CURSUL 5: SEMIGRUPURI. MONOIZI. GRUPURI

SAI

1. SEMIGRUPURI

Definiţia 1. Fie S o mulţime nevidă şi $\cdot$ o lege de compoziţie pe S. Perechea $(S, \cdot)$ se numeşte **semigrup** dacă $\cdot$ este asociativă. Dacă în plus $\cdot$ este şi comutativă, semigrupul $(S, \cdot)$ se numeşte **comutativ**.

Observaţia 2. Dacă legea de compoziţie $\cdot$ este subînţeleasă în context, vom spune frecvent „semigrupul S" în loc de „semigrupul $(S, \cdot)$". De asemenea, în loc de „$(S, \cdot)$ este semigrup" vom spune frecvent „S are o structură de semigrup în raport cu $\cdot$".

1.1. Reguli de calcul în semigrupuri.

Propoziţia 3. Fie $(S, \cdot)$ un semigrup, $x, y \in S$ şi $m, n \in \mathbb{N}^*$. 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: Relaţia de la a) reiese din asociativitatea generalizată. Punctul b) se probează prin inducţie după n, iar c), prin inducţie după m. Lăsăm detaliile în grija cititorului. $\square$

1.2. Morfisme de semigrupuri.

Definiţia 4. Fie S şi S' două semigrupuri (în notaţie multiplicativă). O funcţie $f : S \to S'$ se numeşte **morfism de semigrupuri** dacă

$$\forall x, y \in S \quad f(xy) = f(x)f(y).$$

Propoziţia 5. Dacă $f : S \to S'$ şi $g : S' \to S''$ sunt morfisme de semigrupuri, atunci $g \circ f$ este morfism de semigrupuri.

Demonstraţie: Fie $x, y \in S$. Atunci avem: $(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$. $\square$

Definiţia 6. Fie S şi S' două semigrupuri (în notaţie multiplicativă). Un morfism de semigrupuri $f : S \to S'$ se numeşte **izomorfism** dacă există un morfism de semigrupuri $g : S' \to S$ cu proprietatea că

$$f \circ g = \mathrm{id}_{S'} \text{ şi } g \circ f = \mathrm{id}_S.$$

Exemplul 7. Pentru orice semigrup S, funcţia identică a lui S este izomorfism de semigrupuri.

Exemplul 8. Pentru orice izomorfism f de semigrupuri, f^{-1} este izomorfism de semigrupuri.

Propoziţia 9. $f : S \to S'$ este izomorfism de semigrupuri dacă şi numai dacă f este morfism bijectiv de semigrupuri.

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

2. MONOIZI

2.1. **Monoizi.**

Definiţia 10. Fie M o mulţime nevidă şi $\cdot$ o lege de compoziţie pe M. Perechea $(M, \cdot)$ se numeşte **monoid** dacă $\cdot$ este asociativă şi admite element neutru. Dacă în plus $\cdot$ este şi comutativă, monoidul $(M, \cdot)$ se numeşte **comutativ**.

Observaţia 11. Dacă legea de compoziţie $\cdot$ este subînţeleasă în context, vom spune frecvent „monoidul M" în loc de „monoidul $(M, \cdot)$". De asemenea, în loc de „$(M, \cdot)$ este monoid" vom spune frecvent „M are o structură de monoid în raport cu $\cdot$".

2.2. **Reguli de calcul în monoizi.**

Fie $(M, \cdot)$ un monoid şi $x \in M$. **Notăm** $x^0 \stackrel{\text{def}}{=} 1$.

Propoziţia 12. Fie $(M, \cdot)$ un monoid, $x, y \in M$ şi $m, n \in \mathbb{N}$. 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: Pentru $mn \neq 0$ se aplică propoziţia 3, iar pentru $mn = 0$ relaţiile din enunţ sunt imediate. $\square$

2.3. **Morfisme de monoizi.**

Definiţia 13. Fie M şi M' doi monoizi (în notaţie multiplicativă). O funcţie $f : M \to M'$ se numeşte **morfism de monoizi** dacă:
a) $\forall x, y \in M \quad f(xy) = f(x)f(y)$.
b) $f(1_M) = 1_{M'}$ (1_M şi $1_{M'}$ desemnând aici elementele neutre ale celor doi monoizi).

Propoziţia 14. Dacă $f : M \to M'$ şi $g : M' \to M''$ sunt morfisme de monoizi, atunci $g \circ f$ este morfism de monoizi.

Demonstraţie: Fie $x, y \in M$. Atunci avem: $(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$ şi $(g \circ f)(1_M) = g(f(1_M)) = g(1_{M'}) = 1_{M''}$. □

Definiţia 15. Fie M şi M' doi monoizi (în notaţie multiplicativă). Un morfism de monoizi $f : M \to M'$ se numeşte **izomorfism** dacă există un morfism de monoizi $g : M' \to M$ cu proprietatea că $f \circ g = \mathrm{id}_{M'}$ şi $g \circ f = \mathrm{id}_M$.

Exemplul 16. Pentru orice monoid M, funcţia identică a lui M este morfism de monoizi.

Exemplul 17. Pentru orice izomorfism f de monoizi, f^{-1} este izomorfism de monoizi.

Propoziţia 18. $f : M \to M'$ este izomorfism de monoizi dacă şi numai dacă f este morfism bijectiv de monoizi.

Demonstraţie: „⇒": Evident.
„⇐": Fie $x', y' \in M'$. Punem $x = f^{-1}(x')$ şi $y = f^{-1}(y')$. Atunci $f^{-1}(x'y') = f^{-1}(f(x)f(y)) = f^{-1}(f(xy)) = xy = f^{-1}(x')f^{-1}(y')$. Pe de altă parte, $f^{-1}(1_{M'}) = f^{-1}(f(1_M)) = 1_M$. □

2.4. **Monoidul liber generat de o mulţime.** Fie A o mulţime nevidă. Pe mulţimea înşiruirilor finite de elemente ale lui A definim legea de compoziţie $a_1a_2 \ldots a_m \star a'_1a'_2 \ldots a'_t \stackrel{\text{def}}{=} a_1a_2 \ldots a_ma'_1a'_2 \ldots a'_t$.

Definiţia 19. Înşiruirile de k elemente din A se numesc **cuvinte de lungime** k peste A, iar operaţia $\star$ se numeşte **concatenare**.

Este util să considerăm şi un cuvânt peste A ce ,,nu conţine niciun simbol":

Definiţia 20. Dată fiind o mulţime nevidă A, considerăm că există un (unic) cuvânt de lungime zero peste A. El se numeşte **cuvântul vid** peste A.

Vom nota cuvântul vid cu $\lrcorner$.

Propoziţia 21. Mulţimea cuvintelor peste A are în raport cu operaţia de concatenare o structură de monoid, al cărei element neutru este $\lrcorner$.

Temă: Demonstraţi propoziţia 21!

Definiţia 22. Monoidul la care se face referire în propoziţia 21 se numeşte **monoidul liber generat de mulţimea** A.

Notaţia uzuală pentru monoidul liber generat de mulţimea A este $FM(A)$.

Propoziţia 23. Considerăm o mulţime nevidă A, un monoid M şi o funcţie $f : A \to M$. Atunci funcţia $\tilde{f} : FM(A) \to M$, $\tilde{f}(a_1 a_2 \dots a_n) = f(a_1)f(a_2)\dots f(a_n)$, $f(\_) = e$, este un morfism de monoizi.

Temă: Demonstraţi propoziţia 23!

3. Grupuri

Definiţia 24. 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 25. 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 26. 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.

4. Exemple de grupuri

Exemplul 27. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ şi $(\mathbb{C}, +)$ sunt grupuri abeliene.

Exemplul 28. 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 29. Datorită faptelor evidenţiate în exemplele 27 şi 28, 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 30. $(\mathcal{M}_{m,n}(\mathbb{C}), +)$ este grup abelian.

Exemplul 31. $\mathbb{Z}_n$ este grup abelian în raport cu adunarea modulo n.

Exemplul 32. $\mathbb{Z}_n$ 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 33. Având în vedere exemplele 31 şi 32, 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 34. 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 35. Fie $(G_i)_{i\in I}$ este o familie de grupuri (în notaţie multiplicativă). Pe $G \stackrel{\text{def}}{=} \prod_{i\in I} G_i$ introducem legea de compoziţie

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

Propoziţia 36. Mulţimea G din exemplul 35 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 28, 30, 31, 32, 34 şi propoziţia 36!

Definiţia 37. Grupul de la exemplul 35 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 $I = \{i_1, i_2, \ldots, i_n\}$ **notaţiile** $\prod_{k=1}^{n} G_{i_k}$ sau $G_{i_1} \times G_{i_2} \times \ldots \times G_{i_n}$.

Definiţia 38. Grupul $\mathbb{Z}_2 \times \mathbb{Z}_2$ se numeşte **grupul lui Klein**.

5. Grupul elementelor simetrizabile dintr-un monoid

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

Propoziţia 39. 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. □

Corolarul 40. 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 41. $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ şi $(\mathbb{C}^*, \cdot)$ sunt grupuri abeliene.

Exemplul 42. $(\{-1, 1\}, \cdot)$ este grup abelian.

Exemplul 43. $(U(\mathbb{Z}_n), \cdot)$ 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 44. $U(\mathbb{Z}_n) = \{\widehat{a} \in \mathbb{Z}_n : (a, n) = 1\}$.

Temă: Demonstraţi propoziţia 44!

Observaţia 45. 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 46. $(S(A), \circ)$ este grup.

Observaţia 47. Vom face frecvent referire la $S(\{1, 2, \ldots, n\})$; pentru acest grup vom folosi notaţia S_n.

Observaţia 48. 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 49. $(GL_n(\mathbb{C}), \cdot)$ este grup.

6. 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 50. 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. □

Observaţia 51. Dacă operaţia grupului G este notată aditiv, atunci relaţiile din propoziţia 50 devin:
a) $(m + n)x = mx + nx$.
b) $n(mx) = (nm)x$.
c) Dacă x şi y comută, atunci $m(x + y) = mx + my$.

7. SUBGRUPURI

Definiţia 52. 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 53. Dacă H este subgrup al lui G, atunci H conţine elementul neutru al lui G.

Observaţia 54. 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 55. 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 56. G şi $\{e\}$ sunt subgrupuri ale lui G (ele se numesc **subgrupul impropriu**, respectiv **subgrupul trivial** al lui G).

Exemplul 57. $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.

Propoziţia 58. 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 55.
„$\Rightarrow$": 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 $H \subset n\mathbb{Z}$. $\square$

8. MORFISME DE GRUPURI

Definiţia 59. 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 60. 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 60!

Exemplul 61. Pentru orice grup G, funcţia identică a lui G este morfism de grupuri.

Exemplul 62. Pentru orice două grupuri G şi Γ, funcţia $u : G \to \Gamma$, $u(x) = e_{_\Gamma}$ este morfism de grupuri.

Exemplul 63. Dacă $H \leq G$, funcţia $j : H \to G$, $j(x) = x$ este morfism de grupuri.

Temă: Demonstraţi afirmaţiile de la exemplele 61, 62 şi 63!

Definiţia 64. Morfismul din exemplul 63 se numeşte **injecţia canonică a lui H în G**.

Propoziţia 65. 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 60!

Definiţia 66. 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 67. Pentru orice grup G, funcţia identică a lui G este izomorfism de grupuri.

Exemplul 68. Pentru orice izomorfism f de grupuri, f^{-1} este izomorfism de grupuri.

Propoziţia 69. $f : G \to \Gamma$ 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 70. 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 71. $\mathrm{End}_{\mathrm{Grp}}(G) = \mathrm{Hom}_{\mathrm{Grp}}(G, G)$.

Definiţia 72. 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, $\mathrm{Aut}(G)$.

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.