

OPERATII CU MULTIMI

\emptyset - nu are niciun element (multimea vidă)

Axioma de extensionalitate (prima axiomă ZF)

Două multimi A și B sunt egale dacă au aceleasi elemente.

• dacă A și B sunt multimi : $A \subseteq B$ (A inclusă în B) dacă orice element al lui A este și element în B .

$P(A) := \{ X | X \subseteq A \}$ se numește multimea părților lui A .
(axioma 8 ZF)

Fie A, B două multimi. Definim:

• reuniunea lui A cu B

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

• intersectia lui A cu B

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

• diferența dintre A și B

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

Dacă $A \subseteq X$ este submultime în X , atunci

$C_X(A) := X - A = \overline{A}$ a.n. complementara lui A în X .

Fie A, B două multimi și $a \in A, b \in B$. S.n. pereche ordonată a elementelor a și b multimea notată (a, b) , definită prin : $(a, b) := \{ \{a\}, \{a, b\} \}$

Notăm $A \times B := \{ (a, b) | a \in A, b \in B \}$ și a.n. produsul cartesian (direct) al multimilor A și B .

Definitie: Fie A, B două multimi. Se numește functie (aplicație) f de la A la B și o astă notăm $f: A \rightarrow B$

o submultime $f \subseteq A \times B$ a.ș. :

(H) $a \in A$ ($\exists!$) $b_a \in B$ a.ș. $(a, b_a) \in f$.

Acum unic b_a îl notăm cu $f(a)$.

A = domeniul de definitie ; B = codomeniul lui f .

Definiții de bază: Fie $f: A \rightarrow B$ o funcție. Multimea:

- $G_f := \{(a, f(a)) \mid a \in A\} \subseteq A \times B$ a.ș. graficul lui f .
- $Hom(A, B) := \{f: A \rightarrow B \mid f = \text{funcție}\} \stackrel{\text{not.}}{=} B^A$
- $A' \subseteq A$, $f(A') := \{f(a') \mid a' \in A'\} \subseteq B$ - imaginarea lui A' prin f
Dacă $A' = A \Rightarrow f(A) \stackrel{\text{not.}}{=} \text{Im}(f)$ și imaginarea lui f
- $B' \subseteq B$, atunci $f^{-1}(B') := \{a \in A \mid f(a) \in B'\}$ a.ș. imaginarea inversă (fibra) lui B' prin f .

$$f: \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^2, f^{-1}([0, 1]) = [-1, 1]$$

Compoziția funcțiilor Fie $f: A \rightarrow B$ și $g: B \rightarrow C$

două funcții. Funcția $g \circ f$ definită prin:

$g \circ f : A \rightarrow C$, $(g \circ f)(a) := g(f(a))$, (\forall) $a \in A$ a.ș.
compoziția funcțiilor f și g .

(Asociativitatea compozitiei) Fie funcțiile $f: A \rightarrow B$,

$g: B \rightarrow C$, $h: C \rightarrow D$. Atunci:

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Functia identica pe o multime. Fie A o multime nevidă. Functia $\text{id}_A : A \rightarrow A$, $\text{id}_A(a) := a$, $(\forall) a \in A$ s.n. functia identica a lui A . $\text{id}_A \neq \text{Id}_A$.

$$f : A \rightarrow B \text{ e functie} \Rightarrow \begin{cases} f \circ \text{id}_A = f \\ \text{id}_B \circ f = f \end{cases}$$

Dacă $A \subseteq B$ există o funcție $\tilde{z} : A \rightarrow B$, $\tilde{z}(a) := a$, $(\forall) a \in A$ numită incluziunea lui A în B .

Functii injective, surjective, bijective

Definitie: Fie $f : A \rightarrow B$ o functie. Atunci :

1) f s.n. injectivă dacă :

$(\forall) a_1 \neq a_2 \in A \Rightarrow f(a_1) \neq f(a_2)$ (echivalent: dacă $f(x) = f(y)$ și $x, y \in A \Rightarrow x = y$)

2) f s.n. surjectivă dacă $\text{Im}(f) = B$, i.e. $(\forall) b \in B$ $(\exists) a \in A$ a.s. $b = f(a)$.

3) f s.n. bijectivă dacă este injectivă și surjectivă.

OBS

• $f : A \rightarrow B$ nu e injectivă dacă $(\exists) a_1, a_2 \in A$, $a_1 \neq a_2$ și $f(a_1) = f(a_2)$

• f nu e surjectivă dacă $(\exists) b \in B$ a.i. $(\forall) x \in A$ avem că $f(x) \neq b$

• $f : A \rightarrow B$ e bijectivă $\Leftrightarrow (\forall) b \in B$ $(\exists!) a \in A$ a.i. $f(a) = b$.

Teorema 1 (caracterizarea funcțiilor injective)

Fie $f: A \rightarrow B$ o funcție. S.E.A:

a) f este injectivă

b) f are o retractă: i.e. (\exists) $r: B \rightarrow A$ o funcție a.t.

$$r \circ f = \text{id}_A$$

c) f este monomorfism: i.e. (\forall) $X =$ multime și (\forall) $f_1,$

$$\begin{array}{ccc} X & \xrightarrow{f_1} & A \\ & \xrightarrow{f_2} & \end{array}$$

$f_2: X \rightarrow A$ funcții cu $f_1 \circ f_2 = f_2 \circ f_1$, avem că $f_1 = f_2$.

Teorema 2 (caracterizarea funcțiilor surjective)

Fie $f: A \rightarrow B$ o funcție. S.E.A.

a) f este surjectivă

b) f are o "secțiune": i.e. (\exists) $s: B \rightarrow A$ a.t. $f \circ s = \text{id}_B$

c) f este "epimorfism": i.e. (\forall) $Y =$ multime și (\forall)

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \xrightarrow{f_1} & \xrightarrow{f_2} Y \end{array}$$

cu $f_1 \circ f = f_2 \circ f$, avem că $f_1 = f_2$.

Definiție: O funcție $f: A \rightarrow B$ a.r. inversabilă dacă

(\exists) $g: B \rightarrow A$ o funcție a.t:

$$f \circ g = \text{id}_B \text{ și } g \circ f = \text{id}_A$$

Inversa unei funcții, dacă există, este unică și se notează cu f^{-1} .

Caracterizarea funcțiilor inversabile: O funcție $f: A \rightarrow B$ este inversabilă \Leftrightarrow este bijecțivă.

Produsul direct (cartezian) al mulțimii
Axioma alegerii

Fie $I \neq \emptyset$ o mulțime nevidă și $(A_i)_{i \in I}$ o familie de mulțimi nevide. Atunci:

$$\bigsqcup_{i \in I} A_i := \{x \mid (\exists i \in I \text{ a.s. } x \in A_i)\}$$

$$\bigcap_{i \in I} A_i := \{x \mid x \in A_i, \forall i \in I\}$$

Definiție: Fie $I \neq \emptyset$ și $(A_i)_{i \in I}$ o familie de mulțimi nevide. Mulțimea:

$$\prod_{i \in I} A_i := \{x : I \rightarrow \bigcup_{i \in I} A_i \mid x(i) \in A_i, \forall i \in I\}$$

s.n. produsul direct (cartezian) al familiei $(A_i)_{i \in I}$.

Axioma alegerii: Dacă $(A_i)_{i \in I}$ este o familie nevidă de mulțimi nevide. Atunci $\prod_{i \in I} A_i$ este o mulțime nevidă.

OBS: ① Fie $\prod_{i \in I} A_i$ produsul direct al familiei $(A_i)_{i \in I}$

Un element $x \in \prod_{i \in I} A_i$ este o funcție $x : I \rightarrow \bigcup_{i \in I} A_i$

și se notează $x = (x_i)_{i \in I}$, unde $x_i := x(i) \in A_i, \forall i \in I$.

Pentru fiecare $i \in I$, funcția

$$i_j : \prod_{i \in I} A_i \longrightarrow A_j, \quad i_j(x) := x(i) \stackrel{\text{not.}}{=} x \quad \text{s.n.}$$

proiecția canonica a produsului direct pe componenta A_i .
(i_j este surjectivă)

②. Fie I și A mulțimi nevide și col. de mulțimi $(A_i)_{i \in I}$ cu $A_i := A, \forall i \in I$. Atunci $\prod_{i \in I} A_i = \{x : I \rightarrow A \mid x = \text{funcție}\} = \text{Func}(I, A) \stackrel{\text{not.}}{=} A^I$

Teorema (proprietatea de universalitate a produsului direct de multimi)

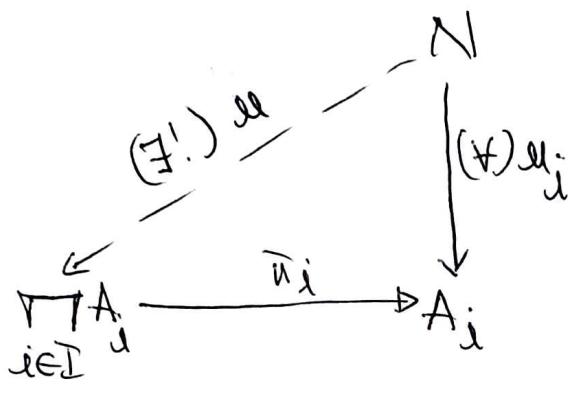
Fie $(A_i)_{i \in I}$ o familie nevidă de multimi nevide.

Atenție: $\forall N =$ multime

$(\exists) u_i : N \rightarrow A_i$ o familie de funcții $(i \in I)$, (\exists)

$u : N \rightarrow \prod_{i \in I} A_i$ o funcție a.t. diagonale sunt comutative.

(i.e. $\pi_j \circ u = u_i, (\forall) i \in I$.)



Multimi numărabile

Definiție: a) Două multimi A și B s.n. echipotente (sau au același cardinal) și notăm asta cu $A \sim B$ (sau $|A| = |B|$) dacă $(\exists) f : A \rightarrow B$ bijedivă.

b) O multime A s.n. numărabilă dacă $A \sim \mathbb{N}$, i.e.

$(\exists) f : \mathbb{N} \rightarrow A$ o familie bijedivă.

c) O multime A s.n. finită dacă $(\exists) n \in \mathbb{N}$ a.t.

$A \sim \{1, \dots, n\}$ în acest caz notăm $|A| = n$.

OBS:

$A =$ numărabilă \Leftrightarrow elementele sale se pot scrie ca un sir infinit, i.e. $A = \{a_0, a_1, \dots, a_n, \dots\}$

TEOREMĂ: Multimea numerelor reale \mathbb{R} nu este numărabilă.

Definiție: Fie A, B două multimi. Spunem că A are cardinal mai mic decât B și notăm $|A| \leq |B|$, dacă $(\exists) f : A \rightarrow B$ o funcție injectivă. Dacă $|A| \leq |B|$ și $|A| \neq |B|$ o notăm $|A| < |B|$.

Teorema: Pentru orice multime A , avem că $|A| \leq |\mathcal{P}(A)|$.

RELATII PE MULTIMI

Definitie: Fie A o multime nevidă. O submultime $\rho \subseteq A \times A$ s.n. relație binară pe A . Dacă $(x, y) \in \rho$, atunci scriem / notăm $x \rho y$.

Ez: i) $\Delta_A := \{(a, a) | a \in A\}$ e o relație pe A , numită diagonala lui A .

Definiții: Fie ρ o relație binară pe A . Atunci:

- a) ρ s.n. reflexivă dacă $\forall x \in A$, ie. $\Delta_A \subseteq \rho$
- b) ρ s.n. simetrică dacă $x \rho y \Rightarrow y \rho x$, $\forall x, y \in A$
- c) ρ s.n. transitivă dacă $x \rho y$ și $y \rho z \Rightarrow x \rho z$, $\forall x, y, z \in A$.
- d) ρ s.n. antisimetrică dacă $x \rho y$ și $y \rho x \Rightarrow x = y$.

Definiții: Fie ρ o relație binară pe A .

- a) ρ s.n. relație de echivalență dacă este reflexivă, simetrică și transitivă.
- b) ρ s.n. relație de ordine (în acest caz poartă numele (A, ρ) și multime ordonată) dacă este reflexivă, antisimetrică și transitivă.

O multime ordonată (A, ρ) se mai notează și cu (A, \leq) .

Definitie: Fie (A, \leq) o multime ordonata.

a) Un element $m \in A$ s.n. maximal dacă $m \leq a, \forall a \in A \Rightarrow a = m$.

b) Un element $p \in A$ s.n. prim element dacă $p \leq x, \forall x \in A$.

c) Fie $B \subseteq A$ o submultime. Un element $a \in A$ s.n.

superiorul (resp. inferiorul) lui B și adem asta

$a = \sup(B)$, (resp. $a = \inf(B)$) dacă au loc următoarele două condiții:

- $\forall x \leq a, \forall x \in B$ (resp., $a \leq x, \forall x \in B$)
- $\forall x \leq a', \forall x \in B \Rightarrow a \leq a'$ (resp., $a' \leq x, \forall x \in B \Rightarrow a' \leq a$).

Fie $B \subseteq (A, \leq)$ o submultime într-o multime ordonată.

Un element $a \in A$ s.n. majorant (resp. minorant) al lui B dacă $x \leq a$ (resp. $a \leq x$), $\forall x \in B$.

O multime ordonată (A, \leq) s.n. latice dacă (\exists)
 $\sup\{a, b\}$ și $\inf\{a, b\}$, $\forall a, b \in A$.

Definiții: Fie (A, \leq) o multime ordonată.

1) (A, \leq) s.n. bine ordonată dacă orice submultime nevidă a sa are un prim element.

2) (A, \leq) s.n. total ordonată dacă ($\forall a, b \in A$ avem $a \leq b$ sau $b \leq a$).

3) (A, \leq) s.n. inductiv ordonată dacă orice submultime total ordonată a sa are un majorant.

Lema lui Zorn: Orice multime inductiv ordonată are un element maximal.

Teorema lui Zermelo: Dacă A e o multime nevidă, atunci există o relație de ordin \leq pe A a.t. (A, \leq) este multime bine ordonată.

ipoteza Continuumului: "Nu există o multime A a.t. $|N|^{\text{nat}} = \aleph_0 < |A| < |R| = |\mathcal{P}(N)|$." - o baza oricărui forume :))

RELATII DE ECHIVALENTĂ

Def: O relație binară ρ pe A s.a. relație de echivalență dacă este reflexivă, simetrică și transitivă.

Notatie: O rel. de echivalență ρ s.n. $a^N \rho b^N$:

$$x \rho y \Leftrightarrow x^N \rho y^N.$$

Ex: ①. Fie $A := \mathbb{Z}$ și $n \in \mathbb{N}$, $n \geq 2$ fixat. Pe \mathbb{Z} definim relația: $a \rho b \stackrel{\text{def}}{\Leftrightarrow} n \mid a-b$; $N = \equiv \pmod{n}$ i.e. $a \equiv b \pmod{n} \stackrel{\text{def}}{\Leftrightarrow} n \mid a-b$.

Atunci $N = \equiv \pmod{n}$ e relație de echivalență pe \mathbb{Z} numită relația de congruență modulo n .

②. Fie $f: A \rightarrow B$ o funcție și pe A definim relația $\rho_f \stackrel{\text{nat}}{=} N_f$ astfel: $a N_f b \stackrel{\text{def}}{\Leftrightarrow} f(a) = f(b)$. Atunci N_f e relație de echivalență pe A numită relația de echivalență inclusă de f .

Definitie: Fie \sim o relatie de echivalenta pe A si $a \in A$. Multimea:

$\hat{a} := \{b \in A \mid b \sim a\}$ s.n. clasa de echivalenta a elementului a . Multimea tuturor claselor de echivalenta se noteaza cu A/\sim si se numeste multimea factor a lui A prin \sim .

Deci, $A/\sim = \{\hat{a} \mid a \in A\}$

Functia $\pi : A \rightarrow A/\sim$, $\pi(a) := \hat{a}$, (\forall) $a \in A$ este surjectiva si s.n. suriectia (proiectia) canonica. ($n_f = n$)

Definitie: Fie A o multime nevida si $(A_i)_{i \in I}$ o familie de submultimi nevide ale lui A . $(A_i)_{i \in I}$ s.n. partitie a lui A daca:

a) $A_i \cap A_j = \emptyset$, (\forall) $i \neq j \in I$

b) $\bigcup_{i \in I} A_i = A$.

Ex: $A_1 := \{2n \mid n \in \mathbb{Z}\}$, $A_2 := \{2n+1 \mid n \in \mathbb{Z}\}$

$\{A_1, A_2\}$ e o partitie a lui \mathbb{Z} .

Propozitie: Fie \sim o relatie de echivalenta pe A .

Atenzi:

1) $a \in \hat{a}$, (\forall) $a \in A$; i.e. $\hat{a} \neq \emptyset$, (\forall) $a \in A$.

2) $\hat{a} = \hat{b} \Leftrightarrow a \sim b$

3) Daca $a, b \in A$. Atenzi: $\hat{a} = \hat{b}$ sau $\hat{a} \cap \hat{b} = \emptyset$

4) $A = \bigcup_{\hat{a} \in A/\sim} \hat{a}$

Definitie: Fie \sim o relatie de echivalenta pe A . O familie de elemente $(a_i)_{i \in I}$ ale lui A s.a. sistem de reprezentanti pentru \sim daca:

- (\forall) $i \neq j \in I$ avem ca $a_i \not\sim a_j$ (a_i nu este echivalent cu a_j).
- (\forall) $a \in A$, (\exists) $i \in I$ a.t. $a \sim a_i$.

o multime

Def (mai pe inteleseul meu): Pentru A , sistem de reprezentanti.

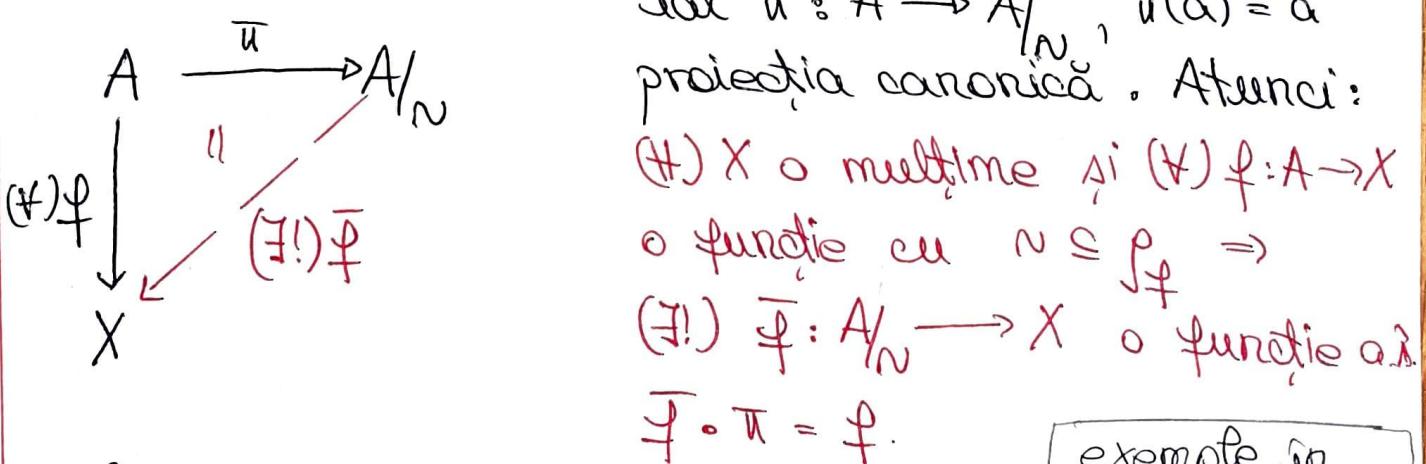
- \forall clasa are un reprezentant in A ($\forall y \in \text{Im } f$, $\exists x \in A$ a.s. $f(x) = y$)
- reprezentantul este unic (daca $x_1 \in A$ si $x_2 \in A$, $\hat{x}_1 \neq \hat{x}_2$ deci $f(x_1) \neq f(x_2)$).

Construcția riguroasă a lui $\mathbb{Z}, \mathbb{Q}, \mathbb{R} \rightarrow$ spus pas (E PREACURATĂ)

Teorema (Proprietatea de universalitate a multimii factor)

Fie A o multime si \sim o relatie de echivalenta pe A ,

iar $\pi : A \rightarrow A/\sim$, $\pi(a) = \bar{a}$ proiecția canonica. Atunci:



(\forall) X o multime si (\forall) $f : A \rightarrow X$ o functie cu $N \subseteq \text{Im } f \Rightarrow$
 $(\exists !) \bar{f} : A/\sim \rightarrow X$ o functie a.i.
 $\bar{f} \circ \pi = f$.

In plus,

- \bar{f} e surjectivă $\Leftrightarrow f$ e surjectivă
- \bar{f} e injectivă $\Leftrightarrow f$ este injectivă

exemplu în curs \rightarrow cap. MULTIMI, pag. 34
+ Seminar

LEGI DE COMPOZITIE. MULTIMI

Definitie: Fie A o multime. O functie $\varphi: A \times A \rightarrow A$ s.n. lege de compozitie pe A . Legea de compozitie $\varphi: A \times A \rightarrow A$ s.n. associativa daca:

$$\varphi(a, \varphi(b, c)) = \varphi(\varphi(a, b), c), (\forall) a, b, c \in A.$$

Un element $e \in A$ s.n. element neutru pentru $\varphi: A^2 \rightarrow A$ daca:

$$\varphi(e, a) = \varphi(a, e) = a, (\forall) a \in A.$$

pe A (o multime)

Definitie (din liceu): „ \circ ” e lege de compozitie daca este parte stabila. i.e. $\forall x, y \in A \Rightarrow x \circ y \in A$.

„ \circ ” e asociativa daca $\forall x, y, z \in A \Rightarrow x \circ (y \circ z) = (x \circ y) \circ z$

„ \circ ” are element neutru daca $\exists e \in A, (\forall) a \in A$ a.t.

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

OBS: - notatie multiplicativa: $\varphi((a, b)) = ab$ ^{not.}

- notatie aditiva: $\varphi((a, b)) = a + b$

In not. multiplicativa, elementul neutru ^{not.} = 1_A sau 1

In notatia aditiva, elementul neutru ^{not.} = 0_A sau 0.

Definitie: Se numeste semigrup o pereche (S, φ) , unde S = multime si $\varphi: S \times S \rightarrow S$ e o lege de compozitie associativa. Se numeste monoid o pereche (M, φ) , unde, M = multime si $\varphi: M \times M \rightarrow M$ e o lege de compozitie associativa si care are element neutru.

Legea asociativității generalizate (L.A.G.)

Fie $f: A \times A \rightarrow A$ o lege de compozitie și $n \in \mathbb{N}^*$.

Definim recursiv functiile $f_n: \underbrace{A \times A \times \dots \times A}_{\text{de } n \text{ ori}} \rightarrow A$ astfel:

$f_1 := \text{id}_A$, $f_2 := f$ și presupunând că avem definit f_n , definim :

$$f_{n+1}(a_1, \dots, a_{n+1}) := \underset{\text{def}}{f(f_n(a_1, \dots, a_n), a_{n+1})} \quad (1)$$

TEOREMĂ (L.A.G.): Fie $f: A \times A \rightarrow A$ o lege de compozitie associativă. Atunci, $\forall m, n \in \mathbb{N}$ și $\forall a_1, \dots, a_{m+n} \in A$ avem :

$$(2) \quad f(f_m(a_1, \dots, a_m), f_n(a_{m+1}, \dots, a_{m+n})) = f_{m+n}(a_1, \dots, a_{m+n})$$

Ideeua teoremei de mai sus este că nu contează unde sunt parantezele.

Ex: Fie $f: A \times A \rightarrow A$, $f(a, b) \stackrel{\text{not.}}{=} ab$ o lege de compozitie associativă i.e. $\forall a, b, c \in A$ a?

$$a(bc) = (ab)c \stackrel{\text{not.}}{=} abc$$

Dacă notăm $f_n(a_1, \dots, a_n) \stackrel{\text{not.}}{=} a_1 a_2 \dots a_n$ atunci (2)

se scrie astfel:

$$(a_1, \dots, a_m)(a_{m+1}, \dots, a_{m+n}) = a_1 \dots a_{m+n}$$

NOTAȚIE: O lege de compozitie $f: A \times A \rightarrow A$ va fi notată tot timpul ~~cu~~ multiplicativ, $f(a, b) \stackrel{\text{not.}}{=} ab$.

Elem. neutru (dacă \exists) se va nota cu 1_A sau 1 .

Definiții: 1) Fie (S_1, \cdot) , $(S_2, *)$ două semigrupuri. O funcție $f: S_1 \rightarrow S_2$ s.n. morfism de grupuri dacă $f(x \cdot y) = f(x) * f(y)$, $\forall x, y \in S_1$

2) Fie M_1 și M_2 doi monoizi. O funcție $f: M_1 \rightarrow M_2$ s.n. morfism de monoizi dacă:

- $f(1_{M_1}) = 1_{M_2}$
 - $f(x \cdot y) = f(x) f(y)$, $\forall x, y \in M_1$.
- prima lege a doua lege.

OBS: Dacă $f: M_1 \rightarrow M_2$ morfism bijectiv de monoizi, atunci $f^{-1}: M_2 \rightarrow M_1$ e morfism de monoizi.

Definiție: Un morfism de monoizi $f: M_1 \rightarrow M_2$ s.n. izomorfism de monoizi dacă $\exists g: M_2 \rightarrow M_1$ morfism de monoizi a.t. $f \circ g = id_{M_2}$ și $g \circ f = id_{M_1}$

(În licență): $f: M_1 \rightarrow M_2$ e izomorfism de monoizi dacă: 1) f morfism de monoizi
2) f e bijectivă.

Reguli de calcul într-un monoid

Fie M un monoid notat multiplicativ cu elementul neutru 1 . Pentru $x \in M$ și $n \in \mathbb{N}$ notăm:

$$x^0 := 1 \quad \text{și} \quad x^n := \underbrace{x \cdot x \cdots x}_{\text{de } n \text{ ori}}$$

(în notația aditivă, $0x := 0$ și $nx = \underbrace{x + \cdots + x}_{\text{de } n \text{ ori}}$)

Așa că:

- 1) $x^m \cdot x^n = x^{m+n}$, (\forall) $m, n \in \mathbb{N}$
- 2) $(x^m)^n = x^{mn}$, (\forall) $m, n \in \mathbb{N}$
- 3) Dacă $x^y = y^x \Rightarrow (xy)^n = x^n y^n$.

Monoidul liber generat de o multime (nu prea important)

Fie A o multime nevidă; o numim "alfabet".

S.n. cuvânt cu elemente din A un sistem ordonat finit de elemente din A de forma $a_1 a_2 \dots a_n$ ($n \in \mathbb{N}$).

Două cuvinte $x = a_1 a_2 \dots a_n$, $y = b_1 b_2 \dots b_t$ sunt egale $\Leftrightarrow \underset{\text{def}}{n} = t$ și $a_i = b_i$, (\forall) $i = \overline{1, n}$.

Fie $L(A) :=$ multimea tuturor cuvintelor cu elemente din A , inclusiv cuvântul vid \emptyset . Atunci $L(A)$ are o structură de monoid cu :

- $x = a_1 \dots a_n$, $y = b_1 b_2 \dots b_t$ definim

$$x \cdot y := \underset{\text{def}}{a_1 a_2 \dots a_n b_1 \dots b_t}$$

numita concatenarea cuvintelor

- $L(A) := \emptyset$, i.e. $x \cdot \emptyset = \emptyset \cdot x = x$, (\forall) $x \in L(A)$.

neemite monoidul liber generat de multimea A.

Elemente inversabile intr-un monoid

Def Fie (M, \circ) un monoid cu elementul neutru \perp . Un element $a \in M$ s.n. inversabil dacă $\exists a' \in M$ a.i. $aa' = a'a = \perp$.

Notam $U(M) := \{a \in M \mid a \text{ element inversabil}\}$.

OBS: inversul unui element $a \in M$ = monoid, dacă există, este unic și se notează cu a^{-1} .

Prop: Fie M un monoid și $x_1, \dots, x_n \in U(M)$ elemente inversabile. Atunci $x_1 x_2 \dots x_n \in U(M)$ și

$$(x_1 x_2 \dots x_n)^{-1} = x_n^{-1} x_{n-1}^{-1} \dots x_2^{-1} x_1^{-1}.$$

OBS: Dacă M e un monoid putem forma monoidul opus $(M^{\text{op}}, *)$, unde $M^{\text{op}} := M$ (ca multime) și legea de compozitie este $x * y := y * x$, $(*)x, y \in M^{\text{op}} = M$.

- $S: U(M) \xrightarrow{\cong} U(M)^{\text{op}}$, $S(x) := x^{-1}$ este un izomorfism de monizi cu $S^2 = \text{id}_M$.

	SEMIGRUP	MONOID	GRUP
associativitate	✓	✓	✓
element neutru		✓	✓
toate elem. inversabile			✓
optimiza [FREE]		[LITE]	[PREMIUM]

GRUPLURI

Definitie Se numeste grup un monoid (G, \cdot) în care orice element este inversabil, i.e. $\cup(G) = G$.

Explicit, un grup este un triplet $G = (G, \cdot, I)$, unde G e o multime (nevidă), $\cdot : G \times G \rightarrow G$ este o lege de compozitie, $I \in G$ a.i.

a) \cdot este associativa, i.e. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, $\forall x, y, z \in G$.

b) I este elementul neutru pentru \cdot , i.e. $x \cdot I = I \cdot x = x$, $\forall x \in G$.

c) $\forall x \in G \exists y \in G$ a.i. $xy = yx = I$.

În plus, un grup G s.n. abelian (sau comutativ) dacă legea de compozitie este comutativă, i.e.:

$$x \cdot y = y \cdot x, \forall x, y \in G.$$

NOTATIE: Ca și la monoidi, legea de comp. într-un grup G va fi notată multiplicativ $\ell(x, y) = xy$, iar elementul neutru cu I_G sau mai simplu cu I .

Definitie: Fie G_1, G_2 două grupe. O funcție $f: G_1 \rightarrow G_2$ s.n. morfism de grupe dacă $f(xy) = f(x)f(y)$, $\forall x, y \in G_1$. În plus, f s.n. izomorfism dacă $(\exists) g: G_2 \rightarrow G_1$ morfism de grupe a.i. $f \circ g = id_{G_2}$ și $g \circ f = id_{G_1}$. Două grupe G_1 și G_2 s.n. izomorfe și scriem asta $G_1 \cong G_2$ dacă $(\exists) f: G_1 \rightarrow G_2$ un izomorfism de grupe.

Licență: $(G_1, \circ), (G_2, *)$ - grupuri. $f: G_1 \rightarrow G_2$ s.t.
morfism de grupuri dacă $f(x \circ y) = f(x) * f(y), \forall x, y \in G_1$.

$f: G_1 \rightarrow G_2$ e izomorfism de grupuri dacă:

- 1) f e morfism de grupuri
- 2) f e bijedivă.

• $(\text{Aut}(G), \circ) := \{ f: G \rightarrow G \mid f \text{ izomorfism de grupuri} \}$
este un grup cu operația de compunere egală,
numit grupul automorfismelor grupului G ; $\text{id}_G = \text{id}_{\text{Aut}(G)}$.

Prop: Fie $f: G_1 \rightarrow G_2$ un morfism de grupuri

Atunci:

$$\text{i)} f(1) = 1$$

$$\text{ii)} f(a^{-1}) = f(a)^{-1}, \forall a \in G_1$$

$$\text{iii)} f(a^n) = f(a)^n, \forall a \in G_1, n \in \mathbb{Z}.$$

(Transferul de structură) Fie G = grup, X = multime și
 $f: G \xrightarrow{\sim} X$ o funcție bijedivă. Atunci, (\exists) o structură
de grup multimea X a.i. f este izomorfism de
grupuri.

În acest caz, spunem că $"*"$ se obține prin
transferul structurii de grup de pe G pe X via f .

Subgrupuri. Teorema de corespondență pt. subgrupuri

Def: Fie $G = (G, \circ)$ un grup și $H \subseteq G$ o submultime.

H s.n. subgrup în G (notăm $H \leq G$) dacă:

(1) H e parte stabilă a lui G , i.e. $(\forall) x, y \in H \Rightarrow xy \in H$

(2) $1 \in H$

(3) Dacă $x \in H \Rightarrow x^{-1} \in H$.

Notăm $\mathcal{L}(G) := \{H \mid H \leq G\}$; ea este o latice (în raport cu relația de incluziune) numită laticea subgrupelor lui G .

Prop: Fie $f: G_1 \rightarrow G_2$ un morfism de grupuri. Atunci:

a) Dacă $H \leq G_1 \Rightarrow f(H) \leq G_2$

b) Dacă $K \leq G_2 \Rightarrow f^{-1}(K) \leq G_1$
fibra.

OBS: Fie G = grup și $H \subseteq G$. Atunci

$$H \leq G \Leftrightarrow xy^{-1} \in H, (\forall) x, y \in H.$$

COROLAR Fie $f: G_1 \rightarrow G_2$ morfism de grupuri.

Atunci:

a) $\text{Im}(f) = f(G_1) \leq G_2$

b) $f^{-1}(\{1\}) = \{x \in G_1 \mid f(x) = 1\} \stackrel{\text{not.}}{=} \text{ker}(f) \leq G_1$

s.n. nucleul lui f .

OBS (imp.): 1 în coloral reprezentă elementul neutru
(adică 1_{G_2})

Propozitie: Fie $f: G_1 \rightarrow G_2$ morfism de grupuri.

Atenții:

- a) f este surjectiv $\Leftrightarrow \text{Im } (f) = G_2$
- b) f este injectiv $\Leftrightarrow \text{Ker } (f) = \{1\}$.

Definție: Un grup G_1 se poate scoala într-un grup G_2 dacă $\exists f: G_1 \rightarrow G_2$ morfism injectiv de grupuri (i.e. dacă G_1 este izomorf cu un subgrup al lui G_2).

Teoremă (Cayley): Orice grup se poate scoala într-un grup de permutări.
nu stiu ce și că ea ...

Teorema de corespondență pentru subgrupuri

Fie $f: G_1 \rightarrow G_2$ un morfism surjectiv de grupuri.

Atenții funcția:

$$F: \{ H \mid H \leq G_1, H \supseteq \text{Ker } (f) \} \xrightarrow{\cong} \mathcal{L}(G_2)$$

$F(H) := f(H)$ este bijecțivă

Propozitie: Fie G un grup și $(H_i)_{i \in I}$ o familie de subgrupuri ale lui G . Atenții:

$\prod_{i \in I} H_i \leq G$ este subgrup în G .

Definție: Fie G un grup și $X \subseteq G$ o submulțime nevidată.

Atenții:

$\langle X \rangle := \bigcap_{X \subseteq H \leq G} H$ s.n. subgrupul generat de X .

Propozitie: Fie $G = \text{grup}$ și $X \subseteq G$. Atunci:

$$\langle X \rangle = \left\{ x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} \mid n \in \mathbb{N}^*, x_i \in X, \varepsilon_i \in \{-1, 1\} \right\} \quad (\forall) i = \overline{1, n}$$

Dacă $G = \text{grup}$ și $A, B \subseteq G$ notăm

$$AB := \{ab \mid a \in A, b \in B\}$$

$$A^{-1} := \{a^{-1} \mid a \in A\}$$

$$\text{Dacă } A = \{a\}, \{a\}B \stackrel{\text{not.}}{=} aB = \{ab \mid b \in B\}$$

Produs direct de grupuri \rightarrow pas prea ușor... :)))

Relatii de echivalență pe un grup. Teorema Lagrange

Def: Fie G un grup și $H \leq G$. Fie $x, y \in G$.

a) spunem că x este congruent la stânga modulo H cu y , și scriem asta ca $x \equiv_L y \pmod{H} \Leftrightarrow \begin{cases} x^{-1}y \in H \\ x, y \in H \end{cases}$

b) — _{$_R$} — congruent la dreapta modulo H cu y , și scriem asta $x \equiv_R y \pmod{H} \Leftrightarrow xy^{-1} \in H$.

Propozitie: Fie $H \leq G$ un subgrup în grupul G . Atunci relația de congruență la stânga (resp. la dreapta) modulo H este o relație de echivalență pe mulțimea G .

$\left. \begin{array}{l} \text{reflexivitate} \\ \text{simetrie} \\ \text{transitivitate} \end{array} \right\}$

Multimile factor făță de cele două relații vor fi notate:

$$(G/H)_{\Delta}^{\text{not.}} = G/\equiv_{\Delta}^{\text{not.}}(\text{mod } H), \quad (G/H)_d^{\text{not.}} = G/\equiv_d^{\text{not.}}(\text{mod } H)$$

Dacă $x \in G$, clasa sa de echivalență la stânga este $\hat{x}^{\Delta} = \{y \in G \mid \hat{x}^{-1}y \in H\} = \{y \in G \mid y \in xH\} = \{xh \mid h \in H\} = xH$.

Analog, pentru $\hat{x}^d = Hx$.

Un sistem de reprezentanți pentru $\equiv_{\Delta}^{\text{not.}}(\text{mod } H)$ s.n. transversală la stânga a lui G prin H .

Prop - Definitie: Fie G un grup și $H \leq G$. Atunci multimile $(G/H)_{\Delta}$ și $(G/H)_d$ sunt cardinal echivalente. i.e. \exists $\varphi: (G/H)_{\Delta} \xrightarrow{\sim} (G/H)_d$ o funcție bijecțivă.

Numește indicele lui H în G numărul cardinal $|(G/H)_{\Delta}| = |(G/H)_d| = |G:H|$ și se numește indicele lui H în G .

OBS: • Spunem că un subgrup H într-un grup G are indice finit dacă $|G:H|$ este un număr natural.

În caz contrar, spunem că H are indice infinit în G și scriem $|G:H| = \infty$.

- Dacă un grup este finit $\Rightarrow |G:H|$ este finit ($\forall H \leq G$), căci multimea factor $(G/H)_{\Delta}$ e finită.

Teorema (Lagrange):

Fie G un grup finit și $H \leq G$ un subgroup în G .

Așadar: $|G| = |H| \cdot |G : H|$

În particular, $|H|$ divide $|G|$.

Corolar (transitivitya indicelelor) Fie G un grup

finat și $K \leq H \leq G$. Așadar:

$$|G : K| = |G : H| \cdot |H : K|$$

Consecință: Fie $p =$ număr prim, G un grup finit, $K \leq G$

a.s. $|G : K| = p$. Fie $H \leq G$ a.s. $K \leq H \leq G \Rightarrow H = K$

sau $H = G$.

Def: Un grup G s.n. ciclic dacă (\exists) $g \in G$ a.s.

$$G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

Corolar: Fie $p =$ număr prim și G un grup, $|G| = p$.

Așadar G este ciclic.

Subgrupuri normale

Definitie: Fie G un grup și $H \leq G$ un subgroup al său.

Așadar H s.n. subgroup normal al lui G (și notăm asta $H \trianglelefteq G$) dacă $\forall h \in H \quad \forall x \in G \quad x^{-1}hx \in H$.

i.e. ($\forall x \in G$ și $\forall h \in H$ avem că $x^{-1}hx \in H$,

i.e. ($\forall x \in G$ și $\forall h \in H$ avem că $x^{-1}hx \in H$,

(exemplu: S_7 - cerc.)

$H := \{1\} \trianglelefteq G \Rightarrow$ subgrupuri normale triviale

$H := G \trianglelefteq G$

Propozitie: Fie G un grup și $H \leq G$ un subgroup al său. S.E.A :

- a) $H \trianglelefteq G$
- b) $\forall h \in H, \forall x \in G \Rightarrow hxh^{-1} \in H$
- c) $\forall h \in H, \forall x \in G \Rightarrow hx = xh$
- d) $(G/H)_\Delta = (G/H)_d$

Cordar: Fie G = grup, $H \leq G$ cu $[G:H] = 2 \Rightarrow H \trianglelefteq G$.

Propozitie: Fie $f: G_1 \rightarrow G_2$ morfism surjectiv de grupeuri. Atunci, funcția :

$$F: \{H \trianglelefteq G_1 \mid H \supseteq \text{ker}(f)\} \xrightarrow{\sim} \{K \mid K \trianglelefteq G_2\}, F(H) := f(H)$$

este bijecțivă.

Grupul factor

Propozitie: Fie G un grup și $H \trianglelefteq G$ subgroup normal.

Atunci G/H are o strucțură de grup cu

$$\hat{x} \cdot \hat{y} := \widehat{xy}, \quad (\forall) \hat{x}, \hat{y} \in G/H \text{ numit}$$

grupul factor al lui G prin H . În plus $\pi: G \rightarrow G/H$, $\pi(x) := \hat{x}, (\forall) x \in G$ e morfism surjectiv de grupeuri și $\text{ker}(\pi) = H$.

Teorema (Proprietatea de universalitate a grupului factor)

Fie G un grup, $H \trianglelefteq G$ și $\bar{u}: G \rightarrow G/H$ proiecția canonica, $\bar{u}(g) = \hat{g}$, $\forall g \in G$. Atunci :

$$\begin{array}{ccc} G & \xrightarrow{\bar{u}} & G/H \\ (\exists!) \varphi \downarrow & \parallel & \swarrow (\exists!) \bar{\varphi} \\ G' & & \end{array}$$

(+) G' un grup și (+) $\varphi: G \rightarrow G'$ morfism de grupuri cu $\text{Ker}(\varphi) \trianglelefteq H$

(+) $\bar{\varphi}: G/H \rightarrow G'$ morfism de grupuri a.s. $\bar{\varphi} \circ \bar{u} = \varphi$.

În plus,

- a) $\bar{\varphi}$ este surjectiv $\Leftrightarrow \varphi$ este surjectiv
- b) $\bar{\varphi}$ este injectiv $\Leftrightarrow \text{Ker}(\varphi) = H$.

example la pag. 62-63 urm.

Teorema (Teorema fundamentală de izomorfism) (T.F.i)

Fie $f: G \rightarrow G'$ un morfism de grupuri. Atunci

$$\tilde{f}: G/\text{Ker}(f) \xrightarrow{\cong} \text{im}(f), \quad \tilde{f}(\tilde{x}) := f(x), \quad \forall \tilde{x} \in G/\text{Ker}(f)$$

este un izomorfism de grupuri. În particular, dacă f este surjectiv $\Rightarrow G/\text{Ker}(f) \cong G'$

Teorema I de izomorfisme pt. grupuri (facultativ)

Fie $f: G_1 \rightarrow G_2$ morfism surjectiv de grupuri și $H \trianglelefteq G_1$ a.s. $H \supseteq \text{Ker}(f)$. Atunci $f(H) \trianglelefteq G_2$ și există un izomorfism de grupuri $G_2/f(H) \cong G_1/H$.

Teorema II de izomorfismu pt. grupuri

Fie G un grup, $H, K \leq G$ a.i. $H \triangleleft K$.

Atenție:

a) $\langle HK \rangle = HK$ și $H \cap K \triangleleft K$.

b) Există un izomorfism de grupuri

$$HK/H \cong K/H \cap K$$

Ordinalul unei elemente

Fie G = grup și $g \in G$. Fie funcția

$$\varphi_g : \mathbb{Z} \rightarrow G, \varphi_g(m) := g^m, \forall m \in \mathbb{Z}.$$

Atenție φ_g e morfism de grupuri $\Rightarrow \text{Ker } (\varphi_g) \leq \mathbb{Z}$

$\Rightarrow (\exists !) n_g \in \mathbb{N}$ a.i.

$$\text{Ker } (\varphi_g) = \{m \in \mathbb{Z} \mid g^m = 1\} = n_g \mathbb{Z}.$$

Definiție: Fie G un grup, $g \in G$ și $\varphi_g : \mathbb{Z} \rightarrow G$,
 $\varphi_g(m) = g^m$, $\text{Ker } (\varphi_g) = n_g \mathbb{Z}$.

a) Spunem că g are ordinalul infinit și scriem $\theta(g) = \infty$
dacă $n_g = 0$, i.e. dacă $g^m \neq 1, \forall m \in \mathbb{Z}, m \neq 0$.

b) Spunem că g are ordinalul n_g și scriem $\theta(g) = n_g$
dacă $n_g \geq 1$.

OBS: ①. Fie G = grup, $g \in G$ a.i. $\theta(g) = n \geq 1$. Atenție
pentru $m \in \mathbb{N}$ avem $g^m = 1 \Leftrightarrow n \mid m$.

② Cum $\vartheta(g)$ este generatorul subgrupului $\text{Ker}(fg)$, $\vartheta(g)$ se poate redefini elementar astfel:

$$\vartheta(g) := \begin{cases} \infty, & \text{daca } g^m = 1, \forall m \in \mathbb{Z} \setminus \{0\} \\ \min\{m \in \mathbb{N}^* \mid g^m = 1\}, & \text{daca } (\exists m \in \mathbb{Z}^*) \text{ a.i. } g^m = 1. \end{cases}$$

Propozitie: Fie G un grup și $g \in G$. Atunci

$$\vartheta(g) = |\langle g \rangle|.$$

Corolar: Fie G un grup finit și $g \in G$.
Atunci, $\underline{\vartheta(g)} \mid |G|$ și $\hat{g}^{|G|} = 1$.

indicatorul lui Euler: funcția $\varphi: \mathbb{N}^* \rightarrow \mathbb{N}^*$,
 $\varphi(n) :=$ numărul întregilor $1 \leq k < n$ și primii cu n s.a.n. indicatorul lui euler.

$$\text{i.e. } \varphi(n) := |\{a \in \{1, 2, \dots, n-1\} \mid (a, n) = 1\}|$$

$$\text{Cum } U(\mathbb{Z}_n) = \{\hat{b} \in \mathbb{Z}_n \mid (b, n) = 1\} \Rightarrow \varphi(n) = |U(\mathbb{Z}_n)|$$

Corolar (teorema lui Euler)

Fie $a, n \in \mathbb{N}^*$ numere naturale prime între ele.
Atunci $a^{\varphi(n)} \equiv 1 \pmod{n}$

Corolar (mica teoremă a lui Fermat)

Fie p un număr prim și $a \in \mathbb{N}$ nedivizibil cu p .
Atunci $a^{p-1} \equiv 1 \pmod{p}$

Lucruri bine de știut:

- $g \in G$ (grup), $\text{ord}(g) = n \geq 1$ și $k \in \mathbb{N}^*$

Atunci : a) $\text{ord}(g^k) = \frac{n}{(n, k)}$

b) $\underbrace{g^k}$ e generator în $\langle g \rangle \Leftrightarrow (n, k) = 1$

c) numărul de generatori din $(\mathbb{Z}_n, +)$ este $\varphi(n)$.

Grupuri ciclice

Un grup G s.n. ciclic dacă $\exists g \in G$ a.s. $G = \langle g \rangle$.

Teoremă (de structură a grupurilor ciclice)

Fie G un grup ciclic. Atunci :

a) $G \cong (\mathbb{Z}, +)$, dacă G este infinit

b) $G \cong (\mathbb{Z}_n, +)$, dacă G e finit și $|G| = n$.

Lema chineză a resturilor

Fie $m, n \in \mathbb{N}^*, (m, n) = 1$. Atunci :

$$\varphi: \mathbb{Z}_{mn} \xrightarrow{\cong} \mathbb{Z}_m \times \mathbb{Z}_n$$

$$\varphi(\hat{x}) := (\bar{x}, \bar{\bar{x}}), \forall \hat{x} \in \mathbb{Z}_{mn}$$

este un izomorfism de grupe.

GRUPLURI DE PERMUTĂRI

Dacă M este o mulțime nevidă, notăm cu Σ_M sau S_M grupul de permutări pe M . Adică,

$\Sigma_M = S_M := \{ f: M \rightarrow M \mid f \text{ bijedivă} \}$, care este grup (necomutativ dacă $|M| > 2$) cu compunerea și inversa a funcțiilor și $I_{S_M} = \text{id}_M$.

În particular, dacă $M = \{1, 2, \dots, n\}$, $n \in \mathbb{N}^*$, atunci

$S_{\{1, \dots, n\}} \stackrel{\text{nd.}}{=} S_n$ s.n. grupul permutărilor de grad n.

Evident $|S_n| = n!$, iar un element $\tau \in S_n$ se notează ca un tabel

$$\tau \stackrel{\text{not.}}{=} \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix}$$

! Orice grup cu n elemente este izomorf cu un subgrup în S_n .

Definiție: Fie $n \in \mathbb{N}$, $n \geq 2$ și $\tau \in S_n$. O pereche (i, j) , $i, j \in \{1, \dots, n\}$ s.n. inversiune a lui τ dacă :

$i < j$ și $\tau(i) > \tau(j)$

Notatie: $\text{inv}(\tau) \stackrel{\text{def}}{=} \text{numărul inversiunilor lui } \tau$.

Definiție: Fie $n \geq 2$ și $\tau \in S_n$. Numărul

$$\epsilon(\tau) \stackrel{\text{def}}{=} \prod_{1 \leq i < j \leq n} \frac{\tau(j) - \tau(i)}{j - i}$$

a.n. ~~signatură~~ semnul (signatura) lui τ .

Definitie: Fie $n \geq 2$ și $\tau \in S_n$. Atunci

$$\varepsilon(\tau) = (-1)^{\text{inv}(\tau)} \in \{-1, 1\}$$

τ s.n. permutare pară (resp. impară) dacă

$$\varepsilon(\tau) = 1 \text{ (resp. } \varepsilon(\tau) = -1)$$

$A_n := \{\tau \in S_n \mid \varepsilon(\tau) = 1\}$ s.n. grupul alterr de grad n.

Definitie: Fie $n \geq 2$, și $1 \leq i < j \leq n$. Permutarea

$\tau_{ij}^{\text{not}} = (i \ j) \in S_n$ definită prin:

$$\tau_{ij}^{(K)} := \begin{cases} K, & K \neq i, K \neq j \\ j, & K = i \\ i, & K = j \end{cases}$$

se numește transpozitie.

Propozitie: Fie $n \geq 2$. Atunci funcția signată

$\varepsilon: S_n \rightarrow \{-1, 1\}$, $\tau \mapsto \varepsilon(\tau)$ este un morfism surjectiv de grupe, unde $(\{-1, 1\}, \cdot)$ este grupul cu înmulțirea și adunare.

În particular, $A_n = \text{ker}(\varepsilon) \trianglelefteq S_n$ și $|A_n| = \frac{n!}{2}$.

Definitie: Fie $n \geq 2$, $\tau \in S_n$ și $K \in \{1, \dots, n\}$. Multimea

$$\Theta_{\tau}(K) := \{ \tau^i(K) \mid i \in \mathbb{Z} \} =$$

$$= \{K, \tau(K), \tau^{-1}(K), \tau^2(K), \tau^{-2}(K), \dots\}$$

se numește τ -orbita lui K. $\Theta_K(K)$ s.n. trivială dacă

$$\Theta_{\tau}(K) = \{K\}, \text{i.e. dacă } K \text{ e pct. fix al lui } \tau$$

Propozitie: Fie $n \geq 2$, $\tau \in S_n$, $K \in \{1, \dots, n\}$. Fie $m := \text{cel mai mic număr natural nenul a.i. } \tau^n(m) = K$. Atunci:

$$\Theta_{\tau}^m(K) = \{K, \tau(K), \dots, \tau^{m-1}(K)\}.$$

Exemplu: Fie $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 1 & 7 & 5 & 8 & 6 \end{pmatrix} \in S_8$

τ -orbitele acestei permutări sunt:

$$\Theta_{\tau}(1) = \{1, 3, 4\}, \quad \Theta_{\tau}(2) = \{2\}$$

$$\Theta_{\tau}(5) = \{5, 7, 8, 6\} = \Theta_{\tau}(7) = \Theta_{\tau}(8) = \Theta_{\tau}(6)$$

$\Theta_{\tau}(1) = \Theta_{\tau}(3) = \Theta_{\tau}(4)$, i.e. τ are 3 orbite, una trivială și două netriviale.

OBS: Fie $\tau \in S_n$. Atunci toate orbitele sunt triviale (i.e. $\Theta_{\tau}(K) = \{K\}, \forall K = \overline{1, n}\} \Leftrightarrow \tau = e$, permutarea identică).

Definitie: Fie $n \geq 2$. O permutare $\tau \in S_n$ s.n. ciclu dacă are o singură orbită netrivială, pe care o să o notăm cu Θ_{τ} . În acest caz, $l(\tau) := |\Theta_{\tau}|$ s.n. lungimea ciclului τ .

OBS: Fie $\tau \in S_n$. Atunci τ este ciclu de lungime 2 $\Leftrightarrow \tau$ e o transpozitie.

Ex. Pe τ de mai sus o putem scrie ca produs de cicli astfel: $\tau = (1 \ 3 \ 4)(5 \ 7 \ 8 \ 6)$

Definitie: Dacă cicli $\tau, \sigma \in S_n$ sunt disjuncti dacă $\Omega_\tau \cap \Omega_\sigma = \emptyset$, i.e. două orbite netriciviale sunt multimi disjuncte.

Propozitie: Fie $\tau, \sigma \in S_n$ doi cicli disjuncti. Atunci, $\tau\sigma = \sigma\tau$. (cicli disjuncti comută)

Propozitie: Fie $2 \leq m \leq n$ și $\tau = (i_1 i_2 \dots i_m) \in S_n$ un ciclu de lungime m . Atunci:

$$a) \tau^{-1} = (i_m i_{m-1} \dots i_2 i_1)$$

$$b) \ell(\tau) = m = l(\tau)$$

BINE De sănătate minte:

τ capodul de transpozitii

$$\tau := (i_1 i_2 \dots i_m) = (i_1 i_2)(i_2 i_3) \dots (i_{m-1} i_m)$$

$$\Rightarrow \varepsilon((i_1 i_2 \dots i_m)) = (-1)^{m-1} = (-1)^{l(\tau)-1}.$$

• cicli de lungime 3, 5, 7 ... = permutări parne.

Teorema: Fie $n \geq 2$ și $\tau \neq e, \tau \in S_n$. Atunci τ se poate descompune ca un produs de cicli disjuncti. Mai mult, abstracție făcând de ordinea termenelor, descompunerea este unică.

Exemplu: $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 1 & 4 & 9 & 10 & 8 & 2 & 6 & 9 \end{pmatrix}$

$$\tau = (1 3)(2 5 7 8)(6 10 9)$$

Corolar 1: Fie $n \geq 2$, $\tau \in S_n$ și $\tau = \zeta_1 \zeta_2 \dots \zeta_r$, descomp. ca produs de cicli disjuncti. Atunci:

$\theta(\tau) = [\ell(\zeta_1), \dots, \ell(\zeta_r)]$, cel mai mic multiplu comun al lungimii cicilor componente.

P.e exemplu anterior: $\theta(\tau) = [2, 4, 3] = 12$

Corolar 2: Orice permutare $\tau \in S_n$ este un produs de transpoziții (dar scrierea nu neapărat unică).

Grupul diedral \rightarrow pas

INELE	+ CORPLURI
-------	------------

Definiție: Se numește inel un triplet (R, α, β) , unde R e o multime nevidă, $\alpha, \beta : R \times R \rightarrow R$ sunt două funcții a.î.

1) (R, α) un grup abelian; notăm $\alpha((a, b)) = a + b$

$(\forall) a, b \in R$ și elementul neutru cu 0_R sau 0 .

2) (R, β) este un monoid; notăm $\beta((a, b)) = ab$,

$(\forall) a, b \in R$ și elementul neutru cu 1_R sau 1 .

3) (distributivitatea) Au loc următoarele egalități:

$$a(b+c) = ab + ac$$

$$(a+b)c = ac + bc, (\forall) a, b, c \in R$$

În plus, R s.n. inel comutativ dacă $ab = ba, (\forall)$ $a, b \in R$.

Liceu: $(R, \circ, *)$ - inel dacă:

- (R, \circ) - grup abelian
- $(R, *)$ - monoid
- $*^*$ este distributivă față de \circ :

$$a * (b \circ c) = (a * b) \circ (a * c)$$

$$(a \circ b) * c = (a * c) \circ (b * c)$$

+ dacă $(R, *)$ - monoid comutativ \Rightarrow inel comutativ

Definiție: Fie R un inel și $a \in R$.

1) • a s.n. divizor al lui zero la stânga (resp. dreapta) dacă (\exists) $0 \neq b \in R$ a.t. $ab = 0$ (resp. $ba = 0$)

• a s.n. divizor al lui zero dacă este divizor al lui zero și la stânga și la dreapta.

Un inel R s.n. integral dacă 0_R este singurul divizor al lui zero.

Un inel comutativ și integral s.n. domeniu de integritate.

2) • a s.n. inversabil la stânga (resp. la dreapta) dacă (\exists) $b \in R$ a.t. $ab = 1$ (resp. $ba = 1$)

• a s.n. inversabil dacă este inversabil și la stânga și la dreapta.

R s.n. CORP dacă orice element nenul al său este inversabil.

Reguli de calcul într-un inel.

Dacă R este un inel, atunci:

- $a_0 = 0 \quad a = 0, \forall a \in R$
- $a(-b) = (-a)b = -ab, \forall a, b \in R$
- Dacă $ab = ba$ și $n = \mathbb{N}^*$ ⇒ $(a+b)^n = \sum_{k=0}^n C_n^k a^{n-k} b^k$.

Notatie dacă $m \in \mathbb{N}^*$ și $x \in R$, atunci:

$$mx := \underbrace{x + \dots + x}_{\text{de } m \text{ ori}}$$

OBS: ①. $\mathbb{Z}, \mathbb{Z}[i] = \{a+bi | a, b \in \mathbb{Z}\}$ sunt domenii de integritate

②. $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R})$ sunt divizori ai lui zero
în $M_2(\mathbb{R})$

④. $U(\mathbb{Z}) = \{\pm 1\}, U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$

⑤. $a \in R$ este inversabil ⇔ $\exists b \in R$ a.t. $ab = ba = 1$.
Un astfel de b , dacă există este unic și se notează a^{-1} .

Definiție. Fie R inel și $S \subseteq R$. S s.n. subinel al lui R dacă:

- $1 \in S$
- $x-y \in S, \forall x, y \in S$
- $xy \in S, \forall x, y \in S$.

ex: \mathbb{Z} subinel în corpul \mathbb{Q}
 \mathbb{Z} subinel în $\mathbb{Z}[i]$

Definitie: Fie R = inel și $I \subseteq R$. I s.n. ideal stâng (resp. drept) al lui R și vorbim astăzi $I \leq_A R$ (resp. $I \leq_d R$), dacă:

1) $I \leq (R, +)$, i.e. $x - y \in I$ ($\forall x, y \in I$)

2) ($\forall r \in R$ și $\forall x \in I$ avem că $r x \in I$ (resp. $x r \in I$))

I s.n. ideal bilateral al lui R dacă este ideal stâng și drept al lui R . Notăm $I \leq R$.

Propozitie: Fie R = inel și $I \leq_A R$ (resp. $I \leq_d R$).

Atunci, $I = R \Leftrightarrow I$ conține un element inversabil

Corolar Fie R = inel comutativ. Atunci R este corp \Leftrightarrow singurile sale ideale sunt $\{0\}$ și R .

Definitie: Fie R = inel și $E \subseteq R$ o submultime. Fie

$$(E)_l := \bigcap_{\substack{I \leq_A R \\ I \ni E}} I ; |E| := \bigcap_{\substack{I \leq_d R \\ I \ni E}} I ; (E) := \bigcap_{\substack{J \leq R \\ J \ni E}} J$$

Atunci $(E)_l, |E|$ și (E) s.n. ideal stâng / drept / bilateral generat de E .

Un ideal stâng I (resp. drept, bilateral) s.n. finit generat dacă există $E \subseteq R$ finită a.i.

$$I = (E) \quad (\text{resp. } I = |E|, I = (E))$$

Def: 1) Un ideal stăng (resp. drept, bilateral) I al unui inel R s.n. principal dacă (\exists) $a \in R$ a.t. $I = Ra$ (resp. $I = aR$, $I = R aR$).

2) Un inel R s.n. inel principal dacă este domeniul de integritate (i.e. comutativ și integral) și orice ideal al său este principal.

Suma și produs de ideale \rightarrow pag. 86, curs

Definitie: Fie R = inel. Un element $x \in R$ s.n. nilpotent dacă (\exists) $n \in \mathbb{N}$ a.t. $x^n = 0$.

Notam: $N(R) := \{x \in R \mid x = \text{nilpotent}\}$

Un element $e \in R$ s.n. idempotent dacă $e^2 = e$.

Notam: $\text{idem}(R) := \{e \in R \mid e \text{ idempotent}\}$.

Morfism de inele

Definitie: Fie R, S două inele. O funcție $f: R \rightarrow S$ s.n. morfism de inele dacă:

- a) $f(x+y) = f(x) + f(y)$; } (\forall) $x, y \in R$.
- b) $f(xy) = f(x)f(y)$;
- c) $f(1_R) = 1_S$.

Def: Un morfism de inele $f: R \rightarrow S$ s.n. $\xrightarrow{\text{bijectiv}} \text{izomorfism}$ dacă este bijectiv.

Un izomorfism de inele $f: R \rightarrow R$ s.n. automorfism al inelii R .

Propozitie: Fie $f: R \rightarrow S$ morfism de inele. Atunci:

- 1) Dacă $R' \subseteq R$ este subinel în $R \Rightarrow f(R')$ este subinel în S . În particular, $\text{Im}(f) \subseteq S$ este subinel.
- 2) Dacă $S' \subseteq S$ este subinel în $S \Rightarrow f^{-1}(S')$ este subinel în R .
- 3) Dacă $J \leq_A S$ (resp. drept, bilateral) $\Rightarrow f^{-1}(J) \leq_A (R)$ (respectiv, drept, bilateral)
În particular, $\text{Ker}(f) = f^{-1}(0_S) = \{r \in R \mid f(r) = 0_S\}$ este ideal bilateral în R .
- 4) Dacă f este surjectiv și $I \leq_A R$ (resp. drept, bilateral) $\Rightarrow f(I) \leq_A S$ (resp. drept, bilateral)

Teorema (teorema de corespondență pentru ideale)

Fie $f: R \rightarrow S$ un morfism surjectiv de inele.

Atunci, funcția

$$F: \{I \mid I \leq_A R, I \supseteq \text{Ker}(f)\} \xrightarrow{\cong} \{J \mid J \leq_A S\}$$

$$F(I) := f(I), \quad (f) \vdash I \dots$$

este bijecțivă cu inversa $F^{-1}(J) := f(J), (f) \vdash J \dots$

(similar pt. ideale drepte, bilaterale)

Caracteristica unui inel Fie $R =$ inel și $(R, +)$ grup abelian sub... inelului. În acest grup putem calcula $\theta(1)$, ordinul elementului 1 . Numărul natural def prior.

$$\text{car}(R) := \begin{cases} \theta(1), & \theta(1) \text{ este finit} \\ \infty, & \theta(1) = \infty \end{cases}$$

d.n. caracteristica inelului R

Produs direct de inele \rightarrow pas (pag. 90, cera)

Inele factor (pag. 92 - ceras)

Definiție: Fie $R = \text{inel}$ și $I \leq R$ un ideal bilateral al lui R . Atunci $(R/I, +, \cdot)$ cu adunarea și înmulțirea definită de:

$$\hat{a} + \hat{b} := \widehat{a+b}, \quad \hat{a} \cdot \hat{b} := \widehat{ab}, \quad (\forall) \hat{a}, \hat{b} \in R/I.$$

este un inel cu $0_{R/I} = \widehat{0} = I$ și $1_{R/I} = \widehat{1} = \{I+y \mid y \in I\}$

numește inelul factor al lui R prin I . În plus,

$\pi: R \rightarrow R/I$, $\pi(r) := \widehat{r}$, $(\forall) r \in R$ este morfism surjectiv de inele numită proiecția canonica a lui R pe R/I .

Exemplu: Fie $R = (\mathbb{Z}, +, \cdot)$. Atunci, $I \leq R = \mathbb{Z} \Leftrightarrow (\exists!) n \in \mathbb{N}$

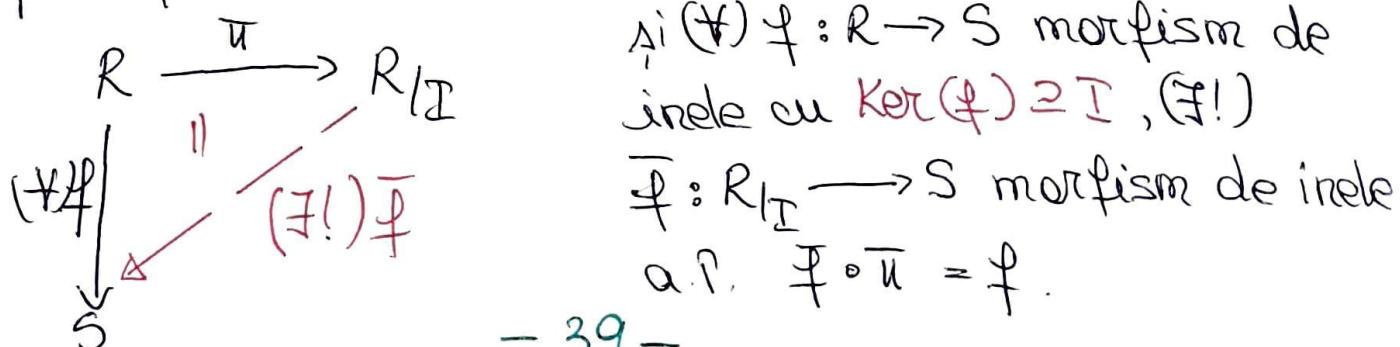
a.t. $I = n\mathbb{Z}$. În acest caz, inelul factor

$$\mathbb{Z}/n\mathbb{Z} \stackrel{\text{not.}}{=} \mathbb{Z}_n = \{0, 1, \dots, \widehat{n-1}\} \text{ s.n. inelul claselor de resturi modulo } n.$$

Teoremă (proprietatea de universalitate a inelului factor)

Fie $R = \text{inel}$, $I \leq R$ ideal bilateral în R și $\pi: R \rightarrow R/I$ proiecția canonica, $\pi(r) = \widehat{r}$. Atunci: (\forall) S un inel

și $(\forall) f: R \rightarrow S$ morfism de inele cu $\text{Ker}(f) \supseteq I$, $(\exists!)$



$\bar{f}: R/I \rightarrow S$ morfism de inele a.t. $\bar{f} \circ \pi = f$.

În plus,

- a) \bar{f} este surjectiv $\Leftrightarrow f$ este surjectiv.
b) \bar{f} este injectiv $\Leftrightarrow \text{Ker } (f) = I$

(T.F.I.I)

Teorema (Teorema fundamentală de izomorfism pt. inele)

Fie R, S două inele și $f: R \rightarrow S$ un morfism de inele. Atunci există un izomorfism de inele:

$$R/\text{Ker } (f) \cong \text{im}(f).$$

Corolar (lema chineză a resturilor)

Fie $A =$ inel comutativ, I și $J \leq A$ ideale în A a.t. $I + J = A$. Atunci există un izomorfism de inele

$$A/[I \cap J] \cong A/I \times A/J$$

Corolar Fie $m, n \in \mathbb{N}$, $m, n \geq 2$ și prime între ele, i.e. $(m, n) = 1$. Atunci

$$f: \mathbb{Z}_{mn} \xrightarrow{\cong} \mathbb{Z}_m \times \mathbb{Z}_n,$$

$f(\tilde{a}) := (\hat{a}, \tilde{\hat{a}})$, $\forall \tilde{a} \in \mathbb{Z}_{mn}$ este izomorfism de inele.

Teoreme de izomorfism pt. inele (facultativ) (-pag 96, verso, curs)

CORPURI - pag. 98, cters.

Definitie: Un inel K s.n. corp dacă orice element nenul al său este inversabil, i.e. $\underline{U(K)} = K \setminus \{0\}$.
 K s.n. corp comutativ dacă $ab = ba$, $\forall a, b \in K$.

Licu: $(K, \circ, *)$ corp dacă:

- (K, \circ) - grup abelian
- $(K, *)$ - grup
- $*$ este distributivă față de \circ

$$a * (b \circ c) = (a * b) \circ (a * c)$$

$$(a \circ b) * c = (a * c) \circ (b * c)$$

+ dacă $(K, *)$ - grup abelian $\Rightarrow K$ corp comutativ

Definitie: Fie K un corp și $T \subseteq K$ o submultime.

T s.n. subcorp al lui K (sau K este o extindere a lui T) dacă:

a) $\forall x, y \in T \Rightarrow x - y \in T$

b) $1 \in T$

c) $\forall x, y \in T, y \neq 0 \Rightarrow xy^{-1} \in T$.

Definitie: Fie K și L două corperi. O funcție $f: K \rightarrow L$ s.n. morfism de corperi dacă f este morfism de inele.

Propozitie: Orice morfism de corperi $f: K \rightarrow L$ este injectiv.

Definitie: Un corp P s.n. corp prim dacă P nu are subcorpuri în afara de el însuși.

Ex: \mathbb{Z}_p ($p = \text{număr prim}$) și \mathbb{Q} sunt corpuri prime.

Propozitie: Fie P un corp prim $\Rightarrow P$ este izomorf cu \mathbb{Q} sau P e izomorf cu \mathbb{Z}_p , $p = \text{număr prim}$.

Propozitie: Fie K un corp și $P_K := \bigcap_{\substack{I \subseteq K \\ \text{subcorp}}} I^{\neq}$. Atunci $P_K \subseteq K$ este un subcorp, P_K este un corp prim, numit corpul prim al lui K.

Definitie: Fie $K = \text{corp}$. Spunem că K are caracteristica zero (și notăm $\text{char}(K) = 0$) dacă $P_K \cong \mathbb{Q}$.

Spunem că K are caracteristica $p > 0$ (și notăm $\text{char}(K) = p > 0$) dacă $P_K \cong \mathbb{Z}_p$, $p = \text{nr. prim}$. - pag. 101

Corpul de fractii al unei domenii de integritate - 102

Definitie: Fie $R = \text{domeniu de integritate}$. Atunci $Q(R)$ are o structură de corp comutativ cu operațiile:

$$\frac{a}{t} + \frac{b}{t} := \frac{at+bt}{st} \quad \text{și} \quad \frac{a}{t} \cdot \frac{b}{t} := \frac{ab}{st}$$

(*) $\frac{a}{t}, \frac{b}{t} \in Q(R)$; $0_{Q(R)} = \frac{0}{1}$, $1_{Q(R)} = \frac{1}{1}$ numit

corpul de fractii al lui R . În plus, $f: R \rightarrow Q(R)$, $f(r) := \frac{r}{1}$, (*) $r \in R$ este un morfism injectiv de inele.

Corpul cuaternionilor

Teorema Fie $M_2(\mathbb{C})$ inelul de matrici cu elemente complexe. Atunci

$$H := \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C}).$$

Atunci H este un subinel necomutativ în $M_2(\mathbb{C})$.
și orice element nenul din H este inversabil în H , i.e. H este corp necomutativ.

Corolar Fie $H = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$

corpul cuaternionilor. Atunci multimea

~~$$Q := \{\pm 1; \pm i; \pm j; \pm k\} \subseteq H$$~~

este un subgrup finit în $U(H)$, cu opt elemente numite unitate sau unități ale corpului cuaternionelor.

Lucrari facultative → pag. 107, curs

The end !! 😊