OPREA TUDOR
FMI GRUPA 141

Structuri Algebrice în Informatică

! Vezi bineînțeles def introductive.

= Mulțimi =

- $C_B A$ = compl. lui A în rap cu B
- de Morgan: $C_M(A \cup B) = C_M A \cap C_M B$
  $C_M(A \cap B) = C_M A \cup C_M B$
- PIE: $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_1 \cap A_3| + |A_1 \cap A_2 \cap A_3|$
- mulțimea părților: $P(A)$; $|P(A)| = 2^{\text{card}A}$
- pt orice A, B: $A \cap B \subset A \subset A \cup B$
- mulțimi EQUIPOTENTE = au același cardinal
  ↳ o mult. echip. cu $\mathbb{N}$ s.n. NUMĂRABILĂ

$\mathbb{R}$ și $(0,1)$ sunt echipot $\leftrightarrow$ $\exists$ o bij de la $\mathbb{R}$ la $(0,1)$

= Funcții =

- f atribuie unui elem din A un unic el din B
- C_b^a = nr. fct. s. cresc
  C_{b-a-1}^a = nr. fct. cresc.
- compunerea fct $\rightsquigarrow$ asociativă $f: A \to B$, $g: B \to C$, $g \circ f: A \to C$

INJECTIVITATE: $x, y \in A$, $f(x) = f(y) \Rightarrow x = y$
f cont și crescătoare

SURJECTIVITATE: $\forall y \in B$, $\exists x \in A$ a.î. $f(x) = y$
f cont și domeniul = Im f

nr. fct. = m^m

nr. fct. bij. = $n!$

nr. fct. surj. = $n^m - C_n^1 (n-1)^m + C_n^2 (n-2)^m + \dots + (-1)^{n-1} C_n^{n-1}$

$f: M \to N$
m elem n elem

⊕ dacă f și g inj / surj / bij $\Rightarrow$ $g \circ f$ inj / surj / bij

$g \circ f$ inj $\Rightarrow f$ inj

$g \circ f$ surj $\Rightarrow g$ surj

- Relații de echivalență → relație ce verifică cele 3 proprietăți

REFLEXIVĂ	SIMETRICĂ	TRANZITIVĂ
$a \sim a$ $\forall a \in A$	$a \sim b \Rightarrow b \sim a$	$a \sim b$, $b \sim c \Rightarrow a \sim c$

CONGRUENȚA MODULO N: este o rel de echivalență

$a \equiv b \pmod n \iff n \mid a-b$

Avem 2^n rel. binare pe mulțimea A.

Partițiile unei mulțimi: familii de submulțimi nevide și disjuncte a căror reuniune este mulțimea vidă $\emptyset$.

$A = A_1 \cup A_2 \cup \dots \cup A_m$

$A_1 \cap A_2 \cap \dots \cap A_m = \emptyset$

Nr. clase de echivalență = nr. partiții

Orice $\sim$ partiționează mulțimea și invers.

Mulțimea factor: $A/\sim := \{\hat{a} \mid a \in A\}$

Clasa de echiv a lui a = $\hat{a}$, $\bar{a}$, $[a]$ (not) $= \{b \in A \mid a \sim b\}$

MULȚIMEA CLASELOR DE ECHIVALENȚĂ sau MULȚIME FACTOR a lui A modulo $\sim$ și se not. cu $A/\sim$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sunt constr. ca mulțimi factor

observații → sem 6 (6.1)

- O rel. binară pe A este de fapt o submulțime a lui A×A.
- O rel binară este ANTISIMETRICĂ (⇒)

$$a \sim b,\ b \sim a \Rightarrow a = b$$

SCR

Fie "~" o rel. de echiv. pe A. O submulțime $S \subseteq A$ s.n. sistem complet de reprezentanți pentru "~" dacă S conține exact câte 1 element din fiecare clasă de echivalență.

↳ S este scr dacă:

1) $\forall a \in A\ \exists s \in S$ a.î. $a \sim s$ ($\Leftrightarrow [a] = [s]$)
2) $\forall s_1 \neq s_2$ cu $s_1, s_2 \in S \Rightarrow s_1 \not\sim s_2$ ($\Leftrightarrow [s_1] \cap [s_2] = \emptyset$)

- Mulțimea claselor de echivalență = o partiție (obs cu rețul)

- operații algebrice - legi de compoziție -

|| funcție $*: A \times A \to A$; not $*(a,b)$ cu $a * b$

- ass, comut, elem. neutru (dacă $\exists$, este unic), parte stabilă

$e = e * f = f$, dacă e și f elem neutre

- MONOID ($\Leftrightarrow$) (M, *)
  - M parte stab
  - * asociativă
  - * are elem. neutru

+ comutativ

- GRUP ($\Leftrightarrow$) (G, ∘)
  - G parte stab
  - ∘ asociativă
  - ∘ elem. neutru
  - elem. simetrizabile

Practic, un monoid este grup dacă $U(M) = M$

exemple: monoizi - $(\mathbb{N},+)$ $(\mathbb{N},\cdot)$ $(\mathbb{Z},\cdot)$ $(\mathbb{Q},\cdot)$ $(\mathbb{R},\cdot)$ $(\mathbb{C},\cdot)$ | monoizi comut - $(P(A),\cup)$ $(P(A),\cap)$

grupuri comut. $(\mathbb{Z},+)$ $(\mathbb{Q},+)$ $(\mathbb{R},+)$ $(\mathbb{C},+)$ $(\mathbb{Z}_n,+)$ $(\mathbb{Q}^*,\cdot)$ $(\mathbb{R}^*,\cdot)$ $(\mathbb{C}^*,\cdot)$

Algoritmul lui Euclid: dacă $(k, n) = d$

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

Fie $(M_1, \cdot)$ și $(M_2, \cdot)$ 2 monoizi. O funcție $f: M_1 \to M_2$ s.n. morfism de monoizi dacă:

- $f(x \cdot y) = f(x) \cdot f(y)$, $\forall x, y \in M_1$
- $f(1_{M_1}) = 1_{M_2}$

↓ Alți = izomorfism

Fie $(G_1, *)$ și $(G_2, \cdot)$ 2 grupuri. Definim produsul lor direct ca fiind $(G_1 \times G_2, \square)$ grup

$G_1 \times G_2 = \{(a, b) \mid a \in G_1, b \in G_2\}$

$(a, b) \square (c, d) \overset{\text{def}}{=} (a * c, b \cdot d)$

Pentru aceleași 2 grupuri, o funcție $f: G_1 \to G_2$ s.n. morfism de grupuri dacă

- $f(x * y) = f(x) \cdot f(y)$, $\forall x, y \in G_1$

! Vezi Anexa 1 pt morfisme de forma $a^{a^{x}}$

= Subgrupuri =

Fie $(G, \cdot)$ un grup. O submulțime nevidă H a lui G s.n. subgrup și se not. $H \leq G$, dacă H este p.s. a lui G închisă la luarea inversului.

$\forall x, y \in H \Rightarrow x \cdot y \in H$ și $x^{-1} \in H$

Subgrupul generat de o mulțime:

Fie $(G,\cdot)$ grup și $A \subseteq G$. Subgrupul lui G generat de mulțimea A se not. cu $\langle A \rangle$, și se reprezintă astfel:

$$\langle A \rangle \overset{def}{=} a_1^{\pm 1} \cdot a_2^{\pm 1} \cdot \ldots \cdot a_n^{\pm 1} \mid a_1, \ldots a_n \in A, n \geq 1 \} \leq G$$

Subgrupul generat de mulț. vidă: $\langle \emptyset \rangle = \{1_G\}$

Obs: $\rightarrow G = \langle G \rangle$

$\rightarrow$ dacă $A = \{a\}$ $\quad \langle \{a\} \rangle \overset{not}{=} \langle a \rangle \overset{not\ H}{=} \{a^k \mid k \in \mathbb{Z}\}$, $a \in G$

NOT: $\langle a \rangle$ = subgrupul ciclic generat de a

$\rightarrow$ **CICLIC** = grup dacă $\exists\, a \in G$ a.î. $G = \langle a \rangle$

$\rightarrow$ **FINIT GENERAT** = dacă $\exists\, A \subseteq G$ cu $|A| < \infty$ a.î. $G = \langle A \rangle$

Relații bune: $x \equiv_s y \pmod H$ $\quad x, y \quad x^{-1}y \in H$

$x \equiv_d y \pmod H$ $\quad x, y \quad xy^{-1} \in H$

Ordinul unui element într-un grup:

$(G,\cdot) \rightsquigarrow$ $\operatorname{ord}(g)$ = cel mai mic $n \in \mathbb{N}^*$ a.î. $g^n = 1$

$(G,+) \rightsquigarrow$ ——— $g \cdot n = 1$

Într-un grup finit, ordinul unui element e mereu finit.

Ordinul elem. neutru este 1.

$$\operatorname{ord}(x) = \frac{n}{(n,k)}$$

CURSUL 9

Fie G grup și $H \leq G$ (un subgrup). Cele $\equiv_s \pmod H$ și $\equiv_d \pmod H$ sunt relații de echivalență pe G.

↓

clasele de echivalență ale:

"$\equiv_s \pmod H$" $\longrightarrow$ $xH = \{x \cdot y \mid y \in H\}$

"$\equiv_d \pmod H$" $\longrightarrow$ $Hx = \{y \cdot x \mid y \in H\}$

↑ numărul claselor de echiv. stânga este același, dar mulțimile sunt diferite: $(G/H)_s$, $(G/H)_d$ pot fi diferite, dar au același cardinal.

↓ G = ABELIAN $\Rightarrow (G/H)_s = (G/H)_d$

Teorema lui Lagrange:

G - grup finit

$H \leq G$

$$|G| = |H| \cdot [G : H]$$

ord lui (card) — indicele lui H în G

- în particular, $|H| \mid |G|$

Teorema lui Euler

$(a, n) = 1$, $a, n \in \mathbb{N}$

$a^{\varphi(n)} \equiv 1 \pmod n$

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

unde $p_1, \dots, p_r$ → factorii primi din descompunerea lui n

n prim $\Rightarrow \varphi(n) = n - 1$

Mica Teoremă a lui Fermat

p - prim, $a \in \mathbb{N}$, $p \nmid a$

$a^{p-1} \equiv 1 \pmod p$

echival. cu

$a^p \equiv a \pmod p$

Def Un subgrup $H \leq G$ s.n. **SUBGRUP NORMAL** al lui G dacă $\boxed{xH = Hx \quad \forall x \in G}$ $\longrightarrow$ not. $H \trianglelefteq$

$\Leftrightarrow (G/H)_s = (G/H)_d$

verif dacă un subgrup este normal : $xHx^{-1} \subseteq H$ $\forall x \in G$

Def : Grupul factor

Fie $(G, \cdot)$ grup, $H \trianglelefteq G$.

$(G/H)_s = (G/H)_d = G/H$

$G/H = \{\hat{x} \mid x \in G\}$ $\hat{x}$ not pt $xH = Hx$

Pe G/H introd. operația alg. $\hat{x} \cdot \hat{y} \overset{\text{def}}{=} \widehat{xy}$ (op. e bine def)

Th : G grup, $H \trianglelefteq G \Rightarrow$ op. def. anterior este o lege de compoziție în raport cu care G/H este GRUP, numit **GRUPUL FACTOR AL lui G modulo H.**

Apl: $G \xrightarrow{\varphi} G/H$ e un morf. surj de grupuri

$a \to \hat{a}$

Teorema fundamentală de izomorfism :

$\varphi : G \to G'$ morf de grupuri.

$G/\ker f \simeq \text{Im } f$

$\bar{f} \mapsto f$ un izomorfism de grupuri $\bar{\varphi} : G/\ker f \to \text{Im } f$

$\bar{\varphi}(\hat{x}) = \varphi(x)$

Teorema de structură a grupurilor ciclice :

Orice grup ciclic infinit e izomorf cu $(\mathbb{Z}, +)$ și orice grup ciclic finit (cu n elem) e izomorf cu $(\mathbb{Z}_n, +)$.

GRUPUL $(S_n, \circ)$ → permutări

Teorema
Th cayley
Cicli disj
Transpoziții

INELE

Anexa o
Structuri Algebrice în Informatică

UREA TUDOR
FMI GRUPA 141

Teorema Cantor – Bernstein

Fie A, B 2 mulț. Avem $|A| = |B|$
$\Leftrightarrow |A| \leq |B| \;\&\; |B| \leq |A|$.

def = 2 mulț. sunt echipotente $\Leftrightarrow$ există f bij $(\exists$ bij $f: A \to B)$

$\Leftrightarrow$ există fcț. ex $g: A \to B$ și $h: B \to A$

Mulțimea părților unei mulțimi

$\mathcal{P}(A) :\overset{def}{=} \{B \mid B \subseteq A\}$
↳ are cardinalul $= 2^m$

Principiul incluziunii și excluziunii

$$\left|\bigcup_{i=1}^{m} A_i\right| = \sum_{i=1}^{m} |A_i| - \sum_{1 \leq i_1 < i_2 \leq m} |A_{i_1} \cap A_{i_2}| + \sum_{1 \leq i_1 < i_2 < i_3 \leq m} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| - \dots$$

$$\dots + (-1)^{k+1} \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq m} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}| + \dots$$

$$\dots + (-1)^{m+1} |A_1 \cap \dots \cap A_m|$$

• $2021^{2021^{2021}} \pmod{22}$

$\uparrow$ $2021^{2021} \pmod{22}$

20

Anexa nr 1
Structuri Algebrice în Informatică
OPREA TUDOR
FMI GRUPA 141

∇ $a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$

$a \equiv r \pmod{n}$
↳ restul împ lui a la n

$2021^{2021^{2021}} \equiv 19^{2021} \pmod{22}$

$2021 \nmid 22 \rightarrow$ rest 19

$19 \overset{22}{\equiv} -3$

$= -3^{2021} \pmod{22}$

Th. EULER $(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

$\varphi(22) = 22 \cdot \frac{1}{2} \cdot \frac{10}{11} = 10$

$-3^{2021} \pmod{22}$

$\equiv -3^{10 \cdot 202 + 1} \pmod{22}$

$\equiv (-3^{10})^{202} \cdot (-3) \pmod{22}$

$\Rightarrow$

$\equiv -3 \pmod{22}$

$\equiv 19 \pmod{22}$