Curs V. Garlan | 20/04/2022

Curs 10

Grup, Sub-grup, Grup-ciclic, Teorema lui Lagrange pentru grupuri finite

Fie $G \neq \emptyset$ o mulțime și $*: G \times G \to G$ o lege de compoziție internă pe $G \Leftrightarrow \forall x, y \in G \Rightarrow x * y \in G$.

Perechea $(G, *)$ se numește grup dacă $*$ are următoarele proprietăți:

a) Asociativitatea: $\forall x, y, z \in G, \Rightarrow (x * y) * z = x * (y * z)$

b) Există element neutru în G în raport cu legea de comp. internă $* \to \exists e \in G$ a.î. $\forall x \in G$

↳ $x * e = e * x = x$ $\quad e$ = unic, dacă există

c) Orice element din G este simetrizabil în raport cu legea de comp. internă $* \to \forall x \in G, \exists x' \in G$

↳ $x * x' = x' * x = e$ $\quad x'$ = (inversa lui x), unic

Dacă nu toate elementele lui G sunt simetrizabile față de legea de comp. internă $*$, atunci $(G, *)$ este monoid

d) Dacă în plus legea de comp. internă $*$ este și comutativă, atunci $(G, *)$ este Grup comutativ (monoid comut)

↳ $\forall x, y \in G \Rightarrow x * y = y * x$

Exemple: $(\mathbb{Z}, +)$; $(\mathbb{R}, +)$; $(\mathbb{Q}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{C}, \cdot)$

= sunt grupuri comutative

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

$(\mathcal{M}_n(\mathbb{R}), \cdot)$ = monoid necomutativ

S_n = mulțimea permutărilor de n elemente =
$\circ$ = compunerea permutărilor

$(S_n, \circ)$ = grup necomutativ

$(\mathbb{Z}_n, +) \neq (\mathbb{Z}_n, \cdot)$

grup comutativ — monoid comutativ

Fie $k \in \mathbb{Z}$, [redacted] și $n \in \mathbb{N}$, $n \geq 2$.

Teorema împărțirii cu rest a numerelor întregi

$\forall K \in \mathbb{Z}$, și $n \in \mathbb{N}$, cu $n \geq 2$. Atunci există și sunt unice două numere $c \in \mathbb{Z}$ și $r \in \mathbb{N}$ cu proprietatile:

$\frac{K}{n} = c + \frac{r}{n}$ unde $c \in \mathbb{Z}$; $0 \leq r \leq n$, numite catul și restul împărțirii lui K la n.

~~Enunțăm această teoremă~~

Clase de resturi

$\hat{0} = \{ \ldots, -3n, -2n, -n, 0, n, 2n, 3n \ldots \}$

$\hat{1} = \{ \ldots, -3n+1, -2n+1, -n+1, \hat{1}, n+1, 2n+1, 3n+1 \ldots \}$

$\hat{2} = \{ \ldots, -3n+2, -2n+2, -n+2, \hat{2}, n+2, 2n+2, 3n+2 \ldots \}$

$\vdots$

$\hat{n-1} = \{ \ldots, -2n-1, -n-1, \hat{-1}, n-1, 2n-1, 3n-1, 4n-1 \ldots \}$

Fie care clasa de echivalență s-a reprezentat prin reprezentantul său generic $\Leftrightarrow \hat{r}$, $0 \leq r \leq n-1$, $r \in \mathbb{N}$

Oricare 2 elemente vecine din oricare clasă, diferă între ele exact prin n unități

Se notează cu $\mathbb{Z}_n$ = mulțimea tuturor claselor de resturi modulo n.

$$\mathbb{Z}_n = \{ \hat{0}, \hat{1}, \hat{2}, \hat{3}, \ldots, \hat{n-1} \} \quad n \in \mathbb{N}, n \geq 2$$

1 Observăm că $\hat{0} \cup \hat{1} \cup \hat{2} \cup \ldots \cup \hat{n-1} = \mathbb{Z}$

2 Observăm că, $\forall i \neq j \Rightarrow \hat{i} \cap \hat{j} = \emptyset$

Vom spune că am realizat o partiție a mulțimii numerelor întregi:

$$\mathbb{Z} = \bigcup_{K=0}^{n-1} \hat{K}$$

$\mathbb{Z}_n$ = mulțime finită

pe $\mathbb{Z}_n$ vom defini 2 operații

$\oplus$ = adunarea claselor

$\hat{x} \oplus \hat{y} = \widehat{x+y} \pmod n \in \mathbb{Z}_n$

$\hat{x} \otimes \hat{y} = \widehat{x \cdot y} \pmod n \in \mathbb{Z}_n$

Ambele operații sunt legi de comp interne pe $\mathbb{Z}_n$ și determină structuri algebrice:

a) $(\mathbb{Z}_n, \oplus)$ = Grup Comutativ

b) $(\mathbb{Z}_n, \otimes)$ = Monoid Comutativ dacă n nu este număr prim

Grup Comutativ dacă n este număr prim

Vom Construi Tabelele legilor de compoziție, $\oplus$ și $\otimes$, pentru $\mathbb{Z}_6$

$(\mathbb{Z}_6, \oplus)$ - g. comutativ

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Element neutru -> $\hat{0}$

$\oplus$ = l.c.i pe $\mathbb{Z}_6$

$\oplus$ = comutativă

Orice element este simetrizabil

$(\mathbb{Z}_6, \otimes)$

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Element absorbant = $\hat{0}$

Element neutru = $\hat{1}$

$\otimes$ = l.c.i pe $\mathbb{Z}_6$ și comutativă

$\{\hat{1}, \hat{5}\}$ = elementele inversabile

$\hat{2} \otimes \hat{3} = \hat{4} \otimes \hat{3} = \hat{0}$ -> $\hat{2}, \hat{3}, \hat{4}$ div. lui $\hat{0}$

Proprietate de Resturi

$\Rightarrow (\mathbb{Z}_n, \oplus, \otimes)$ = inel comutativ cu divizorii lui.

$(\mathbb{Z}_p, \otimes, \oplus)$ = corp comutativ (p prim)

Caracteristica (Indicatorul) lui Euler

Def. Prin asta se intelege functia $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ prin $\varphi(n)$ = numarul claselor modulo n reprezentate prin numere prime cu n

$$\Rightarrow \varphi(n) = \text{card}(U(\mathbb{Z}_n))$$

Cazuri speciale

① Daca $n = p$ si este prim, atunci toate numerele de la $1, \dots, p-1$ sunt prime cu p

$$\varphi(p) = p - 1$$

② Daca $n = p^k$ si este prim, $k \in \mathbb{N}^*$, atunci numerele dintre 1 si p^k, care nu sunt prime cu p, sunt multipli lui p:

$$p, 2p, 3p, \dots, p^{k-1} \cdot p$$

numarul lor este egal cu p^{k-1}. Rezulta ca numarul claselor prime cu n este egal cu $p^k - p^{k-1}$

$$\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

③ Fie $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$; $p_1, p_2, \dots, p_k$ sunt numere prime
$\alpha_1, \alpha_2, \dots, \alpha_k$ sunt ordin. lor de multip.

$$\varphi(n) = \varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) =$$

$$\varphi(n) = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right) =$$

$$\boxed{\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right)}$$