

CURSUL 2: MULȚIMI

G. MINCU

1. MULȚIMI

Noțiunea de mulțime este una primară în matematică.

De obicei, folosim termenul de „mulțime” pentru a desemna o entitate pe care considerăm că o constituie anumite obiecte¹. Acestea din urmă se numesc **elementele** mulțimii.

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

Vom considera că **două mulțimi sunt egale dacă și numai dacă au aceleași elemente**.

Cea mai naturală metodă de a reprezenta o mulțime este de a enumera efectiv elementele acesteia; în mod standard, elementele respective se scriu între acolade, fără repetiții și 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 și mulțimile „uzuale” de numere:

b) $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \dots\}$ - mulțimea numerelor naturale.

c) $\mathbb{Z} = \{\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\}$ - mulțimea numerelor întregi.

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

Nu toate mulțimile pot fi reprezentate de maniera sintetică propusă anterior, de cele mai multe ori motivul fiind acela că respectivele mulțimi au „prea multe” elemente pentru a fi posibilă (sau utilă!) o astfel de reprezentare. În astfel de situații, apelăm la reprezentarea mulțimilor cu ajutorul unei proprietăți caracteristice elementelor lor.

¹fie grație unor proprietăți comune ce justifică punerea laolaltă a acestor obiecte, fie pur și simplu în mod arbitrar/ca exercițiu intelectual

Exemplul 3. a) $\{a \in \mathbb{N} : \exists k \in \mathbb{N} a = 2k + 1\}$ - mulțimea numerelor naturale impare

b) $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\right\}$ - mulțimea numerelor raționale.

c) \mathbb{R} = mulțimea numerelor ce corespund punctelor unei drepte² - mulțimea numerelor reale.

d) $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i^2 = -1\}$ - mulțimea numerelor complexe.

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

Definiția 5. Spunem că mulțimea A este **inclusă** în mulțimea B dacă orice element al lui A îi aparține și lui B . Această situație este descrisă și de exprimarea „**A este submulțime a mulțimii B**”.

Desemnăm situația în care mulțimea A este inclusă în mulțimea B prin notația $A \subset B$.

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

Observația 7. Dată fiind o mulțime M și o proprietate \mathcal{P} care are sens pentru cel puțin unul dintre elementele lui M , admitem că $\{x \in M : x \text{ are proprietatea } \mathcal{P}\}$ este o submulțime a lui M . Acest lucru conferă legitimitate manierei „analitice” de prezentare a mulțimilor pe care am amintit-o mai sus³.

Observația 8. Mulțimile A și B sunt egale dacă și numai dacă $A \subset B$ și $B \subset A$.

O consecință foarte importantă a observației 8 este următoarea:

Observația 9. Întotdeauna egalitatea de mulțimi se demonstrează prin dublă incluziune.

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

Definiția 11. Considerăm că există o mulțime care nu are niciun element. Ea se notează cu \emptyset și se numește **mulțimea vidă**.

²pe care am fixat originea și unitatea

³Atragem atenția asupra faptului că, în lipsa unei mulțimi inițiale M în cadrul căreia să punem problema elementelor cu proprietatea \mathcal{P} , nu avem garanția că acestea constituie o mulțime. Persistența în a lucra cu astfel de „mulțimi” poate conduce la paradoxuri.

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

Se consideră că, dată fiind o mulțime M , submulțimile sale constituie o mulțime.

Definiția 13. Dată fiind mulțimea M , mulțimea $\{A : A \subset M\}$ se numește **mulțimea părților lui M** . Vom nota această mulțime cu $\mathcal{P}(M)$.

2. PRINCIPIUL INDUCȚIEI

O proprietate fundamentală a mulțimii numerelor naturale, care ne oferă o puternică metodă pentru demonstrația de afirmații și pentru construcția de obiecte, este următoarea⁴:

Principiul inducției: *Dacă M este o submulțime a lui \mathbb{N} cu proprietățile*

1) $0 \in M$

și

2) $\forall n \in \mathbb{N} \quad n \in M \Rightarrow n + 1 \in M$,

atunci $M = \mathbb{N}$.

Prezentăm mai jos două consecințe ale acestui principiu. Acestea stau la baza abordării practice a demonstrațiilor prin inducție matematică.

Teorema 14. *Fie P un predicat de variabilă naturală și $n_0 \in \mathbb{N}$ astfel încât:*

1) $P(n_0)$

și

2) $\forall k \geq n_0 \quad P(k) \Rightarrow P(k + 1)$,

atunci $\forall n \geq n_0 \quad P(n)$.

Teorema 15. *Fie P un predicat de variabilă naturală și $n_0 \in \mathbb{N}$ astfel încât:*

1) $P(n_0)$

și

2) $\forall k \geq n_0 \quad (P(n_0) \wedge P(n_0 + 1) \wedge \dots \wedge P(k)) \Rightarrow P(k + 1)$,

atunci $\forall n \geq n_0 \quad P(n)$.

⁴ Principiul inducției este o consecință imediată a axiomaticii teoriei mulțimilor, fie că se utilizează axioma mulțimilor infinite, fie că se pornește de la axiomele lui Peano

3. OPERAȚII CU MULȚIMI

În fiecare dintre situațiile care urmează, în lipsa vreunei alte mențiuni, vom considera că există o mulțime „mare” care conține toate mulțimile în discuție.

Considerăm mulțimile A și B .

Definiția 16. Mulțimea $A \cup B = \{x : x \in A \vee x \in B\}$ se numește **reuniunea** mulțimilor A și B .

Definiția 17. Mulțimea $A \cap B = \{x : x \in A \wedge x \in B\}$ se numește **intersecția** mulțimilor A și B .

Definiția 18. Dacă $A \cap B = \emptyset$, spunem că mulțimile A și B sunt **disjuncte**.

Definiția 19. Mulțimea $A \setminus B = \{x : x \in A \wedge x \notin B\}$ se numește **diferența** mulțimilor A și B .

Definiția 20. $(a, b) \stackrel{\text{def}}{=} \{\{a\}, \{a, b\}\}$ se numește **perechea ordonată** determinată de elementele a și b .

Observația 21. Drept consecință a axiomelor teoriei mulțimilor obținem în acest context faptul că toate perechile ordonate (a, b) cu $a \in A$ și $b \in B$ constituie o mulțime.

Definiția 22. $A \times B = \{(a, b) : a \in A \wedge b \in B\}$ se numește **produsul cartezian** al mulțimilor A și B .

Propoziția 23. Pentru orice mulțimi A , B și C au loc relațiile:

- 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) $A \times (B \cup C) = (A \times B) \cup (A \times C)$; $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Exercițiul 24. Demonstrați propoziția 23!

Punctul c) al propoziției 23 ne sugerează următoarele definiții:

Definiția 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 mulțime.

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

Notăția utilizată pentru complementara lui A în raport cu E este $\mathbb{C}_E A$. Dacă E este subînțeleasă în context, atunci complementara lui A în raport cu E se mai notează și $\mathbb{C}A$ sau \bar{A} .

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

$$\mathbb{C}_E(A \cup B) = (\mathbb{C}_E A) \cap (\mathbb{C}_E B) \quad \text{și} \quad \mathbb{C}_E(A \cap B) = (\mathbb{C}_E A) \cup (\mathbb{C}_E B).$$

Exercițiul 27. Demonstrați regulile lui de Morgan!

Definiția 28. Dacă E este o mulțime înzestrată cu o lege de compoziție \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) $2\mathbb{Z}$ = mulțimea numerelor întregi pare.

e) $3\mathbb{Z} + 1$ = mulțimea acelor numere întregi care prin împărțire la 3 dau restul 1.

f) $\{-1, 1\} \cdot \mathbb{N} = \mathbb{Z}$.

4. FAMILII DE MULȚIMI

Pentru generalizarea chestiunilor din paragraful precedent, este necesară o modalitate de a gestiona „multe” mulțimi. Una dintre cele mai frecvente abordări ale chestiunii este următoarea⁵:

Definiția 30. Prin **familie de mulțimi indexată după mulțimea** I înțelegem o funcție definită pe I și ale cărei valori sunt mulțimi.

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

O consecință imediată a axiomelor teoriei mulțimilor este aceea că putem defini reuniunea oricărei mulțimi de mulțimi. Este legitimă deci:

Definiția 31. Prin **reuniunea** familiei de mulțimi $(M_i)_{i \in I}$ înțelegem mulțimea $\{x : \exists i \in I \ x \in M_i\}$.

Notăția pe care o vom folosi pentru reuniunea familiei de mulțimi $(M_i)_{i \in I}$ este $\bigcup_{i \in I} M_i$. În situația în care $I = \{1, 2, \dots, n\}$, reuniunea

⁵ Pentru a plasa aceste considerații imediat după cele pe care le generalizează, utilizăm aici noțiunea de funcție; aceasta este definită în cursul 3, iar definiția respectivă nu se bazează pe chestiunile din acest paragraf.

familiei menționate se notează și $\bigcup_{i=1}^n M_i$, iar dacă $I = \mathbb{N}$, reuniunea

familiei $(M_i)_{i \in I}$ se notează și $\bigcup_{i=1}^{\infty} M_i$ sau $\bigcup_{i \geq 1} M_i$

Definiția 32. Prin **intersecția** familiei de mulțimi $(M_i)_{i \in I}$ înțelegem mulțimea $\{x : \forall i \in I \ x \in M_i\}$.

Notația pe care o vom folosi pentru intersecția familiei de mulțimi $(M_i)_{i \in I}$ este $\bigcap_{i \in I} M_i$. În situația în care $I = \{1, 2, \dots, n\}$, intersecția

familiei menționate se notează și $\bigcap_{i=1}^n M_i$, iar dacă $I = \mathbb{N}$, intersecția

familiei $(M_i)_{i \in I}$ se notează și $\bigcap_{i=1}^{\infty} M_i$ sau $\bigcap_{i \geq 1} M_i$

Afirmațiile propoziției 23 se generalizează astfel:

Propoziția 33. Pentru orice familie de mulțimi $(A_i)_{i \in I}$ și pentru orice mulțime B au loc relațiile⁶:

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

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

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

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

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

Toate considerațiile anterioare sunt, desigur, valabile și pentru familii de submulțimi ale unei mulțimi date. În acest context funcționează următoarea variantă generalizată a regulilor lui de Morgan:

⁶Punctul b) al propoziției 23 se generalizează la:

b') Pentru orice funcție bijectivă $\sigma : I \rightarrow I$,

$\bigcup_{i \in I} A_{\sigma(i)} = \bigcup_{i \in I} A_i$ și $\bigcap_{i \in I} A_{\sigma(i)} = \bigcap_{i \in I} A_i$.

Propoziția 34. Dată fiind familia $(A_i)_{i \in I}$ de submulțimi ale mulțimii E , au loc relațiile:

$$\mathfrak{C}_E \left(\bigcup_{i \in I} A_i \right) = \bigcap_{i \in I} \mathfrak{C}_E A_i \quad \text{și} \quad \mathfrak{C}_E \left(\bigcap_{i \in I} A_i \right) = \bigcup_{i \in I} \mathfrak{C}_E A_i$$

BIBLIOGRAFIE

- [1] T. Dumitrescu, *Algebra*, Ed. Universității din București, 2006.
- [2] P. Halmos, *Naïve set theory*, Springer Verlag, 1960.
- [3] C. Năstăsescu, C. Niță, C. Vraciu, *Bazele algebrei*, Ed. Academiei, București, 1986.
- [4] C. Năstăsescu, *Introducere în teoria mulțimilor*, Ed. Didactică și Pedagogică, București, 1974.

CURSUL 3: FUNCȚII

G. MINCU

1. FUNCȚII

Definiția 1. (provizorie!) Numim **funcție** orice triplet format din două mulțimi și o „lege de corespondență” care asociază *fiecărui* element din prima mulțime un *unic* element din cea de-a doua.

Definiția 2. Prima dintre cele două mulțimi care intră în componența unei funcții se numește **domeniul** (de **definiție** al) funcției, iar cea de a doua se numește **codomeniul** (sau **domeniul de valori** al) funcției.

Observația 3. Două funcții sunt egale dacă și numai dacă au același domeniu, același codomeniu și aceeași lege de corespondență.

Notăția uzuală pentru o funcție f care are domeniul A și codomeniul B este $f : A \rightarrow B$ (citim „ f este definită pe A și ia valori în B ”). Faptul că elementului $a \in A$ îi corespunde prin f elementul $b \in B$ se notează $f(a) = b$.

Definiția 4. Prin **graficul** unei funcții $f : A \rightarrow B$ înțelegem mulțimea $\Gamma_f = \{(a, b) \in A \times B : b = f(a)\}$.

Observația 5. Dacă $f : A \rightarrow B$, atunci $\Gamma_f \subset A \times B$.

Observația 6. Cunoscând graficul unei funcții, putem identifica domeniul de definiție al funcției, precum și legea de corespondență a acesteia¹. Din acest motiv, se preferă reformularea definiției 1 astfel încât să se evite termenul „lege”, care nu are în situația respectivă un înțeles foarte bine precizat:

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

Observația 8. O consecință a axiomelor din teoria mulțimilor este faptul că, date fiind două mulțimi A și B , funcțiile definite pe A cu valori în B constituie o mulțime.

¹Nu însă și codomeniul; putem însă „vedea” imaginea funcției.

Observația 9. Dacă mulțimile finite A și B au a , respectiv b elemente, se arată ușor (temă!) că numărul funcțiilor definite pe A cu valori în B este b^a . Această observație ne sugerează utilizarea pentru mulțimea tuturor funcțiilor definite pe A cu valori în B a notației B^A .

2. CLASE IMPORTANTE DE FUNCȚII

Definiția 10. Funcția $f : A \rightarrow B$ se numește **injectivă** dacă $\forall a_1, a_2 \in A \quad a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$.

Observația 11. În cuvinte, o funcție este injectivă dacă duce orice două elemente diferite în elemente diferite.

O caracterizare des utilizată a funcțiilor injective este dată de:

Propoziția 12. Funcția $f : A \rightarrow B$ este injectivă dacă și 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 $i : A \rightarrow B$, $i(a) = a$ este o funcție injectivă. Ea se numește **injectia canonică** a lui A în B .

Definiția 14. Funcția $f : A \rightarrow B$ se numește **surjectivă** dacă $\forall b \in B \quad \exists a \in A \quad f(a) = b$.

Observația 15. În cuvinte, o funcție este surjectivă dacă „își umple codomeniul”.

Exemplul 16. $\pi_A : A \times B \rightarrow A$, $\pi_A(a, b) = a$ și $\pi_B : A \times B \rightarrow B$, $\pi_B(a, b) = b$ sunt funcții surjective (ele se numesc **proiecțiile canonice** ale produsului cartezian $A \times B$).

Definiția 17. O funcție injectivă și surjectivă se numește **bijectivă**.

Exemplul 18. Dată fiind o mulțime A , funcția $\text{id}_A : A \rightarrow A$, $\text{id}_A(a) = a$ este o funcție bijectivă. Ea se numește **funcția identică a mulțimii** A .

Definiția 19. O mulțime A se numește **infinită** dacă există $f \in A^A$ injectivă, dar nesurjectivă. Mulțimea A se numește **finită** dacă nu este infinită.

Propoziția 20. Fie A o mulțime nevidă. Următoarele afirmații sunt echivalente:

- A este finită.
- Există un număr $n \in \mathbb{N}^*$ și o funcție bijectivă $f : \{1, 2, \dots, n\} \rightarrow A$.

Pentru considerațiile de până la finalul acestei secțiuni vom considera că A și B desemnează submulțimi ale lui \mathbb{R} .

Definiția 21. Funcția $f : A \rightarrow B$ se numește **crescătoare** dacă $\forall a_1, a_2 \in A \quad a_1 < a_2 \Rightarrow f(a_1) \leq f(a_2)$.

Definiția 22. Funcția $f : A \rightarrow B$ se numește **descrescătoare** dacă $\forall a_1, a_2 \in A \quad a_1 < a_2 \Rightarrow f(a_1) \geq f(a_2)$.

Definiția 23. Funcția $f : A \rightarrow B$ se numește **monotonă** dacă este fie crescătoare, fie descrescătoare.

Definiția 24. Funcția $f : A \rightarrow B$ se numește **strict crescătoare** dacă $\forall a_1, a_2 \in A \quad a_1 < a_2 \Rightarrow f(a_1) < f(a_2)$.

Definiția 25. Funcția $f : A \rightarrow B$ se numește **strict descrescătoare** dacă $\forall a_1, a_2 \in A \quad a_1 < a_2 \Rightarrow f(a_1) > f(a_2)$.

Definiția 26. Funcția $f : A \rightarrow B$ se numește **strict monotonă** dacă este fie strict crescătoare, fie strict descrescătoare.

3. FUNCȚIA CARACTERISTICĂ A UNEI SUBMULTIMI

Definiția 27. Fie E o mulțime și $A \subset E$. Funcția

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

se numește **funcția caracteristică² a lui A în E** .

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

Funcțiile caracteristice ale submulțimilor au proprietăți calculatorii interesante care, laolaltă cu teorema 28, le conferă o largă aplicabilitate:

Propoziția 29. Fie E o mulțime și A, B submulțimi ale sale. Au loc relațiile:

- 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” SUBMULTIMILOR PRIN FUNCȚII

Definiția 30. Dacă $f : A \rightarrow B$ și $C \subset A$, notăm $f(C)$ și numim **imaginea submulțimii C prin funcția f** mulțimea

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

²Uneori, cu precădere în teoria probabilităților, se mai folosește pentru funcția prezentată denumirea de **funcția indicator a submulțimii A a lui E**

Definiția 31. Prin **imaginea** funcției $f : A \rightarrow B$ înțelegem mulțimea $f(A)$.

Notăția folosită în mod uzual pentru imaginea funcției f este $\text{Im} f$.

Observația 32. O funcție este surjectivă dacă și numai dacă imaginea sa coincide cu codomeniul său.

Definiția 33. Dacă $f : A \rightarrow B$ și $D \subset B$, notăm $f^{-1}(D)$ și numim **preimaginea**³ **submulțimii** D **prin funcția** f mulțimea $\{a \in A : f(a) \in D\}$.

Observația 34. Notăția din definiția 33 se utilizează și în situația în care funcția f nu este inversabilă!

Propoziția 35. Considerăm funcția $f : A \rightarrow B$. 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: Demonstrați propoziția 35!

Temă: Generalizați afirmațiile din propoziția 35 la situația unei familii arbitrare de submulțimi!

Observația 36. Observăm că în cazul relațiilor din propoziția 35 imaginea inversă „se poartă mai bine” decât imaginea directă. Aparenta „anomalie” de la punctul c) dispăre pentru funcțiile injective:

Propoziția 37. Funcția $f : A \rightarrow B$ este injectivă dacă și numai dacă

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

5. COMPUNEREA FUNCȚIILOR

Definiția 38. Date fiind funcțiile $f : A \rightarrow B$ și $g : C \rightarrow D$ cu⁴ $B \subset C$, definim funcția $g \circ f : A \rightarrow D$, $g \circ f(x) = g(f(x))$. Funcția $g \circ f$ se numește **compusa lui** g **cu** f .

O situație importantă din punctul de vedere al compunerii funcțiilor este prezentată în

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

⁴în caz de necesitate, se poate impune doar condiția mai slabă $\text{Im} f \subset C$

Exemplul 39. Dată fiind o funcție arbitrară $f : A \rightarrow B$, $\text{id}_B \circ f = f$ și $f \circ \text{id}_A = f$.

Propoziția 40. Fie funcțiile $f : A \rightarrow B$, $g : C \rightarrow D$ și $h : E \rightarrow F$, unde $B \subset C$ și $D \subset E$. Atunci⁵ $h \circ (g \circ f) = (h \circ g) \circ f$.

Propoziția 41. Fie funcțiile $f : A \rightarrow B$ și $g : C \rightarrow D$, unde $B \subset C$. Atunci:

- a) Dacă f și g sunt injective, atunci $g \circ f$ este injectivă.
- b) Dacă $g \circ f$ este injectivă, atunci f este injectivă.
- c) Dacă f și g sunt surjective și $B = C$, atunci $g \circ f$ este surjectivă.
- b) Dacă $g \circ f$ este surjectivă, atunci g este surjectivă.
- e) Dacă f și g sunt bijective și $B = C$, atunci $g \circ f$ este bijectivă.
- b) Dacă $g \circ f$ este bijectivă, atunci f este injectivă, iar g este surjectivă.

Temă: Demonstrați propoziția 41!

Propoziția 42. Fie $A, B, C, D \subset \mathbb{R}$, $B \subset C$, și funcțiile $f : A \rightarrow B$ și $g : C \rightarrow D$. Atunci:

- a) Dacă f și g sunt de aceeași monotonie, atunci $g \circ f$ este crescătoare.
- b) Dacă f și g sunt de monotonii opuse, atunci $g \circ f$ este descrescătoare.
- c) Dacă f și g sunt de aceeași monotonie strictă, atunci $g \circ f$ este strict crescătoare.
- d) Dacă f și g sunt de monotonii stricte opuse, atunci $g \circ f$ este strict descrescătoare.

Temă: Demonstrați propoziția 42!

Propoziția 43. Orice funcție strict monotonă este injectivă.

Temă: Demonstrați propoziția 43!

6. INVERSAREA FUNCȚIILOR

Definiția 44. (provizorie!) Prin **inversă a funcției** $f : A \rightarrow B$ înțelegem orice funcție $g : B \rightarrow A$ cu proprietățile $g \circ f = \text{id}_A$ și $f \circ g = \text{id}_B$.

Definiția 45. Funcția $f : A \rightarrow B$ se numește **inversabilă** dacă ea admite (cel puțin o) inversă.

Propoziția 46. Dacă funcția $f : A \rightarrow B$ este inversabilă, atunci ea admite o unică inversă

⁵Anticipând discuția referitoare la legi de compoziție, această relație arată că, dată fiind o mulțime M , compunerea funcțiilor este o operație asociativă pe M^M .

Demonstrație: Presupunem că f este inversabilă și că g și h sunt inverse ale sale. Atunci,

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

Definiția 47. Dacă funcția $f : A \rightarrow B$ este inversabilă, atunci prin **inversa** lui f înțelegem unica (conform propoziției 46) funcție $g : B \rightarrow A$ cu proprietățile $g \circ f = \text{id}_A$ și $f \circ g = \text{id}_B$.

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

Observația 48. Dacă $f : A \rightarrow B$ este inversabilă, iar $D \subset B$, atunci, în acord cu definiția 33, notația $f^{-1}(D)$ ar desemna atât preimagea lui D prin f , cât și imaginea lui D prin f^{-1} . Întrucât aceste două mulțimi coincid, utilizarea aceleiași notații nu prezintă ambiguități.

Teorema 49. O funcție este inversabilă dacă și numai dacă ea este bijectivă.

7. PRODUSUL CARTEZIAN AL UNEI FAMILII DE MULȚIMI

Observația 50. Perechea ordonată $(a_1, a_2) \in A_1 \times A_2$ poate fi interpretată ca fiind o reprezentare a funcției $a : \{1, 2\} \rightarrow A_1 \cup A_2$, $a(1) = a_1$, $a(2) = a_2$. Evident, $a(1) \in A_1$ și $a(2) \in A_2$. Aceste considerații ne sugerează:

Definiția 51. Dată fiind familia de mulțimi $(A_i)_{i \in I}$, definim produsul său cartezian ca fiind mulțimea $\{a : I \rightarrow \bigcup_{i \in I} A_i : \forall i \in I \ a(i) \in A_i\}$ ^{6,7}

Vom nota produsul cartezian al familiei de mulțimi $(A_i)_{i \in I}$ 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 $(a_i)_{i \in I}$.

Definiția 52. Pentru $j \in I$, funcția $\pi_j : \prod_{i \in I} A_i \rightarrow A_j$, $\pi_j((a_i)_{i \in I}) = a_j$ se numește **proiecția canonică** a produsului $\prod_{i \in I} A_i$ pe componenta j .

Observația 53. Proiecțiile canonice ale produsului cartezian sunt surjective.

⁶Axiomele teoriei mulțimilor au drept consecință faptul că aceasta este într-adevăr o mulțime.

⁷Una dintre axiomele teoriei mulțimilor (așa-numita „axiomă a alegerii”) afirmă că dacă toate mulțimile familiei date sunt nevide, atunci produsul cartezian al familiei este nevid.

Observația 54. Dacă avem familia de mulțimi $(A_i)_{i \in I}$ cu proprietatea $A_i = A$ pentru orice $i \in I$, atunci, conform definiției 51, produsul cartezian $\prod_{i \in I} A_i$ constă exact în funcțiile definite pe I și care iau valori în A . Deci, în acest caz avem $\prod_{i \in I} A_i = A^I$. Dacă în situația prezentată avem $I = \{1, 2, \dots, n\}$, $n \in \mathbb{N}^*$, vom folosi în loc de A^I notația A^n .

Observația 55. Conform observației anterioare,

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

BIBLIOGRAFIE

- [1] T. Dumitrescu, *Algebra*, Ed. Universității din București, 2006.
- [2] P. Halmos, *Naive set theory*, Springer Verlag, 1960.
- [3] C. Năstăsescu, C. Niță, C. Vraciu, *Bazele algebrei*, Ed. Academiei, București, 1986.
- [4] C. Năstăsescu, *Introducere în teoria mulțimilor*, Ed. Didactică și Pedagogică, București, 1974.

CURSUL 5: RELAȚII

G. MINCU

1. CORESPONDENȚE

Definiția 1. Numim **corespondență**¹ orice triplet de mulțimi $\alpha = (A, B, \rho)$ cu proprietatea $\rho \subset A \times B$.

Definiția 2. Cu notațiile din definiția 1, ρ se numește **graficul** corespondenței α .

Observația 3. Noțiunea de corespondență este o generalizare a noțiunii de funcție.

Multe dintre noțiunile și tehnicile pe care le-am întâlnit la studiul funcțiilor pot fi transpuse și pentru cazul corespondențelor. Este de așteptat să întâlnim similitudini pronunțate cu chestiunile omoloage de la funcții, dar nu trebuie să ne surprindă nici anumite diferențe între situația corespondențelor și cea a funcțiilor, diferențe ce decurg din faptul că funcțiile sunt corespondențe de un tip foarte particular. Aceste considerații vor fi concretizate în următoarele două capitole.

2. COMPUNEREA CORESPONDENȚELOR

Definiția 4. Considerăm corespondențele $\alpha = (A, B, \rho)$ și $\beta = (B, C, \sigma)$. Corespondența $\beta \circ \alpha = (A, C, \sigma \circ \rho)$, unde

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

se numește **compusa corespondențelor** β și α .

Propoziția 5. Date fiind corespondențele $\alpha = (A, B, \rho)$, $\beta = (B, C, \sigma)$ și $\gamma = (C, D, \tau)$, are loc egalitatea

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

Definiția 6. Cu notațiile din propoziția 5,

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

¹În loc de „corespondență” unii autori folosesc în context noțiunea „relație binară”. Noi vom prefera să folosim sintagma „relație binară” în accepția din capitolul 4 al cursului. Utilizarea unui alt termen pentru situația de față are drept scop eliminarea anumitor ambiguități de exprimare în contextul din capitolul 4.

Definiția 7. Date fiind $n \in \mathbb{N}$, $n \geq 4$, și corespondențele $\alpha_1, \alpha_2, \dots, \alpha_n$ pentru care expresiile de mai jos au sens, definim

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

Observația 8. Aplicând propoziția 5, constatăm că operațiile de compunere din expresia $\alpha_1 \circ \alpha_2 \circ \dots \circ \alpha_n$ pot fi făcute în orice ordine dorim².

Definiția 9. Dată fiind corespondența $\alpha = (A, A, \rho)$,

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

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

Definiția 11. Dată fiind o mulțime A , corespondența $\text{id}_A = (A, A, \Delta_A)$, unde $\Delta_A = \{(a, a) : a \in A\}$ se numește **corespondența identică** (sau **corespondența unitate**) a mulțimii A .

Propoziția 12. Dată fiind corespondența $\alpha = (A, B, \rho)$, au loc egalitățile

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

3. INVERSAREA CORESPONDENȚELOR

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

Observația 14. Spre deosebire de situația funcțiilor, orice corespondență admite inversă.

Observația 15. Aici poate apărea întrebarea: având în vedere că toate funcțiile sunt corespondențe și că toate corespondențele admit inversă, de ce nu admit toate funcțiile inversă? Răspunsul este că orice funcție admite într-adevăr o *corespondență* inversă, dar aceasta *nu este funcție decât în situația în care funcția de la care am pornit este inversabilă în sensul prezentat în cursul 3*.

O diferență remarcabilă față de situația întâlnită la funcții este dată de

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

Chestiunea menționată în observația 16 are de fapt o formă mult mai precisă:

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

Propoziția 17. Dată fiind corespondența $\alpha = (A, B, \rho)$, au loc egalitățile $\alpha \circ \alpha^{-1} = \text{id}_B$ și $\alpha^{-1} \circ \alpha = \text{id}_A$ dacă și numai dacă α este funcție bijectivă.

Propoziția 18. Date fiind corespondențele $\alpha = (A, B, \rho)$ și $\beta = (B, C, \sigma)$, au loc egalitățile:

- (i) $(\alpha^{-1})^{-1} = \alpha$
- (ii) $((\beta \circ \alpha)^{-1}) = \alpha^{-1} \circ \beta^{-1}$.

4. RELAȚII PE O MULȚIME

În cele ce urmează, vom lua în discuție numai corespondențe (A, B, ρ) în care $A = B$. În situațiile de acest tip, după precizarea inițială a mulțimii A nu vom mai insista în a o include în notațiile ulterioare ale corespondențelor cu care lucrăm. În plus, singura corespondență de la mulțimea la ea însăși este cea vidă. Din acest motiv, noi vom studia în continuare doar corespondențe pe mulțimi nevide. Această discuție se concretizează în următoarea definiție:

Definiția 19. Numim **relație binară pe mulțimea nevidă A** orice submulțime a lui $A \times A$.

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

Vom nota cu $\mathcal{R}(A)$ mulțimea relațiilor pe mulțimea A .

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

Observația 22. Dacă ρ este o relație pe mulțimea A iar $a, b \in A$, vom utiliza frecvent notația $a\rho b$ pentru a desemna situația $(a, b) \in \rho$ și notația $a \not\rho b$ pentru a desemna situația $(a, b) \notin \rho$.

Fiecărei relații ρ pe mulțimea A îi putem asocia corespondența (A, A, ρ) și reciproc. Putem folosi această observație pentru a adapta la cazul relațiilor anumite noțiuni pe care le-am definit pentru corespondențe:

5. COMPUNEREA RELAȚIILOR

Definiția 23. Considerăm o mulțime A și relațiile ρ și σ pe A . Relația $\sigma \circ \rho = \{(x, z) \in A \times A : \exists y \in A (x, y) \in \rho \wedge (y, z) \in \sigma\}$ se numește **compusa relațiilor σ și ρ** .

Propoziția 24. Date fiind corespondențele ρ , σ și τ pe mulțimea A , are loc egalitatea

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

Demonstrație: Afirmatia este o consecință imediată a propoziției 5. \square

Definiția 25. Cu notațiile din propoziția 5,

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

Definiția 26. Date fiind $n \in \mathbb{N}$, $n \geq 4$, și relațiile $\rho_1, \rho_2, \dots, \rho_n$ pe mulțimea A , definim

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

Observația 27. Propoziția 5 ne arată că operațiile de compunere din expresia $\rho_1 \circ \rho_2 \circ \dots \circ \rho_n$ pot fi făcute în orice ordine dorim³.

Definiția 28. Dată fiind relația ρ pe mulțimea A , definim

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

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

Observația 30. Date fiind o relație ρ pe o mulțime A și $m, n \in \mathbb{N}^*$, are loc egalitatea $\rho^{m+n} = \rho^m \circ \rho^n$.

Definiția 31. Dată fiind o mulțime A , mulțimea $\Delta_A = \{(a, a) : a \in A\}$ se numește **diagonala** mulțimii $A \times A$.

Observația 32. În limbajul introdus în textul de față, Δ_A este relația de egalitate pe mulțimea A .

Propoziția 33. Dată fiind relația ρ pe mulțimea A , au loc egalitățile

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

Observația 34. Dacă pe mulțimea A sunt date relațiile ρ , σ , τ și φ astfel încât $\rho \subset \tau$ și $\sigma \subset \varphi$, atunci $\sigma \circ \rho \subset \varphi \circ \tau$.

6. INVERSAREA RELAȚIILOR

Definiția 35. Numim **inversa** relației ρ (dată pe mulțimea A) relația $\rho^{-1} = \{(b, a) \in A \times A : (a, b) \in \rho\}$.

Observația 36. Spre deosebire de situația funcțiilor, orice relație admite inversă.

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

Propoziția 38. Date fiind relațiile ρ și σ pe mulțimea A , au loc egalitățile:

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

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

Demonstrație: Afirmația este o consecință imediată a propoziției 18. \square

Definiția 39. Dată fiind relația ρ pe mulțimea A și $n \in \mathbb{N}^* \setminus \{1\}$,

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

Observația 40. Dată fiind o relație ρ pe o mulțime A , au loc egalitățile:

- (i) $\forall n \in \mathbb{N}^* \quad \rho^{-n} = (\rho^n)^{-1}$
- (ii) $\forall m, n \in \mathbb{N}^* \quad \rho^{-m-n} = \rho^{-m} \circ \rho^{-n}$

Observația 41. Dacă pe mulțimea A sunt date relațiile ρ și σ astfel încât $\rho \subset \sigma$, atunci $\rho^{-1} \subset \sigma^{-1}$.

7. CLASE IMPORTANTE DE RELAȚII

În tot acest capitol ρ va desemna o relație pe mulțimea A .

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

Observația 43. Relația ρ este reflexivă dacă și numai dacă $\rho \supset \Delta_A$.

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

Observația 45. Relația ρ este ireflexivă dacă și numai dacă $\rho \cap \Delta_A = \emptyset$.

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

Propoziția 47. Dată fiind o relație ρ pe o mulțime A , următoarele afirmații sunt echivalente:

- (i) ρ este simetrică.
- (ii) $\rho^{-1} \subset \rho$.
- (iii) $\rho^{-1} = \rho$.

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

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

Observația 49. Relația ρ este antisimetrică dacă și numai dacă

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

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

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

Observația 51. Relația ρ este tranzitivă dacă și numai dacă

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

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

Observația 53. Relația $A \times A$ este reflexivă, simetrică, tranzitivă și totală.

Propoziția 54. Relația ρ este reflexivă (respectiv ireflexivă, simetrică, antisimetrică, tranzitivă, totală) dacă și numai dacă ρ^{-1} este reflexivă (respectiv ireflexivă, simetrică, antisimetrică, tranzitivă, totală).

Propoziția 55. Dată fiind o mulțime nevidă \mathcal{M} de relații pe mulțimea A , $\bigcap_{\rho \in \mathcal{M}} \rho$ este o relație pe A . Dacă toate relațiile din \mathcal{M} sunt reflexive (respectiv ireflexive, simetrice, antisimetrice, tranzitive) atunci $\bigcap_{\rho \in \mathcal{M}} \rho$ este reflexivă (respectiv ireflexivă⁴, simetrică, antisimetrică, tranzitivă).

Observația 56. Dacă relația ρ este ireflexivă și dacă $\sigma \subset \rho$, atunci și σ este ireflexivă.

8. ÎNCHIDERI ALE RELAȚIILOR

În lipsa vreunei mențiuni contrare, în acest capitol ρ va desemna o relație pe o mulțime nevidă A .

Propoziția 57. Dată fiind o relație ρ pe mulțimea A , există o relație σ pe mulțimea A cu proprietățile:

- (i) $\rho \subset \sigma$
- (ii) σ este reflexivă.
- (iii) Dacă pentru o altă relație reflexivă $\tau \in \mathcal{R}(A)$ avem $\rho \subset \tau$, atunci⁵ $\sigma \subset \tau$.

În plus, σ cu aceste proprietăți este unic determinată.

Demonstrație: Pentru partea de existență, definim $\sigma = \rho \cup \Delta_A$.

Evident, $\rho \subset \sigma$ și σ este reflexivă.

Dacă $\tau \in \mathcal{R}(A)$ este reflexivă (adică, conține Δ_A) și conține ρ , atunci τ va conține și $\Delta_A \cup \rho = \sigma$.

Pentru demonstrarea unicității lui σ , să considerăm σ_1 și σ_2 cu proprietățile din enunț. Atunci, conform (iii), $\sigma_1 \subset \sigma_2$ și $\sigma_2 \subset \sigma_1$, de unde $\sigma_1 = \sigma_2$. \square

Definiția 58. Relația a cărei existență este asigurată de propoziția 57 se numește **închiderea reflexivă** a lui ρ .

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

⁴În cazul ireflexivității, deși afirmația prezentei propoziții este adevărată, ea nu dă foarte multă informație. În această situație, informație mai relevantă ne oferă observația 56.

⁵În limbajul pe care îl vom introduce la relații de ordine, aceste condiții spun că „ σ este o relație reflexivă minimală care conține ρ ”.

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

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

Propoziția 61. Dată fiind o relație ρ pe mulțimea A , există o relație σ pe mulțimea A cu proprietățile:

- (i) $\rho \subset \sigma$
- (ii) σ este simetrică.
- (iii) Dacă pentru o altă relație simetrică $\tau \in \mathcal{R}(A)$ avem $\rho \subset \tau$, atunci $\sigma \subset \tau$.

În plus, σ cu aceste proprietăți este unic determinată.

Demonstrație: Pentru partea de existență, definim $\sigma = \rho \cup \rho^{-1}$.

Evident, $\rho \subset \sigma$ și σ este simetrică.

Dacă $\tau \in \mathcal{R}(A)$ este simetrică (deci $\tau = \tau^{-1}$) și conține ρ , atunci, conform observației 41, τ va conține și ρ^{-1} , de unde $\tau \supset \sigma$.

Pentru demonstrarea unicității lui σ , să considerăm σ_1 și σ_2 cu proprietățile din enunț. Atunci, conform (iii), $\sigma_1 \subset \sigma_2$ și $\sigma_2 \subset \sigma_1$, de unde $\sigma_1 = \sigma_2$. \square

Definiția 62. Relația a cărei existență este asigurată de propoziția 57 se numește **închiderea simetrică** a lui ρ .

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

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

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

Propoziția 65. Dată fiind o relație ρ pe mulțimea A , există o relație σ pe mulțimea A cu proprietățile:

- (i) $\rho \subset \sigma$
- (ii) σ este tranzitivă.
- (iii) Dacă pentru o altă relație tranzitivă $\tau \in \mathcal{R}(A)$ avem $\rho \subset \tau$, atunci $\sigma \subset \tau$.

În plus, σ cu aceste proprietăți este unic determinată.

Demonstrație: Pentru partea de existență, definim $\sigma = \bigcup_{n \in \mathbb{N}^*} \rho^n$.

Evident, $\rho \subset \sigma$ și σ este tranzitivă.

Dacă $\tau \in \mathcal{R}(A)$ este tranzitivă (deci $\tau^2 \subset \tau$) și conține ρ , atunci, conform observației 34, τ va conține și ρ^2 . Inductiv, obținem $\tau \supset \rho^n$ pentru orice $n \in \mathbb{N}^*$, de unde $\tau \supset \sigma$.

Pentru demonstrarea unicității lui σ , să considerăm σ_1 și σ_2 cu proprietățile din enunț. Atunci, conform (iii), $\sigma_1 \subset \sigma_2$ și $\sigma_2 \subset \sigma_1$, de unde $\sigma_1 = \sigma_2$. \square

Definiția 66. Relația a cărei existență este asigurată de propoziția 57 se numește **închiderea tranzitivă** a lui ρ .

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

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

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

Propoziția 69. Fie ρ o relație pe mulțimea A . Atunci:

- (i) $R(S(\rho)) = S(R(\rho))$.
- (ii) $R(T(\rho)) = T(R(\rho))$.
- (iii) $S(T(\rho)) \subset T(S(\rho))$.

Demonstrație: (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 $n \in \mathbb{N}^*$ și $c_0 = a, c_1, \dots, c_n = b$ astfel încât $(c_{i-1}, c_i) \in \rho$ pentru orice $i \in \{1, 2, \dots, n\}$ sau există $n \in \mathbb{N}^*$ și $d_0 = b, d_1, \dots, d_n = a$ astfel încât $(d_{i-1}, d_i) \in \rho$ pentru orice $i \in \{1, 2, \dots, n\}$. 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

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

9. RELAȚII DE ECHIVALENȚĂ. MULȚIMI FACTOR

Definiția 71. Fie ρ o relație pe mulțimea nevidă A . ρ se numește **relație de echivalență** dacă este reflexivă, simetrică și tranzitivă.

Propoziția 72. Dată fiind o mulțime \mathcal{M} de relații de echivalență pe mulțimea A , intersecția lor este relație de echivalență pe A .

Demonstrație: Afirmatia este o consecință imediată a propoziției 55. \square

Definiția 73. Dată fiind o relație ρ pe mulțimea A , intersecția tuturor relațiilor de echivalență pe A care conțin ρ se numește **relația de echivalență generată de ρ** .

Observația 74. Relația de echivalență generată de ρ este cea mai mică (în sensul incluziunii) relație de echivalență pe A care conține ρ .

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

Demonstrație: Notăm cu σ relația din enunț. Întrucât $\sigma = T(R(S(\rho)))$, ea este tranzitivă. Cum $\Delta_A \subset \sigma$, σ este reflexivă. Definiția lui σ arată clar și simetria acesteia. Deci, σ este relație de echivalență. Evident, $\rho \subset \sigma$. Dacă considerăm o relație de echivalență τ pe A cu $\rho \subset \tau$, atunci τ , fiind reflexivă și simetrică, conține $R(S(\rho)) = \rho \cup \rho^{-1} \cup \Delta$. Cum însă τ este și tranzitivă, ea trebuie să conțină și închiderea tranzitivă a acesteia, adică pe σ . \square

Definiția 76. Fie ρ o relație de echivalență pe mulțimea nevidă A și $a \in A$. Prin **clasa de echivalență a lui a în raport cu ρ** înțelegem mulțimea $\{b \in A : b \rho a\}$.

Vom nota clasa de echivalență a lui a în raport cu ρ prin $\frac{a}{\rho}$ sau \hat{a} .

Vor exista de asemenea situații în care în locul acestor notații se vor folosi unele adaptate contextului.

Propoziția 77. Dacă ρ este o relație de echivalență pe mulțimea A , iar $a, b \in A$, atunci $\hat{a} = \hat{b}$ sau $\hat{a} \cap \hat{b} = \emptyset$.

Demonstrație: Dacă $a \rho b$, atunci $c \in \hat{a} \Leftrightarrow c \rho a \stackrel{b \rho a}{\Leftrightarrow} c \rho b \Leftrightarrow c \in \hat{b}$. Prin urmare, $\hat{a} = \hat{b}$.

Dacă $a \not\rho b$, să presupunem că există $c \in \hat{a} \cap \hat{b}$. Atunci $a \rho c$ și $c \rho b$, de unde $a \rho b$, contradicție. Rămâne deci că $\hat{a} \cap \hat{b} = \emptyset$. \square

Definiția 78. Numim **partiție** a mulțimii nevide A orice mulțime \mathcal{M} de submulțimi nevide ale lui A cu proprietățile:

1. $A = \bigcup_{B \in \mathcal{M}} B$.
2. Pentru orice $B, C \in \mathcal{M}$ cu $B \neq C$ avem $B \cap C = \emptyset$.

Observația 79. Propoziția 77 se reformulează cu ajutorul noțiunii de partiție astfel: „Mulțimea claselor de echivalență determinate de o relație de echivalență pe o mulțime A constituie o partiție a lui A ”.

Definiția 80. Fie ρ o relație de echivalență pe mulțimea A . Notăm $\frac{A}{\rho}$ și numim **mulțimea factor (cât)** a lui A în raport cu ρ mulțimea tuturor claselor de echivalență ale elementelor lui A în raport cu ρ .

Observația 81. Fie ρ o relație de echivalență pe mulțimea A . Funcția $\pi : A \rightarrow \frac{A}{\rho}$, $\pi(a) = \hat{a}$ este surjectivă.

Definiția 82. Fie ρ o relație de echivalență pe mulțimea A . Funcția din observația 81 numește **surjecția canonică** (sau **proiecția canonică**) a mulțimii factor $\frac{A}{\rho}$.

Definiția 83. Fie ρ o relație de echivalență pe mulțimea A . O submulțime \mathcal{S} a lui A se numește **sistem complet și independent de reprezentanți (pentru elementele mulțimii A) relativ la relația ρ** dacă îndeplinește condițiile:

1. Pentru orice două elemente distincte $s, t \in \mathcal{S}$ avem $s \not\sim t$.
2. Orice element al lui A este echivalent cu un element al lui \mathcal{S} .

Observația 84. În cuvinte, dată fiind o relație de echivalență pe o mulțime A , un sistem complet și independent de reprezentanți relativ la ρ este o submulțime a lui A alcătuită cu câte exact un element din fiecare clasă de echivalență.

Observația 85. Dacă ρ este o relație de echivalență pe mulțimea A iar \mathcal{S} este un sistem complet și independent de reprezentanți relativ la ρ , atunci funcția $f : \mathcal{S} \rightarrow \frac{A}{\rho}$, $f(s) = \hat{s}$ este bijectivă.

9.1. Exemple importante de relații de echivalență.

9.1.1. Egalitatea.

Exemplul 86. Dată fiind o mulțime nevidă, relația de egalitate pe aceasta este o relație de echivalență.

Observația 87. Unicul sistem complet și independent de reprezentanți pentru relația de egalitate pe mulțimea A este chiar A .

9.1.2. *Congruența modulo n .* Fie $n \in \mathbb{Z}$. Considerăm pe mulțimea \mathbb{Z} relația ρ_n dată astfel: $a\rho_nb \stackrel{\text{def}}{\iff} n|b-a$.

Definiția 88. Relația ρ_n se numește relația de **congruență modulo n** .

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

Notăție: În mod tradițional faptul că numerele întregi a și b sunt congruente modulo n se notează $a \equiv b \pmod{n}$. Începând din momentul de față vom folosi și noi această notăție, renunțând la provizoriul ρ_n .

Propoziția 90. Pentru orice $n \in \mathbb{Z}$ relația de congruență modulo n este o relație de echivalență.

Demonstrație: Fie $n, a, b, c \in \mathbb{Z}$.

Evident, $n|0 = a - a$, de unde $a \equiv a \pmod{n}$, deci relația de congruență 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, relația în discuție este simetrică.

Dacă $a \equiv b \pmod{n}$ și $b \equiv c \pmod{n}$, atunci $n|b - a$ și $n|c - b$. De aici, $n|(b - a) + (c - b) = c - a$, deci $a \equiv c \pmod{n}$. Prin urmare, relația de congruență modulo n este tranzitivă. \square

Observația 91. Fie $n \in \mathbb{N}^*$. Atunci:

a) Clasa de congruență modulo n a elementului $a \in \mathbb{Z}$ este $a + n\mathbb{Z}$ (ea constă în elementele care dau același rest ca și a la împărțirea prin n).

b) $\frac{\mathbb{Z}}{\equiv \pmod{n}} = \{\widehat{0}, \widehat{1}, \dots, \widehat{n-1}\} = \{n\mathbb{Z}, n\mathbb{Z} + 1, \dots, n\mathbb{Z} + n - 1\}$.

c) Sistemul complet și independent de reprezentanți cel mai frecvent folosit în context este $\{0, 1, \dots, n - 1\}$; el este alcătuit din resturile ce se pot obține împărțind numerele întregi la n .

Observația 92. Congruența modulo 0 este de fapt egalitatea pe \mathbb{Z} .

Prin urmare, conform observațiilor 85 și 87, $\frac{\mathbb{Z}}{\equiv \pmod{0}}$ este în bijecție cu \mathbb{Z} .

Definiția 93. Mulțimea factor a lui \mathbb{Z} în raport cu congruența modulo n se numește **mulțimea claselor de resturi modulo n** .

Vom folosi notația⁶ \mathbb{Z}_n pentru a desemna mulțimea claselor de resturi modulo n .

9.1.3. *Relația de echivalență asociată unei partiții.* Fie \mathcal{P} o partiție a mulțimii nevide A . Definim pe A relația

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

Propoziția 94. Relația $\sim_{\mathcal{P}}$ este de echivalență pe A .

⁶În teoria numerelor, această notăție este rezervată mulțimii întregilor n -adici (în situația în care n este număr prim). În acel context, inelul claselor de resturi modulo n se notează $\frac{\mathbb{Z}}{n\mathbb{Z}}$ sau $\frac{\mathbb{Z}}{(n)}$. Noi nu ne vom întâlni cu această situație la cursul de Algebră, deci notația este neechivocă.

Temă: Demonstrați propoziția 94!

Definiția 95. Relația $\sim_{\mathcal{P}}$ se numește **relația de echivalență asociată partiției \mathcal{P}** .

Propoziția 96. Dată fiind o mulțime nevidă A , mulțimea relațiilor de echivalență pe A și mulțimea partițiilor lui A sunt în corespondență bijectivă.

Demonstrație: Considerăm funcția Φ care asociază fiecărei relații de echivalență pe A partiția lui A în clasele de echivalență relative la relația respectivă. Considerăm de asemenea funcția Ψ care asociază fiecărei partiții \mathcal{P} a lui A relația $\sim_{\mathcal{P}}$. Atunci Φ și Ψ sunt inverse una celeilalte (lăsăm detaliile în seama cititorului). \square

9.1.4. *Relația de echivalență asociată unei funcții.* Considerăm mulțimile nevide A și B și funcția $f : A \rightarrow B$. Definim în acest context relația

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

Propoziția 97. Relația ρ_f este de echivalență.

Temă: Demonstrați propoziția 97!

Relația ρ_f ne permite să prezentăm un rezultat foarte util pentru definirea de funcții pe mulțimi factor:

Teorema 98. (Proprietatea de universalitate a mulțimii factor)

Fie ρ o relație de echivalență pe mulțimea A , $\pi : A \rightarrow \frac{A}{\rho}$ surjecția canonică, $f : A \rightarrow B$ o funcție și ρ_f relația de echivalență asociată acesteia.

- i) Dacă $\rho \subset \rho_f$, atunci există $u : \frac{A}{\rho} \rightarrow B$ astfel încât $u \circ \pi = f$.
- ii) u este injectivă dacă și numai dacă $\rho = \rho_f$.
- iii) u este surjectivă dacă și numai dacă f este surjectivă.

10. RELAȚII DE ORDINE

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

Definiția 99. Fie A o mulțime nevidă și ρ o relație pe A . Spunem că ρ este o **relație de ordine** dacă ea este reflexivă, antisimetrică și tranzitivă.

Definiția 100. Numim **mulțime ordonată** orice pereche alcătuită dintr-o mulțime nevidă și o relație de ordine pe aceasta.

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

Observația 101. Relația de ordine uzuală pe \mathbb{R} este, desigur, o relație de ordine conform definiției 99. Pe de altă parte, vom constata în cele ce urmează că în categoria relațiilor de ordine se vor încadra și alte relații frecvent întâlnite (iar statutul de relație de ordine al unora dintre acestea va fi la o primă vedere chiar surprinzător).

Exemplul 102. Dată fiind o mulțime nevidă, relația de egalitate pe aceasta este o relație de ordine.

Exemplul 103. Dată fiind o mulțime nevidă, relația de incluziune pe $\mathcal{P}(A)$ este o relație de ordine.

Exemplul 104. Relația de divizibilitate pe \mathbb{N} este o relație de ordine.

Exemplul 105. Relația de divizibilitate pe \mathbb{Z} nu este o relație de ordine.

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

Temă: Argumentați afirmațiile de la exemplele 102, 103, 104, 105 și 106!

Definiția 107. Date fiind două mulțimi ordonate (A, \leq) și (B, \preceq) , o funcție $f : A \rightarrow B$ se numește **morfism de mulțimi ordonate** dacă $\forall x, y \in A \quad x \leq y \Rightarrow f(x) \preceq f(y)$. f se numește **antimorfism de mulțimi ordonate** dacă $\forall x, y \in A \quad x \leq y \Rightarrow f(x) \succeq f(y)$.

Definiția 108. Un (anti)morfism de mulțimi ordonate se numește **(anti)izomorfism de mulțimi ordonate** dacă este inversabil și dacă inversul său este (anti)morfism de mulțimi ordonate.

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

11. RELAȚII ÎNRUDITE CU RELAȚIILE DE ORDINE

Relațiile de la exemplele 105 și 106 sugerează următoarele definiții:

Definiția 110. Fie A o mulțime nevidă și ρ o relație pe A . Spunem că ρ este o **relație de preordine** (sau **de cuasiordine**) dacă ea este reflexivă și tranzitivă.

Observația 111. Orice relație de ordine este și relație de preordine.

Observația 112. Relația de divizibilitate pe \mathbb{Z} este o relație de preordine.

Definiția 113. Numim **mulțime preordonată** orice pereche alcătuită dintr-o mulțime nevidă și o relație de preordine pe aceasta.

Definiția 114. Fie A o mulțime nevidă și ρ o relație pe A . Spunem că ρ este o **relație de ordine strictă** dacă ea este ireflexivă și tranzitivă.

Dată fiind o relație de preordine ρ pe mulțimea A , ei i se poate asocia o relație de ordine (definită pe o mulțime factor a lui A) în următorul mod:

Considerăm pe A relația $a\sigma b \stackrel{\text{def}}{\Leftrightarrow} a\rho b \wedge b\rho a$.

Este imediat faptul că σ este o relație de echivalență pe A .

Pe mulțimea A/σ definim relația $\hat{a}\tau\hat{b} \stackrel{\text{def}}{\Leftrightarrow} a\rho b$.

Se verifică (temă!) că τ este (corect definită și) relație de ordine și că proiecția canonică $p : A \rightarrow A/\sigma$ are proprietatea $\forall a, b \in A$ $a\rho b \Rightarrow p(a)\tau p(b)$.

În ceea ce privește relațiile de ordine strictă, avem:

Propoziția 115. Dată fiind o mulțime nevidă A , există o bijecție canonică între mulțimea relațiilor de ordine pe A și mulțimea relațiilor de ordine strictă pe A .

Demonstrație: Considerăm funcția Φ ce asociază fiecărei relații de ordine ρ pe A relația $\rho \setminus \Delta_A$ și funcția Ψ ce asociază fiecărei relații de ordine strictă σ pe A relația $\sigma \cup \Delta_A$. Este imediat că Φ și Ψ acționează între mulțimile precizate în enunț și că sunt inverse una celeilalte. \square

12. TIPURI INTERESANTE DE MULȚIMI ORDONATE

Fie \leq o relație de ordine pe mulțimea A .

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

Definiția 117. Submulțimea nevidă B a lui A se numește **majorată** dacă există în A cel puțin un majorant pentru B .

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

Definiția 119. Submulțimea nevidă B a lui A se numește **minorată** dacă există în A cel puțin un minorant pentru B .

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

Observația 121. Este posibil ca anumite submulțimi ale lui A să nu admită prim element. Dacă însă o submulțime a lui A admite prim element, antisimetria relației \leq arată că acesta este unic.

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

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

Observația 123. Este posibil ca anumite submulțimi ale lui A să nu admită ultim element. Dacă însă o submulțime a lui A admite ultim element, antisimetria relației \leq arată că acesta este unic.

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

Definiția 124. Numim **element minimal** al mulțimii ordonate A orice element a al lui A cu proprietatea $\forall b \in A \ b \leq a \Rightarrow b = a$.

Definiția 125. Numim **element maximal** al mulțimii ordonate A orice element a al lui A cu proprietatea $\forall b \in A \ b \geq a \Rightarrow b = a$.

Definiția 126. Spunem că mulțimea ordonată (A, \leq) este **total ordonată** dacă relația \leq este totală.

Definiția 127. Spunem că mulțimea ordonată (A, \leq) este **bine ordonată** dacă orice submulțime nevidă a lui A admite prim element.

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

Definiția 129. Numim **supremum** al submulțimii nevide și majorate B a lui A cel mai mic majorant (din A) al lui B .

Observația 130. Este posibil ca anumite submulțimi ale lui A să nu admită supremum. Dacă însă o submulțime a lui A admite supremum, acesta este unic conform observației 121.

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

Definiția 131. Numim **infimum** al submulțimii nevide și minorate B a lui A cel mai mare minorant (din A) al lui B .

Observația 132. Este posibil ca anumite submulțimi ale lui A să nu admită infimum. Dacă însă o submulțime a lui A admite infimum, acesta este unic conform observației 123.

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

Definiția 133. Mulțimea ordonată (A, \leq) se numește **latice** dacă pentru orice $a, b \in A$ există $\inf\{a, b\}$ și $\sup\{a, b\}$.

Definiția 134. Mulțimea ordonată (A, \leq) se numește **latice completă** dacă pentru orice submulțime nevidă B a lui A există $\inf B$ și $\sup B$.

BIBLIOGRAFIE

- [1] T. Dumitrescu, *Algebra*, Ed. Universității din București, 2006.
- [2] P. Halmos, *Naive set theory*, Springer Verlag, 1960.
- [3] C. Năstăsescu, C. Niță, C. Vraciu, *Bazele algebrei*, Ed. Academiei, București, 1986.
- [4] C. Năstăsescu, *Introducere în teoria mulțimilor*, Ed. Didactică și Pedagogică, București, 1974.

CURSUL 6: NUMERE CARDINALE

G. MINCU

1. NUMERE CARDINALE

Așa cum am precizat încă de la al doilea curs, considerarea unei mulțimi a tuturor mulțimilor conduce la paradoxuri. Vom conveni că toate mulțimile alcătuiesc un alt tip de entitate, pe care o vom numi **clasă**. Fără a intra în detalii tehnice, vom considera că definițiile pe care le-am dat pentru relațiile de ordine și relațiile de echivalență pot fi utilizate și în contextul claselor.

Definim relația \sim între două mulțimi astfel: $A \sim B$ dacă și numai dacă există o funcție bijectivă de la A la B .

Propoziția 1. Relația \sim este de echivalență.

Temă: Demonstrați propoziția 1!

Definiția 2. Dacă pentru mulțimile A și B avem $A \sim B$, unde \sim este relația introdusă mai sus, spunem că A și B sunt **cardinal echivalente** sau **echipotente**.

Definiția 3. Clasa de echivalență cardinală a unei mulțimi A se numește **numărul cardinal al lui A** . În acest text, vom folosi pentru numărul cardinal al mulțimii A notațiile $|A|$ sau $\text{Card } A$.

Definiția 4. O mulțime se numește **numărabilă** dacă ea este cardinal echivalentă cu \mathbb{N} .

Definiția 5. O mulțime se numește **cel mult numărabilă** dacă ea este finită sau numărabilă.

Definiția 6. O mulțime se numește **nenumărabilă** dacă nu este cel mult numărabilă.

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

Propoziția 7. Mulțimea \mathbb{Z} este numărabilă.

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

2. INEGALITĂȚI PENTRU NUMERE CARDINALE

Definim pe clasa numerelor cardinale relația $|A| \preceq |B|$ dacă și numai dacă există o funcție injectivă $f : A \rightarrow B$. Vom scrie $|A| \prec |B|$ dacă $|A| \preceq |B|$ și $|A| \neq |B|$.

Observația 8. Relația \preceq este corect definită deoarece dacă $f : A \rightarrow B$ este injectivă, $|A| = |A'|$, iar $|B| = |B'|$, atunci există funcții bijective $\alpha : A \rightarrow A'$ și $\beta : B \rightarrow B'$; în consecință, $\beta \circ f \circ \alpha^{-1} : A' \rightarrow B'$ este injectivă.

Observația 9. Deoarece pentru orice mulțime funcția sa identică este injectivă, relația \preceq este reflexivă.

Observația 10. Deoarece compusa oricăror două funcții injective este injectivă, relația \preceq este tranzitivă.

Teorema 11. (Cantor, Bernstein, Schröder)

Fie două mulțimi A și B . Dacă există funcțiile injective $f : A \rightarrow B$ și $g : B \rightarrow A$, atunci există o funcție bijectivă $h : A \rightarrow B$.

Corolarul 12. Relația \preceq este antisimetrică.

Cele precedente demonstrează

Propoziția 13. Relația \preceq este de ordine.

Utilizând cele precedente, putem proba:

Propoziția 14. Mulțimea \mathbb{Q} este numărabilă.

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

Propoziția 15. Mulțimile \mathbb{R} și \mathbb{C} sunt nenumărabile.

3. OPERAȚII CU NUMERE CARDINALE

3.1. Înmulțirea numerelor cardinale. Observația că pentru $|A| = a \in \mathbb{N}$ și $|B| = b \in \mathbb{N}$ avem $|A \times B| = ab$ ne sugerează:

Definiția 16. Prin **produsul** numerelor cardinale $\alpha = |A|$ și $\beta = |B|$ înțelegem numărul cardinal $\alpha\beta \stackrel{\text{def}}{=} |A \times B|$.

Definiția 16 este corectă în virtutea observației următoare:

Observația 17. Dacă $|A| = |A'|$ și $|B| = |B'|$, atunci $|A \times B| = |A' \times B'|$.

Demonstrație: Date fiind bijecțiile $f : A \rightarrow A'$ și $g : B \rightarrow B'$, funcția $f \times g : A \times B \rightarrow A' \times B'$, $f \times g(a, b) = (f(a), g(b))$ este bijecție (temă!). Prin urmare, $|A \times B| = |A' \times B'|$. \square

3.2. Ridicarea la putere a numerelor cardinale. Observația că pentru $|A| = a \in \mathbb{N}$ și $|B| = b \in \mathbb{N}$ avem $|\{f : A \rightarrow B\}| = b^a$ ne-a condus în cursul 2 la notația $B^A = \{f : A \rightarrow B\}$. În contextul discuției de față, ea ne sugerează:

Definiția 18. Date fiind numerele cardinale $\alpha = |A|$ și $\beta = |B|$,

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

Definiția 18 este corectă în virtutea observației următoare:

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

Demonstrație: Date fiind bijecțiile $f : A \rightarrow A'$ și $g : B \rightarrow B'$, funcția $h : B^A \rightarrow (B')^{A'}$, $h(\varphi) = g \circ \varphi \circ f^{-1}$ este bijecție (temă!). Prin urmare, $|B^A| = |(B')^{A'}|$. \square

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

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

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

Această relație se generalizează după cum urmează:

Propoziția 20 (Principiul includerii și excluderii). Fie $n \in \mathbb{N}^*$ și mulțimile finite A_1, A_2, \dots, A_n . Atunci

$$(1) \quad |A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \\ + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| + \dots + (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n|.$$

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

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

adică tot cu o unitate. \square

Revenind acum pe direcția principală a prezentării, constatăm, inspirându-ne din abordările de la definițiile operațiilor de înmulțire și de ridicare la putere a numerelor cardinale, că ne-ar conveni în acest moment să avem la dispoziție o operație cu mulțimi care să asocieze la două mulțimi date nu reuniunea lor, ci mai degrabă reuniunea a două mulțimi cardinal echivalente cu ele și disjuncte. Aceste considerații conduc la:

Definiția 21. Prin reuniunea disjunctă a mulțimilor A și B înțelegem mulțimea $A \sqcup B \stackrel{\text{def}}{=} (A \times \{1\}) \cup (B \times \{2\})$.

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

Definiția 23. Date fiind numerele cardinale $\alpha = |A|$ și $\beta = |B|$,

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

Definiția 23 este corectă în virtutea observației următoare:

Observația 24. Dacă $|A| = |A'|$ și $|B| = |B'|$, atunci $|A \sqcup B| = |A \sqcup B'|$.

Demonstrație: Date fiind bijecțiile $f : A \rightarrow A'$ și $g : B \rightarrow B'$, funcția

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

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

4. CATEVA PROPRIETĂȚI ALE OPERAȚIILOR CU NUMERE CARDINALE

Prezentăm aici câteva proprietăți ale operațiilor cu numere cardinale definite în capitolul precedent. Cu două excepții, marcate cu asterisc, ele sunt ușor de demonstrat și vi le propunem ca temă. Menționăm și că bună parte dintre aceste proprietăți pot fi enunțate și demonstrate în forme mult mai generale; trimitem cititorul interesat, de pildă, la [4].

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

Propoziția 27. Date fiind numerele cardinale α, β, γ au loc relațiile:

(i) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.

(ii) $\alpha + \beta = \beta + \alpha$.

(iii) $\alpha + 0 = \alpha$.

(iv)* Dacă α este infinit, $\alpha + \alpha = \alpha$.

Propoziția 28. Date fiind numerele cardinale α, β, γ au loc relațiile:

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

Propoziția 29. Date fiind numerele cardinale α, β, γ au loc relațiile:

(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 MULȚIME

Teorema 30 (Cantor). Pentru orice mulțime A avem $\mathcal{P}(A) \approx A$.

Demonstrație: Presupunem că $\mathcal{P}(A) \sim A$. Există deci o bijecție $f : A \rightarrow \mathcal{P}(A)$. 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 $m \notin f(m) = M$, contradicție.

Dacă $m \notin M$, atunci $m \in f(m) = M$, contradicție.

Rămâne așadar că $\mathcal{P}(A) \not\sim A$. \square

Corolarul 31. Pentru orice număr cardinal α are loc relația $\alpha < 2^\alpha$.

Teorema 32. Numerele cardinale nu constituie o mulțime.

Demonstrație: Presupunem că numerele cardinale constituie o mulțime, fie ea \mathcal{M} . Notăm cu R reuniunea mulțimii formate din câte un reprezentant al fiecărui element al lui \mathcal{M} . Atunci $2^{|R|}$ este un număr cardinal și avem relațiile $2^{|R|} \preceq |R| \prec 2^{|R|}$, contradicție. \square

REFERENCES

- [1] T. Dumitrescu, *Algebra*, Ed. Universității din București, 2006.
- [2] P. Halmos, *Naive set theory*, Springer Verlag, 1960.
- [3] C. Năstăsescu, C. Niță, C. Vraciu, *Bazele algebrei*, Ed. Academiei, București, 1986.
- [4] C. Năstăsescu, *Introducere în teoria mulțimilor*, Ed. Didactică și Pedagogică, București, 1974.

CURSUL 7: LEGI DE COMPOZIȚIE

G. MINCU

1. LEGI DE COMPOZIȚIE

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

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

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

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

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

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

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

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

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

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

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

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

2. PARTE STABILĂ. OPERAȚIE INDUSĂ

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

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

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

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

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

3. ASOCIATIVITATE

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

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

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

Temă: Justificați afirmațiile de la observația 17!

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

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

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

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

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

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

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

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

4. COMUTATIVITATE

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

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

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

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

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

Temă: Justificați afirmațiile de la observația 25!

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

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

5. ELEMENT NEUTRU

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6. SIMETRIZABILITATE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. SEMIGRUPURI

7.1. Semigrupuri.

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

Observația 60. Dacă legea de compoziție \cdot este subînțeleasă în context, vom spune frecvent „semigrupul S ” în loc de „semigrupul (S, \cdot) ”. De asemenea, în loc de „ (S, \cdot) este semigrup” vom spune frecvent „ S are o structură de semigrup în raport cu \cdot ”.

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

7.2. Reguli de calcul în semigrupuri.

Propoziția 62. Fie (S, \cdot) un semigrup, $x, y \in S$ și $m, n \in \mathbb{N}^*$. Atunci:

- a) $x^{m+n} = x^m \cdot x^n$.
- b) $(x^m)^n = x^{mn}$.
- c) Dacă x și y comută, atunci $(xy)^m = x^m y^m$.

Demonstrație: Relația de la a) reiese din observația 20. Punctul b) se probează prin inducție după n , iar c), prin inducție după m . Lăsăm detaliile în grija cititorului. \square

7.3. Morfisme de semigrupuri.

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

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

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

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

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

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

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

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

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

Demonstrație: „ \Rightarrow ”: Evident.

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

8. MONOIZI

8.1. Monoizi.

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

Observația 70. Dacă legea de compoziție \cdot este subînțeleasă în context, vom spune frecvent „monoidul M ” în loc de „monoidul (M, \cdot) ”. De asemenea, în loc de „ (M, \cdot) este monoid” vom spune frecvent „ M are o structură de monoid în raport cu \cdot ”.

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

8.2. Reguli de calcul în monoizi. Fie (M, \cdot) un monoid și $x \in M$.

Notăm $x^0 \stackrel{\text{def}}{=} 1$.

Propoziția 72. Fie (M, \cdot) un monoid, $x, y \in M$ și $m, n \in \mathbb{N}$. Atunci:

- a) $x^{m+n} = x^m \cdot x^n$.
- b) $(x^m)^n = x^{mn}$.
- c) Dacă x și y comută, atunci $(xy)^m = x^m y^m$.

Demonstrație: Pentru $mn \neq 0$ se aplică propoziția 62, iar pentru $mn = 0$ relațiile din enunț sunt imediate. \square

8.3. Morfisme de monoizi.

Definiția 73. Fie M și M' doi monoizi (în notație multiplicativă). O funcție $f : M \rightarrow M'$ se numește **morfism de monoizi** dacă:

- a) $\forall x, y \in M \quad f(xy) = f(x)f(y)$.
- b) $f(1_M) = 1_{M'}$ (1_M și $1_{M'}$ desemnând aici elementele neutre ale celor doi monoizi).

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

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

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

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

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

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

Demonstrație: „ \Rightarrow ”: Evident.

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

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

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

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

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

Vom nota cuvântul vid cu \sqcup .

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

Temă: Demonstrați propoziția 81!

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

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

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

Temă: Demonstrați propoziția 83!

BIBLIOGRAFIE

- [1] T. Dumitrescu, *Algebra*, Ed. Universității din București, 2006.
- [2] I. D. Ion, N. Radu, *Algebră*, Ed. Didactică și Pedagogică, București, 1981.
- [3] C. Năstăsescu, C. Niță, C. Vraciu, *Bazele algebrei*, Ed. Academiei, București, 1986.

CURSUL 8: GRUPURI

G. MINCU

1. GRUPURI

Definiția 1. Fie G o mulțime nevidă și „ \cdot ” o lege de compoziție pe G . Perechea (G, \cdot) se numește **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 și comutativă, grupul (G, \cdot) se numește **comutativ** sau **abelian**.

Observația 2. Dacă legea de compoziție „ \cdot ” este subînțeleasă 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 ” ”.

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

2. EXEMPLE DE GRUPURI

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

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

Observația 6. Datorită faptelor evidențiate în exemplele 4 și 5, ne vom permite uneori să facem referire la „grupul \mathbb{Z} ”, „grupul \mathbb{Q} ”, „grupul \mathbb{R} ” sau „grupul \mathbb{C} ” subînțelegând considerarea pe acestea a structurii aditive. Dacă dorim să ne referim la o altă structură de grup pe aceste mulțimi, 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 înmulțirea modulo n . Acest monoid nu este grup, întrucât elementul $\hat{0}$ nu este simetrizabil.

Observația 10. Având în vedere exemplele 8 și 9, ne vom permite uneori să facem referire la „grupul \mathbb{Z}_n ” subînțelegând 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 mulțime nevidă, atunci G^A are o structură de grup (abelian) în raport cu legea de compoziție definită la exemplul 6 din cursul 4.

Exemplul 12. Fie $(G_i)_{i \in I}$ este o familie de grupuri (în notație multiplicativă). Pe $G \stackrel{\text{def}}{=} \prod_{i \in I} G_i$ introducem legea de compoziție

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

Propoziția 13. Mulțimea G din exemplul 12 are în raport cu operația introdusă acolo o structură de grup. Acest grup este abelian dacă și numai dacă toate grupurile G_i sunt abeliene.

Temă: Demonstrați afirmațiile de la exemplele 5, 7, 8, 9, 11 și propoziția 13!

Definiția 14. Grupul de la exemplul 12 se numește **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 mulțimea finită $I = \{i_1, i_2, \dots, i_n\}$ **notațiile** $\prod_{k=1}^n G_{i_k}$ sau $G_{i_1} \times G_{i_2} \times \dots \times G_{i_n}$.

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

3. GRUPUL ELEMENTELOR SIMETRIZABILE DINTR-UN MONOID

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

Propoziția 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 operația indusă de „ \cdot ”.

Demonstrație: a) Fie $x, y \in U(M)$. Atunci $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = e$ și $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = e$, deci $y^{-1}x^{-1} = (xy)^{-1}$, de unde $xy \in U(M)$.

b) Evident. \square

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

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

Exemplul 18. (\mathbb{Q}^*, \cdot) , (\mathbb{R}^*, \cdot) și (\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 notația $U(\mathbb{Z}_n)$ pentru a desemna grupul elementelor din \mathbb{Z}_n simetrizabile în raport cu înmulțirea modulo n .

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

Temă: Demonstrați propoziția 21!

Observația 22. Fie A o mulțime nevidă. Elementele simetrizabile ale monoidului (A^A, \circ) sunt exact funcțiile bijective.

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

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

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

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

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

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

4. REGULI DE CALCUL ÎN GRUPURI

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

Propoziția 27. Fie (G, \cdot) un grup, $x, y \in G$ și $m, n \in \mathbb{Z}$. Atunci:

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

b) $(x^m)^n = x^{mn}$.

c) Dacă x și y comută, atunci $(xy)^m = x^m y^m$.

Demonstrație: Se procedează ca în demonstrația propoziției similare din cursul 4, analizând suplimentar cazurile în care m sau n sunt negative. Lăsăm detaliile în grija cititorului. \square

Observația 28. Dacă operația grupului G este notată aditiv, atunci relațiile din propoziția 27 devin:

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

b) $n(mx) = (nm)x$.

c) Dacă x și y comută, atunci $m(x+y) = mx + my$.

5. SUBGRUPURI

Definiția 29. Fie G un grup și H o submulțime nevidă a sa. Spunem că H este **subgrup** al lui G dacă:

- i) $\forall x, y \in H \quad xy \in H.$
- ii) $\forall x \in H \quad x' \in H.$

Observația 30. Dacă H este subgrup al lui G , atunci H conține elementul neutru al lui G .

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

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

Propoziția 32. Fie G un grup și H o submulțime nevidă a lui G . Următoarele afirmații sunt echivalente:

- i) $H \leq G$
- ii) $\forall x, y \in H \quad xy' \in H.$

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

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

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

Demonstrație: „ \Leftarrow ”: Se aplică propoziția 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 împărțire cu rest, există $q, r \in \mathbb{Z}$, $0 \leq r < n$, așa încât $x = nq + r$. De aici se obține $r = x - nq \in H$, de unde, conform definiției lui n , $r = 0$. Prin urmare, $x = nq \in n\mathbb{Z}$, deci $H \subset n\mathbb{Z}$. \square

6. MORFISME DE GRUPURI

Definiția 36. Fie G și Γ două grupuri (în notație multiplicativă). O funcție $f : G \rightarrow \Gamma$ se numește **morfism de grupuri** dacă:
 $\forall x, y \in G \quad f(xy) = f(x)f(y).$

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

Propoziția 37. Fie $f : G \rightarrow \Gamma$ un morfism de grupuri. Atunci:

- a) $f(e_G) = e_\Gamma$.
- b) $\forall x \in G \quad f(x') = f(x)'$.
- c) $\forall x \in G \quad \forall n \in \mathbb{Z} \quad f(x^n) = f(x)^n$.

Temă: Demonstrați propoziția 37!

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

Exemplul 39. Pentru orice două grupuri G și Γ , funcția $u : G \rightarrow \Gamma$, $u(x) = e_\Gamma$ este morfism de grupuri.

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

Temă: Demonstrați afirmațiile de la exemplele 38, 39 și 40!

Definiția 41. Morfismul din exemplul 40 se numește **injecția canonică a lui H în G** .

Propoziția 42. Dacă $f : G \rightarrow \Gamma$ și $g : \Gamma \rightarrow \Delta$ sunt morfisme de grupuri, atunci $g \circ f$ este morfism de grupuri.

Temă: Demonstrați propoziția 37!

Definiția 43. Fie G și Γ două grupuri. Un morfism de grupuri $f : G \rightarrow \Gamma$ se numește **izomorfism** dacă există un morfism de grupuri $g : \Gamma \rightarrow G$ cu proprietatea că $f \circ g = \text{id}_\Gamma$ și $g \circ f = \text{id}_G$.

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

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

Propoziția 46. $f : G \rightarrow \Gamma$ este izomorfism de grupuri dacă și numai dacă f este morfism bijectiv de grupuri.

Demonstrație: „ \Rightarrow ”: Evident.

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

Definiția 47. Un morfism de grupuri $f : G \rightarrow G$ se numește **endomorfism** al lui G .

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

Observația 48. $\text{End}_{\text{Grp}}(G) = \text{Hom}_{\text{Grp}}(G, G)$.

Definiția 49. Un izomorfism de grupuri $f : G \rightarrow G$ se numește **automorfism** al lui G .

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

7. MORFISME ȘI SUBGRUPURI

Propoziția 50. Fie $f : G \rightarrow \Gamma$ un morfism de grupuri, $H \leq G$ și $K \leq \Gamma$. Atunci:

- a) $f(H) \leq \Gamma$.
- b) $f^{-1}(K) \leq G$.

Demonstrație: a) Fie $y_1, y_2 \in f(H)$. Atunci, există $x_1, x_2 \in H$ astfel încât $y_1 = f(x_1)$ și $y_2 = f(x_2)$. Deducem că $y_1 y_2' = f(x_1) f(x_2)' = f(x_1 x_2') \in f(H)$.

b) Fie $x_1, x_2 \in f^{-1}(K)$. Atunci $f(x_1 x_2') = f(x_1) f(x_2)' \in K$, deci $x_1 x_2' \in f^{-1}(K)$. \square

Nucleul și imaginea unui morfism. Considerațiile din acest paragraf se referă la un morfism de grupuri $f : G \rightarrow \Gamma$.

Definiția 51. Mulțimea $\{x \in G : f(x) = e_\Gamma\}$ se numește **nucleul** lui f și se notează $\ker f$.

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

Propoziția 53. Morfismul f este injectiv dacă și numai dacă $\ker f = \{e_G\}$.

Demonstrație: „ \Rightarrow ”: Dacă $x \in \ker f$, $f(x) = e_\Gamma = f(e_G)$; din injectivitatea lui f deducem că $x = e_G$.

„ \Leftarrow ”: Fie $x_1, x_2 \in G$ astfel ca $f(x_1) = f(x_2)$. Atunci $f(x_1 x_2') = e_\Gamma$, de unde $x_1 x_2' \in \ker f$. Rezultă că $x_1 x_2' = e_G$, deci $x_1 = x_2$. \square

Observația 54. Conform propoziției 50, $\text{Im} f \leq \Gamma$.

Propoziția 55. Morfismul f este surjectiv dacă și numai dacă $\text{Im} f = \Gamma$.

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

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

BIBLIOGRAFIE

- [1] T. Dumitrescu, *Algebra*, Ed. Universității din București, 2006.
- [2] I. D. Ion, N. Radu, *Algebră*, Ed. Didactică și Pedagogică, București, 1981.
- [3] C. Năstăsescu, C. Niță, C. Vraciu, *Bazele algebrei*, Ed. Academiei, București, 1986.

CURSUL 9: SUBGRUP NORMAL. GRUP FACTOR

G. MINCU

1. RELAȚII DE ECHIVALENȚĂ MODULO UN SUBGRUP

Fie G un grup și $H \leq G$. Considerăm următoarele relații pe G :

a) $x \equiv_s y \pmod{H}$ dacă și numai dacă $x^{-1}y \in H$

b) $x \equiv_d y \pmod{H}$ dacă și numai dacă $xy^{-1} \in H$.

Propoziția 1. Relațiile \equiv_s și \equiv_d sunt de echivalență.

Temă: Demonstrați propoziția 1!

Definiția 2. \equiv_s se numește **relația de echivalență la stânga modulo subgrupul H** , iar \equiv_d se numește **relația de echivalență la dreapta modulo subgrupul H** .

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

Propoziția 3. Fie G un grup, $H \leq G$ și $x \in G$. Atunci:

a) Clasa de echivalență a lui x în raport cu $\equiv_s \pmod{H}$ este xH .

b) Clasa de echivalență a lui x în raport cu $\equiv_d \pmod{H}$ este Hx .

Demonstrație: a) $y \in \hat{x} \Leftrightarrow x^{-1}y \in H \Leftrightarrow y \in xH$.

b) Analog. \square

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

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

Demonstrație: Definim $f : (G/H)_s \rightarrow (G/H)_d$, $f(xH) = Hx^{-1}$ și $g : (G/H)_d \rightarrow (G/H)_s$, $g(Hx) = x^{-1}H$.

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 și g sunt inverse una celeilalte, deci ele sunt bijective, de unde concluzia. \square

Definiția 6. Cardinalul comun al mulțimilor $|(G/H)_s|$ și $|(G/H)_d|$ se numește **indicele lui H în G** .

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

Definiția 7. Prin **ordinul** grupului G înțelegem cardinalul lui G . Notăția folosită în mod uzual pentru ordinul lui G este $|G|$.

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

Demonstrație: Definim $f : xH \rightarrow H$, $f(t) = x^{-1}t$ și $g : H \rightarrow xH$, $g(h) = xh$.

Este imediat că f și g sunt corect definite și inverse una celeilalte, deci ele sunt bijective, de unde concluzia. \square

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

Demonstrație: Avem $G = \coprod_{xH \in (G/H)_s} xH$, deci $|G| = \sum_{xH \in (G/H)_s} |xH|$.

Conform lemei 8, din această relație obținem $|G| = |H| \cdot |(G/H)_s|$. \square

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

2. SUBGRUPURI NORMALE

Propoziția 10. Fie G un grup și $H \leq G$. Următoarele afirmații 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: Demonstrați propoziția 10!

Definiția 11. Fie G un grup și $H \leq G$. Spunem că H este **subgrup normal** al lui G dacă îndeplinește una dintre condițiile echivalente din propoziția 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 $f : G \rightarrow G'$ este un morfism de grupuri, atunci $\ker f \trianglelefteq G$.

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

Propoziția 17. Dacă $f : G \rightarrow G'$ 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 corespondență pentru subgrupuri se completează astfel:

Teorema 18. Fie $f : G \rightarrow G'$ un morfism surjectiv de grupuri. Notăm $\mathcal{H} = \{H \leq G : H \supset \ker f\}$ și $\mathcal{K} = \{K : K \leq G'\}$. Atunci funcțiile $\Phi : \mathcal{H} \rightarrow \mathcal{K}$, $\Phi(H) = f(H)$ și $\Psi : \mathcal{K} \rightarrow \mathcal{H}$, $\Psi(K) = f^{-1}(K)$ sunt (bijective și) inverse una celeilalte și păstrează incluziunile. În plus, subgrupurile normale ale lui G care conțin $\ker f$ corespund via aceste funcții subgrupurilor normale ale lui G' .

3. GRUP FACTOR

Observația 19. Fie G un grup și $H \trianglelefteq G$. Atunci pe mulțimea $(G/H)_s$ este corect definită legea de compoziție $(xH) \cdot (yH) = (xy)H$.

Temă: Demonstrați observația 19!

Definiția 20. Fie G un grup și $H \trianglelefteq G$. Prin **grupul factor al lui G în raport cu H** înțelegem grupul care are mulțimea subiacentă $(G/H)_s$ și legea de compoziție $(xH) \cdot (yH) = (xy)H$.

Notăția 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 notația \hat{x} . În notație aditivă, în loc de xH vom scrie, desigur, $x + H$.

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

Observația 22. Fie G un grup și $H \trianglelefteq G$. Aplicația $\pi : G \rightarrow \frac{G}{H}$, $\pi(x) = \hat{x}$ este morfism surjectiv de grupuri.

Definiția 23. Fie G un grup și $H \trianglelefteq G$. Morfismul π din observația 22 se numește **surjecția canonică** (sau **proiecția canonică**) a grupului factor $\frac{G}{H}$.

Proprietatea de universalitate a grupului factor. Fie G un grup, $H \trianglelefteq G$, $\pi : G \rightarrow \frac{G}{H}$ surjecția canonică și $f : G \rightarrow G'$ un morfism de grupuri. Atunci:

- i) Dacă $H \subset \ker f$, atunci există un unic morfism $u : \frac{G}{H} \rightarrow G'$ astfel încât $u \circ \pi = f$. În plus:
- ii) u este injectivă dacă și numai dacă $H = \ker f$.
- iii) u este surjectivă dacă și numai dacă f este surjectivă.

Temă: Demonstrați proprietatea de universalitate a grupului factor!

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

4. TEOREMA FUNDAMENTALĂ DE IZOMORFISM PENTRU GRUPURI

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

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

în mod canonic, via $\bar{f}(\hat{x}) = f(x)$.

*Demonstrație*¹: Definim $\bar{f} : \frac{G}{\ker f} \rightarrow \text{Im } f$, $\bar{f}(\hat{x}) = f(x)$.

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

Dacă $x, y \in G$, atunci $\bar{f}(\hat{x}\hat{y}) = \bar{f}(\widehat{xy}) = f(xy) = f(x)f(y) = \bar{f}(\hat{x})\bar{f}(\hat{y})$.

Așadar, \bar{f} este morfism de grupuri.

Este evident că \bar{f} este surjectivă.

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

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

¹ O demonstrație mai rapidă a acestei teoreme se obține utilizând proprietatea de universalitate a grupului factor. Lăsăm ca exercițiu cititorului această abordare.

BIBLIOGRAFIE

- [1] T. Dumitrescu, *Algebra*, Ed. Universității din București, 2006.
- [2] I. D. Ion, N. Radu, *Algebră*, Ed. Didactică și Pedagogică, București, 1981.
- [3] C. Năstăsescu, C. Niță, C. Vraciu, *Bazele algebrei*, Ed. Academiei, București, 1986.

CURSUL 10: GRUPURI

G. MINCU

1. SUBGRUPUL GENERAT DE O SUBMULTIME

Definiția 1. Fie G un grup și $M \subset G$. Prin **subgrupul lui G generat de M** înțelegem cel mai mic (în sensul incluziunii) subgrup al lui G care conține submulțimea M .

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

Propoziția 2. Fie G un grup și $M \subset G$. Are loc relația

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

Propoziția 3. Fie G un grup și $M \subset G$. Are loc relația

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

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

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

Definiția 6. Fie G un grup. Submulțimea M a lui G se numește **sistem de generatori** al lui G dacă $\langle M \rangle = G$.

Definiția 7. Grupul G se numește **finit generat** dacă el admite un sistem finit de generatori.

Exemplul 8. Orice grup admite ca sistem de generatori mulțimea 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: Demonstrați afirmațiile de la exemplele 8-15!

2. GRUPURI CICLICE

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

Observația 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 $\mathbb{Z}_n = \langle \hat{1} \rangle$.

Observația 20. Generatorul unui grup ciclic nu este unic determinat. De exemplu, avem și $\mathbb{Z} = \langle -1 \rangle$, iar $\mathbb{Z}_n = \langle \hat{a} \rangle$ dacă și 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} .

Demonstrație: Fie G un grup ciclic și g un generator al acestuia. Considerăm $u : \mathbb{Z} \rightarrow G$, $u(n) = g^n$. 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, obținem $G = \text{Im } u \simeq \frac{\mathbb{Z}}{\ker u}$. 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

Observația 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.

Definiția 27. Prin **ordinul** elementului x al grupului G înțelegem ordinul subgrupului generat de x în G .

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

Caracterizări ale ordinului.

Propoziția 28. Fie G un grup și $x \in G$. 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 $x^{\text{ord } x} = e$.

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

Proprietăți ale ordinului.

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

Demonstrație: Ordinul unui element, fiind ordinul unui subgrup, divide, conform teoremei lui Lagrange, ordinul grupului. \square

Propoziția 32. Dacă G , G_1 și G_2 sunt grupuri finite, atunci:

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

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

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

Temă: Rămâne adevărată afirmația de la punctul (iv) al propoziției 32 în lipsa condiției $xy = yx$?

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

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

Este ea adevărată?

4. APLICAȚII

Definiția 33. Funcția $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$, $\varphi(n)$ = numărul numerelor naturale ce nu-l întrec pe n și sunt prime cu n , se numește **indicatorul lui Euler**.

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

Propoziția 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

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

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

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

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

Demonstrație: Întrucât pentru orice număr prim p avem $\varphi(p) = p - 1$, obținem concluzia aplicând teorema lui Euler. \square

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

Demonstrație: „ \Rightarrow ”: Corespondentul (\hat{a}, \bar{b}) al lui $\hat{1}$ prin izomorfism are ordinul $[\text{ord}_{\mathbb{Z}_m} \hat{a}, \text{ord}_{\mathbb{Z}_n} \bar{b}]$, dar și mn . Deci, $mn = [\text{ord}_{\mathbb{Z}_m} \hat{a}, \text{ord}_{\mathbb{Z}_n} \bar{b}] | [m, n]$; cum $mn = [m, n] \cdot (m, n)$, obținem $(m, n) = 1$.

„ \Leftarrow ”: Este imediat că funcția $f : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$, $f(\tilde{a}) = (\hat{a}, \bar{a})$ este (corect definită și) morfism injectiv de grupuri. Cum atât domeniul cât și codomeniul său au mn elemente, ea este și surjectivă. Prin urmare, f este izomorfism de grupuri. \square

Grupuri cu număr „mic” de elemente.

Definiția 37. Prin **tipul de izomorfism** al grupului G înțelegem clasa de echivalență a lui G în raport cu relația de izomorfism. Uneori, ne vom referi la tipul de izomorfism al lui G spunând, pe scurt, **tipul lui G** .

Observația 38. Orice grup cu număr prim de elemente este **ciclic**.

Demonstrație: Considerăm un grup G cu un număr prim p de elemente și $x \in G \setminus \{e\}$. Atunci, $|\langle x \rangle| > 1$ și $|\langle x \rangle|$ 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, și anume \mathbb{Z}_2 .

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

Pentru viitoarele considerații avem nevoie de următorul instrument:

Propoziția 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 $G \simeq \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2}_{n \text{ factori}}$.

Problemă suplimentară: Demonstrați propoziția 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 situația

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

În aceste condiții obținem, aplicând propoziția 42, că $|G| \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Am obținut deci:

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

Grupuri cu șase elemente. Fie G un grup cu șase 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 $\text{ord } x = 2$. În aceste condiții obținem, aplicând propoziția 42, că $|G|$ este putere de doi, ceea ce reprezintă o contradicție.

Prin urmare, G admite elemente de ordin 3; fie x un astfel de element și $y \in G \setminus \{e, x, x^2\}$. Se arată ușor că $G = \{e, x, x^2, y, xy, x^2y\}$ și, eliminând celelalte posibilități, că $y^2 = e$. Dacă $yx = xy$ obținem

imediat faptul că $\text{ord}_G(xy) = 6$, contradicție. Eliminând celelalte posibilități (de pildă, $yx = e$ ar duce la contradicția $y = x^2$, ș. a. m. d.), constatăm că $yx = x^2y$. Prin urmare, $G \simeq D_3 \simeq S_3$.

Am obținut așadar:

Propoziția 44. Există exact două tipuri de grupuri cu șase elemente: \mathbb{Z}_6 și S_3 .

Temă: Determinați tipurile de grupuri cu șapte, respectiv cu opt elemente!

BIBLIOGRAFIE

- [1] T. Dumitrescu, *Algebra*, Ed. Universității din București, 2006.
- [2] I. D. Ion, N. Radu, *Algebra*, Ed. Universității din București, 1981.
- [3] C. Năstăsescu, C. Niță, C. Vraciu, *Bazele algebrei*, Ed. Academiei, București, 1986.

CURSUL 12: GRUPURI DE PERMUTĂRI

G. MINCU

1. GRUPURI DE PERMUTĂRI

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

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

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

Observația 2. S_n este ciclic pentru $n \in \{1, 2\}$.

S_n este necomutativ pentru orice $n \geq 3$.

2. DESCOMPUNERI ALE PERMUTĂRIILOR

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

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

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

Definiția 6. Numim *transpoziție* orice ciclu de lungime doi.

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

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

Propoziția 9. Orice două cicluri disjuncte comută.

Demonstrație: Fie $c_1, c_2 \in S_n$ două cicluri disjuncte și $i \in \{1, 2, \dots, n\}$. Întrucât orbitele ciclurilor considerate sunt disjuncte, i nu poate aparține ambelor orbite.

Dacă $c_1(i) = i$, atunci $(c_1 c_2)(i) = c_1(c_2(i)) = c_2(i) = c_2(c_1(i)) =$

$(c_2c_1)(i)$.

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

Observația 10. Calcule similare celor din demonstrația propoziției 9 conduc la concluzia că pentru orice cicluri disjuncte¹ c_1, c_2, \dots, c_r și pentru orice $k \in \{1, 2, \dots, n\}$ există $j \in \{1, 2, \dots, r\}$ astfel încât $(c_1c_2 \dots c_r)(k) = c_j(k)$.

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

Demonstrație: Pentru $\sigma \in S_n$ notăm $\mathcal{M}_\sigma = \{k : \sigma(k) \neq k\}$. Vom demonstra prin inducție după $m = |\mathcal{M}_\sigma|$ că orice permutare σ se poate scrie în mod unic ca produs de cicluri disjuncte ale căror orbite sunt conținute în \mathcal{M}_σ .

Dacă $e = c_1c_2 \dots c_r$ cu factorii din membrul drept cicluri disjuncte, atunci, conform observației 10, $c_1 = c_2 = \dots = c_r = e$. Acest lucru probează afirmația teoremei pentru $m = 0$.

Să considerăm acum o permutare $\sigma \in S_n$ cu $m = |\mathcal{M}_\sigma| > 0$. Există atunci $k \in \{1, 2, \dots, n\}$ cu $\sigma(k) \neq k$. Cum $k_\sigma \stackrel{\text{def}}{=} \{\sigma(k), \sigma^2(k), \dots\} \subset \{1, 2, \dots, n\}$, 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 mulțimi. Este ușor de probat (temă!) relația $k_\sigma = \{k, \sigma(k), \dots, \sigma^{s-1}(k)\}$; punând $c \stackrel{\text{not}}{=} (k, \sigma(k), \dots, \sigma^{s-1}(k))$, 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 inducție, $c^{-1}\sigma$ se scrie ca un produs $c_1c_2 \dots c_r$ de cicluri disjuncte cu orbitele conținute în $\mathcal{M}_{c^{-1}\sigma}$; drept urmare, $cc_1c_2 \dots c_r$ este o descompunere a lui σ în produs de cicluri disjuncte cu orbitele incluse în \mathcal{M}_σ .

Pentru partea de unicitate, păstrând semnificațiile de mai sus pentru k și c, c_1, \dots, c_r , considerăm și scrierea $\sigma = \gamma_1\gamma_2 \dots \gamma_t$ ca produs de cicluri disjuncte. Având în vedere observația 10, există $j \in \{1, 2, \dots, n\}$ pentru care $\sigma(k) = \gamma_j(k)$. După o eventuală renumerotare, putem considera că $j = 1$. Ciclurile $\gamma_1, \gamma_2, \dots, \gamma_t$ 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 relația $cc_1c_2 \dots c_r = \gamma_1\gamma_2 \dots \gamma_t$ cu c^{-1} , obținem $c_1c_2 \dots c_r = \gamma_2\gamma_3 \dots \gamma_t$. În virtutea ipotezei de inducție, $\{c_1, c_2, \dots, c_r\} = \{\gamma_2, \gamma_3, \dots, \gamma_t\}$. Ținând cont și de unicitatea deja probată a scrierii lui e , demonstrația se încheie. \square

¹ sau chiar permutări arbitrare disjuncte, noțiunea definindu-se ca și în cazul ciclurilor

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

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

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

Temă: Demonstrați că:

- i) $S_n = \langle (1, 2), (1, 3), \dots, (1, n) \rangle$.
- ii) $S_n = \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle$.
- iii) $S_n = \langle (1, 2), (1, 2, \dots, n) \rangle$.

3. PERMUTĂRI PARE ȘI IMPARE. SIGNATURĂ

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

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

Propoziția 17. Orice transpoziție este permutare impară.

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

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

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

Observația 19. În produsul din definiția 18 se simplifică de fapt toți numitorii și toți 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 și numai dacă $\varepsilon(\sigma) = 1$.
b) $\sigma \in S_n$ este impară dacă și numai dacă $\varepsilon(\sigma) = -1$.

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

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 $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$.

Observația 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 .

Definiția 26. A_n se numește *grupul altern* de grad n .

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

Demonstrație: Aplicăm corolarul 22, observația 24 și teorema fundamentală de izomorfism pentru grupuri. \square

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

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

Demonstrație: Aplicăm observația 7 și propozițiile 17 și 21. \square

4. ORDINUL UNEI PERMUTĂRI

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

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

Corolarul 31. Orice transpoziție are ordinul 2.

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

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

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

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

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

Demonstrație: Considerăm funcția $\varphi : G \rightarrow S_G$, $\varphi(g) = h_g$, unde $h_g : G \rightarrow G$, $h_g(x) = gx$. 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 obținem 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. Universității din București, 2006.
- [2] I. D. Ion, N. Radu, *Algebră*, Ed. Didactică și Pedagogică, București, 1981.
- [3] C. Năstăsescu, C. Niță, C. Vraciu, *Bazele algebrei*, Ed. Academiei, București, 1986.

CURSUL 13: ELEMENTE DE ALGEBRĂ UNIVERSALĂ

G. MINCU

1. OPERAȚII DE ARITATE FINITĂ

Definiția 1. Fie M o mulțime nevidă și $n \in \mathbb{N}^*$. Numim **lege de compoziție (operație) n -ară** pe M orice funcție $f : M^n \rightarrow M$.

Definiția 2. Dacă f este o operație n -ară pe mulțimea M , atunci n se numește **aritatea** lui f .

Observația 3. O operație de aritate 1 pe mulțimea M este o funcție $f : M \rightarrow M$; uneori, pentru a desemna o operație de aritate 1 folosim și exprimarea „operație **unară**”.

Observația 4. Noțiunea de operație n -ară generalizează noțiunea de operație cu care am lucrat în cursurile 7-11. Toate acele operații erau, în acord cu terminologia introdusă acum, operații de aritate 2, pe care le vom numi și operații **binare** (acest epitet a fost deja menționat avant la lettre în definițiile din cursul 7).

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

Definiția 5. Fie M o mulțime nevidă. Numim **lege de compoziție (operație) 0-ară** pe M alegerea unui element al lui M .

Definiția 6. Vom spune despre orice operație 0-ară că are aritate 0.

Definiția 7. Dacă există $n \in \mathbb{N}$ astfel ca f să fie o operație de aritate n pe mulțimea M , atunci f se numește operație de aritate finită pe M .

2. ALGEBRE UNIVERSALE

Definiția 8. Prin **tip de algebră universală** vom înțelege o familie \mathcal{F} de numere naturale indexată după o mulțime $S_{\mathcal{F}}$. În acest context vom folosi pentru elementele lui $S_{\mathcal{F}}$ denumirea de **simboluri funcționale**.

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

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

Definiția 10. Mulțimea A din definiția de mai sus se numește **universul** (sau **mulțimea subiacentă a**) algebrei universale \mathbf{A} , \mathcal{F} se numește **tipul** sau **signatura** lui \mathbf{A} , iar operațiile $(f^A)_{f \in S_{\mathcal{F}}}$ se numesc **operațiile fundamentale** ale lui \mathbf{A} .

Observația 11. Dacă $\mathbf{A} = \langle A, F \rangle$ este o algebră universală, vom folosi frecvent notația F și pentru a desemna imaginea familiei F , deducând din context ce înțeles trebuie atribuit notației.

Observația 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 subînțeleasă fără a exista posibilitate de confuzie.

Observația 13. Dacă pentru algebra universală $\mathbf{A} = \langle A, F \rangle$ de tipul \mathcal{F} mulțimea $S_{\mathcal{F}}$ este finită, să zicem $S_{\mathcal{F}} = \{f_1, f_2, \dots, f_r\}$, atunci vom folosi și **notația** $\mathbf{A} = \langle A, f_1, f_2, \dots, f_r \rangle$, simbolurile funcționale fiind scrise în ordinea descrescătoare a arităților. În această situație, signatura lui \mathbf{A} va fi prezentată sub forma r -uplului de numere naturale $(\mathcal{F}(f_1), \mathcal{F}(f_2), \dots, \mathcal{F}(f_r))$.

Observația 14. În practică, exemplele concrete de algebre universale se vor încadra în șabloanele generale prezentate până acum, fiind însă individualizate de anumite condiții pe care le satisfac operațiile fundamentale din contextul respectiv pe întregul lor domeniu de definiție („identități”).

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 identitățile:

$$(A) \quad (x \cdot y) \cdot z = x \cdot (y \cdot z),$$

$$(EN) \quad (x \cdot 1) = 1 \cdot x = x \quad \text{și}$$

$$(TES) \quad x \cdot x^{-1} = x^{-1} \cdot x = 1.$$

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 identitățile:

$$(A) \quad (x \cdot y) \cdot z = x \cdot (y \cdot z),$$

$$(EN) \quad (x \cdot 1) = 1 \cdot x = x,$$

$$(TES) \quad x \cdot x^{-1} = x^{-1} \cdot x = 1 \quad \text{și}$$

$$(C) \quad x \cdot y = y \cdot x.$$

Exemplul 17. Un monoid este o algebră universală $\mathbf{M} = \langle M, \cdot, 1 \rangle$ de semnătură $(2, 0)$ pentru care sunt satisfăcute identitățile:

- (A) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ și
(EN) $(x \cdot 1) = 1 \cdot x = x$.

Exemplul 18. Un monoid comutativ este o algebră universală de semnătură $(2, 0)$, $\mathbf{M} = \langle M, \cdot, 1 \rangle$, pentru care sunt satisfăcute identitățile:

- (A) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
(EN) $(x \cdot 1) = 1 \cdot x = x$ și
(C) $x \cdot y = y \cdot x$.

Exemplul 19. Un semigrup este o algebră universală $\mathbf{S} = \langle S, \cdot \rangle$ de semnătură (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 semnătură (2) , $\mathbf{S} = \langle S, \cdot \rangle$, pentru care sunt satisfăcute identitățile:

- (A) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ și
(C) $x \cdot y = y \cdot x$.

Exemplul 21. O latice este o algebră universală $\mathbf{L} = \langle L, \vee, \wedge \rangle$ de semnătură $(2, 2)$ pentru care sunt satisfăcute identitățile:

- (C) $x \vee y = y \vee x$ și $x \wedge y = y \wedge x$,
(A) $(x \vee y) \vee z = x \vee (y \vee z)$ și $(x \wedge y) \wedge z = x \wedge (y \wedge z)$, și
(Ab) $x \vee (x \wedge y) = x$ și $x \wedge (x \vee y) = x$.

3. SUBALGEBRE UNIVERSALE

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

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

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

Definiția 23. Fie f o operație de aritate 0 pe mulțimea M . Spunem că $N \subset M$ este **parte stabilă a lui M în raport cu f** dacă $\text{Im } f \subset N$.

Definiția 24. Submulțimea B a lui A se numește **parte F -stabilă** a (sau **subunivers** al) lui \mathbf{A} dacă B este parte stabilă a lui A în raport cu fiecare operație fundamentală a lui A .

Definiția 25. O algebră universală $\mathbf{B} = \langle B, G \rangle$ de tip \mathcal{F} se numește **subalgebră universală** a lui \mathbf{A} dacă $B \subset A$ și dacă fiecare operație fundamentală f^B a lui \mathbf{B} se obține din operația corespunzătoare f^A a lui \mathbf{A} prin (restricție și) corestricție.

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

Observația 26. Mulțimea vidă este parte F -stabilă a lui \mathbf{A} .

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

Observația 28. Dacă \mathbf{A} are și operații fundamentale de aritate zero, atunci o parte a lui A este F -stabilă dacă și numai dacă ea este mulțime subiacentă a unei subalgebre universale a lui \mathbf{A} .

Observația 29. Deși obiectele de interes pentru noi sunt subalgebrele universale, proprietăți „mai bune” găsim pentru părțile F -stabile, care sunt mai comod de manevrat decât acestea. Motivul principal pentru această situație este acela că părțile F -stabile pot fi și vide, lucru nepermis mulțimilor subiacente de algebre universale.

4. SUBALGEBRE GENERATE DE SUBMULȚIMI

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

Propoziția 30. Intersecția oricărei familii de părți F -stabile ale lui \mathbf{A} este la rândul său parte F -stabilă a lui \mathbf{A} .

Definiția 31. Fie M o submulțime a lui A . **Prin partea F -stabilă a lui \mathbf{A} generată de M** înțelegem mulțimea

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

Observația 32. $\text{Sg}(M)$ este cea mai mică (în sensul incluziunii) parte F -stabilă a lui \mathbf{A} care conține submulțimea M .

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

Propoziția 34. Pentru orice submulțime M, N ale lui A au loc relațiile:

- (i) $M \subset \text{Sg}(M)$.
- (ii) Dacă $M \subset N$, atunci $\text{Sg}(M) \subset \text{Sg}(N)$.
- (iii) $\text{Sg}(\text{Sg}(M)) = \text{Sg}(M)$.

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

Propoziția 36. Mulțimea părților F -stabile ale lui \mathbf{A} are în raport cu incluziunea o structură de latică completă.

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

5. MORFISME DE ALGEBRE UNIVERSALE

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

Definiția 37. Numim **morfism de algebre universale de la \mathbf{A} la \mathbf{B}** orice funcție $\alpha : A \rightarrow B$ cu proprietățile:

- (i) $\alpha(f^A(a_1, a_2, \dots, a_n)) = f^B(\alpha(a_1), \alpha(a_2), \dots, \alpha(a_n))$ pentru orice $n \in \mathbb{N}^*$, $f \in \mathcal{F}_n$ și $a_1, a_2, \dots, a_n \in A$
- (ii) $\alpha \circ f^A = f^B$ pentru orice $f \in \mathcal{F}_0$.

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

Definiția 39. Morfismul din exemplul 38 se numește **morfismul incluziune** al lui \mathbf{B} în \mathbf{A} .

Propoziția 40. Dacă două morfisme de algebre universale de la \mathbf{A} la \mathbf{B} coincid pe un sistem de generatori al lui \mathbf{A} , atunci ele sunt egale.

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

Definiția 42. Numim **izomorfism de algebre universale de la \mathbf{A} la \mathbf{B}** orice morfism inversabil de la \mathbf{A} la \mathbf{B} al cărui invers este morfism de algebre universale de la \mathbf{B} la \mathbf{A} .

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

Demonstrație: Partea de necesitate este evidentă.

Pentru suficiență, fie $\alpha : A \rightarrow B$ un morfism bijectiv de algebre universale, $n \in \mathbb{N}^*$, $f \in \mathcal{F}_n$ și $b_1, b_2, \dots, b_n \in B$. Avem succesiv:

$$\begin{aligned} \alpha^{-1}(f^B(b_1, b_2, \dots, b_n)) &= \alpha^{-1}(f^B(\alpha(\alpha^{-1}(b_1)), \dots, \alpha(\alpha^{-1}(b_n)))) = \\ \alpha^{-1}(\alpha(f^A(\alpha^{-1}(b_1), \dots, \alpha^{-1}(b_n)))) &= f^A(\alpha^{-1}(b_1), \alpha^{-1}(b_2), \dots, \alpha^{-1}(b_n)). \end{aligned}$$

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

Definiția 44. Prin **endomorfism** al algebrei universale \mathbf{A} înțelegem un morfism de la \mathbf{A} la \mathbf{A} , iar prin **automorfism** al lui \mathbf{A} înțelegem un izomorfism de la \mathbf{A} la \mathbf{A} .

Exemplul 45. id_A este automorfism al algebrei universale \mathbf{A} .

Propoziția 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} .

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

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

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

6. CONGRUENȚE. ALGEBRE FACTOR

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

Definiția 50. O relație de echivalență ρ pe mulțimea A se numește **congruență** a algebrei universale \mathbf{A} dacă pentru orice $n \in \mathbb{N}^*$, $f \in \mathcal{F}_n$ și $a_1, a_2, \dots, a_n, a'_1, a'_2, \dots, a'_n \in A$ are loc

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

Propoziția 51. Dacă ρ este o congruență a algebrei universale \mathbf{A} , $n \in \mathbb{N}^*$ și $f \in \mathcal{F}_n$, atunci operația $f^A/\rho : (A/\rho)^n \rightarrow A/\rho$,

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

este corect definită.

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

Definiția 53. Fie ρ o congruență a algebrei universale \mathbf{A} . Prin **algebra universală factor** a lui \mathbf{A} în raport cu ρ înțelegem algebra universală care are mulțimea subiacentă A/ρ și operațiile 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}/ρ .

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

Definiția 55. Morfismul din propoziția 54 se numește **surjecția canonică** a lui \mathbf{A}/ρ .

7. TEOREMA FUNDAMENTALĂ DE IZOMORFISM

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

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

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

Propoziția 57. În condițiile din definiția anterioară, $\ker \alpha$ este o congruență a lui \mathbf{A} .

Temă: Demonstrați propoziția 57!

Teorema fundamentală de izomorfism pentru algebre universale. Dacă $\mathbf{A} = \langle A, F \rangle$ și $\mathbf{B} = \langle B, G \rangle$ sunt algebre universale de tip \mathcal{F} , α este un morfism de algebre universale de la \mathbf{A} la \mathbf{B} , π este surjecția canonică a lui $\mathbf{A}/\ker \alpha$, iar $j : \text{Im } \alpha \rightarrow B$ este morfismul incluziune, atunci există un (unic) izomorfism de algebre universale $\beta : \mathbf{A}/\ker \alpha \rightarrow \mathbf{Im } \alpha$ 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. Universității din București, 2006.
- [5] I. D. Ion, N. Radu, *Algebră*, Ed. Didactică și Pedagogică, București, 1981.
- [6] C. Năstăsescu, C. Niță, C. Vraciu, *Bazele algebrei*, Ed. Academiei, București, 1986.