CURSUL 8: GRUPURI

G. MINCU

1. Grupuri

Definiţia 1. Fie G o mulţime nevidă şi „$\cdot$” o lege de compoziţie pe G. Perechea $(G, \cdot)$ se numeşte **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 şi comutativă, grupul $(G, \cdot)$ se numeşte **comutativ** sau **abelian**.

Observaţia 2. Dacă legea de compoziţie „$\cdot$” este subînţeleasă 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 „$\cdot$” ”.

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

2. Exemple de grupuri

Exemplul 4. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ şi $(\mathbb{C}, +)$ sunt grupuri abeliene.

Exemplul 5. Monoizii comutativi $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ şi $(\mathbb{C}, \cdot)$ nu sunt grupuri, deoarece elementul 0 nu este simetrizabil în niciunul dintre aceştia.

Observaţia 6. Datorită faptelor evidenţiate în exemplele 4 şi 5, ne vom permite uneori să facem referire la „grupul $\mathbb{Z}$”, „grupul $\mathbb{Q}$”, „grupul $\mathbb{R}$” sau „grupul $\mathbb{C}$” subînţelegând considerarea pe acestea a structurii aditive. Dacă dorim să ne referim la o altă structură de grup pe aceste mulţimi, 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 înmulţirea modulo n. Acest monoid nu este grup, întrucât elementul $\widehat{0}$ nu este simetrizabil.

Observaţia 10. Având în vedere exemplele 8 şi 9, ne vom permite uneori să facem referire la „grupul $\mathbb{Z}_n$" subînţelegând 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 mulţime nevidă, atunci G^A are o structură de grup (abelian) în raport cu legea de compoziţie definită la exemplul 6 din cursul 4.

Exemplul 12. Fie $(G_i)_{i\in I}$ este o familie de grupuri (în notaţie multiplicativă). Pe $G \overset{\text{def}}{=} \prod\limits_{i\in I} G_i$ introducem legea de compoziţie

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

Propoziţia 13. Mulţimea G din exemplul 12 are în raport cu operaţia introdusă acolo o structură de grup. Acest grup este abelian dacă şi numai dacă toate grupurile G_i sunt abeliene.

Temă: Demonstraţi afirmaţiile de la exemplele 5, 7, 8, 9, 11 şi propoziţia 13!

Definiţia 14. Grupul de la exemplul 12 se numeşte **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 mulţimea finită $I = \{i_1, i_2, \dots, i_n\}$ **notaţiile** $\prod\limits_{k=1}^{n} G_{i_k}$ sau $G_{i_1} \times G_{i_2} \times \dots \times G_{i_n}$.

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

3. Grupul elementelor simetrizabile dintr-un monoid

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

Propoziţia 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 operaţia indusă de „$\cdot$".

Demonstraţie: a) Fie $x, y \in U(M)$. Atunci $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = e$ şi $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = e$, deci $y^{-1}x^{-1} = (xy)^{-1}$, de unde $xy \in U(M)$.
b) Evident. $\square$

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

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

Exemplul 18. $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$ şi $(\mathbb{C}^*,\cdot)$ sunt grupuri abeliene.

Exemplul 19. $(\{-1,1\},\cdot)$ este grup abelian.

Exemplul 20. $(U(\mathbb{Z}_n),\cdot)$ este grup abelian.

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

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

Temă: Demonstraţi propoziţia 21!

Observaţia 22. Fie A o mulţime nevidă. Elementele simetrizabile ale monoidului $(A^A,\circ)$ sunt exact funcţiile bijective.

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

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

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

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

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

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

4. Reguli de calcul în grupuri

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

Propoziţia 27. Fie $(G,\cdot)$ un grup, $x,y \in G$ şi $m,n \in \mathbb{Z}$. Atunci:
a) $x^{m+n} = x^m \cdot x^n$.
b) $(x^m)^n = x^{mn}$.
c) Dacă x şi y comută, atunci $(xy)^m = x^m y^m$.

Demonstraţie: Se procedează ca în demonstraţia propoziţiei similare din cursul 4, analizând suplimentar cazurile în care m sau n sunt negative. Lăsăm detaliile în grija cititorului. $\square$

Observaţia 28. Dacă operaţia grupului G este notată aditiv, atunci relaţiile din propoziţia 27 devin:
a) $(m+n)x = mx + nx$.
b) $n(mx) = (nm)x$.
c) Dacă x şi y comută, atunci $m(x+y) = mx + my$.

5. Subgrupuri

Definiţia 29. Fie G un grup şi H o submulţime nevidă a sa. Spunem că H este **subgrup** al lui G dacă:
i) $\forall x, y \in H \quad xy \in H$.
ii) $\forall x \in H \quad x' \in H$.

Observaţia 30. Dacă H este subgrup al lui G, atunci H conţine elementul neutru al lui G.

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

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

Propoziţia 32. Fie G un grup şi H o submulţime nevidă a lui G. Următoarele afirmaţii sunt echivalente:
i) $H \leq G$
ii) $\forall x, y \in H \quad xy' \in H$.

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

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

Propoziţia 35. Fie H o submulţime nevidă a lui $\mathbb{Z}$. H este subgrup al lui $\mathbb{Z}$ dacă şi numai dacă există $n \in \mathbb{N}$ astfel încât $H = n\mathbb{Z}$.

Demonstraţie: „$\Leftarrow$": Se aplică propoziţia 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 împărţire cu rest, există $q, r \in \mathbb{Z}$, $0 \leq r < n$, aşa încât $x = nq + r$. De aici se obţine $r = x - nq \in H$, de unde, conform definiţiei lui n, $r = 0$. Prin urmare, $x = nq \in n\mathbb{Z}$, deci $H \subset n\mathbb{Z}$. $\square$

6. Morfisme de grupuri

Definiţia 36. Fie G şi Γ două grupuri (în notaţie multiplicativă). O funcţie $f : G \to \Gamma$ se numeşte **morfism de grupuri** dacă:
$\forall x, y \in G \quad f(xy) = f(x)f(y)$.

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

Propoziţia 37. Fie $f : G \to \Gamma$ un morfism de grupuri. Atunci:
a) $f(e_G) = e_\Gamma$.
b) $\forall x \in G \ \ f(x') = f(x)'$.
c) $\forall x \in G \ \forall n \in \mathbb{Z} \quad f(x^n) = f(x)^n$.

Temă: Demonstraţi propoziţia 37!

Exemplul 38. Pentru orice grup G, funcţia identică a lui G este morfism de grupuri.

Exemplul 39. Pentru orice două grupuri G şi Γ, funcţia $u : G \to \Gamma$, $u(x) = e_\Gamma$ este morfism de grupuri.

Exemplul 40. Dacă $H \leq G$, funcţia $j : H \to G$, $j(x) = x$ este morfism de grupuri.

Temă: Demonstraţi afirmaţiile de la exemplele 38, 39 şi 40!

Definiţia 41. Morfismul din exemplul 40 se numeşte **injecţia canonică a lui** H **în** G.

Propoziţia 42. Dacă $f : G \to \Gamma$ şi $g : \Gamma \to \Delta$ sunt morfisme de grupuri, atunci $g \circ f$ este morfism de grupuri.

Temă: Demonstraţi propoziţia 37!

Definiţia 43. Fie G şi Γ două grupuri. Un morfism de grupuri $f : G \to \Gamma$ se numeşte **izomorfism** dacă există un morfism de grupuri $g : \Gamma \to G$ cu proprietatea că $f \circ g = \mathrm{id}_\Gamma$ şi $g \circ f = \mathrm{id}_G$.

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

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

Propoziţia 46. $f : G \to \Gamma$ este izomorfism de grupuri dacă şi numai dacă f este morfism bijectiv de grupuri.

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

Definiţia 47. Un morfism de grupuri $f : G \to G$ se numeşte **endomorfism** al lui G.

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

Observaţia 48. $\mathrm{End}_{\mathrm{Grp}}(G) = \mathrm{Hom}_{\mathrm{Grp}}(G, G)$.

Definiţia 49. Un izomorfism de grupuri $f : G \to G$ se numeşte **automorfism** al lui G.

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

7. Morfisme şi subgrupuri

Propoziţia 50. Fie $f : G \to \Gamma$ un morfism de grupuri, $H \leq G$ şi $K \leq \Gamma$. Atunci:
a) $f(H) \leq \Gamma$.
b) $f^{-1}(K) \leq G$.

Demonstraţie: a) Fie $y_1, y_2 \in f(H)$. Atunci, există $x_1, x_2 \in H$ astfel încât $y_1 = f(x_1)$ şi $y_2 = f(x_2)$. 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 şi imaginea unui morfism. Consideraţiile din acest paragraf se referă la un morfism de grupuri $f : G \to \Gamma$.

Definiţia 51. Mulţimea $\{x \in G : f(x) = e_\Gamma\}$ se numeşte **nucleul** lui f şi se notează $\ker f$.

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

Propoziţia 53. Morfismul f este injectiv dacă şi numai dacă $\ker f = \{e_G\}$.

Demonstraţie: „$\Rightarrow$": 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 $x_1 = x_2$. $\square$

Observaţia 54. Conform propoziţiei 50, $\mathrm{Im} f \leq \Gamma$.

Propoziţia 55. Morfismul f este surjectiv dacă şi numai dacă $\mathrm{Im} f = \Gamma$.

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

Propoziţia 57. Fie H o submulţime nevidă a lui $\mathbb{Z}_n$. Atunci $H \leq \mathbb{Z}_n$ dacă şi numai dacă există $d \in \mathbb{N}$, $d|n$, astfel încât $H = \widehat{d} \cdot \mathbb{Z}_n$.

Bibliografie

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