

Curs 11

Ordinalul unui element dintr-un grup

Definiție: Ești (G, \cdot) un grup și $x \in G$. cel mai mic număr natural $n \in \mathbb{N}^*$, cu proprietatea că $x^n = e$ element neutru al lui G , se numește ordinalul lui x în grupul (G, \cdot) .

Vom spune că ordinalul lui x în (G, \cdot) este egal cu $+\infty$ dacă $x^n = e \forall n \in \mathbb{N}^*$.

Ordinalul lui x din (G, \cdot) , dacă există, se notează $\text{ord}(x)$ și se demonstrează că $\text{ord}(x) = \text{ord}(x^{-1})$

Ex. ① În grupul $(\{1, -1, i, -i\}, \cdot)$ avem că $\text{ord}(-1) = 2$ pentru că $(-1)^2 = 1 = e$

$\text{ord}(i) = \text{ord}(-i) = 4$ pentru că $i^4 = (-i)^4 = 1 = e$ $i = \sqrt{-1}$

Puteți calcula orice putere al lui i stând că $i^4 = 1$

$$\text{Ex. } i^{2020} = (i^4)^{505} = 1^{505} = 1$$

$$i^{2022} = (i^4)^{505+2} = 1^{505} + i^2 = 1 + 1 = -1$$

② Ești grupul $(\mathbb{Z}_5^*, \cdot) = \{1, 2, 3, 4\}$ avem

$$\begin{aligned} \text{ord}(1) &= 4 \text{ deoarece } 2^4 = 16 \pmod{5} = 1 \\ \text{ord}(3) &= 4 \text{ deoarece } 3^4 = 81 \pmod{5} = 1 \\ \text{ord}(4) &= 4 \text{ deoarece } 4^4 = 256 \pmod{5} = 1 \end{aligned}$$

OBS: $\text{ord}(x)$ este $= 4 \quad \forall x \in (\mathbb{Z}_5^*, \cdot), x \neq 1$

$$n=5 \rightarrow \text{prim} \Rightarrow \varphi(n) = \varphi(5) = 5-1 = 4$$

③ Ești grupul permutelor (S_5, \circ) cu 5 elemente și $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$

$$\text{ord}(S_5) = 5! = 120$$

Calculăm $\text{ord}(\sigma)$ și determinăm multimea $H = \{\sigma^n \mid n \in \mathbb{N}^*\}$

Așa că că (H, \circ) este grup comutativ și că este subgrup în (S_5, \circ)

De asemenea, să arătăm că $\text{ord}(H) = \text{ord}(\sigma)$, H în subgrupul generat de permutarea σ

$$\sigma^2 \cdot \sigma \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$$

$$\sigma^3 = \sigma^2 \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$$

$$\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = e = \text{ord } \sigma = 5 \Rightarrow \sigma^{-1} = \sigma^4$$

$$\Rightarrow H = \{\sigma, \sigma^2, \sigma^3, \sigma^4, e\}$$

Să se continuă tabelul de compozitie pentru (H, \circ) și să se deducă faptul că este, în modul sau, grup în (S_5, \circ) ; se numește **grupul general de permutări** și elementele sale sunt soluțiile ecuației $\sigma \circ x = x \circ \sigma$ în grupul (S_5, \circ) .

Definiție: Fie (G, \circ) un grup, și $x \in G$

Atunci multimea: $\{x^k \mid k \in \mathbb{Z}\} \stackrel{\text{notatie}}{=} \langle x \rangle$, împreună cu operatia "de grup" al lui G este grup **ciclic** și se numește **grupul ciclic generat de elementul x** .

In exemplul anterior, multimea H este sub-grupul ciclic generat de permutarea σ .

Definitie: Dacă $(G, *)$ este un grup și $H \subset G$, $H \neq \emptyset$ atunci H se numește sub-grup al lui G dacă are proprietățile:

$$a) \forall x, y \in H \Rightarrow x * y \in H$$

$$b) \forall x \in H \Rightarrow x^{-1} \in H$$

Cu aceste proprietăți rezultă că $(H, *)$ este, de asemenea, tot un grup, inclus strict în G .

Mai rezultă că elementul neutru din G se află neapărțit în H .

În continuare, ne vom ocupa de sub-grupurile ciclice generate de un element de ordin finit.

Prin exemplul anterior, am pus în evidență rezultatul exprimat prin teorema următoare:

TEOREMA: Dacă $(G, *)$ este un grup și $x \in G$ este element de ordinul n , $n \in \mathbb{N}$, finit, atunci sub-grupul cyclic generat de elementul x este:

$$\langle x \rangle = \{x, x^2, x^3, \dots, x^{n-1}, x^n = e\} \text{ și } \text{ord}(x) = n$$

Ex. (S_5, \circ) ; $x = \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$;

$$\text{ord}(x) = 5; \quad \sigma^5 = e; \quad H = \{\sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5 = e\} \subset S_5$$

Într-un context mai general, prin grup cyclic vom entinde un grup G în care există un element $g \in G$ cu proprietatea că $\langle g \rangle = G$.

Elementul g s.n. generator lui G

TEOREMA: Două grupuri ciclice cu același element sunt ISOMORFE

CONSECINȚĂ: Dacă ordinul unui grup G este număr prim p , atunci G este izomorf cu grupul $(\mathbb{Z}_p, +)$ ciclic.

TEOREMĂ: Fie G un grup ciclic de ordinul n , (G, \circ) și g un generator al său, atunci
 condiția nec. și suficientă ca elementul g^k să fie și el generator al lui G , dacă și numai dacă K este prim cu n .
 $\langle g^K \rangle = G$.

În continuare vom prezenta ceterul mănușii Fundamentale din teoria grupurilor finite în criptografie.

① T. Lagrange pentru grupuri finite

Ordinul oricărui sub-grup ~~este~~ unui grup finit este un divisor al ordinului ~~grupului~~

Teorema stabilește relația dintre ordinul unui grup finit și ordinul oricărui sub-grup al său.

Consecințele următoare stabilesc rezultate importante și de aplicatii directe în fundamentele matematice și criptografiei.

C1: Într-un grup finit, ordinul oricărui element este finit și este un divisor al ordinului grupului.

Ex. Sub-grupurile de permutări din grupul (S_n, \circ)

C2: Fie (G, \circ) un grup finit de ordinul n , atunci

$$x^n = e, \forall x \in G$$

C3: Orice grup finit de ordin p (nr. prim) $\in \mathbb{N}^*$ este grup ciclic (\cong izomorf cu \mathbb{Z}_p)

② T. Euler

Fie $m \in \mathbb{N}^*$, $m \geq 2$, $a \in \mathbb{Z}$, a este prim cu m ($\Leftrightarrow (a, m) = 1$)

Atunci, $a^{\varphi(m)} \equiv 1 \pmod{m}$ unde $\varphi(m)$ este caracteristica lui Euler

OBS: Dacă $m = p = \text{nr. prim} \Rightarrow \varphi(n) = \varphi(p) = p-1$

\rightarrow Euler $\rightarrow a^{p-1} \equiv 1 \pmod{p}$ unde $(a, p) = 1$

Astfel, în cazul acestuia, T. Euler devine cunoscută sub numele de Fermat.

Teorema lui Fermat

Fie p nr. prim și $a \in \mathbb{Z}$ cu proprietatea că $(a, p) = 1$, atunci $a^{p-1} \equiv 1 \pmod{p}$

Teorema lui Wilson

Dacă p nr. prim atunci $(p-1)! \equiv -1 \pmod{p}$

Teorema 'Chineză' a resturilor

Fie ~~mai~~ $(m, n) = 1$ $m, n \in \mathbb{N}$, m și n prime între ele.

atunci funcția $f: \mathbb{Z}_{m \cdot n} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ definită prin

$f(x_{m \cdot n}) = (x_m, x_n)$ unde x este un număr întreg care cere săz $x_{m \cdot n}, x_m$ și x_n sunt clasele lui $x \pmod{m \cdot n}$, \pmod{m} și \pmod{n} , este izomorfism de unele.

Teorema confirmă că dacă m și n sunt prime între ele, atunci grupul $\mathbb{Z}_m \times \mathbb{Z}_n$ (adică cordon) este izomorf cu grupul $\mathbb{Z}_{m \cdot n}$, deci este grupul ciclic.

~~În cadrul acestei probleme~~