Grupuri finite

Teorema lui Lagrange

Fie G un grup finit și H un subgrup al său. Atunci $|H| \mid |G|$.

Dem: Definim „$\equiv_H$" pe G

$$x \equiv_H y \iff x^{-1} y \in H.$$

- relație de echivalență
- clase de forma xH, $x \in G$.
- Pentru x fixat,

$$\varphi_x : H \to xH$$

$$\varphi_x(y) = x \cdot y \quad \text{bijecție.}$$

Deci fiecare clasă are același cardinal, anume $|H|$.

Clasele partiționează G, deci

$$|G| = |H| \cdot (\text{nr. de clase})$$

Notăm mulțimea claselor $(G/H)_s$ a clase la stânga

$|(G/H)_s| = $ (nr. de clase) se notează $[G:H]$, indicele lui H în G.

$$|G| = |H| \cdot [G:H]. \quad \square$$

Altă relație de echivalență pe G:

$x \sim y \iff (\exists)\, z \in G$ astfel încât $y = z^{-1} x z$.

„$\sim$" s.n. relația de conjugare.

$Orb(x)$ = orbita lui x = clasa lui x

Putem vedea relația $y = z^{-1} x z$ ca pe „z transportă pe x în y"

$Orb(x)$ = „locurile unde ajunge x"

$Stab(x)$ = „acei z care îl țin pe x nemișcat"

$$= \{ z \in G : x = z^{-1} x z \}$$

$$= \{ z \in G : z x = x z \} = C_x$$ comutatorul lui x

C_x e subgrup în G, $(\forall) x \in G$

Exemplu: S^3:

$\{e, (1\,2), (2\,3), (3\,1), (1\,2\,3), (1\,3\,2)\}$

$Orb(e) = \{e\}$

$Orb((1\,2)) = \{(1\,2), (2\,3), (1\,3)\}$

$Orb((1\,2\,3)) = \{(1\,2\,3), (1\,3\,2)\}$

$Stab(1\,2) = \{e, (1\,2)\}$

$C_x = Stab(x)$ e subgrup în G, deci are sens $[G : Stab(x)]$.

Propoziție: Pentru orice $x \in G$,

$$[G : Stab(x)] = |Orb(x)|$$

Intuitiv, dacă $Stab(x) = \{e\}$, atunci elemente distincte $z_1, z_2 \in G$ duc pe x în elemente distincte $z_1^{-1} * z_1$ și $z_2^{-1} * z_2$.

Dacă $\mathrm{Stab}(*) \neq \{e\}$, atunci pt. fiecare element $s \in \mathrm{Stab}(*)$ și $z \in G$,

z și $s \cdot z$ duc pe $*$ în același element

$$z^{-1} \cdot * \cdot z = z^{-1} \cdot s^{-1} \cdot * \cdot s \cdot z .$$

Deci, numărul total de locuri în care ajunge $*$ este $\dfrac{|G|}{|\mathrm{Stab}(*)|} = [G : \mathrm{Stab}\, *]$.

Demonstrație formală:

Definim $\varphi : \left(G/_{\mathrm{Stab}(*)}\right)_s \longrightarrow \mathrm{Orb}(*)$

$$\varphi(y\,\mathrm{Stab}(*)) = y * y^{-1}$$

• Bună definire + injectivitate:

$y\,\mathrm{Stab}(*) = z\,\mathrm{Stab}\, * \iff y \equiv_{\mathrm{Stab}(*)} z \iff$

$\Leftrightarrow y^{-1}z \in Stab(x) \Leftrightarrow$

$\Leftrightarrow z^{-1}y\,x\,y^{-1}z = x \Leftrightarrow y x y^{-1} = z \cancel{x} z^{-1}$

- Surjectivitate:

Orice $y^{-1}xy \in Orb(x)$ este egal cu

$\varphi(y^{-1}Stab(x))$.

Deci φ e bijectivă,

de unde $[G : Stab(x)] = \left|\left(G/_{Stab(x)}\right)_s\right| =$

$= |Orb(x)|$. $\square$

Orbită trivială + centrul grupului.

Ce elemente au orbită trivială,

adică $Orb(x) = \{x\}$?

$y^{-1}xy = x$, $(\forall) y \in G \Leftrightarrow xy = yx$,

$y \in G$,

deci $\mathrm{Orb}(x) = \{x\} \Leftrightarrow$

$\Leftrightarrow$ x comută cu toate elementele grupului

$\Leftrightarrow$ $x \in \underbrace{Z(G)}_{} = \{y \in G : xy = yx\}$

centrul grupului G,
subgrup în G, abelian

„~" relație de echivalență $\Rightarrow$ clasele formează partiție a lui G.

Fie S = sistem de reprezentanți pentru „~" (adică în S este un element și numai unul din fiecare clasă)

Dacă G e grup finit, atunci

$$|G| = \sum_{x \in S} |\mathrm{Orb}(x)| = \sum_{x \in S} [G : \mathrm{Stab}(x)]$$

$$= \sum_{x \in S} [G : C_x]$$

Dacă $Orb(x)$ e trivială i.e. $x \in Z(G)$,
atunci $[G : C_x] = \{1\}$,
deci putem rescrie relația:

$$|G| = |Z(G)| + \sum_{\substack{x \in \{ \\ Orb(x) \\ \text{netrivială}}} [G : C_x]$$

Ecuația claselor de conjugare.

Ordinul unui element

Fie G grup, $x \in G$,

$\langle x \rangle$ = subgrupul generat de x

$= \{ \ \dots x^{-2}, x^{-1}, e, x, x^2, \dots \}$

Dacă $\langle x \rangle$ e finit, atunci

$e, x, x^2, x^3, \ldots$ musai repetă termeni.

Adică $(\exists)\ \underset{i<j}{i, j \in \mathbb{N}}$ $x^i = x^j$, adică $x^{j-i} = e$

Fie acum, $\operatorname{ord}(x) = \min\{n \in \mathbb{N}^* : x^n = e\}$.

Cu această notație,

$\langle x \rangle = \{e, x, x^2, \ldots, x^{\operatorname{ord}(x)-1}\}$,

deci $\operatorname{ord}(x) = |\langle x \rangle|$.

Dacă $\langle x \rangle$ e infinit (adică, echivalent,

$x^n \neq e$, $(\forall) n \in \mathbb{N}$),

atunci spunem că $\operatorname{ord}(x) = \infty$

Definiția corespunde faptului că

$|\langle x \rangle|$ e infinit.

Dacă G e grup finit, orice element are ordin finit şi, din T. Lagrange, ordinul oricărui element divide $|G|$.

O consecinţă a acestui fapt este că

$$x^{|G|} = e, \ (\forall)\, x \in G$$

Exemple:

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

$$\mathrm{ord}(\hat{2}) = 3$$
$$\mathrm{ord}(\hat{3}) = 2$$
$$\mathrm{ord}(\hat{2}+\hat{3}) = \mathrm{ord}(\hat{5}) = 6$$

$(S_3, \cdot)$

$$\mathrm{ord}((1\,2)) = 2$$
$$\mathrm{ord}((2\,3)) = 2$$
$$\mathrm{ord}((1\,2\,3)) = 3$$
$$\mathrm{ord}((1\,2)\cdot(2\,3)) = \mathrm{ord}((1\,2\,3)) = 3$$
$$\mathrm{ord}((1\,2)\cdot(2\,3)) \neq \mathrm{ord}(1\,2)\cdot \mathrm{ord}(2\,3)$$

Dacă $x \in G$ și $ord(G) = o < \infty$,

atunci pt. $n \in \mathbb{Z}$, $x^n = e \iff o \mid n$.

„$\Leftarrow$" $\left.\begin{array}{l} o \mid n \Rightarrow \\ \Rightarrow n = o \cdot k \\ x^o = e \end{array}\right| \Rightarrow x^n = (x^o)^k = e^k = e$

„$\Rightarrow$" Presupunem $o \nmid n$, deci $n = o \cdot k + r$,
$1 \le r < o$
(din Teorema împărțirii cu rest)

$$e = x^n = x^{ok+r} = \underbrace{(x^o)^k}_{=e} \cdot x^r = x^r.$$

$x^r = e$, $r \in \mathbb{N}^*$, $r < o$, ceea ce contrazice minimalitatea lui o.

Deci $o \mid n$ $\square$

Ordinul unui produs de elemente care comută

Fie $a, b \in G$ $\quad ord(a) = m$

$ord(b) = n$

$(m, n) = 1$

Atunci $ord(ab) = mn$

Dem: $\left.\begin{array}{l} m \mid m \cdot n \Rightarrow a^{m \cdot n} = e \\ n \mid m \cdot n \Rightarrow b^{m \cdot n} = e \end{array}\right| \Rightarrow (ab)^{m \cdot n} = e \Rightarrow$

$\Rightarrow ord(ab) \mid m \cdot n.$

Fie $o = ord(ab)$

$(ab)^{o} = e \Rightarrow a^{o} \cdot b^{o} = e \mid ^{n}$

$a^{o \cdot n} \cdot \underbrace{b^{n \cdot o}}_{= e} = e \Rightarrow$

$\Rightarrow a^{o \cdot n} = e \Rightarrow \left.\begin{array}{l} m \mid o \cdot n \\ (m, n) = 1 \end{array}\right| \Rightarrow m \mid o$

Analog, $n \mid o$

$(m, n) = 1$

$\Rightarrow mn \mid o$

$o \mid mn$

Deci $o = mn$ $\square$

Ordinul unei puteri

$a \in G$

$ord(a) = o$

$ord(a^n) = ?$

În $\mathbb{Z}_6$

$ord(\hat{2}) = 3$

$ord(2 \cdot \hat{2}) = ord(\hat{4}) = 3$

$a^o = e$

$a^{[o, n]} = e \Rightarrow a^{\frac{on}{(n, o)}} = e \Rightarrow$

$\Rightarrow (a^n)^{\frac{o}{(n, o)}} = e$

Deci $ord(a^n) \mid \frac{o}{(n, o)}$

Pe de altă parte,

dacă $(a^n)^k = e \Rightarrow o \mid n\cdot k \Rightarrow$

$$\Rightarrow [o, n] \mid n\cdot k \Rightarrow$$

$$\Rightarrow \frac{on}{(n,o)} \mid n\cdot k \Rightarrow$$

$$\Rightarrow \frac{o}{(n,o)} \mid k,$$

deci $\operatorname{ord}(a^n) = \dfrac{o}{(n,o)}$ $\square$

Teorema lui Cauchy pt. grupuri finite.

Fie G un grup finit, $|G| = n$ și p nr. prim, $p \mid n$. Atunci există în G un element de ordin p.

Demonstrație:

Fie $M = \{(x_1, x_2, \dots, x_p) \in G^p :$

$x_1 \cdot x_2 \cdot \dots \cdot x_p = e\}$.

- Oricare ar fi $(x_1, x_2, \dots, x_{p-1}) \in G^{p-1}$,

$(x_1, x_2, \dots, x_{p-1}, (x_1 x_2 \dots x_{p-1})^{-1}) \in M$,

deci $|M| = n^{p-1}$.

- $(e, e, \dots, e) \in M$
- Pe M definim relația

$(x_1, x_2, \dots, x_p) \sim (y_1, y_2 \dots y_p)$

dacă și numai dacă

$(y_1, \dots y_p)$ se obține din

$(x_1, \dots x_p)$ printr-o permutare

circulară

(de ex: $(1, 2, 3, 4, 5) \sim (4, 5, 1, 2, 3)$)

Relația „$\sim$" este relație de echivalență.

• Cum arată clasele?

Dacă $(x, x, x, \dots x) \in M$,

atunci clasa lui $(x, x, \dots x)$ este exact $\{(x, x, \dots x)\}$.

Dacă $(\exists)$ i, j cu $x_i \neq x_j$,

clasa lui $(x_1, x_2, \dots x_p)$ este

$\{(x_2, x_3, \dots x_p, x_1), (x_3, x_4, \dots x_p, x_1, x_2) \dots$

$\dots (x_p, x_1, \dots x_{p-1}), (x_1, x_2, \dots, x_p)\}$,

deci are p elemente.

• Cum clasele formează o partiție a lui M,

$n^{p-1} = |M| = (\text{nr. clase cu 1 elem}) + p \cdot (\text{nr. clase cu } p \text{ elemente})$.

$p \mid n$, deci $p \mid (\text{nr. clase cu 1 element})$

Dar $(e, e, e, \dots, e) \in M$ și clasa lui are un singur element, de unde

(nr. clase cu 1 element) $\neq 0$,

deci (nr. clase cu 1 elem.) $\geq p \geq 2$,

de unde există $x \in G \setminus \{e\}$ cu

$(x, x, \dots, x) \in M$, adică $x^p = e$.

- Am obținut $x \in G$, $x \neq e$ și $x^p = e$.

Deci $ord(x) \neq 1$ și $ord(x) \mid p$, de unde $ord(x) = p$ $\square$

Fie G grup finit, $|G| = n$ și $k \in \mathbb{Z}$. Atunci funcția $f: G \to G$ $f(x) = x^k$ este bijectivă $\Leftrightarrow (n, k) = 1$.

Dem: „$\Rightarrow$" Știm că f e bijectivă.

Presupunem că $(n, k) = d > 1$

Fie p nr. prim cu $p \mid d \Rightarrow p \mid$

Din Teorema lui Cauchy, există $x \in G$ cu $ord(x) = p$.

$p \mid k$, deci $x^k = e$, de unde $x^k = e^k$, dar $x \neq e$, căci $ord(x) = p$.

Am ajuns la o contradicție cu f injectivă.

Deci $(n, k) = 1$.

„$\Leftarrow$" Știm $(n,k)=1$

G e mulțime finită, deci, dacă demonstrăm că f e injectivă $\Rightarrow$ f e bijectivă.

$(n,k)=1$, deci există $a, b \in \mathbb{Z}$ astfel încât $n \cdot a + k \cdot b = 1$

Fie $x, y \in G$ cu $x^k = y^k$.

Ridicând la puterea b și ținând cont că $x^n = y^n = e$, avem

$$x^{k \cdot b} = y^{k \cdot b} \Rightarrow \underbrace{x^{n \cdot a}}_{e} * x^{k \cdot b} = \underbrace{y^{n \cdot a}}_{e} \cdot y^{k \cdot b} \Rightarrow$$

$$\Rightarrow x^{n \cdot a + k \cdot b} = y^{n \cdot a + k \cdot b} \Rightarrow x = y,$$

deci f e injectivă. $\square$

Două aplicații ale Ecuației claselor de conjugare

(1) Fie G un grup cu p^n elemente, unde p e nr. prim. Atunci $|Z(G)| > 1$.

Soluție:

Dacă $Z(G) = G$, atunci $|Z(G)| > 1$

În continuare, presupunem $Z(G) \neq G$

Fie S un sistem de reprezentanți pentru clasele de conjugare netriviale.

Presupunem că $Z(G) \neq G$. Deci S e nevidă.

Scriem ecuația claselor:

$$p^2 = |G| = |Z(G)| + \sum_{x \in S} [G : C_x]$$

Pentru $x \in S$, avem $x \notin Z(G)$ (altfel clasa lui x ar fi trivială),

deci $C_x \neq G$, de unde

$$[G : C_x] \neq 1.$$

$[G : C_x] \mid |G| = p^n$, deci

$p \mid [G : C_x]$

Din ecuația claselor, $p \mid |Z(G)|$ $\Rightarrow$

$e \in Z(G) \Rightarrow |Z(G)| \geq 1$

$\Rightarrow |Z(G)| \geq p > 1$ $\square$

(2) $(G, \cdot)$ grup finit, $|G| = n$

Presupunem că există $k \in \mathbb{N}^*$ a.î.

$|C_x| = k$, $(\forall) x \in G \setminus \{e\}$

Arătați că G e abelian

Soluție:

Remarcă: G e grup abelian $\Leftrightarrow Z(G) = G$

(adică elementele care comută cu toți

sunt toate elementele grupului)

Presupunem că $Z(G) \neq G$.

Fie S un sistem de reprezentanți pt. orbitele netriviale. $Z(G) \neq G$, deci S e nevidă.

Ecuația claselor:

$$|G| = |Z(G)| + \sum_{x \in S} [G : C_x]$$

$$n = |Z(G)| + |S| \cdot \frac{n}{k}$$

(evident $k \mid n$, pentru că C_x e subgrup)

Dacă $Z(G) \neq \{e\}$, atunci există $x \in Z(G) \setminus \{e\}$. Prin urmare, $|C_x| = k$.

Dar $x \in Z(G)$, deci comută cu toți din G, rezultând $C_x = G$, de unde $|Z(G)| = n$, ceea ce contravine faptului că $S \neq \emptyset$.

Deci $|Z(G)| = 1$.

Ecuația claselor devine:

$$n = 1 + |S| \cdot \frac{n}{k}, \text{ deci } \frac{n}{k} \,\Big|\, 1,$$

de unde $n = k$, deci $|C_x| = n$, $(\forall)\, x \in G \setminus \{e\}$

Rezultă că $C_x = G$, $(\forall)\, x \in G \setminus \{e\}$,

de unde $x \in Z(G)$

Prin urmare $Z(G) = G$, contradicție

cu presupunerea că $Z(G) \neq G$.

În concluzie, G e grup abelian. $\square$

Grupuri ciclice

Un grup G se numește ciclic, dacă există $x \in G$ astfel încât $\langle x \rangle = G$.

Proprietăți:

- $\langle x \rangle = G \Rightarrow \text{ord}\, x = |G|$ (finit sau nu)
- Dacă G e grup finit și $x \in G$ cu $\text{ord}(x) = |G|$, atunci $\langle x \rangle = G$, deci G e ciclic.
- Orice grup ciclic este abelian

Elementele $x \in G$ care au proprietatea că $\langle x \rangle = G$ se numesc generatorii lui G.

Exemple:

$(\mathbb{Z}, +)$ e ciclic, generat de 1 sau -1.

$(\mathbb{Z}_n, +)$ e ciclic, generat (printre altele) de $\hat{1}$.

$U_n = \{ z \in \mathbb{C} : z^n = 1 \}$

$(U_n, \cdot)$ e ciclic, generat de

$$\varepsilon = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} .$$

③ Cine sunt generatorii lui $(\mathbb{Z}_n, +)$?

Exemplu: $\mathbb{Z}_6 : \{ \hat{0}, \underline{\hat{1}}, \hat{2}, \hat{3}, \hat{4}, \underline{\hat{5}} \}$

$\mathbb{Z}_{12} : \{ \hat{0}, \underline{\hat{1}}, \hat{2}, \hat{3}, \hat{4}, \underline{\hat{5}}, \hat{6}, \underline{\hat{7}}, \hat{8}, \hat{9}, \hat{10}, \underline{\hat{11}} \}$

$\text{ord}(\hat{k}) = n \iff (n, k) = 1$. "ridicare la putere"

Demonstrație: $\text{ord}(\hat{k}) = \text{ord}(k \cdot \hat{1}) =$

$$= \frac{\text{ord}(\hat{1})}{(\text{ord}(\hat{1}), k)} = \frac{n}{(n, k)} ,$$

care este egal cu n doar dacă $(n, k) = 1$.

Am aplicat formula $\text{ord}(x^m) = \dfrac{\text{ord}(x)}{(\text{ord}\, x, m)}$, doar că am folosit notația aditivă.

Propoziție

Orice grup cu nr. prim de elemente este ciclic.

Dem: $|G|=p$. Din T. Cauchy, există în G un element de ordin p. Deci G e ciclic. $\square$

Propoziție

Orice grup ciclic e izomorf cu $\mathbb{Z}$ sau cu $\mathbb{Z}_n$, unde $n \in \mathbb{N}$.

Demonstrație: Fie x un generator pentru G.

Dacă $|G|$ e infinit, rezultă că, $(\forall)\ n \in \mathbb{N}^*$, $x^n \neq e$.

(altfel, am avea $G \subseteq \{e, x, x^2, \dots, x^{n-1}\}$)

Deci funcția $f: \mathbb{Z} \to G$

$f(n) = x^n$ este bijectivă

(Surjectivă, din faptul că $G = \langle x \rangle$ și injectivă, pentru că $x^n \neq e$, $(\forall)\ n \in \mathbb{N}^*$)

Mai mult, f este morfism, deci

$\mathbb{Z} \simeq G$

Dacă $|G| < \infty$, fie $|G| = n$

Atunci $ord(x) = n$ și

$f : \mathbb{Z}_n \to G$

$f(\hat{k}) = x^k$ este:

- bine definită și injectivă

$\hat{k} = \hat{l} \Leftrightarrow n \mid k - l \Leftrightarrow x^{k-l} = e \Leftrightarrow$

$\Leftrightarrow x^k = x^l$

- surjectivă, căci $G = \langle x \rangle = \{e, x, x^2, \dots x^{n-1}\}$.
- morfism de grupuri

Rezultă $G \simeq \mathbb{Z}_n$

④ Orice subgrup finit al lui $(\mathbb{C}^*, \cdot)$ este de forma U_n cu $n \in \mathbb{N}^*$, deci e ciclic.

Soluție:

Fie $G \leq \mathbb{C}^*$, $|G| = n \in \mathbb{N}^*$.

Orice element $x \in G$ are proprietatea că $\mathrm{ord}(x) \mid n$, deci $x^n = 1$.

Prin urmare, $G \subseteq U_n$.

Dar $|G| = n$ și $|U_n| = n$, de unde

$$G = U_n. \quad \square$$

5. Fie G un grup cu $|G| = 2010$ astfel încât există în $Z(G)$ două elemente de ordine 5, respectiv 6.

Arătați că G e abelian.

Soluție:

Fie $a, b \in G$ $\quad$ $ord(a) = 5$, $ord(b) = 6$, $(5, 6) = 1$, $a, b \in Z(G) \Rightarrow ab = ba$ $\Rightarrow ord(ab) = 30$.

$Z(G)$ e subgrup în G $\Rightarrow ab \in Z(G)$ $\Rightarrow$

$\Rightarrow 30 \mid |Z(G)|$

$2010 = 30 \cdot 67$

67 e nr. prim, deci, din T. Cauchy, există $x \in G$ cu $ord(x) = 67$.

$ab \in Z(G) \Rightarrow ab$ comută cu x, $ord(ab) = 30$, $(30, 67) = 1$ $\Rightarrow$

$\Rightarrow \operatorname{ord}(a \cdot b x) = 30 \cdot 67 = 2010$

de unde G e ciclic, deci abelian. $\square$

⑥ Fie G un grup cu nr. impar de elemente și H un subgrup al lui G.

Arătați că un element $a \in G$ este în H dacă și numai dacă $a^2 \in H$.

Soluție:

„$\Rightarrow$"

H subgrup, deci $a \in H \Rightarrow a^2 \in H$

Fie $|G| = 2n+1$, $n \in \mathbb{N}$

„$\Leftarrow$"

$a^2 \in H \Rightarrow a^{2n} \in H \Rightarrow a^{-2n} \in H$

$|G| = 2n+1 \Rightarrow a^{2n+1} = e \in H$

$\Rightarrow$

$\Rightarrow a = a^{2n+1} \cdot a^{-2n} \in H.$

$\square$

(7) Fie p un nr. prim și G un grup cu p^2 elemente.

Atunci G e grup abelian.

Soluție:

Ne amintim că G e abelian dacă și numai dacă $Z(G) = G$.

Presupunem $Z(G) \neq G$, atunci există clase de conjugare netriviale. Fie S un sistem de reprezentanți pentru aceste clase.

Ecuația claselor:

$$p^2 = |G| = |Z(G)| + \sum_{x \in S} [G : C_x].$$

Dacă $x \notin Z(G)$, atunci $C_x \neq G$, deci $[G : C_x] \neq 1$.

Deoarece $[G:C_x] \mid p^2$, rezultă

$$p \mid [G:C_x].$$

Am obținut $p \mid [G:C_x]$, $(\forall) x \in S$.

Din ecuația claselor, obținem $p \mid |Z(G)|$

$|Z(G)| < p^2$, deci $|Z(G)| = p$

Fie acum $x \in G \setminus Z(G)$.

$Z(G)$ e mulțimea elementelor care comută cu toți, deci $Z(G) \leq C_x$.

$x \in C_x \setminus Z(G)$, deci $C_x \neq Z(G)$.

Din Th. lui Lagrange, $|Z(G)| \mid |C_x|$,

deci $p \mid |C_x|$ și $p < |C_x|$.

Cum $C_x \leq G$, $|C_x| \mid |G| = p^2$ $\Rightarrow$

$\Rightarrow |C_x| = p^2$, de unde $C_x = G$.

Prin urmare, x comută cu orice element din G, adică $x \in Z(G)$, contradicție cu $x \in G \setminus Z(G)$.

În concluzie, $Z(G) = G$, deci G e abelian.

$\square$