

## CURSUL 8: GRUPURI

G. MINCU

### 1. SUBGRUPUL GENERAT DE O SUBMULTIME

- **Definiția 1.** Fie  $G$  un grup și  $M \subset G$ . Prin **subgrupul lui  $G$  generat de  $M$**  înțelegem cel mai mic (în sensul incluziunii) subgrup al lui  $G$  care conține submulțimea  $M$ .

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

**Propoziția 2.** Fie  $G$  un grup și  $M \subset G$ . Are loc relația

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

- **Propoziția 3.** Fie  $G$  un grup și  $M \subset G$ . Are loc relația

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

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

**Observația 5.**  $\langle \emptyset \rangle = \{e\}$ .

- **Definiția 6.** Fie  $G$  un grup. Submulțimea  $M$  a lui  $G$  se numește **sistem de generatori** al lui  $G$  dacă  $\langle M \rangle = G$ .

**Definiția 7.** Grupul  $G$  se numește **finit generat** dacă el admite un sistem finit de generatori.

**Exemplul 8.** Orice grup admite ca sistem de generatori mulțimea 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:** Demonstrați afirmațiile de la exemplele 8-15!

## 2. GRUPURI CICLICE

- **Definiția 16.** Grupul  $G$  se numește **ciclic** dacă el admite un sistem de generatori format dintr-un singur element.
- **Observația 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  $\mathbb{Z}_n = \langle \hat{1} \rangle$ .

**Observația 20.** Generatorul unui grup ciclic nu este unic determinat. De exemplu, avem și  $\mathbb{Z} = \langle -1 \rangle$ , iar  $\mathbb{Z}_n = \langle \hat{a} \rangle$  dacă și 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  $\mathbb{Z}$ .
- *Demonstrație:* Fie  $G$  un grup ciclic și  $g$  un generator al acestuia. Considerăm  $u : \mathbb{Z} \rightarrow G$ ,  $u(n) = g^n$ . 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, obținem  $G = \text{Im } u \simeq \frac{\mathbb{Z}}{\ker u}$ . 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

**Observația 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.

- **Definiția 27.** Prin **ordinul** elementului  $x$  al grupului  $G$  înțelegem ordinul subgrupului generat de  $x$  în  $G$ .

**Vom nota** ordinul elementului  $x$  al grupului  $G$  cu  $\text{ord}_G x$ . Dacă grupul  $G$  este subînțeles în context, atunci vom folosi și notația  $\text{ord } x$ .

**Caracterizări ale ordinului.**

- **Propoziția 28.** Fie  $G$  un grup și  $x \in G$ . 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  $x^{\text{ord } x} = e$ .

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

**Proprietăți ale ordinului.**

- **Propoziția 31.** Ordinul oricărui element al unui grup finit divide ordinul respectivului grup.

*Demonstrație:* Ordinul unui element, fiind ordinul unui subgrup, divide, conform teoremei lui Lagrange, ordinul grupului.  $\square$

- **Propoziția 32.** Dacă  $G$ ,  $G_1$  și  $G_2$  sunt grupuri finite, atunci:

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

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

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

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

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

**Temă:** Rămâne adevărată afirmația de la punctul (iv) al propoziției 32 în lipsa condiției  $xy = yx$ ?

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

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

Este ea adevărată?

## 4. APLICAȚII

- **Definiția 33.** Funcția  $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$ ,  $\varphi(n)$  = numărul numerelor naturale ce nu-l întrec pe  $n$  și sunt prime cu  $n$ , se numește **indicatorul lui Euler**.

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

- **Propoziția 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

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

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

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

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

- *Demonstrație:* Întrucât pentru orice număr prim  $p$  avem  $\varphi(p) = p - 1$ , obținem concluzia aplicând teorema lui Euler.  $\square$

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

*Demonstrație:* „ $\Rightarrow$ ”: Corespondentul  $(\hat{a}, \bar{b})$  al lui  $\tilde{1}$  prin izomorfism are ordinul  $[\text{ord}_{\mathbb{Z}_m} \hat{a}, \text{ord}_{\mathbb{Z}_n} \bar{b}]$ , dar și  $mn$ . Deci,  $mn = [\text{ord}_{\mathbb{Z}_m} \hat{a}, \text{ord}_{\mathbb{Z}_n} \bar{b}] [m, n]$ ; cum  $mn = [m, n] \cdot (m, n)$ , obținem  $(m, n) = 1$ .

„ $\Leftarrow$ ”: Este imediat că funcția  $f : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ ,  $f(\tilde{a}) = (\hat{a}, \bar{a})$  este (corect definită și) morfism injectiv de grupuri. Cum atât domeniul cât și codomeniul său au  $mn$  elemente, ea este și surjectivă. Prin urmare,  $f$  este izomorfism de grupuri.  $\square$

### Grupuri cu număr „mic” de elemente.

**Definiția 37.** Prin **tipul de izomorfism** al grupului  $G$  înțelegem clasa de echivalență a lui  $G$  în raport cu relația de izomorfism. Uneori, ne vom referi la tipul de izomorfism al lui  $G$  spunând, pe scurt, **tipul lui  $G$** .

**Observația 38.** Orice grup cu număr prim de elemente este ciclic.

*Demonstrație:* Considerăm un grup  $G$  cu un număr prim  $p$  de elemente și  $x \in G \setminus \{e\}$ . Atunci,  $|\langle x \rangle| > 1$  și  $|\langle x \rangle|$  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, și anume  $\mathbb{Z}_2$ .
- **Corolarul 41.** Există un singur tip de grupuri cu trei elemente, și anume  $\mathbb{Z}_3$ .

Pentru viitoarele considerații avem nevoie de următorul instrument:

**Propoziția 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  $G \simeq \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2}_{n \text{ factori}}$ .

**Problemă suplimentară:** Demonstrați propoziția 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 situația

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

În aceste condiții obținem, aplicând propoziția 42, că  $|G| \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ . Am obținut deci:

- **Propoziția 43.** Există exact două tipuri de grupuri cu patru elemente:  $\mathbb{Z}_4$  și grupul lui Klein.
- *Grupuri cu șase elemente.* Fie  $G$  un grup cu șase 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  $\text{ord } x = 2$ . În aceste condiții obținem, aplicând propoziția 42, că  $|G|$  este putere de doi, ceea ce reprezintă o contradicție. Prin urmare,  $G$  admite elemente de ordin 3; fie  $x$  un astfel de element și  $y \in G \setminus \{e, x, x^2\}$ . Se arată ușor că  $G = \{e, x, x^2, y, xy, x^2y\}$  și, eliminând celelalte posibilități, că  $y^2 = e$ . Dacă  $yx = xy$  obținem

imediat faptul că  $\text{ord}_G(xy) = 6$ , contradicție. Eliminând celelalte posibilități (de pildă,  $yx = e$  ar duce la contradicția  $y = x^2$ , ș. a. m. d.), constatăm că  $yx = x^2y$ . Prin urmare,  $G \simeq D_3 \simeq S_3$ .

Am obținut așadar:

- **Propoziția 44.** Există exact două tipuri de grupuri cu șase elemente:  $\mathbb{Z}_6$  și  $S_3$ .

**Temă:** Determinați tipurile de grupuri cu șapte, respectiv cu opt elemente!

#### BIBLIOGRAFIE

- [1] T. Dumitrescu, *Algebra*, Ed. Universității din București, 2006.
- [2] I. D. Ion, N. Radu, *Algebra*, Ed. Universității din București, 1981.
- [3] C. Năstăsescu, C. Niță, C. Vraciu, *Bazele algebrei*, Ed. Academiei, București, 1986.