

CURSUL 6: LEGI DE COMPOZIȚIE

G. MINCU

1. LEGI DE COMPOZIȚIE

Definiția 1. Fie M o mulțime nevidă. Numim **lege de compoziție binară** (sau **operație binară**) pe mulțimea M orice funcție

$$\varphi : M \times M \rightarrow M.$$

Observația 2. Întrucât noi vom face referire aproape exclusiv la legi de compoziție binare, le vom numi pe acestea, succint, legi de compoziție (sau operații), subînțelegând epitetul „binare”. În situația în care în cursurile viitoare vom dori să aducem în discuție și altfel de legi de compoziție, vom menționa acest lucru în mod explicit la momentul respectiv.

Notația pe care o folosim în mod uzual în acest context nu este $\varphi(a, b)$, ci $a\varphi b$. De asemenea, vom utiliza o gamă largă de simboluri pentru a desemna legile de compoziție: $\star, \circ, \perp, \Delta$, etc. Foarte frecvent vom folosi simbolurile $+$ și \cdot , chiar și în situația în care legea de compoziție desemnată nu este adunarea sau înmulțirea standard a vreuneia din mulțimile familiare.

Exemplul 3. Adunarea, scăderea și înmulțirea pe \mathbb{C} sunt legi de compoziție.

Exemplul 4. Nu putem considera o lege de compoziție pe \mathbb{N} care să asocieze oricăror două elemente diferența lor.

Exemplul 5. Adunarea matricelor este lege de compoziție pe $\mathcal{M}_{m,n}(\mathbb{C})$. Înmulțirea matricelor este lege de compoziție pe $\mathcal{M}_n(\mathbb{C})$.

Exemplul 6. Dată fiind o lege de compoziție \star pe o mulțime M și o mulțime nevidă A , pe mulțimea M^A putem defini o lege de compoziție astfel: $(f \star g)(a) = f(a) \star g(a)$.

Exemplul 7. Dată fiind o mulțime nevidă A , compunerea uzuală a funcțiilor este o operație binară pe A^A .

Exemplul 8. Dată fiind o mulțime nevidă A , reuniunea și intersecția sunt legi de compoziție pe $\mathcal{P}(A)$.

Exemplul 9. Pe mulțimea \mathbb{Z}_n a claselor de resturi modulo n sunt corect definite următoarele legi de compoziție: $\widehat{a} + \widehat{b} \stackrel{\text{def}}{=} \widehat{a+b}$ și $\widehat{a} \cdot \widehat{b} \stackrel{\text{def}}{=} \widehat{a \cdot b}$. Pentru a vedea acest lucru, să remarcăm de pildă că dacă $\widehat{a} = \widehat{a'}$ și $\widehat{b} = \widehat{b'}$ atunci $n|a' - a$ și $n|b' - b$, deci $n|(a' - a)b' + a(b' - b) = a'b' - ab$, de unde $\widehat{a'b'} = \widehat{ab}$. Am justificat astfel corectitudinea definirii operației „ \cdot ”. Lăsăm verificarea corectitudinii definirii operației „ $+$ ” în grija cititorului.

Definiția 10. Operațiile „ $+$ ” și „ \cdot ” introduse la exemplul 9 se numesc **adunarea modulo n** , respectiv **înmulțirea modulo n** .

2. PARTE STABILĂ. OPERAȚIE INDUSĂ

Definiția 11. Fie \star o lege de compoziție pe o mulțime M , iar N o submulțime a lui M . Spunem că N este **parte stabilă a lui M în raport cu \star** dacă $\forall x, y \in N \quad x \star y \in N$.

Observația 12. Dacă $N \neq \emptyset$ este parte stabilă a lui M în raport cu \star , atunci $N \times N \rightarrow N$, $(x, y) \mapsto x \star y$ este o lege de compoziție pe N .

Definiția 13. Legea de compoziție din observația 12 se numește **legea de compoziție indusă de \star pe N** .

Observația 14. Legea de compoziție \star pe mulțimea M induce o lege de compoziție pe submulțimea nevidă N a lui M dacă și numai dacă N este parte stabilă a lui M în raport cu \star .

Exemplul 15. Mulțimile \mathbb{Z} , \mathbb{Q} și \mathbb{R} sunt părți stabile ale lui \mathbb{C} în raport cu adunarea, scăderea și înmulțirea. Prin urmare, adunarea, scăderea și înmulțirea sunt legi de compoziție pe \mathbb{Z} , \mathbb{Q} și \mathbb{R} . Cu un argument similar, adunarea și înmulțirea sunt legi de compoziție pe \mathbb{N} .

3. ASOCIATIVITATE

Definiția 16. Fie \star o lege de compoziție pe mulțimea M . Spunem că \star este **asociativă** dacă

$$\forall x, y, z \in M \quad (x \star y) \star z = x \star (y \star z).$$

Observația 17. Legile de compoziție de la exemplele 3, 5, 7, 8, 9, 15 sunt asociative. Scăderea numerelor întregi (raționale, reale, complexe) nu este asociativă. Dacă operația \star este asociativă pe M , atunci operația din exemplul 6 este asociativă.

Temă: Justificați afirmațiile de la observația 17!

Definiția 18. Fie \star o operație pe mulțimea M și $x_1, x_2, \dots \in M$. Dacă \star este asociativă, iar $n \geq 3$, definim inductiv $x_1 \star x_2 \star \dots \star x_n$ astfel:

$$x_1 \star x_2 \star \dots \star x_n \stackrel{\text{def}}{=} (x_1 \star x_2 \star \dots \star x_{n-1}) \star x_n$$

Propoziția 19. Fie \star o lege de compoziție asociativă pe mulțimea M , $x_1, x_2, \dots \in M$ și $m, n \in \mathbb{N}^*$. Atunci

$$x_1 \star x_2 \star \dots \star x_{m+n} = (x_1 \star x_2 \star \dots \star x_m) \star (x_{m+1} \star x_{m+2} \star \dots \star x_{m+n}).$$

Observația 20. Dacă pe o mulțime M este dată o operație asociativă notată multiplicativ, $x \in M$ și $n \in \mathbb{N}^*$, vom nota cu x^n elementul $\underbrace{x \cdot x \cdot \dots \cdot x}_{n \text{ factori}}$. Relația din propoziția 19 devine în aceste condiții

$$x^{m+n} = x^m \cdot x^n.$$

Observația 21. Dacă pe o mulțime M este dată o operație asociativă notată aditiv, $x \in M$ și $n \in \mathbb{N}^*$, vom nota cu nx elementul $\underbrace{x + x + \dots + x}_{n \text{ termeni}}$. Relația din propoziția 19 devine în aceste condiții

$$(m+n)x = mx + nx.$$

4. COMUTATIVITATE

Definiția 22. Fie \star o operație pe mulțimea M și $x_1, x_2 \in M$. Spunem că x_1 și x_2 **comută** (în raport cu \star) dacă $x_1 \star x_2 = x_2 \star x_1$.

Definiția 23. Fie \star o operație pe mulțimea M . Spunem că \star este **comutativă** dacă

$$\forall x_1, x_2 \in M \quad x_1 \star x_2 = x_2 \star x_1.$$

Observația 24. Legea de compoziție \star dată pe mulțimea M este comutativă dacă și numai dacă orice două elemente ale lui M comută în raport cu \star .

Observația 25. Legile de compoziție de la exemplele 3, 8, 9, 15 sunt comutative. Adunarea pe $\mathcal{M}_{m,n}(\mathbb{C})$ este comutativă. Scăderea numerelor întregi (raționale, reale, complexe) nu este comutativă. Înmulțirea pe $\mathcal{M}_n(\mathbb{C})$ nu este comutativă decât dacă $n = 1$. Compunerea pe M^M nu este comutativă decât dacă M are cel mult un element. Dacă operația \star este comutativă pe M , atunci operația din exemplul 6 este comutativă.

Temă: Justificați afirmațiile de la observația 25!

Propoziția 26. Fie \star o lege de compoziție asociativă și comutativă pe mulțimea M , $n \in \mathbb{N}^*$, $x_1, x_2, \dots, x_n \in M$ și σ o permutare a mulțimii $\{1, 2, \dots, n\}$. Atunci,

$$x_1 \star x_2 \star \dots \star x_n = x_{\sigma(1)} \star x_{\sigma(2)} \star \dots \star x_{\sigma(n)}.$$

5. ELEMENT NEUTRU

Definiția 27. Fie \star o lege de compoziție pe mulțimea M .

Spunem că $e \in M$ este **element neutru la stânga** pentru \star dacă

$$\forall x \in M \quad e \star x = x.$$

Spunem că $e \in M$ este **element neutru la dreapta** pentru \star dacă

$$\forall x \in M \quad x \star e = x.$$

Spunem că $e \in M$ este **element neutru** pentru \star dacă

$$\forall x \in M \quad e \star x = x \wedge x \star e = x.$$

Observația 28. $e \in M$ este element neutru pentru \star dacă și numai dacă el este atât element neutru la stânga cât și element neutru la dreapta.

Propoziția 29. Fie \star o lege de compoziție asociativă și comutativă pe mulțimea M . Dacă \star admite un element neutru la stânga și un element neutru la dreapta, atunci acestea coincid.

Demonstrație: Fie e elementul neutru la stânga și f elementul neutru la dreapta pentru \star . Atunci $e = e \star f = f$. \square

Corolarul 30. Dacă o lege de compoziție \star admite atât element neutru la stânga cât și element neutru la dreapta, atunci \star admite element neutru.

Corolarul 31. Dacă o lege de compoziție admite element neutru, acesta este unic.

Exemplul 32. 0 este element neutru pentru adunarea pe \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} și \mathbb{C} .

Observația 33. Datorită situației amintite în exemplul 32, pentru elementul neutru al unei legi de compoziție notate aditiv se folosește frecvent notația 0, chiar dacă nu este vorba de numărul complex 0.

Exemplul 34. 1 este element neutru pentru înmulțirea pe \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} și \mathbb{C} .

Observația 35. Datorită situației amintite în exemplul 34, pentru elementul neutru al unei legi de compoziție notate multiplicativ se folosește frecvent notația 1, chiar dacă nu este vorba de numărul complex 1.

Exemplul 36. Scăderea numerelor întregi (raționale, reale, complexe) nu admite element neutru, dar îl are ca element neutru la dreapta pe 0.

Exemplul 37. Matricea cu toate elementele nule este element neutru pentru adunarea pe $\mathcal{M}_{m,n}(\mathbb{C})$. Vom nota această matrice cu $\mathbf{0}_{m,n}$.

Definiția 38. Matricea $\mathbf{0}_{m,n}$ se numește **matricea nulă** de tip m, n .

Exemplul 39. Matricea cu 1 pe diagonala principală și restul elementelor nule este element neutru pentru înmulțirea pe $\mathcal{M}_n(\mathbb{C})$. Vom nota această matrice cu I_n .

Definiția 40. Matricea I_n se numește **matricea identică** (sau **matricea unitate**) de ordin n .

Exemplul 41. Dacă operația \star are elementul neutru e , atunci funcția $E : A \rightarrow M$, $E(a) = e$ este element neutru pentru operația de la exemplul 6.

Exemplul 42. Dată fiind o mulțime A , funcția identică a lui A este element neutru pentru compunerea pe A^A .

Exemplul 43. Dată fiind o mulțime A , mulțimea vidă este element neutru pentru operația de reuniune de pe $\mathcal{P}(A)$.

Exemplul 44. Dată fiind o mulțime A , A este element neutru pentru operația de intersecție de pe $\mathcal{P}(A)$.

Exemplul 45. $\hat{0}$ este element neutru pentru adunarea modulo n .

Exemplul 46. $\hat{1}$ este element neutru pentru înmulțirea modulo n .

Temă: Justificați afirmațiile de la exemplele 36, 37, 39, 41-46!

6. SIMETRIZABILITATE

Definiția 47. Fie \star o lege de compoziție cu element neutru (notat cu e) pe mulțimea M . Fie $x \in M$.

Spunem că $y \in M$ este **simetric la stânga** al lui x în raport cu \star dacă $y \star x = e$.

Spunem că $y \in M$ este **simetric la dreapta** al lui x în raport cu \star dacă $x \star y = e$.

Spunem că $y \in M$ este **simetric** al lui x în raport cu \star dacă $y \star x = x \star y = e$.

Definiția 48. În contextul din definiția 47, x se numește **simetrizabil în raport cu \star** dacă el admite simetric în raport cu \star .

Propoziția 49. Fie \star o lege de compoziție asociativă și cu element neutru e pe mulțimea M și $x \in M$. Dacă x admite un simetric la stânga și un simetric la dreapta, atunci acestea coincid.

Demonstrație: Fie y un simetric la stânga pentru x și z un simetric la dreapta pentru x . Atunci $y = y \star e = y \star (x \star z) = (y \star x) \star z = e \star z = z$.
□

Corolarul 50. Dacă elementul x admite atât simetric la stânga cât și simetric la dreapta în raport cu legea asociativă \star care are și element neutru, atunci x este simetrizabil în raport cu \star .

Temă: Rămâne afirmația din corolarul 50 adevărată și în situația în care legea \star (admite element neutru, dar) nu este asociativă?

Corolarul 51. În condițiile propoziției 49, dacă elementul x este simetrizabil în raport cu \star , atunci simetricul său este unic.

Definiția 52. În condițiile propoziției 49, unicul (conform corolarului 51) simetric al elementului simetrizabil x se numește **simetricul lui x în raport cu \star** .

Exemplul 53. Simetricul elementului $x \in \mathbb{Z}$ (\mathbb{Q} , \mathbb{R} , \mathbb{C}) în raport cu adunarea este $-x$.

Observația 54. Datorită situației semnalate în exemplul 53, pentru simetricul unui element x în raport cu o lege de compoziție notată aditiv se folosește notația $-x$.

Exemplul 55. Simetricul elementului $x \in \mathbb{Q}^*$ (\mathbb{R}^* , \mathbb{C}^*) în raport cu înmulțirea este x^{-1} .

Observația 56. Datorită situației semnalate în exemplul 55, pentru simetricul unui element x în raport cu o lege de compoziție notată multiplicativ se folosește notația x^{-1} .

Exemplul 57. O matrice $A \in \mathcal{M}_n(\mathbb{C})$ este simetrizabilă în raport cu înmulțirea dacă și numai dacă ea este inversabilă. În caz că A este simetrizabilă, simetrica ei este chiar inversa ei.

Exemplul 58. O funcție $f \in A^A$ este simetrizabilă în raport cu compunerea dacă și numai dacă ea este inversabilă. În caz că f este simetrizabilă, simetrica ei este chiar inversa ei.

7. SEMIGRUPURI

7.1. Semigrupuri.

Definiția 59. Fie S o mulțime nevidă și \cdot o lege de compoziție pe S . Perechea (S, \cdot) se numește **semigrup** dacă \cdot este asociativă. Dacă în plus \cdot este și comutativă, semigrupul (S, \cdot) se numește **comutativ**.

Observația 60. Dacă legea de compoziție \cdot este subînțeleasă 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 ”.

Observația 61. Legile de compoziție de la exemplele 3, 5, 7, 8, 9 și 15 conferă mulțimilor respective structură de semigrup. Semigrupurile de la exemplele 3, 8, 9 și 15 sunt comutative.

7.2. Reguli de calcul în semigrupuri.

Propoziția 62. Fie (S, \cdot) un semigrup, $x, y \in S$ și $m, n \in \mathbb{N}^*$. 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: Relația de la a) reiese din observația 20. Punctul b) se probează prin inducție după n , iar c), prin inducție după m . Lăsăm detaliile în grija cititorului. \square

7.3. Morfisme de semigrupuri.

Definiția 63. Fie S și S' două semigrupuri (în notație multiplicativă). O funcție $f : S \rightarrow S'$ se numește **morfism de semigrupuri** dacă

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

Propoziția 64. Dacă $f : S \rightarrow S'$ și $g : S' \rightarrow S''$ sunt morfisme de semigrupuri, atunci $g \circ f$ este morfism de semigrupuri.

Demonstrație: 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

Definiția 65. Fie S și S' două semigrupuri (în notație multiplicativă). Un morfism de semigrupuri $f : S \rightarrow S'$ se numește **izomorfism** dacă există un morfism de semigrupuri $g : S' \rightarrow S$ cu proprietatea că

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

Exemplul 66. Pentru orice semigrup S , funcția identică a lui S este izomorfism de semigrupuri.

Exemplul 67. Pentru orice izomorfism f de semigrupuri, f^{-1} este izomorfism de semigrupuri.

Propoziția 68. $f : S \rightarrow S'$ este izomorfism de semigrupuri dacă și numai dacă f este morfism bijectiv de semigrupuri.

Demonstrație: „ \Rightarrow ”: Evident.

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

8. MONOIZI

8.1. Monoizi.

Definiția 69. Fie M o mulțime nevidă și \cdot o lege de compoziție pe M . Perechea (M, \cdot) se numește **monoid** dacă \cdot este asociativă și admite element neutru. Dacă în plus \cdot este și comutativă, monoidul (M, \cdot) se numește **comutativ**.

Observația 70. Dacă legea de compoziție \cdot este subînțeleasă 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 ”.

Observația 71. Legile de compoziție de la exemplele 3, 5, 7, 8, 9 și 15 conferă mulțimilor respective structură de monoid. Monoizii de la exemplele 3, 8, 9 și 15 sunt comutativi.

8.2. Reguli de calcul în monoizi. Fie (M, \cdot) un monoid și $x \in M$. **Notăm** $x^0 \stackrel{\text{def}}{=} 1$.

Propoziția 72. Fie (M, \cdot) un monoid, $x, y \in M$ și $m, n \in \mathbb{N}$. 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: Pentru $mn \neq 0$ se aplică propoziția 62, iar pentru $mn = 0$ relațiile din enunț sunt imediate. \square

8.3. Morfisme de monoizi.

Definiția 73. Fie M și M' doi monoizi (în notație multiplicativă). O funcție $f : M \rightarrow M'$ se numește **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 și $1_{M'}$ desemnând aici elementele neutre ale celor doi monoizi).

Propoziția 74. Dacă $f : M \rightarrow M'$ și $g : M' \rightarrow M''$ sunt morfisme de monoizi, atunci $g \circ f$ este morfism de monoizi.

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

Definiția 75. Fie M și M' doi monoizi (în notație multiplicativă). Un morfism de monoizi $f : M \rightarrow M'$ se numește **izomorfism** dacă există un morfism de monoizi $g : M' \rightarrow M$ cu proprietatea că $f \circ g = \text{id}_{M'}$ și $g \circ f = \text{id}_M$.

Exemplul 76. Pentru orice monoid M , funcția identică a lui M este morfism de monoizi.

Exemplul 77. Pentru orice izomorfism f de monoizi, f^{-1} este izomorfism de monoizi.

Propoziția 78. $f : M \rightarrow M'$ este izomorfism de monoizi dacă și numai dacă f este morfism bijectiv de monoizi.

Demonstrație: „ \Rightarrow ”: Evident.

„ \Leftarrow ”: Fie $x', y' \in M'$. Punem $x = f^{-1}(x')$ și $y = f^{-1}(y')$. 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, $f^{-1}(1_{M'}) = f^{-1}(f(1_M)) = 1_M$. \square

8.4. Monoidul liber generat de o mulțime. Fie A o mulțime nevidă. Pe mulțimea înșiruirilor finite de elemente ale lui A definim legea de compoziție $a_1a_2 \dots a_m \star a'_1a'_2 \dots a'_t \stackrel{\text{def}}{=} a_1a_2 \dots a_ma'_1a'_2 \dots a'_t$.

Definiția 79. Înșiruirile de k elemente din A se numesc **cuvinte de lungime k** peste A , iar operația \star se numește **concatenare**.

Este util să considerăm și un cuvânt peste A ce „nu conține niciun simbol”:

Definiția 80. Dată fiind o mulțime nevidă A , considerăm că există un (unic) cuvânt de lungime zero peste A . El se numește **cuvântul vid** peste A .

Vom nota cuvântul vid cu \sqcup .

Propoziția 81. Mulțimea cuvintelor peste A are în raport cu operația de concatenare o structură de monoid, al cărei element neutru este \sqcup .

Temă: Demonstrați propoziția 81!

Definiția 82. Monoidul la care se face referire în propoziția 81 se numește **monoidul liber generat de mulțimea A** .

Notăția uzuală pentru monoidul liber generat de mulțimea A este $FM(A)$.

Propoziția 83. Considerăm o mulțime nevidă A , un monoid M și o funcție $f : A \rightarrow M$. Atunci funcția $\tilde{f} : FM(A) \rightarrow M$, $\tilde{f}(a_1a_2 \dots a_n) = f(a_1)f(a_2) \dots f(a_n)$, $\tilde{f}(\sqcup) = e$, este un morfism de monoizi.

Temă: Demonstrați propoziția 83!

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.