2. Teoremele lui Lagrange şi Cauchy pentru grupuri finite

2. 1. Teorema lui Lagrange şi teorema lui Cauchy

2.1.1. Definiţie *Fie H un subgrup al grupului $(G, \cdot)$. Se definesc relaţiile de echivalenţă ρ_H , ρ'_H (la stânga, respectiv la dreapta) pe G, după cum urmează:*
$x \rho_H y \Leftrightarrow x^{-1}y \in H$ şi $x \rho'_H y \Leftrightarrow yx^{-1} \in H$.
xH si Hx sunt clasele de echivalenţă la stânga, respectiv la dreapta ale lui x în raport cu H ($y \in xH \Leftrightarrow x \rho_H y$ şi $y \in Hx \Leftrightarrow x \rho'_H y$)

Mulţimile $G / \rho_H = \{H, xH, yH, ...\}$ şi $G/\rho'_H = \{H, Hx, Hy, ...\}$ sunt mulţimile claselor de echivalenţă la stânga, respectiv la dreapta în raport cu H.

2.1.2. Observaţii

1) Funcţia $f : G / \rho_H \to G / \rho'_H$ dată prin relaţia $f(xH) = Hx^{-1}$ este bijectivă, $|G / \rho_H| = |G / \rho'_H| = |G : H|$ şi se numeşte indicele subgrupului H în grupul G.

2) $xH \cap yH \neq 0 \Leftrightarrow xH = yH$

Într-adevăr, dacă $a \in xH \cap yH$, atunci $\exists\, h_1, h_2 \in H$, astfel încât $a = xh_1 = yh_2$.
Atunci $x = yh_2h_1^{-1}$ şi cum $h_2h_1^{-1} \in H$, rezultă că $x \in yH$, aşadar $xH \subseteq yH$.
Analog se demonstrează cealaltă incluziune.

2.1.3. Definiţie *Fie N un subgrup al grupului $(G, \cdot)$. N se numeşte subgrup normal dacă şi numai dacă pentru orice $x \in G$, $xN = Nx$.*

2.1.4. Observaţii

1) Dacă N este subgrup normal al lui G, $G / \rho_N = G / \rho'_N = G / N = \{N, xN, yN, ...\}$
Se demonstrează uşor că G / N este grup (numit grupul factor al lui G în raport cu N) împreună cu operaţia „$\cdot$“ definită astfel: $xN \cdot yN = (xy)N$.

2) $|G / N| = |G : N|$

3) Orice subgrup de indice 2 este normal.

Demonstraţie: Fie N un subgrup de indice 2. Atunci $G = N \cup xN$ (cu clasele N şi xN disjuncte) şi de asemenea $G = N \cup Nx$ (cu clasele N şi Nx disjuncte).
Rezultă deci că $xN = Nx$ şi N este subgrup normal.

2.1.5. Teorema lui Lagrange

Fie $(G, \cdot)$ un grup finit şi H un subgrup al lui G. Atunci:

a) *ord(H) / ord(G)*

b) *ord(G) = ord(H) · ord(G / H)*

Demonstrație:

Fie ρ_H relația de echivalență la stânga din definiția 2.1. Conform observației 2 ce îi urmează, mulțimea claselor de echivalență la stânga în raport cu H este o partiție a mulțimii G (adică $\bigcup_{x \in G} xH = G$ și clasele sunt disjuncte două câte două). Mai mult, funcția $f : H \to xH$ dată prin $f(h) = xh$ este bijectivă, deci $\forall x, y \in G$, $|xH| = |yH| = |H|$.

Așadar, $ord(G) = ord(H) \cdot ord(G / \rho_H)$, unde G / ρ_H este mulțimea claselor de echivalență modulo ρ_H, numită și mulțime cât a lui G în raport cu relația de echivalență ρ_H.

2.1.6. Consecințe: Fie $(G, \cdot)$ un grup finit. Atunci:

1) Pentru orice $x \in G$, $ord(x) / ord(G)$
2) Pentru orice $x \in G$, $x^{ord(G)} = e$, unde e este elementul neutru al grupului G.
3) Orice grup de ordin prim este ciclic (deci izomorf cu $(\mathbf{Z}_p, +)$)

2.1.7. Teorema lui Cauchy

Fie $(G, \cdot)$ un grup finit și p un număr prim, p / ord(G). Atunci numărul soluțiilor ecuației $x^p = 1$ este un multiplu nenul al lui p.

Demonstrație:

Fie $ord(G) = n$ și $S = \{(a_1, a_2, ..., a_p) \mid a_i \in G, \forall i \in \{1, 2, ..., p\}$ și $a_1 \cdot a_2 \cdots a_p = 1\}$

Pentru orice alegere a elementelor $a_1, a_2, ..., a_{p-1}$, $a_p = (a_1 \cdot a_2 \cdots a_{p-1})^{-1}$, deci a_p este unic determinat. Așadar $ord(S) = n^{p-1}$ (1)

Definim relația de echivalență „~" pe S :

$x \sim y \Leftrightarrow$ x este o permutare circulară a lui y.

Dacă $a_1 = a_2 = \cdots = a_p$, clasa de echivalență a lui $x = (a_1, a_2, ..., a_p)$ conține un singur element și exact p elemente în caz contrar.

Într-adevăr, fie $x = (a_1, a_2, ..., a_p)$ și i, j, primul respectiv ultimul rang pentru care $a_i = a_j$ și $a_i = a_{i1} = a_{i2} = \cdots = a_{ik} = a_j$ pentru $i < i_1 < \cdots < i_k < j$ și $k > 0$, iar pentru $k = 0$, $i_1 = j$. Ca să obținem prin permutări circulare aceleași elemente pe locurile $i, i_1, \cdots, i_k, j$ (și eventual să nu rezulte permutări distincte ale lui x), ar trebui ca „distanțele" dintre elemente să fie aceleași, deci

$$p - j + i = j - i_k = \cdots = i_2 - i_1 = s.$$

Așadar $j - i_k = s$, $\cdots$, $i_2 - i_1 = s$, $i_1 - i = s$ și adunând relațiile membru cu membru obținem $j - i = (k+1) \cdot s$ și cum $p = s + j - i$, avem $p = (k+2) \cdot s$. Cum p este număr prim, rezultă $s = 1$ și deci $j = p - 1 + i$. Cum însă $j \leq p$, obținem că $p - 1 + i \leq p$, deci că $i \leq 1$. Așadar $i = 1$ și $j = p$ și suntem în prima situație, cu toate elementele lui x identice. Deci dacă cel puțin 2 elemente ale permutării

diferă, atunci există exact p permutări circulare ce se pot obține din permutarea respectivă (a p elemente).

Fie r numărul claselor cu un element (r este deci numărul soluțiilor ecuației $x^p = 1$) și t numărul claselor cu câte p elemente.

Din relația (1), rezultă că $n^{p-1} = r + p \cdot t$ și cum p / n, rezultă că p / r.

Observăm că $r \neq 0$, pentru că $(1, 1, \cdots, 1) \in S$

2.1.8. Consecințe

1) Dacă $(G, \cdot)$ e un grup finit și p e un număr prim, $p / ord(G)$, atunci există $x \in G$ astfel încât $ord(x) = p$.

2) Numărul subgrupurilor de ordin p ale lui G, (în condițiile consecintei 1) este congruent cu 1 (mod p).

Demonstrație: Din teorema lui Cauchy, există elemente de ordinul p ale grupului G. Notăm cu $k \in \mathbb{N}^*$ numărul subgrupurilor de ordinul p ale lui G. Numărul p fiind prim, acestea sunt ciclice.

$H_i = \langle x_i \rangle$, $\forall i \in \{1, 2, ..., k\}$ și $H_i \cap H_j = \{e\}$, $\forall i, j \in \{1, 2, ..., k\}$, $i \neq j$.

Fie H mulțimea soluțiilor ecuației $x^p = 1$. Rezultă $H = H_1 \cup H_2 \cup ... \cup H_k$ și deci $ord(H) = ord(H_1 \cup H_2 \cup ... \cup H_k) = k(p - 1) + 1$.

Din teorema lui Cauchy, cum numărul soluțiilor ecuației $x^p = 1$ este un multiplu nenul al lui p, rezultă $k(p - 1) + 1 \equiv 0 \pmod p$, deci $k \equiv 1 \pmod p$.

2.1.9. Propozitie *Fie $(G, \cdot)$ un grup finit astfel încât pentru orice $x \in G$, $x^2 = e$ Atunci:* ***a)*** *$(G, \cdot)$ este grup comutativ*

b) *există $k \in N$, astfel încât $ord(G) = 2^k$*

Demonstrație. Prima parte a propoziției este un exercițiu foarte cunoscut, prezent în manuale, care este adevărat și pentru cazul în care G nu este grup finit. Vom prezenta trei demonstrații pentru afirmația de la b).

Soluția I: Vom demonstra concluzia prin inducție după $n = ord(G)$:

Pentru $n = 1$, evident, $ord(G) = 2^0$. Fie $m \in \mathbb{N}^*$, $m > 1$

Presupunem că afirmația e adevărată pentru grupurile de ordin mai mic decât m cu proprietatea din enunț. Fie $(G, \cdot)$ un grup de ordin m și fie $x \in G$. Cum G este grup comutativ (conform cu punctul a)), subgrupul $N = \{e, x\}$ este un subgrup normal al lui G, adică pentru orice $y \in G$, $yN = Ny$.

Cum $(xN)xN = x^2N = eN = N$, pentru orice $x \in G$, rezultă că $(G / N, \cdot)$ este un grup factor care are proprietatea din enunț.

Din teorema lui Lagrange avem că $ord(G / N) = \dfrac{ord(G)}{ord(N)} < ord(G) = m$ și deci din ipoteza de inducție rezultă că există $k \in \mathbb{N}^*$ astfel încât $ord(G / N) = 2^k$.

Atunci $ord(G) = 2 \cdot ord(G / N) = 2^{k+1}$ şi conform principiului inducţiei matematice, afirmaţia b) este adevărată pentru orice grup finit cu proprietatea din enunţ.

Soluţia a II-a: Vom organiza grupul G ca spaţiu vectorial şi pentru simplitatea scrierii, vom considera de această dată operaţia grupului în notaţie aditivă.

Pe $(G, +)$, care are toate elementele de ordin ≤ 2, se poate introduce o structură de Z_2 – spaţiu vectorial. Cele 4 axiome ale spaţiului vectorial se verifică prin calcul direct, mulţimea scalarilor fiind finită.

Se defineşte $\hat{1} \cdot x = x$ şi $\hat{0} \cdot x = 0$.

Cum G este un spaţiu vectorial finit, el este de dimensiune finită.

Fie $B = \{e_1, e_2, ..., e_n\}$ o bază a acestuia.

Atunci, $\forall x \in G, \exists \alpha_1, \alpha_2, ..., \alpha_n \in \mathbf{Z}_2, x = \sum_{i=1}^{n} \alpha_i \cdot e_i$.

Aşadar, numărul elementelor din G coincide cu numărul n-uplurilor $(\alpha_1, \alpha_2, ..., \alpha_n)$ ce se pot forma cu elemente din $\mathbf{Z}_2$, deci cu numărul funcţiilor ce se pot defini de la o mulţime cu n elemente la $\mathbf{Z}_2$, care este 2^n.

Soluţia a III-a: Presupunem că ordinul grupului G nu este o putere a lui 2. Atunci $\exists p \in \mathbf{N}$, p număr prim, $p \geq 3$, astfel încât $p / ord(G)$. Atunci, din consecinţa 1 a teoremei lui Cauchy rezultă că există $a \in G$, $ord(a) = p$. Avem $a^p = e$ şi cum $a^2 = e$ obţinem $a^{(p, 2)} = a^1 = e$, fals. Aşadar $\exists n \in \mathbf{N}$, $ord(G) = 2^n$.

2.1.10. Generalizare *Fie $(G, \cdot)$ un grup finit şi $p \in N$ un număr prim astfel încât $\forall x \in G, x^p = e$. Atunci ordinul lui G este o putere a lui p.*

Demonstraţia acestui rezultat se face cel mai uşor prin reducere la absurd şi folosind teorema lui Cauchy, ca în cazul precedent.

Bibliografie

1. Gh. Andrei, C-tin Caragea, V. Ene – *Algebră – Culegere de probleme pentru examene de admitere şi olimpiade şcolare*, Ed. Scorpion 7, Bucureşti 1995
2. M. Burtea, G. Burtea – *Matematică – clasa a XII-a – Elemente de analiză matematică. Algebră superioară*, Ed. Carminis 2001
3. D. Popescu, C-tin Vraciu – *Elemente de teoria grupurilor finite*, Ed Ştiinţifică şi Enciclopedică Bucureşti 1986 – pag 77 - 78
4. Colecţia *G. M.*

Probleme rezolvate

R2.2.1. *Fie $(G, \cdot)$ un grup finit. Dacă m şi n sunt divizori ai ordinului grupului, atunci ecuaţiile $x^m = e$ şi $x^n = e$ au o singură soluţie comună dacă şi numai dacă $(m, n) = 1$.*

Mihai Piticari

Soluţie: Observăm că $x = e$ este soluţie comună a ecuaţiilor.

„$\Leftarrow$" $(m, n) = 1 \Rightarrow \exists\, h, k \in \mathbf{Z},\ m \cdot h + n \cdot k = 1$.

Fie $a \in G$ o soluţie comună a celor două ecuaţii. Atunci $a^{m \cdot h} = e$, $a^{n \cdot k} = e$ şi obţinem $a = a^{m \cdot h + n \cdot k} = e$

„$\Rightarrow$" Fie $(m, n) = d$. Dacă $d \geq 2$, există $p \in \mathbf{N}$, p prim, astfel încât $p \mid d$.

Din consecinţa 1 a teoremei lui Cauchy rezultă că există $b \in G \setminus \{e\}$, $ord(b) = p$ $\Rightarrow b^p = e$ şi cum $b^d = e \Rightarrow$ ecuaţia $x^d = e$ nu are soluţie unică, fals.

Rezultă $d = 1$.

R2.2.2. *Fie $(G, \cdot)$ un grup finit. Să se demonstreze că următoarele afirmaţii sunt echivalente:*

a) *G este ciclic*

b) *Pentru orice $d \in \mathbf{N}^*$, există cel mult un subgrup de ordinul d în G.*

Soluţie: Reamintim că pentru $n \in \mathbf{N}$, indicatorul $\varphi(n)$ al lui Euler ($\varphi(n)$ este numărul tuturor numerelor naturale mai mici decât n şi prime cu n) verifică formula lui Gauss: $\sum_{d/n} \varphi(d) = n$ (sumarea făcându-se după toţi divizorii lui n, inclusiv 1 şi n).

„$a \Rightarrow b$" Dacă $ord(G) = n$ şi $d \mid n$, $d \in \mathbf{N}^*$, atunci unicul subgrup de ordinul d al lui G este $H = \{x \in G \mid x^d = 1\}$

Într-adevăr, $ord(H) = d$, pentru că grupul ciclic G are un element de ordinul d $\left(\text{dacă } G = \langle y \rangle \Rightarrow ord\left(y^{\frac{n}{d}} \right) = d \right)$, care se află în H şi care de fapt îl generează pe H. Presupunând că există $H' \neq H$, H' subgrup de ordinul d al lui G, avem că $\forall\, x \in H'$, $x^{ord(H')} = x^d = 1 \Rightarrow x \in H \Rightarrow H' \subset H$ şi cum au acelaşi număr de elemente, rezultă că $H' = H$.

„$b \Leftarrow a$" Dacă afirmaţia b) este adevărată, pentru $d \in \mathbf{N}^*$, fie $M_d = \{a \in G \mid ord(a) = d\}$. Mulţimile M_d sunt disjuncte două câte două şi reuniunea lor este mulţimea elementelor lui G. În plus, dacă $x \in M_d \Rightarrow ord(x) \mid d$.

Dar $ord(x) / ord(G) = n$. În concluzie, $M_d \neq \emptyset \Leftrightarrow d / n \Leftrightarrow \exists$ un subgrup ciclic H_d, de ordin d al lui G, Din ipoteză, H_d este unicul subgrup de ordin d al lui G şi deci $M_d = \{a \in G \mid \langle a \rangle = H_d\}$, iar $|M_d| = \varphi(d)$.

Avem $n = |G| = \sum_{d/n} |M_d| = \sum_{d/n} \varphi(d)$.

Relaţia anterioară este adevărată (Gauss) şi cum unul dintre divizorii lui n din formula anterioară este chiar n, există un subgrup ciclic H_n de ordinul n, al lui G. Atunci $G = H_n$ şi G este ciclic.

R2.2.3. *Fie $(G, \cdot)$ un grup cu $4n + 2$ elemente $(n \in N)$. Să se determine numărul elementelor $x \in G$ astfel încât $x^{2n+1} = e$.*

Marian Andronache

Soluţie: Fie $G = \{e, a_1, ..., a_{n-1}\}$ şi S(G) mulţimea permutărilor lui G (a funcţiilor bijective de la G la G).

Pentru $a \in G$, funcţia $\sigma_a : G \to G$, $\sigma_a(x) = a \cdot x$, $\forall x \in G$ este în S(G), iar $f : G \to S(G)$, $f(a) = \sigma_a$, $\forall a \in G$ este un morfism injectiv de grupuri.

Fie $H = f(G)$. Atunci $G \approx f(G) = H = \{\sigma_e, \sigma_{a_1}, ..., \sigma_{a_{n-1}}\}$ şi H este un subgrup al lui S(G) (Acest rezultat este teorema lui Cayley). $2 / ord(G) \Rightarrow \exists a \in G$, $ord(a) = 2$

Atunci, $\sigma_a^2(x) = a(ax) = x$, $\forall x \in G \Rightarrow \sigma_a^2 = \bar{e}$ (permutarea identică)

$a \neq e \Rightarrow \sigma_a$ nu are puncte fixe $\Rightarrow$ în σ_a apar $2n + 1$ perechi de tipul $\begin{pmatrix} i & j \\ j & i \end{pmatrix} \Rightarrow$

$\Rightarrow \sigma_a$ este produsul a $2n + 1$ transpoziţii disjuncte $\Rightarrow \varepsilon(\sigma_a) = -1$ (1)

În consecinţă, H este un grup de permutări care are o permutare impară şi de aici, numărul permutărilor pare din H este egal cu numărul permutărilor impare din H ($= 2n + 1$). Într-adevăr, dacă $e, \sigma_1, ..., \sigma_{k-1}$ sunt toate permutările pare din H şi $\sigma_k, ..., \sigma_{n-1}$ sunt toate permutările impare din H, avem $\sigma_k^2, ..., \sigma_k \cdot \sigma_{n-1}$ permutări pare $\Rightarrow n - k \leq k$ şi cum $\sigma_k \cdot e, \sigma_k \cdot \sigma_1, ...,$ $\sigma_k \cdot \sigma_{k-1}$ sunt permutări impare $\Rightarrow k \leq n - k$ şi deci $k = n - k$.

Fie $A = \{x \in G \mid x^{2n+1} = e\}$ şi $x \in A$.

$\bar{e} = f(e) = (f(x))^{2n+1} = (\sigma_x)^{2n+1} \Rightarrow \varepsilon((\sigma_x)^{2n+1}) = 1 \Rightarrow \varepsilon(\sigma_x) = 1 \Rightarrow \sigma_x$ permutare pară $\Rightarrow |A| \leq 2n + 1$ (2)

Fie $B = \{x \in G \mid x^{2n+1} \neq e\}$ şi $y \in B \Rightarrow a \overset{not}{=} y^{2n+1} \neq e$ şi $a^2 \overset{(1)}{=} e \Rightarrow \varepsilon(\sigma_a) = -1$

$\sigma_a = f(a) = (f(y))^{2n+1} = (\sigma_y)^{2n+1}$ şi cum $\varepsilon(\sigma_a) = -1$ obţinem că $\varepsilon(\sigma) = -1 \Rightarrow$

$\Rightarrow |B| \leq 2n + 1$ (3) Din (2) şi (3) deducem că $|A| = |B| = 2n + 1$.

R2.2.4. *Demonstrați că un grup cu $4n+2$ elemente admite cel mult un subgrup cu $2n+1$ elemente.*

Eugen Păltănea, Sabin Tăbârcă

Soluție: Dacă H e un subgrup al lui $G \Rightarrow \text{ord}(H) < 4n+2 \Rightarrow \text{ord}(H) \leq 2n+1$.
Pentru $n = 0$ enunțul este adevărat.
Pentru $n \geq 1$, dacă $H = \{e, x_1, ..., x_{2n}\}$ este nu subgrup al lui G cu $2n+1$ elemente și $x \in G$, $\text{ord}(x) = 2$ (există, din consecința teoremei lui Cauchy), atunci $x \notin H \Rightarrow x \cdot x_i \notin H$, $\forall\ i = \overline{1, 2n} \Rightarrow G = H \cup \{x \cdot x_i \mid i = \overline{1, 2n}\}$.

Demonstrăm că $\forall\ y, z \in G \setminus H$, $y \cdot z \in H$ (1)

Fie $y, z \in G \setminus H \Rightarrow \exists\ x_i, x_j \in H$, $y = x \cdot x_i$, $z = x \cdot x_j$. $x_i \cdot x \notin H \Rightarrow \exists\ x_k \in H$, $x_i \cdot x = x \cdot x_k$
Atunci $y \cdot z = x \cdot x_i \cdot x \cdot x_j = x \cdot (x_i \cdot x) \cdot x_j = x \cdot x \cdot x_k \cdot x_j = x_k \cdot x_j$.
Deci $y \cdot z = x_k \cdot x_j$ și cum $x_k, x_j \in H$ deducem că $y \cdot z \in H$, așadar (1) este adevărată.
Presupunem că există subgrupul H' al lui G, de ordin $2n+1$, cu $H' \neq H$.
Avem $H \cap H'$ subgrup al lui G și $H \cap H' \neq H$, $H \cap H' \neq H'$.

Notăm $\text{ord}(H \cap H') = p \Rightarrow p \mid 2n+1$, $p \neq 2n+1$. Atunci $p < \left[\frac{2n+1}{2}\right] = n$.

Notăm, după o eventuală redenumire a elementelor,
$H \cap H' = \{e, x_1, x_2, ..., x_{p-1}\}$.
Atunci $H' = \{e, x_1, x_2, ..., x_{p-1}, y_p, ..., y_{2n}\}$ cu $\{y_p, ..., y_{2n}\} \subset x \cdot H = G \setminus H$.
Din (1) obținem $y_p^2, y_p \cdot y_{p+1}, ..., y_p \cdot y_{2n} \in H \cap H'$ și deci
$p = |H \cap H'| \geq 2n - p + 1 \geq n+1$, fals.

Observații: 1) Dacă G are un subgrup H cu $2n+1$ elemente, atunci din (1) rezultă că subgrupurile K ale lui G astfel încât $K \cap H = \{e\}$ sunt de ordinul 2.
2) Dacă $|G| = 4n+2$, atunci G nu poate avea doar subgrupuri proprii de ordinul 2 (ar rezulta că ordinul lui G este o putere a lui 2, fals.)

R2.2.5. *Fie $(G, \cdot)$ un grup finit și H_1, H_2 subgrupuri ale lui G. Fie mulțimea $H_1H_2 = \{x \cdot y \mid x \in H_1,\ y \in H_2\}$. Dacă $\max\{\text{ord}(H_1), \text{ord}(H_2)\} > \frac{1}{2}\text{ord}(G)$, să se demonstreze că $H_1H_2 = G$.*

Soluție: Presupunem că $\text{ord}(H_1) \geq \text{ord}(H_2)$, deci că $\text{ord}(H_1) > \frac{n}{2}$, unde $\text{ord}(G) = n$.
Atunci, cum din teorema lui Lagrange avem că $\text{ord}(H_1) \mid \text{ord}(G)$, rezultă că $\text{ord}(H_1) = n$ și deci $H_1 = G$. Așadar $H_1H_2 = GH_2 = \{x \cdot y \mid x \in G,\ y \in H_2\}$
Elementul neutru e al grupului G se află și în H_2 și deci, oricare ar fi $x \in G$, $x = x \cdot e \in GH_2$, așadar $G \subset GH_2$ și cum și $GH_2 \subset G$, rezultă că $G = GH_2 = H_1H_2$.