10-11-2017

CURS 6

Definiție: $(G, \cdot)$ grup. $H \subseteq G$, $H \neq \emptyset$.

H s.n. subgrup al lui G (se notează $H \leq G$) dacă:

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

Scop Teorema Lagrange: $(G, \cdot)$ grup finit, $H \leq G$. Să se arate că $|H| \mid |G|$ (cardinal H divide cardinalul lui G)

Demonstrație: Dacă $H = G$ enunțul este evident a/a

Pp. că $H \subsetneq G$. Alg $x_1 \in G \setminus H$.

$\hookrightarrow G \setminus H \neq \emptyset$

Consider mulțimea $x_1 H = \{x_1 \cdot h \mid h \in H\}$

Demonstrez că: 1) $|x_1 H| = |H|$

2) $x_1 H \cap H = \emptyset$

Dem 1): $f : H \to x_1 H$, $f(h) = x_1 \cdot h$

f surjectivă.

Arăt că f este inj.

$h_1, h_2 \in H$ a.î. $f(h_1) = f(h_2) \overset{?}{\Rightarrow} h_1 = h_2$

$x_1 \cdot h_1 = x_1 \cdot h_2$

$(\exists)\ x_1^{-1} \in G$

$h_1 = \underbrace{x_1^{-1} \cdot (x_1 h_1)}_{asoc} = x_1^{-1} \cdot (x_1 \cdot h_2) = e \cdot h_2 = h_2$

$e \cdot h_1 = (x_1^{-1} \cdot x_1) \cdot h_1$

e - ⓔ

$\Rightarrow f$ inj $\Rightarrow f$ bijectivă $\Rightarrow |H| = |x_1 H|$

Scanned by CamScanner

Dem 2): reducere la absurd

Pp. că $(\exists)\ y \in x_1 H \cap H$

$y = x_1 \cdot h_1 = h_2 \qquad h_1, h_2 \in H$

$| \cdot h^{-1}$

$x_1 = x_1 \cdot \underbrace{h_1 \cdot h_1^{-1}}_{=e} = h_2 \cdot h_1^{-1}$

$x_1 \cdot e = x_1\ h_2 \cdot h_1^{-1} \in H$

$h_1 \in H \Rightarrow h_1^{-1} \in H$

$\Rightarrow$ ↯ deoarece $x_1 \notin H$

$$|H \cup x_1 H| = |H| + |x_1 H| = 2|H|$$

$H \cap x_1 H = \emptyset$

Cazul $H \cup x_1 H = G \Rightarrow |G| = 2|H|$ este multiplu de $|H|$

Cazul $H \cup x_1 H \subsetneq G$ În acest caz aleg $x_2 \in G \setminus (H \cup x_1 H)$

$H \cup x_1 H \cup x_2 H \subseteq G$

Dem că $|x_2 H| = |H|$ analog (1)

Dem: $x_2 H \cap (H \cup x_1 H) = \emptyset$

Pp că: $x_2 H \cap (H \cup x_1 H) \neq \emptyset$

pt anumite $h_1, h_2 \in H \Rightarrow$ $x_2 h_1 = h_1$ sau $x_2 h_1 = x_1 h_2$

$x_2 = h_2 h_1^{-1} \in H$ ↯

$x_2 = x_1 h_2 h_1^{-1} \in x_1 H$ ↯

$$|\underbrace{H \cup x_1 H}| \cup x_2 H| = 3|H|$$

$|H \cup x_1 H| + |x_2 H| = 2|H| + |H| = 3|H|$

$\Rightarrow |G| = 3|H|$ este multiplu de $|H|$

Cazul $H \cup x_1 H \cup x_2 H \underset{\neq}{\subset} G$

Aleg $x_3 \in G \setminus (H \cup x_1 H \cup x_2 H) \dots$

Va exista un moment în care vom obține:

$$G = H \cup x_1 H \cup x_2 H \cup \dots \cup x_n H$$

Dacă nu obțin egalitatea menționată $\Rightarrow |G| \geq (n+1) \cdot |H| \geq n+1, \forall n$ ~~abs~~

abs pt că G este finită.

Cazul II): $(G, \cdot)$ grup finit comutativ, $g \in G$

T. Lagrange

Atunci $g^{|G|} = e$. $e = 1$

Azi: Dem pt. necomutativ

G grup finit $g \in G$

$\operatorname{ord} g = \min \underbrace{\{k \in \mathbb{N}^* \mid g^k = e\}}_{\text{nevidă}}$

ordinul lui g

Justificare: $\{g, g^2, g^3, \dots, g^{|G|}, g^{|G|+1}\} \subseteq G$ $\Rightarrow$ are $|G|$ elem.

$\Rightarrow 1 \leq i \leq j \leq |G|+1$

a.î.: $g^i = g^j$

$g^{j-i} = e$

$1 \leq j-i \leq |G|$

T Lagrange: $(G,\cdot)$ gr finit, $H \le G$. Să se arate că $|H| \,|\, |G|$ (exercițiu)

Dem. $g \in G$ $\quad H = \{e, g, g^2, \dots, g^{d-1}\}$ $\quad \boxed{\begin{array}{l} 1)\ H \le G \\ 2)\ |H| = d \end{array}}$

$g^i \cdot g^{d-i} = g^d = e$

$0 \le i \le d-1$

$1 \le j - i \le d-1$

$g^r = g^i \cdot g^j = g^{i+j} \in H$ $\qquad g^0 = e$

$i+j = d q + r$ $\qquad 0 \le i < j \le d-1 \Rightarrow g^i \ne g^j$

$r = \{0, 1, \dots, d-1\},\ q \in \mathbb{Z}$ $\qquad$ Dacă $g^i = g^j \Rightarrow \boxed{g^{d-1} = e}$

def lui d

acum folosim T. Lag $\Rightarrow d = |H| \,|\, |G|$

$|G| = d \cdot m$

$m \in \mathbb{N}^*$

$g^{|G|} = g^{dm} = (g^d)^m = e^m = e$

Exemple:

$G = (\mathbb{Z}_{100}, +)$

ord $\overline{56} = ?$

def: cel mai mic $d \in \mathbb{N}^*$ a.î.

$\overline{56d} = d \cdot \overline{56} = \overline{0}$ $\qquad 100 \,|\, 56d$

$25 \,|\, 14d \Rightarrow 25 \,|\, d$

ord $\overline{56} = 25$

$G_1 = \underset{(G,\cdot)}{U}(\mathbb{Z}_{100}) \to$ grup cu 40 elemente

$\overline{3} \in G$ $\qquad$ ord $\overline{3}$ în G_1

• Cum se calculează ord $\bar{\nu}$, $\bar{\nu} \in S_n$? (ordinul unei permutări)

1) Se descompune $\bar{\nu}$ în produs de cicli disjuncți.

$(a_1, a_2, \dots, a_k)$ este un ciclu al lui $\bar{\nu}$.

Def - k s.n. lungimea ciclului $(a_1, a_2, \dots, a_k)$

$$\bar{\nu}(a_j) = \begin{cases} a_{j+1} & \forall j = \overline{1, k-1} \\ a_1 & j = k \end{cases}$$

ord $(a_1, a_2, \dots, a_k) = k$

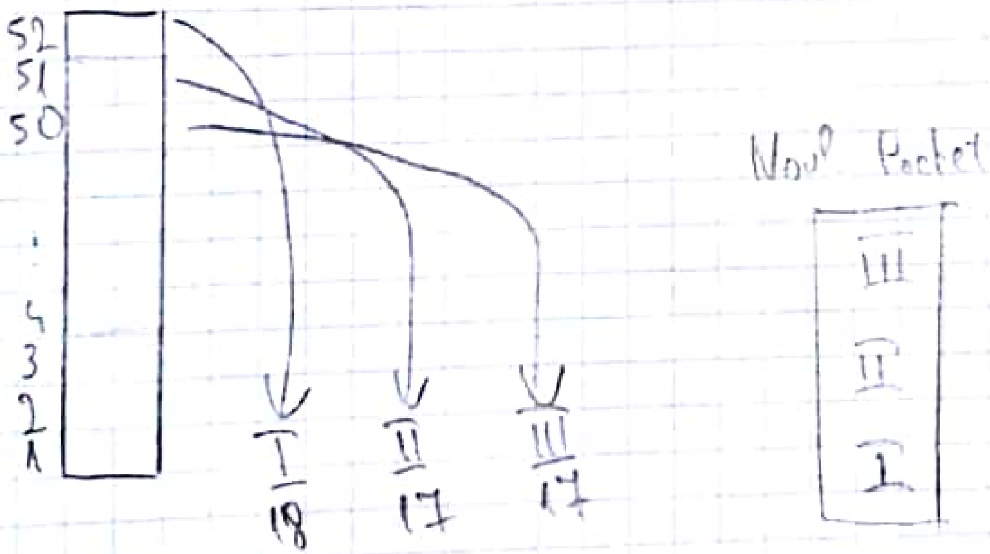
în S_n: $a_i \neq a_j$ pt. $i \neq j$

$$a_j \in \{1, 2, \dots, n\} \quad \forall j = \overline{1, k}$$

2) ord $\bar{\nu}$ = c.m.m.m.c al lungimilor ciclilor care apar în descompunerea lui $\bar{\nu}$

---

problema cu pachetul de cărți (C1?)



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
18	52	35	17	51	34	16	50	33	15	49	32	14	48	31	13	47	30	12	46	29	11	45	28	10	44

27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
27	9	43	26	8	42	25	7	41	24	6	40	23	5	39	22	4	38	21	3	37	20	2	36	19	1