CURSUL 4: LEGI DE COMPOZIŢIE

G. MINCU

1. Legi de compoziţie

Definiţia 1. Fie M o mulţime nevidă. Numim **lege de compoziţie binară** (sau **operaţie binară**) pe mulţimea M orice funcţie

$$\varphi : M \times M \to M.$$

Observaţia 2. Întrucât noi vom face în mod explicit referire numai la legi de compoziţie binare, le vom numi pe acestea, succint, legi de compoziţie (sau operaţii), subînţelegând epitetul „binare".

Notaţia 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 compoziţie: $\star, \circ, \perp, \triangle$, etc. Foarte frecvent vom folosi simbolurile $+$ şi $\cdot$, chiar şi în situaţia în care legea de compoziţie desemnată nu este adunarea sau înmulţirea standard a vreuneia din mulţimile familiare.

Exemplul 3. Adunarea, scăderea şi înmulţirea pe $\mathbb{C}$ sunt legi de compoziţie.

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

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

Exemplul 6. Dată fiind o lege de compoziţie $\star$ pe o mulţime M şi o mulţime nevidă A, pe mulţimea M^A putem defini o lege de compoziţie astfel: $(f \star g)(a) = f(a) \star g(a)$.

Exemplul 7. Dată fiind o mulţime nevidă A, compunerea uzuală a funcţiilor este o operaţie binară pe A^A.

Exemplul 8. Dată fiind o mulţime nevidă A, reuniunea şi intersecţia sunt legi de compoziţie pe $\mathcal{P}(A)$.

Exemplul 9. Pe mulţimea $\mathbb{Z}_n$ a claselor de resturi modulo n sunt corect definite următoarele legi de compoziţie: $\widehat{a} + \widehat{b} \overset{\text{def}}{=} \widehat{a+b}$ şi $\widehat{a} \cdot \widehat{b} \overset{\text{def}}{=}$

$\widehat{a \cdot b}$. Pentru a vedea acest lucru, să remarcăm de pildă că dacă $\widehat{a} = \widehat{a'}$ şi $\widehat{b} = \widehat{b'}$ atunci $n|a' - a$ şi $n|b' - b$, deci $n|(a' - a)b' + a(b' - b) = a'b' - ab$, de unde $\widehat{a'b'} = \widehat{ab}$. Am justificat astfel corectitudinea definirii operaţiei „$\cdot$". Lăsăm verificarea corectitudinii definirii operaţiei „$+$" în grija cititorului.

Definiţia 10. Operaţiile „$+$" şi „$\cdot$" introduse la exemplul 9 se numesc **adunarea modulo** n, respectiv **înmulţirea modulo** n.

2. Parte stabilă. Operaţie indusă

Definiţia 11. Fie $\star$ o lege de compoziţie pe o mulţime M, iar N o submulţime a lui M. Spunem că N este **parte stabilă a lui M în raport cu $\star$** dacă $\quad \forall x, y \in N \quad x \star y \in N$.

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

Definiţia 13. Legea de compoziţie din observaţia 12 se numeşte **legea de compoziţie indusă de $\star$ pe N**.

Observaţia 14. Legea de compoziţie $\star$ pe mulţimea M induce o lege de compoziţie pe submulţimea nevidă N a lui M dacă şi numai dacă N este parte stabilă a lui M în raport cu $\star$.

Exemplul 15. Mulţimile $\mathbb{Z}$, $\mathbb{Q}$ şi $\mathbb{R}$ sunt părţi stabile ale lui $\mathbb{C}$ în raport cu adunarea, scăderea şi înmulţirea. Prin urmare, adunarea, scăderea şi înmulţirea sunt legi de compoziţie pe $\mathbb{Z}$, $\mathbb{Q}$ şi $\mathbb{R}$. Cu un argument similar, adunarea şi înmulţirea sunt legi de compoziţie pe $\mathbb{N}$.

3. asociativitate

Definiţia 16. Fie $\star$ o lege de compoziţie pe mulţimea M. Spunem că $\star$ este **asociativă** dacă

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

Observaţia 17. Legile de compoziţie de la exemplele 3, 5, 7, 8, 9, 15 sunt asociative. Scăderea numerelor întregi (raţionale, reale, complexe) nu este asociativă. Dacă operaţia $\star$ este asociativă pe M, atunci operaţia din exemplul 6 este asociativă.

Temă: Justificaţi afirmaţiile de la observaţia 17!

Definiţia 18. Fie $\star$ o operaţie pe mulţimea M şi $x_1, x_2, \ldots \in M$. Dacă $\star$ este asociativă, iar $n \geq 3$, definim inductiv $x_1 \star x_2 \star \ldots \star x_n$ astfel:

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

Propoziţia 19. Fie $\star$ o lege de compoziţie asociativă pe mulţimea M, x_1, $x_2, \ldots \in M$ şi $m, n \in \mathbb{N}^*$. Atunci

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

Observaţia 20. Dacă pe o mulţime M este dată o operaţie asociativă notată multiplicativ, $x \in M$ şi $n \in \mathbb{N}^*$, vom nota cu x^n elementul $\underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ factori}}$. Relaţia din propoziţia 19 devine în aceste condiţii

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

Observaţia 21. Dacă pe o mulţime M este dată o operaţie asociativă notată aditiv, $x \in M$ şi $n \in \mathbb{N}^*$, vom nota cu nx elementul $\underbrace{x + x + \ldots + x}_{n \text{ termeni}}$. Relaţia din propoziţia 19 devine în aceste condiţii

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

4. COMUTATIVITATE

Definiţia 22. Fie $\star$ o operaţie pe mulţimea M şi x_1, $x_2 \in M$. Spunem că x_1 şi x_2 **comută (în raport cu $\star$)** dacă $x_1 \star x_2 = x_2 \star x_1$.

Definiţia 23. Fie $\star$ o operaţie pe mulţimea M. Spunem că $\star$ este **comutativă** dacă

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

Observaţia 24. Legea de compoziţie $\star$ dată pe mulţimea M este comutativă dacă şi numai dacă orice două elemente ale lui M comută în raport cu $\star$.

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

Temă: Justificaţi afirmaţiile de la observaţia 25!

Propoziţia 26. Fie $\star$ o lege de compoziţie asociativă şi comutativă pe mulţimea M, $n \in \mathbb{N}^*$, x_1, $x_2, \ldots, x_n \in M$ şi σ o permutare a mulţimii $\{1, 2, \ldots, n\}$. Atunci,

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

5. ELEMENT NEUTRU

Definiţia 27. Fie $\star$ o lege de compoziţie pe mulţimea 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

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

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

Propoziţia 29. Fie $\star$ o lege de compoziţie asociativă şi comutativă pe mulţimea M. Dacă $\star$ admite un element neutru la stânga şi un element neutru la dreapta, atunci acestea coincid.

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

Corolarul 30. Dacă o lege de compoziţie $\star$ admite atât element neutru la stânga cât şi element neutru la dreapta, atunci $\star$ admite element neutru.

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

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

Observaţia 33. Datorită situaţiei amintite în exemplul 32, pentru elementul neutru al unei legi de compoziţie notate aditiv se foloseşte frecvent notaţia 0, chiar dacă nu este vorba de numărul complex 0.

Exemplul 34. 1 este element neutru pentru înmulţirea pe $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ şi $\mathbb{C}$.

Observaţia 35. Datorită situaţiei amintite în exemplul 34, pentru elementul neutru al unei legi de compoziţie notate multiplicativ se foloseşte frecvent notaţia 1, chiar dacă nu este vorba de numărul complex 1.

Exemplul 36. Scăderea numerelor întregi (raţionale, 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 $\mathbf{0}_{m,n}$.

Definiţia 38. Matricea din exemplul 37 se numeşte **matricea nulă** de tip m, n.

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

Definiţia 40. Matricea din exemplul 39 se numeşte **matricea identică** (sau **matricea unitate**) de ordin n.

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

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

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

Exemplul 44. Dată fiind o mulţime A, A este element neutru pentru operaţia de intersecţie de pe $\mathcal{P}(A)$.

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

Exemplul 46. $\widehat{1}$ este element neutru pentru înmulţirea modulo n.

Temă: Justificaţi afirmaţiile de la exemplele 36, 37, 39, 41-46!

6. SIMETRIZABILITATE

Definiţia 47. Fie $\star$ o lege de compoziţie cu element neutru (notat cu e) pe mulţimea 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 $y \star x = x \star y = e$.

Definiţia 48. În contextul din definiţia 47, x se numeşte **simetrizabil în raport cu** $\star$ dacă el admite simetric în raport cu $\star$.

Propoziţia 49. Fie $\star$ o lege de compoziţie asociativă şi cu element neutru e pe mulţimea M şi $x \in M$. Dacă x admite un simetric la stânga şi un simetric la dreapta, atunci acestea coincid.

Demonstraţie: Fie y un simetric la stânga pentru x şi z un simetric la dreapta pentru x. Atunci $y = y \star e = y \star (x \star z) = (y \star x) \star z = e \star z = z$. $\square$

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

Temă: Rămâne afirmaţia din corolarul 50 adevărată şi în situaţia în care legea $\star$ (admite element neutru, dar) nu este asociativă?

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

Definiţia 52. În condiţiile propoziţiei 49, unicul (conform corolarului 51) simetric al elementului simetrizabil x se numeşte **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 $-x$.

Observaţia 54. Datorită situaţiei semnalate în exemplul 53, pentru simetricul unui element x în raport cu o lege de compoziţie notată aditiv se foloseşte notaţia $-x$.

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

Observaţia 56. Datorită situaţiei semnalate în exemplul 55, pentru simetricul unui element x în raport cu o lege de compoziţie notată multiplicativ se foloseşte notaţia x^{-1}.

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

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

7. SEMIGRUPURI

7.1. **Semigrupuri.**

Definiţia 59. 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 60. 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 $\cdot$".

Observaţia 61. Legile de compoziţie de la exemplele 3, 5, 7, 8, 9 şi 15 conferă mulţimilor respective structură de semigrup. Semigrupurile de la exemplele 3, 8, 9 şi 15 sunt comutative.

7.2. **Reguli de calcul în semigrupuri.**

Propoziţia 62. 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 observaţia 20. Punctul b) se probează prin inducţie după n, iar c), prin inducţie după m. Lăsăm detaliile în grija cititorului. $\square$

7.3. **Morfisme de semigrupuri.**

Definiţia 63. 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 64. 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 65. 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 66. Pentru orice semigrup S, funcţia identică a lui S este izomorfism de semigrupuri.

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

Propoziţia 68. $f : S \to S'$ 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 $f^{-1}(x'y') = f^{-1}(f(x)f(y)) = f^{-1}(f(xy)) = xy = f^{-1}(x')f^{-1}(y')$ $\square$

8. MONOIZI

8.1. **Monoizi.**

Definiţia 69. 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 70. 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 $\cdot$".

Observaţia 71. Legile de compoziţie de la exemplele 3, 5, 7, 8, 9 şi 15 conferă mulţimilor respective structură de monoid. Monoizii de la exemplele 3, 8, 9 şi 15 sunt comutativi.

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

Propoziţia 72. 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 62, iar pentru $mn = 0$ relaţiile din enunţ sunt imediate. $\square$

8.3. **Morfisme de monoizi.**

Definiţia 73. 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 74. 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 $(g \circ f)(1_M) = g(f(1_M)) = g(1_{M'}) = 1_{M''}$. $\square$

Definiţia 75. 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 76. Pentru orice monoid M, funcţia identică a lui M este morfism de monoizi.

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

Propoziţia 78. $f : M \to M'$ este izomorfism de monoizi dacă şi numai dacă f este morfism bijectiv de monoizi.

Demonstraţie: „$\Rightarrow$": Evident.
„$\Leftarrow$": 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, $f^{-1}(1_{M'}) = f^{-1}(f(1_M)) = 1_M$. $\square$

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

Definiţia 79. 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 80. 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 $\llcorner\!\lrcorner$.

Propoziţia 81. Mulţimea cuvintelor peste A are în raport cu operaţia de concatenare o structură de monoid, al cărei element neutru este $\llcorner\!\lrcorner$.

Temă: Demonstraţi propoziţia 81!

Definiţia 82. Monoidul la care se face referire în propoziţia 81 se numeşte **monoidul liber generat de mulţimea** A.

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

Propoziţia 83. Considerăm o mulţime nevidă A, un monoid M şi o funcţie $f : A \to M$. Atunci funcţia $\tilde{f} : FM(A) \to M$, $\tilde{f}(a_1a_2\ldots a_n) = f(a_1)f(a_2)\ldots f(a_n)$, $f(\llcorner\!\lrcorner) = e$, este un morfism de monoizi.

Temă: Demonstraţi propoziţia 83!

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.