CURSUL 10: GRUPURI

G. MINCU

1. Subgrupul generat de o submulţime

Definiţia 1. Fie G un grup şi $M \subset G$. Prin **subgrupul lui G generat de** M înţelegem cel mai mic (în sensul incluziunii) subgrup al lui G care conţine submulţimea M.

Vom nota subgrupul lui G generat de M cu $\langle M \rangle$. Dacă $M = \{x_1, x_2, \ldots, x_n\}$, vom folosi, în loc de $\langle \{x_1, x_2, \ldots, x_n\} \rangle$, notaţia
$\langle x_1, x_2, \ldots, x_n \rangle$.

Propoziţia 2. Fie G un grup şi $M \subset G$. Are loc relaţia

$$\langle M \rangle = \bigcap_{\substack{H \leq G \\ H \supset M}} H.$$

Propoziţia 3. Fie G un grup şi $M \subset G$. Are loc relaţia

$$\langle M \rangle = \{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} : n \in \mathbb{N}^*,\ x_1, \ldots, x_n \in M,\ \alpha_1, \ldots, \alpha_n \in \mathbb{Z}\}.$$

Observaţia 4. Dacă $g \in G$, atunci $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.

Observaţia 5. $\langle \emptyset \rangle = \{e\}$.

Definiţia 6. Fie G un grup. Submulţimea M a lui G se numeşte **sistem de generatori** al lui G dacă $\langle M \rangle = G$.

Definiţia 7. Grupul G se numeşte **finit generat** dacă el admite un sistem finit de generatori.

Exemplul 8. Orice grup admite ca sistem de generatori mulţimea sa subiacentă.

Exemplul 9. Orice grup finit este finit generat.

Exemplul 10. Pentru orice $n \in \mathbb{N}$ grupul $\mathbb{Z}_n$ este finit generat.

Exemplul 11. Pentru orice $n \in \mathbb{N}^*$ grupul S_n este finit generat.

Exemplul 12. Pentru orice $n \in \mathbb{N}^*$ grupul diedral D_n este finit generat.

Exemplul 13. Grupul $\mathbb{Z}$ este finit generat.

Exemplul 14. Pentru orice $n \in \mathbb{N}^*$ grupul $\mathbb{Z}^n$ este finit generat.

Exemplul 15. Grupurile $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ nu sunt finit generate.

Temă: Demonstraţi afirmaţiile de la exemplele 8-15!

2. GRUPURI CICLICE

Definiţia 16. Grupul G se numeşte **ciclic** dacă el admite un sistem de generatori format dintr-un singur element.

Observaţia 17. Orice grup ciclic este finit generat.

Exemplul 18. Grupul $\mathbb{Z}$ este ciclic, deoarece $\mathbb{Z} = \langle 1 \rangle$.

Exemplul 19. Pentru orice $n \in \mathbb{N}^*$ grupul $\mathbb{Z}_n$ este ciclic, deoarece $\mathbb{Z}_n = \langle \widehat{1} \rangle$.

Observaţia 20. Generatorul unui grup ciclic nu este unic determinat. De exemplu, avem şi $\mathbb{Z} = \langle -1 \rangle$, iar $\mathbb{Z}_n = \langle \widehat{a} \rangle$ dacă şi numai dacă $(a, n) = 1$.

Exemplul 21. Grupul $\mathbb{Z} \times \mathbb{Z}$ nu este ciclic.

Exemplul 22. Grupurile $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ nu sunt ciclice.

Teorema de structură a grupurilor ciclice. Orice grup ciclic cu $n \in \mathbb{N}^*$ elemente este izomorf cu $\mathbb{Z}_n$. Orice grup ciclic infinit este izomorf cu $\mathbb{Z}$.

Demonstraţie: Fie G un grup ciclic şi g un generator al acestuia. Considerăm $u : \mathbb{Z} \to G$, $u(n) = g^n$. Dacă $m, n \in \mathbb{Z}$, avem

$$u(m+n) = g^{m+n} = g^m g^n = u(m)u(n),$$

deci u este morfism de grupuri. În plus, u este în mod evident surjectiv. Aplicând teorema fundamentală de izomorfism pentru grupuri, obţinem $G = \operatorname{Im} u \simeq \dfrac{\mathbb{Z}}{\ker u}$. Prin urmare, dacă $\ker u = n\mathbb{Z}$ cu $n \in \mathbb{N}^*$ avem $G \simeq \mathbb{Z}_n$, iar dacă $\ker u = \{0\}$ avem $G \simeq \mathbb{Z}$. $\square$

Corolarul 23. Orice grup ciclic este comutativ.

Corolarul 24. Orice subgrup al unui grup ciclic este ciclic.

Corolarul 25. Orice grup factor al unui grup ciclic este ciclic.

3. Ordinul unui element într-un grup

Observaţia 26. Dat fiind un element x al unui grup G, subgrupul $\langle x\rangle = \{x^n : n \in \mathbb{Z}\}$ al lui G este ciclic.

Definiţia 27. Prin **ordinul** elementului x al grupului G înţelegem ordinul subgrupului generat de x în G.

Vom nota ordinul elementului x al grupului G cu $\text{ord}_G x$. Dacă grupul G este subînţeles în context, atunci vom folosi şi notaţia ord x.

Caracterizări ale ordinului.

Propoziţia 28. Fie G un grup şi $x \in G$. Atunci

$$\text{ord}_G x = \begin{cases} \min\{n \in \mathbb{N}^* : x^n = e\}, & \text{dacă } \{n \in \mathbb{N}^* : x^n = e\} \text{ este nevidă} \\ +\infty, & \text{altfel} \end{cases}$$

Corolarul 29. Dacă x este un element al grupului finit G, atunci $x^{\text{ord } x} = e$.

Propoziţia 30. Fie G un grup, $x \in G$ şi $n \in \mathbb{N}^*$. Atunci $\text{ord}_G x = n$ dacă şi numai dacă $x^n = e$ şi $\forall m \in \mathbb{Z}\ x^m = e \Rightarrow n|m$.

Proprietăţi ale ordinului.

Propoziţia 31. Ordinul oricărui element al unui grup finit divide ordinul respectivului grup.

Demonstraţie: Ordinul unui element, fiind ordinul unui subgrup, divide, conform teoremei lui Lagrange, ordinul grupului. □

Propoziţia 32. Dacă G, G_1 şi G_2 sunt grupuri finite, atunci:

(i) $\text{ord}_G(x^k) = \dfrac{\text{ord}_G x}{(k, \text{ord}_G x)}$.

(ii) $\text{ord}_{G_1 \times G_2}(x_1, x_2) = [\text{ord}_{G_1} x_1, \text{ord}_{G_2} x_2]$.

(iii) $\text{ord}_G(xy) = \text{ord}_G(yx)$.

(iv) Dacă $xy = yx$ şi $(\text{ord}_G x, \text{ord}_G y) = 1$, atunci

$$\text{ord}_G(xy) = \text{ord}_G x \cdot \text{ord}_G y.$$

Temă: Rămâne adevărată afirmaţia de la punctul (iv) al propoziţiei 32 în lipsa condiţiei $xy = yx$?

Temă: O generalizare naturală a afirmaţiei de la punctul (iv) al propoziţiei 32 este: Dacă $xy = yx$, rezultă că

$$\text{ord}_G(xy) = [\text{ord}_G x, \text{ord}_G y].$$

Este ea adevărată?

4. Aplicaţii

Definiţia 33. Funcţia $\varphi : \mathbb{N}^* \to \mathbb{N}^*$, $\varphi(n)$ = numărul numerelor naturale ce nu-l întrec pe n şi sunt prime cu n, se numeşte **indicatorul lui Euler**.

Observaţia 34. $|U(\mathbb{Z}_n)| = \varphi(n)$.

Propoziţia 35. Dacă $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, unde $p_1, p_2, \dots, p_r$ sunt numere prime distincte două câte două, atunci

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$$

.

Teoremă (Euler). Pentru orice $n \in \mathbb{N}^*$ şi orice $a \in \mathbb{Z}$ prim cu n avem $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Demonstraţie: a fiind prim cu n, $\widehat{a}$ este element al grupului $U(\mathbb{Z}_n)$. Aplicând corolarul 29, $\widehat{a}^{\varphi(n)} = \widehat{1}$ în acest grup, de unde concluzia. □

Teoremă (Fermat). Pentru orice număr prim $p \in \mathbb{N}$ şi orice $a \in \mathbb{Z}$ prim cu p avem $a^{p-1} \equiv 1 \pmod{p}$.

Demonstraţie: Întrucât pentru orice număr prim p avem $\varphi(p) = p - 1$, obţinem concluzia aplicând teorema lui Euler. □

Propoziţia 36. Fie $m, n \in \mathbb{N}$. Grupurile $\mathbb{Z}_m \times \mathbb{Z}_n$ şi $\mathbb{Z}_{mn}$ sunt izomorfe dacă şi numai dacă m şi n sunt prime între ele.

Demonstraţie: „⇒": Corespondentul $(\widehat{a}, \overline{b})$ al lui $\widetilde{1}$ prin izomorfism are ordinul $[\mathrm{ord}_{\mathbb{Z}_m}\widehat{a}, \mathrm{ord}_{\mathbb{Z}_n}\overline{b}]$, dar şi mn. Deci, $mn = [\mathrm{ord}_{\mathbb{Z}_m}\widehat{a}, \mathrm{ord}_{\mathbb{Z}_n}\overline{b}]|[m, n]$; cum $mn = [m, n] \cdot (m, n)$, obţinem $(m, n) = 1$.
„⇐": Este imediat că funcţia $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $f(\widetilde{a}) = (\widehat{a}, \overline{a})$ este (corect definită şi) morfism injectiv de grupuri. Cum atât domeniul cât şi codomeniul său au mn elemente, ea este şi surjectivă. Prin urmare, f este izomorfism de grupuri. □

Grupuri cu număr „mic" de elemente.

Definiţia 37. Prin **tipul de izomorfism** al grupului G înţelegem clasa de echivalenţă a lui G în raport cu relaţia de izomorfism. Uneori, ne vom referi la tipul de izomorfism al lui G spunând, pe scurt, **tipul lui G**.

Observaţia 38. Orice grup cu număr prim de elemente este ciclic.

Demonstraţie: Considerăm un grup G cu un număr prim p de elemente şi $x \in G \setminus \{e\}$. Atunci, $|\langle x\rangle| > 1$ şi $|\langle x\rangle|$ divide $|G| = p$, deci $|\langle x\rangle| = p = |G|$, de unde $G = \langle x\rangle$. $\square$

Corolarul 39. Dacă $p \in \mathbb{N}$ este număr prim, atunci singurul tip de grupuri cu p elemente este $\mathbb{Z}_p$.

Corolarul 40. Există un singur tip de grupuri cu două elemente, şi anume $\mathbb{Z}_2$.

Corolarul 41. Există un singur tip de grupuri cu trei elemente, şi anume $\mathbb{Z}_3$.

Pentru viitoarele consideraţii avem nevoie de următorul instrument:

Propoziţia 42. Fie G un grup cu proprietatea că orice element al său are ordin 1 sau 2. Atunci:
(i) G este comutativ.
(ii) Există $n \in \mathbb{N}^*$ astfel încât $|G| = 2^n$.
(iii) Există $n \in \mathbb{N}^*$ astfel încât $G \simeq \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{n \text{ factori}}$.

Problemă suplimentară: Demonstraţi propoziţia 42!

Grupuri cu patru elemente. Fie G un grup cu patru elemente. Elementele lui G nu pot avea decât ordin 1, 2 sau 4.
Dacă G are elemente de ordin 4, atunci G este ciclic, deci, conform teoremei de structură a grupurilor ciclice, $G \simeq \mathbb{Z}_4$.
Dacă G nu are elemente de ordin 4, atunci suntem în situaţia

$$\forall x \in G \setminus \{e\} \quad \operatorname{ord} x = 2.$$

În aceste condiţii obţinem, aplicând propoziţia 42, că $|G| \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Am obţinut deci:

Propoziţia 43. Există exact două tipuri de grupuri cu patru elemente: $\mathbb{Z}_4$ şi grupul lui Klein.

Grupuri cu şase elemente. Fie G un grup cu şase elemente. Elementele lui G nu pot avea decât ordin 1, 2, 3 sau 6.
Dacă G are elemente de ordin 6, atunci G este ciclic, deci, conform teoremei de structură a grupurilor ciclice, $G \simeq \mathbb{Z}_6$.
Dacă G nu are elemente de ordin 6, să presupunem că pentru orice $x \in G\setminus\{e\}$ avem ord $x = 2$. În aceste condiţii obţinem, aplicând propoziţia 42, că $|G|$ este putere de doi, ceea ce reprezintă o contradicţie.
Prin urmare, G admite elemente de ordin 3; fie x un astfel de element şi $y \in G \setminus \{e, x, x^2\}$. Se arată uşor că $G = \{e, x, x^2, y, xy, x^2y\}$ şi, eliminând celelalte posibilităţi, că $y^2 = e$. Dacă $yx = xy$ obţinem

imediat faptul că $\text{ord}_G(xy) = 6$, contradicţie. Eliminând celelalte posibilităţi (de pildă, $yx = e$ ar duce la contradicţia $y = x^2$, ş. a. m. d.), constatăm că $yx = x^2y$. Prin urmare, $G \simeq D_3 \simeq S_3$.
Am obţinut aşadar:

Propoziţia 44. Există exact două tipuri de grupuri cu şase elemente: $\mathbb{Z}_6$ şi S_3.

Temă: Determinaţi tipurile de grupuri cu şapte, respectiv cu opt elemente!

Bibliografie

[1] T. Dumitrescu, *Algebra*, Ed. Universităţii din Bucureşti, 2006.
[2] I. D. Ion, N. Radu, *Algebra*, Ed. Universităţii din Bucureşti, 1981.
[3] C. Năstăsescu, C. Niţă, C. Vraciu, *Bazele algebrei*, Ed. Academiei, Bucureşti, 1986.