CURSUL 2: MULŢIMI

G. MINCU

1. Mulţimi

Noţiunea de mulţime este una primară în matematică.

De obicei, folosim termenul de „mulţime" pentru a desemna o entitate pe care considerăm că o constituie anumite obiecte[1]. Acestea din urmă se numesc **elementele** mulţimii.

Vom nota faptul că obiectul x este element al mulţimii M prin $x \in M$.

Vom considera că **două mulţimi sunt egale dacă şi numai dacă au aceleaşi elemente**.

Cea mai naturală metodă de a reprezenta o mulţime este de a enumera efectiv elementele acesteia; în mod standard, elementele respective se scriu între acolade, fără repetiţii şi în orice ordine dorim.

Exemplul 1. a) $\{1, 3, -5\}$; $\{-\frac{7}{3}, \pi\}$; {a;b;1, 2(3)}, $\{3, -5, 1\}$, $\{-3, 5, 1\}$, etc.
Reamintim aici şi mulţimile „uzuale" de numere:
b) $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$ - mulţimea numerelor naturale.
c) $\mathbb{Z} = \{\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots\}$ - mulţimea numerelor întregi.

Observaţia 2. $\{1, 3, -5\} = \{3, -5, 1\}$, dar $\{1, 3, -5\} \neq \{-1, 3, 5\}$.

Nu toate mulţimile pot fi reprezentate de maniera sintetică propusă anterior, de cele mai multe ori motivul fiind acela că respectivele mulţimi au „prea multe" elemente pentru a fi posibilă (sau utilă!) o astfel de reprezentare. În astfel de situaţii, apelăm la reprezentarea mulţimilor cu ajutorul unei proprietăţi caracteristice elementelor lor.

[1]fie graţie unor proprietăţi comune ce justifică punerea laolaltă a acestor obiecte, fie pur şi simplu în mod arbitrar/ca exerciţiu intelectual

Exemplul 3. a) $\{a \in \mathbb{N} : \exists k \in \mathbb{N}\ a = 2k+1\}$ - mulţimea numerelor naturale impare
b) $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0\right\}$ - mulţimea numerelor raţionale.
c) $\mathbb{R}$ = mulţimea numerelor ce corespund punctelor unei drepte[2] - mulţimea numerelor reale.
d) $\mathbb{C} = \{a + bi : a, b \in \mathbb{R},\ i^2 = -1\}$ - mulţimea numerelor complexe.

Observaţia 4. În exemplul 3 nu este reprezentată şi mulţimea $\mathbb{R}$ în acord cu ideile pe care le-am introdus. O astfel de reprezentare este posibilă, dar greu de urmărit în acest moment.

Definiţia 5. Spunem că mulţimea A este **inclusă** în mulţimea B dacă orice element al lui A îi aparţine şi lui B. Această situaţie este descrisă şi de exprimarea „**A este submulţime a mulţimii B**".

Desemnăm situaţia în care mulţimea A este inclusă în mulţimea B prin notaţia $A \subset B$.

Observaţia 6. Dacă $A \subset B$, putem avea $A = B$ sau nu. Dacă nu are loc egalitatea celor două mulţimi, spunem că A **este inclusă strict în** B şi scriem $A \subsetneq B$.

Observaţia 7. Dată fiind o mulţime M şi o proprietate $\mathcal{P}$ care are sens pentru cel puţin unul dintre elementele lui M, admitem că $\{x \in M : x$ are proprietatea $\mathcal{P}\}$ este o submulţime a lui M. Acest lucru conferă legitimitate manierei „analitice" de prezentare a mulţimilor pe care am amintit-o mai sus[3].

Observaţia 8. Mulţimile A şi B sunt egale dacă şi numai dacă $A \subset B$ şi $B \subset A$.

O consecinţă foarte importantă a observaţiei 8 este următoarea:

Observaţia 9. Întotdeauna egalitatea de mulţimi se demonstrează prin dublă incluziune.

Observaţia 10. $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Niciuna dintre aceste incluziuni nu este egalitate.

Definiţia 11. Considerăm că există o mulţime care nu are niciun element. Ea se notează cu $\emptyset$ şi se numeşte **mulţimea vidă**.

[2]pe care am fixat originea şi unitatea

[3]Atragem atenţia asupra faptului că, în lipsa unei mulţimi iniţiale M în cadrul căreia să punem problema elementelor cu proprietatea $\mathcal{P}$, nu avem garanţia că acestea constituie o mulţime. Persistenţa în a lucra cu astfel de „mulţimi" poate conduce la paradoxuri.

Observaţia 12. Pentru orice mulţime M avem $\emptyset = \{x \in \text{M}: x \neq x\}$. Prin urmare, $\emptyset \subset M$.

Se consideră că, dată fiind o mulţime M, submulţimile sale constituie o mulţime.

Definiţia 13. Dată fiind mulţimea M, mulţimea $\{A : A \subset M\}$ se numeşte **mulţimea părţilor lui** M. Vom nota această mulţime cu $\mathcal{P}(M)$.

2. Principiul inducţiei

O proprietate fundamentală a mulţimii numerelor naturale, care ne oferă o puternică metodă pentru demonstraţia de afirmaţii şi pentru construcţia de obiecte, este următoarea[4]:

Principiul inducţiei: *Dacă M este o submulţime a lui $\mathbb{N}$ cu proprietăţile*
1) $0 \in M$
şi
2) $\forall n \in \mathbb{N} \;\; n \in M \Rightarrow n+1 \in M$,
atunci $M = \mathbb{N}$.

Prezentăm mai jos două consecinţe ale acestui principiu. Acestea stau la baza abordării practice a demonstraţiilor prin inducţie matematică.

Teorema 14. *Fie P un predicat de variabilă naturală şi $n_0 \in \mathbb{N}$ astfel încât:*
1) $P(n_0)$
şi
2) $\forall k \geq n_0 \;\; P(k) \Rightarrow P(k+1)$,
atunci $\forall n \geq n_0 \; P(n)$.

Teorema 15. *Fie P un predicat de variabilă naturală şi $n_0 \in \mathbb{N}$ astfel încât:*
1) $P(n_0)$
şi
2) $\forall k \geq n_0 \;\; (P(n_0) \wedge P(n_0+1) \wedge \ldots \wedge P(k)) \Rightarrow P(k+1)$,
atunci $\forall n \geq n_0 \; P(n)$.

[4] Principiul inducţiei este o consecinţă imediată a axiomaticii teoriei mulţimilor, fie că se utilizează axioma mulţimilor infinite, fie că se porneşte de la axiomele lui Peano

3. Operaţii cu mulţimi

În fiecare dintre situaţiile care urmează, în lipsa vreunei alte menţiuni, vom considera că există o mulţime „mare" care conţine toate mulţimile în discuţie.

Considerăm mulţimile A şi B.

Definiţia 16. Mulţimea $A \cup B = \{x : x \in A \vee x \in B\}$ se numeşte **reuniunea** mulţimilor A şi B.

Definiţia 17. Mulţimea $A \cap B = \{x : x \in A \wedge x \in B\}$ se numeşte **intersecţia** mulţimilor A şi B.

Definiţia 18. Dacă $A \cap B = \emptyset$, spunem că mulţimile A şi B sunt **disjuncte**.

Definiţia 19. Mulţimea $A \setminus B = \{x : x \in A \wedge x \notin B\}$ se numeşte **diferenţa** mulţimilor A şi B.

Definiţia 20. $(a, b) \stackrel{\text{def}}{=} \{\{a\}, \{a, b\}\}$ se numeşte **perechea ordonată** determinată de elementele a şi b.

Observaţia 21. Drept consecinţă a axiomelor teoriei mulţimilor obţinem în acest context faptul că toate perechile ordonate (a, b) cu $a \in A$ şi $b \in B$ constituie o mulţime.

Definiţia 22. $A \times B = \{(a, b) : a \in A \wedge b \in B\}$ se numeşte **produsul cartezian** al mulţimilor A şi B.

Propoziţia 23. Pentru orice mulţimi A, B şi C au loc relaţiile:
a) $A \cap B \subset A \subset A \cup B$.
b) $A \cup B = B \cup A$; $A \cap B = B \cap A$.
c) $(A \cup B) \cup C = A \cup (B \cup C)$; $(A \cap B) \cap C = A \cap (B \cap C)$.
d) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
e) $A \times (B \cup C) = (A \times B) \cup (A \times C)$; $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Exerciţiul 24. Demonstraţi propoziţia 23!

Punctul c) al propoziţiei 23 ne sugerează următoarele definiţii:

Definiţia 25. $A \cup B \cup C \stackrel{\text{def}}{=} (A \cup B) \cup C$;
$A \cap B \cap C \stackrel{\text{def}}{=} (A \cap B) \cap C$.

Fie E o mulţime.

Definiţia 26. Pentru $A \subset E$, definim **complementara lui A în raport cu E** ca fiind mulţimea $E \setminus A$.

Notaţia utilizată pentru complementara lui A în raport cu E este $\complement_E A$. Dacă E este subînţeleasă în context, atunci complementara lui A în raport cu E se mai notează şi $\complement A$ sau $\overline{A}$.

Regulile lui de Morgan: Dacă $A, B \subset E$, atunci:

$$\complement_E(A \cup B) = \left(\complement_E A\right) \cap \left(\complement_E B\right) \quad \text{şi} \quad \complement_E(A \cap B) = \left(\complement_E A\right) \cup \left(\complement_E B\right).$$

Exerciţiul 27. Demonstraţi regulile lui de Morgan!

Definiţia 28. Dacă E este o mulţime înzestrată cu o lege de compoziţie $\circ$, iar $A, B \subset E$, definim $A \circ B = \{a \circ b : a \in A \wedge b \in B\}$.
Dacă $a \in E$, notăm $a \circ E$ (respectiv, $E \circ a$) în loc de $\{a\} \circ E$ (respectiv, de $E \circ \{a\}$).

Exemplul 29. a) $\{1,2,3\} + \{10,20\} = \{11,12,13,21,22,23\}$
b) $\{1,2,3\} - \{10,20\} = \{-19,-18,-17,-9,-8,-7\}$
c) $\{1,2,3\} \cdot \{10,20\} = \{10,20,30,40,60\}$
d) $2\mathbb{Z}$ = mulţimea numerelor întregi pare.
e) $3\mathbb{Z}+1$ = mulţimea acelor numere întregi care prin împărţire la 3 dau restul 1.
f) $\{-1,1\} \cdot \mathbb{N} = \mathbb{Z}$.

4. FAMILII DE MULŢIMI

Pentru generalizarea chestiunilor din paragraful precedent, este necesară o modalitate de a gestiona „multe" mulţimi. Una dintre cele mai frecvente abordări ale chestiunii este următoarea[5]:

Definiţia 30. Prin **familie de mulţimi indexată după mulţimea** I înţelegem o funcţie definită pe I şi ale cărei valori sunt mulţimi.

Vom nota familia mulţimilor M_i, $i \in I$, cu $(M_i)_{i \in I}$.

O consecinţă imediată a axiomelor teoriei mulţimilor este aceea că putem defini reuniunea oricărei mulţimi de mulţimi. Este legitimă deci:

Definiţia 31. Prin **reuniunea** familiei de mulţimi $(M_i)_{i \in I}$ înţelegem mulţimea $\{x : \exists i \in I \;\; x \in M_i\}$.

Notaţia pe care o vom folosi pentru reuniunea familiei de mulţimi $(M_i)_{i \in I}$ este $\bigcup_{i \in I} M_i$. În situaţia în care $I = \{1,2,\ldots,n\}$, reuniunea

[5] Pentru a plasa aceste consideraţii imediat după cele pe care le generalizează, utilizăm aici noţiunea de funcţie; aceasta este definită în cursul 3, iar definiţia respectivă nu se bazează pe chestiunile din acest paragraf.

familiei menţionate se notează şi $\bigcup_{i=1}^{n} M_i$, iar dacă $I = \mathbb{N}$, reuniunea familiei $(M_i)_{i\in I}$ se notează şi $\bigcup_{i=1}^{\infty} M_i$ sau $\bigcup_{i\geq 1} M_i$

Definiţia 32. Prin **intersecţia** familiei de mulţimi $(M_i)_{i\in I}$ înţelegem mulţimea $\{x : \forall i \in I \;\; x \in M_i\}$.

Notaţia pe care o vom folosi pentru intersecţia familiei de mulţimi $(M_i)_{i\in I}$ este $\bigcap_{i\in I} M_i$. În situaţia în care $I = \{1, 2, \ldots, n\}$, intersecţia familiei menţionate se notează şi $\bigcap_{i=1}^{n} M_i$, iar dacă $I = \mathbb{N}$, intersecţia familiei $(M_i)_{i\in I}$ se notează şi $\bigcap_{i=1}^{\infty} M_i$ sau $\bigcap_{i\geq 1} M_i$

Afirmaţiile propoziţiei 23 se generalizează astfel:

Propoziţia 33. Pentru orice familie de mulţimi $(A_i)_{i\in I}$ şi pentru orice mulţime B au loc relaţiile[6]*:*

a') $\forall i \in I \qquad \bigcap_{i\in I} A_i \subset A_i \subset \bigcup_{i\in I} A_i.$

c') Dacă $I = \bigcup_{j\in J} I_j$, iar mulţimile familiei $(I_j)_{j\in J}$ sunt disjuncte două câte două, atunci

$$\bigcup_{i\in I} A_i = \bigcup_{j\in J} \left(\bigcup_{i\in I_j} A_i \right) \quad \text{şi} \quad \bigcap_{i\in I} A_i = \bigcap_{j\in J} \left(\bigcap_{i\in I_j} A_i \right).$$

d') $B \cap \left(\bigcup_{i\in I} A_i \right) = \bigcup_{i\in I} (B \cap A_i) \quad \text{şi} \quad B \cup \left(\bigcap_{i\in I} A_i \right) = \bigcap_{i\in I} (B \cup A_i).$

e') $B \times \left(\bigcup_{i\in I} A_i \right) = \bigcup_{i\in I} (B \times A_i) \quad \text{şi} \quad B \times \left(\bigcap_{i\in I} A_i \right) = \bigcap_{i\in I} (B \times A_i).$

Toate consideraţiile anterioare sunt, desigur, valabile şi pentru familii de submulţimi ale unei mulţimi date. În acest context funcţionează următoarea variantă generalizată a regulilor lui de Morgan:

[6]Punctul b) al propoziţiei 23 se generalizează la:
b') Pentru orice funcţie bijectivă $\sigma : I \to I$,
$\bigcup_{i\in I} A_{\sigma(i)} = \bigcup_{i\in I} A_i$ şi $\bigcap_{i\in I} A_{\sigma(i)} = \bigcap_{i\in I} A_i$.

Propoziţia 34. Dată fiind familia $(A_i)_{i\in I}$ de submulţimi ale mulţimii E, au loc relaţiile:

$$\complement_E\left(\bigcup_{i\in I} A_i\right) = \bigcap_{i\in I} \complement_E A_i \quad \text{şi} \quad \complement_E\left(\bigcap_{i\in I} A_i\right) = \bigcup_{i\in I} \complement_E A_i$$

Bibliografie

[1] T. Dumitrescu, *Algebra*, Ed. Universităţii din Bucureşti, 2006.

[2] P. Halmos, *Naive set theory*, Springer Verlag, 1960.

[3] C. Năstăsescu, C. Niţă, C. Vraciu, *Bazele algebrei*, Ed. Academiei, Bucureşti, 1986.

[4] C. Năstăsescu, *Introducere în teoria mulţimilor*, Ed. Didactică şi Pedagogică, Bucureşti, 1974.

CURSUL 3: FUNCŢII

G. MINCU

1. Funcţii

Definiţia 1. (provizorie!) Numim **funcţie** orice triplet format din două mulţimi şi o „lege de corespondenţă" care asociază ***fiecărui*** element din prima mulţime un ***unic*** element din cea de-a doua.

Definiţia 2. Prima dintre cele două mulţimi care intră în componenţa unei funcţii se numeşte **domeniul** (**de definiţie** al) funcţiei, iar cea de a doua se numeşte **codomeniul** (sau **domeniul de valori** al) funcţiei.

Observaţia 3. Două funcţii sunt egale dacă şi numai dacă au acelaşi domeniu, acelaşi codomeniu şi aceeaşi lege de corespondenţă.

Notaţia uzuală pentru o funcţie f care are domeniul A şi codomeniul B este $f : A \to B$ (citim „f este definită pe A şi ia valori în B"). Faptul că elementului $a \in A$ îi corespunde prin f elementul $b \in B$ se notează $f(a) = b$.

Definiţia 4. Prin **graficul** unei funcţii $f : A \to B$ înţelegem mulţimea $\Gamma_f = \{(a, b) \in A \times B : b = f(a)\}$.

Observaţia 5. Dacă $f : A \to B$, atunci $\Gamma_f \subset A \times B$.

Observaţia 6. Cunoscând graficul unei funcţii, putem identifica domeniul de definiţie al funcţiei, precum şi legea de corespondenţă a acesteia[1]. Din acest motiv, se preferă reformularea definiţiei 1 astfel încât să se evite termenul „lege", care nu are în situaţia respectivă un înţeles foarte bine precizat:

Definiţia 7. Numim **funcţie** orice triplet format din trei mulţimi A, B, G, $G \subset A \times B$, cu proprietatea: $\forall a \in A\ \exists!\ b \in B\ (a, b) \in G$.

Observaţia 8. O consecinţă a axiomelor din teoria mulţimilor este faptul că, date fiind două mulţimi A şi B, funcţiile definite pe A cu valori în B constituie o mulţime.

[1]Nu însă şi codomeniul; putem însă „vedea" imaginea funcţiei.

Observaţia 9. Dacă mulţimile finite A şi B au a, respectiv b elemente, se arată uşor (temă!) că numărul funcţiilor definite pe A cu valori în B este b^a. Această observaţie ne sugerează utilizarea pentru mulţimea tuturor funcţiilor definite pe A cu valori în B a notaţiei B^A.

2. CLASE IMPORTANTE DE FUNCŢII

Definiţia 10. Funcţia $f : A \to B$ se numeşte **injectivă** dacă $\forall a_1, a_2 \in A \quad a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$.

Observaţia 11. În cuvinte, o funcţie este injectivă dacă duce orice două elemente diferite în elemente diferite.

O caracterizare des utilizată a funcţiilor injective este dată de:

Propoziţia 12. Funcţia $f : A \to B$ este injectivă dacă şi numai dacă $\forall a_1, a_2 \in A \quad f(a_1) = f(a_2) \Rightarrow a_1 = a_2$.

Exemplul 13. Dacă $A \subset B$, atunci $i : A \to B$, $i(a) = a$ este o funcţie injectivă. Ea se numeşte **injecţia canonică** a lui A în B.

Definiţia 14. Funcţia $f : A \to B$ se numeşte **surjectivă** dacă $\forall b \in B$ $\exists a \in A$ $f(a) = b$.

Observaţia 15. În cuvinte, o funcţie este surjectivă dacă „îşi umple codomeniul".

Exemplul 16. $\pi_A : A \times B \to A$, $\pi_A(a, b) = a$ şi $\pi_B : A \times B \to A$, $\pi_B(a, b) = b$ sunt funcţii surjective (ele se numesc **proiecţiile canonice** ale produsului cartezian $A \times B$).

Definiţia 17. O funcţie injectivă şi surjectivă se numeşte **bijectivă**.

Exemplul 18. Dată fiind o mulţime A, funcţia $\mathrm{id}_A : A \to A$, $\mathrm{id}_A(a) = a$ este o funcţie bijectivă. Ea se numeşte **funcţia identică a mulţimii** A.

Definiţia 19. O mulţime A se numeşte **infinită** dacă există $f \in A^A$ injectivă, dar nesurjectivă. Mulţimea A se numeşte **finită** dacă nu este infinită.

Propoziţia 20. Fie A o mulţime nevidă. Următoarele afirmaţii sunt echivalente:
a) A este finită.
b) Există un număr $n \in \mathbb{N}^*$ şi o funcţie bijectivă $f : \{1, 2, \ldots, n\} \to A$.

Pentru consideraţiile de până la finalul acestei secţiuni vom considera că A şi B desemnează submulţimi ale lui $\mathbb{R}$.

Definiţia 21. Funcţia $f : A \to B$ se numeşte **crescătoare** dacă $\forall a_1, a_2 \in A \quad a_1 < a_2 \Rightarrow f(a_1) \leq f(a_2)$.

Definiţia 22. Funcţia $f : A \to B$ se numeşte **descrescătoare** dacă $\forall a_1, a_2 \in A \quad a_1 < a_2 \Rightarrow f(a_1) \geq f(a_2)$.

Definiţia 23. Funcţia $f : A \to B$ se numeşte **monotonă** dacă este fie crescătoare, fie descrescătoare.

Definiţia 24. Funcţia $f : A \to B$ se numeşte **strict crescătoare** dacă $\forall a_1, a_2 \in A \quad a_1 < a_2 \Rightarrow f(a_1) < f(a_2)$.

Definiţia 25. Funcţia $f : A \to B$ se numeşte **strict descrescătoare** dacă $\forall a_1, a_2 \in A \quad a_1 < a_2 \Rightarrow f(a_1) > f(a_2)$.

Definiţia 26. Funcţia $f : A \to B$ se numeşte **strict monotonă** dacă este fie strict crescătoare, fie strict descrescătoare.

3. funcţia caracteristică a unei submulţimi

Definiţia 27. Fie E o mulţime şi $A \subset E$. Funcţia

$$\chi_A : E \to \{0,1\}, \quad \chi_A(x) = \begin{cases} 1 & \text{dacă } x \in A \\ 0 & \text{dacă } x \notin A \end{cases}$$

se numeşte **funcţia caracteristică**[2] **a lui** A **în** E.

Teorema 28. Fie E o mulţime. Funcţia $\chi : \mathcal{P}(E) \to \{0,1\}^E$, $\chi(A) = \chi_A$ este bijectivă.

Funcţiile caracteristice ale submulţimilor au proprietăţi calculatorii interesante care, laolaltă cu teorema 28, le conferă o largă aplicabilitate:

Propoziţia 29. Fie E o mulţime şi A, B submulţimi ale sale. Au loc relaţiile:
a) $\chi_E = 1$; $\chi_\emptyset = 0$.
b) $\chi_{A\cap B} = \min\{\chi_A, \chi_B\} = \chi_A \chi_B$.
c) $\chi_{A\cup B} = \max\{\chi_A, \chi_B\} = \chi_A + \chi_B - \chi_A \chi_B$.
d) $\chi_{\complement_E A} = 1 - \chi_A$.

4. „transportul" submulţimilor prin funcţii

Definiţia 30. Dacă $f : A \to B$ şi $C \subset A$, notăm $f(C)$ şi numim **imaginea submulţimii** C **prin funcţia** f mulţimea

$$\{b \in B : \exists c \in C \ f(c) = b\}.$$

[2]Uneori, cu precădere în teoria probabilităţilor, se mai foloseşte pentru funcţia prezentată denumirea de **funcţia indicator a submulţimii** A **a lui** E

Definiţia 31. Prin **imaginea** funcţiei $f : A \to B$ înţelegem mulţimea $f(A)$.

Notaţia folosită în mod uzual pentru imaginea funcţiei f este $\mathrm{Im} f$.

Observaţia 32. O funcţie este surjectivă dacă şi numai dacă imaginea sa coincide cu codomeniul său.

Definiţia 33. Dacă $f : A \to B$ şi $D \subset B$, notăm $f^{-1}(D)$ şi numim **preimaginea**[3] **submulţimii** D **prin funcţia** f mulţimea $\{a \in A : f(a) \in D\}$.

Observaţia 34. Notaţia din definiţia 33 se utilizează şi în situaţia în care funcţia f nu este inversabilă!

Propoziţia 35. Considerăm funcţia $f : A \to B$. Atunci:
a) Dacă $M \subset N \subset A$, atunci $f(M) \subset f(N)$.
b) Dacă $M, N \subset A$, atunci $f(M \cup N) = f(M) \cup f(N)$.
c) Dacă $M, N \subset A$, atunci $f(M \cap N) \subset f(M) \cap f(N)$.
d) Dacă $P \subset Q \subset B$, atunci $f^{-1}(P) \subset f^{-1}(Q)$.
e) Dacă $P, Q \subset B$, atunci $f^{-1}(P \cup Q) = f^{-1}(P) \cup f^{-1}(Q)$.
f) Dacă $P, Q \subset B$, atunci $f^{-1}(P \cap Q) = f^{-1}(P) \cap f^{-1}(Q)$.

Temă: Demonstraţi propoziţia 35!

Temă: Generalizaţi afirmaţiile din propoziţia 35 la situaţia unei familii arbitrare de submulţimi!

Observaţia 36. Observăm că în cazul relaţiilor din propoziţia 35 imaginea inversă „se poartă mai bine" decât imaginea directă. Aparenta „anomalie" de la punctul c) dispare pentru funcţiile injective:

Propoziţia 37. Funcţia $f : A \to B$ este injectivă dacă şi numai dacă

$$\forall M, N \subset A \quad f(M \cap N) = f(M) \cap f(N).$$

5. COMPUNEREA FUNCŢIILOR

Definiţia 38. Date fiind funcţiile $f : A \to B$ şi $g : C \to D$ cu[4] $B \subset C$, definim funcţia $g \circ f : A \to D$, $g \circ f(x) = g(f(x))$. Funcţia $g \circ f$ se numeşte **compusa lui** g **cu** f.

O situaţie importantă din punctul de vedere al compunerii funcţiilor este prezentată în

[3] sau **imaginea inversă**, sau încă **imaginea reciprocă**

[4] în caz de necesitate, se poate impune doar condiţia mai slabă $\mathrm{Im} f \subset C$

Exemplul 39. Dată fiind o funcţie arbitrară $f : A \to B$, $\mathrm{id}_B \circ f = f$ şi $f \circ \mathrm{id}_A = f$.

Propoziţia 40. Fie funcţiile $f : A \to B$, $g : C \to D$ şi $h : E \to F$, unde $B \subset C$ şi $D \subset E$. Atunci[5] $h \circ (g \circ f) = (h \circ g) \circ f$.

Propoziţia 41. Fie funcţiile $f : A \to B$ şi $g : C \to D$, unde $B \subset C$. Atunci:
a) Dacă f şi g sunt injective, atunci $g \circ f$ este injectivă.
b) Dacă $g \circ f$ este injectivă, atunci f este injectivă.
c) Dacă f şi g sunt surjective şi $B = C$, atunci $g \circ f$ este surjectivă.
b) Dacă $g \circ f$ este surjectivă, atunci g este surjectivă.
e) Dacă f şi g sunt bijective şi $B = C$, atunci $g \circ f$ este bijectivă.
b) Dacă $g \circ f$ este bijectivă, atunci f este injectivă, iar g este surjectivă.

Temă: Demonstraţi propoziţia 41!

Propoziţia 42. Fie $A, B, C, D \subset \mathbb{R}$, $B \subset C$, şi funcţiile $f : A \to B$ şi $g : C \to D$. Atunci:
a) Dacă f şi g sunt de aceeaşi monotonie, atunci $g \circ f$ este crescătoare.
b) Dacă f şi g sunt de monotonii opuse, atunci $g \circ f$ este descrescătoare.
c) Dacă f şi g sunt de aceeaşi monotonie strictă, atunci $g \circ f$ este strict crescătoare.
d) Dacă f şi g sunt de monotonii stricte opuse, atunci $g \circ f$ este strict descrescătoare.

Temă: Demonstraţi propoziţia 42!

Propoziţia 43. Orice funcţie strict monotonă este injectivă.

Temă: Demonstraţi propoziţia 43!

6. INVERSAREA FUNCŢIILOR

Definiţia 44. (provizorie!) Prin **inversă a funcţiei** $f : A \to B$ înţelegem orice funcţie $g : B \to A$ cu proprietăţile $g \circ f = \mathrm{id}_A$ şi $f \circ g = \mathrm{id}_B$.

Definiţia 45. Funcţia $f : A \to B$ se numeşte **inversabilă** dacă ea admite (cel puţin o) inversă.

Propoziţia 46. Dacă funcţia $f : A \to B$ este inversabilă, atunci ea admite o unică inversă

[5] Anticipând discuţia referitoare la legi de compoziţie, această relaţie arată că, dată fiind o mulţime M, compunerea funcţiilor este o operaţie asociativă pe M^M.

Demonstraţie: Presupunem că f este inversabilă şi că g şi h sunt inverse ale sale. Atunci,

$$g = g \circ \mathrm{id}_B = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_A \circ h = h. \quad \square$$

Definiţia 47. Dacă funcţia $f : A \to B$ este inversabilă, atunci prin **inversa** lui f înţelegem unica (conform propoziţiei 46) funcţie $g : B \to A$ cu proprietăţile $g \circ f = \mathrm{id}_A$ şi $f \circ g = \mathrm{id}_B$.

Notaţia pe care o vom folosi pentru a desemna inversa funcţiei inversabile f este f^{-1}.

Observaţia 48. Dacă $f : A \to B$ este inversabilă, iar $D \subset B$, atunci, în acord cu definiţia 33, notaţia $f^{-1}(D)$ ar desemna atât preimaginea lui D prin f, cât şi imaginea lui D prin f^{-1}. Întrucât aceste două mulţimi coincid, utilizarea aceleiaşi notaţii nu prezintă ambiguităţi.

Teorema 49. O funcţie este inversabilă dacă şi numai dacă ea este bijectivă.

7. Produsul cartezian al unei familii de mulţimi

Observaţia 50. Perechea ordonată $(a_1, a_2) \in A_1 \times A_2$ poate fi interpretată ca fiind o reprezentare a funcţiei $a : \{1, 2\} \to A_1 \cup A_2$, $a(1) = a_1$, $a(2) = a_2$. Evident, $a(1) \in A_1$ şi $a(2) \in A_2$. Aceste consideraţii ne sugerează:

Definiţia 51. Dată fiind familia de mulţimi $(A_i)_{i \in I}$, definim produsul său cartezian ca fiind mulţimea $\{a : I \to \bigcup_{i \in I} A_i : \forall i \in I \;\; a(i) \in A_i\}$[6,7]

Vom nota produsul cartezian al familiei de mulţimi $(A_i)_{i \in I}$ cu $\prod_{i \in I} A_i$, iar elementul $a \in \prod_{i \in I} A_i$ cu $(a(i))_{i \in I}$ sau, mai frecvent, cu $(a_i)_{i \in I}$.

Definiţia 52. Pentru $j \in I$, funcţia $\pi_j : \prod_{i \in I} A_i \to A_j$, $\pi_j((a_i)_{i \in I}) = a_j$ se numeşte **proiecţia canonică** a produsului $\prod_{i \in I} A_i$ pe componenta j.

Observaţia 53. Proiecţiile canonice ale produsului cartezian sunt surjective.

[6]Axiomele teoriei mulţimilor au drept consecinţă faptul că aceasta este într-adevăr o mulţime.

[7]Una dintre axiomele teoriei mulţimilor (aşa-numita „axiomă a alegerii") afirmă că dacă toate mulţimile familiei date sunt nevide, atunci produsul cartezian al familiei este nevid.

Observaţia 54. Dacă avem familia de mulţimi $(A_i)_{i\in I}$ cu proprietatea $A_i = A$ pentru orice $i \in I$, atunci, conform definiţiei 51, produsul cartezian $\prod_{i\in I} A_i$ constă exact în funcţiile definite pe I şi care iau valori în A. Deci, în acest caz avem $\prod_{i\in I} A_i = A^I$. Dacă în situaţia prezentată avem $I = \{1, 2, \ldots, n\}$, $n \in \mathbb{N}^*$, vom folosi în loc de A^I notaţia A^n.

Observaţia 55. Conform observaţiei anterioare,

$$A^n = \{(a_1, a_2, \ldots, a_n) : a_1, a_2, \ldots, a_n \in A\}.$$

Bibliografie

[1] T. Dumitrescu, *Algebra*, Ed. Universităţii din Bucureşti, 2006.

[2] P. Halmos, *Naive set theory*, Springer Verlag, 1960.

[3] C. Năstăsescu, C. Niţă, C. Vraciu, *Bazele algebrei*, Ed. Academiei, Bucureşti, 1986.

[4] C. Năstăsescu, *Introducere în teoria mulţimilor*, Ed. Didactică şi Pedagogică, Bucureşti, 1974.

CURSUL 5: RELAŢII

G. MINCU

1. Corespondenţe

Definiţia 1. Numim **corespondenţă**[1] orice triplet de mulţimi $\alpha = (A, B, \rho)$ cu proprietatea $\rho \subset A \times B$.

Definiţia 2. Cu notaţiile din definiţia 1, ρ se numeşte **graficul** corespondenţei α.

Observaţia 3. Noţiunea de corespondenţă este o generalizare a noţiunii de funcţie.

Multe dintre noţiunile şi tehnicile pe care le-am întâlnit la studiul funcţiilor pot fi transpuse şi pentru cazul corespondenţelor. Este de aşteptat să întâlnim similitudini pronunţate cu chestiunile omoloage de la funcţii, dar nu trebuie să ne surprindă nici anumite diferenţe între situaţia corespondenţelor şi cea a funcţiilor, diferenţe ce decurg din faptul că funcţiile sunt corespondenţe de un tip foarte particular. Aceste consideraţii vor fi concretizate în următoarele două capitole.

2. Compunerea corespondenţelor

Definiţia 4. Considerăm corespondenţele $\alpha = (A, B, \rho)$ şi $\beta = (B, C, \sigma)$. Corespondenţa $\beta \circ \alpha = (A, C, \sigma \circ \rho)$, unde

$$\sigma \circ \rho = \{(x, z) \in A \times C : \exists\, y \in B \quad (x, y) \in \rho \wedge (y, z) \in \sigma\},$$

se numeşte **compusa corespondenţelor** β **şi** α.

Propoziţia 5. Date fiind corespondenţele $\alpha = (A, B, \rho)$, $\beta = (B, C, \sigma)$ şi $\gamma = (C, D, \tau)$, are loc egalitatea

$$(\gamma \circ \beta) \circ \alpha = \gamma \circ (\beta \circ \alpha).$$

Definiţia 6. Cu notaţiile din propoziţia 5,

$$\gamma \circ \beta \circ \alpha \stackrel{\text{def}}{=} (\gamma \circ \beta) \circ \alpha.$$

[1] În loc de „corespondenţă” unii autori folosesc în context noţiunea „relaţie binară”. Noi vom prefera să folosim sintagma „relaţie binară” în accepţia din capitolul 4 al cursului. Utilizarea unui alt termen pentru situaţia de faţă are drept scop eliminarea anumitor ambiguităţi de exprimare în contextul din capitolul 4.

Definiţia 7. Date fiind $n \in \mathbb{N}$, $n \geq 4$, şi corespondenţele $\alpha_1, \alpha_2, \ldots, \alpha_n$ pentru care expresiile de mai jos au sens, definim

$$\alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_n \stackrel{\text{def}}{=} (\alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_{n-1}) \circ \alpha_n.$$

Observaţia 8. Aplicând propoziţia 5, constatăm că că operaţile de compunere din expresia $\alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_n$ pot fi făcute în orice ordine dorim[2].

Definiţia 9. Dată fiind corespondenţa $\alpha = (A, A, \rho)$,

(i) $\alpha^1 \stackrel{\text{def}}{=} \alpha$ şi

(ii) Pentru $n \in \mathbb{N}^* \setminus \{1\}$, $\alpha^n \stackrel{\text{def}}{=} \alpha \circ \alpha^{n-1}$.

Observaţia 10. $\alpha^2 = \alpha \circ \alpha$, iar $\alpha^3 = \alpha \circ \alpha^2$.

Definiţia 11. Dată fiind o mulţime A, corespondenţa $\mathrm{id}_A = (A, A, \Delta_A)$, unde $\Delta_A = \{(a, a) : a \in A\}$ se numeşte **corespondenţa identică** (sau **corespondenţa unitate**) a mulţimii A.

Propoziţia 12. Dată fiind corespondenţa $\alpha = (A, B, \rho)$, au loc egalităţile

$$\mathrm{id}_B \circ \alpha = \alpha \quad \text{şi} \quad \alpha \circ \mathrm{id}_A = \alpha.$$

3. INVERSAREA CORESPONDENŢELOR

Definiţia 13. Numim **inversa** corespondenţei $\alpha = (A, B, \rho)$ corespondenţa $\alpha^{-1} = (B, A, \rho^{-1})$, unde $\rho^{-1} = \{(b, a) : (a, b) \in \rho\}$.

Observaţia 14. Spre deosebire de situaţia funcţiilor, orice corespondenţă admite inversă.

Observaţia 15. Aici poate apărea întrebarea: având în vedere că toate funcţiile sunt corespondenţe şi că toate corespondenţele admit inversă, de ce nu admit toate funcţiile inversă? Răspunsul este că orice funcţie admite într-adevăr o *corespondenţă* inversă, dar aceasta *nu este funcţie decât în situaţia în care funcţia de la care am pornit este inversabilă în sensul prezentat în cursul 3.*

O diferenţă remarcabilă faţă de situaţia întâlnită la funcţii este dată de

Observaţia 16. Dacă $\alpha = (A, B, \rho)$ este o corespondenţă, nu este obligatoriu ca $\alpha \circ \alpha^{-1} = \mathrm{id}_B$ sau ca $\alpha^{-1} \circ \alpha = \mathrm{id}_A$.

Chestiunea menţionată în observaţia 16 are de fapt o formă mult mai precisă:

[2] fără a modifica însă ordinea **termenilor**!

Propoziţia 17. Dată fiind corespondenţa $\alpha = (A, B, \rho)$, au loc egalităţile $\alpha \circ \alpha^{-1} = \mathrm{id}_B$ şi $\alpha^{-1} \circ \alpha = \mathrm{id}_A$ dacă şi numai dacă α este funcţie bijectivă.

Propoziţia 18. Date fiind corespondenţele $\alpha = (A, B, \rho)$ şi $\beta = (B, C, \sigma)$, au loc egalităţile:
(i) $(\alpha^{-1})^{-1} = \alpha$
(ii) $((\beta \circ \alpha)^{-1}) = \alpha^{-1} \circ \beta^{-1}$.

4. Relaţii pe o mulţime

În cele ce urmează, vom lua în discuţie numai corespondenţe (A, B, ρ) în care $A = B$. În situaţiile de acest tip, după precizarea iniţială a mulţimii A nu vom mai insista în a o include în notaţiile ulterioare ale corespondenţelor cu care lucrăm. În plus, singura corespondenţă de la mulţimea vidă la ea însăşi este cea vidă. Din acest motiv, noi vom studia în continuare doar corespondenţe pe mulţimi nevide. Această discuţie se concretizează în următoarea definiţie:

Definiţia 19. Numim **relaţie binară pe mulţimea nevidă** A orice submulţime a lui $A \times A$.

Observaţia 20. În acest curs vom lucra doar cu relaţii binare, motiv pentru care în cele ce urmează vom omite acest epitet.

Vom nota cu $\mathcal{R}(A)$ mulţimea relaţiilor pe mulţimea A.

Observaţia 21. $\mathcal{R}(A) = \mathcal{P}(A \times A)$.

Observaţia 22. Dacă ρ este o relaţie pe mulţimea A iar $a, b \in A$, vom utiliza frecvent notaţia $a \rho b$ pentru a desemna situaţia $(a, b) \in \rho$ şi notaţia $a \not\rho b$ pentru a desemna situaţia $(a, b) \notin \rho$.

Fiecărei relaţii ρ pe mulţimea A îi putem asocia corespondenţa (A, A, ρ) şi reciproc. Putem folosi această observaţie pentru a adapta la cazul relaţiilor anumite noţiuni pe care le-am definit pentru corespondenţe:

5. Compunerea relaţiilor

Definiţia 23. Considerăm o mulţime A şi relaţiile ρ şi σ pe A. Relaţia $\sigma \circ \rho = \{(x, z) \in A \times A : \exists\, y \in A \ (x, y) \in \rho \wedge (y, z) \in \sigma\}$ se numeşte **compusa relaţiilor σ şi ρ**.

Propoziţia 24. Date fiind corespondenţele ρ, σ şi τ pe mulţimea A, are loc egalitatea

$$(\tau \circ \sigma) \circ \rho = \tau \circ (\sigma \circ \rho).$$

Demonstraţie: Afirmaţia este o consecinţă imediată a propoziţiei 5. □

Definiţia 25. Cu notaţiile din propoziţia 5,

$$\tau \circ \sigma \circ \rho \stackrel{\text{def}}{=} (\tau \circ \sigma) \circ \rho.$$

Definiţia 26. Date fiind $n \in \mathbb{N}$, $n \geq 4$, şi relaţiile $\rho_1, \rho_2, \ldots, \rho_n$ pe mulţimea A, definim

$$\rho_1 \circ \rho_2 \circ \ldots \circ \rho_n \stackrel{\text{def}}{=} (\rho_1 \circ \rho_2 \circ \ldots \circ \rho_{n-1}) \circ \rho_n.$$

Observaţia 27. Propoziţia 5 ne arată că operaţile de compunere din expresia $\rho_1 \circ \rho_2 \circ \ldots \circ \rho_n$ pot fi făcute în orice ordine dorim[3].

Definiţia 28. Dată fiind relaţia ρ pe mulţimea A, definim

(i) $\rho^1 \stackrel{\text{def}}{=} \rho$ şi

(ii) Pentru $n \in \mathbb{N}^* \setminus \{1\}$, $\rho^n \stackrel{\text{def}}{=} \rho \circ \rho^{n-1}$.

Observaţia 29. $\rho^2 = \rho \circ \rho$, iar $\rho^3 = \rho \circ \rho^2$.

Observaţia 30. Date fiind o relaţie ρ pe o mulţime A şi $m, n \in \mathbb{N}^*$, are loc egalitatea $\rho^{m+n} = \rho^m \circ \rho^n$.

Definiţia 31. Dată fiind o mulţime A, mulţimea $\Delta_A = \{(a, a) : a \in A\}$ se numeşte **diagonala** mulţimii $A \times A$.

Observaţia 32. În limbajul introdus în textul de faţă, Δ_A este relaţia de egalitate pe mulţimea A.

Propoziţia 33. Dată fiind relaţia ρ pe mulţimea A, au loc egalităţile

$$\Delta_A \circ \rho = \rho \quad \text{şi} \quad \rho \circ \Delta_A = \rho.$$

Observaţia 34. Dacă pe mulţimea A sunt date relaţiile ρ, σ, τ şi φ astfel încât $\rho \subset \tau$ şi $\sigma \subset \varphi$, atunci $\sigma \circ \rho \subset \varphi \circ \tau$.

6. INVERSAREA RELAŢIILOR

Definiţia 35. Numim **inversa** relaţiei ρ (dată pe mulţimea A) relaţia $\rho^{-1} = \{(b, a) \in A \times A : (a, b) \in \rho\}$.

Observaţia 36. Spre deosebire de situaţia funcţiilor, orice relaţie admite inversă.

Observaţia 37. Dacă ρ este o relaţie pe mulţimea A, nu este obligatoriu ca $\rho \circ \rho^{-1} = \Delta_A$ sau ca $\rho^{-1} \circ \rho = \Delta_A$.

Propoziţia 38. Date fiind relaţiile ρ şi σ pe mulţimea A, au loc egalităţile:

(i) $(\rho^{-1})^{-1} = \rho$

(ii) $((\sigma \circ \rho)^{-1}) = \rho^{-1} \circ \sigma^{-1}$.

[3] fără a modifica însă ordinea **termenilor**!

Demonstraţie: Afirmaţia este o consecinţă imediată a propoziţiei 18. □

Definiţia 39. Dată fiind relaţia ρ pe mulţimea A şi $n \in \mathbb{N}^* \setminus \{1\}$,

$$\rho^{-n} \stackrel{\text{def}}{=} \rho^{-1} \circ \rho^{1-n}.$$

Observaţia 40. Dată fiind o relaţie ρ pe o mulţime A, au loc egalităţile:
(i) $\forall n \in \mathbb{N}^* \quad \rho^{-n} = (\rho^n)^{-1}$
(ii) $\forall m, n \in \mathbb{N}^* \quad \rho^{-m-n} = \rho^{-m} \circ \rho^{-n}$

Observaţia 41. Dacă pe mulţimea A sunt date relaţiile ρ şi σ astfel încât $\rho \subset \sigma$, atunci $\rho^{-1} \subset \sigma^{-1}$.

7. CLASE IMPORTANTE DE RELAŢII

În tot acest capitol ρ va desemna o relaţie pe mulţimea A.

Definiţia 42. Spunem că ρ este **reflexivă** dacă $\forall a \in A \quad a \rho a$.

Observaţia 43. Relaţia ρ este reflexivă dacă şi numai dacă $\rho \supset \Delta_A$.

Definiţia 44. Spunem că ρ este **ireflexivă** dacă $\forall a \in A \quad a \not\rho a$.

Observaţia 45. Relaţia ρ este ireflexivă dacă şi numai dacă $\rho \cap \Delta_A = \emptyset$.

Definiţia 46. Spunem că ρ este **simetrică** dacă $\forall a, b \in A \quad a \rho b \Rightarrow b \rho a$.

Propoziţia 47. Dată fiind o relaţie ρ pe o mulţime A, următoarele afirmaţii sunt echivalente:
(i) ρ este simetrică.
(ii) $\rho^{-1} \subset \rho$.
(iii) $\rho^{-1} = \rho$.

Definiţia 48. Spunem că ρ este **antisimetrică** dacă

$$\forall a, b \in A \quad a \rho b \wedge b \rho a \Rightarrow a = b.$$

Observaţia 49. Relaţia ρ este antisimetrică dacă şi numai dacă

$$\rho \cap \rho^{-1} \subset \Delta_A.$$

Definiţia 50. Spunem că ρ este **tranzitivă** dacă

$$\forall a, b, c \in A \quad a \rho b \wedge b \rho c \Rightarrow a \rho c.$$

Observaţia 51. Relaţia ρ este tranzitivă dacă şi numai dacă

$$\rho^2 \subset \rho.$$

Definiţia 52. Spunem că ρ este **totală** dacă $\rho \cup \rho^{-1} = A \times A$.

Observaţia 53. Relaţia $A \times A$ este reflexivă, simetrică, tranzitivă şi totală.

Propoziţia 54. Relaţia ρ este reflexivă (respectiv ireflexivă, simetrică, antisimetrică, tranzitivă, totală) dacă şi numai dacă ρ^{-1} este reflexivă (respectiv ireflexivă, simetrică, antisimetrică, tranzitivă, totală).

Propoziţia 55. Dată fiind o mulţime nevidă $\mathcal{M}$ de relaţii pe mulţimea A, $\bigcap_{\rho\in\mathcal{M}} \rho$ este o relaţie pe A. Dacă toate relaţiile din $\mathcal{M}$ sunt reflexive (respectiv ireflexive, simetrice, antisimetrice, tranzitive) atunci $\bigcap_{\rho\in\mathcal{M}} \rho$ este reflexivă (respectiv ireflexivă[4], simetrică, antisimetrică, tranzitivă).

Observaţia 56. Dacă relaţia ρ este ireflexivă şi dacă $\sigma \subset \rho$, atunci şi σ este ireflexivă.

8. ÎNCHIDERI ALE RELAŢIILOR

În lipsa vreunei menţiuni contrare, în acest capitol ρ va desemna o relaţie pe o mulţime nevidă A.

Propoziţia 57. Dată fiind o relaţie ρ pe mulţimea A, există o relaţie σ pe mulţimea A cu proprietăţile:
(i) $\rho \subset \sigma$
(ii) σ este reflexivă.
(iii) Dacă pentru o altă relaţie reflexivă $\tau \in \mathcal{R}(A)$ avem $\rho \subset \tau$, atunci[5] $\sigma \subset \tau$.
În plus, σ cu aceste proprietăţi este unic determinată.

Demonstraţie: Pentru partea de existenţă, definim $\sigma = \rho \cup \Delta_A$.
Evident, $\rho \subset \sigma$ şi σ este reflexivă.
Dacă $\tau \in \mathcal{R}(A)$ este reflexivă (adică, conţine Δ_A) şi conţine ρ, atunci τ va conţine şi $\Delta_A \cup \rho = \sigma$.
Pentru demonstrarea unicităţii lui σ, să considerăm σ_1 şi σ_2 cu proprietăţile din enunţ. Atunci, conform (iii), $\sigma_1 \subset \sigma_2$ şi $\sigma_2 \subset \sigma_1$, de unde $\sigma_1 = \sigma_2$. □

Definiţia 58. Relaţia a cărei existenţă este asigurată de propoziţia 57 se numeşte **închiderea reflexivă** a lui ρ.

Vom nota închiderea reflexivă a lui ρ cu $R(\rho)$.

[4]În cazul ireflexivităţii, deşi afirmaţia prezentei propoziţii este adevărată, ea nu dă foare multă informaţie. În această situaţie, informaţie mai relevantă ne oferă observaţia 56.

[5]În limbajul pe care îl vom introduce la relaţii de ordine, aceste condiţii spun că „σ este o relaţie reflexivă minimală care conţine ρ”.

Corolarul 59. $R(\rho) = \rho \cup \Delta_A$.

Propoziţia 60. $R(\rho) \bigcap_{\substack{\tau \in \mathcal{R}(A) \\ \tau \text{ e reflexivă}}} \tau$.

Propoziţia 61. Dată fiind o relaţie ρ pe mulţimea A, există o relaţie σ pe mulţimea A cu proprietăţile:
(i) $\rho \subset \sigma$
(ii) σ este simetrică.
(iii) Dacă pentru o altă relaţie simetrică $\tau \in \mathcal{R}(A)$ avem $\rho \subset \tau$, atunci $\sigma \subset \tau$.
În plus, σ cu aceste proprietăţi este unic determinată.

Demonstraţie: Pentru partea de existenţă, definim $\sigma = \rho \cup \rho^{-1}$.
Evident, $\rho \subset \sigma$ şi σ este simetrică.
Dacă $\tau \in \mathcal{R}(A)$ este simetrică (deci $\tau = \tau^{-1}$) şi conţine ρ, atunci, conform observaţiei 41, τ va conţine şi ρ^{-1}, de unde $\tau \supset \sigma$.
Pentru demonstrarea unicităţii lui σ, să considerăm σ_1 şi σ_2 cu proprietăţile din enunţ. Atunci, conform (iii), $\sigma_1 \subset \sigma_2$ şi $\sigma_2 \subset \sigma_1$, de unde $\sigma_1 = \sigma_2$. □

Definiţia 62. Relaţia a cărei existenţă este asigurată de propoziţia 57 se numeşte **închiderea simetrică** a lui ρ.

Vom nota închiderea reflexivă a lui ρ cu $S(\rho)$.

Corolarul 63. $S(\rho) = \rho \cup \rho^{-1}$.

Propoziţia 64. $S(\rho) = \bigcap_{\substack{\tau \in \mathcal{R}(A) \\ \tau \text{ e simetrică}}} \tau$.

Propoziţia 65. Dată fiind o relaţie ρ pe mulţimea A, există o relaţie σ pe mulţimea A cu proprietăţile:
(i) $\rho \subset \sigma$
(ii) σ este tranzitivă.
(iii) Dacă pentru o altă relaţie tranzitivă $\tau \in \mathcal{R}(A)$ avem $\rho \subset \tau$, atunci $\sigma \subset \tau$.
În plus, σ cu aceste proprietăţi este unic determinată.

Demonstraţie: Pentru partea de existenţă, definim $\sigma = \bigcup_{n \in \mathbb{N}^*} \rho^n$.
Evident, $\rho \subset \sigma$ şi σ este tranzitivă.
Dacă $\tau \in \mathcal{R}(A)$ este tranzitivă (deci $\tau^2 \subset \tau$) şi conţine ρ, atunci, conform observaţiei 34, τ va conţine şi ρ^2. Inductiv, obţinem $\tau \supset \rho^n$ pentru orice $n \in \mathbb{N}^*$, de unde $\tau \supset \sigma$.

Pentru demonstrarea unicităţii lui σ, să considerăm σ_1 şi σ_2 cu proprietăţile din enunţ. Atunci, conform (iii), $\sigma_1 \subset \sigma_2$ şi $\sigma_2 \subset \sigma_1$, de unde $\sigma_1 = \sigma_2$. $\square$

Definiţia 66. Relaţia a cărei existenţă este asigurată de propoziţia 57 se numeşte **închiderea tranzitivă** a lui ρ.

Vom nota închiderea reflexivă a lui ρ cu $T(\rho)$.

Corolarul 67. $T(\rho) = \bigcup_{n \in \mathbb{N}^*} \rho^n$.

Propoziţia 68. $T(\rho) = \bigcap_{\substack{\tau \in \mathcal{R}(A) \\ \tau \text{ e tranzitivă}}} \tau$.

Propoziţia 69. Fie ρ o relaţie pe mulţimea A. Atunci:
(i) $R(S(\rho)) = S(R(\rho))$.
(ii) $R(T(\rho)) = T(R(\rho))$.
(iii) $S(T(\rho)) \subset T(S(\rho))$.

Demonstraţie: (i): $R(S(\rho)) = R(\rho \cup \rho^{-1}) = \rho \cup \rho^{-1} \cup \Delta_A = \rho \cup \Delta_A \cup \rho^{-1} \cup \Delta_A = (\rho \cup \Delta_A) \cup (\rho \cup \Delta_A)^{-1} = S(\rho \cup \Delta_A) = S(R(\rho))$.
(ii): Inductiv, $\bigcup_{k=1}^{n} (\rho \cup \Delta_A)^k = \bigcup_{k=1}^{n} \rho^k \cup \Delta_A$ pentru orice $n \in \mathbb{N}^*$. Prin urmare, $R(T(\rho)) = (\bigcup_{n \in \mathbb{N}^*} \rho^n) \cup \Delta_A = \bigcup_{n \in \mathbb{N}^*} (\rho^n \cup \Delta_A) = \bigcup_{n \in \mathbb{N}^*} (\rho \cup \Delta_A)^n = T(R(\rho))$.
(iii): Fie $(a, b) \in S(T(\rho)) = \left(\bigcup_{n \in \mathbb{N}^*} \rho^n \right) \cup \left(\bigcup_{n \in \mathbb{N}^*} \rho^n \right)^{-1}$. Atunci există $n \in \mathbb{N}^*$ şi $c_0 = a, c_1, \ldots, c_n = b$ astfel încât $(c_{i-1}, c_i) \in \rho$ pentru orice $i \in \{1, 2, \ldots, n\}$ sau există $n \in \mathbb{N}^*$ şi $d_0 = b, d_1, \ldots, d_n = a$ astfel încât $(d_{i-1}, d_i) \in \rho$ pentru orice $i \in \{1, 2, \ldots, n\}$. Este însă clar că în oricare din aceste variante avem $(a, b) \in \bigcup_{n \in \mathbb{N}^*} (\rho \cup \rho^{-1})^n = T(S(\rho))$. $\square$

Observaţia 70. Nu putem afirma că are loc relaţia $S(T(\rho)) = T(S(\rho))$: Dacă, de exemplu, definim pe $\{1, 2\}$ relaţia $\{(1, 2)\}$, constatăm că $(1, 1) \in T(S(\rho)) \setminus S(T(\rho))$.

9. Relaţii de echivalenţă. Mulţimi factor

Definiţia 71. Fie ρ o relaţie pe mulţimea nevidă A. ρ se numeşte **relaţie de echivalenţă** dacă este reflexivă, simetrică şi tranzitivă.

Propoziţia 72. Dată fiind o mulţime $\mathcal{M}$ de relaţii de echivalenţă pe mulţimea A, intersecţia lor este relaţie de echivalenţă pe A.

Demonstraţie: Afirmaţia este o consecinţă imediată a propoziţiei 55. □

Definiţia 73. Dată fiind o relaţie ρ pe mulţimea A, intersecţia tuturor relaţiilor de echivalenţă pe A care conţin ρ se numeşte **relaţia de echivalenţă generată de** ρ.

Observaţia 74. Relaţia de echivalenţă generată de ρ este cea mai mică (în sensul incluziunii) relaţie de echivalenţă pe A care conţine ρ.

Propoziţia 75. Relaţia de echivalenţă generată de ρ este egală cu $\bigcup_{n\in\mathbb{N}^*} (\rho \cup \rho^{-1} \cup \Delta_A)^n$.

Demonstraţie: Notăm cu σ relaţia din enunţ. Întrucât $\sigma = T(R(S(\rho)))$, ea este tranzitivă. Cum $\Delta_A \subset \sigma$, σ este reflexivă. Definiţia lui σ arată clar şi simetria acesteia. Deci, σ este relaţie de echivalenţă. Evident, $\rho \subset \sigma$. Dacă considerăm o relaţie de echivalenţă τ pe A cu $\rho \subset \tau$, atunci τ, fiind reflexivă şi simetrică, conţine $R(S(\rho)) = \rho \cup \rho^{-1} \cup \Delta$. Cum însă τ este şi tranzitivă, ea trebuie să conţină şi închiderea tranzitivă a acesteia, adică pe σ. □

Definiţia 76. Fie ρ o relaţie de echivalenţă pe mulţimea nevidă A şi $a \in A$. Prin **clasa de echivalenţă a lui** a **în raport cu** ρ înţelegem mulţimea $\{b \in A : b \rho a\}$.

Vom nota clasa de echivalenţă a lui a în raport cu ρ prin $\frac{a}{\rho}$ sau $\hat{a}$. Vor exista de asemenea situaţii în care în locul acestor notaţii se vor folosi unele adaptate contextului.

Propoziţia 77. Dacă ρ este o relaţie de echivalenţă pe mulţimea A, iar $a, b \in A$, atunci $\hat{a} = \hat{b}$ sau $\hat{a} \cap \hat{b} = \emptyset$.

Demonstraţie: Dacă $a \rho b$, atunci $c \in \hat{a} \Leftrightarrow c \rho a \overset{b\rho a}{\Leftrightarrow} c \rho b \Leftrightarrow c \in \hat{b}$. Prin urmare, $\hat{a} = \hat{b}$.
Dacă $a \not\rho b$, să presupunem că există $c \in \hat{a} \cap \hat{b}$. Atunci $a \rho c$ şi $c \rho b$, de unde $a \rho b$, contradicţie. Rămâne deci că $\hat{a} \cap \hat{b} = \emptyset$. □

Definiţia 78. Numim **partiţie** a mulţimii nevide A orice mulţime $\mathcal{M}$ de submulţimi nevide ale lui A cu proprietăţile:
1. $A = \bigcup_{B\in\mathcal{M}} B$.
2. Pentru orice $B, C \in \mathcal{M}$ cu $B \neq C$ avem $B \cap C = \emptyset$.

Observaţia 79. Propoziţia 77 se reformulează cu ajutorul noţiunii de partiţie astfel: „Mulţimea claselor de echivalenţă determinate de o relaţie de echivalenţă pe o mulţime A constituie o partiţie a lui A".

Definiţia 80. Fie ρ o relaţie de echivalenţă pe mulţimea A. Notăm $\frac{A}{\rho}$ şi numim **mulţimea factor (cât)** a lui A în raport cu ρ mulţimea tuturor claselor de echivalenţă ale elementelor lui A în raport cu ρ.

Observaţia 81. Fie ρ o relaţie de echivalenţă pe mulţimea A. Funcţia $\pi : A \to \frac{A}{\rho}$, $\pi(a) = \hat{a}$ este surjectivă.

Definiţia 82. Fie ρ o relaţie de echivalenţă pe mulţimea A. Funcţia din observaţia 81 numeşte **surjecţia canonică** (sau **proiecţia canonică**) **a mulţimii factor** $\frac{A}{\rho}$.

Definiţia 83. Fie ρ o relaţie de echivalenţă pe mulţimea A. O submulţime $\mathcal{S}$ a lui A se numeşte **sistem complet şi independent de reprezentanţi (pentru elementele mulţimii A) relativ la relaţia** ρ dacă îndeplineşte condiţiile:
1. Pentru orice două elemente distincte $s, t \in \mathcal{S}$ avem $s \not\rho t$.
2. Orice element al lui A este echivalent cu un element al lui $\mathcal{S}$.

Observaţia 84. În cuvinte, dată fiind o relaţie de echivalenţă pe o mulţime A, un sistem complet şi independent de reprezentanţi relativ la ρ este o submulţime a lui A alcătuită cu câte exact un element din fiecare clasă de echivalenţă.

Observaţia 85. Dacă ρ este o relaţie de echivalenţă pe mulţimea A iar $\mathcal{S}$ este un sistem complet şi independent de reprezentanţi relativ la ρ, atunci funcţia $f : \mathcal{S} \to \frac{A}{\rho}$, $f(s) = \hat{s}$ este bijectivă.

9.1. **Exemple importante de relaţii de echivalenţă.**

9.1.1. *Egalitatea.*

Exemplul 86. Dată fiind o mulţime nevidă, relaţia de egalitate pe aceasta este o relaţie de echivalenţă.

Observaţia 87. Unicul sistem complet şi independent de reprezentanţi pentru relaţia de egalitate pe mulţimea A este chiar A.

9.1.2. *Congruenţa modulo n.*

Fie $n \in \mathbb{Z}$. Considerăm pe mulţimea $\mathbb{Z}$ relaţia ρ_n dată astfel: $a \rho_n b \overset{\text{def}}{\Leftrightarrow} n | b - a$.

Definiţia 88. Relaţia ρ_n se numeşte relaţia de **congruenţă modulo n.**

Observaţia 89. Pentru orice $n \in \mathbb{Z}$ avem $\rho_{-n} = \rho_n$.

Notaţie: În mod tradiţional faptul că numerele întregi a şi b sunt congruente modulo n se notează $a \equiv b \pmod{n}$. Începând din momentul de faţă vom folosi şi noi această notaţie, renunţând la provizoriul ρ_n.

Propoziţia 90. Pentru orice $n \in \mathbb{Z}$ relaţia de congruenţă modulo n este o relaţie de echivalenţă.

Demonstraţie: Fie $n, a, b, c \in \mathbb{Z}$.
Evident, $n|0 = a-a$, de unde $a \equiv a \pmod{n}$, deci relaţia de congruenţă modulo n este reflexivă.
Dacă $a \equiv b \pmod{n}$, atunci $n|b-a$, de unde $n|-(b-a) = a-b$, deci $b \equiv a \pmod{n}$. Prin urmare, relaţia în discuţie este simetrică.
Dacă $a \equiv b \pmod{n}$ şi $b \equiv c \pmod{n}$, atunci $n|b-a$ şi $n|c-b$. De aici, $n|(b-a)+(c-b) = c-a$, deci $a \equiv c \pmod{n}$. Prin urmare, relaţia de congruenţă modulo n este tranzitivă. □

Observaţia 91. Fie $n \in \mathbb{N}^*$. Atunci:
a) Clasa de congruenţă modulo n a elementului $a \in \mathbb{Z}$ este $a + n\mathbb{Z}$ (ea constă în elementele care dau acelaşi rest ca şi a la împărţirea prin n).
b) $\dfrac{\mathbb{Z}}{\equiv \pmod{n}} = \{\widehat{0}, \widehat{1}, \ldots, \widehat{n-1}\} = \{n\mathbb{Z}, n\mathbb{Z}+1, \ldots, n\mathbb{Z}+n-1\}$.
c) Sistemul complet şi independent de reprezentanţi cel mai frecvent folosit în context este $\{0, 1, \ldots, n-1\}$; el este alcătuit din resturile ce se pot obţine împărţind numerele întregi la n.

Observaţia 92. Congruenţa modulo 0 este de fapt egalitatea pe $\mathbb{Z}$. Prin urmare, conform observaţiilor 85 şi 87, $\dfrac{\mathbb{Z}}{\equiv \pmod{0}}$ este în bijecţie cu $\mathbb{Z}$.

Definiţia 93. Mulţimea factor a lui $\mathbb{Z}$ în raport cu congruenţa modulo n se numeşte **mulţimea claselor de resturi modulo** n.

Vom folosi notaţia[6] $\mathbb{Z}_n$ pentru a desemna mulţimea claselor de resturi modulo n.

9.1.3. *Relaţia de echivalenţă asociată unei partiţii.* Fie $\mathcal{P}$ o partiţie a mulţimii nevide A. Definim pe A relaţia

$$a \sim_{\mathcal{P}} b \overset{\text{def}}{\Leftrightarrow} \exists B \in \mathcal{P} \quad a, b \in B.$$

Propoziţia 94. Relaţia $\sim_{\mathcal{P}}$ este de echivalenţă pe A.

[6] În teoria numerelor, această notaţie este rezervată mulţimii întregilor n-adici (în situaţia în care n este număr prim). În acel context, inelul claselor de resturi modulo n se notează $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sau $\dfrac{\mathbb{Z}}{(n)}$. Noi nu ne vom întâlni cu această situaţie la cursul de Algebră, deci notaţia este neechivocă.

Temă: Demonstraţi propoziţia 94!

Definiţia 95. Relaţia $\sim_{\mathcal{P}}$ se numeşte **relaţia de echivalenţă asociată partiţiei** $\mathcal{P}$.

Propoziţia 96. Dată fiind o mulţime nevidă A, mulţimea relaţiilor de echivalenţă pe A şi mulţimea partiţiilor lui A sunt în corespondenţă bijectivă.

Demonstraţie: Considerăm funcţia Φ care asociază fiecărei relaţii de echivalenţă pe A partiţia lui A în clasele de echivalenţă relative la relaţia respectivă. Considerăm de asemenea funcţia Ψ care asociază fiecărei partiţii $\mathcal{P}$ a lui A relaţia $\sim_{\mathcal{P}}$. Atunci Φ şi Ψ sunt inverse una celeilalte (lăsăm detaliile în seama cititorului). □

9.1.4. *Relaţia de echivalenţă asociată unei funcţii.* Considerăm mulţimile nevide A şi B şi funcţia $f : A \to B$. Definim în acest context relaţia

$$a_1 \rho_f a_2 \overset{\text{def}}{\Leftrightarrow} f(a_1) = f(a_2).$$

Propoziţia 97. Relaţia ρ_f este de echivalenţă.

Temă: Demonstraţi propoziţia 97!

Relaţia ρ_f ne permite să prezentăm un rezultat foarte util pentru definirea de funcţii pe mulţimi factor:

Teorema 98. (Proprietatea de universalitate a mulţimii factor) Fie ρ o relaţie de echivalenţă pe mulţimea A, $\pi : A \to \dfrac{A}{\rho}$ surjecţia canonică, $f : A \to B$ o funcţie şi ρ_f relaţia de echivalenţă asociată acesteia.
i) Dacă $\rho \subset \rho_f$, atunci există $u : \dfrac{A}{\rho} \to B$ astfel încât $u \circ \pi = f$.
ii) u este injectivă dacă şi numai dacă $\rho = \rho_f$.
iii) u este surjectivă dacă şi numai dacă f este surjectivă.

10. RELAŢII DE ORDINE

Este imediat faptul că relaţia uzuală de ordine pe $\mathbb{R}$ este reflexivă, antisimetrică şi tranzitivă. Aceasta ne sugerează

Definiţia 99. Fie A o mulţime nevidă şi ρ o relaţie pe A. Spunem că ρ este o **relaţie de ordine** dacă ea este reflexivă, antisimetrică şi tranzitivă.

Definiţia 100. Numim **mulţime ordonată** orice pereche alcătuită dintr-o mulţime nevidă şi o relaţie de ordine pe aceasta.

Vom folosi în cele ce urmează, în acord cu uzanţele, semnul $\leq$ (sau semne asemănătoare, ca de pildă $\preceq$) pentru relaţiile de ordine (chiar dacă este vorba de alte relaţii decât cea de ordine naturală de pe $\mathbb{R}$).

Observaţia 101. Relaţia de ordine uzuală pe $\mathbb{R}$ este, desigur, o relaţie de ordine conform definiţiei 99. Pe de altă parte, vom constata în cele ce urmează că în categoria relaţiilor de ordine se vor încadra şi alte relaţii frecvent întâlnite (iar statutul de relaţie de ordine al unora dintre acestea va fi la o primă vedere chiar surprinzător).

Exemplul 102. Dată fiind o mulţime nevidă, relaţia de egalitate pe aceasta este o relaţie de ordine.

Exemplul 103. Dată fiind o mulţime nevidă, relaţia de incluziune pe $\mathcal{P}(A)$ este o relaţie de ordine.

Exemplul 104. Relaţia de divizibilitate pe $\mathbb{N}$ este o relaţie de ordine.

Exemplul 105. Relaţia de divizibilitate pe $\mathbb{Z}$ nu este o relaţie de ordine.

Exemplul 106. Relaţia definită pe $\mathbb{Z}$ prin $x < y$ nu este o relaţie de ordine.

Temă: Argumentaţi afirmaţiile de la exemplele 102, 103, 104, 105 şi 106!

Definiţia 107. Date fiind două mulţimi ordonate $(A, \leq)$ şi $(B, \preceq)$, o funcţie $f : A \to B$ se numeşte **morfism de mulţimi ordonate** dacă $\forall x, y \in A \quad x \leq y \Rightarrow f(x) \preceq f(y)$. f se numeşte **antimorfism de mulţimi ordonate** dacă $\forall x, y \in A \quad x \leq y \Rightarrow f(x) \succeq f(y)$.

Definiţia 108. Un (anti)morfism de mulţimi ordonate se numeşte **(anti)izomorfism de mulţimi ordonate** dacă este inversabil şi dacă inversul său este (anti)morfism de mulţimi ordonate.

Definiţia 109. Două mulţimi ordonate se numesc **(anti)izomorfe** dacă există un (anti)izomorfism între ele.

11. RELAŢII ÎNRUDITE CU RELAŢIILE DE ORDINE

Relaţiile de la exemplele 105 şi 106 sugerează următoarele definiţii:

Definiţia 110. Fie A o mulţime nevidă şi ρ o relaţie pe A. Spunem că ρ este o **relaţie de preordine** (sau **de cuasiordine**) dacă ea este reflexivă şi tranzitivă.

Observaţia 111. Orice relaţie de ordine este şi relaţie de preordine.

Observaţia 112. Relaţia de divizibilitate pe $\mathbb{Z}$ este o relaţie de preordine.

Definiţia 113. Numim **mulţime preordonată** orice pereche alcătuită dintr-o mulţime nevidă şi o relaţie de preordine pe aceasta.

Definiţia 114. Fie A o mulţime nevidă şi ρ o relaţie pe A. Spunem că ρ este o **relaţie de ordine strictă** dacă ea este ireflexivă şi tranzitivă.

Dată fiind o relaţie de preordine ρ pe mulţimea A, ei i se poate asocia o relaţie de ordine (definită pe o mulţime factor a lui A) în următorul mod:
Considerăm pe A relaţia $a\sigma b \overset{def}{\Leftrightarrow} a\rho b \wedge b\rho a$.
Este imediat faptul că σ este o relaţie de echivalenţă pe A.
Pe mulţimea A/σ definim relaţia $\hat{a}\tau\hat{b} \overset{def}{\Leftrightarrow} a\rho b$.
Se verifică (temă!) că τ este (corect definită şi) relaţie de ordine şi că proiecţia canonică $p : A \to A/\sigma$ are proprietatea $\forall a, b \in A$ $a\rho b \Rightarrow p(a)\tau p(b)$.

În ceea ce priveşte relaţiile de ordine strictă, avem:

Propoziţia 115. Dată fiind o mulţime nevidă A, există o bijecţie canonică între mulţimea relaţiilor de ordine pe A şi mulţimea relaţiilor de ordine strictă pe A.

Demonstraţie: Considerăm funcţia Φ ce asociază fiecărei relaţii de ordine ρ pe A relaţia $\rho \setminus \Delta_A$ şi funcţia Ψ ce asociază fiecărei relaţii de ordine strictă σ pe A relaţia $\sigma \cup \Delta_A$. Este imediat că Φ şi Ψ acţionează între mulţimile precizate în enunţ şi că sunt inverse una celeilalte. □

12. TIPURI INTERESANTE DE MULŢIMI ORDONATE

Fie $\leq$ o relaţie de ordine pe mulţimea A.

Definiţia 116. Numim **majorant** al submulţimii nevide B a lui A orice element $a \in A$ cu proprietatea $\forall b \in B$ $b \leq a$.

Definiţia 117. Submulţimea nevidă B a lui A se numeşte **majorată** dacă există în A cel puţin un majorant pentru B.

Definiţia 118. Numim **minorant** al submulţimii nevide B a lui A orice element $a \in A$ cu proprietatea $\forall b \in B$ $a \leq b$.

Definiţia 119. Submulţimea nevidă B a lui A se numeşte **minorată** dacă există în A cel puţin un minorant pentru B.

Definiţia 120. Numim **prim element** (sau **minimum**, sau **cel mai mic element**) al submulţimii nevide B a lui A orice element $a \in B$ cu proprietatea $\forall b \in B \ a \leq b$.

Observaţia 121. Este posibil ca anumite submulţimi ale lui A să nu admită prim element. Dacă însă o submulţime a lui A admite prim element, antisimetria relaţiei $\leq$ arată că acesta este unic.

Vom nota primul element al submulţimii B a lui A cu $\min B$.

Definiţia 122. Numim **ultim element** (sau **maximum**, sau încă **cel mai mare element**) al submulţimii nevide B a lui A orice element $a \in B$ cu proprietatea $\forall b \in B \ b \leq a$.

Observaţia 123. Este posibil ca anumite submulţimi ale lui A să nu admită ultim element. Dacă însă o submulţime a lui A admite ultim element, antisimetria relaţiei $\leq$ arată că acesta este unic.

Vom nota ultimul element al submulţimii B a lui A cu $\max B$.

Definiţia 124. Numim **element minimal** al mulţimii ordonate A orice element a al lui A cu proprieatea $\forall b \in A \ \ b \leq a \Rightarrow b = a$.

Definiţia 125. Numim **element maximal** al mulţimii ordonate A orice element a al lui A cu proprieatea $\forall b \in A \ \ b \geq a \Rightarrow b = a$.

Definiţia 126. Spunem că mulţimea ordonată $(A, \leq)$ este **total ordonată** dacă relaţia $\leq$ este totală.

Definiţia 127. Spunem că mulţimea ordonată $(A, \leq)$ este **bine ordonată** dacă orice submulţime nevidă a lui A admite prim element.

Definiţia 128. Spunem că mulţimea ordonată $(A, \leq)$ este **inductiv ordonată** dacă orice parte total ordonată a sa este majorată.

Definiţia 129. Numim **supremum** al submulţimii nevide şi majorate B a lui A cel mai mic majorant (din A) al lui B.

Observaţia 130. Este posibil ca anumite submulţimi ale lui A să nu admită supremum. Dacă însă o submulţime a lui A admite supremum, acesta este unic conform observaţiei 121.

Vom nota cu $\sup B$ supremumul submulţimii B a lui A.

Definiţia 131. Numim **infimum** al submulţimii nevide şi minorate B a lui A cel mai mare minorant (din A) al lui B.

Observaţia 132. Este posibil ca anumite submulţimi ale lui A să nu admită infimum. Dacă însă o submulţime a lui A admite infimum, acesta este unic conform observaţiei 123.

Vom nota cu $\inf B$ infimumul submulţimii B a lui A.

Definiţia 133. Mulţimea ordonată $(A, \leq)$ se numeşte **latice** dacă pentru orice $a, b \in A$ există $\inf\{a, b\}$ şi $\sup\{a, b\}$.

Definiţia 134. Mulţimea ordonată $(A, \leq)$ se numeşte **latice completă** dacă pentru orice submulţime nevidă B a lui A există $\inf B$ şi $\sup B$.

Bibliografie

[1] T. Dumitrescu, *Algebra*, Ed. Universităţii din Bucureşti, 2006.
[2] P. Halmos, *Naive set theory*, Springer Verlag, 1960.
[3] C. Năstăsescu, C. Niţă, C. Vraciu, *Bazele algebrei*, Ed. Academiei, Bucureşti, 1986.
[4] C. Năstăsescu, *Introducere în teoria mulţimilor*, Ed. Didactică şi Pedagogică, Bucureşti, 1974.

CURSUL 6: NUMERE CARDINALE

G. MINCU

1. Numere cardinale

Aşa cum am precizat încă de la al doilea curs, considerarea unei mulţimi a tuturor mulţimilor conduce la paradoxuri. Vom conveni că toate mulţimile alcătuiesc un alt tip de entitate, pe care o vom numi **clasă**. Fără a intra în detalii tehnice, vom considera că definiţiile pe care le-am dat pentru relaţiile de ordine şi relaţiile de echivalenţă pot fi utilizate şi în contextul claselor.

Definim relaţia $\sim$ între două mulţimi astfel: $A \sim B$ dacă şi numai dacă există o funcţie bijectivă de la A la B.

Propoziţia 1. Relaţia $\sim$ este de echivalenţă.

Temă: Demonstraţi propoziţia 1!

Definiţia 2. Dacă pentru mulţimile A şi B avem $A \sim B$, unde $\sim$ este relaţia introdusă mai sus, spunem că A şi B sunt **cardinal echivalente** sau **echipotente**.

Definiţia 3. Clasa de echivalenţă cardinală a unei mulţimi A se numeşte **numărul cardinal al lui** A. În acest text, vom folosi pentru numărul cardinal al mulţimii A notaţiile $|A|$ sau Card A.

Definiţia 4. O mulţime se numeşte **numărabilă** dacă ea este cardinal echivalentă cu $\mathbb{N}$.

Definiţia 5. O mulţime se numeşte **cel mult numărabilă** dacă ea este finită sau numărabilă.

Definiţia 6. O mulţime se numeşte **nenumărabilă** dacă nu este cel mult numărabilă.

Vom nota numărul cardinal al mulţimii $\mathbb{N}$ cu $\aleph_0$, iar numărul cardinal al mulţimii $\mathbb{R}$ cu $\mathfrak{c}$.

Propoziţia 7. Mulţimea $\mathbb{Z}$ este numărabilă.

Demonstraţie: Funcţia $f : \mathbb{N} \to \mathbb{Z}$ care trimite numerele pare în jumătăţile lor, iar pe cele impare în numerele întregi negative, luate la rând, începând cu -1 şi în ordine descrescătoare este bijectivă. Lăsăm verificările calculatorii în grija cititorului. $\square$

2. inegalitatăţi pentru numere cardinale

Definim pe clasa numerelor cardinale relaţia $|A| \preceq |B|$ dacă şi numai dacă există o funcţie injectivă $f : A \to B$. Vom scrie $|A| \prec |B|$ dacă $|A| \preceq |B|$ şi $|A| \neq |B|$.

Observaţia 8. Relaţia $\preceq$ este corect definită deoarece dacă $f : A \to B$ este injectivă, $|A| = |A'|$, iar $|B| = |B'|$, atunci există funcţii bijective $\alpha : A \to A'$ şi $\beta : B \to B'$; în consecinţă, $\beta \circ f \circ \alpha^{-1} : A' \to B'$ este injectivă.

Observaţia 9. Deoarece pentru orice mulţime funcţia sa identică este injectivă, relaţia $\preceq$ este reflexivă.

Observaţia 10. Deoarece compusa oricăror două funcţii injective este injectivă, relaţia $\preceq$ este tranzitivă.

Teorema 11. (Cantor, Bernstein, Schröder)
Fie două mulţimi A şi B. Dacă există funcţiile injective $f : A \to B$ şi $g : B \to A$, atunci există o funcţie bijectivă $h : A \to B$.

Corolarul 12. Relaţia $\preceq$ este antisimetrică.

Cele precedente demonstrează

Propoziţia 13. Relaţia $\preceq$ este de ordine.

Utilizând cele precedente, putem proba:

Propoziţia 14. Mulţimea $\mathbb{Q}$ este numărabilă.

Temă: Demonstraţi propoziţia 14 utilizând eventual funcţia $f : \mathbb{Q} \to \mathbb{Z}$, $f\left(\frac{a}{b}\right) = \operatorname{sgn} a \cdot 2^{|a|} \cdot 3^b$, unde $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, $(a, b) = 1$.

Propoziţia 15. Mulţimile $\mathbb{R}$ şi $\mathbb{C}$ sunt nenumărabile.

3. operaţii cu numere cardinale

3.1. **Înmulţirea numerelor cardinale.** Observaţia că pentru $|A| = a \in \mathbb{N}$ şi $|B| = b \in \mathbb{N}$ avem $|A \times B| = ab$ ne sugerează:

Definiţia 16. Prin **produsul** numerelor cardinale $\alpha = |A|$ şi $\beta = |B|$ înţelegem numărul cardinal $\alpha\beta \stackrel{\text{def}}{=} |A \times B|$.

Definiţia 16 este corectă în virtutea observaţiei următoare:

Observaţia 17. Dacă $|A| = |A'|$ şi $|B| = |B'|$, atunci $|A \times B| = |A' \times B'|$.

Demonstraţie: Date fiind bijecţiile $f : A \to A'$ şi $g : B \to B'$, funcţia $f \times g : A \times B \to A' \times B'$, $f \times g\,(a, b) = (f(a), g(b))$ este bijecţie (temă!). Prin urmare, $|A \times B| = |A' \times B'|$. $\square$

3.2. **Ridicarea la putere a numerelor cardinale.** Observaţia că pentru $|A| = a \in \mathbb{N}$ şi $|B| = b \in \mathbb{N}$ avem $|\{f : A \to B\}| = b^a$ ne-a condus în cursul 2 la notaţia $B^A = \{f : A \to B\}$. În contextul discuţiei de faţă, ea ne sugerează:

Definiţia 18. Date fiind numerele cardinale $\alpha = |A|$ şi $\beta = |B|$,

$$\beta^\alpha \stackrel{\text{def}}{=} |B^A|.$$

Definiţia 18 este corectă în virtutea observaţiei următoare:

Observaţia 19. Dacă $|A| = |A'|$ şi $|B| = |B'|$, atunci $|B^A| = |(B')^{A'}|$.

Demonstraţie: Date fiind bijecţiile $f : A \to A'$ şi $g : B \to B'$, funcţia $h : B^A \to (B')^{A'}$, $h(\varphi) = g \circ \varphi \circ f^{-1}$ este bijecţie (temă!). Prin urmare, $|B^A| = |(B')^{A'}|$. $\square$

3.3. **Adunarea numerelor cardinale.** Ordinea întrucâtva nefirească a prezentării operaţiilor cu numere cardinale este cauzată de faptul că, în timp ce pentru înmulţirea şi ridicarea la putere a numerelor cardinale am putut utiliza operaţii binecunoscute cu mulţimi, pentru adunare sunt necesare câteva pregătiri. Începem prin a constata că, dacă $|A| = a \in \mathbb{N}$, $|B| = b \in \mathbb{N}$ şi $A \cap B = \emptyset$, atunci $|A \cup B| = a + b$, relaţia nerămânând valabilă dacă $A \cap B \neq \emptyset$.

Este instructiv să precizăm în acest punct, abătându-ne un moment de la direcţia prezentării, că în condiţiile descrise mai sus avem

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Această relaţie se generalizează după cum urmează:

Propoziţia 20 (Principiul includerii şi excluderii). Fie $n \in \mathbb{N}^*$ şi mulţimile finite $A_1, A_2, \ldots, A_n$. Atunci

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \tag{1}$$

$$+ \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| + \ldots + (-1)^{n-1} |A_1 \cap A_2 \cap \ldots \cap A_n|.$$

Demonstraţie: Fie $x \in A_1 \cup A_2 \cup \ldots \cup A_n$. Elementul x contribuie cu o unitate la membrul stâng al relaţiei (1). Dacă x se află în m dintre mulţimile $A_1, A_2 \ldots, A_n$, el contribuie la suma din membrul drept al relaţiei (1) cu

$$\mathbf{C}_m^1 - \mathbf{C}_m^2 + \ldots + (-1)^{m-1}\mathbf{C}_m^m = 1 - (1-1)^m,$$

adică tot cu o unitate. □

Revenind acum pe direcţia principală a prezentării, constatăm, inspirându-ne din abordările de la definiţiile operaţiilor de înmulţire şi de ridicare la putere a numerelor cardinale, că ne-ar conveni în acest moment să avem la dispoziţie o operaţie cu mulţimi care să asocieze la două mulţimi date nu reuniunea lor, ci mai degrabă reuniunea a două mulţimi cardinal echivalente cu ele şi disjuncte. Aceste consideraţii conduc la:

Definiţia 21. Prin reuniunea disjunctă a mulţimilor A şi B înţelegem mulţimea $A \sqcup B \stackrel{\text{def}}{=} (A \times \{1\}) \cup (B \times \{2\})$.

Observaţia 22. (i) $f : A \to A \times \{1\}$, $f(a) = (a, 1)$ şi $g : B \to B \times \{2\}$, $g(b) = (b, 2)$ sunt bijective, deci $|A \times \{1\}| = |A|$ şi $|B \times \{2\}| = |B|$.
(ii) Evident, $(A \times \{1\}) \cap (B \times \{2\}) = \emptyset$.

Definiţia 23. Date fiind numerele cardinale $\alpha = |A|$ şi $\beta = |B|$,

$$\alpha + \beta \stackrel{\text{def}}{=} |A \sqcup B|.$$

Definiţia 23 este corectă în virtutea observaţiei următoare:

Observaţia 24. Dacă $|A| = |A'|$ şi $|B| = |B'|$, atunci $|A \sqcup B| = |A \sqcup B'|$.

Demonstraţie: Date fiind bijecţiile $f : A \to A'$ şi $g : B \to B'$, funcţia

$$h : A \sqcup B \to A' \sqcup B', \quad h(x) = \begin{cases} (f(a), 1) & \text{dacă} \quad x = (a, 1) \\ (g(b), 2) & \text{dacă} \quad x = (b, 2) \end{cases}$$

este bijecţie (temă!). Prin urmare, $|A \sqcup B| = |A \sqcup B'|$. □

4. CATEVA PROPRIETĂŢI ALE OPERAŢIIOR CU NUMERE CARDINALE

Prezentăm aici câteva proprietăţi ale operaţiilor cu numere cardinale definite în capitolul precedent. Cu două excepţii, marcate cu asterisc, ele sunt uşor de demonstrat şi vi le propunem ca temă. Menţionăm şi că bună parte dintre aceste proprietăţi pot fi enunţate şi demonstrate în forme mult mai generale; trimitem cititorul interesat, de pildă, la [4].

Propoziţia 25. (i) $\aleph_0 + \aleph_0 = \aleph_0$.
(ii) $\aleph_0 \cdot \aleph_0 = \aleph_0$.
(iii) $\mathfrak{c} = 2^{\aleph_0}$.
(iv) $\mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$.
(v) $\mathfrak{c}^{\aleph_0} = \mathfrak{c}$.
(vi) $\mathfrak{c} + \mathfrak{c} = \mathfrak{c}$.
(vii) $\aleph_0 \cdot \mathfrak{c} = \mathfrak{c}$.
(viii) $\aleph_0^{\aleph_0} = \mathfrak{c}$.

Corolarul 26. $|\mathbb{C}| = \mathfrak{c} = |\mathbb{R}|$.

Propoziţia 27. Date fiind numerele cardinale α, β, γ au loc relaţiile:
(i) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.
(ii) $\alpha + \beta = \beta + \alpha$.
(iii) $\alpha + 0 = \alpha$.
(iv)* Dacă α este infinit, $\alpha + \alpha = \alpha$.

Propoziţia 28. Date fiind numerele cardinale α, β, γ au loc relaţiile:
(i) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.
(ii) $\alpha\beta = \beta\alpha$.
(iii) $\alpha \cdot 0 = 0$.
(iv) $\alpha \cdot 1 = \alpha$.
(v)* Dacă α este infinit, $\alpha \cdot \alpha = \alpha$.
(vi) $\alpha(\beta + \gamma) = (\alpha\beta) + (\alpha\gamma)$.

Propoziţia 29. Date fiind numerele cardinale α, β, γ au loc relaţiile:
(i) $\alpha^{\beta+\gamma} = (\alpha^{\beta})(\alpha^{\gamma})$.
(ii) $(\alpha\beta)^{\gamma} = (\alpha^{\gamma})(\beta^{\gamma})$.
(iii) $(\alpha^{\beta})^{\gamma} = \alpha^{\beta\gamma}$.
(iv) $\alpha^0 = 1$.
(v) $\alpha^1 = \alpha$.

5. NUMERELE CARDINALE NU CONSTITUIE O MULŢIME

Teorema 30 (**Cantor**). Pentru orice mulţime A avem $\mathcal{P}(A) \nsim A$.

Demonstraţie: Presupunem că $\mathcal{P}(A) \sim A$. Există deci o bijecţie $f : A \to \mathcal{P}(A)$. Notăm $M = \{a \in A : a \notin f(a)\}$; fie $m \in A$ astfel încât $f(m) = M$ (există, căci f e surjectivă!).
Dacă $m \in M$, atunci $m \notin f(m) = M$, contradicţie.
Dacă $m \notin M$, atunci $m \in f(m) = M$, contradicţie.
Rămâne aşadar că $\mathcal{P}(A) \nsim A$. □

Corolarul 31. Pentru orice număr cardinal α are loc relaţia $\alpha \prec 2^{\alpha}$.

Teorema 32. Numerele cardinale nu constituie o mulţime.

Demonstraţie: Presupunem că numerele cardinale constituie o mulţime, fie ea $\mathcal{M}$. Notăm cu R reuniunea mulţimii formate din câte un reprezentant al fiecărui element al lui $\mathcal{M}$. Atunci $2^{|R|}$ este un număr cardinal şi avem relaţiile $2^{|R|} \preceq |R| \prec 2^{|R|}$, contradicţie. $\square$

References

[1] T. Dumitrescu, *Algebra*, Ed. Universităţii din Bucureşti, 2006.
[2] P. Halmos, *Naive set theory*, Springer Verlag, 1960.
[3] C. Năstăsescu, C. Niţă, C. Vraciu, *Bazele algebrei*, Ed. Academiei, Bucureşti, 1986.
[4] C. Năstăsescu, *Introducere în teoria mulţimilor*, Ed. Didactică şi Pedagogică, Bucureşti, 1974.

CURSUL 7: 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 referire aproape exclusiv la legi de compoziţie binare, le vom numi pe acestea, succint, legi de compoziţie (sau operaţii), subînţelegând epitetul „binare". În situaţia în care în cursurile viitoare vom dori să aducem în discuţie şi altfel de legi de compoziţie, vom menţiona acest lucru în mod explicit la momentul respectiv.

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: $\widehat{a}+\widehat{b} \stackrel{\text{def}}{=} \widehat{a+b}$ şi $\widehat{a}\cdot\widehat{b} \stackrel{\text{def}}{=} \widehat{a\cdot b}$. Pentru a vedea acest lucru, să remarcăm de pildă că dacă $\widehat{a}=\widehat{a'}$ 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 $\forall x,y\in N \quad x\star y\in N$.

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 decât dacă $n = 1$. 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 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 $\mathbf{0}_{m,n}$ 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 I_n 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 $y = y\star e = y\star(x\star z) = (y\star x)\star z = e\star z = z$. □

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. □

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 $(g \circ f)(1_M) = g(f(1_M)) = g(1_{M'}) = 1_{M''}$. □

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 $a_1a_2 \dots a_m \star a'_1a'_2 \dots a'_t \stackrel{\text{def}}{=} a_1a_2 \dots a_ma'_1a'_2 \dots a'_t$.

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 $\lrcorner$.

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

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 $\tilde{f} : FM(A) \to M$, $\tilde{f}(a_1a_2 \dots a_n) = f(a_1)f(a_2) \dots f(a_n)$, $f(\lrcorner) = e$, 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.

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 $G \stackrel{\text{def}}{=} \prod_{i\in I} G_i$ introducem legea de compoziţie

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

Propoziţia 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 $I = \{i_1, i_2, \ldots, i_n\}$ **notaţiile** $\prod_{k=1}^{n} G_{i_k}$ sau $G_{i_1} \times G_{i_2} \times \ldots \times G_{i_n}$.

Definiţia 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. □

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 $S(\{1, 2, \ldots, n\})$; 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. □

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 $x_1 x_2' \in f^{-1}(K)$. □

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: „⇒”: Dacă $x \in \ker f$, $f(x) = e_\Gamma = f(e_G)$; din injectivitatea lui f deducem că $x = e_G$.
„⇐”: 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 $x_1 = x_2$. □

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.

CURSUL 9: SUBGRUP NORMAL. GRUP FACTOR

G. MINCU

1. Relaţii de echivalenţă modulo un subgrup

Fie G un grup şi $H \leq G$. Considerăm următoarele relaţii pe G:
a) $x \equiv_s y \pmod{H}$ dacă şi numai dacă $x^{-1}y \in H$
b) $x \equiv_d y \pmod{H}$ dacă şi numai dacă $xy^{-1} \in H$.

Propoziţia 1. Relaţiile $\equiv_s$ şi $\equiv_d$ sunt de echivalenţă.

Temă: Demonstraţi propoziţia 1!

Definiţia 2. $\equiv_s$ se numeşte **relaţia de echivalenţă la stânga modulo subgrupul H**, iar $\equiv_d$ se numeşte **relaţia de echivalenţă la dreapta modulo subgrupul H**.

Notaţia folosită pentru mulţimea factor a lui G în raport cu $\equiv_s$ este $(G/H)_s$, iar cea pentru mulţimea factor a lui G în raport cu $\equiv_d$ este $(G/H)_d$.

Propoziţia 3. Fie G un grup, $H \leq G$ şi $x \in G$. Atunci:
a) Clasa de echivalenţă a lui x în raport cu $\equiv_s \pmod{H}$ este xH.
b) Clasa de echivalenţă a lui x în raport cu $\equiv_d \pmod{H}$ este Hx.

Demonstraţie: a) $y \in \widehat{x} \Leftrightarrow x^{-1}y \in H \Leftrightarrow y \in xH$.
b) Analog. □

Corolarul 4. $(G/H)_s = \{xH : x \in G\}$, iar $(G/H)_d = \{Hx : x \in G\}$.

Propoziţia 5. Fie G un grup şi $H \leq G$. Atunci $|(G/H)_s| = |(G/H)_d|$.

Demonstraţie: Definim $f : (G/H)_s \to (G/H)_d$, $f(xH) = Hx^{-1}$ şi $g : (G/H)_d \to (G/H)_s$, $g(Hx) = x^{-1}H$.
Dacă $xH = yH$, atunci $x^{-1}y \in H$, deci $x^{-1}(y^{-1})^{-1} \in H$, de unde $Hx^{-1} = Hy^{-1}$. Prin urmare, f este corect definită. Faptul că g este corect definită se probează analog.
Este imediat că f şi g sunt inverse una celeilalte, deci ele sunt bijective, de unde concluzia. □

Definiţia 6. Cardinalul comun al mulţimilor $|(G/H)_s|$ şi $|(G/H)_d|$ se numeşte **indicele lui H în G**.

Vom nota indicele lui H în G cu $[G : H]$.

Definiţia 7. Prin **ordinul** grupului G înţelegem cardinalul lui G. Notaţia folosită în mod uzual pentru ordinul lui G este $|G|$.

Lemma 8. Fie G un grup, $H \leq G$ şi $x \in G$. Atunci $|xH| = |H|$.

Demonstraţie: Definim $f : xH \to H$, $f(t) = x^{-1}t$ şi $g : H \to xH$, $g(h) = xh$.
Este imediat că f şi g sunt corect definite şi inverse una celeilalte, deci ele sunt bijective, de unde concluzia. □

Teorema lui Lagrange Fie G un grup şi $H \leq G$. Atunci $|G| = |H| \cdot [G : H]$.

Demonstraţie: Avem $G = \coprod_{xH \in (G/H)_s} xH$, deci $|G| = \sum_{xH \in (G/H)_s} |xH|$.
Conform lemei 8, din această relaţie obţinem $|G| = |H| \cdot |(G/H)_s|$.
□

Corolarul 9. Ordinul oricărui subgrup al unui grup finit divide ordinul respectivului grup.

2. SUBGRUPURI NORMALE

Propoziţia 10. Fie G un grup şi $H \leq G$. Următoarele afirmaţii sunt echivalente:
i) $(G/H)_s = (G/H)_d$.
ii) Pentru orice $x \in G$ avem $xH = Hx$.
iii) Pentru orice $x \in G$ avem $xHx^{-1} = H$.
iv) Pentru orice $x \in G$ avem $xHx^{-1} \subset H$.

Temă: Demonstraţi propoziţia 10!

Definiţia 11. Fie G un grup şi $H \leq G$. Spunem că H este **subgrup normal** al lui G dacă îndeplineşte una dintre condiţiile echivalente din propoziţia 10.

Vom nota faptul că H este subgrup normal al lui G cu $H \trianglelefteq G$.

Exemplul 12. $\{e\} \trianglelefteq G$, $G \trianglelefteq G$.

Exemplul 13. Pentru orice familie $(H_i)_{i \in I}$ de subgrupuri normale ale lui G avem $\bigcap_{i \in I} H_i \trianglelefteq G$.

Exemplul 14. Orice subgrup al unui grup abelian este normal.

Exemplul 15. Orice subgrup de indice doi al unui grup este normal.

Exemplul 16. Dacă $f : G \to G'$ este un morfism de grupuri, atunci $\ker f \trianglelefteq G$.

Exemplul 16 este un caz particular al următoarei propoziţii, care ne oferă şi o altă clasă de exemple de subgrupuri normale:

Propoziţia 17. Dacă $f : G \to G'$ este un morfism de grupuri, atunci:
a) Pentru orice $K \trianglelefteq G'$ avem $f^{-1}(K) \trianglelefteq G$.
b) Dacă f este surjectiv, atunci pentru orice $H \trianglelefteq G'$ avem $f(H) \trianglelefteq G'$.

Teorema de corespondenţă pentru subgrupuri se completează astfel:

Teorema 18. Fie $f : G \to G'$ un morfism surjectiv de grupuri. Notăm $\mathcal{H} = \{H \leq G : H \supset \ker f\}$ şi $\mathcal{K} = \{K : K \leq G'\}$. 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. În plus, subgrupurile normale ale lui G care conţin $\ker f$ corespund via aceste funcţii subgrupurilor normale ale lui G'.

3. GRUP FACTOR

Observaţia 19. Fie G un grup şi $H \trianglelefteq G$. Atunci pe mulţimea $(G/H)_s$ este corect definită legea de compoziţie $(xH) \cdot (yH) = (xy)H$.

Temă: Demonstraţi observaţia 19!

Definiţia 20. Fie G un grup şi $H \trianglelefteq G$. Prin **grupul factor al lui G în raport cu H** înţelegem grupul care are mulţimea subiacentă $(G/H)_s$ şi legea de compoziţie $(xH) \cdot (yH) = (xy)H$.

Notaţia uzuală pentru grupul factor al lui G în raport cu H este $\frac{G}{H}$. Pentru elementul $xH \in \frac{G}{H}$ vom prefera uneori notaţia $\widehat{x}$. În notaţie aditivă, în loc de xH vom scrie, desigur, $x + H$.

Exemplul 21. $\frac{\mathbb{Z}}{n\mathbb{Z}} = \mathbb{Z}_n$.

Observaţia 22. Fie G un grup şi $H \trianglelefteq G$. Aplicaţia $\pi : G \to \frac{G}{H}$, $\pi(x) = \widehat{x}$ este morfism surjectiv de grupuri.

Definiţia 23. Fie G un grup şi $H \trianglelefteq G$. Morfismul π din observaţia 22 se numeşte **surjecţia canonică** (sau **proiecţia canonică**) a grupului factor $\frac{G}{H}$.

Proprietatea de universalitate a grupului factor. Fie G un grup, $H \trianglelefteq G$, $\pi : G \to \dfrac{G}{H}$ surjecţia canonică şi $f : G \to G'$ un morfism de grupuri. Atunci:

i) Dacă $H \subset \ker f$, atunci există un unic morfism $u : \dfrac{G}{H} \to G'$ astfel încât $u \circ \pi = f$. În plus:

ii) u este injectivă dacă şi numai dacă $H = \ker f$.

iii) u este surjectivă dacă şi numai dacă f este surjectivă.

Temă: Demonstraţi proprietatea de universalitate a grupului factor!

Exemplul 24. Conform proprietăţii de universalitate a grupului factor, proiecţia canonică a lui $\mathbb{Z}$ pe $\mathbb{Z}_4$ induce morfismul de grupuri $u : \mathbb{Z}_{12} \to \mathbb{Z}_4$, $u(\widehat{a}) = \overline{a}$. Pe de altă parte, deoarece $4\mathbb{Z} \not\subset 12\mathbb{Z}$, nu ne aşteptăm ca $v : \mathbb{Z}_4 \to \mathbb{Z}_{12}$, $v(\overline{a}) = \widehat{a}$ să fie morfism de grupuri; verificarea arată că, într-adevăr, v nu este o funcţie corect definită.

4. Teorema fundamentală de izomorfism pentru grupuri

4.1. **Teorema fundamentală de izomorfism pentru grupuri.** Fie $f : G \to \Gamma$ un morfism de grupuri. Atunci

$$\frac{G}{\ker f} \xrightarrow{\sim} \operatorname{Im} f$$

în mod canonic, via $\overline{f}(\widehat{x}) = f(x)$.

Demonstraţie[1]*:* Definim $\overline{f} : \dfrac{G}{\ker f} \to \operatorname{Im} f$, $\overline{f}(\widehat{x}) = f(x)$.

Dacă $\widehat{x} = \widehat{y}$, atunci $x^{-1}y \in \ker f$, deci $f(x^{-1}y) = e_\Gamma$. f fiind morfism de grupuri, obţinem de aici $f(x)^{-1}f(y) = e_\Gamma$, deci $f(x) = f(y)$. Prin urmare, valorile lui $\overline{f}$ sunt independente de alegerea reprezentanţilor argumentelor. Cum valorile lui $\overline{f}$ sunt valori ale lui f, ele se află în $\operatorname{Im} f$. Prin urmare, $\overline{f}$ este corect definită.

Dacă $x, y \in G$, atunci $\overline{f}(\widehat{xy}) = \overline{f}(\widehat{xy}) = f(xy) = f(x)f(y) = \overline{f}(\widehat{x})\overline{f}(\widehat{y})$. Aşadar, $\overline{f}$ este morfism de grupuri.

Este evident că $\overline{f}$ este surjectivă.

Dacă $\overline{f}(\widehat{x}) = e_\Gamma$, atunci $f(x) = e_\Gamma$, deci $x \in \ker f$, de unde $\widehat{x} = \widehat{e}$. În consecinţă, $\overline{f}$ este injectivă.

Din toate faptele arătate mai sus rezultă că $\overline{f}$ este morfism bijectiv de grupuri. Prin urmare, f este izomorfism. $\square$

[1] O demonstraţie mai rapidă a acestei teoreme se obţine utilizând proprietatea de universalitate a grupului factor. Lăsăm ca exerciţiu cititorului această abordare.

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.

CURSUL 10: GRUPURI

G. MINCU

1. Subgrupul generat de o submulţime

Definiţia 1. Fie G un grup şi $M \subset G$. Prin **subgrupul lui G generat de M** înţelegem cel mai mic (în sensul incluziunii) subgrup al lui G care conţine submulţimea M.

Vom nota subgrupul lui G generat de M cu $\langle M \rangle$. Dacă $M = \{x_1, x_2, \ldots, x_n\}$, vom folosi, în loc de $\langle \{x_1, x_2, \ldots, x_n\} \rangle$, notaţia $\langle x_1, x_2, \ldots, x_n \rangle$.

Propoziţia 2. Fie G un grup şi $M \subset G$. Are loc relaţia

$$\langle M \rangle = \bigcap_{\substack{H \leq G \\ H \supset M}} H.$$

Propoziţia 3. Fie G un grup şi $M \subset G$. Are loc relaţia

$$\langle M \rangle = \{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} : n \in \mathbb{N}^*, \ x_1, \ldots, x_n \in M, \ \alpha_1, \ldots, \alpha_n \in \mathbb{Z}\}.$$

Observaţia 4. Dacă $g \in G$, atunci $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.

Observaţia 5. $\langle \emptyset \rangle = \{e\}$.

Definiţia 6. Fie G un grup. Submulţimea M a lui G se numeşte **sistem de generatori** al lui G dacă $\langle M \rangle = G$.

Definiţia 7. Grupul G se numeşte **finit generat** dacă el admite un sistem finit de generatori.

Exemplul 8. Orice grup admite ca sistem de generatori mulţimea sa subiacentă.

Exemplul 9. Orice grup finit este finit generat.

Exemplul 10. Pentru orice $n \in \mathbb{N}$ grupul $\mathbb{Z}_n$ este finit generat.

Exemplul 11. Pentru orice $n \in \mathbb{N}^*$ grupul S_n este finit generat.

Exemplul 12. Pentru orice $n \in \mathbb{N}^*$ grupul diedral D_n este finit generat.

Exemplul 13. Grupul $\mathbb{Z}$ este finit generat.

Exemplul 14. Pentru orice $n \in \mathbb{N}^*$ grupul $\mathbb{Z}^n$ este finit generat.

Exemplul 15. Grupurile $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ nu sunt finit generate.

Temă: Demonstraţi afirmaţiile de la exemplele 8-15!

2. GRUPURI CICLICE

Definiţia 16. Grupul G se numeşte **ciclic** dacă el admite un sistem de generatori format dintr-un singur element.

Observaţia 17. Orice grup ciclic este finit generat.

Exemplul 18. Grupul $\mathbb{Z}$ este ciclic, deoarece $\mathbb{Z} = \langle 1 \rangle$.

Exemplul 19. Pentru orice $n \in \mathbb{N}^*$ grupul $\mathbb{Z}_n$ este ciclic, deoarece $\mathbb{Z}_n = \langle \widehat{1} \rangle$.

Observaţia 20. Generatorul unui grup ciclic nu este unic determinat. De exemplu, avem şi $\mathbb{Z} = \langle -1 \rangle$, iar $\mathbb{Z}_n = \langle \widehat{a} \rangle$ dacă şi numai dacă $(a, n) = 1$.

Exemplul 21. Grupul $\mathbb{Z} \times \mathbb{Z}$ nu este ciclic.

Exemplul 22. Grupurile $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ nu sunt ciclice.

Teorema de structură a grupurilor ciclice. Orice grup ciclic cu $n \in \mathbb{N}^*$ elemente este izomorf cu $\mathbb{Z}_n$. Orice grup ciclic infinit este izomorf cu $\mathbb{Z}$.

Demonstraţie: Fie G un grup ciclic şi g un generator al acestuia. Considerăm $u : \mathbb{Z} \to G$, $u(n) = g^n$. Dacă $m, n \in \mathbb{Z}$, avem

$$u(m+n) = g^{m+n} = g^m g^n = u(m)u(n),$$

deci u este morfism de grupuri. În plus, u este în mod evident surjectiv. Aplicând teorema fundamentală de izomorfism pentru grupuri, obţinem $G = \operatorname{Im} u \simeq \dfrac{\mathbb{Z}}{\ker u}$. Prin urmare, dacă $\ker u = n\mathbb{Z}$ cu $n \in \mathbb{N}^*$ avem $G \simeq \mathbb{Z}_n$, iar dacă $\ker u = \{0\}$ avem $G \simeq \mathbb{Z}$. $\square$

Corolarul 23. Orice grup ciclic este comutativ.

Corolarul 24. Orice subgrup al unui grup ciclic este ciclic.

Corolarul 25. Orice grup factor al unui grup ciclic este ciclic.

3. Ordinul unui element într-un grup

Observaţia 26. Dat fiind un element x al unui grup G, subgrupul $\langle x\rangle = \{x^n : n \in \mathbb{Z}\}$ al lui G este ciclic.

Definiţia 27. Prin **ordinul** elementului x al grupului G înţelegem ordinul subgrupului generat de x în G.

Vom nota ordinul elementului x al grupului G cu $\text{ord}_G x$. Dacă grupul G este subînţeles în context, atunci vom folosi şi notaţia ord x.

Caracterizări ale ordinului.

Propoziţia 28. Fie G un grup şi $x \in G$. Atunci

$$\text{ord}_G x = \begin{cases} \min\{n \in \mathbb{N}^* : x^n = e\}, & \text{dacă } \{n \in \mathbb{N}^* : x^n = e\} \text{ este nevidă} \\ +\infty, & \text{altfel} \end{cases}$$

Corolarul 29. Dacă x este un element al grupului finit G, atunci $x^{\text{ord } x} = e$.

Propoziţia 30. Fie G un grup, $x \in G$ şi $n \in \mathbb{N}^*$. Atunci $\text{ord}_G x = n$ dacă şi numai dacă $x^n = e$ şi $\forall m \in \mathbb{Z}\ x^m = e \Rightarrow n|m$.

Proprietăţi ale ordinului.

Propoziţia 31. Ordinul oricărui element al unui grup finit divide ordinul respectivului grup.

Demonstraţie: Ordinul unui element, fiind ordinul unui subgrup, divide, conform teoremei lui Lagrange, ordinul grupului. □

Propoziţia 32. Dacă G, G_1 şi G_2 sunt grupuri finite, atunci:

(i) $\text{ord}_G(x^k) = \dfrac{\text{ord}_G x}{(k, \text{ord}_G x)}$.

(ii) $\text{ord}_{G_1\times G_2}(x_1, x_2) = [\text{ord}_{G_1} x_1, \text{ord}_{G_2} x_2]$.

(iii) $\text{ord}_G(xy) = \text{ord}_G(yx)$.

(iv) Dacă $xy = yx$ şi $(\text{ord}_G x, \text{ord}_G y) = 1$, atunci

$$\text{ord}_G(xy) = \text{ord}_G x \cdot \text{ord}_G y.$$

Temă: Rămâne adevărată afirmaţia de la punctul (iv) al propoziţiei 32 în lipsa condiţiei $xy = yx$?

Temă: O generalizare naturală a afirmaţiei de la punctul (iv) al propoziţiei 32 este: Dacă $xy = yx$, rezultă că

$$\text{ord}_G(xy) = [\text{ord}_G x, \text{ord}_G y].$$

Este ea adevărată?

4. Aplicaţii

Definiţia 33. Funcţia $\varphi : \mathbb{N}^* \to \mathbb{N}^*$, $\varphi(n) =$ numărul numerelor naturale ce nu-l întrec pe n şi sunt prime cu n, se numeşte **indicatorul lui Euler**.

Observaţia 34. $|U(\mathbb{Z}_n)| = \varphi(n)$.

Propoziţia 35. Dacă $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, unde $p_1, p_2, \dots, p_r$ sunt numere prime distincte două câte două, atunci

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$$

.

Teoremă (Euler). Pentru orice $n \in \mathbb{N}^*$ şi orice $a \in \mathbb{Z}$ prim cu n avem $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Demonstraţie: a fiind prim cu n, $\widehat{a}$ este element al grupului $U(\mathbb{Z}_n)$. Aplicând corolarul 29, $\widehat{a}^{\varphi(n)} = \widehat{1}$ în acest grup, de unde concluzia. □

Teoremă (Fermat). Pentru orice număr prim $p \in \mathbb{N}$ şi orice $a \in \mathbb{Z}$ prim cu p avem $a^{p-1} \equiv 1 \pmod{p}$.

Demonstraţie: Întrucât pentru orice număr prim p avem $\varphi(p) = p - 1$, obţinem concluzia aplicând teorema lui Euler. □

Propoziţia 36. Fie $m, n \in \mathbb{N}$. Grupurile $\mathbb{Z}_m \times \mathbb{Z}_n$ şi $\mathbb{Z}_{mn}$ sunt izomorfe dacă şi numai dacă m şi n sunt prime între ele.

Demonstraţie: „$\Rightarrow$”: Corespondentul $(\widehat{a}, \overline{b})$ al lui $\widetilde{1}$ prin izomorfism are ordinul $[\mathrm{ord}_{\mathbb{Z}_m} \widehat{a}, \mathrm{ord}_{\mathbb{Z}_n} \overline{b}]$, dar şi mn. Deci, $mn = [\mathrm{ord}_{\mathbb{Z}_m} \widehat{a}, \mathrm{ord}_{\mathbb{Z}_n} \overline{b}]|[m, n]$; cum $mn = [m, n] \cdot (m, n)$, obţinem $(m, n) = 1$.
„$\Leftarrow$”: Este imediat că funcţia $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $f(\widetilde{a}) = (\widehat{a}, \overline{a})$ este (corect definită şi) morfism injectiv de grupuri. Cum atât domeniul cât şi codomeniul său au mn elemente, ea este şi surjectivă. Prin urmare, f este izomorfism de grupuri. □

Grupuri cu număr „mic” de elemente.

Definiţia 37. Prin **tipul de izomorfism** al grupului G înţelegem clasa de echivalenţă a lui G în raport cu relaţia de izomorfism. Uneori, ne vom referi la tipul de izomorfism al lui G spunând, pe scurt, **tipul lui G**.

Observaţia 38. Orice grup cu număr prim de elemente este ciclic.

Demonstraţie: Considerăm un grup G cu un număr prim p de elemente şi $x \in G \setminus \{e\}$. Atunci, $|\langle x\rangle| > 1$ şi $|\langle x\rangle|$ divide $|G| = p$, deci $|\langle x\rangle| = p = |G|$, de unde $G = \langle x\rangle$. $\square$

Corolarul 39. Dacă $p \in \mathbb{N}$ este număr prim, atunci singurul tip de grupuri cu p elemente este $\mathbb{Z}_p$.

Corolarul 40. Există un singur tip de grupuri cu două elemente, şi anume $\mathbb{Z}_2$.

Corolarul 41. Există un singur tip de grupuri cu trei elemente, şi anume $\mathbb{Z}_3$.

Pentru viitoarele consideraţii avem nevoie de următorul instrument:

Propoziţia 42. Fie G un grup cu proprietatea că orice element al său are ordin 1 sau 2. Atunci:
(i) G este comutativ.
(ii) Există $n \in \mathbb{N}^*$ astfel încât $|G| = 2^n$.
(iii) Există $n \in \mathbb{N}^*$ astfel încât $G \simeq \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{n \text{ factori}}$.

Problemă suplimentară: Demonstraţi propoziţia 42!

Grupuri cu patru elemente. Fie G un grup cu patru elemente. Elementele lui G nu pot avea decât ordin 1, 2 sau 4.
Dacă G are elemente de ordin 4, atunci G este ciclic, deci, conform teoremei de structură a grupurilor ciclice, $G \simeq \mathbb{Z}_4$.
Dacă G nu are elemente de ordin 4, atunci suntem în situaţia

$$\forall x \in G \setminus \{e\} \quad \operatorname{ord} x = 2.$$

În aceste condiţii obţinem, aplicând propoziţia 42, că $|G| \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Am obţinut deci:

Propoziţia 43. Există exact două tipuri de grupuri cu patru elemente: $\mathbb{Z}_4$ şi grupul lui Klein.

Grupuri cu şase elemente. Fie G un grup cu şase elemente. Elementele lui G nu pot avea decât ordin 1, 2, 3 sau 6.
Dacă G are elemente de ordin 6, atunci G este ciclic, deci, conform teoremei de structură a grupurilor ciclice, $G \simeq \mathbb{Z}_6$.
Dacă G nu are elemente de ordin 6, să presupunem că pentru orice $x \in G \setminus \{e\}$ avem ord $x = 2$. În aceste condiţii obţinem, aplicând propoziţia 42, că $|G|$ este putere de doi, ceea ce reprezintă o contradicţie.
Prin urmare, G admite elemente de ordin 3; fie x un astfel de element şi $y \in G \setminus \{e, x, x^2\}$. Se arată uşor că $G = \{e, x, x^2, y, xy, x^2y\}$ şi, eliminând celelalte posibilităţi, că $y^2 = e$. Dacă $yx = xy$ obţinem

imediat faptul că $\mathrm{ord}_G(xy) = 6$, contradicţie. Eliminând celelalte posibilităţi (de pildă, $yx = e$ ar duce la contradicţia $y = x^2$, ş. a. m. d.), constatăm că $yx = x^2y$. Prin urmare, $G \simeq D_3 \simeq S_3$.
Am obţinut aşadar:

Propoziţia 44. Există exact două tipuri de grupuri cu şase elemente: $\mathbb{Z}_6$ şi S_3.

Temă: Determinaţi tipurile de grupuri cu şapte, respectiv cu opt elemente!

Bibliografie

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

CURSUL 12: GRUPURI DE PERMUTĂRI

G. MINCU

1. Grupuri de permutări

Reamintim din cursul 8 faptul că, dată fiind o mulţime nevidă A, $S_A = \{f \in A^A : f \text{ este bijectivă } \}$ este grup în raport cu operaţia de compunere.

Noi vom face în acest curs referire la grupurile $S_n \overset{\text{not}}{=} S_{\{1,2,\ldots,n\}}$, $n \in \mathbb{N}^*$.

Observaţia 1. Pentru orice $n \in \mathbb{N}^*$ avem $|S_n| = n!$.

Observaţia 2. S_n este ciclic pentru $n \in \{1, 2\}$.
S_n este necomutativ pentru orice $n \geq 3$.

2. Descompuneri ale permutărilor

Definiţia 3. O permutare $\sigma \in S_n$ se numeşte *ciclu* dacă există $k \in \mathbb{N}^*$ şi $\{i_1, i_2, \ldots, i_k\} \subset \{1, 2, \ldots, n\}$ astfel încât $\sigma(i_r) = i_{r+1}$ pentru orice $r \in \{1, 2, \ldots, k-1\}$, $\sigma(i_k) = i_1$, iar $\sigma(j) = j$ pentru orice $j \in \{1, 2, \ldots, n\} \backslash \{i_1, i_2, \ldots, i_k\}$. Notăm un astfel de ciclu prin $(i_1, i_2, \ldots, i_k)$, numărul k se numeşte *lungimea* ciclului, iar mulţimea $\{i_1, i_2, \ldots, i_k\}$ poartă numele de *orbita* ciclului.

Observaţia 4. $(i_1, i_2, \ldots, i_k)^{-1} = (i_k, i_{k-1}, \ldots, i_1)$.

Observaţia 5. Permutarea inversă unui ciclu este tot un ciclu!

Definiţia 6. Numim *transpoziţie* orice ciclu de lungime doi.

Observaţia 7. $(i_1, i_2, \ldots, i_k) = (i_1, i_2)(i_2, i_3) \ldots (i_{k-1}, i_k)$, deci orice ciclu este produs de transpoziţii.

Definiţia 8. Două cicluri din S_n se numesc *disjuncte* dacă orbitele lor sunt disjuncte.

Propoziţia 9. Orice două cicluri disjuncte comută.

Demonstraţie: Fie $c_1, c_2 \in S_n$ două cicluri disjuncte şi $i \in \{1, 2, \ldots, n\}$. Întrucât orbitele ciclurilor considerate sunt disjuncte, i nu poate aparţine ambelor orbite.
Dacă $c_1(i) = i$, atunci $(c_1c_2)(i) = c_1(c_2(i)) = c_2(i) = c_2(c_1(i)) =$

$(c_2c_1)(i)$.
Dacă $c_2(i) = i$, atunci $(c_2c_1)(i) = c_2(c_1(i)) = c_1(i) = c_1(c_2(i)) = (c_1c_2)(i)$. □

Observaţia 10. Calcule similare celor din demonstraţia propoziţiei 9 conduc la concluzia că pentru orice cicluri disjuncte[1] $c_1, c_2, \ldots, c_r$ şi pentru orice $k \in \{1, 2, \ldots, n\}$ există $j \in \{1, 2, \ldots, r\}$ astfel încât $(c_1c_2 \ldots c_r)(k) = c_j(k)$.

Teorema 11. Orice permutare din S_n se poate scrie ca produs de cicluri disjuncte. Abstracţie făcând de ordinea factorilor, această scriere este unică.

Demonstraţie: Pentru $\sigma \in S_n$ notăm $\mathcal{M}_\sigma = \{k : \sigma(k) \neq k\}$. Vom demonstra prin inducţie după $m = |\mathcal{M}_\sigma|$ că orice permutare σ se poate scrie în mod unic ca produs de cicluri disjuncte ale căror orbite sunt conţinute în $\mathcal{M}_\sigma$.
Dacă $e = c_1c_2 \ldots c_r$ cu factorii din membrul drept cicluri disjuncte, atunci, conform observaţiei 10, $c_1 = c_2 = \ldots = c_r = e$. Acest lucru probează afirmaţia teoremei pentru $m = 0$.
Să considerăm acum o permutare $\sigma \in S_n$ cu $m = |\mathcal{M}_\sigma| > 0$. Există atunci $k \in \{1, 2, \ldots, n\}$ cu $\sigma(k) \neq k$. Cum $k_\sigma \overset{\text{def}}{=} \{\sigma(k), \sigma^2(k), \ldots\} \subset \{1, 2, \ldots, n\}$, k_σ este finită, deci există $i < j$ astfel încât $\sigma^i(k) = \sigma^j(k)$, de unde $\sigma^{j-i}(k) = k$. Prin urmare, $\{t \in \mathbb{N}^* : \sigma^t(k) = k\} \neq \emptyset$; fie s cel mai mic element al acestei mulţimi. Este uşor de probat (temă!) relaţia $k_\sigma = \{k, \sigma(k), \ldots, \sigma^{s-1}(k)\}$; punând $c \overset{\text{not}}{=} (k, \sigma(k), \ldots, \sigma^{s-1}(k))$, constatăm că avem $\mathcal{M}_{c^{-1}\sigma} \subset \mathcal{M}_\sigma \setminus \{k\}$, deci $|\mathcal{M}_{c^{-1}\sigma}| < |\mathcal{M}_\sigma|$. Conform ipotezei de inducţie, $c^{-1}\sigma$ se scrie ca un produs $c_1c_2 \ldots c_r$ de cicluri disjuncte cu orbitele conţinute în $\mathcal{M}_{c^{-1}\sigma}$; drept urmare, $cc_1c_2 \ldots c_r$ este o descompunere a lui σ în produs de cicluri disjuncte cu orbitele incluse în $\mathcal{M}_\sigma$.
Pentru partea de unicitate, păstrând semnificaţiile de mai sus pentru k şi $c, c_1, \ldots, c_r$, considerăm şi scrierea $\sigma = \gamma_1\gamma_2 \ldots \gamma_t$ ca produs de cicluri disjuncte. Având în vedere observaţia 10, există $j \in \{1, 2, \ldots, n\}$ pentru care $\sigma(k) = \gamma_j(k)$. După o eventuală renumerotare, putem considera că $j = 1$. Ciclurile $\gamma_1, \gamma_2, \ldots, \gamma_t$ fiind disjuncte, $c^u(k) = \sigma^u(k) = \gamma_1^u(k)$ pentru orice $u \in \mathbb{Z}$, de unde $\gamma_1 = c$. Compunând acum relaţia $cc_1c_2 \ldots c_r = \gamma_1\gamma_2 \ldots \gamma_t$ cu c^{-1}, obţinem $c_1c_2 \ldots c_r = \gamma_2\gamma_3 \ldots \gamma_t$. În virtutea ipotezei de inducţie, $\{c_1, c_2, \ldots, c_r\} = \{\gamma_2, \gamma_3, \ldots, \gamma_t\}$. Ţinând cont şi de unicitatea deja probată a scrierii lui e, demonstraţia se încheie. □

[1] sau chiar permutări arbitrare disjuncte, noţiunea definindu-se ca şi în cazul ciclurilor

Corolarul 12. Orice permutare din S_n se poate scrie ca produs de transpoziţii.

Observaţia 13. Spre deosebire de descompunerea în produs de cicluri disjuncte, descompunerea unei permutări în produs de transpoziţii nu este unică.

Observaţia 14. $S_n = \langle \{(i,j) : 1 \leq i < j \leq n\} \rangle$.

Temă: Demonstraţi că:
i) $S_n = \langle (1,2), (1,3), \ldots, (1,n) \rangle$.
ii) $S_n = \langle (1,2), (2,3), \ldots, (n-1,n) \rangle$.
iii) $S_n = \langle (1,2), (1,2,\ldots,n) \rangle$.

3. Permutări pare şi impare. Signatură

Definiţia 15. Fie $\sigma \in S_n$, $n \geq 2$. O pereche (i,j), unde $1 \leq i < j \leq n$ se numeşte *inversiune* a lui σ dacă $\sigma(i) > \sigma(j)$.

Definiţia 16. Permutarea $\sigma \in S_n$ se numeşte *pară* dacă are un număr par de inversiuni; σ se numeşte *impară* dacă are un număr impar de inversiuni.

Propoziţia 17. Orice transpoziţie este permutare impară.

Demonstraţie: Inversiunile transpoziţiei (i,j), unde $1 \leq i < j \leq n$, sunt (i,k), $k \in \{i+1, i+2, \ldots, j\}$ şi (l,j), $l \in \{i+1, i+2, \ldots, j-1\}$; numărul acestora este $(j-i) + (j-1-i) = 2(j-i) - 1$, care este impar. $\square$

Definiţia 18. Prin *signatura* permutării $\sigma \in S_n$, $n \geq 2$, înţelegem numărul

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Observaţia 19. În produsul din definiţia 18 se simplifică de fapt toţi numitorii şi toţi numărătorii, la numărători rămânând câte un -1 de fiecare dată când $\sigma(j) - \sigma(i) < 0$. Prin urmare,

$$\varepsilon(\sigma) = (-1)^{\text{Numărul inversiunilor lui } \sigma}$$

Corolarul 20. a) $\sigma \in S_n$ este pară dacă şi numai dacă $\varepsilon(\sigma) = 1$.
b) $\sigma \in S_n$ este impară dacă şi numai dacă $\varepsilon(\sigma) = -1$.

Propoziţia 21. Pentru orice $\sigma, \tau \in S_n$ are loc relaţia $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$.

Corolarul 22. ε este morfism de grupuri de la S_n la $(\{-1,1\}, \cdot)$.

Corolarul 23. *i)* $\varepsilon(e) = 1$.
ii) Pentru orice $\sigma \in S_n$ avem $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$.

Observaţia 24. $\ker \varepsilon$ constă în permutările pare din S_n.

Corolarul 25. Permutările pare din S_n constituie un subgrup normal al lui S_n.

Notăm subgrupul permutărilor pare din S_n cu A_n.

Definiţia 26. A_n se numeşte *grupul altern* de grad n.

Corolarul 27. $\dfrac{S_n}{A_n} \simeq \{-1, 1\}$.

Demonstraţie: Aplicăm corolarul 22, observaţia 24 şi teorema fundamentală de izomorfism pentru grupuri. □

Corolarul 28. Pentru orice $n \geq 2$ avem $|A_n| = \dfrac{n!}{2}$.

Corolarul 29. i) Orice ciclu de lungime pară este impar.
ii) Orice ciclu de lungime impară este par.

Demonstraţie: Aplicăm observaţia 7 şi propoziţiile 17 şi 21. □

4. Ordinul unei permutări

Observaţia 30. Ordinul oricărui ciclu este egal cu lungimea sa.

Demonstraţie: Considerând un ciclu $\sigma = (i_1, i_2, \ldots, i_k) \in S_n$, constatăm că $\sigma^j(i_1) = i_{j+1}$, deci $\sigma^j \neq e$, pentru orice $j < k$. Demonstraţia se încheie observând că $\sigma^k = e$. □

Corolarul 31. Orice transpoziţie are ordinul 2.

Propoziţia 32. Ordinul unei permutări $\sigma \in S_n$ este egal cu cel mai mic multiplu comun al ordinelor ciclurilor disjuncte din descompunerea sa standard.

Demonstraţie: Fie $\sigma \in S_n$ şi $\sigma = c_1 c_2 \ldots c_r$ descompunerea acesteia în produs de cicluri disjuncte. Notăm $t_j = \text{ord } c_j$, $j \in \{1, 2, \ldots, r\}$, şi $m = [t_1, t_2, \ldots, t_r]$. Conform propoziţiei 9, avem $\sigma^t = c_1^t c_2^t \ldots c_r^t$ pentru orice $t \in \mathbb{Z}$. Prin urmare, $\sigma^m = e$, iar $\sigma^t = e$ dacă şi numai dacă $c_j^t = e$ pentru orice $j \in \{1, 2, \ldots, r\}$ dacă şi numai dacă ord $c_j | t$ pentru orice $j \in \{1, 2, \ldots, r\}$ dacă şi numai dacă $m | t$. Afirmaţia este acum consecinţă a propoziţiei 30 din cursul 10. □

5. ORICE GRUP SE SCUFUNDĂ ÎNTR-UN GRUP DE PERMUTĂRI

Aşa cum arată şi titlul paragrafului, orice grup poate fi regăsit ca subgrup al unui grup de permutări. Acest lucru este consecinţă a următoarei teoreme a lui Cayley:

Teorema 33. Orice grup G este izomorf cu un subgrup al lui S_G.

Demonstraţie: Considerăm funcţia $\varphi : G \to S_G$, $\varphi(g) = h_g$, unde $h_g : G \to G$, $h_g(x) = gx$. Întrucât $h_{g^{-1}} = h_g^{-1}$, h_g este într-adevăr un element al lui S_G, deci φ este corect definită.
Pentru $g, g', x \in G$ avem $h_{gg'}(x) = (gg')x = g(g'x) = h_g(h_{g'}(x)) = (h_g h_{g'})(x)$, de unde $h_{gg'} = h_g \circ h_{g'}$. De aici obţinem faptul că φ este morfism de grupuri.
Dacă $g, g' \in G$ sunt astfel încât $h_g = h_{g'}$, atunci $g = h_g(e) = h_{g'}(e) = g'$, deci morfismul φ este injectiv. $\square$

Corolarul 34. Orice grup cu n elemente este izomorf cu un subgrup al lui S_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.

CURSUL 13: ELEMENTE DE ALGEBRĂ UNIVERSALĂ

G. MINCU

1. Operaţii de aritate finită

Definiţia 1. Fie M o mulţime nevidă şi $n \in \mathbb{N}^*$. Numim **lege de compoziţie (operaţie) n-ară** pe M orice funcţie $f : M^n \to M$.

Definiţia 2. Dacă f este o operaţie n-ară pe mulţimea M, atunci n se numeşte **aritatea** lui f.

Observaţia 3. O operaţie de aritate 1 pe mulţimea M este o funcţie $f : M \to M$; uneori, pentru a desemna o operaţie de aritate 1 folosim şi exprimarea ,,operaţie **unară**".

Observaţia 4. Noţiunea de operaţie n-ară generalizează noţiunea de operaţie cu care am lucrat în cursurile 7-11. Toate acele operaţii erau, în acord cu terminologia introdusă acum, operaţii de aritate 2, pe care le vom numi şi operaţii **binare** (acest epitet a fost deja menţionat avant la lettre în definiţiile din cursul 7).

Convenind că pentru orice mulţime nevidă M are loc $M^0 = \{\emptyset\}$, putem extinde definiţia 1 la $n \in \mathbb{N}$:

Definiţia 5. Fie M o mulţime nevidă. Numim **lege de compoziţie (operaţie) 0 -ară** pe M alegerea unui element al lui M.

Definiţia 6. Vom spune despre orice operaţie 0-ară că are aritate 0.

Definiţia 7. Dacă există $n \in \mathbb{N}$ astfel ca f să fie o operaţie de aritate n pe mulţimea M, atunci f se numeşte operaţie de aritate finită pe M.

2. Algebre universale

Definiţia 8. Prin **tip de algebră universală** vom înţelege o familie $\mathcal{F}$ de numere naturale indexată după o mulţime $S_{\mathcal{F}}$. În acest context vom folosi pentru elementele lui $S_{\mathcal{F}}$ denumirea de **simboluri funcţionale**.

Notaţie Dat fiind un tip $\mathcal{F}$ de algebră universală, vom nota cu $\mathcal{F}_n$ mulţimea $\{f \in S_{\mathcal{F}} : \mathcal{F}(f) = n\}$.

Definiţia 9. Numim **algebră universală de tipul** $\mathcal{F}$ orice pereche $\mathbf{A} = \langle A, F\rangle$ în care A este o mulţime nevidă, iar F este o familie indexată după $S_{\mathcal{F}}$ de operaţii de aritate finită pe mulţimea A cu proprietatea că pentru orice $f \in S_{\mathcal{F}}$ aritatea operaţiei asociate f^A este egală cu $\mathcal{F}(f)$.

Definiţia 10. Mulţimea A din definiţia de mai sus se numeşte **universul** (sau **mulţimea subiacentă a**) algebrei universale $\mathbf{A}$, $\mathcal{F}$ se numeşte **tipul** sau **signatura** lui $\mathbf{A}$, iar operaţiile $(f^A)_{f\in S_{\mathcal{F}}}$ se numesc **operaţiile fundamentale** ale lui $\mathbf{A}$.

Observaţia 11. Dacă $\mathbf{A} = \langle A, F\rangle$ este o algebră universală, vom folosi frecvent notaţia F şi pentru a desemna imaginea familiei F, deducând din context ce înţeles trebuie atribuit notaţiei.

Observaţia 12. Vom face uneori referire la algebra universală $\mathbf{A} = \langle A, F\rangle$ spunând ,,algebra universală A". Când se va întâmpla acest lucru, F trebuie să fie subînţeleasă fără a exista posibilitate de confuzie.

Observaţia 13. Dacă pentru algebra universală $\mathbf{A} = \langle A, F\rangle$ de tipul $\mathcal{F}$ mulţimea $S_{\mathcal{F}}$ este finită, să zicem $S_{\mathcal{F}} = \{f_1, f_2, \ldots, f_r\}$, atunci vom folosi şi **notaţia** $\mathbf{A} = \langle A, f_1, f_2, \ldots, f_r\rangle$, simbolurile funcţionale fiind scrise în ordinea descrescătoare a arităţilor. În această situaţie, signatura lui $\mathbf{A}$ va fi prezentată sub forma r-uplului de numere naturale $(\mathcal{F}(f_1), \mathcal{F}(f_2), \ldots, \mathcal{F}(f_r))$.

Observaţia 14. În practică, exemplele concrete de algebre universale se vor încadra în şabloanele generale prezentate până acum, fiind însă individualizate de anumite condiţii pe care le satisfac operaţiile fundamentale din contextul respectiv pe întregul lor domeniu de definiţie (,,identităţi").

Exemplul 15. Un grup este o algebră universală $\mathbf{G} = \langle G, \cdot, {}^{-1}, 1\rangle$ de signatură $(2, 1, 0)$ pentru care sunt satisfăcute identităţile:
(A) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
(EN) $(x \cdot 1) = 1 \cdot x = x$ şi
(TES) $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

Exemplul 16. Un grup abelian este o algebră universală de signatură $(2, 1, 0)$, $\mathbf{G} = \langle G, \cdot, {}^{-1}, 1\rangle$, pentru care sunt satisfăcute identităţile:
(A) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
(EN) $(x \cdot 1) = 1 \cdot x = x$,
(TES) $x \cdot x^{-1} = x^{-1} \cdot x = 1$ şi
(C) $x \cdot y = y \cdot x$.

Exemplul 17. Un monoid este o algebră universală $\mathbf{M} = \langle M, \cdot, 1\rangle$ de signatură $(2, 0)$ pentru care sunt satisfăcute identităţile:
(A) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ şi
(EN) $(x \cdot 1) = 1 \cdot x = x$.

Exemplul 18. Un monoid comutativ este o algebră universală de signatură $(2, 0)$, $\mathbf{M} = \langle M, \cdot, 1\rangle$, pentru care sunt satisfăcute identităţile:
(A) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
(EN) $(x \cdot 1) = 1 \cdot x = x$ şi
(C) $x \cdot y = y \cdot x$.

Exemplul 19. Un semigrup este o algebră universală $\mathbf{S} = \langle S, \cdot\rangle$ de signatură (2) pentru care este satisfăcută identitatea
(A) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

Exemplul 20. Un semigrup comutativ este o algebră universală de signatură (2), $\mathbf{S} = \langle S, \cdot\rangle$, pentru care sunt satisfăcute identităţile:
(A) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ şi
(C) $x \cdot y = y \cdot x$.

Exemplul 21. O latice este o algebră universală $\mathbf{L} = \langle L, \vee, \wedge\rangle$ de signatură $(2, 2)$ pentru care sunt satisfăcute identităţile:
(C) $x \vee y = y \vee x$ şi $x \wedge y = y \wedge x$,
(A) $(x \vee y) \vee z = x \vee (y \vee z)$ şi $(x \wedge y) \wedge z = x \wedge (y \wedge z)$, şi
(Ab) $x \vee (x \wedge y) = x$ şi $x \wedge (x \vee y) = x$.

3. SUBALGEBRE UNIVERSALE

În acest capitol $\mathbf{A} = \langle A, F\rangle$ va desemna o algebră universală de tip $\mathcal{F}$.

Definiţia 22. Date fiind $n \in \mathbb{N}^*$ şi o operaţie n-ară $f : M^n \to M$, spunem că $N \subset M$ este **parte stabilă a lui** M **în raport cu** f dacă

$$\forall x_1, x_2, \ldots, x_n \in N \quad f(x_1, x_2, \ldots, x_n) \in N.$$

Definiţia 23. Fie f o operaţie de aritate 0 pe mulţimea M. Spunem că $N \subset M$ este **parte stabilă a lui** M **în raport cu** f dacă $\operatorname{Im} f \subset N$.

Definiţia 24. Submulţimea B a lui A se numeşte **parte** F**-stabilă** a (sau **subunivers** al) lui $\mathbf{A}$ dacă B este parte stabilă a lui A în raport cu fiecare operaţie fundamentală a lui A.

Definiţia 25. O algebră universală $\mathbf{B} = \langle B, G\rangle$ de tip $\mathcal{F}$ se numeşte **subalgebră universală** a lui $\mathbf{A}$ dacă $B \subset A$ şi dacă fiecare operaţie fundamentală f^B a lui $\mathbf{B}$ se obţine din operaţia corespunzătoare f^A a lui $\mathbf{A}$ prin (restricţie şi) corestricţie.

Vom nota faptul că $\mathbf{B}$ este subalgebră universală a lui $\mathbf{A}$ cu $\mathbf{B} \leq \mathbf{A}$.

Observaţia 26. Mulţimea vidă este parte F-stabilă a lui $\mathbf{A}$.

Observaţia 27. Orice parte F-stabilă nevidă a lui $\mathbf{A}$ este mulţime subiacentă pentru o subalgebră universală a lui $\mathbf{A}$.

Observaţia 28. Dacă $\mathbf{A}$ are şi operaţii fundamentale de aritate zero, atunci o parte a lui A este F-stabilă dacă şi numai dacă ea este mulţime subiacentă a unei subalgebre universale a lui $\mathbf{A}$.

Observaţia 29. Deşi obiectele de interes pentru noi sunt subalgebrele universale, proprietăţi ,,mai bune" găsim pentru părţile F-stabile, care sunt mai comod de manevrat decât acestea. Motivul principal pentru această situaţie este acela că părţile F-stabile pot fi şi vide, lucru nepermis mulţimilor subiacente de algebre universale.

4. subalgebre generate de submulţimi

În acest capitol $\mathbf{A} = \langle A, F \rangle$ va desemna o algebră universală de tip $\mathcal{F}$.

Propoziţia 30. Intersecţia oricărei familii de părţi F-stabile ale lui $\mathbf{A}$ este la rândul său parte F-stabilă a lui $\mathbf{A}$.

Definiţia 31. Fie M o submulţime a lui A. **Prin partea F-stabilă a lui A generată de** M înţelegem mulţimea

$$\mathrm{Sg}(M) \overset{\text{not}}{=} \bigcap \{N : N \text{ este parte } F\text{-stabilă a lui } \mathbf{A}\}.$$

Observaţia 32. $\mathrm{Sg}(M)$ este cea mai mică (în sensul incluziunii) parte F-stabilă a lui $\mathbf{A}$ care conţine submulţimea M.

Definiţia 33. Fie M o submulţime a lui A. Spunem că M este **sistem de generatori** pentru $\mathbf{A}$ dacă $\mathrm{Sg}(M) = A$.

Propoziţia 34. Pentru orice submulţime M, N ale lui A au loc relaţiile:
(i) $M \subset \mathrm{Sg}(M)$.
(ii) Dacă $M \subset N$, atunci $\mathrm{Sg}(M) \subset \mathrm{Sg}(N)$.
(iii) $\mathrm{Sg}(\mathrm{Sg}(M)) = \mathrm{Sg}(M)$.

Observaţia 35. În acord cu terminologia introdusă la cursul de Logică, propoziţia 34 afirmă că Sg este un operator de închidere.

Propoziţia 36. Mulţimea părţilor F-stabile ale lui $\mathbf{A}$ are în raport cu incluziunea o structură de latice completă.

Demonstraţie: Pentru orice familie $\mathcal{M} = (M_\tau)_{\tau \in T}$ de părţi F-stabile ale lui A avem $\inf \mathcal{M} = \bigcap_{\tau \in T} M_\tau$ şi $\sup \mathcal{M} = \mathrm{Sg}\left(\bigcup_{\tau \in T} M_\tau \right)$. $\square$

5. MORFISME DE ALGEBRE UNIVERSALE

În acest capitol $\mathbf{A} = \langle A, F\rangle$ şi $\mathbf{B} = \langle B, G\rangle$ desemnează două algebre universale de tip $\mathcal{F}$.

Definiţia 37. Numim **morfism de algebre universale de la A la B** orice funcţie $\alpha : A \to B$ cu proprietăţile:
(i) $\alpha(f^A(a_1, a_2, \ldots, a_n)) = f^B(\alpha(a_1), \alpha(a_2), \ldots, \alpha(a_n))$ pentru orice $n \in \mathbb{N}^*$, $f \in \mathcal{F}_n$ şi $a_1, a_2, \ldots, a_n \in A$
(ii) $\alpha \circ f^A = f^B$ pentru orice $f \in \mathcal{F}_0$.

Exemplul 38. Dacă $\mathbf{B} \leq \mathbf{A}$, atunci $j : B \to A$, $j(b) = b$ este un morfism de algebre universale.

Definiţia 39. Morfismul din exemplul 38 se numeşte **morfismul incluziune** al lui **B** în **A**.

Propoziţia 40. Dacă două morfisme de algebre universale de la **A** la **B** coincid pe un sistem de generatori al lui **A**, atunci ele sunt egale.

Propoziţia 41. Fie $\mathbf{A} = \langle A, F\rangle$, $\mathbf{B} = \langle B, G\rangle$ şi $\mathbf{E} = \langle E, H\rangle$ trei algebre universale de tip $\mathcal{F}$, α un morfism de algebre universale de la **A** la **B** şi β un morfism de algebre universale de la **B** la **E**. Atunci $\beta \circ \alpha$ este morfism de algebre universale de la **A** la **E**.

Definiţia 42. Numim **izomorfism de algebre universale de la A la B** orice morfism inversabil de la **A** la **B** al cărui invers este morfism de algebre universale de la **B** la **A**.

Teorema 43. Un morfism de algebre universale este izomorfism dacă şi numai dacă este bijectiv.

Demonstraţie: Partea de necesitate este evidentă.
Pentru suficienţă, fie $\alpha : A \to B$ un morfism bijectiv de algebre universale, $n \in \mathbb{N}^*$, $f \in \mathcal{F}_n$ *şi* $b_1, b_2, \ldots, b_n \in B$. Avem succesiv:

$$\alpha^{-1}(f^B(b_1, b_2, \ldots, b_n)) = \alpha^{-1}(f^B(\alpha(\alpha^{-1}(b_1)), \ldots, \alpha(\alpha^{-1}(b_n)))) =$$

$$\alpha^{-1}(\alpha(f^A(\alpha^{-1}(b_1), \ldots, \alpha^{-1}(b_n)))) = f^A(\alpha^{-1}(b_1), \alpha^{-1}(b_2), \ldots, \alpha^{-1}(b_n)).$$

Pentru $f \in \mathcal{F}_0$, $\quad \alpha^{-1} \circ f^B = \alpha^{-1} \circ (\alpha \circ f^A) = f^A$. $\square$

Definiţia 44. Prin **endomorfism** al algebrei universale **A** înţelegem un morfism de la **A** la **A**, iar prin **automorfism** al lui **A** înţelegem un izomorfism de la **A** la **A**.

Exemplul 45. id_A este automorfism al algebrei universale **A**.

Propoziţia 46. Fie α un morfism de algebre universale de la $\mathbf{A}$ la $\mathbf{B}$.
(i) Dacă M e parte F-stabilă a lui $\mathbf{A}$, atunci $\alpha(M)$ este parte G-stabilă a lui $\mathbf{B}$.
(ii) Dacă N e parte G-stabilă a lui $\mathbf{B}$, atunci $\alpha^{-1}(N)$ este parte F-stabilă a lui $\mathbf{A}$.

Definiţia 47. Fie α un morfism de algebre universale de la $\mathbf{A}$ la $\mathbf{B}$ şi $\mathbf{C} \leq \mathbf{A}$. Numim **imaginea lui C prin** α, şi notăm $\alpha(\mathbf{C})$, subalgebra universală a lui $\mathbf{B}$ care are ca mulţime subiacentă $\alpha(C)$.

Definiţia 48. Fie α un morfism de algebre universale de la $\mathbf{A}$ la $\mathbf{B}$ Numim **imaginea lui** α, şi notăm **Im** α, imaginea lui $\mathbf{A}$ prin α.

Definiţia 49. Fie α un morfism de algebre universale de la $\mathbf{A}$ la $\mathbf{B}$ şi $\mathbf{D} \leq \mathbf{B}$. Dacă $\alpha^{-1}(D) \neq \emptyset$, numim **preimaginea lui D prin** α, şi notăm $\alpha^{-1}(\mathbf{D})$, subalgebra universală a lui $\mathbf{A}$ care are ca mulţime subiacentă $\alpha^{-1}(D)$.

6. Congruenţe. Algebre factor

În acest capitol $\mathbf{A} = \langle A, F\rangle$ va desemna o algebră universală de tip $\mathcal{F}$.

Definiţia 50. O relaţie de echivalenţă ρ pe mulţimea A se numeşte **congruenţă** a algebrei universale $\mathbf{A}$ dacă pentru orice $n \in \mathbb{N}^*$, $f \in \mathcal{F}_n$ şi $a_1, a_2, \ldots, a_n, a'_1, a'_2, \ldots, a'_n \in A$ are loc

$$(\forall j \in \{1, 2, \ldots, n\} \quad a_j \rho\, a'_j) \Rightarrow f^A(a_1, a_2, \ldots, a_n) \rho f^A(a'_1, a'_2, \ldots, a'_n).$$

Propoziţia 51. Dacă ρ este o congruenţă a algebrei universale $\mathbf{A}$, $n \in \mathbb{N}^*$ şi $f \in \mathcal{F}_n$, atunci operaţia $f^A/\rho : (A/\rho)^n \to A/\rho$,

$$(f^A/\rho)(a_1/\rho, \ldots, a_n/\rho) = f^A(a_1, \ldots, a_n)/\rho$$

este corect definită.

Definiţia 52. Fie ρ o congruenţă a algebrei universale $\mathbf{A}$ şi $f \in \mathcal{F}_0$. Definim $(f^A/\rho)(\emptyset) = f^A(\emptyset)/\rho$.

Definiţia 53. Fie ρ o congruenţă a algebrei universale $\mathbf{A}$. Prin **algebra universală factor** a lui $\mathbf{A}$ în raport cu ρ înţelegem algebra universală care are mulţimea subiacentă A/ρ şi operaţiile fundamentale $(f^A/\rho)_{f \in S_{\mathcal{F}}}$.

Vom nota algebra universală factor a lui $\mathbf{A}$ în raport cu ρ prin $\mathbf{A}/\rho$.

Propoziţia 54. Dacă ρ este o congruenţă a algebrei universale $\mathbf{A}$, atunci $\pi : A \to A/\rho$, $\pi(a) = a/\rho$ este morfism surjectiv de algebre universale.

Definiţia 55. Morfismul din propoziţia 54 se numeşte **surjecţia canonică** a lui $\mathbf{A}/\rho$.

7. TEOREMA FUNDAMENTALĂ DE IZOMORFISM

În acest capitol $\mathbf{A} = \langle A, F\rangle$ şi $\mathbf{B} = \langle B, G\rangle$ vor desemna algebre universale de tip $\mathcal{F}$.

Definiţia 56. Fie α un morfism de algebre universale de la $\mathbf{A}$ la $\mathbf{B}$. Vom numi **nucleul** lui α mulţimea

$$\ker \alpha \stackrel{\text{not}}{=} \{(a_1, a_2) \in A^2 : \alpha(a_1) = \alpha(a_2)\}.$$

Propoziţia 57. În condiţiile din definiţia anterioară, $\ker \alpha$ este o congruenţă a lui $\mathbf{A}$.

Temă: Demonstraţi propoziţia 57!

Teorema fundamentală de izomorfism pentru algebre universale. Dacă $\mathbf{A} = \langle A, F\rangle$ şi $\mathbf{B} = \langle B, G\rangle$ sunt algebre universale de tip $\mathcal{F}$, α este un morfism de algebre universale de la $\mathbf{A}$ la $\mathbf{B}$, π este surjecţia canonică a lui $\mathbf{A}/\ker\alpha$, iar $j : \operatorname{Im}\alpha \to B$ este morfismul incluziune, atunci există un (unic) izomorfism de algebre universale $\beta : \mathbf{A}/\ker\alpha \to \mathbf{Im}\ \alpha$ cu proprietatea că $j \circ \beta \circ \pi = \alpha$.

Bibliografie

[1] G. Birkhoff, *On the structure of abstract algebras*, Proceedings of the Cambridge Philosophical Society 31, 1935, pp.433-454.

[2] S. Burris, H. P. Sankappanavar, *A course in universal algebra*, Springer-Verlag, 1981.

[3] P. M. Cohn, *Algebra*, Wiley and sons, 1991.

[4] T. Dumitrescu, *Algebra*, Ed. Universităţii din Bucureşti, 2006.

[5] I. D. Ion, N. Radu, *Algebră*, Ed. Didactică şi Pedagogică, Bucureşti, 1981.

[6] C. Năstăsescu, C. Niţă, C. Vraciu, *Bazele algebrei*, Ed. Academiei, Bucureşti, 1986.