

CURSUL 6: GRUPURI

G. MINCU

1. GRUPURI

- **Definiția 1.** Fie G o mulțime nevidă și „ \cdot ” o lege de compoziție pe G . Perechea (G, \cdot) se numește **grup** dacă:
A: „ \cdot ” este asociativă
EN: „ \cdot ” admite element neutru
TES: Toate elementele lui G sunt simetrizabile în raport cu „ \cdot ”.
Dacă în plus „ \cdot ” este și comutativă, grupul (G, \cdot) se numește **comutativ** sau **abelian**.

Observația 2. Dacă legea de compoziție „ \cdot ” este subînțeleasă în context, vom spune frecvent „grupul G ” în loc de „grupul (G, \cdot) ”. De asemenea, în loc de „ (G, \cdot) este grup” vom spune frecvent „ G are o structură de grup în raport cu „ \cdot ” ”.

Observația 3. Când ne vom referi la grupuri neprecizate vom folosi notația multiplicativă, pentru elementul neutru vom folosi notația e , iar simetricul unui element x va fi desemnat prin x' . Dacă există însă o notație consacrată în context, vom face apel la aceasta.

2. EXEMPLE DE GRUPURI

- **Exemplul 4.** $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ și $(\mathbb{C}, +)$ sunt grupuri abeliene.
- **Exemplul 5.** Monoizii comutativi (\mathbb{N}, \cdot) , (\mathbb{Z}, \cdot) , (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) și (\mathbb{C}, \cdot) nu sunt grupuri, deoarece elementul 0 nu este simetrizabil în niciunul dintre aceștia.
- **Observația 6.** Datorită faptelor evidențiate în exemplele 4 și 5, ne vom permite uneori să facem referire la „grupul \mathbb{Z} ”, „grupul \mathbb{Q} ”, „grupul \mathbb{R} ” sau „grupul \mathbb{C} ” subînțelegând considerarea pe acestea a structurii aditive. Dacă dorim să ne referim la o altă structură de grup pe aceste mulțimi, trebuie să o precizăm explicit.
- **Exemplul 7.** $(\mathcal{M}_{m,n}(\mathbb{C}), +)$ este grup abelian.
- **Exemplul 8.** \mathbb{Z}_n este grup abelian în raport cu adunarea modulo n .

- **Exemplul 9.** \mathbb{Z}_n este, conform cursului 4, monoid comutativ în raport cu înmulțirea modulo n . Acest monoid nu este grup, întrucât elementul $\hat{0}$ nu este simetrizabil.

Observația 10. Având în vedere exemplele 8 și 9, ne vom permite uneori să facem referire la „grupul \mathbb{Z}_n ” subînțelegând considerarea pe acesta a structurii aditive. Dacă dorim să ne referim la o altă structură de grup pe \mathbb{Z}_n , trebuie să o precizăm explicit.

- **Exemplul 11.** Dacă G este un grup (abelian) iar A o mulțime nevidă, atunci G^A are o structură de grup (abelian) în raport cu legea de compoziție definită la exemplul 6 din cursul 4.
- **Exemplul 12.** Fie $(G_i)_{i \in I}$ este o familie de grupuri (în notație multiplicativă). Pe $G \stackrel{\text{def}}{=} \prod_{i \in I} G_i$ introducem legea de compoziție

$$(a_i)_i \cdot (b_i)_i = (a_i b_i)_i.$$

Propoziția 13. Mulțimea G din exemplul 12 are în raport cu operația introdusă acolo o structură de grup. Acest grup este abelian dacă și numai dacă toate grupurile G_i sunt abeliene.

Temă: Demonstrați afirmațiile de la exemplele 5, 7, 8, 9, 11 și propoziția 13!

Definiția 14. Grupul de la exemplul 12 se numește **produsul direct** al familiei de grupuri $(G_i)_{i \in I}$.

Vom folosi frecvent pentru produsul direct al unei familii de grupuri $(G_i)_{i \in I}$ indexate după mulțimea finită $I = \{i_1, i_2, \dots, i_n\}$ **notațiile** $\prod_{k=1}^n G_{i_k}$ sau $G_{i_1} \times G_{i_2} \times \dots \times G_{i_n}$.

Definiția 15. Grupul $\mathbb{Z}_2 \times \mathbb{Z}_2$ se numește **grupul lui Klein**.

3. GRUPUL ELEMENTELOR SIMETRIZABILE DINTR-UN MONOID

Fie (M, \cdot) un monoid. **Notăm** cu $U(M)$ mulțimea elementelor simetrizabile ale lui M .

Propoziția 16. a) $U(M)$ este parte stabilă a lui M în raport cu „ \cdot ”.
b) $U(M)$ are o structură de grup în raport cu operația indusă de „ \cdot ”.

Demonstrație: a) Fie $x, y \in U(M)$. Atunci $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = e$ și $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = e$, deci $y^{-1}x^{-1} = (xy)^{-1}$, de unde $xy \in U(M)$.

b) Evident. \square

Corolarul 17. Dacă x și y sunt elemente simetrizabile ale unui monoid (M, \cdot) , atunci $(xy)^{-1} = y^{-1}x^{-1}$.

Aceste considerații ne permit să dăm o nouă serie de exemple de grupuri:

- **Exemplul 18.** (\mathbb{Q}^*, \cdot) , (\mathbb{R}^*, \cdot) și (\mathbb{C}^*, \cdot) sunt grupuri abeliene.
- **Exemplul 19.** $(\{-1, 1\}, \cdot)$ este grup abelian.
- **Exemplul 20.** $(U(\mathbb{Z}_n), \cdot)$ este grup abelian.

Vom folosi notația $U(\mathbb{Z}_n)$ pentru a desemna grupul elementelor din \mathbb{Z}_n simetrizabile în raport cu înmulțirea modulo n .

Propoziția 21. $U(\mathbb{Z}_n) = \{\hat{a} \in \mathbb{Z}_n : (a, n) = 1\}$.

Temă: Demonstrați propoziția 21!

Observația 22. Fie A o mulțime nevidă. Elementele simetrizabile ale monoidului (A^A, \circ) sunt exact funcțiile bijective.

Vom folosi notația $S(A) \stackrel{\text{not}}{=} \{f \in A^A : f \text{ este bijectivă}\}$.

- **Exemplul 23.** $(S(A), \circ)$ este grup.

Observația 24. Vom face frecvent referire la $S(\{1, 2, \dots, n\})$; pentru acest grup vom folosi notația S_n .

Observația 25. Elementele simetrizabile ale monoidului $(\mathcal{M}_n(\mathbb{C}), \cdot)$ sunt exact matricile inversabile.

Vom folosi notația $GL_n(\mathbb{C}) \stackrel{\text{not}}{=} \{A \in \mathcal{M}_n(\mathbb{C}) : A \text{ este inversabilă}\}$.

- **Exemplul 26.** $(GL_n(\mathbb{C}), \cdot)$ este grup.

4. REGULI DE CALCUL ÎN GRUPURI

Fie (G, \cdot) un grup, $x \in G$ și $n \in \mathbb{N}^*$. Vom nota cu x^{-n} elementul $(x^n)'$.

Propoziția 27. Fie (G, \cdot) un grup, $x, y \in G$ și $m, n \in \mathbb{Z}$. Atunci:

- a) $x^{m+n} = x^m \cdot x^n$.
- b) $(x^m)^n = x^{mn}$.
- c) Dacă x și y comută, atunci $(xy)^m = x^m y^m$.

Demonstrație: Se procedează ca în demonstrația propoziției similare din cursul 4, analizând suplimentar cazurile în care m sau n sunt negative. Lăsăm detaliile în grija cititorului. \square

Observația 28. Dacă operația grupului G este notată aditiv, atunci relațiile din propoziția 27 devin:

- a) $(m+n)x = mx + nx$.
- b) $n(mx) = (nm)x$.
- c) Dacă x și y comută, atunci $m(x+y) = mx + my$.

5. SUBGRUPURI

- **Definiția 29.** Fie G un grup și H o submulțime nevidă a sa. Spunem că H este **subgrup** al lui G dacă:

- i) $\forall x, y \in H \quad xy \in H.$
- ii) $\forall x \in H \quad x' \in H.$

Observația 30. Dacă H este subgrup al lui G , atunci H conține elementul neutru al lui G .

Observația 31. Dacă H este subgrup al lui G , atunci H este grup în raport cu operația indusă.

Vom folosi notația $H \leq G$ pentru a desemna faptul că H este subgrup al lui G .

Propoziția 32. Fie G un grup și H o submulțime nevidă a lui G . Următoarele afirmații sunt echivalente:

- i) $H \leq G$
- ii) $\forall x, y \in H \quad xy' \in H.$

- **Exemplul 33.** G și $\{e\}$ sunt subgrupuri ale lui G (ele se numesc **subgrupul impropriu**, respectiv **subgrupul trivial** al lui G).

- **Exemplul 34.** $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +).$

- **Propoziția 35.** Fie H o submulțime nevidă a lui \mathbb{Z} . H este subgrup al lui \mathbb{Z} dacă și numai dacă există $n \in \mathbb{N}$ astfel încât $H = n\mathbb{Z}$.

Demonstrație: „ \Leftarrow ”: Se aplică propoziția 32.

„ \Rightarrow ”: Dacă $H = \{0\}$, alegem $n = 0$.

Dacă $H \neq \{0\}$, există $a \in H \setminus \{0\}$. Atunci $|a| \in H \cap \mathbb{N}^*$. Deci $H \cap \mathbb{N}^* \neq \emptyset$. Atunci $H \cap \mathbb{N}^*$ are un cel mai mic element; notăm acest element cu n . Cum $H \leq \mathbb{Z}$, este imediat că $n\mathbb{Z} \subset H$. Fie acum $x \in H$. Conform teoremei de împărțire cu rest, există $q, r \in \mathbb{Z}$, $0 \leq r < n$, așa încât $x = nq + r$. De aici se obține $r = x - nq \in H$, de unde, conform definiției lui n , $r = 0$. Prin urmare, $x = nq \in n\mathbb{Z}$, deci $H \subset n\mathbb{Z}$. \square

6. MORFISME DE GRUPURI

- **Definiția 36.** Fie G și Γ două grupuri (în notație multiplicativă). O funcție $f : G \rightarrow \Gamma$ se numește **morfism de grupuri** dacă:
 $\forall x, y \in G \quad f(xy) = f(x)f(y).$

Vom nota cu $\text{Hom}_{\text{Grp}}(G, \Gamma)$ mulțimea morfismelor de grupuri de la G la Γ . În cazul în care este subînțeles faptul că ne referim la structuri de grup vom scrie, pe scurt, $\text{Hom}(G, \Gamma)$.

- **Propoziția 37.** Fie $f : G \rightarrow \Gamma$ un morfism de grupuri. Atunci:

- a) $f(e_G) = e_\Gamma$.
- b) $\forall x \in G \quad f(x') = f(x)'$.
- c) $\forall x \in G \quad \forall n \in \mathbb{Z} \quad f(x^n) = f(x)^n$.

Temă: Demonstrați propoziția 37!

- **Exemplul 38.** Pentru orice grup G , funcția identică a lui G este morfism de grupuri.
- **Exemplul 39.** Pentru orice două grupuri G și Γ , funcția $u : G \rightarrow \Gamma$, $u(x) = e_\Gamma$ este morfism de grupuri.
- **Exemplul 40.** Dacă $H \leq G$, funcția $j : H \rightarrow G$, $j(x) = x$ este morfism de grupuri.

Temă: Demonstrați afirmațiile de la exemplele 38, 39 și 40!

Definiția 41. Morfismul din exemplul 40 se numește **injecția canonică a lui H în G** .

Propoziția 42. Dacă $f : G \rightarrow \Gamma$ și $g : \Gamma \rightarrow \Delta$ sunt morfisme de grupuri, atunci $g \circ f$ este morfism de grupuri.

Temă: Demonstrați propoziția 37!

Definiția 43. Fie G și Γ două grupuri. Un morfism de grupuri $f : G \rightarrow \Gamma$ se numește **izomorfism** dacă există un morfism de grupuri $g : \Gamma \rightarrow G$ cu proprietatea că $f \circ g = \text{id}_\Gamma$ și $g \circ f = \text{id}_G$.

Exemplul 44. Pentru orice grup G , funcția identică a lui G este izomorfism de grupuri.

Exemplul 45. Pentru orice izomorfism f de grupuri, f^{-1} este izomorfism de grupuri.

Propoziția 46. $f : G \rightarrow \Gamma$ este izomorfism de grupuri dacă și numai dacă f este morfism bijectiv de grupuri.

Demonstrație: „ \Rightarrow ”: Evident.

„ \Leftarrow ”: Fie $z, t \in \Gamma$. Punem $x = f^{-1}(z)$ și $y = f^{-1}(t)$. Atunci $f^{-1}(zt) = f^{-1}(f(x)f(y)) = f^{-1}(f(xy)) = xy = f^{-1}(z)f^{-1}(t)$. \square

- **Definiția 47.** Un morfism de grupuri $f : G \rightarrow G$ se numește **endomorfism** al lui G .

Vom nota cu $\text{End}_{\text{Grp}}(G)$ mulțimea endomorfismelor de grup ale lui G . În cazul în care este subînțeles faptul că ne referim la structura de grup a lui G vom scrie, pe scurt, $\text{End}(G)$.

Observația 48. $\text{End}_{\text{Grp}}(G) = \text{Hom}_{\text{Grp}}(G, G)$.

● **Definiția 49.** Un izomorfism de grupuri $f : G \rightarrow G$ se numește **automorfism** al lui G .

Vom nota cu $\text{Aut}_{\text{Grp}}(G)$ mulțimea automorfismelor de grup ale lui G . În cazul în care este subînțeles faptul că ne referim la structura de grup a lui G vom scrie, pe scurt, $\text{Aut}(G)$.

7. MORFISME ȘI SUBGRUPURI

Propoziția 50. Fie $f : G \rightarrow \Gamma$ un morfism de grupuri, $H \leq G$ și $K \leq \Gamma$. Atunci:

- a) $f(H) \leq K$.
- b) $f^{-1}(K) \leq G$

Demonstrație: a) Fie $y_1, y_2 \in f(H)$. Atunci există $x_1, x_2 \in H$ astfel încât $y_1 = f(x_1)$ și $y_2 = f(x_2)$. Deducem că $y_1 y_2' = f(x_1) f(x_2)' = f(x_1 x_2') \in f(H)$.

b) Fie $x_1, x_2 \in f^{-1}(K)$. Atunci $f(x_1 x_2') = f(x_1) f(x_2)' \in K$, deci $x_1 x_2' \in f^{-1}(K)$. \square

Nucleul și imaginea unui morfism de grupuri. Considerațiile din acest paragraf se referă la un morfism de grupuri $f : G \rightarrow \Gamma$.

Definiția 51. Mulțimea $\{x \in G : f(x) = e_\Gamma\}$ se numește **nucleul** lui f și se notează $\ker f$.

Observația 52. Deoarece $\ker f = f^{-1}(e_\Gamma)$, din propoziția 50 deducem că $\ker f \leq G$.

Propoziția 53. Morfismul de grupuri $f : G \rightarrow \Gamma$ este injectiv dacă și numai dacă $\ker f = \{e_\Gamma\}$.

Demonstrație: „ \Rightarrow ”: Dacă $x \in \ker f$, $f(x) = e_\Gamma = f(e_G)$; din injectivitatea lui f deducem că $x = e_G$.

„ \Leftarrow ”: Fie $x_1, x_2 \in G$ astfel ca $f(x_1) = f(x_2)$. Atunci $f(x_1 x_2') = e_\Gamma$, de unde $x_1 x_2' \in \ker f$. Rezultă că $x_1 x_2' = e_G$, deci $x_1 = x_2$. \square

Observația 54. Conform propoziției 50, $\text{Im} f \leq \Gamma$.

Propoziția 55. Morfismul de grupuri $f : G \rightarrow \Gamma$ este surjectiv dacă și numai dacă $\text{Im} f = \Gamma$.

Teorema 56. Fie $f : G \rightarrow \Gamma$ un morfism de grupuri. Notăm $\mathcal{H} = \{H \leq G : H \supset \ker f\}$ și $\mathcal{K} = \{K : K \leq \Gamma\}$. Atunci funcțiile $\Phi : \mathcal{H} \rightarrow \mathcal{K}$, $\Phi(H) = f(H)$ și $\Psi : \mathcal{K} \rightarrow \mathcal{H}$, $\Psi(K) = f^{-1}(K)$ sunt (bijective și) inverse una celeilalte și păstrează incluziunile.

Propoziția 57. Fie $n \in \mathbb{N}^*$ și H o submulțime a lui \mathbb{Z}_n . Atunci $H \leq \mathbb{Z}_n$ dacă și numai dacă există $d \in \mathbb{N}$ astfel încât $d|n$ și $H = \widehat{d}\mathbb{Z}_n$.

BIBLIOGRAFIE

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