } |M| = m \Rightarrow |M \times M| = m^2 \Rightarrow m^2 \text{ moduri.}$$

2. Fie  $M$  o multime numarabilă,  $m \in \mathbb{N}^*$ . Să se det.

a) Nr. legile de compozitie care sunt fi det pe  $N$ .

b) Nr. legile de compozitie care sunt el. neutru și sunt fi det pe  $N$ .

$$\text{sol: a) Notăm } M = \{x_1, x_2, \dots, x_m\}$$

A da o legătura între numărul de legile de compozitie și numărul elementelor.

$$\text{a) fct } f: M \times M \rightarrow M \text{ cu } f(x, y) = f(y, x) \text{ pt } x, y \in M.$$

$$\text{Dacă avem } n \text{ elemente în } M \text{ atunci avem } n \times n \text{ moduri de a combina elementele.}$$

$$\frac{n(n+1)}{2} \text{ elemente.}$$

$$\Rightarrow \text{nr. cardinat } M \geq \frac{n(n+1)}{2}$$

b) Dacă  $\forall m \in M$ , at.  $\exists i \in M$  astfel încât  $m = f(i)$ . Avem pl. urm. ( $\Rightarrow$ )

cu o construcție a funcției  $f: M \times M \rightarrow M$  cu  $f(x, i) = f(i, x) = x$ ,  $\forall x \in M$ .

Aceasta este analogie la un lucru similar de cardinalitate  $\{f(x, y) \mid x, y \in M\} \subseteq M$ .

$$\Rightarrow M \text{ are o reprezentare formală } n^{(n-1)^2} = n^{n^2 - 2n + 1}$$

Dacă suntem el. nr. mult.  $M$  trebuie să avem ca el. mult. și reprezentare formală  $n^2 - 2n + 1$ .  
 Această reprezentare formală este  $n^2 - 2n + 1 = \boxed{n^2 - 2n + 2}$  număr logic de cardinalitate.

$\forall M$ .

3. Fie  $M$  o mulțime cu  $m$  el.,  $m \in N^*$ . Vom da def. nr. logici de cardinalitate.

El.  $a$  este fiabil în  $M$  dacă și numai dacă există elementele  $b_1, b_2, \dots, b_m$

Totodată sunt de probă astăzi, deducem că nu există  $a$ :

$$n^{\frac{2(m-1)}{2}} \quad (\text{nu există nr. logici de cardinalitate } m \text{ care să aducre el. mult. } m)$$

el. fiind cel din  $M$ ) fiind de la noi, indicat  $m \cdot n^{\frac{2(m-1)}{2}} = m^{\frac{2(m-1)+2}{2}}$

## TEMA

### 7) Mată + Info (Funcții permutații)

Fie  $a, b \in N$ ;  $A = \{1, 2, \dots, a\}$ ;  $B = \{1, 2, \dots, b\}$ . Prob. diferențială sau

a) Nr. de funcții de la  $A$  la  $B$  sunt  $b^a$ .

b) Dacă  $a \leq b$ , at. nr.  $N_s$  al injectiilor (funcții inj.) de la  $A$  la  $B$ .

$$\text{Este } A^a = \frac{b!}{(b-a)!}$$

În particular, nr. permutații sunt numai el. nr.:  $n!$

c) Dacă  $a > b$ , nr.  $N_s$  al surjectiilor de la  $A$  la  $B$  este

$$b^a - C_b^1 (b-1)^{a-1} + C_b^2 (b-2)^{a-2} + \dots + (-1)^{b-a} C_b^{b-a}$$

d) Dacă  $a < b$ , nr.  $N_s$  al funcțiilor surjective de la  $A$  la  $B$  este:  $C_a^b$

e) Nr.  $N_c$  al funcțiilor surjective de la  $A$  la  $B$  este  $C_{a+b-1}^a$ .

✓ 2) se cere un program care:

M<sub>n</sub>-V

✓ a) să rezolve toate f(x) cuj det nu A nu valim B (tab. de rezolvare)

✓ b) să rezolve cu m=2 cuj f:A→B (obi: tab. de rezolvare)

✓ c) să rezolve f(x) cuj f:A→B + cuj

✓ d) să rezolve f(x) cuj f:A→B.

✓ e) să rezolve f(x) cuj f:A→B (Borkhovski / rezolvare)

✓ (2) Dacă  $m \geq 1$ , fil  $P(1)$  nu are rezoluții pozitive  $c = m$  și urmărește

$m$ . fil  $P$  nu are rezoluții pozitive (fie Euler). Astfel că  $P_m =$

$$= m \left(1 - \frac{1}{n_1}\right) \left(1 - \frac{1}{n_2}\right) \dots \left(1 - \frac{1}{n_m}\right),$$
 unde  $n_1, n_2, \dots, n_m$  sunt factorii

primi ai lui  $m$ .

Există totuși oare  $m \in N^*$  astfel încât să fie totuși rezolvabile  
prin fizi Euler.

Ex:  $m = 24$  (obi)  $\Rightarrow 1 = 2^3 \cdot 3.$   $\left\{ \begin{array}{l} n_1 = 2 \\ [m/n_1, \dots, n_m] \\ n_2 = 3. \end{array} \right.$

$$P(1) = 24 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 24 \cdot \frac{1}{2} \cdot \frac{2}{3} = \frac{24}{3} = 8.$$

$$P(24) = \{5, 7, 11, 13, 17, 19, 23\} = 8 \text{ (An. Euler).}$$

✓ (3) Se cere un program care să mulțime  $M_m$  să se dă:

✓ a) fil. rezolvare cu jocul det nu M.

✓ b)  $m$  - rezolvare corect  $\rightarrow m -$

✓ c)  $m$  - rezolvare el. neutrală  $\rightarrow m -$

✓ d)  $m$  - rezolvare corect și cu el. neutral  $\rightarrow m -$

✓ (4) Se cere un progr. ce calculează rezolvările.

$$T_m = C_{m-1}^{m-1} / m$$

- nr. de rezolvări care nu pot fi rezolvate după cum  
rezolvării de la 1...m.

Denumire:  $T_2$  este  $T_1 T_{m-1} + T_2 T_{m-2} + \dots + T_{m-1} T_1$

## Abrindă monoid

### Submonoid

Dacă  $(M, *)$  este monoid în el-sentințe și  $H$  o submulțime a lui  $M$ , atunci  $(H, *)$  este un submonoid al lui  $(M, *)$ . Dacă:

1)  $H$  este stabilită cu privire la  $M$ .

2)  $\emptyset \in H$ .

### Morfism de monoid

Fie  $(M, \cdot)$  și  $(M', \cdot')$  două monoizi având el-sentințe și să se verifice:

Fie o aplicație  $f: M \rightarrow M'$  cu proprietatea:

1)  $f(x \cdot y) = f(x) \cdot' f(y)$  ,  $\forall x, y \in M$

2)  $f(1) = 1'$  o.m. monoid de numere.

O astfel de monoid  $f: (M, \cdot) \rightarrow (M', \cdot')$  se numește isomorfism d.d.

un morfism bijectiv. Notăm:  $M \cong M'$

### Aplicații:

1. Aflat că  $I(X) = \{f | f: X \rightarrow X\}$ , unde  $X$  este multime nevidată. Șă se arate că  $(I(X), \circ)$  este un monoid

Sol: Dacă  $f, g: X \rightarrow X$  sunt funcții, at.  $f \circ g$  este o funcție, atunci  $I(X)$  este stabilită în rap. cu comp. pt.

" $\circ$ " este orel. și ca el-sentință  $1_X \in I(X)$ :  $f \circ 1_X = f$ ,  $1 \circ f = f$ ,  $\forall f \in I(X)$

Prin urmare  $(I(X), \circ)$  monoid.

2. Șă se arate că:

a)  $(P(M), \cup)$  și  $(P(M), \cap)$  sunt monoizi

b)  $(P(M), \cup) \cong (P(M), \cap)$

Sol: a)  $\cup$  și  $\cap$  sunt op. algebraice monoidale, iar  $E = \emptyset$ ,  $m_n$ ,  $E = M$  sunt el-sentințe. Deși  $(P(M), \cup)$  nu este  $(P(M), \cap)$ , deci cele două sunt monoizi.

b)  $f: (P(M), \cap) \rightarrow (P(M), \cup)$ ,  $f(x) = C(x)$  și  $f(x \cap y) = C(x \cap y) = C(x) \cup C(y) = f(x) \cup f(y)$  ①

$$\textcircled{2} \quad f(m) = c(m) \Rightarrow \xrightarrow{\text{def}} f \text{ bijzi zwert} \Rightarrow (P(M), \cap) \text{ is zw. } (P(M), \cup)$$

FEMA

$$? \quad ?$$

$$\text{1. Dl } R \text{ re. cons. leg. de comp. } "0" \quad x \circ y = \sqrt{x^5 + y^5}.$$

a)  $\exists \circ_R$  măreță în  $(R, \circ)$  monoid comutativ.

b)  $\exists \circ_R$  măreță în  $U(R) = R$ .

c)  $\exists \circ_R$  măreță și. de ex.  $\begin{cases} x \circ y, \circ(-2) = y \\ x^5 + 3y = y^5 \end{cases}$

$$\textcircled{2} \quad \text{Fie } M = \left\{ \begin{pmatrix} \gamma - x & 0 & x \\ 0 & 0 & 0 \\ x & 0 & \gamma - x \end{pmatrix} \mid x \in \mathbb{R} \right\}$$

a)  $\exists \circ_M$  măreță în  $(M, \cdot)$  monoid comut

b)  $\exists \circ_M$  det  $U(M)$ .

$$\text{a)} \quad \begin{pmatrix} \gamma - x & 0 & x \\ 0 & 0 & 0 \\ x & 0 & \gamma - x \end{pmatrix} \begin{pmatrix} \gamma - l & 0 & l \\ 0 & 0 & 0 \\ l & 0 & \gamma - l \end{pmatrix} = \begin{pmatrix} (\gamma - x)(\gamma - l) + xl & 0 & l(\gamma - x) - x(\gamma - l) \\ 0 & 0 & 0 \\ x(\gamma - l) + l(\gamma - x) & 0 & xl + (x - l)(\gamma - l) \end{pmatrix}$$

$$xl + (\gamma - x)(\gamma - l) = \gamma - x \rightarrow l = 0$$

$$x(\gamma - l) + l(\gamma - x) = x \rightarrow l = 0.$$

Aplikatii - Exercizi

5. 11. 2013

Ex. de grupuri: 1)  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  grup. abeliene cu prop. cu +.

2)  $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$  grup. abeliene în prop. cu  $\cdot$  (inversul)

3)  $\mathbb{Z}_{\geq 22}, \mathbb{Z}_n = \{0, 1, \dots, n-1\}$  grup. cu prop. cu +.

(mult. celor de resturi modul n)

~~$\leftrightarrow U(\mathbb{Z}_n) = \{x \mid x \in \mathbb{Z}, (x, n) = 1\}$~~  grup. fără div.  
Inversi.

4) Fie  $M$  o mulț. Mult.  $S(M) = \{f: M \rightarrow M \mid f \text{ bij}\}$  formătoare de  
o fn. cu prop. care să grupă mulț.  $\rightarrow M$ .

5) S.  $\Rightarrow$  isometriile a măsurii Euclidiană  $\mathbb{R}^2 \rightarrow$  lipsă (fiecare)

$f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$  care nu preseră distanța, adică  $d(f(x), f(y)) = d(x, y)$

L distanță

$(P, Q \in \mathbb{R})$  unde  $d((x_1, y_1); (x_2, y_2)) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$

Mult, isometriile izom.  $(\mathbb{R})$  sunt un grup. Față de corespond.

Prop 2.  $\boxed{H \subseteq G}$  un grup  $G$  și  $H \subseteq G$  u.a.r.l.:

Subgrup

al lui  $G$

a)  $H \subseteq G$ :

b)  $x \in H, y \in H \Rightarrow xy^{-1} \in H$  și  $x \in H \Rightarrow x^{-1} \in H$ .

c)  $x, y \in H \Rightarrow xy^{-1} \in H$ .

Prop 3. Subgrup al lui  $G$  o.m. subgrup normal al lui  $G$  dacă

$(\forall) x \in G$  și pentru orice  $x^{-1} \in H$

Nat  $\boxed{H \trianglelefteq G} \rightarrow subgrup normal al lui  $G$ :$

Aplicații

cp. metric. (spatiu metric)

① Zil  $(X, d)$  un sp. metric, iorz; izom  $X = \{f \in GS(X)\}$

$d(f(x), f(y)) = d(x, y) \quad (\forall) x, y \in X$

toate zile izom  $X \subseteq S(X)$ .

Zol: 1) Evident  $\forall x \in S_{\text{izom}}(X)$  || ordine b)

2) Zil  $f, g \in S_{\text{izom}}(X)$  și  $x, y \in X$ .

Amen  $d(f \circ g(x), f \circ g(y)) = d(f(g(x)), f(g(y))) = d(g(x), g(y))$

$= d(x, y) \Rightarrow f \circ g \in S_{\text{izom}}(X)$ .

3)  $f^{-1} \in D_{\text{dom}}(X)$  decouere:  $d(f^{-1}(x), f^{-1}(y)) = d(f(f^{-1}(x)), f(f^{-1}(y))) = d(x, y)$ .

$\underline{(1)(2)(3)} \Rightarrow D_{\text{dom}}(X) \subseteq S(X)$ .

(2) Fie  $(X, d)$  un spatiu metric,  $y \in X$  iar  $S_X(Y) = \{f \in D_{\text{dom}}(X) \mid f(y) = y\}$

grupul de simetrie al lui  $y$  în raport cu  $X$

șă se arate că  $S_X(Y) \subseteq D_{\text{dom}}(X)$ .

Sol: Fie  $t, \gamma \in S_X(Y)$ , adică  $f(\gamma) = g(\gamma) = \gamma$ .

Astăzi  $(f \circ g^{-1})(\gamma) = f(g^{-1}(\gamma)) = f(\gamma) = \gamma$ , adică  $\gamma$  este abilă ca  $f \circ g^{-1} \in S_X(Y)$ .

$\Rightarrow S_X(Y) \subseteq D_{\text{dom}}(X)$ .

### T.E.M.A

① De mult,  $M$  nu cons. legăt. de comp.:  $M \times M \rightarrow M$ ,  $(x, y) \mapsto x \circ y$ .

șă se studieze dacă  $(M, \circ)$  este un grup în sensul.

$$a) M=2, \quad x \circ y = x+y+3$$

$$b) M=\mathbb{R}, \quad x \circ y = xy - 10x - 10y + 710$$

$$c) M=\mathbb{C}, \quad x \circ y = ix y.$$

③ Fie  $(G, \cdot)$  un grup și  $H$  subsp. finită a lui  $G$ . să se arate că  $H$  este subgrup a lui  $G$  d.d. (⇒). H este multe stabilită a lui  $G$ .

Sol: Dacă nu subsp. finită  $H$  a lui  $G$  este multe stabilită.

Fie  $h \in H$ , atunci  $\{h^n \mid n \in \mathbb{N}^*\} \subset H$  și cum  $H$  finită  $\Rightarrow$

$\Rightarrow \exists i, j \leq n$  cu  $i \neq j$ , adică  $h^{i-j} = e$  (el. neutru al lui  $G$ )

$\Rightarrow h \in H$ . De asemenea, dacă  $h \neq e$ , ct.  $j-i > 1$  și cu  $h^{-j} =$

$$= h^{j-i-1} \in H \Rightarrow H$$
 subgrup.

④ Fie  $A \in \mathbb{R}^{n \times n}$ ,  $\exists \epsilon \in \mathbb{R}, \epsilon > 0$

Not  $GL_n(A) = \{M \in M_n(A) \mid \det(M) \in U(A^*)\}$ .

$$SL_n(A) = \{M \in M_n(A) \mid \det(M) = 1\}$$

Zădăcă cu  $GL_n(A)$  este grupul de similituuri subînălțări.

$$SL_n(A) \triangleq GL_n(A)$$

(subgr. normal)

Def:  $GL_n(A)$  - grup. matrice general | de grad  $\Rightarrow$  grup

$SL_n(A)$  - grup. special | include  $A$ .

Sol: Dacă  $M, N \in GL_n(A) \Rightarrow \det(M), \det(N) \in U(A^*)$

Lăsată.

Avem  $\det(M \cdot N) = \det(M) \cdot \det(N) \Rightarrow M \cdot N \in GL_n(A)$ .

Evident  $I_n \in GL_n(A)$ , iar dacă  $M \in GL_n(A)$  avem  $\det(M^{-1}) = \det(M)^{-1} \Rightarrow \det(M^{-1}) \in U(A^*) \Rightarrow M^{-1} \in GL_n(A)$ .

$\Rightarrow GL_n(A)$  ) grup.

7) Folosim def. subgrupului normal.

Dacă  $M, N \in SL_n(A) \Rightarrow \det(M) = \det(N) = 1$ . și deoarece  $\det(MN^{-1}) = \det(M) \cdot (\det(N))^{-1} = 1 \cdot 1^{-1} = 1$ .

$\Rightarrow MN^{-1} \in SL_n(A) \Rightarrow SL_n(A) \triangleq GL_n(A)$ .

5) Dacă  $H, K$  sunt grupuri măritări  $\underbrace{H \times \{z\}}_{(x,z)} \triangleq \underbrace{H \times K}_{(x,y), (x_0y, z_0k)}$ .

Sol: Fie  $(x, z) \in H \times \{z\}$  și  $(y, z) \in H \times K$ , cu  $x, y \in H$  și  $z \in K$ .

Atunci  $(y, z)^{-1}(x, z) = (y^{-1}, z^{-1})(x, z)(z, z) =$

$$= (y^{-1}x, z^{-1}z) = (y^{-1}x, z) \in H \times K.$$

- Eguri, subeguri

- Exemple de morfism de grupuri

- E.M.A { 1)  $f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$ ,  $f(n) = 2^n$  este morfism de grupuri.

2)  $\varphi: (\mathbb{R}, +) \rightarrow ((0, \infty), \cdot)$ ,  $\varphi(x) = e^x$  izomorfism

TEMA ① Se cere să se arate că  $(\mathbb{R}, +)$  și  $(\mathbb{R} \setminus \{0\}, \cdot)$  sunt isomorfe prin  $\varphi(x) = e^x$ .

$$f(\mathbb{R}) = (0, \infty) \rightarrow (-1, 1)$$

Sol: Bij:  $f: (0, \infty) \rightarrow (-1, 1)$ ,  $f(x) = \frac{x-1}{x+1}$  verifică condiția.

$$f(x\gamma) = f(x) * f(\gamma) \Rightarrow \frac{x-1}{x+1} * \frac{\gamma-1}{\gamma+1} = \frac{\frac{x-1}{x+1} + \frac{2-\gamma}{\gamma+1}}{1 + \frac{(x-1)(\gamma-1)}{(x+1)(\gamma+1)}} = \frac{\frac{(x-1)(\gamma+1) + (2-\gamma)(x+1)}{(x+1)(\gamma+1)}}{\frac{(x+1)(\gamma-1) + (x-1)(\gamma+1)}{(x+1)(\gamma+1)}}$$

Bet: rezolvare similară (1 din 30%).

Aleatori - ordinele unui elem. anticiclic grup.

- Fie  $G$  un grup. Notăm  $\text{ord}(G)$  sau  $|G|$ .

- Ns. elem. grup  $\mathbb{Z}_n$ , dacă  $G$  are ns. finit de elemente și nu

ns.  $\text{ord}(G) = +\infty$  dacă  $G$  are s. infinit de elemente

.  $\forall x \in G$ , def ordinele lui  $x$ , minimul  $\{m \in \mathbb{N}^*, |x^m| = 1\} = l$ .

În caz general,  $\text{ord } x = +\infty$

. Dacă  $G$  nu este finit, at.  $\forall x \in G \setminus \{1\}$ ,  $\text{ord}(x) / |G| \cdot (\text{ord } G)$ .

② Fie  $G$  un grup, i.e.  $x, y \in G$ . Se cere să se arate că  $\text{ord}(xy) = \text{ord}(yx)$  și  $\text{ord}(x) = \text{ord}(x^{-1})$ .

Sol: Deoarece  $x^{-1}(yx)x = yx$ , deoarece există  $\forall m \in \mathbb{N}^*$ ,

$x^{-1}(xy)^m x = (yx)^m \Rightarrow (yx)^m = 1 \Rightarrow \text{ord}(xy) = \text{ord}(yx)$ .

Întotdeauna  $\text{ord}(x) = \text{ord}(x^{-1})$ .  $\Rightarrow$  (dini echivalență)  $x^k = 1 \Leftrightarrow x^{-k} = 1$ ,

$\forall k \in \mathbb{N}$ .

(2) Fie  $G$  un grup și  $(x, y) \in G$  cu  $\text{ord}(x), \text{ord}(y)$  finite și orice  
entă ele, iar  $yx = xy$ . să se arate că  $\text{ord}(xy) = \text{ord}(x) \cdot \text{ord}(y)$ .  
Sol: Fie  $\text{ord}(x) = m_1$ ,  $\text{ord}(y) = m_2$ ,  $(m_1, m_2) = 1$ .  
Avem  $(xy)^{m_1 m_2} = x^{m_1 m_2} \cdot y^{m_1 m_2} = (x^{m_1})^{m_2} \cdot (y^{m_1})^{m_2}$

Fie acum  $n \in \mathbb{N}$  s.t.  $(xy)^n = 1$ , atunci  $x^n = y^{-n}$  și  $x^n =$   
 $= (y^{m_2})^{-n} = 1 \Rightarrow m_1 | n \cdot m_2$  și cum  $(m_1, m_2) = 1 \Rightarrow m_1 | n$ .

Analog  $\Rightarrow m_2 | n$ .

(1) și (2)  $\Rightarrow m_1 m_2 | n$ . Am obținut echivalența  $(xy)^n = 1 \Leftrightarrow$   
 $\Leftrightarrow m_1 m_2 | n \Leftrightarrow \text{ord}(xy) = m_1 m_2 = \text{ord}(x) \cdot \text{ord}(y)$ .

(3) să se determine subgrupurile lui  $\mathbb{Z}_{m_1}, \mathbb{Z}_{m_2}$ .

Apliicatii nt  $\mathbb{Z}_d$ .

Sol: Fie  $n$  un m.e.z.f. și fiindcă grupul abelian, orice  
subgrup  $H$  al  $\mathbb{Z}_n$  este subgrup normal al  $\mathbb{Z}_n$ .

Dacă  $\mathbb{Z}_n = \mathbb{Z} / m\mathbb{Z}$  ord  $m$ , conform Teoreme de corespondență,  
toate subgrupurile lui  $\mathbb{Z}_n$  sunt de forma  $H / m\mathbb{Z}$ ,  $H$  subgrup al lui  $\mathbb{Z}$   
 $\hookrightarrow$  (factorizat)

care conține  $m\mathbb{Z}$ .

Triv arătă  $H$  este de forma  $d\mathbb{Z}$   $\forall d \in \mathbb{N}$  cu  $d | n$ .

!! Dacă, orice subgrup al lui  $\mathbb{Z}_n$  este de forma  $d\mathbb{Z} / m\mathbb{Z}$ , unde  $d$  este  
un div matrelui al lui  $m$ .

Conform relației de izomorfism  $\mathbb{Z}_n \cong \mathbb{Z} / m\mathbb{Z}$

$$\begin{aligned} \mathbb{Z}_n / (d\mathbb{Z} / m\mathbb{Z}) &= (\mathbb{Z} / d\mathbb{Z}) / (\mathbb{Z} / m\mathbb{Z}) \cong \mathbb{Z} / d\mathbb{Z} \text{ și deci } |\mathbb{Z} / d\mathbb{Z}| = \\ &= |\mathbb{Z}_n| / |d\mathbb{Z} / m\mathbb{Z}| = m / |d\mathbb{Z} / m\mathbb{Z}| \Rightarrow |d\mathbb{Z} / m\mathbb{Z}| = \frac{m}{d}. \end{aligned}$$

Subgrupuri:  $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ .

Divizori mat. ai lui 6 sunt: 1, 2, 3, 6.

Subgrupuri reziduale sunt:  $72/6^2 = \mathbb{Z}_6$ . [clasa lui 2]

$$72/6^2 = \{0, 1, 2\} = \{1\}$$

$$3^2/6^2 = \{0, 1, 2\} = \{1\} \text{ - clasa lui 3}$$

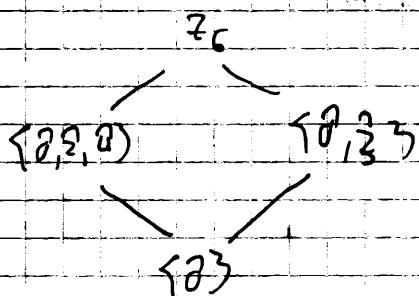
$$6^2/6^2 = \{0\}$$

Ob. Notam  $L_G$  familia subgrupurilor lui grup  $G$ , astfel

$(L(G), \subseteq)$  este cea mai

inclusivitate.

Astfel, subgrupuri ale  $\mathbb{Z}_6$  sunt:



(4) Cerintă subgrupurile lui  $\mathbb{Z}_{12}$ .

[Inversor de rezolvare -

$$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

Div. mat ai lui 12: 1, 2, 3, 4, 6, 12

Subgr. reziduale:  $72/12^2 = \mathbb{Z}_{12}$

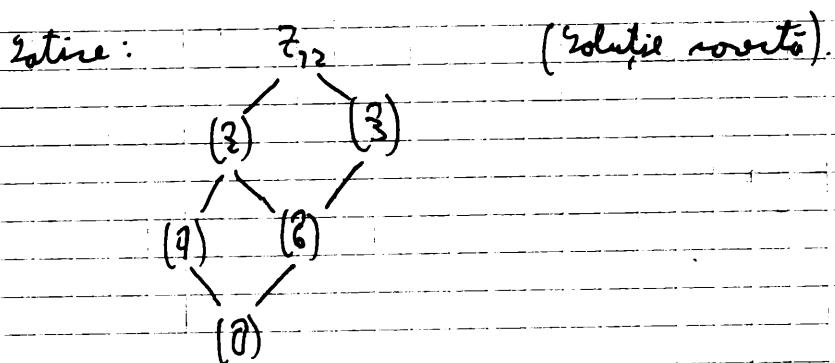
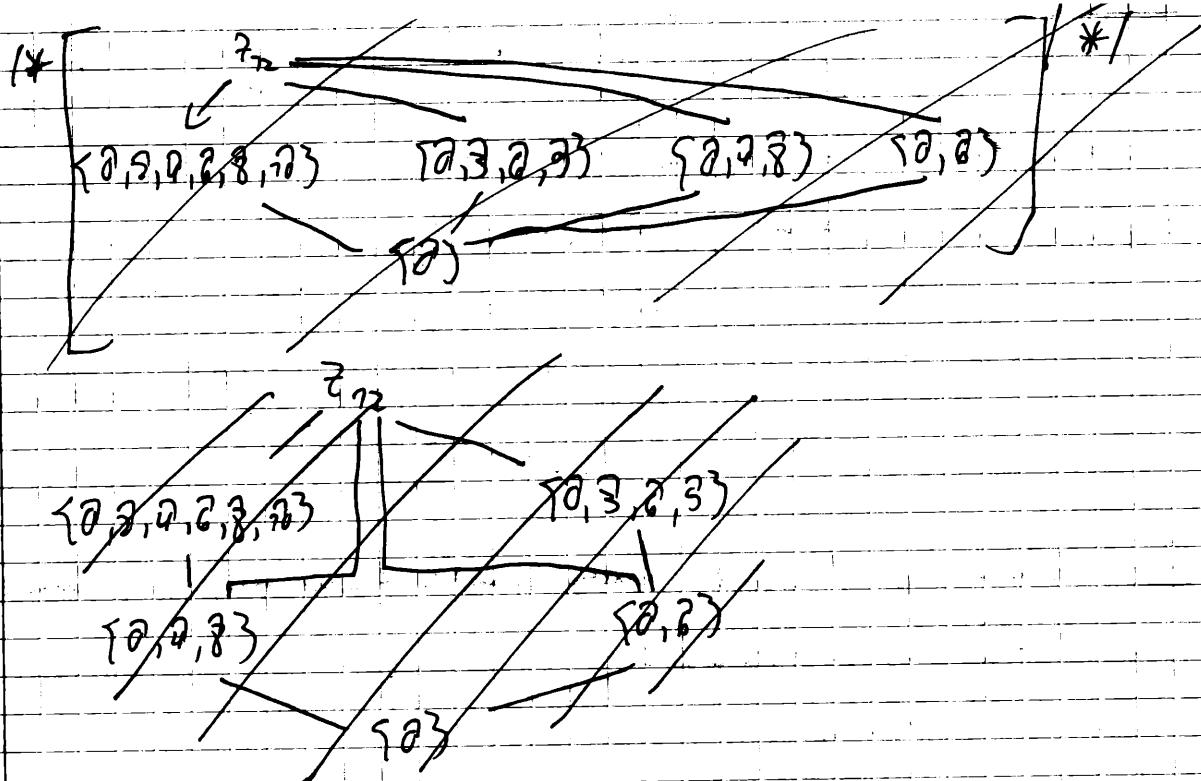
$$72/12^2 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} = \{1\}$$

$$3^2/12^2 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} = \{3\}$$

$$4^2/12^2 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} = \{4\}$$

$$6^2/12^2 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} = \{6\}$$

$$12^2/12^2 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} = \{1\}$$



(5) Fie  $G$  un grup finit. să se arate că  $G$  are un element de ordinul 2 d.d.  $|G|$  par.

Sol: Ef. Th. lui Lopasov  $\rightarrow$  dacă  $G$  are un elem de ordinul 2, at.

$|G|$  este par. ( $\checkmark$ )

Răspuns: Prengăduim că  $|G|$  par. Dacă  $G$  are sl. de ordinul 2, at. există  $x \neq e$ , astfel  $x + x^{-1} = e$  și atunci multimea  $G = \{e\} \cup \bigcup_{x \in G} \{x, x^{-1}\}$   $\Rightarrow G$  are un număr impar de elemente.

Justificare: mulțimea care conține în același timp și el și inversul său disjuncte, nu poate fi par.

(6) să se determine sl. de ordin 8 din  $\mathbb{Z}_6 \times \mathbb{Z}_{10}$  și sl. de ordin 4 din  $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$ .

Sol:

Obs: Dacă  $G$  și  $H$  sunt grupuri și  $g \in G, h \in H$  sunt sl. de ordin finit

el. de forma  $(g, h) \in G \times H$  are ordinul  $[\text{ord}(g), \text{ord}(h)]$ .

Aceasta devine  $(g, h)^n = (g^n, h^n) \Leftrightarrow g^n = g$  și  $h^n = h$  ceea ce este echivalent cu  $\text{ord}(g) | n$  și  $\text{ord}(h) | n$ .

Așași  $(g, h) \in \mathbb{Z}_6 \times \mathbb{Z}_{10}$  are ordinul 8 dă  $[m, n] = 8$ , unde  
cel mai mic multiplu.

$m = \text{ord}(g)$  și  $n = \text{ord}(h)$ . Dacă  $m/6$  și  $n/10$  este imposibil  $[m, n] = 8$ .  
 $\Rightarrow$  nu există elevi. al ord 8.

- Inversul de rezervor  $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$ .

$(g, h) \in \mathbb{Z}_{12} \times \mathbb{Z}_{15}$  are ordinul 4 dă  $[m, n] = 4$ , unde  $m = \text{ord}(g)$  și  
 $n = \text{ord}(h)$ . Dacă  $m/12$  și  $n/15$ .

$(g, h) \in \mathbb{Z}_{12} \times \mathbb{Z}_{15}$ , cu ord 4, dacă  $[m, n] = 4$ , unde  $m = \text{ord}(g)$ ,  $n = \text{ord}(h)$ ,  
 $\Rightarrow m/12$  și  $n/15$ .  $\Rightarrow mn = 4$  (în fizică el face numărul de revoluții)

$$mn = 1$$

Vezi că el. de ord 4 din  $\mathbb{Z}_{12}$  sunt  $\{3, 9\}$ . (clară fără să calculezi)

un grup sau de  $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$  există 2 elevi de ordinul 4, revăzute  
 $(3, 0)$  și  $(9, 0)$ .

7) Date exemplul de un grup  $(G, \circ)$  finit, cu  $x, y \in G$  a.s. astfel încât

a)  $\text{ord}(x)$  și  $\text{ord}(y)$  finite, dar  $\text{ord}(xy)$  infinit.

b)  $\text{ord}(xy)$  finit, dar  $\text{ord}(x)$  și  $\text{ord}(y)$  infinit.

Sol: a) În grupul  $GL_2(\mathbb{R})$  al matricelor inversibile de ordinul 2, cu

elementi reali, non. elevi.  $X = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$  și  $Y = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$

Dacă  $X^2 = Y^2 = I_2 \Rightarrow \text{ord}(X) = \text{ord}(Y) = 2$

și totuși  $X \cdot Y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  și nu există  $n \in \mathbb{N}^*$  a.s.  $(XY)^n = I_2$ .

$$\Rightarrow \text{ord}(XY) = +\infty$$

Tenă (b)?

(8) Dacă este de un element  $x \neq 0$  din  $\mathbb{Z}$  grupuri  $G, G_1$  a.n.  $\text{ord}(x) < +\infty$  în  $G$  și  $\text{ord}(x) = +\infty$  în  $G_1$ .

rez: Fie  $x = \frac{-1+i\sqrt{3}}{2}$  în grupurile  $(C^*, \cdot)$  și  $(C_1^*, \cdot)$ .

Dacă  $x^2 = \frac{-1-i\sqrt{3}}{2} \neq x^3 = 1 \Rightarrow \text{ord}(x) = 3$  în  $(C_1^*, \cdot)$

Dacă  $-x \neq 0$ , și  $(*) \rightarrow \epsilon \in \mathbb{N}^*$   $\Rightarrow \text{ord}(x) = +\infty$  în  $(C_1^*, \cdot)$ .

Apliștii - grupuri.

26.7.7.2019

① Fie  $n \in \mathbb{N}$ . Vom arăta că  $U_n = \{z \in \mathbb{C}^* \mid |z^n| = 1\}$ ,  $T = \{z \in \mathbb{C}^* \mid |z| = 1\}$ , sunt subgrupuri ale lui  $(C^*, \cdot)$ .

Să fie  $z_1, z_2 \in U_n \Rightarrow z_1^n \cdot z_2^{-n} = 1$ .

Dacă  $(z_1 \cdot z_2^{-1})^n = z_1^n \cdot z_2^{-n} = 1 \Rightarrow U_n \subseteq (C^*, \cdot)$

Analog, dacă  $z_1, z_2 \in T \Rightarrow |z_1| = |z_2| = 1$ .

$\Rightarrow |z_1 \cdot z_2^{-1}| = |z_1| \cdot |z_2^{-1}| = 1 \Rightarrow z_1 \cdot z_2^{-1} \in T$ .

$\Rightarrow T \subseteq (C^*, \cdot)$ .

② Arătăm că  $z = \cos(\sqrt{2}\pi) + i \sin(\sqrt{2}\pi)$  nu este element de ordin  $\infty$  al grupului  $(C^*, \cdot)$ . // Fermat-Mersenne.

Să  $n, m \in \mathbb{N}$  a.s.  $z^n = 1 \Rightarrow$

$\Rightarrow \cos(k\sqrt{2}\pi) + i \sin(k\sqrt{2}\pi) = 1$

$\Leftrightarrow (\exists k \in \mathbb{Z}$  a.s.  $\sqrt{2}k\pi = 2m\pi$ ). //  $\sin = 0$ ;  $\cos = 1$ .

$\Rightarrow \sqrt{2} = \frac{m}{k} \in \mathbb{Q}$  contradicție  $\Rightarrow$  nu există ordinul lui  $z$  //  $\text{ord}(z) = +\infty$ .

③ Fie grupul  $(\mathbb{C}^*, \cdot)$ ,  $n > 0$  și  $\varepsilon = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ . Arătă că este element de ordin  $n$  al grupului  $(\mathbb{C}^*, \cdot)$ .

Să arătăm că  $\varepsilon^n = \cos \left( n \frac{2\pi}{n} \right) + i \sin \left( n \frac{2\pi}{n} \right) = \cos 2\pi + i \sin 2\pi = 1$ . // deoarece în ordinea cardinală nu are sens ( $\Rightarrow$ ) că e minim.

Dacă  $\varepsilon^n = 1$ ,  $k \in \mathbb{N}^*$  și  $\varepsilon^k = \cos k \frac{2\pi}{n} + i \sin k \frac{2\pi}{n} = 1$ .

$\Rightarrow \frac{2k\pi}{n} = 2\pi T$ ,  $T \in \mathbb{Z} \Rightarrow k = n \cdot T \Leftrightarrow n | k \Leftrightarrow \text{ord } (\varepsilon) = n$ .

④ Det. Elementele de ordin 6 ale grupului  $(\mathbb{C}^*, \cdot)$ .

Să propună: Elementele de ordinul 6 ale lui  $(\mathbb{C}^*, \cdot)$  sunt:

$$z = \underbrace{\varepsilon^1}_1, \quad 0 \leq n \leq 5, \quad (n, 6) = 1 \quad \text{!!!}$$

c.m.m.d.c.

Fie  $\varepsilon = \cos \frac{2\pi}{6} + i \sin \frac{2\pi}{6} = \frac{1}{2} + i \frac{\sqrt{3}}{2}$

Elevem la  $n$  astfel încât  $(n, 6) = 1$ :  $(1, 6) = 1$  și  $(5, 6) = 1$  și  $\varepsilon^5 = \cos 5 \cdot \frac{2\pi}{6} + i \sin 5 \cdot \frac{2\pi}{6} = \cos \frac{5\pi}{3} + i \sin \frac{5\pi}{3} = \frac{1}{2} - i \frac{\sqrt{3}}{2}$

⑤ Toate două produse multplii finitelor următoare se poate defini o structură de grup. comutativ. // com., el.-inv., el.-rest.

Să fie  $G = \langle a_0, a_1, \dots, a_{n-1} \rangle$ .  $\circ$  și  $\circ$  fiinduri cu proprietăți  $\Rightarrow G \in \mathbb{N}^*$

Dacă  $i, j \in \{0, 1, \dots, n-1\}$  def.  $a_i \circ a_j = a_n$  unde  $n = \text{nr. prod. fin.}$  și

$i+j < n$ . (Nu mai rămâne să se demonstreze)

Evident, o astfel de structură este asociativă, comutativă, deschisă față de adunare și multipli ai lui  $a_i$  și  $a_{n-i}$ ,  $i = 0, 1, \dots, n-1$  // Verificare (probabil greșit).

## Teoria

• Grupe H și G, n.o. xeb.:

$$(xH = \{xh \mid h \in H\})$$

$$(Hx = \{hx \mid h \in H\})$$

$$\text{Not } (G/H)_S = \{xH \mid x \in G\}$$

$$(G/H)_d = \{Hx \mid x \in G\}.$$

$$\text{Indicele lui } H \text{ în } G \stackrel{\text{def}}{=} \underbrace{|G:H|}_{\text{cardinal}} = \underbrace{|(G/H)_S|}_{\text{cardinal}} = \underbrace{|(G/H)_d|}_{\text{cardinal}}$$

• Grupe, E ⊂ G submultimi

Pentru ca tuturor submultimilor care contin mult E să se

subgrupul generat de E în G. Notăm subgrupul  $\langle E \rangle$ .

L1  
T  
R  
O  
L2

$$\text{Dacă } \langle E \rangle = \bigcap H$$

$$E \subset H \subset G, H \leq G.$$

Dacă  $\langle E \rangle = H$  și că E este un sistem de generatori al H

- Un subgrup H al lui G este adesea un prod. de generatori format dintr-un singur element sau subgrup ciclic.

Notăm  $H = \langle a \rangle$ ,  $a \in a \in H$ .

Dacă  $H = \langle a \rangle$ , at  $H = \{a^n \mid n \in \mathbb{Z}\}$ .

## Aplicații

① Fie elei  $j = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$  și  $K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  în  $(GL_2(\mathbb{C}), \cdot)$

Not  $\gamma = \langle j \rangle$  și  $K = \langle K \rangle$  și cu  $\mathcal{Q}_8 = \langle j, K \rangle$ .

$\mathcal{Q}_8$  și datează:

a)  $|j| = |K| = 4$  și  $|j \cap K| = 2$

b)  $j, K$  sunt subgrupuri normale în  $\mathcal{Q}_8$  și  $\mathcal{Q}_8 / \langle j \rangle \cong \mathcal{Q}_8 / \langle K \rangle \cong \mathbb{Z}_2$ .

c)  $j^2 = k^2$  este singulară de ordin 2 în  $\mathbb{Q}_p$ .

S: a)  ~~$j^2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, j^2 = \begin{pmatrix} i^2 & 0 \\ 0 & -i^2 \end{pmatrix}$~~

a)  $j^2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

$j^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$

$j^4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$

$J = \{j, j^2, j^3, I_2\}$

$k^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix}$

$k^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

$k^4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$

$K = \{k, k^2, k^3, I_2\}$

(Obs. că  $j^2 = k^2$ ) Din cauza ord(j) = ord(k) = 4 ( $|J| = |K| = 4$ )

Obs. că  $j^2 = k^2 \Rightarrow J \cap K = \{j^3, I_2\}$

$|J \cap K| = 2$

a) Avem  $j^{-1} j j = j j j^{-1} = j \in J$   
(prin calcul)

$K j k^{-1} = k^{-1} j k = j^3 \in J$

$\Rightarrow j \Delta Q_8$

De mod similar,  $k \Delta Q_8$  fol. rel.  $j^k j^{-1} = j^{-1} k j = k^3$

Astăzi  $J \cap K$  este subgrup din  $Q_8$  și cum  $j, k \in J \cap K \Rightarrow j, k \in Q_8$ .

Din Th. 2 de izomorfismi  $\Rightarrow \mathcal{Q}_8/\mathcal{J} \cong K/\mathcal{J}_{\mathcal{K}}$ .

Dacă  $|\mathcal{Q}_8| = |\mathcal{J}_K| = |\mathcal{J}| \cdot |K| / |\mathcal{J}_{\mathcal{K}}| = 8$ .

$$\begin{array}{c} // (4 \cdot 4 : 2) \\ \cap \end{array}$$

c) Eram  $|\mathcal{Q}_8 : \mathcal{J}| = 2$  și  $K \in \mathcal{J} \Rightarrow \mathcal{Q}_8 = \mathcal{J} \cap K$

dacă  $\mathcal{Q}_8 = \langle I_2, j, j^2, j^3, K, Kj, Kj^2, Kj^3 \rangle$ .

Folosind rel. de la b)  $\Rightarrow j^2 = K^2$  și  $j$  nu este abelian  
dor să se subspun diam  $\mathcal{Q}_8$  nu este abelian.

(2) Eu rotabil anterior (de la a) nu este astăzi că  $\mathcal{Q}_8$  nu este abelian  
dor să se subspun diam  $\mathcal{Q}_8$  nu este abelian.

S: zile H subgrup al lui  $\mathcal{Q}_8$ . Din T. Lagrange  $\Rightarrow |H| \in \{1, 2, 4\}$ .

Dacă  $|H| \in \{1, 2\} \Rightarrow$  că H subgrup normal al lui  $\mathcal{Q}_8$ . ( $H \trianglelefteq \mathcal{Q}_8$ )

Dacă  $|H| = 4 \Rightarrow |\mathcal{Q}_8 : H| = 2 \Rightarrow H \trianglelefteq \mathcal{Q}_8$ .

Dacă  $|H| = 2 \stackrel{a)}{\Rightarrow} H = \langle I_2, j^2 \rangle$  At.  $H = \langle j^2 \rangle$  și cum

$$jj^2j^{-1} = j^{-1}j^2j = j^2 \in H \quad \Rightarrow \cancel{j \in \mathcal{Q}_8}$$

$$Kj^2K^{-1} = K^{-1}j^2K = K^2 \in H \quad \Rightarrow H \trianglelefteq \mathcal{Q}_8$$

Eram  $Kj \neq jk \Rightarrow \mathcal{Q}_8$  nu este abelian.

→ TEMATICA: ! Probleme C/C++ pe foaie.

• Să se arate că dacă  $\forall n \in \mathbb{N}^*$ , numărul  $(C^*)_n$  reprezentă numărul subgrupurilor cu ordinul  $n$  și avem  $U_n = \{K \in C \mid 2^n = |K|\}$ .

• Program C/C++ care gen. sub. lui  $\mathbb{Z}_m$  să se dă.

Lembogrupuri

// Dacă fățim, atunci multă liniște din cînd.

⑦ Găsește rezolvarea ecuației  $3x^2 - 4x + 1 = 0$  în  $\mathbb{Z}_5$  și  $\mathbb{Z}_{17}$ .

S: În orice corp. comutativ constantă ( $k \neq 0$ ) există formă obișnuită de rezolvare a ecuației de gradul al 2-lea.

Este  $ax^2 + bx + c = 0$ ,  $a, b, c \in k$ ,  $a \neq 0$  are soluții  $x_1, x_2 \in k \Leftrightarrow (x_1 - a)^2 + (x_2 - a)^2 = 0$ .

$$(b^2 - 4ac) = a^2 \text{ și soluțiile sunt } x_{1,2} = \frac{(-b \pm \sqrt{b^2 - 4ac})}{2a}.$$

Dacă  $3x^2 - 4x + 1 = 0$ .

- din  $\mathbb{Z}_5$ :  $i^2 \equiv 1 \pmod{5}$

$$b^2 - 4ac = 16 - 4 \cdot 3 \cdot 1 \equiv 16 - 12 = 4 \quad (\text{datorită } \mathbb{Z}_5 \text{ nu are } \sqrt{-1} \pmod{5})$$

$$\begin{cases} x_1 = (-4) + 2 = 2 \cdot 3^{-1} = 2 \cdot 6^{-1} = 2 \cdot 7 = 2 \\ x_2 = (-4) - 2 = 2 \cdot 3^{-1} = 2 \cdot 6^{-1} = 2 \cdot 7 = 7 \end{cases}$$

$$x_1 = (-4) + 2 = 2 \cdot 3^{-1} = 2 \cdot 6^{-1} = 2 \cdot 7 = 2 \pmod{5}$$

$$x_2 = (-4) - 2 = 2 \cdot 3^{-1} = 2 \cdot 6^{-1} = 2 \cdot 7 = 7 \pmod{5}$$

⑧ găsește inclusiv rezolvările ale ecuației din discuția pe care o face.

S:  $a \in U(\mathbb{Z}_m) \Leftrightarrow b \in \mathbb{Z}_m^{\times} \text{ și } a \cdot b \equiv 1$ .

$$\Leftrightarrow \exists b \in \mathbb{Z}_m^{\times} \text{ s.t. } ab \equiv 1 \pmod{m} \Leftrightarrow (3) \text{ } b, k \in \mathbb{Z}_m^{\times} \text{ cu proprietatea } ab \equiv 1 \pmod{m} \Leftrightarrow$$

$$\Leftrightarrow (a, m) = 1$$

$$\text{Deci } |U(\mathbb{Z}_m)| = |\{a \in \mathbb{Z}_m^{\times} \mid (a, m) = 1\}| = \varphi(m) \text{ indicat de Euler.}$$

Imediat rezultă că este chiar al lui Fermat.  $(\Rightarrow (a, m) \neq 1 \Rightarrow m \text{ divizor la } a^{\varphi(m)} \equiv 1 \pmod{m})$

③ Fie  $I$  un ideal unitar. Iară, în Babu docă  $x^2 = x$ ,  $\forall x \in I$ .

Aș. nu:

a) Dacă  $I$  este un ideal Babu, atunci este comutativ.  $\exists x \in I$ ,  $\forall x \in I$

b) Un ideal Babu integral este  $\mathbb{Z}_2$ .

S: a) Aș. nu  $\exists x \in I$  s.t.  $x^2 = x - x \Rightarrow x = -x$ .

$\Rightarrow x + x = 0 \Rightarrow 2x = 0$ ,  $\forall x \in I$ .

Fixezi  $x, y \in I \Rightarrow (x+y)^2 = x+y$

$$\Rightarrow x^2 + xy + yx + y^2 = x+y.$$

$$\Rightarrow xy + yx = 0 \Rightarrow xy = -yx \Rightarrow xy = yx.$$

(Babu)

b) Dim.  $x^2 = x$ ,  $x \in I \Rightarrow x^2 - x = 0 \Rightarrow x(x-1) = 0$ .

$\Rightarrow x = 0$  sau  $x = 1$ .

$I \cong \mathbb{Z}_2$   
în mod.

④ Fie  $I$  un ideal unitar și  $M = \{x \in I \mid x = x^2\}$  multimea celor ridicate.

În se notează că  $M$  este o mulțime finită, atunci există un număr de elemente.

Y: Dacă  $x \in M \Rightarrow 1-x \in M$ .

Într-o altă formă  $(1-x)^2 = 1-2x+x^2 = (1-2x+x) = 1-x$

$\rightarrow$  elementul  $1-x$  nu poate fi de forma  $(x, 1-x)$ . El este

deci orice (produs) generat sunt distincte

Într-o altă formă, dacă  $\exists x_0 \in M$  s.t.  $x_0 = 1-x_0$   $\xrightarrow{\text{adună}} x_0^2 = x_0 - x_0^2 (=)$

$$\Rightarrow x_0 = x_0 - x_0 \quad (\Rightarrow x_0 > 0).$$

În final avem o inegalitate  $x_0 = 1-x_0$  ( $\Rightarrow 0 = 1$ ) contradiction!

Nu există prea multe din  $M$  de tipul descris mai sus.

$\rightarrow M$  are 2-3 elemente.

(5) Fie  $I$  un inel comutativ finit cu  $1 \neq 0$ . Sa se calculeze numarul elementelor din idealul  $I$ .

S: Este clar ca  $1^2 = 1 \Rightarrow 1$  este singurul idempotent. singurul numar pozitiv.

1) Singurul idempotent real este  $1 \Rightarrow I = \{1\}$

2) Dacă există număruri idempotentărele diferite de  $1$ .

Fie  $x$  un astfel de elem.  $\Rightarrow x \cdot x$  idempotent (Ex. prob 4). Dacă  $x \cdot (x-x) = x - x^2 = x - x = 0$ . Atunci produsul tuturor a.i. idemp. este 0.

(6) Se consideră idealul  $I_m, m \in \mathbb{N}, m \geq 2$ . Sa se calculeze numărul elementelor ale a.i. nilpotente.

S: Fie  $I$  un inel. Un elem  $x \in I$  nu poate fi  $\forall n \in \mathbb{N}^*$  a.s.  $x^n = 0$  nici.

Se numește a.i. nilpotent al lui  $I$ .

Așadar  $a \in I_m$  ( $\exists m$ ) ( $\Rightarrow a \in \{1, \alpha_1, \alpha_2, \dots, \alpha_m\}$ ) unde  $\alpha_1, \alpha_2, \dots, \alpha_m$  sunt factorii primi ai lui  $m$ .

Atunci  $a^k \in I_m$  ( $\forall k \in \mathbb{N}$  a.s.  $a^k = 0 \Rightarrow a | a^k$ . Deoarece  $a^k \in I_m$ ,

$\forall i \in \overline{1, m} \Rightarrow \alpha_i | \alpha_1 \alpha_2 \dots \alpha_m | a$ .

Fie  $a \in \alpha_1 \alpha_2 \dots \alpha_m$  ( $\Rightarrow \exists j \in \{1, 2, \dots, m\}$  a.s.  $a = \alpha_1 \alpha_2 \dots \alpha_j b$ )

Fie  $k \in \mathbb{N}$  a.s.  $k \geq d_i$ ,  $\forall i \in \overline{1, m}$ , unde  $d_i$  = exponentul lui  $\alpha_i$  în descompun. evident  $a | a^k \Rightarrow a^k = 0$ .

III) În acamă,  $N(I_m) = \alpha_1 \alpha_2 \dots \alpha_m$  ( $\Rightarrow |N(I_m)| = |\alpha_1 \alpha_2 \dots \alpha_m|^2 / 2^m =$

$$= \frac{1}{2^m} |\alpha_1 \alpha_2 \dots \alpha_m|$$

(7) Să se calculeze  $U(\mathbb{Z}[i\sqrt{5}])$ .

$\hookrightarrow$  el. invers.

număr. (număr)

S: Fie  $N_1: \mathbb{Z}[i\sqrt{5}] \rightarrow \mathbb{N}$  definită prin  $N_1(a+ib\sqrt{5}) = a^2 + 5b^2$ . Dacă

$\alpha, \beta \in \mathbb{Z}[i\sqrt{5}]$  și dacă factorul său N este număr  $\Rightarrow N_1(\alpha) \cdot N_1(\beta) = N_1(\alpha\beta)$ .

$\Rightarrow d \in U(\mathbb{Z}[i\sqrt{5}]) \Leftrightarrow N_1(d) = 1 \Rightarrow a^2 + 5b^2 = 1$

Dacă  $a, b \in \mathbb{Z} \Rightarrow 5b^2 = 1$ . Dacă  $b \neq 0 \Rightarrow$  avem doar  $b = 0 \Rightarrow$   
 $\Rightarrow a \geq 1 \Rightarrow U(\mathbb{Z}[i\sqrt{5}]) = \{\pm 1\}$ .

(8) Vom arăta că nu există  $\mathbb{Z}[\sqrt{6}] \times \mathbb{Z}[\sqrt{26}]$  nu sunt înmulțirea factorilor.

S:  $\exists t \in \mathbb{Z}[\sqrt{6}]$  astfel că  $6 = 2 \cdot 3 = (i\sqrt{6}) \cdot (-i\sqrt{6})$

iar și  $\mathbb{Z}[\sqrt{26}]$  avem  $26 = 2 \cdot 13 = (i\sqrt{26}) \cdot (-i\sqrt{26})$ .

dori și drepturi distincte.

Lărgire.

Laborator 10.12.2019

Axialitate - Teoreme și Corolari

• Dacă  $I$  este ideal,  $I \subseteq R$ ,  $I \neq \emptyset$

$I$  este ideal stâng (stărt) al lui  $R$  dacă  $x-y \in I$ ,  $\forall x, y \in I$  și  $x \in I \Rightarrow x-a \in I$  ( $x-a \in I$ )

$\forall a \in R$  și  $x \in \underline{I}$   
 $\underline{I}$  (ideal)

• Dacă  $I$  este ideal stărt și drept  $\Rightarrow I$  este ideal bilateral.

• Dacă  $R$  este comutativ  $\Rightarrow$  Definitia comună și rezultă că  $I$  este ideal.

• Dacă  $I$  este ideal bilateral în idealul  $R$ , notăm cu  $R/I$  idealul factor.

• Dacă  $R$  este comutativ și  $P \subseteq R$  ideal:

- R este ideal prim ( $\Rightarrow P \neq R$  și  $\forall p \in P$  numărătorii și numitorii lui  $p$  sunt din  $P$  sau  $a, b \in R$ ).

$\Leftrightarrow R/P$  este domeniu de integrabilitate.

-  $P$  este ideal maximal dacă  $P+R$  nu este un alt ideal maxim al lui  $R$  și nu conține strict  $P$

$\Leftrightarrow R/P$  este corp.

• Pentru un ideal  $R$ , folosim notările:  $U(R) =$  mult. el. inversibile din  $R$

$D(R) =$  mult. div. lui 0 din  $R$ .

$N(R) =$  mult. el. nilpotente din  $R$ .

$\text{id}_{\text{max}}(R) = \text{mult el. ideale divizori ai } R \quad (x^2 = x)$

$\text{Zer}(R) = \text{mult, idealele nule ai } R$

$\text{Max}(R) = \text{mult, idealele maxime ai } R$

⑦ Să se determine idealul, id trivial și id maximal ai  $\mathbb{Z}_m$ . dim  $\mathbb{Z}_m$  și m.

Avem  $m = m_1 \cdot m_2 \cdots m_n$  cu  $m_i$  prime și  $m_i \neq m_j$  pentru  $i \neq j$ .

Să fie  $R = \mathbb{Z}_m$ , unde  $m = p_1^{d_1} p_2^{d_2} \cdots p_n^{d_n}$  cu  $p_i$  prime și  $d_i$  diferențe și  $K_1, \dots, K_n \in \mathbb{N}^*$

Idealele lui  $\mathbb{Z}_m$  sunt de forma  $m^2 / n^2$  unde  $n$  este un divizor natural al lui  $m \Rightarrow \mathbb{Z}_m$  are  $\boxed{(n+1)(n+2) \cdots (n+d_n)}$  ideale (n.)

Cu  $n_i$  este idealul nul și idealul maximal  $\mathbb{Z}_m$   $\Rightarrow$  idealul prim  $\neq 1$  este dim  $\mathbb{Z}_m$  maxim și sunt de forma  $n_i^2 / n^2$  cu  $i = 1, 2, \dots, n$   $\Rightarrow$  există  $m$  de găsit, 0-dim. în factori primi.

② Fie  $R$  inel unitar,  $R \neq \mathbb{Z}$ . inel local dacă  $x^2 = x$ ,  $\forall x \in R$ .

$\mathbb{Z}$  este  $\mathbb{Z} = \text{Zer}(R) = \text{Max}(R)$

VP

③ Fie  $P \in \text{Zer}(R)$ . Există  $M \in \text{Max}(P)$  a.s.t.  $P \subseteq M$ . Dacă  $P \neq M \Rightarrow \exists x \in M$ :

Dacă  $x^2 = x \Rightarrow x(x - 1) = 0 \in P \Rightarrow (x - 1) \in P \Rightarrow x - 1 \in M$ . contr.

Dacă  $P = M \in \text{Max}(R)$ .

④ Fie  $R$  inel comutativ și unitar.

a) Dacă  $j(R)$  este radicalul Jacobson al lui R def. ca fiind

intersecția idealilor maximi ai lui  $R$ . Atunci  $j(R) = \{x \in R \mid$

$\forall a \in U(R), \forall \alpha \in R\}$ .

b) să se dea st. că inele  $R$  și  $N(R) \neq j(R)$  și inele  $R$  și  $N(R) = j(R)$ .

$N(R) = j(R)$ .

S: a) Fie  $x \in j(R)$  și  $a \in R$ .

Dacă  $a \neq 0$  și  $x \notin U(R)$  at  $(\exists) m \in \text{Max}(R)$  a.s.t.  $a \cdot m \in M$

Dacă  $x \in j(R) \Rightarrow x \in M \Rightarrow a \cdot x \in M$  și  $\forall n \in R$  cu  $n \neq 0$  și  $n \cdot x \in M \Rightarrow n \in M$  (cont.)

• Reciproc, fie  $x \in R$  și  $n \cdot x \in U(R)$ , nu  $\forall a \in R$  și  $m \in \text{Max}(R)$

Dacă  $x \notin M$  at  $m \in M + (x) \Rightarrow m + (x) = R \Rightarrow (\exists) a \in R$  a.s.t.  $n \cdot a \in M \Rightarrow$

$\Rightarrow n \cdot a \notin U(R)$  fals

b) Dacă  $R = \mathbb{Z}$  avem  $N(\mathbb{Z}) = j(\mathbb{Z}) = 0$ .

De la altă parte, ducă  $R = \mathbb{Z}$  în cel total, cu modul  $\mathbb{Z}$  în  $\mathbb{Z}[x] \neq \text{Max}(\mathbb{Z})$  și  $N(\mathbb{Z}) + j(\mathbb{Z})$ . (deoarece  $P = R(x)$ )

(4) Dacă multimea  $I = \mathbb{Z}_{20} \times \mathbb{Z} \times \mathbb{Z}_{19}$ , să se determine idealele, imbarele factor, idealele primări, idealele maximale,  $N(I)$ ,  $j(I)$  și să se calculeze numărul lor.

S:  $\begin{bmatrix} (a, b, c) \\ \downarrow \quad \downarrow \quad \downarrow \\ \mathbb{Z}_{20} \quad \mathbb{Z} \quad \mathbb{Z}_{19} \end{bmatrix}$

6x.

Imbarel  $\mathbb{Z}_{20}$  are idealele (pr. 7):  $\{0, \mathbb{Z}_{20}, 2\mathbb{Z}_{20}, 3\mathbb{Z}_{20}, 5\mathbb{Z}_{20}, 6\mathbb{Z}_{20}, 7\mathbb{Z}_{20}, 10\mathbb{Z}_{20}, 12\mathbb{Z}_{20}, 14\mathbb{Z}_{20}, 15\mathbb{Z}_{20}, 18\mathbb{Z}_{20}\}$

Bună,  $\mathbb{Z}$  și  $\mathbb{Z}_{19}$  sunt corpuri. De unde avem 24 de ideale doar pe 0 și pe 1 însăși. (2x)

• Dacă  $I$  va avea 24 de ideale  $(6 \times 2 \times 2)$  formate din produsele dintre idealele de mai sus.

Cum  $\text{Max}(\mathbb{Z}_{20}) = \text{Max}(\mathbb{Z}_{20}) = \{\mathbb{Z}_{20}, 3\mathbb{Z}_{20}\}$  (Din an ①)

$\Rightarrow$  ~~idealele primăre~~  $\text{Max}(I) = \text{Max}(I) = \{\mathbb{Z}_{20} \times \{0\}; \mathbb{Z}_{20} \times \{0\} \times \mathbb{Z}_{19}\}$

$\mathbb{Z}_{20} \times \{0\} \times \mathbb{Z}_{19}; \mathbb{Z}_{20} \times \{0\} \times \{0\}\}$

Imbarele factor sunt izomorfe cu unul din imbarele  $0, \mathbb{Z}_{20}, \mathbb{Z}_5, \mathbb{Z}_{19}$  sau cu modul direct produsul acestora și unul din imbarele  $\mathbb{Z}, \mathbb{Z}_{19}, \mathbb{Z}$ .

•  $N(I) = j(I) = N(\mathbb{Z}_{20}) \times N(\mathbb{Z}) \times N(\mathbb{Z}_{19}) = \mathbb{Z} \mathbb{Z}_{20} \times \{0\} \times \{0\}$ .

$$\bullet \text{Iden}(I) = \text{Iden}(\mathbb{Z}_{20}) \times \text{Iden}(\mathbb{Q}) \times \text{Iden}(\mathbb{Z}_{18}) = \{0, 2, 3, 6\} \times$$

$$\times \{0, 1\} \times \{0, 1\}$$

! Atm info: Sunt ele. iden, nesimile.

### Aplicații recunoscătorice

① Considerăm  $A = N, Z, Q, R$  sau  $C$ .

Dati ex. de fct def ne  $A$  cu valori în  $A$  care sunt injective (nuj) și nu surjective (injektiv)

② Fie  $F = \{f | f: X \rightarrow X \text{ cu } f \circ f = f\}$

Este def: a) fct inj. din  $F$ ;

b) fct nuj. din  $F$ ;

Evidență ①.  $\text{Inj} \Leftrightarrow \forall a, b \in A, f(a) = f(b)$ .

$\text{nuj} \Leftrightarrow \exists f \in F, f(a) = x, x \in A$ .

③ Fie  $f: X \rightarrow Y$  și  $g: Y \rightarrow Z$ . Este orice să două fct sunt injective, at.  
și dacă sunt și doar o fct nuj atăcum este nuj.

④ Fie fct  $f: X \rightarrow Y$ ,  $g: Y \rightarrow Z$ . Este orice să două fct sunt nuj atăcum  
sunt și doar o fct nuj atăcum este nuj.

⑤  $f, g$  injective  $\Rightarrow g \circ f$  injectiv  $\Rightarrow f$  injectiv

Fie  $x, y \in A$  cu  $g \circ f(x) = g \circ f(y)$  ( $\Rightarrow g(f(x)) = g(f(y))$ )  $\Rightarrow$

$f$  injectiv ( $\Rightarrow f(x) = f(y)$ )

$g$  injectiv ( $\Rightarrow g(x) = g(y)$ )

$\Rightarrow f(x) = f(y) \Leftrightarrow x = y \Rightarrow g \circ f$  injectiv.

Solutie 3: a)  $\exists x, y \in A$  ( $x \neq y \Rightarrow g \circ f(x) = (g \circ f(y)) \Leftrightarrow g(f(x)) = g(f(y))$ )  
 Evid.  $g$  este injectivă ( $\Rightarrow g(f(x)) = g(f(y)) \Rightarrow f(x) = f(y)$ ) și din faptul că  $f$  este injectivă  $\Rightarrow x = y$ .

Dacă  $g \circ f(x) = g \circ f(y)$  și  $x \neq y \Rightarrow f$  este injectivă.  $\checkmark$

b)  ~~$\exists x, y \in A$ ,  $g \circ f$  este surjectivă ( $\Rightarrow g(f(x)) = g(f(y)) \Rightarrow x = y$ )~~

b)  $\exists x, y \in A$  cu  $f(x) = f(y)$ . Aplicând  $g$  obținem  $(g \circ f)(x) = (g \circ f)(y)$  și cum  $g \circ f$  este surjectivă  $\Rightarrow x = y$ ?

Solutie 4:

a)  $\exists z \in A$ . Evid.  $g, f$  sunt surjective ( $\exists y \in A$  cu  $g(y) = z$  și  $\exists x \in A$  cu  $f(x) = y \Rightarrow g \circ f(x) = g(y) = z$ ).

b)  $\exists z \in C$ . Evid.  $g \circ f$  este surjectivă,  $\forall z \in C$   $\exists (g \circ f)(x) = z$ . Dacă  $y = f(x) \in B$  și  $g(y) = z$ .

Solutie 1:

• Injective dar nu surjective:

-  $f: N \rightarrow N$ ,

1)  $\exists n_0$ :

Receptoare:

① scrie în program C/C++ să se rezolvă de m. matricele  
 $A \cup B$ ,  $A \cap B$ ,  $A \setminus B$ ,  $B \setminus A$ ,  $A \times B$ ,  $B \times A$   $D(z_n), M(z_n)$

② m - nr. de elemente  $\geq 2$ , det. submatricele lui  $Z_m$ ,  $U(Z_m)$ ,  
 $\text{Zden}(Z_m)$ ,  $\text{Inv}(Z_m)$ ,  $\text{max}(Z_m)$  și m. sol.

## 7. #include <iostream>

using namespace std;

void AUB(int A[], int nA, int B[], int nB);

cout << "AUB = { " ;

for (int i=0; i<nA; i++)

cout << A[i] << " " ;

bool res = true;

for (int i=0; i<nB; i++)

for (int j=0; j<=i; j++)

res = true;

if (B[i] == A[j])

res = false;

break;

}

← if(res)

← cout << B[i] << " " ;

}

}

cout << " } " ;

for (int i=0; i<nA; i++)

for (int j=0; j<nB; j++)

if (A[i] == B[j])

cout << A[i] << " " ;

cout << " } " ;

+ →

void A\B(int A[], int nA, int B[], int nB); //Analogy B\A

cout << "A\B = { " ;

bool res = true;

for (int i=0; i<nA; i++)

for (int j=0; j<nB; j++)

if (B[j] == A[i])

res = false;

break;

if(res)

cout << B[j] << " " ;

3

3

```

void AxB (int A[], int nA, int B[], int nB) {
    cout << "AxB = ";
    for (int i=0; i<nA; i++) {
        for (int j=0; j<nB; j++) {
            cout << "(" << A[i] << ", " << B[j] << ")");
        }
    }
}

```

3

---

\*

```

void Uzam (int n) {
    cout << "Uzam ";
    for (int i=q; i<n; i++) {
        if (Esonde (n, i) == 1)
            cout << i << " ";
    }
    cout << "p";
}

```

)

\* int Esonde (int a, int b)

$$\text{int } r = a \% b;$$

while (r)

$$a = b;$$

$$b = r;$$

$$D = a \% b;$$

3

).

$$\text{Zab} : \frac{0,5 \times \text{Prog} + 0,5 \times \text{Aktivität} + \text{Notat Int}}{2} + 1.$$

$$\frac{(7 + 0,5 \cdot 3 + 6)}{2} + 1 = \frac{14,5}{2} + 1 = 7,25 + 1 = 8,25$$

## Aplicații - Contraposiție de inclusiune

$$\text{Definim } H = \left\{ \begin{pmatrix} u & v \\ \bar{v} & \bar{u} \end{pmatrix} \mid u, v \in \mathbb{C} \right\}$$

a) Dacă re or, re H este un corp rezumativ (nu ocluziv și nu există niciunul) sau nu corpul extinsiorilor și re C este inclusiv.

Avem prop. al lui H:

$$b) \text{ Considerăm } \tau \in H \text{ elev. } i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

De re are loc re  $\tau \in H$  re următoare mod. urmă sub forma  $x =$

$$= a_0 + a_1 i + a_2 j + a_3 k \text{ cu } a_0, a_1, a_2, a_3 \in \mathbb{R}.$$

Nout  $\bar{x} = a_0 - a_1 i - a_2 j - a_3 k$ ,  $N(x) = x \cdot \bar{x}$  și  $T(x) = x + \bar{x}$ . De re or. re.

$$x^2 - T(x)x + N(x) = 0 \text{ și re } N(x) = N(jx).$$

Egal,

1. Corp  $(K, +, \cdot)$  cu  $\tau \cdot (K, +)$  gr. abelian cu  $\lambda = 0$ .

2.  $(K^*, \cdot)$  cu  $\lambda = 7$ .

3. det. + proprietate de t.

$$x \cdot (j+2) = x \cdot j + x \cdot 2.$$

Bucătării imediat re H este un subiect al lui  $M_2(\mathbb{C})$ . De re obisnuit det re.

$A \in H$ ,  $A = \begin{pmatrix} u & v \\ \bar{v} & \bar{u} \end{pmatrix}$  este nulă ( $\Rightarrow \det A = 0 \Rightarrow u \cdot \bar{u} + v \cdot \bar{v} = 0$ ). ( $\Rightarrow$ )

$$(\Rightarrow) |u|^2 + |v|^2 = 0 \Leftrightarrow |u| = |v| = 0 \Leftrightarrow u = v = 0. \Rightarrow A = 0_2.$$

Dacă  $A \neq 0_2$  ( $\Rightarrow$  det  $A \neq 0 \Rightarrow A$  inversabilă în  $M_2(\mathbb{C})$  și inversă reale:

not  $\frac{1}{\det(A)} \begin{pmatrix} \bar{u} & v \\ \bar{v} & \bar{u} \end{pmatrix}$  corectă inversă în H, dacă A este inversă în H.

Găsim. f: G  $\rightarrow H$ , f(u) = u · I\_2, f este morfism inj de inclusiune,

drii C sătăcători și al lui H.

b) Dacă  $A = \begin{pmatrix} \mu & v \\ -\bar{v} & \bar{\mu} \end{pmatrix}$ , unde  $\mu = a + bi$ ,  
 $v = c + di$ ,  $a, b, c, d \in \mathbb{R}$ .

At. avem  $A = a \cdot I_2 + b \cdot i + c \cdot j + d \cdot k$  și nu mod evident, nu  
avem astăzi.

### RESTUL CALCUL [TEMA] (decont)

2. Determinați  $\mathfrak{I}(H)$ , unde H este corpul cuaternionilor.

Sol: Vom arăta că  $\mathfrak{I}(H) \cong C$ .

Fix  $A = \begin{pmatrix} \mu & v \\ -\bar{v} & \bar{\mu} \end{pmatrix} \in \mathfrak{I}(H) \Rightarrow \forall A = A_i \Rightarrow -\bar{v}_i = v_i \Rightarrow v = 0$ .

!( $i, j, k$  de la pct 1)

De altă parte, din  $f_j = jA \Rightarrow \mu = \bar{\mu}$ , adică  $\mu \in \mathbb{R} \Rightarrow A = \mu \cdot I_2$ .

Prin urmare de la prob. ant  $f: C \rightarrow H$ ,  $f(u) = \mu \cdot I_2$ , obținem  
isomorfism.

③ Se cere să se arate că în corpul cuaternion. H, ec.  $x^2 + 7 = 0$  nu are soluții.

Sol: în mult.  $\lambda = a + bi + cj + dk$  sol. a ec.  $x^2 + 7 = 0$ , adică  $a^2 + b^2 + c^2 + d^2 = 0$  și  
 $d^2 + 7 = 0$ .

Construcție.  $\bar{\lambda} = a - bi - cj - dk$ . Deși  $\bar{\lambda} \cdot \bar{\lambda}^2 + \bar{\lambda} = 0$ , adică

$$(\bar{\lambda} \cdot \bar{\lambda}) \cdot \bar{\lambda} + \bar{\lambda} = 0 \quad (*)$$

Not  $\mu = a \cdot \bar{\lambda} = a^2 + b^2 + c^2 + d^2$

Relația (\*) devine  $ad + \bar{\lambda} = 0$ . adică  $(\mu + a) + (mb - b)i + (mc - c)j +$

+  $(md - d)k = 0$ , adică  $\begin{cases} \mu + a = 0 \\ mb - b = 0 \\ mc - c = 0 \\ md - d = 0 \end{cases}$

cum  $(1+n)a = 0 \Rightarrow a = 0$ .

Deci  $b+c+d=0$  și putem scrie  $b=c=d=0$ .

• Dacă  $b \neq 0$  și  $a \neq 0$ , atunci  $b, c, d$  sunt abiații numere reale.

d. Fie  $i+j+k+l \in \mathbb{Z}$  cu  $b^2 + c^2 + d^2 = 7$  numărul soluției

(4) Considerăm  $H$ , corpul numerei reale reale, cu  $H = \{a+bi+ci+kj \mid a, b, c, k \in \mathbb{R}, i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j\}$ .

Fie quaternionul  $\alpha = 7+8i+9j+72k \in H$ . Vom căuta  $x^n$  astfel încât

sol: În general, unul quaternion  $\alpha = a+bi+ci+kj$  nu poate fi multiplu al lui  $\alpha^2 = 2a^2 - b^2 - c^2 - d^2$  deci nu poate fi multiplu al lui  $\alpha$  și verifică mulțimea.

$$\phi \subset X^2 - 2ax + a^2 + b^2 + c^2 + d^2 \in \mathbb{C}[X].$$

În cazul nostru,  $\alpha = 7+8i+9j+72k$  nu poate fi multiplu al lui  $\alpha$ .

Este:  $\rho = X^2 - 2x + 290 \in \mathbb{C}[X]$ . Este o ecuație algebraică de gradul doi.

Rădăcinile:  $X_1 = 7+77i$  și  $X_2 = 7-77i$ .

Bunătatea extensiei  $B_1, B_2$  nu se va vedea în restul formulei.

$$B_1 + B_2 = 7$$

$$(7+77i)B_1 + (7-77i)B_2 = 7+8i+9j+72k.$$

Un obișnuit:  $B_1 = \frac{25}{34} + \frac{6}{77}j + \frac{9}{34}k$ .

(-rădăcine)  $B_2 = \frac{9}{34} - \frac{6}{77}j + \frac{5}{34}k$ .

Așadar avem:  $\alpha^n = (7+8i+9j+72k)^n = (7+77i)^n \left( \frac{25}{34} + \frac{6}{77}j + \frac{9}{34}k \right) +$   
 $+ (7-77i)^n \left( \frac{9}{34} - \frac{6}{77}j + \frac{5}{34}k \right)$

Prop D:  $\exists n \geq 2$  an număr, încât  $f \in \mathbb{Z}[x]$  nu poate fi scrisă sub forma  $F = f^{-1} + n \cdot g$ , unde  $f, g \in \mathbb{Z}[x]$ ,  $n \in \mathbb{N}^*$ .

Dacă  $f$  (prin redus modulo  $n$  la  $k$ ) este ireducibil în  $\mathbb{F}_p[x]$  și

$f$  nu-l divide pe  $g$ , atunci  $F = f^{-1} + n \cdot g$  este ireducibil în  $\mathbb{Z}[x]$ .

- (Schreier)

Aplicare: Arătă că pol.  $F(x) = (x^2+2)^{-1} + 5(x^{2n-7} + 10x^7 + 5)$  este ireducibil în  $\mathbb{Z}[x]$ .

Sol: Aplicând prop. ant., cau că  $f = x^2+2 \nmid g = x^{2n-7} + 10x^7 + 5$ .

cum  $n=5$ , atunci  $f = x^2+2$  este ireducibil în  $\mathbb{Z}_5[x]$ . (se rezolvă mod  $\mathbb{Z}_5$ ), iar  $g = x^{2n-7}$  nu-l divide pe  $x^2+2$  în  $\mathbb{Z}_5[x]$ , deoarece

$F(x)$  este ireducibil în  $\mathbb{Z}[x]$ .