Introducere în
Logica matematică şi teoria mulţimilor

Andrei Mărcuş

3 mai 2021

Cuprins

Capitolul 0

Descrierea cursului

0.1 Tematica

Logica este studiul şi folosirea raţionamentelor valide. Logica are două aspecte: *informal*, adică studiul argumentelor în limbaj natural, şi *formal*, adică studiul inferenţelor din punct de vedere al formei, sau altfel spus, studiul regulilor abstracte de deducţie. Cele mai vechi studii de logică formală sunt datorate lui Aristotel. Atunci când folosim simboluri abstracte în studiul formal al inferenţelor, vorbim de *logică simbolică*; de obicei, aceasta se împarte în logica propoziţiilor şi logica predicatelor.

Logica matematică este parte a Matematicii şi a Logicii. Rolul ei este de a fundamenta riguros ideea de valoare de adevăr a unei afirmaţii şi de a explora aplicarea metodelor logicii formale (simbolice) în diferite ramuri ale matematicii. De asemenea, logica matematică se ocupă cu aplicarea metodelor şi tehnicilor matematice la studiul logicii formale.

Dezvoltarea logicii matematice a fost puternic motivată de studiul fundamentelor matematicii, studiu început în secolul 19, şi are importante aplicaţii în filozofie sau lingvistică, dar şi în domenii mai recente precum informatica (programare logică, inteligenţă artificială etc).

În zilele noastre, logica matematică este împărţită în patru subdomenii, fiecare concentrându-se asupra unor aspecte distincte, dar evident, liniile de demarcaţie nu sunt stricte:

- teoria mulţimilor, care studiază colecţii abstracte de obiecte şi corespondenţele între ele, având rol important pentru fundamentele matematicii;
- teoria demonstraţiei, care în esenţă înseamnă analiza formală a demonstraţiilor matematice.
- teoria modelelor, care este studiul formal al structurilor matematice, având strânsă legatură cu algebra abstractă;
- teoria recursiei (sau teoria calculabilităţii), care studiază calculabilitatea efectivă a funcţiilor definite pe mulţimea numerelor naturale, având rol important pentru fundamentele informaticii;

În acest curs introductiv dedicat studenţilor din anul I de la Facultatea de Matematică şi Informatică vom atinge câte o mică parte din subiectele menţionate, de multe ori într-o manieră informală. Sunt incluse şi câteva teme elementare de Algebră, Aritmetică şi Combinatorică strâns legate de cele de mai sus, dar care în mod uzual depăşesc cadrul Logicii matematice.

0.2 Evaluare

Lucrări scrise, în total 2 ore de lucru efectiv. Nota se calculează la sfârşitul semestrului astfel:

$$\mathsf{N} = \frac{1}{4}(\mathsf{N1} + \mathsf{N2} + \mathsf{N3} + \mathsf{N4}) + \mathsf{S}$$

unde N=nota, $\mathsf{N1}, \mathsf{N2}, \mathsf{N3}, \mathsf{N4}$=notele obţinute pe fiecare subiect de lucrare scrisă, S=puncte acordate pe evaluarea activităţii de la seminar.

(Vezi şi syllabus-ul cursului pe website-ul FMI.)

Capitolul 1

LOGICA PROPOZIŢIILOR

În limbajul comun, prin propoziţie înţelegem o afirmaţie despre care putem decide dacă e adevărată sau falsă. Putem forma propoziţii compuse, cărora de asemenea le asociem o valoare de adevăr, folosind cuvinte precum şi, sau, nu, dacă şi numai dacă etc. Din punct de vedere matematic, o astfel de definiţie nu este satisfăcătoare, fiind necesară o abordare formală.

1.1 Formulele logicii propoziţiilor

Definiţia 1.1.1 a) **Simbolurile logicii propoziţiilor** sunt:

1. Parantezele: (şi).
2. Conectori (simbolurile operaţiilor logice): $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$.
3. Formule atomice $p, q, r, \ldots, x_1, x_2, \ldots$

b) O **formulă propoziţională** este un şir finit de simboluri ce satisface următoarele reguli:

1. Formulele atomice sunt formule.
2. Dacă A şi B sunt formule, atunci $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, $(A \leftrightarrow B)$ sunt de asemenea formule.
3. Alte formule decât cele descrise mai sus nu există.

Observaţii 1.1.2 a) În limbaj comun, conectorii $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ se citesc *non, şi, sau, dacă ... atunci, dacă şi numai dacă.*

b) Uzual, pentru simplificarea scrierii, unele paranteze pot fi omise prin adoptarea unei ordini de prioritate a conectorilor: $\neg$, apoi $\wedge$ şi $\vee$, apoi $\rightarrow$ şi $\leftrightarrow$. De asemenea, pot fi omise parantezele exterioare.

Exemplul 1.1.3 1) Următoarele şiruri de simboluri sunt formule:
$(p \vee q) \rightarrow (r \leftrightarrow (\neg s))$,
$((p \vee (\neg q)) \vee r) \rightarrow (s \wedge (\neg s))$,
$((p \rightarrow q) \rightarrow r) \vee (s \wedge r)$,
$(\neg((p \wedge q) \vee (\neg r))) \rightarrow (t \vee p)$,
$((p \vee q) \rightarrow (p \vee r)) \leftrightarrow ((\neg q) \wedge (\neg p))$.

2) Următoarele şiruri de simboluri nu sunt formule:
$p\wedge \rightarrow q$, $p \rightarrow$, $pq \wedge t$, $p \wedge q \vee r$ $p \wedge (q \rightarrow \wedge r)$, $(pq \wedge (r \wedge p \neg q)$.

Definiţia 1.1.4 a) Spunem că B **subformulă** a formulei A dacă B este obţinut în cursul construcţiei lui A.

b) Vorbim de **substituţie**, dacă în formula A o formulă atomică p sau o subformulă B este înlocuită cu formula C (notaţie $A(C/p)$ respectiv $A(C/B)$).

Exemplul 1.1.5 1) $p\wedge q$, $t\vee p$ sunt subformule ale formulei $(\neg((p\wedge q)\vee(\neg r))) \rightarrow (t\vee p)$, în timp ce $p \rightarrow (t\vee p)$ nu este.

2) Dacă $A = (\neg((p\wedge q)\vee(\neg r))) \rightarrow (t\vee p)$, atunci pentru $C = r\wedge s$ avem $A(C/p) = (\neg(((r\wedge s)\wedge q)\vee(\neg r))) \rightarrow (t \vee (r \wedge s))$ şi $A(C, p \wedge q) = (\neg((r \wedge s) \vee (\neg r))) \rightarrow (t \vee p)$.

1.2 Interpretarea formulelor propoziţionale

Definiţia 1.2.1 Fie $V = \{0, 1\}$ mulţimea **valorilor de adevăr**. Aici 0 corespunde *falsului*, iar 1 corespunde *adevărului*. O funcţie de n variabile $f : V^n \to V$ se numeşte **funcţie de adevăr**.

O funcţie de adevăr de n variabile poate fi dată printr-un **tabel de adevăr**, care are $n + 1$ coloane şi 2^n linii. Primele n coloane conţin toate combinaţiile posibile ale variabilelor, iar ultima coloană conţine valorile corespunzătoare ale funcţiei.

De asemenea, o funcţie de adevăr poate fi vizualizată cu ajutorul diagramelor Euler-Venn sau cu ajutorul schemelor (circuitelor) cu contacte şi relee.

Definiţia 1.2.2 Cele mai frecvent utilizate funcţii de adevăr sunt **operaţiile logice fundamentale** corespunzătoare celor cinci conectori, pe care le definim mai jos cu ajutorul tabelelor de adevăr:

a) **Negaţia („non"):** $\neg p$, definită prin

p	$\neg p$
0	1
1	0

b) **Conjuncţia („şi"):** $p \wedge q$, definită prin

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

c) **Disjuncţia („sau"):** $p \vee q$, definită prin

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

d) **Implicaţia („dacă ... atunci"):** $p \to q$, definită prin

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

e) **Echivalenţa („dacă şi numai dacă"):** $p \leftrightarrow q$, definită prin

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Definiţia 1.2.3 Dacă A este o formulă şi $\mathcal{A}$ este mulţimea formulelor atomice din A, atunci o **interpretare** a lui A este o funcţie $\nu : \mathcal{A} \to V = \{0, 1\}$. Elementul $\nu(p) \in V$ se numeşte **valoarea de adevăr** a formulei atomice p.

Fie $A = A(p_1, \dots, p_n)$ o formulă ce conţine atomii $p_1, \dots, p_n$, şi fie ν o interpretare a lui A. Notăm cu $\tilde{A} : V^n \to V$ funcţia de adevăr corespunzătoare lui A, obţinută folosind funcţiile logice fundamentale. Atunci **valoarea de adevăr a formulei** A corespunzătoare interpretării ν este dată de:

$$H_\nu(A) := \tilde{A}(\nu(p_1), \dots, \nu(p_n)).$$

Exemplul 1.2.4 în tabelul de mai jos avem interpretările şi valorile de adevăr corespunzătoare pentru formula $A = A(p, q) = ((p \vee q) \wedge (\neg p)) \to q$ (punând în evidenţă şi câteva subformule):

p	q	$p \vee q$	$\neg p$	$(p \vee q) \wedge \neg p$	A
0	0	0	1	0	1
0	1	1	1	1	1
1	0	1	0	0	1
1	1	1	0	0	1

Vom vedea mai târziu că din Teorema 6.4.6 rezultă următoarea teoremă, pe care o vom folosi în exerciţiile de mai jos.

Teorema 1.2.5 *Orice funcţie de adevăr de $n \geq 1$ variabile poate fi exprimată numai cu ajutorul operaţiilor logice fundamentale.*

Exemplul 1.2.6 În afară de operaţiile logice fundamentale, menţionăm şi următoarele funcţii de adevăr:

1) **Adunarea şi înmulţirea modulo** 2, notate prin simbolurile $\oplus$ respectiv $\odot$.

2) **Funcţia lui Sheffer (non şi; not and):** $p \mid q = \neg(p \wedge q)$. Este adevărat, dacă cel mult unul din p sau q este adevărat.

3) **Funcţia lui Webb–Peirce (nici-nici; neither-nor; non sau; not or):** $p \downarrow q = (\neg p) \wedge (\neg q)$. Este adevărat, dacă niciunul din p şi q nu este adevărat.

4) **Disjuncţia exclusivă (sau-sau; xor):** $p \oplus q = \neg(p \leftrightarrow q)$. Este adevărat, dacă exact unul din p sau q este adevărat.

Exerciţiul 1 Să se întocmească tabelele de adevăr pentru funcţiile din exemplul de mai sus.

Exerciţiul 2 Să se verifice cu ajutorul tabelelor de adevăr următoarele egalităţi între funcţii:

1) $\neg p = 1 \oplus p$.
2) $p \wedge q = p \odot q$.
3) $p \vee q = p \oplus q \oplus p \odot q$.
4) $p \to q = 1 \oplus p \oplus p \odot q$.
5) $p \leftrightarrow q = 1 \oplus p \oplus q$.

Exerciţiul 3 1) Să se scrie toate funcţiile de adevăr de 1 respectiv 2 variabile.

2) Câte funcţii de adevăr de n variabile există?

Exerciţiul 4 Să se arate că orice funcţie de adevăr de $n \geq 1$ variabile poate fi exprimată numai cu ajutorul negaţiei şi conjuncţiei (sau numai cu ajutorul negaţiei şi disjuncţiei. Mai exact, să se verifice următoarele egalităţi:

1) $p \vee q = \neg((\neg p) \wedge (\neg q))$.
2) $p \wedge q = \neg((\neg p) \vee (\neg q))$.
3) $p \to q = \neg(p \wedge (\neg q)) = \neg p \vee q$.
4) $p \leftrightarrow q = (\neg(p \wedge (\neg q))) \wedge (\neg(q \wedge (\neg p)))$.
5) $p \oplus q = (p \vee q) \wedge (\neg(p \wedge q))$.

Exerciţiul 5 Să se arate că orice funcţie de adevăr de $n \geq 1$ variabile poate fi exprimată numai cu ajutorul negaţiei şi implicaţiei. Mai exact, să se scrie conjuncţia, disjuncţia şi echivalenţa cu folosind doar negaţia şi implicaţia.

Exerciţiul 6 Să se arate că orice funcţie de adevăr de $n \geq 1$ variabile poate fi exprimată numai cu ajutorul funcţiei lui Sheffer. Mai exact, să se verifice următoarele egalităţi:

1) $\neg p = p \mid p$.
2) $p \wedge q = (p \mid q) \mid (p \mid q)$.
3) $p \vee q = (p \mid p) \mid (q \mid q)$.
4) $p \to q = p \mid (q \mid q) = p \mid (p \mid q)$.

Exerciţiul 7 Să se arate că orice funcţie de adevăr poate fi exprimată numai cu ajutorul funcţiei lui Webb–Peirce. Mai exact, să se verifice următoarele egalităţi:

0) $p \downarrow q = \neg(p \vee q)$.
1) $\neg p = p \downarrow p$.
2) $p \wedge q = (p \downarrow p) \downarrow (q \downarrow q)$.
3) $p \vee q = (p \downarrow q) \downarrow (p \downarrow q)$.
4) $p \to q = ((p \downarrow p) \downarrow q) \downarrow ((p \downarrow p) \downarrow q)$.

Definiţia 1.2.7 a) O formulă se numeşte **realizabilă** dacă are o interpretare pentru care valoarea de adevăr este 1.

b) Dacă nu există o astfel de interpretare formula se numeşte **contradicţie** (**identic falsă**) şi o notăm cu 0.

c) O formulă se numeşte **tautologie (identic adevărată)**, dacă pentru orice interpretare valoarea de adevăr este 1, şi atunci o notăm cu 1.

Definiţia 1.2.8 Introducem două *relaţii* între formule:

a) Dacă formula $A \to B$ este o tautologie, atunci spunem că formula B **rezultă** din formula A şi notăm $A \Rightarrow B$.

În teoremele din matematică folosim următoarele exprimări: *dacă* A*, atunci* B*;* A *este condiţie suficientă pentru* B*;* B *este condiţie necesară pentru* A*.*

b) Dacă formula $A \leftrightarrow B$ este o tautologie, atunci spunem că A este **echivalent** cu B, şi notăm $A \Leftrightarrow B$.

În teoremele din matematică folosim următoarele exprimări: A *este condiţie necesară şi suficientă pentru* B*;* B *dacă şi numai dacă* A*;* B *exact atunci când* A*;* A *este echivalent cu* B.

Exemplul 1.2.9 1) Pentru orice formulă A, formula $(\neg A) \vee A$ este tautologie şi $(\neg A) \wedge A$ contradicţie.

2) A este contradicţie dacă şi numai dacă $\neg A$ este tautologie.

3) A este tautologie dacă şi numai dacă $\neg A$ este contradicţie.

4) Dacă $A = p \wedge (\neg p)$, $B = p \vee (\neg p)$, $C = p \to p$, $D = p \to q$, $E = (\neg p) \vee q$, $F = p \leftrightarrow (\neg p)$, atunci B şi C sunt tautologii, A şi F sunt contradicţii, D şi E sunt realizabile. De asemenea, aceste perechi sunt echivalente.

Observaţii 1.2.10 Fie A o tautologie, p o formulă atomică şi B o subformulă a lui A. Atunci pentru orice formulă C, $A(C/p)$ is tautologie. Dacă $C \Leftrightarrow B$, atunci $A(C/B)$ este tautologie.

Teorema 1.2.11 Enumerăm câteva tautologii importante. Fie A, B, C formule propoziţionale.

1) $(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$, $(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$ (asociativitate),

2) $A \wedge B \Leftrightarrow B \wedge A$, $A \vee B \Leftrightarrow B \vee A$ (comutativitate),

3) $A \wedge (A \vee B) \Leftrightarrow A$, $A \vee (A \wedge B) \Leftrightarrow A$ (absorbţie),

4) $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$, $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$ (distributivitate),

5) $A \wedge A \Leftrightarrow A$, $A \vee A \Leftrightarrow A$ (idempotenţă),

6) $A \wedge \mathbf{1} \Leftrightarrow A$, $A \vee \mathbf{0} \Leftrightarrow A$,

7) $A \wedge \mathbf{0} \Leftrightarrow \mathbf{0}$, $A \vee \mathbf{1} \Leftrightarrow \mathbf{1}$,

8) $\neg(\neg A) \Leftrightarrow A$ (legea dublei negaţii),

9) $A \vee (\neg A) \Leftrightarrow \mathbf{1}$ (legea terţului exclus), $A \wedge (\neg A) \Leftrightarrow \mathbf{0}$ (legea contradicţiei),

10) $\neg(A \wedge B) \Leftrightarrow (\neg A) \vee (\neg B)$, $\neg(A \vee B) \Leftrightarrow (\neg A) \wedge (\neg B)$ (legile lui De Morgan [1])

11) $A \leftrightarrow B \Leftrightarrow (A \to B) \wedge (B \to A)$ (legea echivalenţei),

12) $A \to B \Leftrightarrow (\neg A) \vee B$ (legea implicaţiei),

13) $A \to B \Leftrightarrow (\neg B) \to (\neg A)$ (legea contrapoziţiei),

14) $(A \wedge B) \to C \Leftrightarrow A \to (B \to C)$ (legea separării/reunirii premiselor),

15) $A \to (B \to C) \Leftrightarrow B \to (A \to C)$ (legea permutării premiselor),

Exerciţiul 8 Să se verifice tautologiile (1) – (15) din teorema de mai sus cu ajutorul tabelelor de adevăr.

1.3 Problema deciziei

Problema deciziei în logica propoziţiilor înseamnă găsirea unui algoritm care să stabilească dacă o formulă propoziţională este *tautologie, contradicţie, sau realizabilă* precum şi găsirea metodelor corecte de deducţie. Vom discuta trei metode, în principiu echivalente: a tabelelor de adevăr, a formelor normale şi a deducţiei formale bazate pe scheme de deducţie.

1.3.1 Metoda tabelului de adevăr

Am văzut deja în paragraful precedent această metodă, care este eficientă în cazul formulelor cu un număr mic de atomi.

[1] Augustus De Morgan (1806–1871), matematician şi logician britanic.

1.3.2 Metoda formelor normale

Definiţia 1.3.1 Fie $A = A(x_1, x_2, \ldots, x_n)$ o formulă propoziţională.
a) A este o **conjuncţie elementară** dacă este o conjuncţie ce are ca factori atomi sau negaţii de atomi.
b) A este o **disjuncţie elementară** dacă este o disjuncţie ce are ca termeni atomi sau negaţii de atomi.

Exemplul 1.3.2 a) Formulele $A = x_1 \wedge \neg x_2 \wedge \neg x_3$, $B = x_1 \wedge x_2 \wedge x_3$, $C = \neg x_1 \wedge \neg x_2 \wedge \neg x_3$ sunt conjuncţii elementare.
b) Formulele $A = x_1 \vee \neg x_2 \vee \neg x_3$, $B = x_1 \vee x_2 \vee x_3$, $C = \neg x_1 \vee \neg x_2 \vee \neg x_3$ sunt disjuncţii elementare.

Definiţia 1.3.3 a) Formula $A = A(x_1, x_2, \ldots, x_n)$ are **formă normală conjunctivă** (**FNC**), dacă este o conjuncţie de disjuncţii elementare, adică:

$$A = A_1 \wedge A_2 \wedge \cdots \wedge A_m,$$

unde subformula $A_i = A_i(x_1, x_2, \ldots, x_n)$ este o disjuncţie elementară, pentru orice $i = 1, 2, \ldots, m$.
b) Spunem că formula $B = B(x_1, x_2, \ldots, x_n)$ are **formă normală disjunctivă** (**FND**), dacă este o disjuncţie de conjuncţii elementare, adică:

$$B = B_1 \vee B_2 \vee \cdots \vee B_m,$$

unde subformula $B_i = B_i(x_1, x_2, \ldots, x_n)$ este o conjuncţie elementară, pentru orice $i = 1, 2, \ldots, m$.

Observaţii 1.3.4 Orice formulă propoziţională A este logic echivalentă cu o FNC, respectiv cu o FND (nu neapărat unic determinată). Formula A se aduce la o FNC, respectiv la o FND, printr-un şir finit de echivalenţe logice, utilizând legile fundamentale ale logicii propoziţiilor, prezentate în Teorema 1.2.11, astfel:

1. Se exprimă formula A numai cu conectorii $\neg$, $\wedge$, $\vee$, folosind legea implicaţiei şi legea echivalenţei.
2. Se trece negaţia numai asupra atomilor, utilizând legile lui De Morgan şi legea dublei negaţii.
3. Se obţin conjuncţii de disjuncţii (pentru FNC), respectiv disjuncţii de conjuncţii (pentru FND), folosindu-se distributivitatea, absorbţia, idempotenţa, comutativitatea sau asociativitatea.

Exemplul 1.3.5 Fie $A = \neg x \to x \wedge y$. Aplicând cele de mai sus, obţinem

$$A = \neg x \to x \wedge y \Leftrightarrow \neg\neg x \vee (x \wedge y) \Leftrightarrow x \vee (x \wedge y)$$

şi am ajuns astfel la o FND. Mai departe, avem

$$x \vee (x \wedge y) \Leftrightarrow (x \vee x) \wedge (x \vee y)$$

şi obţinem o FNC. Folosind acum idempotenţa avem:

$$(x \vee x) \wedge (x \vee y) \Leftrightarrow x \wedge (x \vee y)$$

şi obţinem o altă FNC. Aplicând absorbţia, avem:

$$x \wedge (x \vee y) \Leftrightarrow x,$$

care este încă o FNC, dar o putem considera şi ca o FND.

Observaţii 1.3.6 Metoda formelor normale se aplică astfel. Fie $C = C(x_1, x_2, \ldots, x_n)$ o formulă propoziţională şi fie $A = A_1 \wedge A_2 \wedge \cdots \wedge A_m$ o FNC respectiv $B = B_1 \vee B_2 \vee \cdots \vee B_m$ o FND cu care C este logic echivalentă. Atunci:
a) C este tautologie dacă şi numai dacă în FNC A, pentru orice $i = 1, 2, \ldots, m$, A_i conţine cel puţin un atom împreună cu negaţia sa;
b) C este o contradicţie dacă şi numai dacă în FND B, pentru orice $i = 1, 2, \ldots, m$, B_i conţine cel puţin un atom împreună cu negaţia sa.

Exemplul 1.3.7 Să rezolvăm problema deciziei prin metoda formelor normale.
a) Fie $C = x \wedge \neg y \to x$. Aducem pe C la o formă normală:

$$C = x \wedge \neg y \to x \Leftrightarrow \neg(x \wedge \neg y) \vee x \Leftrightarrow (\neg x \vee \neg\neg y) \vee x \Leftrightarrow (\neg x \vee y) \vee x \Leftrightarrow \neg x \vee y \vee x.$$

Am obţinut formula $A = \neg x \vee y \vee x$, care poate fi privită şi ca FNC, dar şi ca FND. Considerând A ca FNC cu un singur factor, x apare împreună cu negaţia sa $\neg x$, deci φ este o tautologie.

b) Fie $C = \neg x \wedge (\neg x \vee y \to x)$. Aducem C la o formă normală:

$$C = \neg x \wedge (\neg x \vee y \to x) \Leftrightarrow \neg x \wedge (\neg(\neg x \vee y) \vee x) \Leftrightarrow \neg x \wedge ((\neg\neg x \wedge \neg y) \vee x) \Leftrightarrow$$
$$\Leftrightarrow \neg x \wedge ((x \wedge \neg y) \vee x) \Leftrightarrow (\neg x \wedge x \wedge \neg y) \vee (\neg x \wedge x)$$

Am obţinut FND $B = (\neg x \wedge x \wedge \neg y) \vee (\neg x \wedge x)$. În fiecare termen al lui B, apare atomul x împreună cu negaţia sa $\neg x$, deci C este o contradicţie.

c) Fie $C = (x \to y) \wedge (y \to z)$. Aducem C la o formă normală:

$$C = (x \to y) \wedge (y \to z) \Leftrightarrow (\neg x \vee y) \wedge (\neg y \vee z).$$

Am obţinut FNC $A = (\neg x \vee y) \wedge (\neg y \vee z)$, şi vedem că C nu este tautologie. Determinăm şi o FND:

$$A = (\neg x \vee y) \wedge (\neg y \vee z) \Leftrightarrow (\neg x \wedge \neg y) \vee (\neg x \wedge z) \vee (y \wedge \neg y) \vee (y \wedge z).$$

Am obţinut FND $B = (\neg x \wedge \neg y) \vee (\neg x \wedge z) \vee (y \wedge \neg y) \vee (y \wedge z)$, din care citim că C nu este contradicţie, deci C este o formulă realizabilă.

Exerciţiul 9 Să se aducă la formă normală conjunctivă şi la formă normală disjunctivă şi să se rezolve problema deciziei pentru formulele:

1) $((x \to y) \to (z \to \neg x)) \to (\neg y \to \neg z)$.
2) $((((x \to y) \to \neg x) \to \neg y) \to \neg z) \to z$.
3) $(x \to (y \to z)) \to ((x \to \neg z) \to (x \to \neg y))$.
4) $(\neg x \to \neg y) \to ((y \wedge z) \to (x \wedge z))$.
5) $((x \to y) \to \neg x) \to (x \to (y \wedge x))$.
6) $\neg((x \wedge y) \to \neg x) \wedge \neg((x \wedge y) \to \neg y)$.
7) $(z \to x) \to (\neg(y \vee z) \to x)$.
8) $\neg((x \wedge y) \to x) \vee (x \wedge (y \vee z))$.
9) $\neg(x \wedge (y \vee z)) \to \neg((x \wedge y) \vee z)$.

1.3.3 Scheme de deducţie

Definiţia 1.3.8 Spunem că formula propoziţională B este **consecinţă** a mulţimii de formule $\Sigma = \{A_1, \ldots, A_n\}$ (unde $n \geq 0$), dacă orice interpretare care face $A_1, \ldots, A_n$ adevărate, face şi formula B adevărată.

Notăm aceasta prin

$$A_1, \ldots, A_n \models B \qquad \text{sau} \qquad \Sigma \models B \qquad \text{sau} \qquad \frac{A_1, \ldots, A_n}{B}$$

şi o numim **schemă de deducţie (inferenţă)**. Formulele $A_1, \ldots, A_n$ se numesc **premise**, iar B se numeşte **concluzie**.

Este evident din definiţie că avem $A_1, \ldots, A_n \models B$ exact când formula

$$A_1 \wedge \cdots \wedge A_n \to B$$

este tautologie, adică are loc relaţia $A_1 \wedge \cdots \wedge A_n \Rightarrow B$.

Mai general, dacă $\Gamma = \{B_1, \ldots, B_m\}$ este o mulţime de formule, atunci notăm $\Sigma \models \Gamma$ dacă $\Sigma \models B_j$ pentru orice $j = 1, \ldots, m$.

Observaţii 1.3.9 1) Dacă în particular $n = 0$ (adică $\Sigma = \emptyset$), atunci înseamnă că B este tautologie (respectiv fiecare formulă din Γ este tautologie).

2) Are loc $\Sigma \models \Gamma$ dacă şi numai dacă formula $(A_1 \wedge \cdots \wedge A_n) \to (B_1 \wedge \cdots \wedge B_m)$ este tautologie.

3) Are loc proprietatea de *reflexivitate* $A \models A$, deoarece formula $A \to A$ este tautologie, pe baza legii implicaţiei şi a legii terţului exclus. Mai general, dacă $\Gamma \subseteq \Sigma$ sunt mulţimi de formule, atunci $\Sigma \models \Gamma$.

Exemplul 1.3.10 Prezentăm mai jos câteva scheme de deducţie ale logicii clasice (aristotelice[2]). Ele pot fi verificate uşor cu ajutorul tabelelor de adevăr şi sunt frecvent utilizate în demonstrarea teoremelor din matematică. Să observăm că unele variante se obţin din altele înlocuind o formulă cu negaţia ei.

1. **Moduri clasice de argumentare.**

   (a) $\frac{A,\ A\to B}{B}$ **(modus ponendo ponens** sau pe scurt **modus ponens (MP))**[3]

[2] Aristotel (384–322 BC), filosof grec. Contribuţii sale la Logică sunt colectate în *Organon*.
[3] modul de a afirma prin afirmare

(b) $\frac{\neg A,\ \neg A \to \neg B}{\neg B}$ **(modus tollendo tollens)** [4]

(c) $\frac{\neg A,\ \neg A \to B}{B}$ **(modus tollendo ponens)**

(d) $\frac{A,\ A \to \neg B}{\neg B}$ **(modus ponendo tollens)**

2. **Reductio ad absurdum.**

(a) $\frac{B,\ \neg A \to \neg B}{A}$; $\frac{\neg B,\ \neg A \to B,}{A}$; $\frac{B,\ A \to \neg B}{\neg A}$; $\frac{\neg B,\ A \to B}{\neg A}$.

(b) $\frac{(\neg A) \to B,\ (\neg A) \to (\neg B)}{A}$; $\frac{A \to B,\ A \to (\neg B)}{\neg A}$.

3. **Contrapoziţie.**

$$\frac{A \to B}{\neg B \to \neg A}$$

4. **Silogism ipotetic.**

$$\frac{A \to B, B \to C}{A \to C}$$

5. **Silogism disjunctiv.**

$$\frac{A \vee B,\ \neg A}{B}$$

6. **Metoda analizei cazurilor.**

$$\frac{B \vee C,\ B \to A,\ C \to A}{A}$$

Exerciţiul 10 Să se verifice validitatea schemelor de deducţie de mai sus cu ajutorul tabelelor de adevăr, respectiv folosind metoda formelor normale.

Observaţii 1.3.11 Prezentăm câteva proprietăţi generale ale schemelor de deducţie, care sunt utile în demonstrarea teoremelor din matematică:

1. Dacă $A_1, \ldots, A_n \models B_j$ (pentru orice $j = 1, \ldots, m$) şi $B_1, \ldots, B_m \models C$, atunci $A_1, \ldots, A_n \models C$ (aceasta este proprietatea de *tranzitivitate*, care generalizează silogismul ipotetic).

2. Dacă $A_1 \models A_2, \ldots, A_{n-1} \models A_n$, şi $A_n \models A_1$, atunci formulele $A_1, \ldots, A_n$ sunt echivalente (aceasta este **metoda demonstraţiei ciclice**).

3. $\Sigma \cup \{A\} \models B$ dacă şi numai dacă $\Sigma \models A \to B$.

Exerciţiul 11 Să se demonstreze proprietăţile de mai sus.

Observaţii 1.3.12 Multe demonstraţii din matematică devin mai uşoare dacă înlocuim o schemă dată cu una echivalentă.

1. **Demonstraţie directă**: înlocuim $\frac{A}{B \to C}$ cu $\frac{A, B}{C}$ (adică *reunim premisele*).

2. **Demonstraţie prin contrapoziţie**: înlocuim $\frac{A,\ B}{C}$ cu $\frac{A,\ \neg C}{\neg B}$.

3. **Demonstraţie indirectă (reducere la absurd)**: în loc de $\frac{A}{B}$ arătăm că $A \wedge (\neg B)$ este contradicţie.

Exerciţiul 12 Să se demonstreze echivalenţa schemelor de deducţie de mai sus.

[4] modul de a nega prin negare

1.3.4 Deducţie formală

O altă abordare a problemei deciziei se bazează pe manipularea simbolurilor pornind de la câteva axiome şi scheme de deducţie şi nu face apel la interpretarea formulelor. Vom vedea că metoda deducţiei formale este echivalentă cu cea bazată pe tabele de adevăr.

1.3.13 Prezentăm aici pe scurt *calculul lui Hilbert.*[5] (Există şi alte abordări, cum ar fi *calculul secvenţial al lui Gentzen.*) Această metodă porneşte cu următoarele date:

- câteva tautologii speciale, numite **axiomele logicii propoziţiilor**.

  A1: $A \to (B \to A)$

  A2: $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

  A3: $((\neg B) \to (\neg A)) \to (((\neg B) \to A) \to B))$, unde A, B, C sunt formule arbitrare;

- schema de deducţie **Modus Ponens (MP)**, adică $\frac{A, A\to B}{B}$.

Exerciţiul 13 Să se verifice că formulele **A1**, **A2** şi **A3** de mai sus sunt tautologii, folosind metoda tabelelor de adevăr, respectiv metoda formelor normale.

Definiţia 1.3.14 Fie acum $A_1, \dots, A_n$ $(n \geq 0)$ formule propoziţionale. O **deducţie** din formulele $A_1, \dots, A_n$ (numite **premise** sau **ipoteze**) este un şir finit $E_1, \dots, E_k$ de formule astfel încât pentru orice $i = 1, \dots, k$ avem:

(1) E_i este axiomă, sau

(2) există l astfel încât $E_i = A_l$, sau

(3) E_i se obţine din E_j, E_l $(j, l < i)$ folosind schema (MP).

Definiţia 1.3.15 a) Spunem că formula B **deductibilă** din formulele $A_1, \dots, A_n$ (notaţie: $A_1, \dots, A_n \vdash B$), dacă B este ultimul termen al unei deducţii din formulele $A_1, \dots, A_n$. Dacă $n = 0$, atunci notăm $\vdash B$.

Definiţia se generalizează imediat la cazul a două mulţimi de formule Σ şi Γ; notăm $\Sigma \vdash \Gamma$ dacă $\Sigma \vdash B$ pentru orice $B \in \Gamma$.

b) Spunem că mulţimea de formule Σ este **contradictorie**, dacă există o formulă A, astfel ca $\Sigma \vdash A$ şi $\Sigma \vdash \neg A$. Altfel, spunem că Σ este **consistentă**.

Exemplul 1.3.16 a) Să se arate că $\vdash A \to A$.

1.	$(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$	A2
2.	$A \to ((A \to A) \to A)$	A1
3.	$(A \to (A \to A)) \to (A \to A)$	1,2 MP
4.	$A \to (A \to A)$	A1
5.	$A \to A$	3,4 MP

b) Să se arate că $A \to B,\ B \to C \vdash A \to C$.

1.	$(B \to C) \to (A \to (B \to C))$	A1
2.	$B \to C$	Ipoteză
3.	$A \to (B \to C)$	1,2 MP
4.	$(A \to (B \to C)) \to ((A \to B) \to (A \to C))$	A2
5.	$(A \to B) \to (A \to C)$	4,3 MP
6.	$A \to B$	Ipoteză
7.	$A \to C$	5,6 MP

c) Să se arate că $A,\ \neg A \vdash B$.

1.	$\neg A$	Ipoteză

[5] David Hilbert (1862–1943), matematician german. Între multele sale contribuţii, a fost unul din fondatorii teoriei demonstraţiei şi un susţinător al teoriei mulţimilor create de Georg Cantor.

2. $(\neg A) \to ((\neg B) \to (\neg A))$ A1
3. $(\neg B) \to (\neg A)$ 1,2 MP
4. A Ipoteză
5. $A \to ((\neg B) \to A)$ A1
6. $(\neg B) \to A$ 4,5 MP
7. $((\neg B) \to (\neg A)) \to (((\neg B) \to A) \to B)$ A3
8. $((\neg B) \to A) \to B$ 3,7 MP
9. B 6,8 MP

Vedem că această metodă nu e foarte uşor de aplicat. Următoarele observaţii simplifică oarecum lucrurile.

Observaţii 1.3.17 a) Dacă $\Sigma \vdash B$ şi $\Sigma \vdash B \to C$, atunci $\Sigma \to C$.
b) Dacă $\Sigma \subseteq \Delta$ şi $\Sigma \vdash B$, atunci $\Delta \vdash B$.
c) Dacă $\Sigma \vdash \Gamma$ şi $\Gamma \vdash B$, atunci $\Sigma \vdash B$.
d) Dacă $\Sigma \vdash B \wedge \neg B$, atunci $\Sigma \vdash C$ pentru orice formulă C .
e) (*Teorema lui Herbrand*[6]*, 1930*): $\Sigma \vdash B \to C$ dacă şi numai dacă $\Sigma \cup \{B\} \vdash C$.

Exemplul 1.3.18 Pentru a arăta că $A \to B, B \to C \vdash A \to C$ este suficient de arătat că $A,\ A \to B,\ B \to C \vdash C$. Pentru aceasta, avem:

1. A Ipoteză
2. $A \to B$ Ipoteză
3. B 1,2 MP
4. $B \to C$ Ipoteză
5. C 3,4 MP.

Următoarea teoremă spune că metoda de deducţie bazată pe valorile de adevăr (,,rezultă " $\Rightarrow, \models$) este echivalentă cu deducţia formală ($\vdash$)). Prima implicaţie este mai uşor de demonstrat, a doua este dificilă.

Teorema 1.3.19 (Frege–Łukasiewicz, de completitudine) *Are loc* $\Sigma \vdash B$ *dacă şi numai dacă* $\Sigma \models B$.[7] [8]

[6] Jacques Herbrand (1908–1931), matematician francez.
[7] Gottlob Frege (1848–1925), matematician, logician şi filosof german, unul din fondatorii logicii moderne.
[8] Jan Łukasiewicz (1878–1956), matematician, logician şi filosof polonez.

Capitolul 2

LOGICA DE ORDINUL ÎNTÂI

Am văzut că logica propoziţiilor formalizează utilizarea operaţiilor logice *non, şi, sau, dacă ... atunci, dacă şi numai dacă*). Logica de ordinul întâi merge mai departe introducând *cuantificatori*, pentru a formaliza noţiunile de *pentru orice* şi *există*. Astfel, logica de ordinul întâi va fi utilă pentru formalizarea a mult mai multe teorii matematice.

În logica de ordinul I se cuantifică doar variabilele, în logica de ordinul II se cuantifică şi predicatele (sau mulţimile) etc.

2.1 Noţiunea de predicat

Definiţia 2.1.1 Fie M o mulţime nevidă şi fie $n \in \mathbb{N}^*$. Un **predicat n-ar pe mulţimea** M este o submulţime a mulţimii M^n (adică o relaţie n-ară pe M).

Observaţii 2.1.2 În limbajul comun, un predicat n-ar pe mulţimea M este o afirmaţie ,,deschisă" $P(x_1, \ldots, x_n)$, în care putem înlocui variabilele $x_1, \ldots, x_n$ cu elementele $a_1, \ldots a_n \in M$ pentru a obţine propoziţia $P(a_1, \ldots, a_n)$. În acest caz,

$$\{(a_1, \ldots, a_n) \in M^n \mid P(a_1, \ldots, a_n) \text{ adevărat } \}$$

este o relaţie n-ară, deci un predicat n-ar pe M. Această abordare nu este însă suficient de precisă.

Exemplul 2.1.3 a) ,,$x + y = z$" predicat de 3 variabile pe $M = \mathbb{R}$.
b) ,,$x < y$" este predicat binar pe $M = \mathbb{N}$.
c) ,,$|x| = 1$" este un predicat unar pe $M = \mathbb{C}$.

2.2 Limbaje de ordinul întâi

Simbolurile şi regulile de formare a formulelor date mai jos formează **limbajul ordinul întâi**.

Definiţia 2.2.1 Simbolurile unui limbajului de ordinul întâi $\mathcal{L}$ sunt următoarele:

1. Paranteze: (şi).
2. Conectori: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$.
3. Cuantificatori: $\forall$ (*pentru orice*) şi $\exists$ (*există*).
4. Simbolul de egalitate: $=$.
5. Variabile: $x, y, z, \ldots$.
6. Constante: $a, b, c, \ldots$.
7. Funcţii (operaţii): $f, g, \ldots$.
8. Predicate: $P, Q, \ldots$.

Presupunem în plus că pentru fiecare funcţie şi fiecare predicat se dă **aritatea** ≥ 1 (adică numărul variabilelor sale). Cuantificatorii pot apărea doar înaintea variabilelor.

Utilizarea simbolurilor depinde de teoria matematică pe care dorim să o formalizăm.

Exemplul 2.2.2 1) *Limbajul* $\mathcal{L}_S$ al teoriei mulţimilor foloseşte un singur predicat binar $\in$ („aparţine").

2) *Limbajul* $\mathcal{L}_G$ al teoriei grupurilor foloseşte constanta 1 (simbolul elementului neutru), inversa este o funcţie unară iar produsul este o funcţie binară.

3) *Limbajul* $\mathcal{L}_\mathbb{N}$ al teoriei numerelor naturale foloseşte constanta 0 şi trei operaţii $s, +, \cdot$: funcţia succesor s este unară, adunarea şi înmulţirea sunt binare.

Definiţia 2.2.3 a) **Expresiile (termenii)** limbajului $\mathcal{L}$ de ordinul întâi sunt şiruri finite de simboluri ce satisfac regulile:

1. Orice variabilă este expresie.
2. Orice constantă este expresie.
3. Dacă f este o funcţie de n variabile şi $t_1, \dots, t_n$ sunt expresii, atunci $f(t_1, \dots, t_n)$ este expresie. (De multe ori, în loc de $f(x, y)$ notăm xfy, de exemplu, $x + y$.)
4. Alte expresii nu există.

b) **Formulele** limbajului $\mathcal{L}$ de ordinul întâi sunt şiruri finite se simboluri ce satisfac regulile:

1. Dacă P este un predicat n-ar şi $t_1, \dots, t_n$ sunt expresii, atunci $P(t_1, \dots, t_n)$ este formulă.
2. Dacă t_1 şi t_2 sunt expresii, atunci $(t_1 = t_2)$ este formulă.
3. Dacă φ, ψ sunt formule, atunci $(\neg\varphi)$, $(\varphi \vee \psi)$, $(\varphi \wedge \psi)$, $(\varphi \to \psi)$, $(\varphi \leftrightarrow \psi)$ sunt formule. (După caz, vom omite unele paranteze.)
4. Dacă φ este formulă şi x este o variabilă, atunci $\forall x\varphi$ şi $\exists x\varphi$ sunt formule. În acest caz spunem că x este variabilă **cuantificată**.
5. Alte formule nu există.

Formulele de tip 1,2 sunt **formule atomice**.

Definiţia 2.2.4 Fie x o variabilă a limbajului $\mathcal{L}$. Spunem că x este **variabilă liberă** a formulei φ dacă:

1. φ este formulă atomică şi x apare în φ.
2. φ are forma $(\neg\alpha)$ şi x este variabilă liberă în α.
3. φ este de forma $(\alpha \vee \beta)$ sau $(\alpha \wedge \beta)$ sau $(\alpha \to \beta)$ sau $(\alpha \leftrightarrow \beta)$ şi x este variabilă liberă în α sau în β.
4. φ este de forma $\forall y\alpha$ sau $\exists y\alpha$, unde y este diferit de x, şi x este variabilă liberă în α.

Spunem că variabila x este **legată**, dacă nu e liberă. O formulă în care orice variabilă este legată se numeşte **formulă închisă**.

Exemplul 2.2.5 1) În formula „$\forall x(x = y)$" variabila x este legată, iar y este liberă. Formula „$\forall x\forall y(x \wedge y = y \wedge x)$" este închisă.

2) Fie formula $\forall x((x = y) \wedge (P(x) \to Q(y)))$; atunci $x = y$, $P(x) \to Q(y)$, $P(x)$ sunt subformule, dar $\forall x(x = y)$ nu este.

Definiţia 2.2.6 a) Fie φ o formulă. Spunem că **variabila** x **este substituită cu expresia** t, dacă în φ, orice apariţie a lui x este înlocuită cu t, exceptând subformulele de forma $\forall x\delta$ sau $\exists x\delta$, care rămân neschimbate. Notăm noua formula prin φ^x_t.

b) Substituţia variabilei x cu expresia t este **permisă** în următoarele cazuri:

1. Dacă φ este formulă atomică.
2. Dacă φ are forma $(\neg\alpha)$ sau $(\alpha \wedge \beta)$ sau $(\alpha \vee \beta)$ sau $(\alpha \to \beta)$ sau $(\alpha \leftrightarrow \beta)$ şi substituţia lui x cu t în α şi β este permisă.
3. Dacă φ are forma $\forall y\alpha$ sau $\exists y\alpha$ şi suntem în una din următoarele cazuri:
   (i) x nu este liberă în φ.
   (ii) y nu apare în t şi substituţia lui x cu t în α este permisă.

c) Printr-o **generalizare** a formulei φ înţelegem o formulă de forma $\forall x_1 x_2 \dots x_n \varphi$.

Exemplul 2.2.7 1) Evident, avem $\varphi_x^x = \varphi$.
2) În formula $\forall y(x = y)$ substituţia lui x cu y nu e permisă.

Exerciţiul 14 Fie f, g, h simboluri de funcţii de 1, 2 respectiv 3 variabile, şi fie P, Q simboluri de predicate de 1 respectiv 3 variabile.

1. Sunt termeni următoarele cuvinte?
   (a) $f(g(x, y))$.
   (b) $g(f(z), h(x, y, z))$.
   (c) $f(g(x), h(x, y, z))$.
2. Sunt formule următoarele cuvinte?
   (a) $Q(x, f(x), h(y, z, z))$.
   (b) $(P(x) \to (\forall y)(Q(x, y, z) \land P(g(x, y))))$.
   (c) $Q(P(x), f(y), z)$.
   (d) $f(h(x, y, z))$.

Exerciţiul 15 Să se scrie toate subformulele formulei:
a) $Q(f(x), g(x, y))$;
b) $\exists x Q(x, y) \to \neg(P(g(x, y)) \land \forall x P(z))$.

Exerciţiul 16 Să se descrie mulţimea termenilor (expresiilor) unui limbaj de ordinul I, dacă se dau:
a) o variabilă x şi un simbol de funcţie unară (de o variabilă) f;
b) o variabilă x şi un simbol de funcţie binară (de două variabile) f;

2.3 Structura unui limbaj de ordinul întâi. Modele

Acum dăm semnificaţie şi valori de adevăr formulelor unui limbaj de ordinul întâi.

Definiţia 2.3.1 O **structură a** $\mathcal{M}$ a unui limbaj de ordinul întâi $\mathcal{L}$ constă din următoarele date:

1. O mulţime nevidă M, pe care o numim **univers** şi o notăm cu $|\mathcal{M}|$.
2. Fiecărei constante a îi corespunde un element $\widetilde{a} \in M$.
3. Fiecărui simbol de funcţie n-ară f îi corespunde o funcţie $\widetilde{f} : M^n \to M$.
4. Fiecărui simbol de predicat n-ar P îi corespunde un predicat n-ar $\widetilde{P}$ pe mulţimea M (adică o submulţime $\widetilde{P} \subseteq M^n$).
5. Simbolului de egalitate îi corespunde relaţia de egalitate pe M.

De multe ori vom nota simplu $\widetilde{a}$ cu a, $\widetilde{f}$ cu f, $\widetilde{P}$ cu P. În continuare considerăm fixat un limbaj de ordinul întâi $\mathcal{L}$ şi o structură $\mathcal{M}$ a lui $\mathcal{L}$, cu $M = |\mathcal{M}|$.

Definiţia 2.3.2 a) Dacă $\mathcal{V}$ este mulţimea variabilelor lui $\mathcal{L}$, atunci o funcţie $s : \mathcal{V} \to M$ se numeşte **interpretare** a structurii $\mathcal{M}$.
b) Definim inductiv **valoarea** $H_s^{\mathcal{M}}(t) \in M$ a expresiei t, corespunzătoare interpretării s, astfel:

1. Pentru fiecare variabilă x, avem $H_s^{\mathcal{M}}(x) = s(x)$.
2. Pentru fiecare constantă a, avem $H_s^{\mathcal{M}}(a) = \widetilde{a}$.
3. Pentru fiecare funcţie n-ară f şi expresii $t_1, \dots, t_n$ avem
$$H_s^{\mathcal{M}}(f(t_1, \dots, t_n)) = \widetilde{f}(H_s^{\mathcal{M}}(t_1), \dots, H_s^{\mathcal{M}}(t_n)).$$

c) Definim inductiv **valoarea** $H_s^{\mathcal{M}}(\varphi) \in V = \{0, 1\}$ a formulei φ, corespunzătoare interpretării s astfel:

1. pentru orice predicat P n-ar şi orice expresii $t_1, \dots, t_n$, $H_s^{\mathcal{M}}(P(t_1, \dots, t_n)) = 1$ dacă $(H_s^{\mathcal{M}}(t_1), \dots, H_s^{\mathcal{M}}(t_n)) \in \widetilde{P}$, altfel $H_s^{\mathcal{M}}(P(t_1, \dots, t_n)) = 0$.
2. $H_s^{\mathcal{M}}(t_1 = t_2) = 1$, dacă $H_s^{\mathcal{M}}(t_1) = H_s^{\mathcal{M}}(t_2)$, altfel $H_s^{\mathcal{M}}(t_1 = t_2) = 0$.

3. $H_s^{\mathcal{M}}(\neg\varphi) = 1$, dacă $H_s^{\mathcal{M}}(\varphi) = 0$, altfel $H_s^{\mathcal{M}}(\neg\varphi) = 0$.
   $H_s^{\mathcal{M}}(\varphi \vee \psi) = 1$, dacă $H_s^{\mathcal{M}}(\varphi) = 1$ sau $H_s^{\mathcal{M}}(\psi) = 1$, altfel $H_s^{\mathcal{M}}(\varphi \vee \psi) = 0$.
   $H_s^{\mathcal{M}}(\varphi \wedge \psi) = 1$, dacă $H_s^{\mathcal{M}}(\varphi) = H_s^{\mathcal{M}}(\psi) = 1$, altfel $H_s^{\mathcal{M}}(\varphi \wedge \psi) = 0$.
   $H_s^{\mathcal{M}}(\varphi \to \psi) = 0$, dacă $H_s^{\mathcal{M}}(\varphi) = 1$ şi $H_s^{\mathcal{M}}(\psi) = 0$, altfel $H_s^{\mathcal{M}}(\varphi \to \psi) = 1$.
   $H_s^{\mathcal{M}}(\varphi \leftrightarrow \psi) = 1$, dacă $H_s^{\mathcal{M}}(\varphi) = H_s^{\mathcal{M}}(\psi)$, altfel $H_s^{\mathcal{M}}(\varphi \leftrightarrow \psi) = 0$.

4. Considerăm funcţia (interpretarea)

$$s(x|m) : \mathcal{V} \to M, \qquad s(x|m)(y) = \begin{cases} s(y), & \text{dacă } y \neq x \\ m & \text{dacă } y = x \end{cases}.$$

   Atunci:
   $H_s^{\mathcal{M}}(\forall x\varphi) = 1$ dacă şi numai dacă pentru orice $m \in M$ avem $H_{s(x|m)}^{\mathcal{M}}(\varphi) = 1$.
   $H_s^{\mathcal{M}}(\exists x\varphi) = 1$ dacă şi numai dacă există $m \in M$ astfel încât $H_{s(x|m)}^{\mathcal{M}}(\varphi) = 1$.

Definiţia 2.3.3 a) Spunem că $\mathcal{M}$ este **model** al lui φ (sau că $\mathcal{M}$ **satisface** φ), dacă $H_s^{\mathcal{M}}(\varphi) = 1$ pentru orice interpretare s a lui $\mathcal{M}$. Notaţie: $\mathcal{M} \models \varphi$.

Spunem că $\mathcal{M}$ este **model** pentru mulţimea de formule Γ (sau că $\mathcal{M}$ **satisface** pe Γ), dacă $\mathcal{M} \models \gamma$ pentru orice $\gamma \in \Gamma$. Notaţie: $\mathcal{M} \models \Gamma$.

Prin inducţie se arată:

Teorema 2.3.4 1) *Dacă interpretările* s *şi* r *coincid pe variabilele ce apar în expresia* t*, atunci* $H_s^{\mathcal{M}}(t) = H_r^{\mathcal{M}}(t)$.
2) *Dacă* s *şi* r *coincid pe variabilele libere ce apar în formula* φ*, atunci* $H_s^{\mathcal{M}}(\varphi) = H_r^{\mathcal{M}}(\varphi)$.

Corolar 2.3.5 *Dacă* σ *este o formulă închisă, atunci* $\mathcal{M} \models \sigma$ *dacă şi numai dacă există o interpretare* s *astfel ca* $H_s^{\mathcal{M}}(\sigma) = 1$. (Deci valoarea unei formule închise este independentă de interpretarea fixată a structurii.)

Definiţia 2.3.6 a) O formulă φ este **tautologie** (**identic adevărată**), dacă orice structură $\mathcal{M}$ este model al lui φ. Formula φ se numeşte **contradicţie**, dacă $\neg\varphi$ este tautologie.
b) Dacă formula $\varphi \to \psi$ este tautologie, atunci spunem că ψ **rezultă** din φ şi notăm $\varphi \Rightarrow \psi$.
c) Dacă formula $\varphi \leftrightarrow \psi$ este tautologie, atunci spunem că φ este **echivalent** cu ψ şi notăm $\varphi \Leftrightarrow \psi$.

Exemplul 2.3.7 1) Pentru orice formulă φ avem că $\varphi \to \varphi$ tautologie, iar $\neg(\varphi \to \varphi)$ este contradicţie.
2) $\forall y(y = y)$ este tautologie, în timp ce $\exists y(\neg(y = y))$ este contradicţie.
3) Dacă φ este tautologie, atunci orice generalizare $\forall x_1 \ldots \forall x_n \varphi$ este tautologie.

Observaţii 2.3.8 a) φ este contradicţie dacă şi numai dacă pentru orice structură $\mathcal{M}$ şi interpretare $s : \mathcal{V} \to |\mathcal{M}|$, avem $H_s^{\mathcal{M}}(\varphi) = 0$.
b) Dacă φ este contradicţie, atunci nu are model. Afirmaţia inversă are loc doar pentru formule închise.
c) $\varphi \Rightarrow \psi$ dacă şi numai dacă pentru orice structură $\mathcal{M}$ şi pentru orice interpretare $s : \mathcal{V} \to |\mathcal{M}|$, dacă s satisface pe φ, atunci satisface şi pe ψ.
d) Dacă $\varphi \Rightarrow \psi$, atunci orice model $\mathcal{M}$ al lui φ este şi model al lui ψ. Afirmaţia inversă are loc doar pentru formule închise.
e) $\varphi \Leftrightarrow \psi$ dacă şi numai dacă pentru orice structură $\mathcal{M}$ şi pentru orice interpretare $s : \mathcal{V} \to |\mathcal{M}|$, s satisface pe φ dacă şi numai dacă satisface pe ψ.
f) Dacă $\varphi \Leftrightarrow \psi$, atunci are φ exact aceleaşi modele ca şi ψ. Afirmaţia inversă are loc doar pentru formule închise.

2.3.9 Prezentăm câteva tautologii importante, care vor fi folosite în demonstraţiile din capitolele următoare. Fie A, B şi C formule ale limbajului $\mathcal{L}$ ordinul întâi astfel încât în C variabila x nu e liberă.

(1) $\forall x\forall yA \Leftrightarrow \forall y\forall xA$, $\exists x\exists yA \Leftrightarrow \exists y\exists xA$

(2) $(\exists x)(\forall y)A \Rightarrow (\forall y)(\exists x)A$, $\forall xA \Rightarrow \exists xA$

(3) $\forall x(A \wedge B) \Leftrightarrow \forall xA \wedge \forall xB$

(4) $\exists x(A \vee B) \Leftrightarrow \exists xA \vee \exists xB$

(5) $\forall xA \vee \forall xB \Rightarrow \forall x(A \vee B)$

(6) $\exists x(A \wedge B) \Rightarrow \exists xA \wedge \exists xB$

(7) $\neg\forall x A \Leftrightarrow \exists x(\neg A)$, $\quad \neg\exists x A \Leftrightarrow \forall x(\neg A)$ (legile lui De Morgan)

(8) $C \wedge \forall x A \Leftrightarrow \forall x(C \wedge A)$,
$C \vee \forall x A \Leftrightarrow \forall x(C \vee A)$,
$C \wedge \exists x A \Leftrightarrow \exists x(C \wedge A)$,
$C \vee \exists x A \Leftrightarrow \exists x(C \vee A)$.

(9) $C \to \forall x A \Leftrightarrow \forall x(C \to A)$,
$C \to \exists x A \Leftrightarrow \exists x(C \to A)$,
$\forall x A \to C \Leftrightarrow \exists x(A \to C)$,
$\exists x A \to C \Leftrightarrow \forall x(A \to C)$.

(10) $\forall x\varphi \Rightarrow \varphi^x_t$ şi $\varphi^x_t \Rightarrow \exists x\varphi$ (dacă în formula φ înlocuirea variabilei libere x cu expresia t este permisă).

Exerciţiul 17 a) Să se arate că în (2), (5) şi (6) implicaţiile inverse nu sunt adevărate (dând contraexemple).
b) Să se demonstreze (9) folosind (8) şi (7).

Exerciţiul 18 Considerăm structura $\mathcal{M} = (\mathbb{N}, S, P)$, unde S şi P sunt predicate de 3 variabile definite astfel: $S(x, y, z)$ este adevărat dacă şi numai dacă $x + y = z$, iar $P(x, y, z)$ este adevărat dacă şi numai dacă $xy = z$.

1. Să se scrie o formulă cu o variabilă liberă x, adevărată dacă şi numai dacă:
   (a) $x = 0$;
   (b) $x = 1$;
   (c) $x = 2$;
   (d) x este număr par;
   (e) x este număr impar;
   (f) x este număr prim.
2. Să se scrie o formulă cu două variabile libere x, y, adevărată dacă şi numai dacă:
   (a) $x = y$;
   (b) $x \leq y$;
   (c) $x < y$;
   (d) x divide y;
   (e) x şi y sunt numere prime gemene (diferenţa lor e 2).
3. Să se scrie o formulă cu trei variabile libere x, y, z, adevărată dacă şi numai dacă:
   (a) z este cel mai mic multiplu comun al lui x şi y;
   (b) z este cel mai mare divizor comun al lui x şi y;
4. Să se scrie propoziţia (formula închisă) care exprimă:
   (a) comutativitatea adunării;
   (b) asociativitatea adunării;
   (c) comutativitatea înmulţirii;
   (d) asociativitatea înmulţirii;
   (e) distributivitatea adunării faţă de înmulţire;
   (f) pentru orice număr natural există unul strict mai mare;
   (g) infinitatea mulţimii numerelor prime;
   (h) infinitatea mulţimii perechilor de numere prime gemene;
   (i) orice număr natural este suma a 4 pătrate perfecte;
   (j) existenţa celui mai mic multiplu comun şi a celui mai mare divizor comun;
   (k) orice număr par > 2 este suma a două numere prime.

Exercişiul 19 (Hexagonul opoziţiilor din logica aristotelică) Fie S şi P două proprietăţi referitoare la elementele unei mulţimi M, astfel ca S corespunde unei submulţimi nevide a lui M. Considerăm următoarele afirmaţii în limbaj natural:

A: toţi S sunt P;
E: niciun S nu e P (altfel formulat: toţi S nu sunt P);
I: unii S sunt P;
O: unii S nu sunt P;
U: toţi S sunt P sau niciun S nu e P;
Y: unii S sunt P şi unii S nu sunt P.

a) Să se scrie aceste afirmaţii ca formule închise ale unui limbaj de ordinul I.
b) Să se găsească cele $C_6^2 = 15$ relaţii între propoziţiile A, E, I, O, U şi Y (sau negaţiile acestora).

2.4 Problema deciziei în logica de ordinul întâi

Fixăm un limbaj $\mathcal{L}$ de ordinul întâi.

Definiţia 2.4.1 a) Spunem că a formula ψ este **consecinţă** a formulelor $\varphi_1, \ldots, \varphi_n$ dacă pentru orice structură $\mathcal{M}$ şi pentru orice interpretare $s : V \to |\mathcal{M}|$, dacă s satisface toate formulele $\varphi_1, \ldots, \varphi_n$, atunci satisface şi formula ψ.

Notaţie: $\varphi_1, \ldots, \varphi_n \models B$ sau $\frac{\varphi_1, \ldots, \varphi_n}{\psi}$, şi numim aceasta **schemă de deducţie**. Formulele $\varphi_1, \ldots, \varphi_n$ se numesc **premize (ipoteze)**, iar ψ este **concluzie (consecinţă)**.

Dacă mai sus $n = 0$, atunci ψ este tautologie.

Mai general, pentru mulţimile de formule Σ, Γ e clar ce se înţelege prin notaţiile $\Sigma \Rightarrow \Gamma$ sau $\Sigma \models \Gamma$.

Observaţii 2.4.2 a) Vedem că ψ este consecinţă a lui $\varphi_1, \ldots, \varphi_n$ (adică $\varphi_1, \ldots, \varphi_n \models \psi$), dacă şi numai dacă ψ rezultă din $\varphi_1 \wedge \cdots \wedge \varphi_n$ (adică $\varphi_1 \wedge \cdots \wedge \varphi_n \to \psi$ este tautologie, adică $\varphi_1 \wedge \cdots \wedge \varphi_n \Rightarrow \psi$).

b) Alonzo Church a demonstrat în 1936 că pentru un limbaj de ordinul întâi nu se poate da o *procedură generală de decizie.*

2.4.1 Deducţia formală în logica de ordinul întâi

Ca şi în logica propoziţiilor, şi în logica de ordinul întâi se poate introduce o noţiune de deducţie formală independentă de structuri, interpretări şi modele. Vom vedea în paragraful următor că în cazul formulelor închise cele două abordări sunt echivalente.

2.4.3 Pentru a defini noţiunea de deducţie avem nevoie de:

1) Un set de tautologii speciale, numite **axiome logice** (axiomele (A7)-(A11) se numesc **axiomele egalităţii**).

(A1) $\varphi \to (\psi \to \varphi)$.

(A2) $(\varphi \to (\psi \to \sigma)) \to ((\varphi \to \psi) \to (\varphi \to \sigma))$

(A3) $((\neg\psi) \to (\neg\varphi)) \to (((\neg\psi) \to \varphi) \to \psi))$, unde φ, ψ, σ sunt formule arbitrare.

(A4) $\forall x\varphi \to \varphi_t^x$, dacă în φ înlocuirea lui x cu t este permisă.

(A5) $\forall x(\varphi \to \psi) \to (\forall x\varphi \to \forall x\psi)$, unde φ, ψ sunt formule arbitrare.

(A6) $\varphi \to \forall x\varphi$, dacă x este variabilă legată în φ.

(A7) $x = x$

(A8) $(x = y) \to (y = x)$

(A9) $((x = y) \wedge (y = z)) \to (x = z)$, unde x, y, z sunt variabile arbitrare.

(A10) $((x_1 = y_1) \wedge \cdots \wedge (x_n = y_n)) \to (P(x_1, \ldots, x_n) \to P(y_1, \ldots, y_n))$, unde P este un predicat n-ar.

(A11) $((x_1 = y_1) \wedge \cdots \wedge (x_n = y_n)) \to (f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n))$, unde f este o funcţie n-ară.

2) schema de deducţie **Modus Ponens** (MP), adică $\frac{\varphi, \varphi \to \psi}{\psi}$.

Definiţia 2.4.4 Fie formulele $\varphi_1, \ldots, \varphi_n$ $(n \geq 0)$.

a) O **deducţie** din formulele $\varphi_1, \ldots, \varphi_n$ este un şir de formule $\delta_1, \ldots, \delta_k$ astfel încât pentru orice $i = 1, \ldots, k$ avem:

1. δ_i este axiomă logică, sau

2. $\delta_i = \varphi_l$ pentru un $l = 1, \ldots, n$, sau

3. δ_i se obţine din δ_j,δ_l (unde $j, l < i$) aplicând schema Modus Ponens (MP).

b) Spunem că formula ψ este **deductibilă** din formulele $\varphi_1, \ldots, \varphi_n$ (notaţie: $\varphi_1, \ldots, \varphi_n \vdash \psi$), dacă ψ este ultimul termen al unei deducţii din $\varphi_1, \ldots, \varphi_n$. Formulele $\varphi_1, \ldots, \varphi_n$ sunt **premizele** (**ipotezele** deducţiei.

Dacă $n = 0$, atunci notăm $\vdash \psi$. Mai general, pentru mulţimile de formule Σ, Γ folosim notaţia $\Sigma \vdash \Gamma$.

c) Spunem că mulţimea de formule Σ este **contradictorie**, dacă există o formulă φ astfel ca $\Sigma \vdash \varphi \wedge (\neg\varphi)$.

Teorema 2.4.5 a) *Dacă* $\delta_1, \ldots, \delta_k$ *este o deducţie, atunci şi* $\delta_1, \ldots, \delta_i$ *este o deducţie pentru orice* $i = 1, \ldots, k$.

b) *Dacă* $\Sigma \vdash \psi$ *şi* $\Sigma \vdash \psi \to \sigma$*, atunci* $\Sigma \to \sigma$.

c) *Dacă* $\Sigma \subseteq \Delta$ *şi* $\Sigma \vdash \psi$*, atunci* $\Delta \vdash \psi$.

d) *Dacă* $\Sigma \vdash \Gamma$ *şi* $\Gamma \vdash \psi$*, atunci* $\Sigma \vdash \psi$.

e) *Dacă* $\Sigma \vdash \psi \wedge (\neg\psi)$*, atunci* $\Sigma \vdash \sigma$ *pentru orice formulă* σ.

f) Teorema deducţiei (Herbrand, 1930): $\Sigma \vdash \psi \to \sigma$ *dacă şi numai dacă* $\Sigma \cup \{\psi\} \vdash \sigma$.

g) Teorema generalizării (GEN)*: Fie* Γ *o mulţime de formule unde* x *este variabilă legată. Dacă* $\Gamma \vdash \varphi$*, atunci* $\Gamma \vdash \forall x\varphi$.

h) Generalizare pe constante*: Fie* Γ *o mulţime de formule unde constanta* c *nu apare. Dacă* $\Gamma \vdash \varphi$*, atunci există o variabilă* x *care nu apare în* φ *astfel ca* $\Gamma \vdash \forall x\varphi^c_x$*. Mai mult, există o deducţie a lui* $\forall x\varphi^c_x$ *din* Γ*, în care* c *nu apare.*

Exemplul 2.4.6 Arătăm că $\forall x\forall y\varphi \vdash \forall y\forall x\varphi$.

1. $\forall x\forall y\varphi$ — Ipoteză
2. $\forall x\forall y\varphi \to \forall y\varphi$ — A4
3. $\forall y\varphi$ — 1,2 MP
4. $\forall y\varphi \to \varphi$ — A4
5. φ — 3,4 MP
6. $\forall x\varphi$ — 5 GEN
7. $\forall y\forall x\varphi$ — 6 GEN.

2.4.2 Teoremele principale ale teoriei modelelor

Fixăm un limbaj $\mathcal{L}$ de ordinul întâi. Fie Σ o mulţime de formule închise. Mulţimea formulelor deductibile din Σ se numeşte **teorie**, iar formulele din Σ sunt **axiome** ale teoriei.

Teorema 2.4.7 (Teorema lui Gödel de completitudine)[1] *Fie* φ *o formulă închisă. Are loc* $\Sigma \models \varphi$ *dacă şi numai dacă* $\Sigma \vdash \varphi$.

Teorema 2.4.8 (Teorema lui Gödel de completitudine, varianta model-teoretică) *Mulţimea* Σ *de formule nu este contradictorie dacă şi numai dacă are model.*

Teorema 2.4.9 (Teorema de compactitate) Σ *are model dacă şi numai dacă orice submulţime finită a sa are.*

2.4.3 Teorii formale

Să degajăm câteva idei generale din discuţia de până acum, idei care vor reveni şi în capitolele următoare. În matematică, un sistem formal constă din următoarele date: un **alfabet**, adică o mulţime finită de simboluri ce pot fi folosite pentru a construi *formule* (care sunt şiruri finite de simboluri); o **gramatică** care spune cum se construiesc corect formulele; o mulţime de **axiome** (fiecare axiomă e o formulă corect formată); o mulţime de **reguli de deducţie** (sau de inferenţă). O teorie formală este un sistem formal împreună cu toate **teoremele**, adică toate formulele ce pot fi deduse din axiome aplicând regulile de deducţie.

Şirul de formule deduse care conduce la o teoremă se numeşte demonstraţie formală. *Teoria demonstraţiei* este ramura Logicii matematice care studiază demonstraţiile formale. Teoremele despre un sistem formal sunt numite de obicei *metateoreme.*

[1] Kurt Gödel (1906–1978), logician, matematician şi filosof austriac, cunoscut mai ales pentru teoremele sale de *incompletitudine.*

Sistemul formal se numeşte **complet** dacă pentru pentru fiecare formulă ϕ, ϕ sau $\neg\phi$ este deductibil. Sistemul formal se numeşte **necontradictoriu** dacă odată cu o formulă nu poate fi dedusă şi negaţia ei. Spunem că avem de a face cu un sistem logic, dacă sistemului formal i se asociază şi o **semantică** (semnificaţie), de obicei sub forma unei interpretări model-teoretice, prin care fiecărei formule închise (propoziţii) i se dă o valoare de adevăr. Sistemul se numeşte **consistent (satisfiabil)** dacă are model, adică fiecare teoremă (formulă dedusă) este adevărată în interpretarea dată. O teorie consistentă (semantic) este necontradictorie (sintactic), dar în general cele două aspecte nu sunt echivalente. (Vedem deci că teoria demonstraţiei se referă la **sintaxă**, iar teoria modelelor la semantică.)

În mod uzual, teoriile matematice sunt doar semi-formalizate, efortul pentru o formalizare totală fiind prea mare (şi chiar ar fi o pedanterie inutilă). Demonstraţiile matematice obişnuite pot fi privite ca nişte schiţe pe baza cărora pot fi construite, în principiu, demonstraţii formale.

La formalizarea logicii au contribuit în mare măsură Richard Dedekind, Gottlob Frege, Giuseppe Peano şi Bertrand Russell, iar teoria demonstraţiei a fost motivată de programul lui David Hilbert (numit *formalism*) de fundamentare a matematicii prin reducerea sa la sisteme formale finitiste (adică de a da demonstraţii formale finite a consistenţei tuturor teoriilor formale). Teoremele de completitudine menţionate mai sus au dat iniţial suport acestui program. Mai târziu însă, teoremele de incompletitudine ale lui Gödel au arătat că o teorie formală suficient de largă încât să conţină aritmetica lui Peano (pe care o vom discuta în Secţiunea 7.1) nu poate fi concomitent completă şi consistentă, şi astfel, programul lui Hilbert nu poate fi dus până la capăt. Totuşi, programul formalist a contribuit din plin la dezvoltarea nu doar a logicii, ci şi a bazelor teoretice ale calculatoarelor de către Alonzo Church şi Alan Turing.

2.5 Logică clasică şi logici neclasice

Teoria discutată în cele două capitole de mai sus aparţine Logicii clasice, iniţiată de Aristotel în *Organon*, unde a introdus silogismul. Aceasta se caracterizează prin: legea terţului exclus, legea dublei negaţii, legea necontradicţiei, monotonia şi idempotenţa implicaţiei, comutativitatea conjuncţiei, dualitatea De Morgan etc. Din punct de vedere semantic, logica clasică este bivalentă, propoziţiile având două valori de adevăr (mai general, valorile de adevăr sunt elemente ale unei *algebre Boole*). Reformularea algebrică a logicii a fost facută de George Boole, iar logica predicatelor de ordinul I a fost introdusă de Gottlob Frege.

Prin logici neclasice înţelegem sisteme formale care diferă de logica clasică sub diferite aspecte, scopul fiind de a construi modele pentru alte tipuri de raţionamente. Prezentăm pe scurt câteva asfel de sisteme formale.

Logicile polivalente (sau **multivalente**), incluzând **Logica fuzzy**, renunţă la legea terţului exclus şi permit şi alte valori de adevăr în afara lui 0 şi 1. Sunt studiate încă din anii 1920 de Jan Łukasiewicz şi Alfred Tarski.

Logica intuiţionistă înlocuieşte conceptul tradiţional de adevăr cu cel de *demonstrabilitate constructivă*. Altfel spus, o afirmaţie este considerată adevărată doar dacă avem o demonstraţie efectivă a ei, şi este falsă dacă din ea se poate deduce o contradicţie. O afirmaţie nedemonstrată nu are valoare de adevăr. Demonstraţia constructivă existenţei unui obiect poate fi transformată într-un algoritm prin care se generează un exemplu concret. Legea terţului exclus, legea dublei negaţii şi legile lui De Morgan nu sunt admise ca axiome, dar pot fi demonstrate de la caz la caz. Logica intuiţionistă a fost formalizată de Arend Heyting pornind de la programul intuiţionist al lui L.E.J. Brower de fundamentare a matematicii. Semantica logicii intuiţioniste foloseşte fie aşa-numitele *algebre Heyting* în locul algebrelor Boole din logica clasică, fie *modelele Kripke*, dezvoltate în anii 1950-1960 de Saul Kripke şi André Joyal. Logica liniară este o variantă a logicii intuiţioniste în care se renunţă şi la idempotenţa implicaţiei, adică la regula $\frac{\Gamma, C, C \vdash B}{\Gamma, C \vdash B}$. Are aplicaţii importante în domenii precum limbaje de programare, mecanica cuantică şi lingvistică. Există şi alte dezvoltări mai recente ale acestor idei.

Logica modală este un tip de logică formală dezvoltată în anii 1960 care extinde logica clasică prin adăugarea unor operatori care exprimă *modalitatea*. În lingvistică, modalitatea permite vorbitorului să ataşeze unei afirmaţii expresia unei atitudini, credinţe, obligaţii etc. De exemplu, avem modalităţi *aletice* (p este posibil, este necesar, este imposibil), *temporale* (a fost p, a fost intotdeauna p, va fi p, va fi întotdeauna p), *deontice* (p este obligatoriu, notat Op, p este permis, notat Pp), *epistemice* (se ştie că p), *ale credinţei* (se crede că p). Operatorii modali se reprezintă prin simboluri cum ar fi $\Box$ pentru *peste necesar* sau $\Diamond$ pentru *este posibil*. Astfel, de exemplu, au loc tautologiile $\Diamond p \leftrightarrow \neg\Box\neg p$; $\Box p \leftrightarrow \neg\Diamond\neg P$; $Pp \to \neg O \neg p$ (în limbaj natural spunem, de exemplu, ,,este posibil să ningă azi dacă şi numai dacă nu este necesar să nu ningă azi"; ,,este necesar să ningă azi dacă şi numai dacă nu este posibl să nu ningă azi"; ,,dacă p is permis, atunci non p nu este obligatoriu"). Logica modală este folosită în ştiinţe umaniste precum teoria literară, estetica, istoria.

Capitolul 3

MULŢIMI

3.1 Teoria naivă şi teoria axiomatică a mulţimilor

Începem cu o recapitulare a cunoştinţelor dobândite în liceu.

3.1.1 Prin **mulţime** înţegem o colecţie de lucruri (obiecte, noţiuni) bine determinate, numite **elementele** sale. Faptul că elementul a **aparţine** mulţimii A se notează $a \in A$; notaţia $b \notin A$ înseamnă: b nu aparţine lui A. Aceste noţiuni sunt primare, adică nu le definim.

O mulţime poate fi dată prin enumerarea elementelor, de exemplu $A = \{1, 2, 3, 4\}$, $B = \{x, y, z\}$ sau printr-o proprietate (predicat) $P(x)$:

$$A = \{x \mid P(x)\},$$

de exemplu $A = \{x \mid x \in \mathbb{R} \text{ şi } 0 \le x \le 3\}$.

Mulţimile A şi B sunt **egale**, $A = B$, dacă au acelea şi elemente.

Mulţimea vidă este unica mulţime care nu are niciun element. Notaţie: $\emptyset$.

Definiţia 3.1.2 a) O mulţime A este **submulţime** a mulţimii B, dacă orice element al lui A este element al lui B; notaţie: $A \subseteq B$. Orice mulţime nevidă A are două submulţimi **triviale**: $\emptyset$ şi A.

Să reţinem că $A = B$ dacă şi numai dacă $A \subseteq B$ şi $B \subseteq A$. Dacă $A \subseteq B$ şi există $x \in B$ astfel încât $x \notin A$, atunci spunem că A este **submulţime proprie** a lui B. Notaţiee: $A \subset B$.

b) Submulţimile unei mulţimi U formează **mulţimea părţilor (mulţimea putere)** a lui U:

$$\mathcal{P}(U) = \{A \mid A \subseteq U\},$$

adică $A \in \mathcal{P}(U) \Leftrightarrow A \subseteq U$.

Definiţia 3.1.3 **Intersecţia** mulţimilor A şi B este mulţimea elementelor comune, adică

$$A \cap B = \{x \mid x \in A \text{ şi } x \in B\}.$$

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

Reuniunea mulţimilor A şi B este mulţimea

$$A \cup B = \{x \mid x \in A \text{ sau } x \in B\}.$$

Diferenţa mulţimilor $A \setminus B$ este mulţimea

$$A \setminus B = \{x \mid x \in A \text{ şi } x \notin B\}.$$

Dacă $B \subseteq A$, atunci $A \setminus B$ este **complementara** mulţimii B relativ la A. Notaţie: $\complement_A(B)$.

Diferenţa simetrică a mulţimilor A şi B este mulţimea

$$A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

Produsul cartezian al mulţimilor $A_1, A_2, \dots, A_n$ este mulţimea

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \dots, x_n) \mid x_1 \in A_1,\ x_2 \in A_2,\ \dots, x_n \in A_n\}.$$

Dacă pentru un i, $A_i = \emptyset$, atunci $A_1 \times A_2 \times \cdots \times A_n = \emptyset$.

Exerciţiul 20 Fie A, B, C mulţimi incluse în universul U. Să se demonstreze următoarele proprietăţi de bază:
a) $A \subseteq A$ (*reflexivitate*);
b) dacă $A \subseteq B$ şi $B \subseteq C$, atunci $A \subseteq C$ (*tranzitivitate*);
c) dacă $A \subseteq B$ şi $B \subseteq A$, atunci $A = B$ (*antisimetrie*);
d) $A \cup B = B \cup A$, $A \cap B = B \cap A$ (*comutativitate*);
e) $(A \cup B) \cup C = A \cup (B \cup C))$, $(A \cap B) \cap C = A \cap (B \cap C))$ (*asociativitate*);
f) $A \cap A = A$, $A \cap A = A$ (*idempotenţă*);
g) $A \cup (A \cap B) = A$; $A \cap (B \cup A) = A$ (*absorbţie*);
h) $A \cup \emptyset = A$; $A \cap \emptyset = \emptyset$;
i) $A \cup \complement A = U$; $A \cap \complement A = \emptyset$;
j) $\complement\complement A = A$;

Exerciţiul 21 Fie A, B, C mulţimi. Să se demonstreze:
a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (*distributivitate*);
b) $A \setminus B = A \cap \complement B$;
c) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C) = (A \setminus B) \setminus C$;
d) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$;
e) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$;
f) $(A \cap B) \setminus C = A \cap (B \setminus C) = (A \setminus C) \cap B$;
g) $\complement(A \cup B) = \complement A \cap \complement B$; $\complement(A \cap B) = \complement A \cup \complement B$ (*formulele lui De Morgan*).

Exerciţiul 22 Să se arate că pentru orice mulţimi A, B, C avem:
a) $A \triangle B = (A \cap \complement B) \cup (B \cap \complement A)$;
b) $A \triangle B = B \triangle A$;
c) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$;
d) $A \triangle \emptyset = A$; $\complement A = A \triangle U$; $A \triangle A = \emptyset$;
e) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$;
f) $A \cup B = A \triangle B \triangle (A \cap B)$.

Exerciţiul 23 Să se arate că pentru orice mulţimi A, B, C, dacă $A \cap C = B \cap C$ şi $A \cup C = B \cup C$ atunci $A = B$.

Exerciţiul 24 Fie A, B, C mulţimi date. Să se determine mulţimea X care satisface:
a) $A \cap X = B$, $A \cup X = C$;
b) $A \setminus X = B$, $X \setminus A = C$.

Exerciţiul 25 Dacă A, B, C, D sunt mulţimi, atunci:
a) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$;
b) afirmaţia $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D)$ nu e adevărată în general;
c) $(A \cup B) \times C = (A \times C) \cup (B \times C)$;
d) $(A \cap B) \times C = (A \times C) \cap (B \times C)$;
e) $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$.

3.1.4 Abordarea din acest paragraful ţine de aşa-numita **teorie naivă a mulţimilor**, dezvoltată de matematicianul german Georg Cantor după 1870. S-a arătat mai târziu că această teorie duce la contradicţii, din cauza faptului că permite formarea de mulţimi ,,mari”, fără restricţii. Paradoxul lui Bertrand Russel (1902) este printre cele mai cunoscute: considerăm mulţimea R a tuturor mulţimilor care nu se conţin ca element; atunci $R \in R$ înseamnă că $R \notin R$, iar $R \notin R$ înseamnă că $R \in R$; în orice caz avem o contradicţie care vine din faptul că teoria permite ca R să fie considerată mulţime.

Teoria axiomatică a mulţimilor a fost creată pentru a elimina aceste contradicţii. Cele mai utilizate sunt axiomatizările dezvoltate de Zermelo şi Fraenkel (ZF), respectiv von Neumann, Bernays şi Gödel (NBG).

Din punctul de vedere al logicii predicatelor, axiomele ambelor teorii pot fi date prin formule închise în limbajul de ordinul întâi $\mathcal{L}_S$, menţionat în capitolul anterior, care foloseşte un singur predicat binar $\in$ (,,aparţine”). Kurt Gödel a demonstrat în 1939 ca ambele sisteme axiomatice admit model, deci sunt necontradictorii.

3.2 Sistemul axiomatic von Neumann–Bernays–Gödel

Vom prezenta pe scurt sistemul axiomatic NBG, evitând totuşi o formalizare completă, iar *axioma alegerii* va fi enunţată doar în capitolele următoare.

Definiţia 3.2.1 a) Limbajul $\mathcal{L}_S$ al teoriei axiomatice NBG foloseşte pe lângă simbolurile logice in singur predicat de două variabile notat $\in$. Deci formulele atomice ale teoriei sunt $x = y$ şi $x \in y$. Simbolurile de variabile $x, y, z, \dots$ notează **clase**. Formula $x \in y$ se citeşte **clasa** x **aparţine clasei** y (sau y **conţine pe** x), iar $x = y$ se citeşte: clasa x este egală cu clasa y. Noţiunile de **clasă**, respectiv **aparţine** sunt considerate primare, nu se definesc.

b) O clasă x se numeşte **mulţime**, dacă există o clasă y, căreia îi aparţine (adică există y astfel încât $x \in y$). Dacă o clasă nu e mulţime, atunci se numeşte **clasă proprie**.

Se pune întrebarea dacă există mulţimi. Vom vedea mai jos că răspunsul este afirmativ.

3.2.2 Prezentăm în continuare axiomele.

1. Axioma extensionalităţii. Două clase sunt egale exact când au aceleaşi elemente, adică

$$\forall A \forall B((A = B) \leftrightarrow \forall x(x \in A \leftrightarrow x \in B)).$$

2. Axioma clasificării. Dacă $P(x)$ este o formulă, în care variabila x este liberă, atunci există o clasă care conţine exact elementele satisfăscând $P(x)$. Formal, exprimăm aceasta prin formula închisă

$$\forall y_1 \dots \forall y_n \exists z \forall x((x \in z) \leftrightarrow (\exists t(x \in t) \wedge P(x))).$$

Din axioma egalităţii rezultă că clasa de mai sus este unică şi o notăm

$$\{x \mid P(x)\}.$$

Folosind axioma clasificării, definim **clasa vidă** $\emptyset$ respectiv **universul** U, astfel:

$$\emptyset = \{x \mid x \neq x\}, \qquad U = \{x \mid x = x\}.$$

Vedem că clasa vidă nu are elemente, în timp ce toate mulţimile sunt elemente ale universului. Mai târziu vom vedea că în timp ce clasa vidă este mulţime, universul este clasă proprie.

3. Axioma perechii. Dacă x şi y sunt mulţimi, atunci clasa $\{z \mid (z = x) \vee (z = y)\}$ este mulţime.

Vom nota această mulţime prin $\{x, y\}$ şi o numim **pereche neordonată**. Dacă $x = y$, atunci perechea neordonată $\{x, y\}$ se notează $\{x\}$ şi se numeşte **mulţime cu un element**.

Definiţia 3.2.3 a) Fie A şi B clase. **Reuniunea claselor** A **şi** B este

$$A \cup B = \{x \mid (x \in A) \vee (x \in B)\},$$

iar **intersecţia claselor** A **şi** B este clasa

$$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}.$$

Mai general, $A \cup B \cup C = (A \cup B) \cup C$ (respectiv $A \cap B \cap C = (A \cap B) \cap C$), ...

b) **Reuniunea clasei** A este clasa

$$\bigcup A = \{x \mid \exists y((y \in A) \wedge (x \in y))\},$$

iar **intersecţia clasei** A este clasa

$$\bigcap A = \{x \mid \forall y((y \in A) \to (x \in y))\}.$$

(Să observăm că dacă A şi B sunt mulţimi, atunci $A \cup B = \bigcup\{A, B\}$, $A \cap B = \bigcap\{A, B\}$ şi $\{A\} \cup \{B\} = \{A, B\}$.)

c) **Complementara clasei** A este clasa

$$\complement A = \{x \mid x \notin A\},$$

unde $x \notin A$ este negaţia lui $x \in A$.

d) **Diferenţa claselor** A **şi** B este clasa

$$A \setminus B = \{x \mid (x \in A) \wedge (x \notin B)\} = A \cap \complement B.$$

e) Spunem că **clasa** A **este subclasă a clasei** B, dacă pentru orice $x \in A$ avem şi $x \in B$. Notaţie: $A \subseteq B$. Dacă A este mulţime şi $A \subseteq B$, atunci spunem că A este **submulţime** a clasei B.

f) **Clasa putere** a clasei A este clasa

$$\mathcal{P}(A) = \{x \mid x \subseteq A\}.$$

4. Axioma mulţimii putere. Pentru orice mulţime x există o mulţime y, care conţine exact subclasele mulţimii x.

Observaţii 3.2.4 1) Rezultă ca subclasele unei mulţimi sunt mulţimi, iar clasa putere a unei mulţimi este mulţime.

2) Paradoxul lui Russell este eliminat în această teorie. Mai exact, arătăm că **clasa Russell**

$$R = \{x \mid x \notin x\}$$

este clasă proprie, nu e mulţime. Evident, dacă $R \in R$, atunci R este mulţime şi $R \notin R$; invers, dacă presupunem că R este mulţime, atunci din $R \notin R$ rezultă că $R \in R$. Deci avem contradicţie în ambele cazuri, adică R nu e mulţime.

3) Universul U nu e mulţime, deoarece clasa Russell îi este subclasă.

4) Intersecţia şi diferenţa mulţimilor sunt mulţimi. Într-adevăr, fie A o clasă nevidă. Atunci $\cap A$ este mulţime, deoarece dacă $a \in A$, atunci evident $\cap A \subseteq a$; dar a este mulţime (deoarece $a \in A$), deci şi $\cap A$ este mulţime (fiind subclasă a unei mulţimi). În consecinţă, $A \cap B = \cap\{A, B\}$ şi $A \setminus B = A \cap \complement B$ sunt mulţimi.

5) Au loc egalităţile: $\cap\emptyset = U$; $\cup\emptyset = \emptyset$; $\cap U = \emptyset$; $\cup U = U$; $\mathcal{P}\emptyset = \{\emptyset\}$; $\mathcal{P}(U) = U$.

5. Axioma reuniunii. Dacă A este mulţime, atunci $\cup A$ este mulţime.

(În particular, dacă A şi B sunt mulţimi, atunci $A \cup B = \cup\{A, B\}$ este mulţime.)

6. Axioma regularităţii. Dacă X o clasă nevidă, atunci există $x \in X$ astfel încât $X \cap x = \emptyset$.

(Această axiomă elimină ,,anomalia" $a \in a$ pentru mulţimi. În consecinţă, clasa Russell R coincide cu universul U.)

Definiţia 3.2.5 Fie x o mulţime. Atunci mulţimea $x^+ = x \cup \{x\}$ se numeşte **succesorul** lui x.

7. Axioma infinitului. Există o mulţime y pentru care $\emptyset \in y$ şi pentru orice $x \in y$ avem $x^+ \in y$.

(În particular, clasa vidă $\emptyset$ este mulţime.)

Pe baza axiomei infinitului se introduce mulţimea $\mathbb{N}$ a numerelor naturale. Vom face această discuţie în Secţiunea 7.1.

Exerciţiul 26 Să se arate că mulţimile $\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \ldots$ sunt distincte două câte două. (Indicaţie: folosim inducţia matematică.)

Definiţia 3.2.6 a) Fie a şi b mulţimi. Atunci mulţimea $\{\{a\}, \{a, b\}\}$ se notează prin (a, b) şi se numeşte **pereche ordonată** cu **prima componentă** a şi **a doua componentă** b.

b) **Produsul cartezian** al claselor A şi B este clasa

$$A \times B = \{t \mid \exists x \exists y((x \in A) \wedge (y \in B) \wedge (t = (x, y)))\}.$$

Mai departe, $A \times B \times C = (A \times B) \times C, \ldots$

Exerciţiul 27 Dacă a, b, c, d sunt mulţimi, atunci $(a, b) = (c, d)$ dacă şi numai dacă $a = c$ şi $b = d$.

Observaţii 3.2.7 1) Dacă $P(x, y)$ este o formulă în care x şi y sunt variabile libere, atunci notăm

$$\{(x, y) \mid P(x, y)\} = \{t \mid \exists x \exists y(P(x, y) \wedge (t = (x, y)))\}.$$

Deci

$$A \times B = \{(x, y) \mid (x \in A) \wedge (y \in B)\}.$$

2) Dacă A şi B sunt mulţimi, atunci şi $A \times B$ este mulţime. Într-adevăr, dacă $a \in A$ şi $b \in B$, atunci $(a, b) \subseteq \mathcal{P}(A \cup B)$, deci $A \times B \subseteq \mathcal{P}(\mathcal{P}(A \cup B))$; dar $\mathcal{P}(\mathcal{P}(A \cup B))$ este mulţime, deci şi $A \times B$ este mulţime.

Capitolul 4

RELAŢII ŞI FUNCŢII

O relaţie binară sau corespondenţă între elementele mulţimilor A şi B este o mulţime de perechi din $A \times B$. Acest concept formalizează şi generalizează noţiuni precum *mai mare ca*, *egal cu*, *divide pe*, *aparţine lui*, *este inclus în*, *paralel cu*, *perpendicular pe*, *congruent cu*, *adiacent lui* etc. Conceptul de funcţie este caz particular al celui de relaţie.

4.1 Relaţii binare

Definiţia 4.1.1 Fie $n \in \mathbb{N}^*$ şi fie $A_1, A_2, \dots, A_n$ mulţimi.

a) Numim **relaţie n-ară** sistemul $\rho = (A_1, A_2, \dots, A_n, R)$, unde $R \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Dacă $n = 2$, atunci $\rho = (A_1, A_2, R)$ este **relaţie binară** (sau **corespondenţă**) între elementele mulţimilor A_1 şi A_2, unde $R \subseteq A_1 \times A_2$. În continuare ne ocupăm doar de relaţii binare, numite pe scurt relaţii. De multe ori identificăm relaţia cu graficul său.

b) Fie $\rho = (A, B, R), R \subseteq A \times B$ o relaţie. Mulţimea R se numeşte **graficul** lui ρ şi **notăm**:

$$(a, b) \in R \Leftrightarrow a\rho b,$$

citind: a este în relaţia ρ cu b. În caz contrar, $(a, b) \notin R \Leftrightarrow a \not\rho b$.

c) Spunem că ρ este **relaţie omogenă**, dacă $A = B$.

d) ρ **relaţie vidă**, dacă $R = \emptyset$; ρ este **relaţie universală**, dacă $R = A \times B$.

e) Pe mulţimea A definm **relaţia diagonală**

$$1_A = (A, A, \Delta_A), \quad \Delta_A = \{(a, a) \mid a \in A\}$$

(unde $a 1_A b \Leftrightarrow a = b$).

Exemplul 4.1.2 1) Fie $A = \{a, b, c, d\}$, $B = \{1, 2\}$ şi $\rho = (A, B, R)$, unde $R = \{(a, 1), (a, 2), (b, 2), (c, 1)\}$. Atunci $a\rho 1, a\rho 2$ şi $c \not\rho 2$.

2) Relaţia de asemănare pe mulţimea triunghiurilor din plan.

3) Relaţia de divizibilitate pe $\mathbb{Z}$ este următoarea relaţie omogenă: $\rho = (\mathbb{Z}, \mathbb{Z}, R)$, unde

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a|b\} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \exists c \in \mathbb{Z} : \ b = ac\}.$$

4) Dacă $A = \emptyset$ sau $B = \emptyset$, atunci există o unică relaţie $\rho = (A, B, R)$, şi anume relaţia vidă, cu graficul $R = \emptyset$.

4.1.1 Operaţii cu relaţii

Definiţia 4.1.3 a) Spunem că $\rho = (A, B, R)$ este **subrelaţie** relaţiei $\sigma = (A, B, S)$, notaţie $\rho \subseteq \sigma$, dacă $R \subseteq S$, adică, dacă pentru orice $(a, b) \in A \times B$ avem $a\rho b \Rightarrow a\sigma b$.

Considerăm relaţiile $\rho = (A, B, R), \rho' = (A, B, R'), \sigma = (C, D, S)$.

b) **Intersecţia relaţiilor** ρ şi ρ' este relaţia $\rho \cap \rho' = (A, B, R \cap R')$, deci $a(\rho \cap \rho')b \Leftrightarrow a\rho b \wedge a\rho' b$.

c) **Reuniunea relaţiilor** ρ şi ρ' este relaţia $\rho \cup \rho' = (A, B, R \cup R')$, deci $a(\rho \cup \rho')b \Leftrightarrow a\rho b \vee a\rho' b$.

d) **Complementara relaţiei** ρ este relaţia $\complement\rho = (A, B, \complement R)$, unde $\complement R$ se ia relativ la $A \times B$. Deci $a\complement\rho b \Leftrightarrow a \not\rho b$.

e) **Inversa relaţiei** ρ este relaţia $\rho^{-1} = (B, A, R^{-1})$ relaţie, unde

$$R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}.$$

Deci $b\rho^{-1}a \Leftrightarrow a\rho b$.

f) **Compunerea relaţiilor** ρ şi σ este relaţia $\sigma \circ \rho = (A, D, S \circ R)$, unde

$$S \circ R = \{(a, d) \in A \times D \mid \exists x \in B \cap C \mid (a, x) \in R,\ (x, d) \in S\},$$

adică $a(\sigma \circ \rho)b \Leftrightarrow \exists x \in B \cap C : a\rho x$ şi $x\rho d$. Notăm $\rho \circ \rho = \rho^2$.

Exemplul 4.1.4 1) Pe mulţimea $\mathbb{Z}$, relaţia de egalitate „=" este subrelaţie a relaţiei $\leq$. Relaţia de divizibilitate $|$ nu este subrelaţie a lui $\leq$, pentru că de exemplu $2|-6$ şi $2 \not\leq -6$.

2) Pe $\mathbb{R}$, intersecţia lui $\leq$ şi $\geq$ este relaţia de egalitate $=$; reuniunea relaţiilor „=" şi „<" este relaţia „≤—; complementara lui $<$ este $\geq$; inversa lui $<$ este relaţia $>$.

3) Compunerea relaţiilor nu e comutativă, adică în general $\sigma \circ \rho \neq \rho \circ \sigma$. Într-adevăr, fie relaţiile „<" respectiv „>" pe $\mathbb{N}$. Atunci $a(< \circ >)b \Leftrightarrow \exists c \in \mathbb{N} : a > c$ şi $c < b \Leftrightarrow a, b \in \mathbb{N}^* \times \mathbb{N}^*$, adică graficul lui $< \circ >$ este mulţimea $\mathbb{N}^* \times \mathbb{N}^*$; pe de altă parte $a(> \circ <)b \Leftrightarrow \exists c \in \mathbb{N} : a < c$ şi $c > b \Leftrightarrow a, b \in \mathbb{N} \times \mathbb{N}$, adică $> \circ <$ are graficul $\mathbb{N} \times \mathbb{N}$.

Teorema 4.1.5 *Fie* $\rho = (A, B, R)$, $\sigma = (C, D, S)$ *şi* $\tau = (E, F, T)$ *relaţii. Atunci:*

1) $(\tau \circ \sigma) \circ \rho = \tau \circ (\sigma \circ \rho)$ (compunerea relaţiilor este asociativă),

2) $\rho \circ 1_A = 1_B \circ \rho = \rho$ (relaţia de egalitate este element neutru faţă de compunere).

Demonstraţie. 1) Arătăm asociativitatea compunerii. Avem $\tau \circ \sigma = (C, F, T \circ S)$, $(\tau \circ \sigma) \circ \rho = (A, F, (T \circ S) \circ R)$, $\sigma \circ \rho = (A, D, S \circ R)$ şi $\tau \circ (\sigma \circ \rho) = (A, F, T \circ (S \circ R)$. Mai departe, pentru orice $(a, f) \in A \times F$ avem:

$$\begin{aligned}
(a, f) \in (T \circ S) \circ R &\Leftrightarrow a(\tau \circ \sigma) \circ \rho f \Leftrightarrow && \text{(notaţie)}\\
&\Leftrightarrow (\exists x)\ x \in B \cap C \text{ şi } (a\rho x \text{ şi } x(\tau \circ \sigma)f) \Leftrightarrow && \text{(Definiţia 4.1.3. f))}\\
&\Leftrightarrow (\exists x)\ x \in B \cap C \text{ şi } (a\rho x \text{ şi } (\exists y)\ y \in E \cap D \text{ şi } (x\sigma y \text{ şi } y\tau f)) \Leftrightarrow && \text{(Definiţia 4.1.3. f))}\\
&\Leftrightarrow (\exists x)\ (\exists y)\ x \in B \cap C \text{ şi } y \in E \cap D \text{ şi } (a\rho x \text{ şi } x\sigma y \text{ şi } y\tau f) \Leftrightarrow && \text{(tautologia 2.3.9 (8))}\\
&\Leftrightarrow (\exists y)\ y \in E \cap D \text{ şi } (\ (\exists x)\ x \in B \cap C \text{ şi } a\rho x \text{ şi } x\sigma y) \text{ şi } y\tau f \Leftrightarrow && \text{(tautologiile 2.3.9 (1), (8))}\\
&\Leftrightarrow (\exists y)\ y \in E \cap D \text{ şi } (a(\sigma \circ \rho)y \text{ şi } y\tau f) \Leftrightarrow && \text{(Definiţia 4.1.3. f))}\\
&\Leftrightarrow a\tau \circ (\sigma \circ \rho)f \Leftrightarrow && \text{(Definiţia 4.1.3. f))}\\
&\Leftrightarrow (a, f) \in T \circ (S \circ R) && \text{(notaţie).}
\end{aligned}$$

Am arătat astfel că $(T \circ S) \circ R = T \circ (S \circ R)$. ■

Exerciţiul 28 Fie mulţimile $A = \{1, 2\}$, $B = \{1, 2, 3\}$, $C = \{1, 2, 3, 4\}$, $R_1 = \{(1, 2), (1, 3), (2, 3)\} \subseteq A \times B$, $R_2 = \{(1, 4), (3, 1), (3, 4)\} \subseteq B \times C$, $\rho_1 = (A, B, R_1)$, $\rho_2 = (B, C, R_2)$. Să se determine relaţiile: $\rho_2 \circ \rho_1$, $\rho_1 \circ \rho_2$, ρ_1^{-1}, ρ_1^{-1}, $(\rho_1 \circ \rho_2)^{-1}$, $\rho_2^{-1} \circ \rho_1^{-1}$.

Exerciţiul 29 Fie $\rho = (\mathbb{N}, \mathbb{N}, <)$. Să se determine relaţiile $<^2$, $<^3$, $< \circ >$ şi $> \circ <$.

Exerciţiul 30 Fie $A = \{1, 2, 3, 4\}$ şi R, S, $S' \subseteq A \times A$, unde $R = \{(1, 2),\ (1, 4), (2, 3), (4, 1), (4, 3)\}$, $S = \{(1, 1), (2, 4), (3, 4)\}$, $S' = \{(1, 4), (4, 4)\}$.

Să se determine relaţiile $(S \cap S') \circ R$, $(S \circ R) \cap (S' \circ R)$, $R \circ (S \cap S')$ şi $(R \circ S) \cap (R \circ S')$.

Exerciţiul 31 Considerăm relaţiile $\rho = (A, B, R)$, $\rho' = (A, B, R')$, $\sigma = (C, D, S)$ şi $\sigma' = (C, D, S')$. Să se demonstreze (specificându-se tautologiile din lista 2.3.9 care au fost utilizate):

a) $(\rho^{-1})^{-1} = \rho$; $(\complement\rho)^{-1} = \complement\rho^{-1}$;

b) $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}$;

c) $(\rho \cap \rho')^{-1} = \rho^{-1} \cap \rho'^{-1}$; $(\rho \cup \rho')^{-1} = \rho^{-1} \cup \rho'^{-1}$;

d) $\sigma \circ (\rho \cup \rho') = (\sigma \circ \rho) \cup (\sigma \circ \rho')$; $(\sigma \cup \sigma') \circ \rho = (\sigma \circ \rho) \cup (\sigma' \circ \rho)$;

e) $\sigma \circ (\rho \cap \rho') \subseteq (\sigma \circ \rho) \cap (\sigma \circ \rho')$; $(\sigma \cap \sigma') \circ \rho \subseteq (\sigma \circ \rho) \cap (\sigma' \circ \rho)$;

f) dacă $\sigma \subseteq \sigma'$, $\rho \subseteq \rho'$ atunci $\sigma \circ \rho \subseteq \sigma' \circ \rho'$.

Definiţia 4.1.6 Fie $\rho = (A, B, R)$ o relaţie şi fie $X \subseteq A$. Mulţimea

$$\rho(X) = \{b \in B \mid \exists x \in X \mid x\rho b\} \subseteq B$$

se numeşte **secţiunea relaţiei** ρ **după submulţimea** X. Dacă submulţimea $X = \{x\}$ are un singur element, atunci notăm:

$$\rho\langle x\rangle = \rho(\{x\}) = \{b \in B \mid x\rho b\}.$$

Exemplul 4.1.7 În exemplul 4.1.4 1) avem $\rho(\{a, b\}) = \{1, 2\}$, $\rho(\{c, d\}) = \{1\}$, $\rho\langle a\rangle = \{1, 2\}$, $\rho\langle d\rangle = \emptyset$, $\rho(A) = \{1, 2\}$, $\rho^{-1}(B) = \{a, b, c\}$.

Teorema 4.1.8 *Fie* $\rho = (A, B, R)$ *şi* $\sigma = (C, D, S)$ *relaţii şi fie* $X \subseteq A$. *Atunci avem*

$$(\sigma \circ \rho)(X) = \sigma(\rho(X) \cap C);$$

dacă în plus $B = C$, *atunci* $(\sigma \circ \rho)(X) = \sigma(\rho(X))$.

Demonstraţie. Pentru orice $d \in D$ avem:

$$\begin{aligned}
d \in (\sigma \circ \rho)(X) &\Leftrightarrow (\exists x)\ x \in X \text{ şi } x(\sigma \circ \rho)d \Leftrightarrow && \text{(Definiţia 4.1.6)}\\
&\Leftrightarrow (\exists x)\ x \in X \text{ şi } ((\exists z)\ z \in B \cap C \text{ şi } x\rho z \text{ şi } z\sigma d) \Leftrightarrow && \text{(Definiţia 4.1.3. f))}\\
&\Leftrightarrow (\exists x)\ (\exists z)\ (x \in X \text{ şi } z \in B \cap C \text{ şi } x\rho z \text{ şi } z\sigma d \Leftrightarrow && \text{(tautologia 2.3.9 (8))}\\
&\Leftrightarrow (\exists z)\ z \in B \cap C \text{ şi } ((\exists x)\ x \in X \text{ şi } x\rho z) \text{ şi } z\sigma d \Leftrightarrow && \text{(tautologiile 2.3.9 (1), (8))}\\
&\Leftrightarrow (\exists z)\ z \in B \cap C \text{ şi } (z \in \rho(X) \text{ şi } z\sigma d) \Leftrightarrow && \text{(Definiţia 4.1.6)}\\
&\Leftrightarrow (\exists z)\ z \in \rho(X) \cap C \text{ şi } z\sigma y \Leftrightarrow && \text{(deoarece } \rho(X) \subseteq B \text{)}\\
&\Leftrightarrow d \in \sigma(\rho(X) \cap C)), && \text{(Definiţia 4.1.6)}
\end{aligned}$$

deci afirmaţia e demonstrată. ■

Exerciţiul 32 Fie mulţimile $A = \{a_1, a_2, a_3, a_4\}$, $B = \{b_1, b_2, b_3, b_4, b_5\}$, $X = \{a_2, a_4\}$, $Y = \{b_1, b_2, b_4, b_5\}$ şi considerăm relaţia $R = \{(a_1, b_2), (a_3, b_5), (a_1, b_3), (a_2, b_4)\} \subseteq A \times B$. Să se determine mulţimile $R(X)$, $R\langle a_2\rangle$, $R^{-1}(Y)$, $R^{-1}\langle b_5\rangle$, $R^{-1}(B)$ şi $R(A)$.

Exerciţiul 33 Fie $\delta = (\mathbb{N}, \mathbb{N}, |)$ relaţia de divizibilitate. Să se determine mulţimile $\delta\langle 1\rangle$, $\delta^{-1}(\{4, 9\})$, $\delta^{-1}(\mathbb{N})$ şi $\delta(\mathbb{N})$.

Exerciţiul 34 Fie $\rho = (A, B, R)$ şi $\rho' = (A, B, R')$ relaţii. Să se arate că următoarele afirmaţii sunt echivalente:
(i) $\rho \subseteq \rho'$;
(ii) $(\forall\, x \in A)\ \rho\langle x\rangle \subseteq \rho'\langle x\rangle$;
(iii) $(\forall\, X \subseteq A)\ \rho(X) \subseteq \rho'(X)$.

Exerciţiul 35 Fie $\rho = (A, B, R)$ şi $\rho' = (A, B, R')$ relaţii şi fie $X, X' \subseteq A$. Să se demonstreze (specificându-se tautologiile din lista 2.3.9 care au fost utilizate):
a) dacă $X \subseteq X'$ şi $\rho \subseteq \rho'$, atunci $\rho(X) \subseteq \rho'(X')$;
b) $\rho(X \cup X') = \rho(X) \cup \rho(X')$; $(\rho \cup \rho')(X) = \rho(X) \cup \rho'(X)$;
c) $\rho(X \cap X') \subseteq \rho(X) \cap \rho(X')$; $(\rho \cap \rho')(X) \subseteq \rho(X) \cap \rho'(X)$;

Observaţii 4.1.9 În c) egalitatea nu are loc în general. Fie de exemplu $\rho = (A, A, R)$, unde $A = \{1, 2, 3\}, R = \{(1, 1), (1, 3), (2, 2), (3, 1)(3, 3)\}$ şi fie $X = \{1, 2\}, X' = \{2, 3\}$. Atunci $\rho(X) \cap \rho(X') = \{1, 2, 3\}$ şi $\rho(X \cap X') = \rho\langle 2\rangle = \{2\}$.

Exerciţiul 36 Fie $\rho = (A, B, R)$ o relaţie. Să se arate că următoarele afirmaţii sunt echivalente:
(i) $\forall\, x \in A,\ R\langle x\rangle \neq \emptyset$;
(ii) $\Delta_A \subseteq R^{-1} \circ R$;
(iii) $R^{-1}(B) = A$;
(iv) $\forall\, A'$ mulţime, $\forall\, P_1, P_2 \subseteq A' \times A$, dacă $(R \circ P_1) \cap (R \circ P_2) = \emptyset$, atunci $P_1 \cap P_2 = \emptyset$;
(v) $\forall\, A'$ mulţime, $\forall\, P \subseteq A' \times A$ avem $R \circ P = \emptyset \Rightarrow P = \emptyset$;
(vi) $\forall\, X_1, X_2 \subseteq A,\ R(X_1) \cap R(X_2) = \emptyset \Rightarrow X_1 \cap X_2 = \emptyset$;
(vii) $\forall\, X \subseteq A$ avem $R(X) = \emptyset \Rightarrow X = \emptyset$.

Exerciţiul 37 Fie $\rho = (A, B, R)$ o relaţie. Să se arate că următoarele afirmaţii sunt echivalente:
(i) Pentru orice $x \in A$, $|R\langle x\rangle| \leq 1$;
(ii) $R \circ R^{-1} \subseteq \Delta_B$;
(iii) Pentru orice mulţime B' şi pentru orice relaţii $S_1, S_2 \subseteq B \times B'$ avem $(S_1 \cap S_2) \circ R = (S_1 \circ R) \cap (S_2 \circ R)$;
(iv) Pentru orice mulţime B' şi pentru orice relaţii $S_1, S_2 \subseteq B \times B'$ avem $S_1 \cap S_2 = \emptyset \Rightarrow (S_1 \circ R) \cap (S_2 \circ R) = \emptyset$;
(v) Pentru orice mulţime B' şi pentru orice $S \subseteq B \times B'$ avem $(S \circ R) \cap (\complement S \circ R) = \emptyset$;
(vi) Pentru orice $Y_1, Y_2 \subseteq B$ avem $Y_1 \cap Y_2 = \emptyset \Rightarrow R^{-1}(Y_1) \cap R^{-1}(Y_2) = \emptyset$;
(vii) Pentru orice $Y \subseteq B$ avem $R^{-1}(Y) \cap R^{-1}(\complement Y) = \emptyset$;
(viii) Pentru orice $Y \subseteq B$ avem $R^{-1}(B) \setminus R^{-1}(Y) = R^{-1}(\complement Y)$.

Exerciţiul 38 Fie $S \subseteq B \times C$. Următoarele afirmaţii sunt echivalente:
(i) $\forall\, Y_1, Y_2 \subseteq B,\ Y_1 \neq Y_2 \Rightarrow S(Y_1) \neq S(Y_2)$;
(ii) $\forall\, A$ mulţime, $\forall\, R_1, R_2 \subseteq A \times B$, $S \circ R_1 = S \circ R_2 \Rightarrow R_1 = R_2$.

Exerciţiul 39 Fie $R \subseteq A \times B$. Următoarele afirmaţii sunt echivalente:
(i) $\forall\, Y_1, Y_2 \subseteq B,\ Y_1 \neq Y_2 \Rightarrow R^{-1}(Y_1) \neq R^{-1}(Y_2)$;
(ii) $\forall$ C mulţime, $\forall\, S_1, S_2 \subseteq B \times C$, $S_1 \circ R = S_2 \circ R \Rightarrow S_1 = S_2$.

Exerciţiul 40 (Matricea booleană (de adiacenţă) a unei relaţii binare) Fie $\mathbb{B} = \{0, 1\}$. Definim următoarele operaţii cu matrice booleene:

- dacă $A, A' \in M_{m,n}(\mathbb{B})$, atunci $\neg A = (\neg a_{ij})$, $A \wedge A' = (a_{ij} \wedge a'_{ij})$ şi $A \vee A' = (a_{ij} \vee a'_{ij})$;
- dacă $A = (a_{ij}) \in M_{m,n}(\mathbb{B})$ şi $B = (b_{ij}) \in M_{n,p}(\mathbb{B})$, atunci $A \circ B = (c_{lj}) \in M_{m,p}(\mathbb{B})$, unde prin definiţie, $c_{ij} = \bigvee_{k=1}^{n} b_{ik} \wedge a_{kj}$.

Fie relaţia $\rho = (A, B, R)$, unde $A = \{a_1, \ldots, a_m\}$, $B = \{b_1, \ldots, b_n\}$. Asociem relaţiei ρ matricea $M_\rho \in M_{m,n}(\mathbb{B})$ care are pe 1 pe poziţia (i, j) dacă şi numai dacă $(a_i, b_j) \in R$.

Fie $\rho = (A, B, R)$, $\rho' = (A, B, R')$ şi $\sigma = (B, C, S)$, unde A, B, C sunt mulţimi finite. Să se demonstreze:
a) $M_{\rho\cup\rho'} = M_\rho \vee M_{\rho'}$, $M_{\rho\cap\rho'} = M_\rho \wedge M_{\rho'}$, $M_{\complement\rho} = \neg M_\rho$;
b) $M_{\rho^{-1}} = M_\rho^t$, $M_{\sigma\circ\rho} = M_\sigma \circ M_\rho$.

4.2 Funcţii

Definiţia 4.2.1 a) Relaţia $f = (A, B, F)$, unde $F \subseteq A \times B$, se numeşte **funcţie (relaţie funcţională)**, dacă pentru orice $a \in A$, secţiunea $f\langle a\rangle$ are exact un element.

b) Dacă $f = (A, B, F)$ este o funcţie, atunci A se numeşte **domeniul de definiţie** al lui f, notaţie $A = \operatorname{dom} f$.

c) Mulţimea B este **codomeniul** lui f, notaţie $B = \operatorname{codom} f$, iar secţiunea $f(A)$ este **domeniul valorilor** sau **imaginea** lui f, notaţie $f(A) = \operatorname{Im} f$.

d) Mulţimea $F \subseteq A \times B$ este **graficul** funcţiei f.

Dacă $f = (A, B, F)$ este funcţie, atunci folosim următoarea notaţie:

$$f : A \to B, \quad A \xrightarrow{f} B.$$

Dacă $a \in A$, atunci elementul $b \in B$ determinat de egalitatea $f\langle a\rangle = \{b\}$ se notează $b = f(a)$ sau $a \mapsto b = f(a)$.

Observaţii 4.2.2 a) Funcţiile $f : A \to B$ şi $f' : A' \to B'$ sunt egale $(f = f')$ dacă şi numai dacă, $A = A', B = B'$ şi $f(a) = f(a')$ pentru orice $a \in A$.

b) Dacă $A = \emptyset$, atunci unica relaţie $\rho = (A, B, R)$ este relaţia vidă $(R = \emptyset)$; aceasta este funcţie pentru orice mulţime B.

Dacă $A \neq \emptyset$ şi $B = \emptyset$, atunci relaţia vidă $\rho = (A, \emptyset, \emptyset)$ nu e funcţie.

c) Dacă $f : A \to B$ este o funcţie şi $X \subseteq A, Y \subseteq B, y \in Y$, atunci

$$f(X) = \{b \in B \mid \exists x \in X : f(x) = b\} = \{f(x) \mid x \in X\},$$
$$f^{-1}(Y) = \{a \in A \mid \exists y \in Y : af^{-1}y\} = \{a \in A \mid \exists y \in Y : f(a) = y\} = \{a \in A \mid f(a) \in Y\}$$

şi

$$f^{-1}\langle y\rangle = f^{-1}(y) = \{a \in A \mid f(a) = y\},$$

iar graficul este $F = \{(a, f(a)) \mid a \in A\}$.

Exemplul 4.2.3 1) În exemplul 4.1.1.1), relaţia ρ nu e funcţie, pentru că de exemplu $\rho\langle a\rangle = \{1, 2\}$. Relaţia $\rho' = (A, B, R')$, $A = \{a, b, c, d\}$, $B = \{1, 2\}$, $R' = \{(a, 1), (b, 1), (c, 2), (d, 2)\}$ este funcţie.

Teorema 4.2.4 *1) Fie* $f = (A, B, F)$ *şi* $g = (C, D, G)$ *funcţii.*

Relaţia compusă $g \circ f = (A, D, G \circ F)$ *este funcţie dacă şi numai dacă* $f(A) \subseteq C$, *adică* $\operatorname{Im} f \subseteq \operatorname{Dom} g$, *şi atunci* $(g \circ f)(a) = g(f(a))$ *pentru orice* $a \in A$.

2) Dacă $f : A \to B, g : B \to C, h : C \to D$ *sunt funcţii, atunci* $f \circ 1_A = 1_B \circ f = f$ *şi* $(h \circ g) \circ f = h \circ (g \circ f)$.

Demonstraţie. 1) „$\Rightarrow$” Presupunem că $g \circ f$ este funcţie şi fie $b \in f(A)$. Arătăm că $b \in C$, adică $f(A) \subseteq C$. Într-adevăr, deoarece $b \in f(A)$, există $a \in A$ astfel încât $b = f(a)$. Fie $d = (g \circ f)(a)$ (unde $g \circ f$ este funcţie), adică $a(g \circ f)d$, de unde rezultă că există $c \in B \cap C$ astfel încât afc şi cgd. De aici afc şi afb, deoarece f este funcţie, deci $b = c \in B \cap C$.

„$\Leftarrow$” Presupunem acum că $f(A) \subseteq C$, şi fie $a \in A$. Deoarece f este funcţie, există $b \in f(A)$ astfel ca $f(a) = b$ (adică afb). Aici $b \in f(A) \subseteq C$, şi deoarece g este funcţie, există $d \in D$ astfel ca $g(b) = d$ (adică $b\, g\, d$). De aici $a\,(g \circ f)\, d$ şi $(g \circ f)\langle a\rangle = \{d\}$, adică $g \circ f$ este funcţie şi $(g \circ f)(a) = d = g(b) = g(f(a))$.

Avem

$$(g\circ f)\langle a\rangle = g(f\langle a\rangle) = g(f(a)) = g\langle f(a)\rangle = \{g(f(a)),\}$$

deci $g\circ f$ este funcţie şi $(g\circ f)(a) = g(f(a))$.

2) Rezultă din proprietatea referitoare la relaţii, sau poate fi uşor demonstrată direct. ■

Exerciţiul 41 Fie $\rho = (A, B, R)$ o relaţie. Să se arate că ρ este funcţie dacă şi numai dacă

$$1_A \subseteq \rho^{-1}\circ\rho \quad \text{şi} \quad \rho\circ\rho^{-1} \subseteq 1_B.$$

Exerciţiul 42 Fie $f : A \to B$ o funcţie. Să se arate că:
a) Pentru orice $X \subseteq A$ avem $X \subseteq f^{-1}(f(X))$;
b) Pentru orice $Y \subseteq B$ avem $Y \supseteq f(f^{-1}(Y))$;
c) $f\circ f^{-1}\circ f = f$.

4.2.1 Diagrame comutative

Considerăm funcţiile $f : A \to B$, $g : B \to C$ şi $h : A \to C$, reprezentate prin următoarea diagramă:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "g"'] & B \\ C \arrow[ur, "h"'] & \end{tikzcd}$$

Spunem că aceasta este o **diagramă comutativă** dacă $f = h\circ g$. Avem şi alte situaţii, de exemplu:

$$\begin{tikzcd} A \arrow[r, "k"] \arrow[d, "f"'] & D \arrow[d, "h"] \\ B \arrow[r, "g"] & C \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "k"] \arrow[d, "f"'] & D \\ B \arrow[r, "g"] & C \arrow[u, "h"'] \end{tikzcd}$$

Acestea sunt **diagrame comutative** dacă $h\circ k = g\circ f$, respectiv $h\circ g\circ f = k$.

4.2.2 Familie de elemente şi familie de mulţimi

Definiţia 4.2.5 a) Fie $f : I \to A$ o funcţie, şi fie $F = \{(i, f(i)) \mid i \in I\}$ graficul lui f. Identificăm de multe ori funcţia f cu F şi notăm $(a_i)_{i\in I}$, unde $a_i = f(i)$; spunem că $(a_i)_{i\in I}$ este o **familie de elemente**, iar I este **mulţimea de indici**.

Analog, dacă $f : I \to \mathcal{P}(U)$ o funcţie, atunci spunem că $(A_i)_{i\in I}$ **familie de mulţimi**, unde $A_i = f(i) \subseteq U$.

b) **Reuniunea familiei de mulţimi** $(A_i)_{i\in I}$ este mulţimea

$$\bigcup\nolimits_{i\in I} A_i = \{a \in U \mid \exists i \in I : a \in A_i\}.$$

c) **Intersecţia familie de mulţimi** $(A_i)_{i\in I}$ este mulţimea

$$\bigcap\nolimits_{i\in I} A_i = \{a \in U \mid \forall i \in I : a \in A_i\}.$$

Observăm că dacă $I = \emptyset$, atunci $\bigcup_{i\in I} A_i = \emptyset$, pentru că atunci pentru niciun $a \in A$ nu e adevărat că $\exists i \in I : a \in A_i$, şi $\bigcap_{i\in I} A_i = A$, pentru că afirmaţia $\exists i \in I : a \notin A_i$ este falsă pentru orice $a \in A$, deci negaţia ei $\forall i \in I : a \in A_i$ este adevărată pentru orice $a \in A$.

Exerciţiul 43 Să se demonstreze următoarele identităţi (specificându-se tautologiile din lista 2.3.9 care au fost utilizate), unde $A_{ij}, A_i, B_j, A \in \mathcal{P}(U)$ pentru orice $i \in I$, $j \in J$:
a) $\bigcup_{i\in I}\bigcup_{j\in J} A_{ij} = \bigcup_{j\in J}\bigcup_{i\in I} A_{ij}$;
b) $\bigcap_{i\in I}\bigcap_{j\in J} A_{ij} = \bigcap_{j\in J}\bigcap_{i\in I} A_{ij}$;
c) $\complement(\bigcup_{i\in I} A_i) = \bigcap_{i\in I} \complement(A_i)$;
d) $\complement(\bigcap_{i\in I} A_i) = \bigcup_{i\in I} \complement(A_i)$;
e) $(\bigcup_{i\in I} A_i) \cup (\bigcup_{i\in I} B_i) = \bigcup_{i\in I}(A_i \cup B_i)$;
f) $\bigcup_{j\in J}(A \cap B_j) = A \cap (\bigcup_{j\in J} B_j)$;
g) $\bigcap_{j\in J}(A \cup B_j) = A \cup (\bigcap_{j\in J} B_j)$;
h) $\bigcup_{i\in I}(\bigcap_{j\in J} A_{ij}) \subseteq \bigcap_{j\in J}(\bigcup_{i\in I} A_{ij})$;
i) $(\bigcup_{i\in I} A_i) \cap (\bigcup_{j\in J} B_j) = \bigcup_{(i,j)\in I\times J}(A_i \cap B_j)$;
j) $(\bigcap_{i\in I} A_i) \cup (\bigcap_{j\in J} B_j) = \bigcap_{(i,j)\in I\times J}(A_i \cup B_j)$.

Exerciţiul 44 Să se arate că (specificându-se tautologiile din lista 2.3.9 care au fost utilizate):
a) $(\bigcap_{i\in I} X_i) \times (\bigcap_{i\in I} Y_i) = \bigcap_{i\in I}(X_i \times Y_i)$;
b) $(\bigcup_{i\in I} X_i) \times (\bigcup_{j\in J} Y_j) = \bigcup_{(i,j)\in I\times J}(X_i \times Y_j)$.

Exerciţiul 45 Fie $A_n \in \mathcal{P}(U)$, $n \in \mathbb{N}$. Să se demonstreze $\bigcup_{n\in\mathbb{N}} A_n = \bigcup_{n\in\mathbb{N}} B_n$ şi $B_m \cap B_n = \emptyset$, dacă $m \neq n$, unde $B_0 = A_0$, $B_n = A_n \setminus (\bigcup_{i=0}^{n-1} A_i)$.

Exerciţiul 46 Fie $f : A \to B$ o funcţie şi $X_i \subseteq A$, $Y_i \subseteq B$ $\forall\ i \in I$. Să se arate că(specificându-se tautologiile din lista 2.3.9 care au fost utilizate):
a) $f(\bigcup_{i\in I} X_i) = \bigcup_{i\in I} f(X_i)$;
b) $f(\bigcap_{i\in I} X_i) \subseteq \bigcap_{i\in I} f(X_i)$. Să se dea un exemplu în care incluziunea este strictă;
c) $f^{-1}(\bigcup_{i\in I} Y_i) = \bigcup_{i\in I} f^{-1}(Y_i)$;
d) $f^{-1}(\bigcap_{i\in I} Y_i) = \bigcap_{i\in I} f^{-1}(Y_i)$.

Exerciţiul 47 Să se arate că $\mathcal{P}(\bigcap_{i\in I} A_i) = \bigcap_{i\in I} \mathcal{P}(A_i)$.

Exerciţiul 48 Fie relaţiile $\rho_i = (A, B, R_i)$, $i \in I$ şi $\sigma = (C, D, S)$. Să se arate că (specificându-se tautologiile din lista 2.3.9 care au fost utilizate):
a) $\sigma \circ (\bigcup_{i\in I} \rho_i) = \bigcup_{i\in I}(\sigma \circ \rho_i)$;
b) $(\bigcup_{i\in I} \rho_i) \circ \sigma = \bigcup_{i\in I}(\rho_i \circ \sigma)$;
c) $\sigma \circ (\bigcap_{i\in I} \rho_i) \subseteq \bigcap_{i\in I}(\sigma \circ \rho_i)$;
d) $(\bigcap_{i\in I} \rho_i) \circ \sigma \subseteq \bigcap_{i\in I}(\rho_i \circ \sigma)$.

4.3 Funcţii injective, surjective şi bijective

Definiţia 4.3.1 Fie $f : A \to B$ o funcţie. Spunem că
a) f este **injectivă**, dacă $\forall x_1, x_2 \in A, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, sau echivalent, $\forall x_1, x_2 \in A, f(x_1) = f(x_2) \Rightarrow x_1 = x_2$;
b) f este **surjectivă**, dacă $\forall y \in B\ \exists x \in A : f(x) = y$, sau echivalent, $f(A) = B$;
c) f este **bijectivă**, dacă este injectivă şi surjectivă, sau echivalent, dacă $\forall y \in B$ există unic $x \in A$ astfel ca $f(x) = y$.

Exemplul 4.3.2 1) Funcţia $f : \mathbb{R} \to \mathbb{R}$, $\quad f(x) = x^2$ nu e injectivă, pentru că de exemplu $-1 \neq 1$ şi $f(-1) = f(1) = 1$; nu e nici surjectivă, pentru că de exemplu $y = -1 \in \mathbb{R}$, dar nu există $x \in \mathbb{R}$ astfel încât $f(x) = x^2 = -1$.
Funcţia $g : [0, \infty) \to \mathbb{R}$, $g(x) = x^2$ este injectivă şi nu e surjectivă, funcţia $h : [0, \infty) \to [0, \infty)$, $\quad h(x) = x^2$ este injectivă şi surjectivă, deci bijectivă.
2) Pentru orice mulţime A, relaţia diagonală $1_A = (A, A, \Delta_A)$ este funcţie bijectivă.
3) Proiecţia canonică $p_j : \prod_{i\in I} A_i \to A_j$ este surjectivă, şi injecţia canonică $p_j : A_j \to \coprod_{i\in I} A_i$ este funcţie injectivă.

Teorema 4.3.3 (caracterizarea funcţiilor injective) *Fie* $f : A \to B$ *o funcţie. Următoarele afirmaţii sunt echivalente:*
(i) f *este injectivă*
(ii) *pentru orice mulţime* A' *şi pentru orice funcţii* $\alpha, \beta : A' \to A$*, dacă* $f \circ \alpha = f \circ \beta$*, atunci* $\alpha = \beta$ *(adică cu* f *se poate simplifica la stânga);*
(iii) (*presupunem că* $A \neq \emptyset$) f *are inversă la stânga (retractă), adică există o funcţie* $r : B \to A$ *astfel încât* $r \circ f = 1_A$.

Demonstraţie. (i) $\Rightarrow$ (ii) Dacă $f \circ \alpha = f \circ \beta$, atunci pentru orice $a \in A'$ avem $f(\alpha(a)) = f(\beta(a))$; din injectivitatea lui f rezultă $\alpha(a) = \beta(a)$, deci $\alpha = \beta$.
(ii) $\Rightarrow$ (i) Presupunem că afirmaţia (ii) este adevărată şi că f nu e injectiv, adică există $x_1, x_2 \in A, x_1 \neq x_2$ astfel încât $f(x_1) = f(x_2)$.
Fie $A' = \{x_1, x_2\}$ şi $\alpha, \beta : A' \to A, \alpha(x_1) = x_1, \alpha(x_2) = x_2, \beta(x_1) = x_1, \beta(x_2) = x_1$. Atunci $\alpha \neq \beta$, dar $f \circ \alpha = f \circ \beta$, pentru că

$$(f \circ \alpha)(x_1) = f(\alpha(x_1)) = f(x_1) = f(\beta(x_1)) = (f \circ \beta)(x_1),$$
$$(f \circ \alpha)(x_2) = f(\alpha(x_2)) = f(x_2) = f(x_1) = f(\beta(x_2)) = (f \circ \beta)(x_2),$$

deci avem o contradicţie.
(i) $\Rightarrow$ (iii) Presupunem că f injectiv şi $a_0 \in A$. Considerăm funcţia

$$r : B \to A, \qquad r(b) = \begin{cases} a, & \text{dacă } b = f(a) \in f(A) \\ a_0, & \text{dacă } b \in B \setminus f(A) \end{cases},$$

care este bine definită, deoarece din injectivitatea lui f, pentru orice $b \in f(A)$, există unic a pentru care $f(a) = b$. Deci $(r \circ f)(a) = r(f(a)) = r(b) = a = 1_A(a)$ pentru orice $a \in A$, adică $r \circ f = 1_A$.

(iii) $\Rightarrow$ (i) Dacă există o funcţie $r : B \to A$ astfel încât $r \circ f = 1_A$ şi dacă $f(x_1) = f(x_2)$, atunci $r(f(x_1)) = r(f(x_2))$, de unde $x_1 = x_2$.

Teorema 4.3.4 (caracterizarea funcţiilor surjective) *Fie* $f : A \to B$ *o funcţie. Următoarele afirmaţii sunt echivalente:*

(i) f *este surjectivă;*

(ii) *pentru orice mulţime* B' *şi pentru orice funcţii* $\alpha, \beta : B \to B'$ *dacă* $\alpha \circ f = \beta \circ f$, *atunci* $\alpha = \beta$ *(adică cu* f *se poate simplifica la dreapta);*

(iii) f *are inversă la dreapta (secţiune), adică există o funcţie* $s : B \to A$ *pentru care* $f \circ s = 1_B$.

Demonstraţie. (i) $\Rightarrow$ (ii) Presupunem că $\alpha \circ f = \beta \circ f$, adică $\alpha(f(a)) = \beta(f(a))$ pentru orice $a \in A$. Din surjectivitatea lui f avem că pentru orice $b \in B$, există $a \in A$ astfel încât $b = f(a)$; astfel $\alpha(b) = \beta(b)$, adică $\alpha = \beta$.

(ii) $\Rightarrow$ (i) Presupunem că afirmaţia (ii) este adevărată şi că f nu e surjectiv, adică există $b_0 \in B \setminus f(A)$. Fie $A \neq \emptyset, B' = B$ şi considerăm funcţiile α, $\beta : B \to B$, unde $\alpha = 1_B$ şi

$$\beta(b) = \begin{cases} b, & \text{dacă } b \neq b_0, \\ b_0', & \text{dacă } b = b_0, \end{cases}$$

unde $b_0' \in f(A)$. Atunci $\alpha \neq \beta$, pentru că $\beta(b_0) = b_0' \neq b_0$ $(b_0 \notin f(A), b_0 \in f(A))$, dar $\alpha \circ f = \beta \circ f$, deoarece $(\alpha \circ f)(a) = \alpha(f(a)) = f(a) = \beta(f(a)) = (\beta \circ f)(a)$ pentru orice $a \in A$, ceea ce este o contradicţie.

Dacă $A = \emptyset$, atunci fie $B' = \{0, 1\}$, $\alpha, \beta : B \to B'$, $\alpha(b) = 0$, $\beta(b) = 1$ pentru orice $b \in B$. Atunci $\alpha \neq \beta$ şi $\alpha \circ f = \beta \circ f = \emptyset$.

(i) $\Rightarrow$ (iii) Presupunem că funcţia f este surjectivă. Atunci pentru orice $b \in B$, $f^{-1}(b) = \{a \in A \mid f(a) = b\} \neq \emptyset$. Pentru orice b alegem un element $a \in f^{-1}(b)$; astfel obţinem o funcţie $s : B \to A$, $s(b) = a$, şi avem

$$(f \circ s)(b) = f(s(b)) = f(a) = b = 1_B(b),$$

adică $f \circ s = 1_B$.

(iii) $\Rightarrow$ (i) Fie $s : B \to A$ o funcţie pentru care $f \circ s = 1_B$. Atunci pentru orice $b \in B$, $b = 1_B(b) = f(s(b))$, astfel că notând $a = s(b) \in A$, avem $f(a) = b$; deci f este surjectiv.

Teorema 4.3.5 (caracterizarea funcţiilor bijective) *Fie* $f : A \to B$ *o funcţie. Următoarele afirmaţii sunt echivalente:*

(i) f *este funcţie bijectivă;*

(ii) *relaţia inversă* f^{-1} *este funcţie şi avem* $f^{-1} \circ f = 1_A$, $f \circ f^{-1} = 1_B$*;*

(iii) f *are inversă, adică există o funcţie* $g : B \to A$, *astfel ca*

$$g \circ f = 1_A, \qquad f \circ g = 1_B.$$

Demonstraţie. (i) $\Leftrightarrow$ (ii) f este bijectiv $\Leftrightarrow$ pentru orice $b \in B$, mulţimea $f^{-1}(b) = \{a \in A \mid f(a) = b\}$ are exact un element $\Leftrightarrow$ f^{-1} este funcţie şi $a(f^{-1} \circ f)a' \Leftrightarrow \exists b \in B : afb$ şi $bf^{-1}a' \Leftrightarrow \exists b \in B : f(a) = b$ şi $f(a') = b \Leftrightarrow a = a'$ (pentru că f este funcţie injectivă) $\Leftrightarrow a 1_A a'$, adică $f^{-1} \circ f = 1_A$.

Mai departe, $b(f \circ f^{-1})b' \Leftrightarrow \exists a \in A : bf^{-1}a$ şi $afb' \Leftrightarrow \exists a \in A : f(a) = b$ şi $f(a) = b' \Leftrightarrow b = b'$ (pentru că f este surjectiv) $\Leftrightarrow b 1_B b'$, adică $f \circ f^{-1} = 1_B$.

(i) $\Rightarrow$ (iii) Dacă f este bijectiv, atunci fie $g = f^{-1}$, despre care tocmai am arătat că satisface condiţia (iii).

(iii) $\Rightarrow$ (i) Rezultă din implicaţiile (iii) $\Rightarrow$ (i) ale teoremelor de mai sus.

Observaţii 4.3.6 Dacă f este funcţie bijectivă, atunci şi funcţia f^{-1} este bijectivă, deorece $(f^{-1})^{-1} = f$.

Exerciţiul 49 Fie $f : A \to B$ şi $g : B \to C$ două funcţii. Să se arate că:

a) Dacă f şi g este injectiv (surjectiv), atunci $g \circ f$ este injectiv (surjectiv);

b) Dacă $g \circ f$ este injectiv (surjectiv), atunci f este injectiv (g este surjectiv);

c) Dacă $g \circ f$ este injectiv şi f este surjectiv, atunci g este injectiv;

d) Dacă $g \circ f$ este surjectiv şi g este injectiv, atunci f este surjectiv.

Exerciţiul 50 Fie $f : A \to B$ o funcţie, $X_1, X_2 \subseteq A$, $(X_i)_{i \in I}, X_i \subseteq A$, şi $Y_1, Y_2 \subseteq B$. Să se arate că:

a) $f^{-1}(Y_1 \setminus Y_2) = f^{-1}(Y_1) \setminus f^{-1}(Y_2)$;

b) dacă f este injectiv, atunci

(1) $f(X_1 \setminus X_2) = f(X_1) \setminus f(X_2)$,

(2) $f(\bigcap_{i \in I} X_i) = \bigcap_{i \in I} f(X_i)$.

Exerciţiul 51 Fie $f : A \to B$ o funcţie.

a) Să se arate că următoarele afirmaţii sunt echivalente:

(i) f este injectiv;

(ii) $f^{-1} \circ f = 1_A$;

(iii) $\forall\, X \subseteq A\;\; f^{-1}(f(X)) = X$;

(iv) $\forall\, X \subseteq A\;\; f(\complement(X)) \subseteq \complement f(X)$;

(v) $\forall\, X_1, X_2 \subseteq A\;\; f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$.

b) Să se arate că următoarele afirmaţii sunt echivalente:

(i) f este surjectiv;

(ii) $f \circ f^{-1} = 1_B$;

(iii) $\forall\, Y \subseteq B\;\; f(f^{-1}(Y)) = Y$;

(iv) $\forall\, X \subseteq A\;\; \complement f(X) \subseteq f(\complement(X))$.

Exerciţiul 52 Fie $f : A \to B$ o funcţie.

a) Presupunem că f este surjectiv. Să se arate că f este injectiv $\Leftrightarrow$ f are exact o inversă la drepta.

b) Presupunem că $A \neq \emptyset$ şi că f este injectiv. Dacă f este surjectiv, atunci să se arate că f are exact o inversă la stânga; afirmaţia inversă nu e adevărată.

Exerciţiul 53 Fie $A \neq \emptyset$ şi $f : A \to B$ o funcţie. Să se demonstreze că există $g : B \to A$ astfel încât $f \circ g \circ f = f$.

4.3.1 Produsul direct al unei familii de mulţimi şi al unei familii de funcţii

Fie $(A_i)_{i\in I}$ o familie de mulţimi. Prin definiţie,

$$\begin{aligned}\prod_{i\in I} A_i &= \{f : I \to \bigcup_{i\in I} A_i \mid \;\forall\, i \in I :\; f(i) \in A_i\} = \\ &= \{(a_i)_{i\in I} \mid \;\forall\, i \in I :\; a_i \in A_i\}\end{aligned}$$

este **produsul cartezian generalizat** al familiei $(A_i)_{i\in I}$. Funcţia

$$p_j : \prod_{i\in I} A_i \to A_j, \quad p_j((a_i)_{i\in I}) = a_j$$

se numeşte **proiecţia canonică**, şi perechea $(\prod_{i\in I} A_i, (p_i)_{i\in I})$ este **produsul direct** al familiei $(A_i)_{i\in I}$.

Mai departe, dacă $(f_i : A_i \to A_i')_{i\in I}$ este o familie de funcţii, atunci

$$\prod_{i\in I} f_i : \prod_{i\in I} A_i \to \prod_{i\in I} A_i', \quad (\prod_{i\in I} f_i)((a_i)_{i\in I}) = (f_i(a_i))_{i\in I}$$

produsul direct al familiei $(f_i)_{i\in I}$.

Observăm că $\prod_{i\in I} A_i$ este nevidă dacă şi numai dacă $I \neq \emptyset$ şi $A_i \neq \emptyset$ pentru orice $i \in I$. Dacă $I = \{1\}$, atunci $\prod_{i\in I} A_i = A_1$; dacă $I = \{1, 2\}$, atunci $\prod_{i\in I} A_i$ se identifică cu produsul cartezian $A_1 \times A_2$. În acest caz, dacă $f_i : A_i \to A_i'$, $i = 1, 2$, atunci

$$f_1 \times f_2 : A_1 \times A_2 \to A_1' \times A_2', \qquad (f_1 \times f_2)(a_1, a_2) = (f_1(a_1), f_2(a_2)).$$

Exerciţiul 54 Fie funcţiile $f : A \to A'$, $g : B \to B'$, $f' : A' \to A''$ şi $g' : B' \to B''$. Să se demonstreze:

a) $1_A \times 1_B = 1_{A\times B}$;

b) $(f' \times g') \circ (f \times g) = (f' \circ f) \times (g' \circ g)$;

c) $\forall\, X \subseteq A$ şi $\forall\, Y \subseteq B$ $(f \times g)(X \times Y) = f(X) \times g(Y)$;

d) $\forall\, X' \subseteq A'$ şi $\forall\, Y' \subseteq B'$ $(f \times g)^{-1}(X' \times Y') = f^{-1}(X') \times g^{-1}(Y')$;

e) nu orice submulţime $M \subseteq A \times B$ este de forma $X \times Y$, unde $X \subseteq A$ şi $Y \subseteq B$, şi nu orice funcţie $\varphi : A \times B \to A' \times B'$ este de forma $f \times g$.

Exerciţiul 55 Fie $(A_i)_{i\in I}$, $(A_i')_{i\in I}$ şi $(A_i'')_{i\in I}$ familii de mulţimi, $(f_i : A_i \to A_i')_{i\in I}$ şi $(f_i' : A_i' \to A_i'')_{i\in I}$ familii de funcţii. Să se demonstreze :

a) Următoarea diagramă este comutativă pentru orice $i \in I$:

$$\begin{array}{ccc} \prod_{i\in I} A_i & \xrightarrow{p_i} & A_i \\ {\scriptstyle \prod_{i\in I} f_i}\downarrow & & \downarrow{\scriptstyle f_i} \\ \prod_{i\in I} A_i' & \xrightarrow{p_i'} & A_i' \end{array}$$

b) $\prod_{i\in I} \mathbf{1}_{A_i} = \mathbf{1}_{\prod_{i\in I} A_i}$;

c) $(\prod_{i\in I} f_i') \circ (\prod_{i\in I} f_i) = \prod_{i\in I}(f_i' \circ f_i)$.

Exerciţiul 56 Fie $f : A \to A'$, $g : B \to B'$ funcţii şi $(f_i : A_i \to A_i')_{i\in I}$ o familie de funcţii. Să se arate că:

a) f şi g sunt injective (surjective) $\Leftrightarrow$ $f \times g$ este injectiv (surjectiv);

b) Dacă f_i injectiv (respectiv surjectiv) pentru orice $i \in I$, atunci $\prod_{i\in I} f_i$ injectiv (respectiv surjectiv).

4.3.2 Suma directă a unei familii de mulţimi şi a unei familii de funcţii

Fie $(A_i)_{i\in I}$ o familie de mulţimi. Prin definiţie,

$$\coprod_{i\in I} A_i = \bigcup_{i\in I} A_i \times \{i\} = \{(a_i, i) \mid \ i \in I,\ a_i \in A_i\}$$

este **reuniunea disjunctă** a familiei $(A_i)_{i\in I}$. Funcţia

$$q_j : A_j \to \coprod_{i\in I} A_i, \qquad q_j(a_j) = (a_j, j)$$

se numeşte **injecţia canonică**, iar perechea $(\coprod_{i\in I} A_i, (q_i)_{i\in I})$ este **suma directă** a familiei $(A_i)_{i\in I}$.

Mai departe, dacă $(f_i : A_i \to A_i')_{i\in I}$ este o familie de funcţii, atunci

$$\coprod_{i\in I} f_i : \coprod_{i\in I} A_i \to \coprod_{i\in I} A_i', \qquad (\coprod_{i\in I} f_i)(a_i, i) = (f_i(a_i), i)$$

este **suma directă** a familiei $(f_i)_{i\in I}$.

Observăm că $\coprod_{i\in I} A_i$ este mulţimea vidă dacă şi numai dacă $I = \emptyset$ sau $A_i = \emptyset$ pentru orice $i \in I$.

Exerciţiul 57 Fie funcţiile $f : A \to A'$, $g : B \to B'$, $f' : A' \to A''$ şi $g' : B' \to B''$. Să se demonstreze:

a) $\mathbf{1}_A \coprod \mathbf{1}_B = \mathbf{1}_{A \coprod B}$;

b) $(f' \coprod g') \circ (f \coprod g) = (f' \circ f) \coprod (g' \circ g)$.

Exerciţiul 58 Fie $(A_i)_{i\in I}$, $(A_i')_{i\in I}$ şi $(A_i'')_{i\in I}$ familii de mulţimi, $(f_i : A_i \to A_i')_{i\in I}$ şi $(f_i' : A_i' \to A_i'')_{i\in I}$ familii de funcţii. Să se demonstreze :

a) Următoarea diagramă este comutativă pentru orice $i \in I$:

$$\begin{array}{ccc} \coprod_{i\in I} A_i & \xleftarrow{q_i} & A_i \\ {\scriptstyle \coprod_{i\in I} f_i}\downarrow & & \downarrow{\scriptstyle f_i} \\ \coprod_{i\in I} A_i' & \xleftarrow{q_i'} & A_i' \end{array}$$

b) $\coprod_{i\in I} \mathbf{1}_{A_i} = \mathbf{1}_{\coprod_{i\in I} A_i}$;

c) $(\coprod_{i\in I} f_i') \circ (\coprod_{i\in I} f_i) = \coprod_{i\in I}(f_i' \circ f_i)$.

Exerciţiul 59 Fie $f : A \to A'$, $g : B \to B'$ funcţii şi $(f_i : A_i \to A_i')_{i\in I}$ o familie de funcţii. Să se arate că:

a) Dacă f şi g sunt injective (surjective), atunci $f \amalg g$ este injectiv (surjectiv);

b) Dacă f_i injectiv (respectiv surjectiv) pentru orice $i \in I$, atunci $\coprod_{i\in I} f_i$ este injectiv (respectiv surjectiv).

4.3.3 Mulţimea $\mathrm{Hom}(A, B)$ şi funcţia $\mathrm{Hom}(f, g)$

Dacă A şi B mulţimi, atunci notăm $\mathrm{Hom}(A, B)$ mulţimea funcţiilor $f : A \to B$:

$$\mathrm{Hom}(A, B) = \{f \mid f : A \to B\}.$$

Dacă $A = \emptyset$, atunci $\mathrm{Hom}(\emptyset, B) = \{\emptyset\}$, şi dacă $A \neq \emptyset$, $B = \emptyset$, atunci $\mathrm{Hom}(A, \emptyset) = \emptyset$.

Fie $f : A' \to A, g : B \to B'$ funcţii; definim următoarea funcţie:

$$\mathrm{Hom}(f, g) : \mathrm{Hom}(A, B) \to \mathrm{Hom}(A', B'), \qquad \mathrm{Hom}(f, g)(\alpha) = g \circ \alpha \circ f,$$

deci următoarea diagramă este comutativă.

$$\begin{tikzcd} A' \arrow[r, "f"] \arrow[d, "(g^f)(\alpha)"'] & A \arrow[d, "\alpha"] \\ B' & B \arrow[l, "g"] \end{tikzcd}$$

Folosim şi notaţiile $\mathrm{Hom}(A, B) = B^A$ şi $\mathrm{Hom}(f, g) = g^f$.

Exerciţiul 60 Fie funcţiile $f : A' \to A$, $g : B \to B'$, $f' : A'' \to A'$ şi $g' : B' \to B''$.

a) Dacă $A' = B' = \{1, 2, 3\}$ şi $A = B = \{1, 2\}$, $f(1) = f(2) = 1$, $f(3) = 2$, $g(1) = 2$ şi $g(2) = 3$, să se determine funcţia $\mathrm{Hom}(f, g)$.

Să se demonstreze:

b) $\mathrm{Hom}(\mathbf{1}_A, \mathbf{1}_B) = \mathbf{1}_{\mathrm{Hom}(A,B)}$;

c) $\mathrm{Hom}(f \circ f', g' \circ g) = \mathrm{Hom}(f', g') \circ \mathrm{Hom}(f, g)$.

Exerciţiul 61 Fie $f : A' \to A$ şi $g : B \to B'$ două funcţii. Să se arate că:

a) Dacă f este surjectiv şi g este injectiv, atunci $\mathrm{Hom}(f, g)$ este injectiv;

b) Dacă $A' \neq \emptyset$, g este surjectiv şi f este injectiv, atunci $\mathrm{Hom}(f, g)$ este surjectiv;

c) g este injectiv dacă şi numai dacă pentru orice mulţime A, $\mathrm{Hom}(\mathbf{1}_A, g) : \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, B')$ este injectiv;

d) f este surjectiv dacă şi numai dacă pentru orice mulţime B, $\mathrm{Hom}(f, \mathbf{1}_B) : \mathrm{Hom}(A, B) \to \mathrm{Hom}(A', B)$ este injectiv. •

4.3.4 Mulţimea părţilor şi funcţia caracteristică a unei submulţimi

Amintim că mulţimea părţilor unei mulţimi A este mulţimea $\mathcal{P}(A) = \{X \mid X \subseteq A\}$, adică avem $X \in \mathcal{P}(A) \iff X \subseteq A$. O funcţie $f : A \to B$ induce funcţiile

$$f_* : \mathcal{P}(A) \to \mathcal{P}(B), \qquad f_*(X) = f(X),$$

$$f^* : \mathcal{P}(B) \to \mathcal{P}(A), \qquad f^*(Y) = f^{-1}(Y).$$

Exerciţiul 62 Fie $f : A \to B$ şi $g : B \to C$ funcţii. Să se demonstreze:

a) $\mathbf{1}_{A*} = {\mathbf{1}_A}^* = \mathbf{1}_{\mathcal{P}(A)}$;

b) $(g \circ f)_* = g_* \circ f_*$; $(g \circ f)^* = f^* \circ g^*$;

c) $f^* \circ f_* \circ f^* = f^*$;

d) dacă $\varphi = f^* \circ f_*$ şi $\psi = f_* \circ f^*$, atunci $\varphi \circ \varphi = \varphi$ şi $\psi \circ \psi = \psi$.

Exerciţiul 63 Fie $f : A \to B$ o funcţie.

a) Următoarele afirmaţii sunt echivalente:

(i) f este injectiv; (ii) f_* este injectiv; (iii) $f^* \circ f_* = \mathbf{1}_{\mathcal{P}(A)}$; (iv) f^* este surjectiv.

b) Următoarele afirmaţii sunt echivalente:

(i) f este surjectiv; (ii) f_* este surjectiv; (iii) $f_* \circ f^* = \mathbf{1}_{\mathcal{P}(B)}$; (iv) f^* este injectiv.

Exerciţiul 64 Fie A şi B două mulţimi şi definim funcţia

$$\varphi_{A,B} : \mathcal{P}(A \times B) \to \mathrm{Hom}(A, \mathcal{P}(B)), \qquad \varphi_{A,B}(R)(a) = R\langle a\rangle,$$

pentru orice $R \subseteq A \times B$ şi $a \in A$.

a) Să se arate că funcţia $\varphi_{A,B}$ este bijectivă.

b) Fie $f : A \to A'$ şi $g : B \to B'$ două funcţii. Să se arate că următoarea diagramă este comutativă:

$$\begin{tikzcd}
\mathcal{P}(A \times B) \arrow[r, "\varphi_{A,B}"] & \mathrm{Hom}(A, \mathcal{P}(B)) \\
\mathcal{P}(A' \times B') \arrow[u, "(f\times g)^*"] \arrow[r, "\varphi_{A',B'}"'] & \mathrm{Hom}(A', \mathcal{P}(B')) \arrow[u, "\mathrm{Hom}(f, g^*)"']
\end{tikzcd}$$

Observaţie. Acest exerciţiu spune că o relaţie $\rho = (A, B, R)$ se identifică în mod canonic cu o *funcţie multivocă* $f : A \to \mathcal{P}(B)$.

Definiţia 4.3.7 Fie A o mulţime şi $X \subseteq A$. Funcţia

$$\chi_X : A \to \{0, 1\}, \qquad \chi_X(x) = \begin{cases} 1, & \text{dacă } x \in X, \\ 0, & \text{dacă } x \notin X \end{cases}$$

se numeşte **funcţia caracteristică** a submulţimii X. Astfel am definit funcţia

$$\varphi_A : \mathcal{P}(A) \to \mathrm{Hom}(A, \{0, 1\}), \qquad \varphi_A(X) = \chi_X$$

Exerciţiul 65 Fie A o mulţime. Să se arate că:
a) Funcţia φ_A este bijectivă şi avem $\varphi_A^{-1}(\chi) = \chi^{-1}(1)$, pentru orice funcţie $\chi : A \to \{0, 1\}$;
b) Fie $f : A \to B$ o funcţie. Să se arate că următoarea diagrama este comutativă:

$$\begin{tikzcd}
\mathcal{P}(A) \arrow[r, "\varphi_A"] & \mathrm{Hom}(A, \{0, 1\}) \\
\mathcal{P}(B) \arrow[u, "f^*"] \arrow[r, "\varphi_B"'] & \mathrm{Hom}(B, \{0, 1\}) \arrow[u, "\mathrm{Hom}(f, 1_{\{0,1\}})"']
\end{tikzcd}$$

Exerciţiul 66 Dacă $X, Y \subseteq A$, atunci:
(1) $X \subseteq Y \Leftrightarrow \chi_X(x) \leq \chi_Y(x), \quad \forall x \in A,$
(2) $\chi_{\bar{X}}(x) = 1 - \chi_X(x), \quad \forall x \in A,$
(3) $\chi_{X\cap Y}(x) = \chi_X(x)\chi_Y(x), \quad \forall x \in A,$
(4) $\chi_{X\cup Y}(x) = \chi_X(x) + \chi_Y(x) - \chi_X(x)\chi_Y(x), \quad \forall x \in A,$
(5) $\chi_{X\setminus Y}(x) = \chi_X(x)(1 - \chi_Y(x)), \quad \forall x \in A,$
(6) $\chi_{X\Delta Y}(x) = \chi_X(x) + \chi_Y(x) - 2\chi_X(x)\chi_Y(x), \quad \forall x \in A.$

Observaţii 4.3.8 Proprietăţile de mai sus ale funcţiei caracteristice sunt utile la demonstrarea egalităţilor de mulţimi. De exemplu, să arătăm că $(X\Delta Y)\Delta Z = X\Delta(Y\Delta Z)$:

$$\begin{aligned}
\chi_{(X\Delta Y)\Delta Z} &= \chi_{X\Delta Y} + \chi_Z - 2\chi_{X\Delta Y}\chi_Z = \\
&= \chi_X + \chi_Y - 2\chi_X\chi_Y - 2(\chi_X + \chi_Y - 2\chi_X\chi_Y)\chi_Z = \\
&= \chi_X + \chi_Y + \chi_Z - 2(\chi_X\chi_Y + \chi_X\chi_Z + \chi_Y\chi_Z) + 4\chi_X\chi_Y\chi_Z. \qquad (*)
\end{aligned}$$

Calculând analog $\chi_{X\Delta(Y\Delta Z)}$ obţinem aceeaşi expresie (*). Altfel, din comutativitatea lui Δ şi din (*) deducem

$$\begin{aligned}
\chi_{X\Delta(Y\Delta Z)} &= \chi_{(Y\Delta Z)\Delta X} = \\
&= \chi_Y + \chi_Z + \chi_X - 2(\chi_Y\chi_Z + \chi_Y\chi_X + \chi_Z\chi_X) + 4\chi_Y\chi_Y\chi_X = \\
&= \chi_X + \chi_Y + \chi_Z - 2(\chi_X\chi_Y + \chi_X\chi_Z + \chi_Y\chi_Z) + 4\chi_X\chi_Y\chi_Z.
\end{aligned}$$

4.4 Relaţii de echivalenţă

4.4.1 Clase importante de relaţii omogene

Definiţia 4.4.1 Fie $\rho = (A, A, R)$ o relaţie omogenă. Spunem că
a) ρ este **reflexiv**, dacă pentru orice $x \in A$, $x\rho x$, adică

$$(\forall\, x \in A)(x\rho x);$$

ρ este **ireflexiv** dacă pentru orice $a \in A$ avem $a \not\rho\, a$, adică are loc $\neg(a\rho a)$;

b) ρ este **tranzitiv**, dacă pentru orice $x, y, z \in A, x\rho y$ şi $y\rho z$ implică $x\rho z$, adică

$$(\forall\ x, y, z \in A)(x\rho y \wedge y\rho z \to x\rho z);$$

c) ρ este **simetric**, dacă pentru orice $x, y \in A, x\rho y$ implică $y\rho x$, adică

$$(\forall\ x, y \in A)(x\rho y \to y\rho x);$$

d) ρ este **antisimetric**, dacă pentru orice $x, y \in A, x\rho y$ şi $y\rho x$ implică $x = y$, adică

$$(\forall\ x, y \in A)(x\rho y \wedge y\rho x \Rightarrow x = y);$$

ρ este **asimetric**, dacă pentru orice $x, y \in A$, $x\rho y$ implică $y \not\rho x$;

e) ρ este **relaţie de preordine**, dacă ρ este reflexiv şi tranzitiv. Atunci spunem că (A, ρ) este **mulţime preordonată**;

f) ρ este **relaţie de echivalenţă**, dacă ρ este reflexiv, tranzitiv şi simetric. Notăm $\mathcal{E}(A)$ mulţimea relaţiilor de echivalenţă definite pe A;

g) ρ este **relaţie de ordine**, dacă ρ este reflexiv, tranzitiv şi antisimetric. Atunci spunem că (A, ρ) este **mulţime ordonată**;

h) ρ este **relaţie de ordine strictă**, dacă ρ este ireflexiv şi tranzitiv.

Observaţii 4.4.2 Sunt uşor de demonstrat următoarele afirmaţii:

1) ρ este reflexiv $\Leftrightarrow 1_A \subseteq \rho$;
2) ρ este tranzitiv $\Leftrightarrow \rho^2 \subseteq \rho$;
3) ρ este simetric $\Leftrightarrow \rho = \rho^{-1}$;
4) ρ este antisimetric $\Leftrightarrow \rho \cap \rho^{-1} \subseteq 1_A$;
5) ρ este reflexiv şi antisimetric $\Rightarrow \rho \cap \rho^{-1} = 1_A$;
6) ρ este ireflexiv $\Leftrightarrow \rho \cap 1_A = \emptyset$;
6) ρ este asimetric $\Leftrightarrow \rho \cap \rho^{-1} = \emptyset$;
7) ρ este relaţie de preordine $\Rightarrow \rho^2 = \rho$;
8) ρ este relaţie de echivalenţă $\Leftrightarrow 1_A \subseteq \rho$ şi $\rho = \rho^2 = \rho^{-1}$;
9) ρ este relaţie de echivalenţă şi relaţie de ordine $\Leftrightarrow \rho = 1_A$.

Exemplul 4.4.3 1) Pe mulţimea numerelor întregi $\mathbb{Z}$, relaţia de divizibilitate este relaţie de preordine, nu e simetrică şi nu e antisimetrică, pentru că de exemplu $3|-3$ şi $-3|3$, dar $-3 \neq 3$.

2) Pe mulţimea numerelor naturale $\mathbb{N}$ relaţia de divizibilitate este relaţie de ordine, deci $(\mathbb{N}, |)$ este mulţime ordonată.

3) Pe mulţimea numerelor întregi $\mathbb{Z}$, relaţia de congruenţă definită prin $a \equiv b \pmod{n} \Leftrightarrow n|a-b$ este relaţie de echivalenţă.

4) Relaţia universală $(A, A, A \times A)$ este relaţie de echivalenţă.

5) Restricţia la o submulţime a unei relaţii de echivalenţă este relaţie de echivalenţă. Mai exact, dacă $\rho = (A, A, R)$ este relaţie de echivalenţă pe A, iar $B \subseteq A$, atunci $(B, B, R \cap (B \times B))$ este relaţie de echivalenţă pe B.

4.4.2 Echivalenţe şi partiţii

Definiţia 4.4.4 Dacă ρ este relaţie de echivalenţă pe mulţimea A, atunci secţiunea

$$\rho\langle x\rangle = \{y \in A \mid x\rho y\}$$

după elementul $x \in A$ se numeşte **clasă de echivalenţă**. Mulţimea acestor clase se numeşte **mulţimea factor** modulo ρ:

$$A/\rho = \{\rho\langle x\rangle \mid x \in A\}.$$

Exemplul 4.4.5 1) Pe mulţimea $\mathbb{Z}$ relaţiei de congruenţă $a \equiv b \pmod{n}$ (unde $n \neq 0$) îi corespunde mulţimea factor

$$\mathbb{Z}/\equiv \pmod{n} = \{\widehat{0}, \widehat{1}, \widehat{2}, \dots, \widehat{n-1}\},$$

unde

$$\begin{aligned}\widehat{k} = \equiv \pmod{n}\langle k\rangle &= \{x \in \mathbb{Z} \mid x \equiv k \pmod{n}\} = \\ &= \{x \in \mathbb{Z} \mid n|x-k\} = \\ &= \{x \in \mathbb{Z} \mid \exists j \in \mathbb{Z} :\ x = jn + k\} = \\ &= n\mathbb{Z} + k\end{aligned}$$

2) $A/1_A = \{\{x\} : x \in A\}$ şi $A/(A \times A) = \{A\}$.

Lema 4.4.6 *Dacă* ρ *este o relaţie de echivalenţă mulţimea* A *şi* $x, y \in A$, *atunci sunt echivalente următoarele afirmaţii:*
(i) $x\rho y$; (ii) $y \in \rho\langle x\rangle$; (iii) $\rho\langle x\rangle = \rho\langle y\rangle$.

Demonstraţie. (i) $\Leftrightarrow$ (ii) este evident din definiţie.
(i) $\Rightarrow$ (iii) Fie $x\rho y$ şi fie $z \in \rho\langle x\rangle$. Atunci $x\rho y$ şi $x\rho z \Rightarrow z\rho x$ şi $x\rho y$ (pentru că ρ simetric), deci $z\rho y$ (pentru că ρ tranzitiv) $\Rightarrow z \in \rho\langle y\rangle$, deci $\rho\langle x\rangle \subseteq \rho\langle y\rangle$. Analog, $\rho\langle y\rangle \subseteq \rho\langle x\rangle$, deci (iii) are loc.
(iii) $\Rightarrow$ (i) Dacă $\rho\langle x\rangle = \rho\langle y\rangle$, atunci $y \in \rho\langle y\rangle = \rho\langle x\rangle \Rightarrow y\rho x \Rightarrow x\rho y$.

Definiţia 4.4.7 Fie A o mulţime nevidă şi $\pi \subseteq \mathcal{P}(A) \setminus \{\emptyset\}$.
a) Spunem că π este o **partiţie** a lui A dacă

(1) $A = \bigcup_{B\in\pi} B$ şi

(2) $\forall B_1, B_2 \in \pi, B_1 \neq B_2 \Rightarrow B_1 \cap B_2 = \emptyset$, adică orice două mulţimi distincte din π sunt disjuncte.

Dacă $B \in \pi$ şi $b \in B$, atunci spunem că b este un **reprezentant** al lui B. Notăm prin $P(A)$ mulţimea partiţiilor lui A.
b) Dacă $\pi_1, \pi_2 \in P(A)$, atunci π_1 este **mai fin** ca π_2 (notaţie: $\pi_1 \leq \pi_2$) dacă

$$\forall B_1 \in \pi_1 \exists B_2 \in \pi_2 : B_1 \subseteq B_2,$$

adică dacă a orice submulţime din partiţia mai fină π_1 este conţinută de o submulţime din partiţia π_2.

Relaţiile de echivalenţă şi partiţiile se determină reciproc.

Teorema 4.4.8 *Fie* A *o mulţime nevidă .*
1) *Dacă* ρ *relaţie de echivalenţă pe* A, *atunci mulţimea factor*

$$A/\rho = \{\rho\langle x\rangle \mid x \in A\}$$

este partiţie a lui A.
2) *Fie* $\pi \subseteq \mathcal{P}(A) \setminus \{\emptyset\}$ *o partiţie a lui* A *şi definim relaţia*

$$\rho_\pi = (A, A, R_\pi), \quad R_\pi = \bigcup_{B\in\pi} (B \times B),$$

adică $x\rho_\pi y \Leftrightarrow \exists B \in \pi : x, y \in B$.
Atunci ρ_π *este relaţie de echivalenţă pe* A.
3) *Considerăm funcţiile*

$$\phi : \mathcal{E}(A) \to P(A), \quad \phi(\rho) = A/\rho,$$

$$\psi : P(A) \to \mathcal{E}(A), \quad \psi(\pi) = \rho_\pi.$$

Atunci $\psi \circ \phi = 1_{\mathcal{E}(A)}$ *şi* $\phi \circ \psi = 1_{\mathcal{P}(A)}$.
4) *Dacă* $\rho_1 \subseteq \rho_2$, *atunci* $\phi(\rho_1) \leq \phi(\rho_2)$. *Invers, dacă* $\pi_1 \leq \pi_2$, *atunci* $\psi(\pi_1) \subseteq \psi(\pi_2)$.

Demonstraţie. 1) Arătăm că $A = \bigcup_{x\in A} \rho\langle x\rangle$. Incluziunea „$\supseteq$" este evidentă, pentru că $\rho\langle x\rangle \subseteq A$ pentru orice $x \in A$. Mai departe, pentru orice $y \in A$, $y \in \rho\langle y\rangle$ (pentru că ρ este reflexiv), deci $y \in \bigcup_{x\in A} \rho\langle x\rangle$, de unde rezultă incluziunea „$\subseteq$".
Presupunem acum că $\rho\langle x\rangle \cap \rho\langle y\rangle \neq \emptyset$, unde $x, y \in A$. Arătăm că atunci clasele $\rho\langle x\rangle$ şi $\rho\langle y\rangle$ sunt egale. Într-adevăr, din ipoteză $\exists u \in \rho\langle x\rangle \cap \rho\langle y\rangle \Rightarrow x\rho u$ şi $y\rho u \Rightarrow x\rho u$ şi $u\rho y$ (pentru că ρ este simetric) $\Rightarrow x\rho y$ (ρ tranzitiv) $\Rightarrow \rho\langle x\rangle = \rho\langle y\rangle$ conform Lemei 4.4.6.
2) ρ_π este reflexiv, pentru că $\forall x \in A = \bigcup_{B\in\pi} B \Rightarrow \exists B \in \pi : x \in B \Rightarrow (x, x) \in B \times B \Rightarrow x\rho_\pi x$.
ρ_π este tranzitiv, pentru că $\forall x, y, z \in A : x\rho_\pi y$ şi $y\rho_\pi z \Rightarrow \exists B, C \in \pi : x, y \in B$ şi $y, z \in C$. Deci $y \in B \cap C$, şi obţinem $B = C$ (pentru că $B \neq C$, conform definiţiei $B \cap C = \emptyset$, contradicţie). Deci $x, z \in B = C \Rightarrow x\rho_\pi z$.
Mai departe, ρ_π este simetric, pentru că $\forall x, y \in A : x\rho_\pi y \Rightarrow \exists B \in \pi : x, y \in B \Rightarrow y\rho_\pi x$.
Deci ρ este relaţie de echivalenţă.
3) Pentru orice $\rho \in \mathcal{E}(A)$, $(\psi \circ \phi)(\rho) = \psi(\phi(\rho)) = \rho_{\phi(\rho)} = \rho_{A/\rho}$. Arătăm că $\rho_{A/\rho} = \rho$. Într-adevăr,

$$\begin{aligned} x\rho_{A/\rho} y &\Leftrightarrow \exists B \in A/\rho : x, y \in B \Leftrightarrow \\ &\Leftrightarrow \exists z \in A : B = \rho\langle z\rangle \in A/\rho \text{ şi } \quad x, y \in B = \rho\langle z\rangle \Leftrightarrow \\ &\Leftrightarrow \exists z \in A : x\rho z \text{ şi } y\rho z \Leftrightarrow \\ &\Leftrightarrow \exists z \in A : x\rho z \quad \text{şi} \quad z\rho y \quad (\rho \quad \text{este simetric}) \Leftrightarrow \\ &\Leftrightarrow x(\rho \circ \rho)y \Leftrightarrow x\rho y \qquad (\text{pentru că } \rho^2 = \rho). \end{aligned}$$

Deci $(\psi \circ \phi)(\rho) = \rho$, adică $\psi \circ \phi = 1_{\mathcal{E}(A)}$.

Pentru orice $\pi \in P(A)$, $(\phi \circ \psi)(\pi) = \phi(\psi(\pi)) = A/\psi(\pi) = A/\rho_\pi$. Arătăm că $A/\rho_\pi = \pi$. Într-adevăr, $B \in A/\rho_\pi \Leftrightarrow \exists z \in A : B = \rho_\pi\langle z\rangle$. Aici $z \in A = \bigcup_{C\in\pi} C$, deci există $C \in \pi$ astfel încât $z \in C$ şi

$$B = \{x \in A \mid x\rho_\pi z\} = \{x \in A \mid x \in C\} = C \in \pi,$$

deci $A/\rho_\pi \subseteq \pi$.

Invers, pentru orice $C \in \pi$, există $z \in C$ astfel încât

$$C = \{x \in A \mid x\rho_\pi z\} = \rho\langle z\rangle \in A/\rho_\pi,$$

de unde $\pi \subseteq A/\rho_\pi$. Deci $(\phi \circ \psi)(\pi) = \pi$, adică $\phi \circ \psi = 1_{P(A)}$.

4) Fie $\rho_1 \subseteq \rho_2$. Atunci pentru orice $\rho_1\langle x\rangle \in A/\rho_1 = \phi(\rho_1)$, $\rho_1\langle x\rangle \subseteq \rho_2\langle x\rangle$, unde $\rho_2\langle x\rangle \in A/\rho_2 = \phi(\rho_2)$, deci $\phi(\rho_1) \le \phi(\rho_2)$.

Acum fie $\pi_1 \le \pi_2$ şi arătăm că $\psi(\pi_1) = \rho_{\pi_1} \subseteq \rho_{\pi_2} = \psi(\pi_2)$. Într-adevăr, pentru orice $x, y \in A$,

$$x\rho_{\pi_1} y \Rightarrow \exists B_1 \in \pi_1 : x, y \in B_1 \Rightarrow$$
$$\Rightarrow \exists B_2 \in \pi_2 : B_1 \subseteq B_2 \text{ şi } x, y \in B_1 \subseteq B_2 \Rightarrow x\rho_{\pi_2} y.$$

Exerciţiul 67 Fie $\rho = (A, B, R)$ o relaţie. Să se demonstreze:

a) Dacă ρ este reflexiv, simetric şi antisimetric, atunci $\rho = 1_A$;

b) Dacă ρ este reflexiv şi tranzitiv, atunci $\rho^2 = \rho$.

Exerciţiul 68 Fie $A = \{1, 2, 3, 4\}$.

a) Dacă $\rho = \{(1, 1), \dots, (4, 4), (1, 2), (2, 1), (3, 2), (2, 3), (1, 3), (3, 1)\}$, să se determine partiţia corespunzătoare.

b) Dacă $\pi = \{\{1, 2\}, \{3\}, \{4\}\}$, să se determine relaţia de echivalenţă corespunzătoare.

Exerciţiul 69 Să se determine toate relaţiile de echivalenţă pe o mulţime cu $1, 2, 3$, respectiv 4 elemente.

Exerciţiul 70 Să se arate că:

a) $(\mathbb{Z}, |)$ este mulţime preordonată, ,,|” nu e simetric şi nu e antisimetric;

b) $(\mathbb{N}, |)$ este mulţime ordonată;

Exerciţiul 71 Pe mulţimea $\mathbb{C}$ a numerelor complexe considerăm relaţiile ρ_1 şi ρ_2, unde $z\rho_1 w \Leftrightarrow |z| = |w|$ şi $z\rho_2 w \Leftrightarrow z = w = 0$ sau $\arg z = \arg w$. Să se arate că ρ_1 şi ρ_2 sunt relaţii de echivalenţă şi să se reprezinte grafic clasele din $\mathbb{C}/\rho_1$ şi $\mathbb{C}/\rho_2$.

Exerciţiul 72 Fie ρ_1 şi ρ_2 două relaţii de echivalenţă pe mulţimea A. Să se demonstreze:

a) ρ_1^{-1} şi $\rho_1 \cap \rho_2$ sunt relaţii de echivalenţă. (Mai general, dacă $(\rho_i)_{i\in I}$ sunt relaţii de echivalenţă pe A, atunci $\bigcap_{i\in I} \rho_i$ este relaţie de echivalenţă pe mulţimea A.)

b) $\complement\rho_1$ şi $\rho_1 \cup \rho_2$ în general nu sunt relaţii de echivalenţă;

c) $\rho_1 \circ \rho_2$ este relaţie de echivalenţă dacă şi numai dacă $\rho_1 \circ \rho_2 = \rho_2 \circ \rho_1$. În acest caz să se arate că $\rho_1 \circ \rho_2$ este cea mai mică relaţie de echivalenţă ce conţine pe ρ_1 şi ρ_2.

Exerciţiul 73 Fie ρ_1 şi ρ_2 două relaţii pe mulţimea A.

a) Să se arate că $(\rho_1 \cup \rho_2)^2 = \rho_1^2 \cup \rho_2^2 \cup (\rho_1 \circ \rho_2) \cup (\rho_2 \circ \rho_1)$.

b) Presupunem că ρ_1 şi ρ_2 sunt relaţii de echivalenţă. Să se arate că $\rho_1 \cup \rho_2$ relaţie de echivalenţă dacă şi numai dacă $\rho_1 \circ \rho_2$ şi $\rho_2 \circ \rho_1$ sunt subrelaţii ale lui $\rho_1 \cup \rho_2$.

Exerciţiul 74 Fie $\rho = (A, A, R)$ o relaţie, $\rho^0 = 1_A$, $\rho^n = \rho \circ \cdots \circ \rho$ (de n ori), şi fie $\bar\rho = 1_A \cup \rho \cup \rho^{-1}$. Să se arate că:

a) $\bigcup_{n\ge 1} \rho^n$ este cea mai mică relaţie tranzitivă ce conţine pe ρ;

b) $\bigcup_{n\ge 1} \bar\rho^n$ este cea mai mică relaţie de echivalenţă ce conţine pe ρ.

4.5 Teoreme de factorizare a funcţiilor

Definiţia 4.5.1 a) Fie $f : A \to B$ o funcţie. Relaţia $\ker f$ pe mulţimea A definită prin

$$a_1 \rho a_2 \Leftrightarrow f(a_1) = f(a_2)$$

se numeşte **nucleul** lui f.

b) Fie ρ o relaţie de echivalenţă pe mulţimea A. Funcţia

$$p_\rho : A \to A/\rho, \quad p_\rho(x) = \rho\langle x\rangle$$

se numeşte **proiecţia canonică** a lui A în mulţimea factor A/ρ.

Este uşor de arătat că relaţia $\ker f$ este relaţie de echivalenţă pe A, iar proiecţia canonică $p_\rho : A \to A/\rho$ este funcţie surjectivă şi avem $\ker p_\rho = \rho$.

Exerciţiul 75 Fie $f : A \to B$ o funcţie. Să se arate că:
1) $\ker f$ este relaţie de echivalenţă pe A şi $\ker f = f^{-1} \circ f$,
2) $A/\ker f = \{f^{-1}(b) \mid b \in \operatorname{Im} f\}$,
3) f este injectiv $\Leftrightarrow \ker f = 1_A$,
4) f este surjectiv $\Leftrightarrow \operatorname{Im} f = B$.
5) Graficul relaţiei $f \circ f^{-1}$ este $\Delta_{\operatorname{Im} f}$, unde $\Delta_{\operatorname{Im} f} = \{(b, b) \mid b \in \operatorname{Im} f\}$.

Exerciţiul 76 Dacă ρ este o relaţie de echivalenţă pe A, atunci proiecţia canonică $p_\rho : A \to A/\rho$ este surjectivă şi avem $\ker p_\rho = \rho$.

Teorema 4.5.2 (factorizare după o funcţie injectivă) *Fie $f : B \to A$ o funcţie şi $g : C \to A$ o funcţie injectivă.*

$$\begin{tikzcd} A \arrow[d, shift right, dashed, "r"'] & B \arrow[l, "f"'] \arrow[dl, dotted, "h"] \\ C \arrow[u, shift right, "g"'] & \end{tikzcd}$$

1) *Există o funcţie $h : B \to C$, astfel încât $f = g \circ h$ dacă şi numai dacă $\operatorname{Im} f \subseteq \operatorname{Im} g$. Atunci:*
2) h *este unic determinat şi dacă $C \neq \emptyset$, atunci $h = r \circ f$, unde r este o inversă la stânga a lui g,*
3) h *este surjectiv dacă şi numai dacă $\operatorname{Im} f = \operatorname{Im} g$,*
4) $\ker h = \ker f$. *(În particular, h este injectiv $\Longleftrightarrow$ f este injectiv.)*

Demonstraţie. 1) Presupunem că există o funcţie $h : B \to C$ astfel încât $f = g \circ h$. Atunci pentru orice $a \in A$, $a \in \operatorname{Im} f \Rightarrow \exists b \in B : a = f(b) = g(h(b)) \Rightarrow a \in \operatorname{Im} g$, deci $\operatorname{Im} f \subseteq \operatorname{Im} g$.

Invers, dacă $C \neq \emptyset$ şi $\operatorname{Im} f \subseteq \operatorname{Im} g$, atunci fie r o inversă la stânga a lui g, adică $r : A \to C, r \circ g = 1_C$, care există conform Teoremei 4.1.8. Fie $h = r \circ f$. Rezultă că pentru orice $b \in B$ avem $f(b) \in \operatorname{Im} f \subseteq \operatorname{Im} g \Rightarrow \exists c \in C : f(b) = g(c)$, deci există $c \in C$ astfel încât

$$(g \circ h)(b) = g(h(b)) = g(r(f(b))) = g(r(g(c))) = g((r \circ g)(c)) = g(c) = f(b),$$

de unde $g \circ h = f$. Dacă $C = \emptyset$, atunci $\emptyset = \operatorname{Im} g = \operatorname{Im} f$, deci $B = \emptyset$, şi fie $h = \emptyset$.

2) unicitatea lui h: dacă $h, h' : B \to C$ sunt funcţii, astfel încât $f = g \circ h = g \circ h'$, atunci $h = h'$, conform Teoremei 4.3.3.

3) Trebuie să arătăm că h este surjectiv $\Leftrightarrow \operatorname{Im} g \subseteq \operatorname{Im} f$.

„$\Rightarrow$" Presupunem că h este surjectiv. Atunci $\forall a \in A$, $a \in \operatorname{Im} g \Rightarrow \exists c \in C : a = g(c)$ şi $\exists b \in B : c = h(b) \Rightarrow \exists c \in C$ şi $\exists b \in B : a = g(c) = g(h(b)) = f(b) \Rightarrow a \in \operatorname{Im} f$.

„$\Leftarrow$" Pentru orice $c \in C$, $g(c) \in \operatorname{Im} g \subseteq \operatorname{Im} f \Rightarrow \exists b \in B : g(c) = f(b) \Rightarrow \exists b \in B : h(b) = r(f(b)) = r(g(c)) = (r \circ g)(c) = c$, deci h este surjectiv.

4) Pentru orice $b_1, b_2 \in B$, $b_1 \ker f\, b_2 \Leftrightarrow f(b_1) = f(b_2) \Leftrightarrow (g \circ h)(b_1) = (g \circ h)(b_2) \Leftrightarrow h(b_1) = h(b_2)$ (pentru că g injectiv) $\Leftrightarrow b_1 \ker h\, b_2$. ∎

Exerciţiul 77 a) Fie $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \cos x$, $C = [-2, +\infty)$ şi $g : C \to \mathbb{R}$, $g(x) = 2x + 1$. Să se determine o funcţie $h : \mathbb{R} \to C$ astfel încât $f = g \circ h$.

b) Aceeaşi problemă dacă $f(x) = \sin x$, $C = [0, +\infty)$ şi $g(x) = 2x + 1$.

Teorema 4.5.3 (factorizare după o funcţie surjectivă) *Fie $f : A \to B$ o funcţie şi $g : A \to C$ o funcţie surjectivă.*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, shift right, "g"'] & B \\ C \arrow[u, shift right, dashed, "s"'] \arrow[ur, dotted, "h"'] & \end{tikzcd}$$

1) *Există o funcţie $h : C \to B$ astfel încât $f = h \circ g$, dacă şi numai dacă $\ker g \subseteq \ker f$. Atunci:*
2) h *este unic determinat şi $h = f \circ s$, unde s este o inversă la drepta a lui g,*
3) h *este injectiv dacă şi numai dacă $\ker f = \ker g$,*
4) $\operatorname{Im} h = \operatorname{Im} f$. *(În particular, h este surjectiv $\Longleftrightarrow$ f este surjectiv).*

Demonstraţie. 1) Presupunem că există o funcţie $h : C \to B$ astfel încât $f = h \circ g$. Atunci pentru orice $x_1, x_2 \in A$ avem $x_1 \ker g\ x_2 \Rightarrow g(x_1) = g(x_2) \Rightarrow h(g(x_1)) = h(g(x_2)) \Rightarrow f(x_1) = f(x_2) \Rightarrow x_1 \ker f\ x_2$, deci $\ker g \subseteq \ker f$.

Invers, dacă $\ker g \subseteq \ker f$, atunci fie s o inversă la drepta a lui g, adică $s : C \to A, g \circ s = 1_C$, care există conform Teoremei 4.3.4. Rezultă că $g \circ s \circ g = g$, adică $g(s(g(x))) = g(x)$ pentru orice $x \in A$, $\Rightarrow f(s(g(x))) = f(x)$ (din ipoteza $\ker g \subseteq \ker f$) $\Rightarrow f \circ s \circ g = f$. Fie $h = f \circ s$; atunci $h \circ g = f \circ s \circ g = f$.

2) unicitatea lui h: dacă $h, h' : C \to B$ sunt funcţii astfel încât $f = h \circ g = h' \circ g$, atunci $h = h'$, conform Teoremei 4.1.9.

3) Trebuie să arătăm că h este injectiv $\Leftrightarrow \ker f \subseteq \ker g$.

„$\Rightarrow$" Presupunem că h este injectiv. Atunci pentru orice $x_1, x_2 \in A$, $x_1 \ker f\ x_2 \Rightarrow f(x_1) = f(x_2) \Rightarrow h(g(x_1)) = h(g(x_2)) \Rightarrow g(x_1) = g(x_2) \Rightarrow x_1 \ker g\ x_2$.

„$\Leftarrow$" Presupunem acum că $\ker f \subseteq \ker g$. Atunci pentru orice $z_1, z_2 \in C$, din $h(z_1) = h(z_2)$ rezultă că există $x_1, x_2 \in A$ astfel încât $z_1 = g(x_1), z_2 = g(x_2), \Rightarrow \exists x_1, x_2 \in A : f(x_1) = h(g(x_1)) = h(g(x_2)) = f(x_2)$, deci $g(x_1) = g(x_2)$ (din ipoteză) $\Rightarrow z_1 = z_2$, deci h injectiv.

4) Pentru orice $y \in B$, $y \in \operatorname{Im} h \Leftrightarrow \exists z \in C : y = h(z) \Leftrightarrow \exists z \in C$ şi $\exists x \in A : y = h(z)$ şi $z = g(x)$ (pentru că g este surjectiv) $\Leftrightarrow \exists x \in A : y = h(g(x)) = f(x) \Leftrightarrow y \in \operatorname{Im} f$. ■

Exerciţiul 78 a) Fie $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \cos x$ şi $g : \mathbb{R} \to \mathbb{R}_+$, $g(x) = x^2$. Să se determine o funcţie $h : \mathbb{R}_+ \to \mathbb{R}$ astfel încât $f = h \circ g$.

b) Aceeaşi problemă dacă $f(x) = \sin x$ şi $g(x) = x^2$.

Corolar 4.5.4 (factorizare după o proiecţie canonică) *Fie* $f : A \to B$ *o funcţie şi* ρ *o relaţie de echivalenţă pe mulţimea* A.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "p_\rho"'] & B \\ A/\rho \arrow[ur, dotted, "f'"'] & \end{tikzcd}$$

1) *Există o funcţie* $f' : A/\rho \to B$ *astfel încât* $f = f' \circ p_\rho$ *dacă şi numai dacă* $\rho \subseteq \ker f$. *Atunci:*
2) $f'(\rho\langle x\rangle) = f(x)$ *pentru orice* $x \in A$,
3) f' *este injectiv dacă şi numai dacă* $\rho = \ker f$,
4) $\operatorname{Im} f' = \operatorname{Im} f$.

Demonstraţie. În Teorema 4.5.3 fie $g = p_\rho$. ■

Teorema 4.5.5 (prima teoremă de factorizare) *Dacă* $f : A \to B$ *este o funcţie, atunci există o unică funcţie bijectivă* $\bar{f} : A/\ker f \to \operatorname{Im} f$ *astfel încât diagrama de mai jos este comutativă, adică* $f = i \circ \bar{f} \circ p_{\ker f}$, *unde* $i : \operatorname{Im} f \to B, i(y) = y$. *Pentru orice* $x \in A$ *avem* $\bar{f}(\ker f\langle x\rangle) = f(x)$.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "p_{\ker f}"'] & B \\ A/\ker f \arrow[r, "\bar{f}"'] & \operatorname{Im} f \arrow[u, "i"'] \end{tikzcd}$$

Demonstraţie. Aplicăm Teorema 4.5.2 pentru funcţia $f : A \to B$ şi funcţia injectivă $g = i : \operatorname{Im} f \to B$. Are loc condiţia $\operatorname{Im} g = \operatorname{Im} f$, deci conform teoremei, există funcţia $h : A \to \operatorname{Im} f$ astfel încât $f = i \circ h$ şi $\ker h = \ker f$.

Acum aplicăm Corolarul 4.5.4 pentru funcţia h şi relaţia $\rho = \ker f \in \mathcal{E}(A)$. Deoarece $\ker f = \ker h$, există o funcţie $\bar{f} : A/\ker f \to \operatorname{Im} f$ astfel încât $h = \bar{f} \circ p_{\ker f}$; dar $\bar{f}$ este injectiv şi $\operatorname{Im} \bar{f} = \operatorname{Im} f$, adică $\bar{f}$ este surjectiv, deci este bijectiv.

Rezultă că $f = i \circ \bar{f} \circ p_{\ker f}$ şi $\bar{f}(\ker f\langle x\rangle) = f(x)$ pentru orice $x \in A$, de unde rezultă unicitatea lui $\bar{f}$. ■

Exerciţiul 79 Să se aplice prima teoremă de factorizare în următoarele cazuri:

a) $f, g : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, $g(x) = x^4$;

b) $f, g : \mathbb{C} \to \mathbb{C}$, $f(z) = z^2$, $g(z) = z^4$.

Exerciţiul 80 Fie A şi B mulţimi, ρ o relaţie de echivalenţă pe A şi $\sigma \in \mathcal{E}(B)$. Pe produsul cartezian $A \times B$ definim relaţia $\rho \times \sigma$ astfel: $(a, b)\rho \times \sigma(a', b') \Leftrightarrow a\rho a'$ şi $b\sigma b'$.

a) Să se arate că $\rho \times \sigma$ este relaţie de echivalenţă şi există funcţia bijectivă canonică

$$\varphi : A \times B/\rho \times \sigma \to A/\rho \times B/\sigma.$$

b) Dacă $f : A \to A'$ şi $g : B \to B'$ sunt funcţii, atunci $\ker(f \times g) = \ker f \times \ker g$ şi $\operatorname{Im}(f \times g) = \operatorname{Im} f \times \operatorname{Im} g$.

Exerciţiul 81 Fie A o mulţime şi fie $B \subseteq A$. Pe mulţimea părţilor $\mathcal{P}(A)$ definim relaţia ρ astfel: pentru orice $X, Y \in \mathcal{P}(A)$, $X\rho Y \Leftrightarrow X \cap B = Y \cap B$. Să se arate că ρ este relaţie de echivalenţă şi există funcţia bijectivă canonică $\varphi : \mathcal{P}(A)/\rho \to \mathcal{P}(B)$.

Exerciţiul 82 Fie A şi B mulţimi, $a_0 \in A$ şi fie $A' \subseteq A$. Pe mulţimea $\mathrm{Hom}(A, B)$ definim următoarele relaţii: pentru orice $f, g \in \mathrm{Hom}(A, B)$, $f\rho g \Leftrightarrow f(a_0) = g(a_0)$ şi $f\sigma g \Leftrightarrow f(x) = g(x)\ \forall\ x \in A'$. Să se arate că:

a) ρ este relaţie de echivalenţă şi există o funcţie bijectivă $\varphi : \mathrm{Hom}(A, B)/\rho \to B$;
b) σ este relaţie de echivalenţă şi există o funcţie bijectivă $\psi : \mathrm{Hom}(A, B)/\sigma \to \mathrm{Hom}(A', B)$;
c) Să observăm că a) precum şi exerciţiul anterior sunt cazuri particulare ale lui b).

Exerciţiul 83 Fie A şi B două mulţimi şi fie $\mathrm{Hom}_{\mathrm{surj}}(A, B) = \{f : A \to B \mid f \text{ este surjectiv}\}$. Considerăm funcţia $\varphi : \mathrm{Hom}_{\mathrm{surj}}(A, B) \to \mathcal{E}(A)$, $\varphi(f) = \ker f$. Să se arate că:

a) Dacă $f, g \in \mathrm{Hom}_{\mathrm{surj}}(A, B)$, atunci $f \ker \varphi g \Leftrightarrow \exists \alpha : B \to B$ funcţie bijectivă astfel încât $g = \alpha \circ f$;
b) $\mathrm{Im}\,\varphi = \{\rho \in \mathcal{E}(A) \mid \exists \alpha : A/\rho \to B$ funcţie bijectivă $\}$.

Teorema 4.5.6 (a doua teoremă de factorizare) *Fie o relaţie de echivalenţă pe A, $B \subseteq A$ şi fie $\sigma = (B \times B) \cap \rho$, $\tau = (\rho(B) \times \rho(B)) \cap \rho$, adică σ şi τ sunt restricţiile lui ρ la B, respectiv la $\rho(B)$.*

Atunci există o unică funcţie bijectivă $F : B/\sigma \to \rho(B)/\tau$ astfel încât a următoarea diagramă este comutativă, adică $p_\tau \circ i = F \circ p_\sigma$. Pentru orice $x \in B$ avem $F(\sigma\langle x\rangle) = \tau\langle x\rangle$.

$$\begin{tikzcd}
B \arrow[r, "i"] \arrow[d, "p_\sigma"'] & \rho(B) \arrow[d, "p_\tau"] \\
B/\sigma \arrow[r, "F"'] & \rho(B)/\tau
\end{tikzcd}$$

Demonstraţie. Avem $B \subseteq \rho(B)$ şi $i : B \to \rho(B)$, $i(b) = b$, pentru orice $b \in B$. Fie $f : B \to \rho(B)/\tau$, $f = p_\tau \circ i$, deci $f(x) = p_{\tau(x)} = \tau\langle x\rangle, \forall x \in B$. Funcţia f este surjectivă. Într-adevăr, $\forall \tau\langle y\rangle \in \rho(B)/\tau$, unde $y \in \rho(B) \Rightarrow \exists x \in B \subseteq \rho(B) :\ x\rho y \Rightarrow x\tau y$, deci $f(x) = \tau\langle x\rangle = \tau\langle y\rangle$. Deci $\mathrm{Im}\, f = \rho(B)/\tau$. Mai departe, pentru orice $x, y \in B$ avem

$$x \ker f y \Leftrightarrow f(x) = f(y) \Leftrightarrow \tau\langle x\rangle = \tau\langle y\rangle \Leftrightarrow x\tau y \Leftrightarrow x\sigma y.$$

Aplicăm Corolarul 4.5.4 funcţiei f şi relaţiei $\sigma = \ker f$. Rezultă că există o funcţie injectivă

$$F : B/\sigma \to \rho(B)/\tau, \qquad F(\sigma\langle x\rangle) = \tau\langle x\rangle$$

astfel încât $f = F \circ p_\sigma$ şi $\mathrm{Im}\, F = \mathrm{Im}\, f = \rho(B)/\tau$. Deci $F \circ p_\sigma = p_\tau \circ i$, F este bijectiv şi $F(\sigma\langle x\rangle) = \tau\langle x\rangle, \forall x \in B$, de unde rezultă unicitatea lui F. ∎

Exerciţiul 84 Fie $A = \mathbb{C}$, $B = \{x \in \mathbb{R} \mid x > 1\} \subseteq \mathbb{C}$, $\rho \subseteq A \times A$ şi $z\rho w \Leftrightarrow |z| = |w|$. Să se aplice a doua teoremă de factorizare şi să se reprezinte grafic funcţiile ce apar în diagramă.

Teorema 4.5.7 (a treia teoremă de factorizare) *Fie ρ şi σ două relaţii de echivalenţă pe mulţimea A astfel încât $\rho \subseteq \sigma$. Atunci există o unică funcţie surjectivă $g : A/\rho \to A/\sigma$ şi există o unică funcţie bijectivă $\bar{g} : (A/\rho)/(\sigma/\rho) \to A/\sigma$, unde $\sigma/\rho = \ker g$, astfel încât a următoarea diagramă este comutativă:*

$$\begin{tikzcd}
A \arrow[r, "p_\rho"] \arrow[dr, "p_\sigma"'] & A/\rho \arrow[r, "p_{\sigma/\rho}"] \arrow[d, dotted, "g"] & \frac{A/\rho}{\sigma/\rho} \arrow[dl, dotted, "\bar{g}"] \\
 & A/\sigma &
\end{tikzcd}$$

Demonstraţie. Aplicăm de două ori Corolarul 4.5.4 întâi pentru p_σ, apoi pentru g. ∎

Exerciţiul 85 Să se aplice a treia teoremă de factorizare în următoarele cazuri:

a) $A = \{1, 2, 3, 4, 5\}$, $\rho_1 = \Delta_A \cup \{(1, 2), (2, 1)\}$ şi $\rho_2 = \rho_1 \cup \{(1, 3), (3, 1), (2, 3), (3, 2), (4, 5), (5, 4)\}$.
b) $A = \mathbb{Z}$, $\rho_1 = \equiv \pmod 4$ şi $\rho_2 = \equiv \pmod 2$.
c) $A = \mathbb{Z}$, $\rho_1 = \equiv \pmod 9$ şi $\rho_2 = \equiv \pmod 3$.

Capitolul 5

MULŢIMI ORDONATE

Noţiunea de mulţime ordonată formalizează şi generalizează ideea intuitivă de ordonare, aranjare sau înşiruire a obiectelor unei colecţii.

5.1 Relaţii de ordine

Fie $\rho = (A, A, R)$ o relaţie omogenă. Amintim că ρ este **relaţie de ordine** şi (A, ρ) este **mulţime ordonată** dacă ρ este reflexiv, tranzitiv şi antisimetric. Dacă ρ este o relaţie de ordine, atunci în loc de $x\rho y$ deseori notăm $x \leq y$. Notăm $\mathcal{O}(A) = \{\rho = (A, A, R) \mid \rho \text{ relaţie de ordine }\}$ mulţimea relaţiilor de ordine pe A.

Amintim că ρ este **relaţie de ordine strictă** dacă ρ este ireflexiv şi tranzitiv. Notaţii: $x < y$, dacă $x \leq y$ şi $x \neq y$ (strict mai mic); $x > y$, dacă $y < x$ etc.

Definiţia 5.1.1 Spunem că (A, ρ) este **mulţime total ordonată** (sau **lanţ**) dacă :

$$\text{pentru orice } \ x, y \in A \ \text{ are loc } \ x\rho y \ \text{ sau } \ y\rho x$$

(altfel spus, $\rho \cup \rho^{-1} = A \times A$ este relaţia universală, adică orice două elemente ale lui A sunt **comparabile** relativ la relaţia ρ).

Exemplul 5.1.2 1) $(\mathbb{N}, \leq), (\mathbb{Z}, \leq), (\mathbb{Q}, \leq), (\mathbb{R}, \leq)$ sunt mulţimi total ordonate.

2) $(\mathbb{N}, |)$, (unde „|” este relaţia de divizibilitate) este mulţime ordonată şi nu e total ordonată, pentru că de exemplu 2 şi 3 nu sunt comparabile.

3) Dacă A este o mulţime, atunci $(\mathcal{P}(A), \subseteq)$ este mulţime ordonată. Dacă A are mai mult de un element, atunci $(\mathcal{P}(A), \subseteq)$ nu e total ordonată.

4) Dacă (A, ρ) este o mulţime ordonată (total ordonată) şi $B \subseteq A$, atunci $(B, \rho \cap (B \times B))$ este ordonată (total ordonată).

Exerciţiul 86 Fie $A \neq \emptyset$ şi fie $\rho, \rho' \in \mathcal{O}(A)$. Să se arate că:

a) $\rho \cap \rho', \rho^{-1} \in \mathcal{O}(A)$.

b) $\complement\rho \notin \mathcal{O}(A)$.

c) În general $\rho \cup \rho' \notin \mathcal{O}(A)$.

d) Dacă σ este o relaţie de ordine strictă pe A, atunci σ este asimetric, iar $\sigma \cup 1_A \in \mathcal{O}(A)$.

e) $\sigma := \rho \setminus 1_A$ este relaţie de ordine strictă pe A.

f) Relaţia de ordine ρ este totală $\Longleftrightarrow$ ρ satisface proprietatea de **trihotomie**, adică pentru orice $x, y \in A$, exact una din următoarele trei afirmaţii este adevărată: (1) $a\sigma b$; (2) $a = b$; (3) $a\sigma^{-1}b$.

O mulţime ordonată finită poate fi reprezentată grafic cu ajutorul unei **diagrame Hasse**, conform următoarei reguli: dacă $x < y$ şi dacă nu există $z \in A$ astfel încât $x < z < y$, atunci aşezăm punctul y mai sus decât punctul x şi le unim cu un segment.

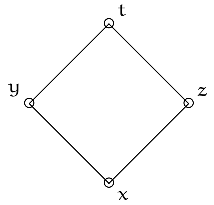
Exemplul 5.1.3 Fie $A = \{x, y, z, t\}$ şi considerăm relaţiile de ordine pe mulţimea A având graficele

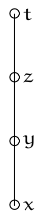
$$R = \{(x, x), (y, y), (z, z), (t, t), (x, y), (x, z), (x, t),\ (y, t), (z, t)\},$$

respectiv

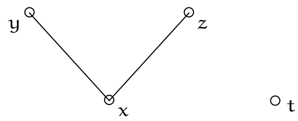
$$R = \{(x, x), (y, y), (z, z), (t, t), (x, y), (x, z), (x, t), (y, z),\ (y, t), (z, t)\}.$$

Atunci diagramele Hasse sunt:





În următoarea diagramă $x < y, x < z$, y şi z nu sunt comparabile, mai departe t nu e comparabil cu x, y, z.



Exerciţiul 87 Să se întocmească diagramele Hasse ale următoarelor mulţimi ordonate:
a) $(\mathcal{P}(\{a, b, c, d\}), \subseteq)$;
b) Mulţimea divizorilor lui 60, ordonată de relaţia de divizibilitate;
c) Mulţimea partiţiilor mulţimii $\{a, b, c, d\}$, ordonată de relaţia ,,mai fin" $\preccurlyeq$.

Definiţia 5.1.4 Fie $(A, \leq)$ şi $(B, \leq)$ două mulţimi ordonate şi $f : A \to B$ o funcţie.
a) Spunem că f este **crescător** (**descrescător**), dacă pentru orice $x, y \in A$,

$$x \leq y \Rightarrow f(x) \leq f(y) \qquad (f(y \leq f(x));$$

mai departe f este **izomorfism de ordine** (sau **asemănare**), dacă f este crescător, bijectiv şi f^{-1} este crescător;

Exemplul 5.1.5 1) Mulţimile ordonate $\mathbb{N} = \{1, 2, 3, \dots\}$ şi $2\mathbb{N} = \{2, 4, 6, \dots\}$ sunt asemenea, pentru că $f : \mathbb{N} \to 2\mathbb{N}$, $f(n) = 2n$ este o asemănare.
2) Mulţimile ordonate $(\mathbb{N}, |)$ şi $(\mathbb{N}, \leq)$ nu sunt asemenea. Într-adevăr, dacă ar exista o asemănare $f : (\mathbb{N}, |) \to (\mathbb{N}, \leq)$, atunci fie $f(2) = n$ şi $f(3) = m$, unde $n \neq m$. Dacă $n < m$, atunci $f^{-1}(n) = 2|3 = f^{-1}(m)$, iar dacă $m < n$, atunci $f^{-1}(m) = 3|2 = f^{-1}(n)$, deci avem contradicţie în ambele cazuri.

Exerciţiul 88 Să se determine toate relaţiile de ordine pe mulţimea $A = \{a, b, c\}$ (folosind diagrame Hasse). Să se împartă aceste ordonări în clase de asemănare.

Exerciţiul 89 Fie $(A, \leq)$, $(B, \leq)$ şi $(C, \leq)$ mulţimi ordonate şi fie $f : A \to B$, $g : B \to C$ două funcţii.
a) Dacă f şi g sunt crescătoare (descrescătoare), atunci $g \circ f$ este funcţie crescătoare.
b) Dacă f este crescătoare (descrescătoare) şi g este descrescătoare (crescătoare), atunci $g \circ f$ este descrescătoare.

Exerciţiul 90 Fie $(A, \leq)$ şi $(B, \leq)$ mulţimi ordonate şi $f : A \to B$ funcţie bijectivă şi crescătoare.
a) Dacă A este total ordonată, atunci f^{-1} este crescătoare şi B este total ordonată.
b) Să se arate că $\mathbf{1}_{\mathbb{N}^*} : (\mathbb{N}^*, |) \to (\mathbb{N}^*, \leq)$ este bijectivă, crescătoare şi nu e izomorfism de ordine.

Exerciţiul 91 Fie $(A, \leq)$ şi $(B, \leq)$ mulţimi ordonate şi fie $f : A \to B$, $g : B \to A$ funcţii crescătoare. Fie $M = \{a \in A \mid g(f(a)) = a\}$ şi $N = \{b \in B \mid f(g(b)) = b\}$.
Să se arate că $(M, \leq) \simeq (N, \leq)$.

Teorema 5.1.6 (preordine, echivalenţă şi ordine) *Fie* $\rho = (A, A, R)$ *o relaţie de preordine şi fie* $\sigma = \rho \cap \rho^{-1}$. *Atunci:*
1) σ *este relaţie de echivalenţă pe* A*;*
2) *pe mulţimea factor* A/σ *definim relaţia ,,*$\leq$*" prin:* $\sigma\langle x \rangle \leq \sigma\langle y \rangle \Leftrightarrow x\rho y$. *Atunci* $(A/\sigma, \leq)$ *mulţime ordonată.*

Demonstraţie. 1) Relaţia σ este reflexivă (evident), tranzitivă: $\forall x, y, z \in A : x\sigma y$ şi $y\sigma z \Rightarrow x(\rho \cap \rho^{-1})y$ şi $y(\rho \cap \rho^{-1})z \Rightarrow (x\rho y$ şi $x\rho^{-1}y)$ şi $(y\rho z$ şi $y\rho^{-1}z) \Rightarrow (x\rho y$ şi $y\rho z)$ şi $(x\rho^{-1}y$ şi $y\rho^{-1}z) \Rightarrow x\rho z$ şi $x\rho^{-1}z$ (pentru că ρ şi ρ^{-1} sunt tranzitive) $\Rightarrow x(\rho \cap \rho^{-1})z \Rightarrow x\sigma z$, şi simetrică: $\forall x, y \in A : x\sigma y \Rightarrow x(\rho \cap \rho^{-1})y \Rightarrow x\rho y$ şi $x\rho^{-1}y \Rightarrow y\rho x$ şi $y\rho^{-1}x \Rightarrow y(\rho \cap \rho^{-1})x \Rightarrow y\sigma x$.
2) Definiţia relaţiei $\leq$ nu depinde de alegerea reprezentanţilor x şi y: dacă $\sigma\langle x \rangle = \sigma\langle x' \rangle$, $\sigma\langle y \rangle = \sigma\langle y' \rangle$ şi dacă $x\rho y$, atunci $x'\rho y'$. Într-adevăr, pe baza ipotezelor avem: $x\sigma x'$ şi $y\sigma y'$ şi $x\rho y \Rightarrow (x\rho x'$ şi $x\rho^{-1}x')$ şi $(y\rho y'$ şi $y\rho^{-1}y')$ şi $x\rho y \Rightarrow x'\rho x$ şi $x\rho y$ şi $y\rho y' \Rightarrow x'\rho y'$ (pentru că ρ este tranzitiv).
Relaţia $\leq$ este reflexivă, tranzitivă şi antisimetrică. Verificăm ultima proprietate. Pentru orice $\sigma\langle x \rangle, \sigma\langle y \rangle \in A/\sigma$, $\sigma\langle x \rangle \leq \sigma\langle y \rangle$ şi $\sigma\langle y \rangle \leq \sigma\langle x \rangle \Rightarrow x\rho y$ şi $y\rho x \Rightarrow x\rho y$ şi $x\rho^{-1}y \Rightarrow x(\rho \cap \rho^{-1})y \Rightarrow x\sigma y \Rightarrow \sigma\langle x \rangle = \sigma\langle y \rangle$. ∎

Exercițiul 92 Să se aplice Teorema 5.1.6 în cazul mulţimii preordonate $(\mathbb{Z}, |)$.

Definiţia 5.1.7 Fie $(A, \leq)$ o mulţime ordonată şi fie $x \in A$. Spunem că x este **cel mai mic element** sau **minimum** (*cel mai mare element* sau **maximum**) al lui A dacă pentru orice $a \in A$, $x \leq a$ (respectiv pentru orice $a \in A$, $a \leq x$).

Notaţie: $x = \min A$ (respectiv $x = \max A$).

Observaţii 5.1.8 Dacă există cel mai mic element (cel mai mare element), atunci el este unic. Într-adevăr, dacă de exemplu x şi x' sunt ambele cele mai mic elemente, atunci $x \leq x'$ (pentru că x este cel mai mic element) şi $x' \leq x$ (pentru că x' este cel mai mic element), astfel din antisimetrie avem $x = x'$.

Exemplul 5.1.9 1) În $(\mathbb{N}, \leq)$ $x = 0$ este cel mai mic element şi nu există cel mai mare element.

2) În $(\mathbb{N}, |)$ 1 este cel mai mic element şi a 0 este cel mai mare element, pentru că $1|a$ şi $a|0$ pentru orice $a \in \mathbb{N}$.

3) În $(\mathbb{N} \setminus \{0, 1\}, |)$ nu există cel mai mic element şi nu există cel mai mare element.

4) În $(\mathcal{P}(A), \subseteq)$ $\min \mathcal{P}(A) = \emptyset$ şi $\max \mathcal{P}(A) = A$.

Definiţia 5.1.10 În mulţimea ordonată $(A, \leq)$ x este **element minimal** (**element maximal**), dacă $\forall a \in A : a \leq x \Rightarrow a = x$ (respectiv $\forall a \in A : x \leq a \Rightarrow a = x$). Altfel spus, $x \in A$ este element minimal (element maximal), dacă A nu are niciun element a astfel încât $a < x$ (respectiv $a > x$).

Exemplul 5.1.11 1) În $(\mathbb{N}, \leq)$, numărul 0 este element minimal şi nu există elemente maximale.

2) În $(\mathbb{N}, |)$, numărul 1 este element minimal şi 0 este element maximal.

3) În $(\mathbb{N} \setminus \{0, 1\}, |)$ numerele prime sunt elemente minimale şi nu există elemente maximale.

4) Din definiţii este evident că dacă există cel mai mic (cel mai mare) element, atunci el este unicul element minimal (maximal). Afirmaţia reciprocă nu e adevărată; de exemplu dacă $A = \{2^k \mid k \in \mathbb{N}\} \cup \{3, 9\}$, atunci în mulţimea ordonată $(A, |)$ $a = 9$ este unicul element maximal şi nu există cel mai mare element.

5) Dacă $(A, \leq)$ este o mulţime total ordonată, atunci noţiunile de element minimal (element maximal) şi cel mai mic element (respectiv cel mai mare element) sunt echivalente.

Exerciţiul 93 Fie $(A, \leq)$ o mulţime ordonată. Să se arate că dacă există $a = \min A$, atunci a este unicul element minimal al lui A, iar afirmaţia reciprocă nu e adevărată.

5.2 Latici

Definiţia 5.2.1 Fie $(A, \leq)$ o mulţime ordonată, $x \in A$ şi fie $B \subseteq A$.

a) Spunem că x este **minorant** (**majorant**) al lui B, dacă pentru orice $b \in B$ avem $x \leq b$ (respectiv pentru orice $b \in B$ avem $b \leq x$).

b) Spunem că x este **infimum** sau (respectiv **supremum**) al lui B, dacă x este *cel mai mare minorant* al lui B (respectiv x este *cel mai mic majorant* al lui B). Notaţie: $x = \inf B$ sau $x = \inf_A B$ (respectiv $x = \sup B$ sau $x = \sup_A B$).

Exemplul 5.2.2 1) În $(\mathbb{N} \setminus \{0, 1\}, |)$, submulţimea $B = \{2k + 1 \mid k \in \mathbb{N}\}$ are un unic minorant, pe $x = 1$, deci $\inf B = 1$; mai departe, B nu are majoranţi şi nu are supremum.

2) În $(\mathbb{R}, \leq)$ intervalul $B = (1, 3]$ are ca minorant orice $x \leq 1$ şi majorant orice $x \geq 3$; mai departe, $\inf B = 1 \notin B$, $\sup B = 3 \in B$.

3) Dacă $(A, \leq)$ este o mulţime ordonată, atunci orice element al lui A este minorant şi majorant al lui $B = \emptyset$. Mai departe $\exists \inf \emptyset \Leftrightarrow \exists \max A \Leftrightarrow \exists \sup A$, $\exists \sup \emptyset \Leftrightarrow \exists \min A \Leftrightarrow \exists \inf A$ şi atunci $\inf \emptyset = \max A = \sup A$, $\sup \emptyset = \min A = \inf A$.

4) Orice submulţime $B \subseteq A$ are cel mult un infimum şi cel mult un supremum; mai departe, dacă B are minorant x (majorant y) ce aparţine lui B, atunci $x = \inf B$ (respectiv $y = \sup B$).

Exerciţiul 94 Fie $(A, \leq)$ o mulţime ordonată şi fie $X \subseteq B \subseteq A$.

a) Dacă există $\inf_B X$ şi $\inf_A X$, atunci $\inf_B X \geq \inf_A X$.

b) Dacă există $\sup_B X$ şi $\sup_A X$, atunci $\sup_B X \leq \sup_A X$.

Definiţia 5.2.3 a) Mulţimea ordonată $(A, \leq)$ se numeşte **latice**, dacă orice submulţime cu două elemente a lui A are infimum şi supremum (pentru orice $a, b \in A$, $a \neq b$, $\exists \inf\{a, b\}$ şi $\exists \sup\{a, b\}$).

b) $(A, \leq)$ este **latice completă**, dacă orice submulţime a lui A are infimum şi supremum (pentru orice $B \subseteq A$, $\exists \inf B$ şi $\exists \sup B$).

Exemplul 5.2.4 1) $(\mathbb{N}, |)$ este latice. Într-adevăr, pentru orice $a, b \in \mathbb{N}$, $\inf\{a, b\} = \text{cmmdc}(a, b)$ iar $\sup\{a, b\} = \text{cmmmc}(a, b)$.

2) Dacă $(A, \leq)$ este total ordonată, atunci $(A, \leq)$ este latice: $\forall a, b \in A : \inf\{a, b\} = \min\{a, b\}$ şi $\sup\{a, b\} = \max\{a, b\}$.

3) $(\mathbb{R}, \leq)$ nu e latice completă, pentru că de exemplu a $B = (-\infty, 0)$ nu are minorant deci nu are supremum în $(\mathbb{R}, \leq)$.

4) $(\mathcal{P}(A), \subseteq)$ este latice completă. Dacă $X = \{X_i \mid i \in I\} \subseteq \mathcal{P}(A)$, atunci $\inf X = \bigcap_{i \in I} X_i$ şi $\sup X = \bigcup_{i \in I} X_i$.

Exerciţiul 95 Să se determine, abstracţie făcând de izomorfisme (asemănări), toate laticile cu 1, 2, 3, 4, 5 şi respectiv 6 elemente (folosind diagrame Hasse).

Exerciţiul 96 Fie A o mulţime şi $(B, \leq)$ o mulţime ordonată. Pe mulţimea $\text{Hom}(A, B)$ definim următoarea relaţie: $f \leq g \iff f(a) \leq g(a)$ pentru orice $a \in A$.

Să se arate că:

a) ,,$\leq$" este relaţie de ordine.

b) Dacă B este latice, atunci şi $\text{Hom}(A, B)$ este latice.

Teorema 5.2.5 (caracterizarea laticilor complete) *Fie* $(A, \leq)$ *o mulţime ordonată. Următoarele afirmaţii sunt echivalente:*

(i) $(A, \leq)$ *este latice completă;*

(ii) *orice submulţime a lui* A *are infimum;*

(iii) *orice submulţime a lui* A *are supremum.*

Demonstraţie. (i) $\Rightarrow$ (ii) şi (i) $\Rightarrow$ (iii) sunt evidente din definiţie.

(ii) $\Rightarrow$ (i) Trebuie să arătăm că orice submulţime B a lui A are supremum. Notăm cu C mulţimea majoranţilor lui B. Avem $C \neq \emptyset$, pentru că conform lui (ii), există $\inf \emptyset = \max A \in C$. Fie $x = \inf C$, care există conform ipotezei. Arătăm că $x = \sup B$. Într-adevăr, pentru orice $b \in B$ şi $c \in C$ avem $b \leq c$ (din definiţia lui C), deci orice $b \in B$ este minorant al lui C; rezultă că $\forall b \in B : b \leq x$ (pentru că $x = \inf C$), deci x este majorant al lui B.

Mai departe, fie $x' \in A$ un majorant al lui B, adică avem $b \leq x', \forall b \in B$. Atunci $x' \in C$ (conform definiţiei lui C), de unde $x \leq x'$ (pentru că $x = \inf C$), deci x este cel mai mic majorant al lui B, adică $x = \sup B$.

Similar se arată că (iii) $\Rightarrow$ (i). ∎

Exerciţiul 97 Fie $(A, \leq)$ o latice completă şi fie $f : A \to A$ o funcţie crescătoare. Să se arate că există $a \in A$ astfel încât $f(a) = a$. (Spunem că a este **punct fix** al lui f.)

5.3 Mulţimi bine ordonate şi mulţimi artiniene

Definiţia 5.3.1 Fie $(A, \leq)$ o mulţime ordonată. Spunem că A este **bine ordonată** dacă orice submulţime nevidă a lui A are cel mai mic element (adică, pentru orice $B \subseteq A, B \neq \emptyset$, $\exists \min B \in B$).

Exemplul 5.3.2 a) $(\mathbb{N}, \leq)$ mulţime bine ordonată.

b) Dacă $(A, \leq)$ este bine ordonată, atunci $(A, \leq)$ este total ordonată. Invers nu e adevărat, de exemplu $(\mathbb{R}, \leq)$ nu e bine ordonată, pentru că de exemplu intervalul $(0, 1)$ nu are cel mai mic element. De asemenea, $(\mathbb{Z}, \leq)$ este total ordonată dar nu e bine ordonată.

c) Orice mulţime finită total ordonată bine ordonată.

Într-adevăr, trebuie să arătăm că $\forall\ B \subseteq A,\ B \neq \varnothing,\ \exists\ \min B$. Fie $B \subseteq A$, $B \neq \varnothing$. Deoarece A finită $\Rightarrow$ B este finită, deci fie $B = \{b_1, b_2, \ldots, b_n\}$. Deoarece $(A, \leq)$ este total ordonată, rezultă că orice două elemente din A (deci şi din B) sunt comparabile. Comparăm primele două elemente ale lui B, păstrăm pe cel mai mic dintre ele, şi apoi îl comparăm cu al treilea element al lui B şi păstrăm pe cel mai mic dintre ele. Continuând, prin inducţie, după n paşi am găsit elementul $\min B$.

Următoarea teoremă arată că pe mulţimile bine ordonate se poate aplica metoda inducţiei matematice.

Teorema 5.3.3 (caracterizarea mulţimilor bine ordonate) *Dacă* $(A, \leq)$ *este o mulţime ordonată nevidă, atunci următoarele afirmaţii sunt echivalente:*

(i) $(A, \leq)$ *este bine ordonată,*

(ii) A *este total ordonată, există* $a_0 = \min A$ *şi pentru orice* $B \subseteq A$, *dacă* B *satisface proprietăţile:*

a) $a_0 \in B$,

b) *pentru orice* $a \in A$, $\{x \in A \mid x < a\} \subseteq B \Rightarrow a \in B$,

atunci $B = A$.

Demonstraţie. (i) $\Rightarrow$ (ii) Presupunem că $(A, \leq)$ este bine ordonată. Atunci A este total ordonată, şi există $a_0 = \min A$. Presupunem că a doua condiţie din (ii) nu e adevărată, adică există $B \subseteq A$, astfel încât au loc a) şi b) şi $B \neq A$.

Deci $A \setminus B \neq \emptyset$ şi din ipoteză există $x = \min A \setminus B$. Aici $x \in A \setminus B$, adică $x \notin B$. Mai departe $\forall y \in A : y < x \Rightarrow y \in B$ (pentru că dacă $y \in A \setminus B$, atunci contrazice definiţia lui x), deci $\{y \in A \mid y < x\} \subseteq B$, şi de aici $x \in B$, conform lui b), ceea ce e o contradicţie.

(ii) $\Rightarrow$ (i) Presupunem că (ii) este adevărat şi presupunem prin absurd că A nu e bine ordonată, adică există $B \subseteq A, B \neq \emptyset$, care nu are cel mai mic element. Atunci

α) $a_0 \in A \setminus B$, pentru că dacă $a_0 = \min A \in B$, atunci $a_0 = \min B$, contradicţie.

β) Pentru orice $a \in A$, $\{x \in A \mid x < a\} \subseteq A \setminus B \Rightarrow a \in A \setminus B$. Într-adevăr, dacă nu ar fi aşa, atunci $a \in B$, şi deoarece A este total ordonată, elementele x mai mici ca a sunt în $A \setminus B$, deci obţinem că $a = \min B$, contradicţie.

Din α şi β deducem că submulţimea $A \setminus B$ satisface ipotezele a) şi b, şi astfel $A \setminus B = A$, adică $B = \emptyset$, contradicţie. ■

Corolar 5.3.4 *Fie* $(A, \leq)$ *o mulţime nevidă bine ordonată,* $a_0 = \min A$ *şi fie* P *un predicat de o variabilă definită pe* A*. Presupunem că*

1. $P(a_0)$ *este adevărat,*
2. *Pentru orice* $a \in A$*, dacă* $P(x)$ *este adevărat pentru orice* $x < a$*, atunci* $P(a)$ *este adevărat.*

Atunci $P(a)$ *este adevărat pentru orice* $a \in A$.

Demonstraţie. Fie

$$B = \{a \in A \mid P(a) \text{ este adevărat}\} \subseteq A,$$

care satisface ipotezele a) şi b) ale teoremei precedente, deci $B = A$. ■

Exerciţiul 98 a) Să se arate că:

1) Dacă $(A, \leq)$ este o mulţime bine ordonată şi $f : A \to A$ este o aplicaţie strict crescătoare, atunci pentru orice $a \in A$ avem $a \leq f(a)$.

2) Între două mulţimi bine ordonate există cel mult un izomorfism.

Următoarea teoremă generalizează Teorema 5.3.3 la cazul mulţimilor care nu sunt total ordonate.

Definiţia 5.3.5 O mulţime ordonată $(A, \leq)$ se numeşte **artiniană** sau **bine fondată** dacă satisface condiţiile echivalete de mai jos.

Noţiunea duală este cea de **mulţime noetheriană**.

Teorema 5.3.6 (caracterizarea mulţimilor artiniene) *Fie* $(A, \leq)$ *o mulţime ordonată. Următoarele afirmaţii sunt echivalente:*

(i) **(condiţia minimalităţii)** *Orice submulţime nevidă* $B \subseteq A$ *are elemente minimale.*

(ii) **(condiţia inductivităţii)** *Pentru orice* $B \subseteq A$*, dacă* B *satisface proprietăţile:*

(1) B *conţine toate elementele minimale ale lui* A*;*

(2) *dacă* $a \in A$ *şi* $\{x \in A \mid x < a\} \subseteq B$*, atunci* $a \in B$*,*

atunci $B = A$.

(iii) **(condiţia lanţurilor descrescătoare)** *Orice şir strict descrescător* $a_1 > a_2 > \cdots > a_n > \cdots$ *de elemente din* A *este finit.*

Demonstraţie. (i)$\Rightarrow$(ii). Presupunem că $B \subsetneq A$ satisface condiţiile (1) şi (2), dar $B \neq A$. Fie $x \in A \setminus B$ un element minimal. Atunci x nu e minimal în A, pentru că B conţine toate elementele minimale ale lui. Din minimalitatea lui x rezultă că dacă $y \in A$, $y < x$, atunci $y \in B$. Atunci din (2) rezultă că $x \in B$, contradicţie.

(ii)$\Rightarrow$(iii). Considerăm mulţimea

$$B := \{a \in A \mid \text{pentru orice şir finit } \ a > a_1 > a_2 > \dots\}.$$

Dacă $a \in A$ este un element minimal, atunci e evident, că $a \in B$. Fie $b \in A$ astfel încât orice $x \in A$ cu $x < b$ aparţine lui B. Atunci avem $b \in B$, deci $B = A$.

(iii)$\Rightarrow$(i). Presupunem că $B \subseteq A$, $B \neq \emptyset$, şi că B nu conţine elemente minimale. Atunci pentru orice $a_1 \in B$, există $a_2 \in B$, $a_2 < a_1$, şi prin inducţie construim un şir strict descrescător $a_1 > a_2 > \cdots > a_n > \cdots$, ceea ce contrazice ipoteza. ■

Exemplul 5.3.7 O mulţime total ordonată artiniană este bine ordonată. Dăm câteva exemple de mulţimi artiniene care nu sunt bine ordonate.

1) Mulţimea $(\mathbb{N}, |)$ a numerelor naturale ordonată de relaţia de divizibilitate.

2) Mulţimea $(\mathcal{P}_f(M), \subseteq)$ a submulţimilor finite ale unei mulţimi M.

3) Mulţimea $(\mathbb{N} \times \mathbb{N}, \leq)$ a perechilor de numere naturale, unde $(a, b) \leq (a', b') \Leftrightarrow a \leq a'$ şi $b \leq b'$.

4) Mulţimea $M^{(\mathbb{N})}$ a şirurilor finite de elemente din mulţimea M, unde $s \leq s' \Leftrightarrow s$ este subşir al şirului s'.

5.4 Axioma alegerii

De multe ori în matematică ne întâlnim cu propoziţia: ,,alegem un element din mulţimea ...” sau mai precis:

(A_0) Pentru orice mulţime $X \neq \emptyset$ există un element $x \in X$, deci $\{x\} \subseteq X$.

Aceasta este cea mai simplă formulare a axiomei alegerii. La prima vedere, propoziţia (A_0) pare evidentă, pentru că $X \neq \emptyset$ înseamnă că există cel puţin un element $x \in X$. Se pune însă întrebarea ce înseamnă expresia ,,există un element $x \in X$”. Să dăm două exemple:

a) Fie $f : [a, b] \to \mathbb{R}$ o funcţie continuă astfel încât $f(a) \cdot f(b) \leqslant 0$. Definim mulţimea

$$X = \{x \in [a, b] \mid f(x) = 0\}.$$

Teorema lui Darboux arată că există $x_0 \in [a, b]$ astfel încât $f(x_0) = 0$. Una din demonstraţiile teoremei dă o metodă care determină cea mai mică valoare $x_0 \in [a, b]$ astfel încât $f(x_0) = 0$.

b) Fie $P(x)$ polinom cu coeficienţi complecşi. Considerăm mulţimea

$$X = \{x \mid x \text{ număr complex astfel ca } P(x) = 0\}.$$

Teorema lui Gauss-d’Alembert afirmă că mulţimea X este nevidă şi finită, dar nicio demonstraţie nu dă o metodă de a găsi rădăcinile unui polinom arbitrar. Teorema este una de existenţă pură.

În aceste exemple, vedem că expresia ,,există un element $x \in X$” are un sens restrâns (se dă o metodă pentru găsirea elementului x) şi un sens larg.

5.4.1 *Forma generală a axiomei alegerii este următoarea:*

(A) *Fie $F \neq \emptyset$ o mulţime de mulţimi nevide disjuncte două câte două. Atunci există o mulţime A cu următoarele proprietăţi:*

(1) $A \subseteq \bigcup_{X \in F} X$*;*

(2) pentru orice $X \in F$, $A \bigcap X$ conţine exact un element.

Mulţimea A se numeşte **mulţime selectivă** pentru F. Observăm că **(A_0)** este caz particular al lui (A).

Axioma alegerii a fost formulată de Ernst Zermelo în 1904. Ea este independentă de celelalte axiome, şi are diferite formulări echivalente, după cum vom vedea mai jos. Considerând teoria mulţimilor fără axioma alegerii şi privind aceast enunţ ca o formulă închisă, Kurt Gödel a construit un model pentru teoria mulţimilor în care axioma alegerii este adevărată. Pe de altă parte, Paul Cohen a construit în 1963 un alt model pentru teoria mulţimilor în care axioma alegerii nu este adevărată. Altfel spus, teoria mulţimilor fără axioma alegerii este nedecidabilă.

Multe rezultate din matematică folosesc efectiv axioma alegerii, adică nu s-au descoperit demonstraţii care să nu facă apel la ea. Deoarece axioma alegerii duce la unele rezultate surprinzătoare (de exemplu, paradoxurile lui Hausdorff, Banach-Tarski, von Neumann), există în matematică orientări filozofice ,,constructiviste” care evită utilizarea ei.

Teorema 5.4.2 *Următoarele afirmaţii sunt echivalente:*

1) *Axioma alegerii* **(A)**.

2) *Pentru orice mulţime nevidă F de mulţimi nevide există o funcţie $f : F \to \bigcup_{X \in F} X$ astfel încât $f(X) \in X$ pentru orice $X \in F$.*

3) *Pentru orice mulţime $X \neq \emptyset$ există o funcţie $f : \mathcal{P}(X) \setminus \{\emptyset\} \to X$ astfel încât pentru orice $A \in \mathcal{P}(X) \setminus \{\emptyset\}$,* $f(A) \in A$ (f se numeşte **funcţie selectivă**).

4) *Dacă $(X_i)_{i \in I}$ este o familie de mulţimi astfel încât $I \neq \emptyset$ şi $X_i \neq \emptyset$ pentru orice $i \in I$, atunci produsul direct $\prod_{i \in I} X_i$ este nevid (adică, există o funcţie $f : I \to \bigcup_{i \in I} X_i$ astfel încât pentru orice $i \in I$ avem $f(i) \in X_i$).*

5) **(Lema lui Zorn)** *Fie $(A, \leq)$ o mulţime nevidă ordonată. Dacă orice lanţ (submulţime total ordonată) $L \subseteq A$ are majorant, atunci pentru orice $a \in A$ există un element maximal $m \in A$ astfel ca $a \leq m$.*

6) **(Axioma lui Hausdorff)** *Dacă $(A, \leq)$ este o mulţime ordonată şi $L \subseteq A$ este un lanţ, atunci există un lanţ maximal $L' \subseteq A$ astfel ca $L \subseteq L'$.*

7) **(Teorema lui Zermelo)** *Pentru orice mulţime A, există o relaţie de ordine ,,$\leq$” astfel ca $(A, \leq)$ este mulţime bine ordonată.*

8) *Orice funcţie surjectivă are cel puţin o secţiune (inversă la dreapta).*

Exerciţiul 99 Fie A o mulţime şi considerăm mulţimea ordonată $(\mathcal{O}(A), \subseteq)$ a relaţiilor de ordine pe A. Folosind lema lui Zorn, să se demonstreze:

a) ρ este element maximal al lui $\mathcal{O}(A)$ dacă şi numai dacă ρ este ordonare totală.

b) Pentru orice $\rho \in \mathcal{O}(A)$ există o ordonare totală $\bar{\rho} \in \mathcal{O}(A)$ astfel încât $\rho \subseteq \bar{\rho}$.

Exerciţiul 100 Spunem că o mulţime $\mathcal{F}$ de mulţimi *este de caracter finit* dacă satisface următoarea proprietate:

(*) Dacă A este o mulţime, atunci $A \in \mathcal{F}$, dacă şi numai dacă orice submulţime finită a lui A aparţine lui $\mathcal{F}$.

Folosind lema lui Zorn, să se demonstreze:

a) Dacă $\mathcal{F}$ este de caracter finit şi $A \in \mathcal{F}$, atunci orice submulţime a lui A aparţine lui $\mathcal{F}$

b) **(Lema lui Tukey)** Orice mulţime nevidă $\mathcal{F}$ de mulţimi de caracter finit are cel puţin un element maximal relativ la incluziune.

Capitolul 6

LATICI ŞI ALGEBRE BOOLE

6.1 Laticea ca structură algebrică

În capitolul anterior am definit laticea ca fiind o mulţime ordonată cu proprietăţi adiţionale. Existenţa infimumului şi a supremumului a oricărei perechi de elemente permite definirea a două operaţii pe mulţimea respectivă.

Definiţia 6.1.1 a) Structura algebrică $(A, \wedge, \vee)$ cu două operaţii binare ,,$\wedge$" şi ,,$\vee$" se numeşte **latice**, dacă sunt satisfăcute axiomele:

1. ambele operaţii sunt asociative,

2. ambele operaţii sunt comutative,

3. pentru orice $x, y \in A$ avem $x \wedge (x \vee y) = x$ şi $x \vee (x \wedge y) = x$ (**absorbţie**).

b) Spunem ca A are **element unitate** 1, dacă 1 este element neutru faţă de $\wedge$, adică $x \wedge 1 = x$ pentru orice $x \in A$. Spunem ca A are **element nul** 0, dacă 0 este element neutru faţă de $\vee$, adică $x \vee 0 = x$ pentru orice $x \in A$.

b) Fie $(A, \wedge, \vee)$ şi $(A', \wedge, \vee)$ latici. Funcţia $f : A \to A'$ se numeşte **morfism de latici** dacă pentru orice $a, b \in A$ avem

$$f(a \vee b) = f(a) \vee f(b), \qquad f(a \wedge b) = f(a) \wedge f(b).$$

Mai departe, f este **izomorfism de latici**, dacă este morfism bijectiv de latici.

Teorema 6.1.2 a) *Dacă mulţimea ordonată* $(A, \leq)$ *este o latice, atunci operaţiile*

$$a \wedge b = \inf\{a, b\}, \qquad a \vee b = \sup\{a, b\}, \quad \forall\ a, b \in A$$

definesc pe mulţimea A *o structură de latice* $(A, \wedge, \vee)$.

b) *Invers, dacă structura algebrică* $(A, \wedge, \vee)$ *este o latice, atunci relaţia*

$$a \leq b \Longleftrightarrow a \wedge b = a, \quad \forall\ a, b \in A$$

definită pe mulţimea A *este o relaţia de ordine astfel încât* $(A, \leq)$ *este latice; mai mult, pentru orice* $a, b \in A$ *avem*

$$a \vee b = \sup\{a, b\}, \quad a \wedge b = \inf\{a, b\}.$$

Demonstraţie. a) Comutativitatea operaţiilor $\wedge$ şi $\vee$ este evidentă din definiţie. Demonstrăm că $\vee$ este asociativă: fie $x = (a \vee b) \vee c, y = a \vee (b \vee c)$. Avem $a \vee b \leq x, c \leq x \Longrightarrow a \leq x, b \leq x, c \leq x \Longrightarrow a \leq x, b \vee c \leq x \Longrightarrow a \vee (b \vee c) \leq x$, de unde $y \leq x$. Analog obţinem că $x \leq y$, deci $x = y$.

Fie acum $v = a \vee (a \wedge b)$. De aici $a \leq v$, pe de altă parte $a \wedge b \leq a, a \leq a \Longrightarrow a \vee (a \wedge b) \leq a \Longrightarrow v \leq a \Longrightarrow v = a$.

b) Observăm că avem

$$(*) \qquad a \vee b = b \Longleftrightarrow a \wedge b = a.$$

Într-adevăr, pe baza proprietăţii de absorbţie, avem $a \vee b = b \Longrightarrow a = a \wedge (a \vee b) = a \wedge b$; mai departe, $a \wedge b = a \Longrightarrow b = b \vee (b \wedge a) = b \vee (a \wedge b) = b \vee a = a \vee b$.

Mai departe, să observăm că cele două operaţii sunt idempotente, adică avem

$$(**) \qquad a \vee a = a \wedge a = a.$$

Într-adevăr, pe baza proprietăţii de absorbţie, pentru orice $a \in A$ avem $a = a \wedge (a \vee a)$ şi apoi $a \vee a = a \vee (a \wedge (a \vee a)) = a$. Analog se verifică proprietatea duală.

Arătăm că $\leq$ este relaţie de ordine. Am văzut că $a \vee a = a$, de unde $a \leq a$, deci relaţia este reflexivă.

Antisimetria: fie $a \leq b, b \leq a$. Rezultă că $a \vee b = b$, $b \vee a = a \Longrightarrow a = b$.

Tranzitivitatea: pentru orice $a, b, c \in A$ avem $a \leq b, b \leq c \Longrightarrow a \vee b = b, b \vee c = c \Longrightarrow a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c \Longrightarrow a \leq c$.

Arătăm că $a \vee b = \sup\{a, b\}$. Într-adevăr, putem scrie $a \vee (a \vee b) = (a \vee a) \vee b = a \vee b$, de unde $a \leq a \vee b$; analog avem $b \leq a \vee b$, deci $a \vee b$ este majorantă a lui a şi b. Dacă c este o majorantă, adică $a \leq c, b \leq c$, atunci $a \vee c = c, b \vee c = c \Longrightarrow (a \vee b) \vee c = a \vee (b \vee c) = a \vee c \Longrightarrow a \vee b \leq c$, deci $a \vee b$ este cea mai mică majorantă.

Egalitatea $a \wedge b = \inf\{a, b\}$ rezultă din (*). ■

Exemplul 6.1.3 1) $(\mathbb{N}, \wedge, \vee)$ este o latice cu element nul şi element unitate, unde $x \wedge y = (x, y)$, este cel mai mare divizor comun al lui x şi y, iar $x \vee y = [x, y]$ este cel mai mic multiplu comun al lui x şi y. Elementul nul este numărul natural 1, deoarece $x \vee 1 = [x, 1] = x$ pentru orice x. Elementul unitate este numărul natural 0, deoarece $x \wedge 0 = (x, 0) = x$ pentru orice x. Această latice corespunde mulţimii ordonate $(\mathbb{N}, |)$.

2) Dacă M este o mulţime, atunci $(\mathcal{P}(M), \cap, \cup)$ este o latice cu element nul şi element unitate. Elementul nul este mulţimea vidă $\emptyset$, iar elementul unitate este M. Această latice corespunde mulţimii ordonate $(\mathcal{P}(M), \subseteq)$.

Exerciţiul 101 Să se arate că:

a) Dacă $f : A \to B$, atunci $f^* : \mathcal{P}(B) \to \mathcal{P}(A)$, $f^*(Y) = f^{-1}(Y)$ este morfism de latici.

b) Funcţia $f_* : \mathcal{P}(A) \to \mathcal{P}(B)$, $f_*(X) = f(X)$ este morfism de latici dacă şi numai dacă f este injectivă.

Exerciţiul 102 Fie mulţimile $A = \{1, 2, 3\}$ şi $B = \{d > 0 \mid d|30\}$. Să se determine toate izomorfismele de latici $f : (\mathcal{P}(A), \subseteq) \to (B, |)$.

Exerciţiul 103 Fie $(A, \leq, \wedge, \vee)$ şi $(B, \leq, \wedge, \vee)$ două latici şi fie $f : A \to B$ o funcţie. Să se arate că:

a) Dacă f este morfism de latici, atunci f este crescător.

b) Afirmaţia reciprocă nu e adevărată, adică există funcţii crescătoare care nu sunt morfisme de latici.

c) Dacă A este total ordonată şi f este crescător, atunci f este morfism de latici.

d) Dacă f este morfism bijectiv de latici, atunci $f^{-1} : B \to A$ este de asemenea morfism de latici.

e) f este izomorfism de latici $\Longleftrightarrow$ f este izomorfism de ordine.

Definiţia 6.1.4 a) Laticea $(A, \wedge, \vee)$ este **distributivă**, dacă pentru orice $a, b, c \in A$,

$$(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c).$$

b) Laticea $(A, \wedge, \vee)$ este **modulară**, dacă pentru orice $a, b, c \in A$,

$$a \leq c \Longrightarrow a \vee (b \wedge c) = (a \vee b) \wedge c.$$

Observaţii 6.1.5 1) Se poate arăta că laticea $(A, \wedge, \vee)$ este distributivă dacă şi numai dacă pentru orice $a, b, c \in A$, $(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$.

2) Laticile din exemplele 6.1.3 de mai sus sunt distributive.

3) Orice latice distributivă este modulară. Într-adevăr, pentru orice $a, b, c \in A, a \leq c$, avem $a \vee c = c$ şi $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$.

Afirmaţia reciprocă nu este adevărată, există latici modulare, care nu sunt distributive.

Exerciţiul 104 Să se demonstreze :

a) În laticea $(A, \wedge, \vee)$ avem $a \leq a'$, $b \leq b' \Longrightarrow a \vee b \leq a' \vee b'$ şi $a \wedge b \leq a' \wedge b'$.

b) Latice $(A, \wedge, \vee)$ este distributivă dacă şi numai dacă pentru orice $a, b, c \in A$ avem $(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$.

c) Dacă A este distributivă, atunci pentru orice $a, b, c \in A$ avem

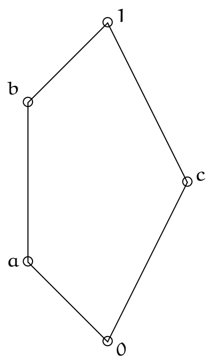
$$a \vee c = b \vee c,\ a \wedge c = b \wedge c \Longrightarrow a = b.$$

d) Dacă A este modulară, atunci pentru orice $a, b, c \in A$ avem

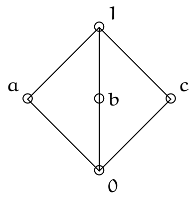
$$a \leq b,\ a \vee c = b \vee c,\ a \wedge c = b \wedge c \Longrightarrow a = b.$$

e) Laticea (1) nu e modulară (deci nici distributivă); laticea (2) este modulară, dar nu e distributivă:

(1)



(2)



Exerciţiul 105 Să se arate că :
a) Dacă $(A, \leq)$ este total ordonată, atunci A este latice distributivă.
b) $(\mathbb{N}, |)$ este latice distributivă.

6.2 Latici Boole şi inele Boole

Definiţia 6.2.1 Laticea A se numeşte **latice Boole** (sau **algebră Boole**) dacă A este distributivă, există cel mai mic element $0 = \min A$, există cel mai mare element $1 = \max A$ şi pentru orice $a \in A$ există un **complement** $a' \in A$ astfel încât $a \wedge a' = 0$ şi $a \vee a' = 1$. Vom nota această structură algebrică prin $(A, \vee, \wedge, 0, 1, ')$.

Exemplul 6.2.2 $(\mathcal{P}(M), \cap, \cup)$ este latice Boole, unde $\min \mathcal{P}(M) = \emptyset$, $\max \mathcal{P}(M) = M$, iar complementul lui $X \subseteq M$ este $\complement_M X = M \setminus X$.

Teorema 6.2.3 *Dacă A este o latice Boole, atunci*
a) *Pentru orice $a \in A$ există un unic complement $a' \in A$ astfel încât $a \wedge a' = 0$ şi $a \vee a' = 1$.*
b) $0' = 1, \quad 1' = 0, \quad (a')' = a,$
c) *Pentru orice $a, b \in A$,*

$$(a \wedge b)' = a' \vee b', \qquad (a \vee b)' = a' \wedge b'$$

(formulele lui de Morgan).

Demonstraţie. a) Dacă $a \vee a' = a \vee \bar{a} = 1$ şi $a \wedge a' = a \wedge \bar{a} = 0$, atunci

$$\begin{aligned} a' &= a' \vee 0 = a' \vee (a \wedge \bar{a}) = (a' \vee a) \wedge (a' \vee \bar{a}) = \\ &= (\bar{a} \vee a) \wedge (a' \vee \bar{a}) = \bar{a} \vee (a \wedge a') = \bar{a} \vee 0 = \bar{a}. \end{aligned}$$

b) Avem $0 \vee 1 = 1$, $\; 0 \wedge 1 = 0$, deci $0' = 1$ şi $1' = 0$. Mai departe, $a' \wedge a = 0$, $a' \vee a = 1$, deci $(a')' = a$.

c) $(a \vee b) \vee (a' \wedge b') = (a \vee b \vee a') \wedge (a \vee b \vee b') = (1 \vee b) \wedge (1 \vee a) = 1 \wedge 1 = 1$ şi $(a \vee b) \wedge (a' \wedge b') = (a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') = 0 \vee 0 = 0$, deci $(a \vee b)' = a' \wedge b'$; analog se arată că $(a \wedge b)' = a' \vee b'$. ∎

Definiţia 6.2.4 Inelul asociativ cu unitate $(A, +, \cdot)$ se numeşte **inel Boole** dacă $x^2 = x$ pentru orice $x \in A$ (adică orice element al lui A este idempotent).

Teorema 6.2.5 *Dacă $(A, +, \cdot)$ este un inel Boole, atunci*
a) $1 + 1 = 0$ *(deci $x + x = 0$ pentru orice $x \in A$).*
b) *A este comutativ.*

Demonstraţie. a) $1 + 1 = (1 + 1)^2 = 1 + 1 + 1 + 1$, deci $1 + 1 = 0$.
b) Dacă $x, y \in A$, atunci

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + y + xy + yx,$$

deci $xy = -yx$; deoarece $1 = -1$, rezultă că $xy = yx$. ∎

Următoarea teoremă descoperită de Marshall H. Stone (1903 – 1989) spune că noţiunile de latice Boole şi de inel Boole sunt echivalente.

Teorema 6.2.6 (Stone) a) *Fie* $(A, \vee, \wedge, 0, 1, ')$ *o latice Boole şi definim operaţiile:*

$$\begin{aligned} a + b &= (a \wedge b') \vee (a' \wedge b) = (a \vee b) \wedge (a' \vee b') \\ a \cdot b &= a \wedge b. \end{aligned}$$

Atunci $(A, +, \cdot)$ *este inel Boole cu element nul* 0 *şi element unitate* 1.

b) *Fie* $(A, +, \cdot, 0, 1)$ *un inel Boole şi definim operaţiile:*

$$a \vee b = a + b + ab, \qquad a \wedge b = ab.$$

Atunci $(A, \vee, \cdot)$ *este latice Boole, în care* $a' = 1 + a$, $\min A = 0$ *şi* $\max A = 1$.

c) *Corespondenţele definite de* a) *şi* b) *sunt inverse una alteia.*

d) *Dacă* $f : A \to A'$ *este un morfism de latici Boole, atunci* f *este şi morfism de inele Boole, iar dacă* $g : B \to B'$ *este un morfism de inele Boole, atunci* g *este şi morfism de latici Boole.*

Demonstraţie. a) Evident, „+" este comutativ. Dacă $a, b, c \in A$, atunci

$$\begin{aligned} a + (b + c) &= (a \wedge (b + c)') \vee (a' \wedge (b + c)) = \\ &= (a \wedge ((b \wedge c') \vee (b' \wedge c'))') \vee (a' \wedge ((b \wedge c') \vee (b' \wedge c))) = \\ &= (a \wedge (b \wedge c')' \wedge (b' \wedge c)') \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c) = \\ &= (a \wedge (b' \vee c) \wedge (b \vee c')) \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c) = \\ &= (a \wedge b' \wedge c') \vee (a \wedge b \wedge c) \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c). \end{aligned}$$

Rezultă că $(a + b) + c = c + (a + b) = a + (b + c)$; mai departe

$$\begin{aligned} a + 0 &= (a \wedge 0') \vee (a' \wedge 0) = a \vee 0 = a \\ a + a &= (a \wedge a') \vee (a' \wedge a) = 0 \vee 0 = 0, \end{aligned}$$

deci $-a = a$ pentru orice $a \in A$

Operaţia „$\cdot$" este comutativă şi asociativă, $a \cdot 1 = a \wedge 1 = a$, $a^2 = a \wedge a = a$; verificăm distributivitatea:

$$\begin{aligned} a(b + c) &= a \wedge ((b' \wedge c) \vee (b \wedge c')) = \\ &= (a \wedge b' \wedge c) \vee (a \wedge b \wedge c') \\ ab + ac &= ((a \wedge b) \wedge (a \wedge c)') \vee ((a \wedge b)' \wedge (a \wedge c)) = \\ &= (ab \wedge (a' \vee c')) \vee ((a' \vee b') \wedge a \wedge c) = \\ &= (a \wedge b \wedge a') \vee (a \wedge b \wedge c') \vee (a' \wedge a \wedge c) \vee (b' \wedge a \wedge c) = \\ &= (a \wedge b \wedge c') \vee (b' \wedge a \wedge c); \end{aligned}$$

rezultă că $(A, +, \cdot, 0, 1)$ este inel Boole.

b) Se arată uşor că „$\vee$" şi „$\wedge$" sunt comutative şi asociative, au loc proprietăţile de distributivitate şi şi absorbţie, şi pentru orice $a \in A$, $a \vee 0 = = a + 0 + a \cdot 0 = a$; $a \wedge 1 = a \cdot 1 = a$; $a \wedge (1 + a) = a(1 + a) = a + a^2 = a + a = 0$ şi $a \vee (1 + a) = a + 1 + a + a(1 + a) = 1 + a + a^2 = 1$.

c) Fie $(A, \vee, \wedge, 0, 1, ')$ o latice Boole, $(A, +, \cdot, 0, 1)$ inelul Boole corespunzător, şi fie $a \cup b = a + b + ab$, $a \cap b = a \cdot b$, $\bar{a} = a + 1$. Atunci se arată că $a \cup b = a \vee b$, $a \cap b = a \wedge b$ şi $a' = \bar{a}$.

Invers, fie $(A, +, \cdot, 0, 1)$ un inel Boole, $(A, \vee, \wedge, 0, 1, ')$ laticea Boole corespunzătoare, şi fie $a \oplus b = (a \wedge b') \vee (a' \wedge b)$, $a \odot b = a \wedge b$. Atunci $a \oplus b = a + b$ şi $a \odot b = ab$.

d) Afirmaţia referitoare la morfisme este lasată pe seama cititorului. ■

Exemplul 6.2.7 1) $(\mathbb{Z}_2, +, \cdot)$ este un inel Boole, iar laticea Boole corespunzătoare este dată de

$\vee$	$\hat{0}$	$\hat{1}$
$\hat{0}$	$\hat{0}$	$\hat{1}$
$\hat{1}$	$\hat{1}$	$\hat{1}$

$\wedge$	$\hat{0}$	$\hat{1}$
$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$

$'$	
$\hat{0}$	$\hat{1}$
$\hat{1}$	$\hat{0}$

2) A $(\mathcal{P}(M), \cup, \cap, \emptyset, M, \complement)$ este o latice Boole căreia îi corespunde inelul Boole $(\mathcal{P}(M), \Delta, \cap)$, unde $A \Delta B = (A \setminus B) \cup (B \setminus A)$ este diferenţa simetrică a lui A şi B.

Exerciţiul 106 a) Dacă $B_1, \dots, B_n$ sunt inele Boole, atunci $B_1 \times \cdots \times B_n$ este inel Boole.

b) Dacă M o mulţime şi B este un inel Boole, atunci $B^M = \mathrm{Hom}(M, B)$ este inel Boole.

Exerciţiul 107 a) Să se completeze demonstraţia teoremei lui Stone.
b) Dacă A este o latice Boole şi $a, b \in A$, atunci

$$a \le b \iff b' \le a' \iff a \wedge b' = 0 \iff a' \vee b = 1.$$

Exerciţiul 108 Folosind structura de inel Boole a lui $\mathcal{P}(U)$, să se rezolve următoarele sisteme de ecuaţii, unde $A, B, C \in \mathcal{P}(U)$ sunt date, iar $X \in \mathcal{P}(U)$ este necunoscuta:
a) $A \cap X = B$, $A \cup X = C$.
b) $A \setminus X = B$, $X \setminus A = C$.

Exerciţiul 109 Să se demonstreze că funcţiile de mai jos sunt izomorfisme de inele Boole:
a) $\mathcal{P}(M) \simeq \mathbb{Z}_2^M$, $X \mapsto \chi_X$ (unde χ_X este funcţia caracteristică a lui X).
b) $\mathcal{P}(M \cup N) \simeq \mathcal{P}(M) \times \mathcal{P}(N)$, dacă $M \cap N = \varnothing$.
c) Dacă $N \subseteq M$, atunci $\mathcal{P}(N) \trianglelefteq \mathcal{P}(M)$ şi $\mathcal{P}(M)/\mathcal{P}(N) \simeq \mathcal{P}(\complement N)$.

Exerciţiul 110 Fie A este un inel comutativ. Notăm $\mathrm{Idemp}(A) := \{e \in A \mid e^2 = e\}$ mulţimea idempotenţilor lui A. Pentru orice $e, f \in \mathrm{Idemp}(A)$ definim $e \oplus f = e + f - 2ef$.
a) Să se arate că $(\mathrm{Idemp}(A), \oplus, \cdot)$ este un inel Boole.
b) Să se întocmească diagrama Hasse a laticii Boole $(\mathrm{Idemp}(A), \vee, \wedge)$, dacă $A = \mathbb{Z}_{24}$, respectiv $A = \mathbb{Z}_{180}$.

6.3 Algebra Lyndenbaum–Tarski

Logica propoziţiilor furnizează un exemplu important de latice Boole.

Definiţia 6.3.1 a) Fie $\mathcal{F}$ mulţimea formulelor propoziţionale peste o mulţime dată de formule atomice. Considerăm structura algebrică $(\mathcal{F}, \wedge, \vee, ^-)$. În Capitolul 1 am definit pe $\mathcal{F}$ relaţiile „$\Rightarrow$" (*rezultă*) respectiv „$\Leftrightarrow$" (*echivalent*). Este evident că $\Rightarrow$ este o relaţie de preordine, în timp ce $\Leftrightarrow = (\Rightarrow \cap \Rightarrow^{-1})$ este o relaţie de echivalenţă pe $\mathcal{F}$, compatibilă cu operaţiile $\wedge$, $\vee$ şi $^-$.
b) Construim mulţimea factor $\hat{\mathcal{F}} = \mathcal{F}/\Leftrightarrow$, deci $\hat{\mathcal{F}} = \{\hat{A} \mid A \in \mathcal{F}\}$, unde

$$\hat{A} = \{A' \in \mathcal{F} \mid A \Leftrightarrow A'\}.$$

Pe mulţimea $\hat{\mathcal{F}}$ definim operaţiile

$$\hat{A} \wedge \hat{B} = \widehat{A \wedge B}, \quad \hat{A} \vee \hat{B} = \widehat{A \vee B}, \quad \bar{\hat{A}} = \hat{\bar{A}}.$$

Aceste definiţii nu depind de alegerea reprezentanţilor.
c) Clasa tautologiilor se notează cu 1, iar clasa contradicţiilor cu 0. Deci avem

$$1 = \{A \in \mathcal{F} \mid A \text{ tautologie}\}, \qquad 0 = \{A \in \mathcal{F} \mid A \text{ contradicţie}\}.$$

d) Conform Teoremei 5.1.6 pe mulţimea factor $\hat{\mathcal{F}}$ se poate defini o relaţie de ordine prin $\hat{A} \Rightarrow \hat{B}$ dacă şi numai dacă $A \Rightarrow B$.

Demonstraţia următoarei teoreme este lăsată cititorului.

Teorema 6.3.2 *a) Structura algebrică* $(\hat{\mathcal{F}}, \wedge, \vee, ^-, 0, 1)$ *este o latice Boole.*
b) *Următoarele afirmaţii sunt echivalente:*
(i) $\hat{A} \Rightarrow \hat{B}$; (ii) $\hat{A} \wedge \hat{B} = \hat{A}$; (iii) $\hat{A} \vee \hat{B} = \hat{B}$.

Structura algebrică $(\hat{\mathcal{F}}, \wedge, \vee, ^-, 0, 1)$ se numeşte *algebra Lyndenbaum–Tarski.* Teorema de mai sus dă posibilitatea utilizării metodelor algebrei în logica matematică.

Exerciţiul 111 a) Să se arate că relaţiile „$\Rightarrow$" şi „$\Leftrightarrow$" sunt compatibile cu operaţiile $\wedge$, $\vee$ şi $^-$.
b) Să se demonstreze Teorema 6.3.2.

6.4 Formule şi funcţii Boole. Forme normale

Fie B o mulţime finită.

Definiţia 6.4.1 a) Numim **formule (polinoame) Boole** (peste B) şirurile de simboluri construite astfel:

1. Dacă $x \in B$, atunci x este formulă Boole;

2. Dacă x, y sunt formule Boole, atunci următoarele şirurile de simboluri sunt formule Boole

$$(x \vee y), \quad (x \wedge y), \quad \text{şi} \quad (\bar{x});$$

3. Nu există alte formule Boole în afara celor construite la (1) şi (2).

b) Dacă x este o formulă Boole, atunci **duala** lui x (notaţie: x^*) se obţine schimbând între ele simbolurile „$\wedge$" şi „$\vee$".

c) Vom folosi uneori şi simbolurile „$\rightarrow$" şi „$\leftrightarrow$", dar acestea se reduc la cele de mai sus conform formulelor cunoscute deja din logica propoziţiilor.

Observaţii 6.4.2 a) Presupunem că B este chiar o latice Boole, deci dacă x este o formulă Boole peste B, atunci lui x îi corespunde un unic element din B, pe care îl notăm tot x. Deoarece axiomele laticii Boole sunt simetrice rezultă imediat **principiul dualităţii**:

$(*)$ *Dacă x şi y sunt formule Boole şi $x = y$ în B, atunci avem şi egalitatea $x^* = y^*$ în B.*

b) O formulă Boole se poate transforma în multe alte formule echivalente folosind axiomele laticii Boole. Există însă câteva formule mai importante, numite **forme normale**.

Introducem întâi câteva notaţii:

- Dacă $\alpha \in V = \{0, 1\}$, fie $x^\alpha = \begin{cases} x, & \text{dacă } \alpha = 1, \\ \bar{x}, & \text{dacă } \alpha = 0. \end{cases}$

- Dacă $\alpha = (\alpha_1, \dots, \alpha_n) \in V^n$, atunci formulele

$$x_1^{\alpha_1} \wedge x_2^{\alpha_2} \wedge \dots \wedge x_n^{\alpha_n} \quad \text{şi} \quad x_1^{\alpha_1} \vee x_2^{\alpha_2} \vee \dots \vee x_n^{\alpha_n}.$$

se numesc **conjuncţii elementare**, respectiv **disjuncţii elementare** .

Definiţia 6.4.3 a) Dacă $c_1, \dots, c_m$ sunt conjuncţii elementare, atunci formula $\bigvee_{i=1}^m c_k$ se numeşte **formă normală disjunctivă**.

b) Dacă $d_1, \dots, d_m$ disjuncţii elementare, atunci formula $\bigwedge_{i=1}^m d_k$ se numeşte **formă normală conjunctivă**.

Nu e greu de demonstrat că orice formulă Boole are o formă normală disjunctivă (conjunctivă) echivalentă cu ea. Aceste forme normale nu sunt unice.

Exemplul 6.4.4 *Considerăm formula $\bar{x}_1 \rightarrow (x_1 \wedge x_2)$ şi o aducem la formă normală disjunctivă respectiv conjunctivă:*

$$\begin{aligned} \bar{x}_1 \rightarrow (x_1 \wedge x_2) &= \bar{\bar{x}}_1 \vee (x_1 \wedge x_2) = x_1 \vee (x_1 \wedge x_2) = x_1 = \\ &= (x_1 \vee x_1) \wedge (x_1 \vee x_2) = x_1 \wedge (x_1 \vee x_2). \end{aligned}$$

Definiţia 6.4.5 a) Considerăm acum laticea Boole $B = V = \{0, 1\}$. Dacă $x = x(x_1, \dots, x_n)$ este o formulă Boole, atunci atribuind valori $x_i \in V$, formulei x îi corespunde o unică funcţie $x : V^n \rightarrow V$. O funcţie obţinută în acest fel se numeşte **funcţie Boole**.

b) Fie $f : V^n \rightarrow V$ o funcţie şi definim mulţimile T_f (*true*) şi F_f (*false*) astfel:

$$\begin{aligned} T_f &= \{\alpha = (\alpha_1, \dots, \alpha_n) \in V^n \mid f(\alpha_1, \dots, \alpha_n) = 1\}, \\ F_f &= \{\alpha = (\alpha_1, \dots, \alpha_n) \in V^n \mid f(\alpha_1, \dots, \alpha_n) = 0\}. \end{aligned}$$

În continuare arătăm că orice formulă Boole are formă normală disjunctivă sau conjunctivă specială, pe care o numim *perfectă.* Obţinem de asemenea că orice funcţie $f : V^n \rightarrow V$ este o funcţie Boole.

Teorema 6.4.6 *Fie $f : V^n \rightarrow V$ o funcţie Boole.*

1) *Dacă $T_f \neq \emptyset$, atunci*

$$f(x_1, \dots, x_n) = \bigvee_{\alpha \in T_f} \bigwedge_{i=1}^n x_i^{\alpha_i}.$$

2) *Dacă $F_f \neq \emptyset$, atunci*

$$f(x_1, \dots, x_n) = \bigwedge_{\alpha \in F_f} \bigvee_{i=1}^n x_i^{\bar{\alpha}_i}.$$

Demonstraţie. 1) Dacă $(\alpha_1,\ldots,\alpha_n)\in T_f$, atunci $f(\alpha_1,\ldots,\alpha_n)=1$ şi $\bigwedge_{i=1}^n \alpha_i^{\alpha_i}=1$; dacă $(\beta_1,\ldots,\beta_n)\neq(\alpha_1,\ldots,\alpha_n)$, atunci $\bigwedge_{i=1}^n \beta_i^{\alpha_i}=1$, deoarece $\beta_i^{\alpha_i}=0$ dacă $\beta_i\neq\alpha_i$; rezultă că $\bigvee_{\alpha\in T_f}\bigwedge_{i=1}^n x_i^{\alpha_i}=1$.

Invers, dacă $\bigvee_{\alpha\in T_f}\bigwedge_{i=1}^n x_i^{\alpha_i}=1$, atunci există $\alpha\in T_f$, astfel încât $\bigwedge_{i=1}^n x_i^{\alpha_i}=1$, deci $x_i^{\alpha_i}=1$ pentru orice $i=1,\ldots,n$. Rezultă că $x_i=\alpha_i$, $i=1,\ldots,n$, deci $(x_1,\ldots,x_n)=(\alpha_1,\ldots,\alpha_n)\in T_f$ şi $f(x_1,\ldots,x_n)=1$.

Analog se demonstrează 2). ■

Definiţia 6.4.7 Formula de la punctul 1) (respectiv 2)) se numeşte **normală disjunctivă perfectă (FNDP)** (respectiv **normală conjunctivă perfectă (FNCP)**).

Să reţinem că funcţia constantă 0 nu are FNDP, iar funcţia constantă 1 nu are FNCP.

Exemplul 6.4.8 Fie $f(x_1,x_2)=x_1\to x_2$; atunci avem $T_f=\{(0,0),(0,1),(1,1)\}$ şi $F_f=\{(1,0)\}$, deci

$$f(x_1,x_2)=(x_1^0\wedge x_2^0)\vee(x_1^0\wedge x_2^1)\vee(x_1^1\wedge x_2^1)=(\bar{x}_1\wedge\bar{x}_2)\vee(\bar{x}_1\wedge x_2)\vee(x_1\wedge x_2); \qquad \text{(FNDP)}$$

$$f(x_1,x_2)=x_1^{\bar{1}}\vee x_2^{\bar{0}}=\bar{x}_1\vee x_2. \qquad \text{(FNCP)}$$

Exerciţiul 112 Să se arate că $f(x_1,x_2)=\overline{x_1\wedge x_2}\to(\bar{x}_1\vee\bar{x}_2)$ este egală cu funcţia constantă 1, folosind:
a) tabele de adevăr ; b) inele Boole.

Exerciţiul 113 Să se determine FNDP şi FNCP pentru $f(x_1,x_2,x_3)=\bar{x}_1\to(x_2\wedge\bar{x}_3)$.

Exerciţiul 114 Fie $f:V^3\to V$ astfel încât $T_f=\{(1,1,1),(1,1,0),(1,0,1),(1,0,0)\}$.
a) Să se determine FNDP şi FNCP pentru $f(x_1,x_2,x_3)$.
b) Să se arate că $f(x_1,x_2,x_3)=x_1$.

Capitolul 7

MULŢIMI DE NUMERE

7.1 Mulţimea numerelor naturale

7.1.1 Axiomele lui Peano

Definiţia 7.1.1 Axioma infinitului 3.1.2 spune că există o mulţime y astfel încât $\emptyset \in y$ şi $x \in y$, $x^+ \in y$, unde $x^+ = x \cup \{x\}$.

Fie $\mathcal{A}$ clasa mulţilor satisfăcând proprietatea de mai sus, numită clasa mulţimilor **inductive**, adică

$$\mathcal{A} = \{A \mid \emptyset \in A;\ \text{dacă } x \in A, \text{ atunci } x^+ \in A\}.$$

Avem că $\bigcap \mathcal{A}$ este mulţime, care se numeşte **mulţimea numerelor naturale**. Notaţii: $\mathbb{N}$, $0 := \emptyset$, $1 := 0^+ = \{0\}$, $2 := 1^+ = \{0, 1\}$, $3 := 2^+ = \{0, 1, 2\}, \dots$. Elementul $s(n) = n^+$ se numeşte **succesorul** lui n. Notăm prin mai departe $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.

Teorema 7.1.2 (Axiomele lui Peano) *Tripletul format din mulţimea numerelor naturale* $\mathbb{N}$*, elementul* 0 *şi funcţia succesor* $s : \mathbb{N} \to \mathbb{N}$ *satisface* **axiomele lui Peano***:*

1) $0 \in \mathbb{N}$.

2) *Dacă* $n \in \mathbb{N}$*, atunci* $n^+ \in \mathbb{N}$ *(adică* s *este bine definită).*

3) **(Principiul inducţiei matematice)** *Dacă* $S \subseteq \mathbb{N}$*,* $0 \in S$ *şi* $n \in S$*,* $n^+ \in S$*, atunci* $S = \mathbb{N}$ *(adică orice submulţime inductivă a lui* $\mathbb{N}$ *coincide cu* $\mathbb{N}$*).*

4) *Dacă* $n \in \mathbb{N}$*, atunci* $n^+ \neq 0$*.*

5) *Dacă* $n, m \in \mathbb{N}$*, atunci din* $n^+ = m^+$ *rezultă* $n = m$*.*

Demonstraţie. 1), 2) şi 3) sunt imediate din definiţia lui $\mathbb{N}$. Pentru 4) vedem că n^+ este nevidă.

Pentru 5) este suficient de arătat că pentru orice $n \in \mathbb{N}$ avem $\cup n^+ = n$. Este evident că $n \subseteq \cup n^+$. Invers, dacă $x \in \cup n^+$, atunci $x \in n$, sau există $y \in n$ astfel ca $x \in y$. Dacă arătăm că din $y \in n$ rezultă $y^+ \subseteq n$, atunci am terminat. Fie

$$S = \{n \mid (n \in \mathbb{N}) \wedge \forall y((y \in n) \to (y^+ \subseteq n))\}.$$

Evident $S \subseteq \mathbb{N}$, $0 \in S$ şi dacă $n \in S$, atunci $n^+ = n \cup \{n\} \in S$. Într-adevăr, din $y \in n^+$ avem $y \in n$ sau $y = n$. Dacă $y \in n$, atunci din $n \in S$ obţinem $y^+ \subseteq n \subseteq n^+$, iar dacă $y = n$, atunci evident $y^+ = n^+$. Folosind 3) vedem că $S = \mathbb{N}$. ■

Observaţii 7.1.3 a) Observăm că $n \neq n^+$, deoarece axioma regularităţii exclude anomalia $n \in n$.

b) Folosind principiul inducţiei matematice vedem uşor că orice număr natural nenul este succesorul unui număr natural, adică $\forall n \in \mathbb{N}^*$, $\exists m \in \mathbb{N}$ astfel ca $n = m^+$.

c) Axiomele 2), 4) şi 5) respectiv observaţia de mai sus spun că **funcţia succesor**

$$s : \mathbb{N} \to \mathbb{N}, \qquad s(n) = n^+$$

este bine definită, este injectivă, dar nu este surjectivă, pentru că avem $\operatorname{Im} s = \mathbb{N}^*$.

d) Am văzut că $y \in n$ implică $y^+ \subseteq n$, adică $y \subset n$. Şi invers este adevărat: dacă $y \subset n$, atunci $y \in n$. Într-adevăr, considerăm mulţimea

$$S = \{n \mid (n \in \mathbb{N}) \wedge \forall y((y \subset n) \to (y \in n))\}.$$

Evident, $S \subseteq \mathbb{N}$, $0 \in S$, deci este suficient de arătat că dacă $n \in S$, atunci $n^+ = n \cup \{n\} \in S$. Fie $n \in S$ şi $y \subset n^+ = n \cup \{n\}$. Dacă $n \in y$, atunci $n^+ \subseteq y$, ceea ce contrazice $y \subset n^+$. Deci $n \notin y$, adică $y \subseteq n$. Avem două cazuri: dacă $y \subset n$, atunci din faptul că $n \in S$ obţinem $y \in n \subseteq n^+$; dacă $y = n$, atunci evident $y \in n^+$.

e) Dacă $n \in \mathbb{N}$, atunci $n \subseteq \mathbb{N}$. Într-adevăr, fie $S = \{n \mid n \in \mathbb{N} \wedge n \subseteq \mathbb{N}\}$. Evident, $0 \in S$ şi dacă $n \in S$, atunci $n^+ = n \cup \{n\} \in S$.

Următoarea teoremă creează posibilitatea **definiţiilor recursive (inductive)**.

Teorema 7.1.4 (Teorema recurenţei) *Dacă X este o mulţime, $a \in X$ un element fixat şi $f : X \to X$ o funcţie, atunci există o unică funcţie $u : \mathbb{N} \to X$ astfel încât $u(0) = a$ şi $u(n^+) = f(u(n))$ pentru orice $n \in \mathbb{N}$.*

Demonstraţie. Considerăm relaţiile $\rho \in \mathbb{N} \times X$ şi definim clasa

$$C = \{\rho \mid \rho \subseteq \mathbb{N} \times X;\ (0, a) \in \rho;\ \text{dacă } (n, x) \in \rho, \text{ atunci } (n^+, f(x)) \in \rho\}.$$

Deoarece C nevidă (căci $\mathbb{N} \times X \in C$), rezultă că $u := \bigcap C$ este o relaţie satisfăcând proprietăţile de mai sus. Este suficient de arătat că u este funcţie, adică pentru orice $n \in \mathbb{N}$ există unic $x \in X$ astfel încât $(n, x) \in u$. Fie

$$S = \{n \in \mathbb{N} \mid \exists! x \in X : (n, x) \in u\}.$$

Vom arăta că $0 \in S$ şi $n \in S$, $n^+ \in S$, de unde din principiul inducţiei matematice rezultă că $S = \mathbb{N}$, adică u este funcţie.

Dacă presupunem că $0 \notin S$, atunci ar exista $b \neq a$ în X astfel încât $(0, b) \in u$. Dar atunci avem $u \setminus \{(0, b)\} \in C$, contradicţie.

Fie acum $n \in S$ şi aratăm că $n^+ \in S$. Deoarece $n \in S$, există unic $x \in X$ astfel ca $(n, x) \in u$, dar atunci $(n^+, f(x)) \in u$. Presupunem acum că există $y \neq f(x)$ în X astfel ca $(n^+, y) \in u$. Atunci $u \setminus \{(n^+, y)\} \in C$, contradicţie. Rezultă pe de o parte că $(0, a) \in u \setminus \{(n^+, y)\}$, iar pe de altă parte dacă $(m, t) \in u \setminus \{(n^+, y)\}$, atunci $(m^+, f(t)) \in u \setminus \{(n^+, y)\}$, pentru că $(m^+, f(t)) = (n^+, y)$, $m = n$, deci $t = x$, adică $f(t) = f(x) = y$, ceea ce e imposibil (deoarece $f(x) \neq y$). ∎

Corolarul de mai jos spune că axiomele lui Peano determină tripletul $(\mathbb{N}, 0, s)$ în mod unic, abstracţie făcând de un unic izomorfism.

Corolar 7.1.5 *Dacă tripletul $(N', 0', s')$ satisface axiomele lui Peano, atunci este izomorf cu tripletul $(\mathbb{N}, 0, s)$, adică există o unică funcţie $u : \mathbb{N} \to N'$ care satisface proprietăţile:*
(1) $u(0) = 0'$, (2) $u \circ s = s' \circ u$, (3) u *este bijectiv.*

Exerciţiul 115 Să se demonstreze Corolarul 7.1.5.

7.1.2 Operaţii şi relaţia de ordine pe mulţimea numerelor naturale

Definiţia 7.1.6 (operaţii cu numere naturale) a) Pe baza teoremei recurenţei, pentru orice $m \in \mathbb{N}$ există unic $s_m : \mathbb{N} \to \mathbb{N}$ astfel încât $s_m(0) = m$ şi $s_m(n^+) = s(s_m(n)) = (s_m(n))^+$ pentru orice $n \in \mathbb{N}$. Valoarea $s_m(n)$ se numeşte **suma** lui m şi n, şi notăm $s_m(n) =: m + n$. Deci adunarea numerelor naturale se defineşte inductiv prin

$$m + 0 = m, \qquad m + s(n) = s(m + n).$$

Să observăm că $s(n) = n^+ = n + 1$.

b) Pe baza teoremei recurenţei, pentru orice $m \in \mathbb{N}$ există unic $p_m : \mathbb{N} \to \mathbb{N}$ astfel încât $p_m(0) = 0$ şi $p_m(n^+) = p_m(n) + m$ pentru orice $n \in \mathbb{N}$. Valoarea $p_m(n)$ se numeşte **produsul** lui m şi n, şi notăm $p_m(n) =: mn$. Deci înmulţirea numerelor naturale se defineşte inductiv prin

$$m \cdot 0 = 0, \qquad ms(n) = mn + m.$$

Să observăm că $n \cdot 1 = n$.

Teorema 7.1.7 (proprietăţile de bază ale operaţiilor) *Dacă $m, n, p \in \mathbb{N}$, atunci*
1) $(m + n) + p = m + (n + p)$;
2) $m + 0 = 0 + m$;
3) $m + 1 = 1 + m$;
4) $m + n = n + m$;
5) *Dacă* $m + p = n + p$, *atunci* $m = n$. *În particular, dacă* $m + p = m$, *atunci* $p = 0$.
6) *Dacă* $m + n = 0$, *atunci* $m = n = 0$;
7) **(Trihotomie)** *Din următoarele trei afirmaţii exact una este adevărată:*
(i) $m = n$, (ii) $\exists p \in \mathbb{N}^*$ *astfel încât* $m = n + p$, (iii) $\exists p \in \mathbb{N}^*$ *astfel încât* $n = m + p$;
8) $(m + n)p = mp + np$; $p(m + n) = pm + pn$;
9) $m(np) = (mn)p$;

10) $0 \cdot m = 0$;
11) $1 \cdot m = m$;
12) $mn = nm$;
13) *Dacă* $mn = 0$, *atunci* $m = 0$ *sau* $n = 0$;
14) *Dacă* $mp = np$ *şi* $p \neq 0$, *atunci* $m = n$;
15) *Dacă* $mn = 1$, *atunci* $m = n = 1$.

Exerciţiul 116 Să se demonstreze Teorema 7.1.7.

Definiţia 7.1.8 (ordonarea numerelor naturale) Fie $m, n \in \mathbb{N}$. Spunem că m **este mai mic decât** n, notaţie $m < n$, dacă există $p \in \mathbb{N}^*$ astfel încât $m + p = n$. Dacă $m = n$ sau $m < n$, atunci spunem că m **mai mic decât sau egal cu** n şi notăm $m \leq n$.

Propoziţia 7.1.9 (caracterizarea relaţiei „$<$") *Pentru orice numere naturale* m *şi* n *următoarele afirmaţii sunt echivalente:*
(i) $m < n$; (ii) $m \in n$; (iii) $m \subset n$.

Demonstraţie. Am văzut că $m \in n \Leftrightarrow m \subset n$. Arătăm că $m < n \Rightarrow m \in n$. Fie

$$S = \{n \mid (n \in \mathbb{N}) \wedge \forall m((m < n) \to (m \in n))\}.$$

Evident $0 \in S$, deci prin inducţie este suficient de arătat că $n \in S \Rightarrow n' \in S$. Într-adevăr, dacă $n \in S$ şi $m < n'$, atunci există $p \in \mathbb{N}^*$ astfel ca $n^+ = m + p$, adică $n^+ = m + r^+$, unde $p = r^+$. Dar atunci $n^+ = (m + r)^+$, deci $n = m + r$, de unde $m \leq n$. Dacă $m < n$, atunci din $n \in S$ rezultă $m \in n \subset n^+$, deci $m \in N^+$. Dacă $m = n$, atunci evident $m \in n^+$.

Arătăm că $m \in n \Rightarrow m < n$. Fie

$$S = \{n \mid (n \in \mathbb{N}) \wedge \forall m((m \in n) \to (m < n))\}.$$

Evident $0 \in S$, deci prin inducţie este suficient de arătat că $n \in S \Rightarrow n' \in S$. Într-adevăr, dacă $n \in S$ şi $m \in n'$, atunci $m \in n$ sau $m = n$. Dacă $m \in n$, atunci din $n \in S$ avem $m < n < n^+ = n + 1$, deci $m < n^+$. Dacă $m = n$, atunci evident $m < n^+ = n + 1$. ■

Teorema 7.1.10 (proprietăţile de bază ale relaţiei de ordine) *Fie* $m, n, p \in \mathbb{N}$. *Atunci*
1) *„$\leq$" este relaţie de ordine totală;*
2) $0 \leq n$;
3) *Dacă* $n \neq 0$, *atunci* $1 \leq n$;
4) $m < n$ *dacă şi numai dacă* $m^+ \leq n$;
5) $m \leq n$ *dacă şi numai dacă* $m < n^+$;
6) *Nu există* $n \in \mathbb{N}$ *astfel încât* $m < n < m^+$;
7) $(\mathbb{N}, \leq)$ *este bine ordonată;*
8) **(principiul inducţiei matematice, varianta 2: inducţie completă sau tare)** *Dacă* $P(n)$ *este un predicat pe mulţimea numerelor naturale astfel ca* $P(0)$ *este adevărat şi* $P(k)$ *adevărat pentru orice* $k < n$, *atunci şi* $P(n)$ *este adevărat;*
9) *Dacă* $m < n$, *atunci* $m + p < n + p$;
10) *Dacă* $m < n$ *şi* $p \neq 0$, *atunci* $mp < np$
11) **(axioma lui Arhimede)** *Dacă* $m \in \mathbb{N}$ *şi* $n \in \mathbb{N}^*$, *atunci există* $p \in \mathbb{N}$ *astfel încât* $pn > m$;
12) **(teorema împărţirii cu rest)** *Dacă* $m \in \mathbb{N}$ *şi* $n \in \mathbb{N}^*$, *atunci există unic* $q, r \in \mathbb{N}$ *astfel încât* $m = nq + r$ *şi* $r < n$.

Demonstraţie. 7) Presupunem că $(\mathbb{N}, \leq)$ nu e bine ordonată, adică există o submulţime $A \neq \emptyset$ care nu are cel mai mic element. Fie S mulţimea minoranţilor stricţi ai lui A, adică

$$S = \{n \in \mathbb{N} \mid n < a \ \forall a \in A\}.$$

Atunci evident $0 \in S$, deoarece A nu are cel mai mic element. Dacă $n \in S$, atunci $n^+ \leq a$ pentru orice $a \in A$. Dar $n^+ \notin A$ (deoarece în caz contrar ar fi cel mai mic element din A), deci $n^+ < a$ pentru orice $a \in A$, adică $n^+ \in S$. Prin inducţie rezultă că $S = \mathbb{N}$, deci $A = \emptyset$, contradicţie. ■

Exerciţiul 117 Să se demonstreze Teorema 7.1.10.

7.1.3 Sistemul formal al aritmeticii. Teorema lui Gödel de incompletitudine

Din punctul de vedere al logicii predicatelor, axiomele lui Peano, respectiv definiţiile adunării şi înmulţire se pot scrie ca formule închise în limbajul $\mathcal{L}_\mathbb{N}$ introdus în Exemplul 2.2.2. Amintim că limbajul $\mathcal{L}_\mathbb{N}$ foloseşte, în afară de simbolurile logicii, simbolul de constantă 0 şi trei simboluri de funcţii: s de o variabilă, adunarea ,,+" de două variabile şi înmulţirea ,,·" de două variabile. Axiomele lui Peano sunt:

(N1) Dacă φ este o formulă în $\mathcal{L}_\mathbb{N}$, atunci $(\varphi^x_0 \wedge \forall y(\varphi^x_y \to \varphi^x_{S(y)})) \to \forall x\varphi$.

Aici $\varphi^x_0, \varphi^x_y, \varphi^x_{s(y)}$ înseamnă că în φ, variabila x se înlocuieşte cu expresiile 0, y, $s(y)$, respectiv.

(N2) $\forall x(s(x) \neq 0)$

(N3) $\forall x\forall y((s(x) = s(y)) \to (x = y))$

(N4) $\forall x(x + 0 = x)$

(N5) $\forall x\forall y(x + s(y) = s(x + y))$

(N6) $\forall x(x \cdot 0 = 0)$

(N7) $\forall x\forall y(xs(y) = xy + x)$

Conform definiţiei ,,teoriei" date în paragraful 2.4.2, putem spune că **teoria numerelor (aritmetica)** este mulţimea formulelor închise deductibile din axiomele lui Peano. Teorema 7.1.2 şi definiţiile ulterioare spun că mulţimea $\mathbb{N}$ a numerelor naturale (cu elementul $0 \in \mathbb{N}$, funcţia succesor $s : \mathbb{N} \to \mathbb{N}$, definiţiile inductive ale adunării şi înmulţirii) este un model al teoriei numerelor. Corolarul 7.1.5 spune că oricare două modele ale teoriei numerelor sunt izomorfe.

Următoarea teoremă este una din rezultatele surprinzătoare ale logicii matematice.

Teorema 7.1.11 (teorema de incompletitudine a lui Gödel) *Sistemul axiomatic al teoriei numerelor nu este complet, adică există o formulă închisă care nu este deductibilă şi nici negaţia ei nu este deductibilă.*

Mai general, dacă un sistem axiomatic necontradictoriu este suficient de larg încât să conţină teoria numerelor şi este ,,suficient de regular", atunci există o formula închisă care nu este deductibilă şi nici negaţia ei nu este deductibilă.

7.2 Mulţimea numerelor întregi

Teoremele 7.1.7 şi 7.1.10 spun că structura $(\mathbb{N}, +, \cdot, \leq)$ este un semiinel asociativ, comutativ, cu unitate, fără divizori ai lui zero, bine ordonat şi arhimedian. Una din probleme e că $(\mathbb{N}, +)$ nu e grup. Rezolvăm asta prin lărgirea mulţimii $\mathbb{N}$. Vom construi mai jos mulţimea numerelor întregi pornind de la mulţimea numerelor naturale, respectiv definim adunarea, înmulţirea şi ordonarea numerelor întregi.

Definiţia 7.2.1 a) Pe mulţimea $\mathbb{N} \times \mathbb{N}$ definim relaţia omogenă

$$(m, n) \sim (p, q) \text{ dacă } m + q = n + p,$$

care este o relaţie de echivalenţă. Notăm prin $\widetilde{(m, n)}$ clasă de echivalenţă a perechii (m, n), deci

$$\widetilde{(m, n)} = \{(p, q) \in \mathbb{N} \times \mathbb{N} \mid (p, q) \sim (m, n)\}.$$

Mulţimea factor $\mathbb{Z} := \mathbb{N} \times \mathbb{N}/\sim = \{\widetilde{(m, n)} \mid m, n \in \mathbb{N}\}$ se numeşte **mulţimea numerelor întregi**, iar clasele $\widetilde{(m, n)}$ se numesc **numere întregi**.

b) Adunare şi înmulţirea numerelor întregi se definesc astfel:

$$\widetilde{(m, n)} + \widetilde{(p, q)} := \widetilde{(m + p, n + q)}, \qquad \widetilde{(m, n)}\widetilde{(p, q)} := \widetilde{(mp + nq, np + mq)}.$$

Aceste definiţii nu depind de alegerea reprezentanţilor.

Teorema 7.2.2 $(\mathbb{Z}, +, \cdot)$ *este domeniu de integritate, în care elementul nul este* $0 := \widetilde{(0, 0)} = \{(m, m) \mid m \in \mathbb{N}\}$, *elementul unitate este* $1 := \widetilde{(1, 0)} = \{(m+1, m) \mid m \in \mathbb{N}\}$ *şi opusul unui număr întreg* $\widetilde{(m, n)}$ *este* $-\widetilde{(m, n)} := \widetilde{(n, m)}$.

Exerciţiul 118 a) Să se arate că relaţia ,,∼" este o relaţie de echivalenţă.

b) Să se arate că definiţiile adunării şi înmulţirii nu depind de alegerea reprezentanţilor.

c) Să se demonstreze Teorema 7.2.2.

Definiţia 7.2.3 Numerele întregi se ordonează prin relaţia:

$$\widetilde{(m,n)} < \widetilde{(p,q)} \quad \text{dacă şi numai dacă} \quad q+m < p+n.$$

Teorema 7.2.4 1) *Definiţia relaţiei „$\leq$" nu depinde de alegerea reprezentanţilor.*
2) $(\mathbb{Z},\leq)$ *este total ordonată.*
3) *Funcţia* $\alpha : \mathbb{N} \to \mathbb{Z}_+$, $\alpha(n) = \widetilde{(n,0)}$ *este bine definită, strict crescătoare şi este izomorfism de semiinele.*
4) *Ordonarea numerelor întregi este compatibilă cu adunarea şi înmulţirea, adică pentru orice* $a,b,c,d \in \mathbb{Z}$ *avem*

$$a<b,\ c\leq d \Rightarrow a+c<b+d, \qquad a<b,\ c>0 \Rightarrow ac<bc, \qquad a<b,\ c<0 \Rightarrow ac>bc.$$

5) **(Axioma lui Arhimede)** *Pentru orice* $a \in \mathbb{Z}_+^*$ *şi* $b \in \mathbb{Z}$ *există* $n \in \mathbb{N}$ *astfel ca* $na > b$.

Observaţii 7.2.5 Vom identifica: n cu $\alpha(n) = \widetilde{(n,0)}$, $\mathbb{N}$ cu $\mathbb{Z}_+$, unde

$$\mathbb{Z}_+ = \{a \in \mathbb{Z} \mid a \geq 0\} = \{\widetilde{(m,n)} \mid m \geq n\}.$$

Ţinând cont de aceste identificări, pentru orice $m,n \in \mathbb{N}$ avem

$$m-n = m+(-n) = \widetilde{(m,0)} + (-\widetilde{(n,0)}) = \widetilde{(m,0)} + \widetilde{(0,n)} = \widetilde{(m,n)}.$$

Exerciţiul 119 Să se demonstreze Teorema 7.2.4.

7.3 Elemente de aritmetica numerelor întregi

Aritmetica este partea elemntară a teoriei numerelor şi studiază în special proprietăţile operaţiilor de bază. Cele mai vechi dovezi ale utilizării operaţiilor aritmetice au aproape 400 de ani şi provin de la egipteni şi babilonieni. Sistemul de numeraţie al babilonienilor era în baza 60 şi folosea notaţia poziţională. Civilizaţia Greciei antice a început dezvoltarea aritmeticii moderne chiar înainte de publicarea *Elementelor* lui Euclid în jurul anului 300 î.e.n. Grecii antici au considerat probleme privind divizibilitatea, numerele prime şi rezolvarea ecuaţiilor în numere în tregi. Numeralele hindu-arabe au început să fie folosite din secolul 6 e.n. Introducerea cifrei 0, notaţia poziţională şi ideea de valoare dependentă de poziţie au dus la dezvoltarea unor metode simple de calcul în baza 10.

7.3.1 Teorema împărţirii cu rest

Ştim că inelul $(\mathbb{Z},+,\cdot)$ al numerelor întregi este domeniu de integritate. Vom formula teorema împărţirii cu rest în acest context. Am vazut la 7.1.10. 12) că această teoremă poate fi demonstrată în semiinelul $(\mathbb{N},+,\cdot)$ doar pe baza axiomelor lui Peano.

Amintim ca orice număr real $x \in \mathbb{R}$ poate fi scris în mod unic sub forma $x = n+\varepsilon$, unde $n \in \mathbb{Z}$ şi $\varepsilon \in [0,1)$. Notaţie: $n =: [x]$ este *partea întreagă* a lui x, iar $\varepsilon =: \{x\}$ este *partea fracţionară* a lui x. Aşadar, $[x] \in \mathbb{Z}$, $\{x\} = x-[x] \in [0,1)$, şi $[x] \leq x < [x]+1$.

Teorema 7.3.1 (Teorema împărţirii cu rest, varianta I) *Fie* $a,b \in \mathbb{Z}$, $b \neq 0$. *Atunci există numerele* $q,r \in \mathbb{Z}$ *unic determinate astfel încât*

$$a = bq+r, \quad 0 \leq r < |b|, \quad q = \left[\frac{a}{b}\right] \in \mathbb{Z}, \quad r = b\left\{\frac{a}{b}\right\}.$$

Spunem că r a **cel mai mic rest pozitiv**.

Demonstraţie. Fie $r := \min(\{a-kb \mid k \in \mathbb{Z}\} \cap \mathbb{N})$, şi fie $q := (a-r)/b$, deci q şi r există.

Dacă $a = bq+r = bq_1+r_1$, unde $0 \leq r, r_1 < |b|$, atunci $|b||q-q_1| = |r-r_1| < |b|$, deci $q-q_1 = 0$, şi de aici $r = r_1$. ∎

Corolar 7.3.2 (Teorema împărţirii cu rest, varianta I) *Fie* $a,b \in \mathbb{Z}$, $b \neq 0$. *Atunci există numerele* $q,r \in \mathbb{Z}$ *unic determinate astfel încât*

$$a = bq+r, \quad -\frac{|b|}{2} < r \leq \frac{|b|}{2}.$$

Mai mult, $r \geq 0 \Leftrightarrow \left\{\frac{a}{b}\right\} \leq \frac{1}{2}$, *şi* $r < 0 \Leftrightarrow \left\{\frac{a}{b}\right\} > \frac{1}{2}$. Spunem că r az **cel mai mic rest în modul**.

De exemplu, dacă $b \geq 3$ este un număr impar, atunci resturile sunt $0, \pm 1, \pm 2, \ldots, \pm \frac{b-1}{2}$; dacă $b \geq 2$ este un număr par, atunci resturile sunt $0, \pm 1, \pm 2, \ldots, \pm(\frac{b}{2} - 1), \frac{b}{2}$.

Exerciţiul 120 Să se arate că
a) pătratul oricărui număr întreg este de forma $3k$ sau $3k + 1$;
b) pătratul oricărui număr întreg este de forma $5k$ sau $5k + 1$ sau $5k - 1$;
c) pătratul oricărui număr întreg este de forma $7k$ sau $7k + 1$ sau $7k - 1$.

Corolar 7.3.3 (sistem de numeraţie în baza b) *Fie $b \in \mathbb{N}$, $b > 1$. Atunci orice număr $n \in \mathbb{N}^*$ se scrie în mod unic sub forma*

$$n = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_1 b + c_0,$$

unde $c_i \in \mathbb{N}$, $0 \leq c_i \leq a - 1, i \in \{1, 2, \ldots, k\}, c_k \neq 0$. (Numerele c_i sunt **cifrele** lui n.) *Numărul cifrelor este $k = [\log_a n] + 1$.*

Demonstraţie. Conform Teoremei 7.3.1 avem

$$\begin{aligned} n &= bq_0 + c_0, \quad 0 \leq c_0 \leq b - 1 \\ q_0 &= bq_1 + c_1, \quad 0 \leq c_1 \leq b - 1, \\ q_1 &= bq_2 + c_2, \quad 0 \leq c_2 \leq b - 1, \\ &\ldots \end{aligned}$$

şi q_i, c_i în mod unic determinate. Aici $q_0 > q_1 > q_2 > \ldots$, şi dacă $q_k = 0$ este primul cât nul, atunci $q_{k-1} = c_k$, $0 < c_k \leq b - 1$. Înlocuind obţinem

$$n = b(bq_1 + c_1) + c_0 = b(b(bq_2 + c_2) + c_1) + c_0 = \cdots = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_1 b + c_0.$$

Observăm că deoarece $0 < c_k < b$, avem $b^k \leq n < b^{k+1}$, deci $k \leq \log_b n < k + 1$. ∎

Exerciţiul 121 Să se scrie numărul:
1) $309_{(10)}$ în bazele 7, 2, 16;
2) $214_{(7)}$ în bazele 10, 2, 16;

Exerciţiul 122 Să se arate că pentru orice $m > n$, numărul

$$123 \ldots (n-1)n(n-1) \ldots 321$$

scris în baza m este pătrat perfect.

7.3.2 Divizibilitate. Cel mai mare divizor comun

Definiţia 7.3.4 Fie a şi b numere întregi.
a) Spunem că a **divide** pe b-nek (notaţie: $a|b$) dacă există $x \in \mathbb{Z}$ astfel încât $b = ax$.
b) Un număr $d \in \mathbb{N}$ este **cel mai mare divizor comun** al lui a şi b (notaţie: $d = (a, b)$) dacă

1. $d|a$ şi $d|b$;

2. dacă $d' \in \mathbb{Z}$, $d'|a$ şi $d'|b$, atunci $d'|d$.

c) Un număr $m \in \mathbb{N}$ este **cel mai mic multiplu comun** al lui a şi b (notaţie: $m = [a, b]$) dacă

1. $a|m$ şi $b|m$;

2. dacă $m' \in \mathbb{Z}$, $a|m'$ şi $b|m'$, atunci $m|m'$.

d) a şi b sunt **relativ prime** dacă $(a, b) = 1$.

Exerciţiul 123 a) 0 este divizibil cu orice număr; orice număr este divizibil cu 1.
b) $a|b,\ a|c \Rightarrow a|b \pm c$.
c) $a|b \Rightarrow ax|bx$ pentru orice $x \in \mathbb{Z}$. Invers, dacă $ax|bx,\ x \neq 0$, atunci $a|b$.
d) $x|y \iff (x, y) = x \iff [x, y] = y$.

Exerciţiul 124 a) Fie $a, b \in \mathbb{Z}$. Să se arate că (a, b) există, şi mai mult, există $u, v \in \mathbb{Z}$ astfel încât $(a, b) = au + bv$. Mai exact, dacă $a = b = 0$, atunci evident $(a, b) = 0$. În caz contrar, fie

$$d := \min\{ax + by \mid x, y \in \mathbb{Z},\ ax + by > 0\}$$

şi să se arate că $d = (a, b)$.

b) $(a, b) = 1 \Leftrightarrow$ există $u, v \in \mathbb{Z}$ astfel încât $au + bv = 1$.

Definiţia 7.3.5 Următorul şir de calcule se numeşte **algoritmul lui Euclid** aplicat numerelor a şi b.

$$\begin{aligned}
a &= bq_0 + r_0, \quad 0 < r_0 < |b|;\\
b &= r_0q_1 + r_1, \quad 0 < r_2 < r_1;\\
r_0 &= r_1q_2 + r_2, \quad 0 < r_3 < r_2;\\
r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2;\\
&\dots\\
r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2};\\
r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1};\\
r_{n-1} &= r_nq_{n+1} + r_{n+1}, \quad 0 < r_{n+1} < r_n;\\
r_n &= r_{n+1}q_{n+2} + r_{n+2}, \quad r_{n+2} = 0.
\end{aligned}$$

Algoritmul se termină, deoarece şirul $(r_k)_{k\geq 0}$ este strict descrescător, deci există n astfel încât $r_{n+1} = 0$. Spunem că r_n este *ultimul rest nenul.*

Teorema 7.3.6 1) *Cel mai mare divizor comun* d *al lui* a *şi* b *este egal cu ultimul rest nenul, adică* $d := (a, b) = r_{n+1}$.

2) *Ştim că există* $u, v \in \mathbb{Z}$ *astfel încât* $d = (a, b) = au+bv$. *Numerele* u *şi* v *pot fi calculate folosind algoritmul lui Euclid.*

Demonstraţie. 1) Se arată uşor că dacă $a = bq + r$, atunci $(a, b) = (b, r)$; rezultă că

$$(a, b) = (b, r_0) = (r_0, r_1) = \ldots = (r_{n-1}, r_n) = (r_n, r_{n+1}) = r_{n+1}.$$

2) Avem următorul şi de calcule ce *extinde* algoritmul lui Euclid:

$$\begin{aligned}
(a, b) = r_{n+1} &= r_{n-1} - r_nq_{n+1} =\\
&= r_{n-1} - (r_{n-2} - r_{n-1}q_n)q_{n+1} =\\
&= r_{n-1}(1 + q_nq_{n+1}) - r_{n-2}g_{n-1} =\\
&= r_{n-1}u_{n-1} + r_{n-2}v_{n-1},
\end{aligned}$$

şi continuăm prin inducţie. ■

Exerciţiul 125 Să se aplice algoritmul extins al lui Euclid în următoarele cazuri (să se determine d, u, v):

(1) $a = 19,\ b = 26.$
(2) $a = -187,\ b = 34.$
(3) $a = -841,\ b = -160.$
(4) $a = 2613,\ b = -2171.$

Exerciţiul 126 a) Dacă $x \in \mathbb{N}$, atunci $(ax, bx) = (a, b)x$.

b) Dacă $d = (a, b)$, $a = da'$ şi $b = db'$, atunci $(a', b') = 1$.

c) Fie $a, b, c \in \mathbb{Z}$ astfel încât $(a, b) = 1$. Să se arate că :

(1) $(a, bc) = (a, c)$; (2) $(a, c) = 1 \Rightarrow (a, bc) = 1$; (3) $a|bc \Rightarrow a|c$; (4) $a|c$ şi $b|c \Rightarrow ab|c$.

d) Dacă $d = (a, b)$, $a = da'$ şi $b = db'$, atunci

$$[a, b] = a'b'd = \frac{ab}{d}.$$

Definiţia 7.3.7 Fie $x_1, \ldots, x_n$ numere întregi, unde $n \in \mathbb{N}^*$, şi fie $d, m \in \mathbb{N}$. Prin definiţie,

a) $d = (x_1, \ldots, x_n) \iff \begin{cases} d|x_1, \ldots, d|x_n,\\ \text{dacă } d'|x_1, \ldots, d'|x_n, \text{ atunci } d'|d. \end{cases}$

b) $m = [x_1, \ldots, x_n] \iff \begin{cases} x_1|m, \ldots, x_n|m,\\ \text{dacă } x_1|m', \ldots, x_n|m', \text{ atunci } m|m'. \end{cases}$

Exerciţiul 127 Fie $x_1, \dots, x_n$ numere întregi. Să se arate că:

a) $(x_1, \dots, x_{n-1}, x_n) = ((x_1, \dots, x_{n-1}), x_n)$; $[x_1, \dots, x_{n-1}, x_n] = [[x_1, \dots, x_{n-1}], x_n]$.

b) $(x_1, \dots, x_n) = \min\{x \in \mathbb{N}^* \mid \exists u_i \in \mathbb{Z}$ astfel încât $x = \sum_{i=1}^n u_i x_i\}$. În particular, $(x_1, \dots, x_n) = d \Rightarrow \exists u_i \in \mathbb{Z}$ astfel ca $\sum_{i=1}^n u_i x_i = d$.

c) $(x_1, \dots, x_n) = 1 \Leftrightarrow \exists u_i \in \mathbb{Z}$ astfel încât $\sum_{i=1}^n u_i x_i = 1$.

d) $(x_1 x, \dots, x_n x) = (x_1, \dots, x_n)x$ pentru orice $x \in \mathbb{N}$.

e) Dacă $(x, x_i) = 1$, $i = 1, \dots, n$, atunci $(x, x_1 \dots x_n) = 1$.

f) Dacă $(x_i, x_j) = 1$ orice $i, j = 1, \dots, n$, $i \neq j$, atunci $[x_1, \dots, x_n] = x_1 \dots x_n$. (În acest caz spunem că numerele x_i, $i = 1, \dots, n$ sunt *relativ prime două câte două.*)

Exerciţiul 128 Fie $a, b \in \mathbb{Z}$ şi $n \in \mathbb{N}^*$. Atunci

1) $a - b \mid a^n - b^n$,

2) dacă n este impar, atunci $a + b \mid a^n + b^n$,

3) dacă n este par, atunci $a + b \mid a^n - b^n$.

Exerciţiul 129 Să se arate că:

1) pentru orice $n \in \mathbb{N}$, $n^5 - n$ este divizibil 30;

2) $7 \mid 2^n - 1$ dacă şi numai dacă $3 \mid n$, unde $n \in \mathbb{N}$;

3) pentru orice număr impar $m \in \mathbb{N}^*$ avem $240 \mid m^5 - m$.

Exerciţiul 130 Fie $a, b, c \in \mathbb{Z}$. Să se arate că

1) $(a, [b, c]) = [(a, b), (a, c)]$, $\quad [a, (b, c)] = ([a, b], [a, c])$;

2) dacă $(a, b) = (a, c)$ şi $[a, b] = [a, c]$, atunci $b = c$.

3) $[a, b, c](a, b)(b, c)(c, a) = abc(a, b, c)$.

Exerciţiul 131 Fie $a, m, n \in \mathbb{N}^*$, $a \geq 2$. Să se arate că

1) $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

2) Dacă $(a, b) = 1$, atunci $(a^m - b^m, a^n - b^n) = a^d - b^d$.

3) Dacă $m > n$, atunci $a^{2^n} + 1 \mid a^{2^m} - 1$.

7.3.3 Numere prime. Teorema fundamentală a aritmeticii

Definiţia 7.3.8 Numărul $p \in \mathbb{N}$ se numeşte **prim**, dacă $p \neq 1$, şi dacă $a \in \mathbb{Z}$, $a|p$, atunci $a = \pm 1$ sau $a = \pm p$ (adică p nu are divizori proprii).

Observaţii 7.3.9 Un algoritm ce enumeră toate numerele prime mai mici decât un număr natural dat n este **sita lui Eratostene** (aprox. 200 î.e.n). Paşii sunt următorii:

(1) Se scriu toate numerele de la 2 la n.

(2) Iniţial, fie $p := 2$.

(3) Marcăm în listă toţi multipli lui p cu excepţia lui p (adică pe $2p$, $3p$, …).

(4) Căutăm în listă primul număr nemarcat $q > p$. Dacă un astfel de q nu există, am terminat; altfel fie $p := q$ şi mergem din nou la pasul (3).

Algoritmul evident se termină, iar numerele nemarcate sunt toate numerele prime mai mici decât n.

Exerciţiul 132 Dacă $n \in \mathbb{N}$ este număr compus, atunci cel mai mic divizor prim al lui n este $\leq \sqrt{n}$.

Lema 7.3.10 *Fie* $p \in \mathbb{N}$, $p > 1$. *Să se arate că* p *număr prim* $\Leftrightarrow$ *pentru orice* $a, b \in \mathbb{Z}$, *dacă* $p|ab$, *atunci* $p|a$ *sau* $p|b$.

Demonstraţie. Fie $p \in \mathbb{N}$ prim. Atunci $p \neq 0$, $p \not| 1$, şi presupunem că $p|ab$, $p \nmid a$. Trebuie să arătăm că $p|b$. Deoarece $p|ab$, rezultă că $(ab, p) = p$, dar $p \nmid a$ de aceea $(a, p) = 1$. Mai departe

$$(p, b) = (p, (a, p)b) = (p, (ab, pb)) = ((p, ap), ab) = (p, ab) = p,$$

deci $p|b$. Invers, presupunem că $p = ab$; atunci $p|ab$ şi din ipoteză putem presupune că $p|a$; dar $a|p$, deci $a = \pm p$; rezulta că p nu are divizori proprii. ■

Teorema 7.3.11 (Teorema fundamentală a aritmeticii) *Orice număr întreg* $a \neq 0, \pm 1$ *se descompune în mod unic (abstracţie făcând de ordinea factorilor) în produs de numere prime sub forma:*

$$a = \pm p_1^{k_1} \dots p_r^{k_r},$$

unde p_i *sunt numere prime distincte şi* $k_i \in \mathbb{N}^*$, $1 \leq i \leq r$.

Demonstraţie. *Existenţa descompunerii*: Putem lua $a \in \mathbb{N}$, $a \neq 0$, $a \neq 1$. Dacă a este prim, atunci $a = a$. Dacă a nu e prim, atunci din $a = a_1 a_1'$ rezultă că $a_1|a$ şi $a_1 \neq a$. Dacă a_1 nu e prim, atunci $a_1 = a_2 a_2'$ rezultă că $a_2|a_1$ şi $a_2 \neq a_1$ (adică $a_2 < a_1$). Continuând procedura, am obţine şirul infinit strict descrescător $a > a_1 > a_2 > a_3 > \dots$ de numere naturale, ceea ce e imposibil, deci procedura se încheie după un număr finit de paşi, adică a are o descompunere în produs de numere prime.

Unicitatea descompunerii: presupunem că $a = p_1 \dots p_n = q_1 \dots q_m$, unde p_i, q_i sunt prime. Deoarece $p_1|q_1 \dots q_m$ şi p_1 este prim, putem presupune că $p_1|q_1$, dar q_1 este prim deci $p_1 = q_1$; rezultă că $p_1 \dots p_n = q_1 \dots q_m$, deci $p_2 \dots p_n = q_2 \dots q_m$. Continuând prin inducţie, obţinem că $n = m$ şi $p_i = q_i$ pentru orice $i \in \{1, \dots, n\}$. ■

Corolar 7.3.12 *Dacă* $a = \pm p_1^{k_1} \dots p_r^{k_r}$ *şi* $b = \pm p_1^{l_1} \dots p_r^{l_r}$*, unde* $k_i, l_i \geq 0$, $1 \leq i \leq r$*, atunci*

$$\begin{aligned} a|b &\iff k_i \leq l_i \text{ pentru orice } i \in \{1, \dots, r\} \\ a = \pm b &\iff k_i = l_i \text{ pentru orice } i \in \{1, \dots, r\} \\ (a, b) &= p_1^{\min\{s_1,t_1\}} \dots p_r^{\min\{s_r,t_r\}} \\ [a, b] &= p_1^{\max\{s_1,t_1\}} \dots p_r^{\max\{s_r,t_r\}}. \end{aligned}$$

Teorema 7.3.13 (Euclid) *Există o infinitate de numere prime.*

Demonstraţie. Presupunem prin absurd că afirmaţia nu e adevărată şi fie $p_1, p_2, \dots, p_r$ toate numerele prime. Considerăm numărul $N = p_1 p_2 \dots p_r + 1$, care eviden nu e divizibil cu nuciunul din numerele $p_1, p_2, \dots, p_r$. Dar N are un divizor prim q care nu e în şirul $p_1, p_2, \dots, p_r$, cee a ce este o contradicţie. ■

Exerciţiul 133 Să se arate că dacă p număr prim, atunci $p \mid C_p^k$, pentru orice k, $1 \leq k \leq p - 1$.

Exerciţiul 134 Să se arate că:

1) Dacă $2^n + 1$ număr prim, atunci n este o putere a lui 2, adică este de forma $n = 2^k$, unde $k \in \mathbb{N}$.

2) Dacă $2^n - 1$ număr prim, atunci n este număr prim.

Observaţii 7.3.14 1) Numerele de forma $F_n = 2^{2^n} + 1, n \in \mathbb{N}$ se numesc *numere Fermat*. Avem că $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ sunt prime; Euler a arătat că F_5 este divizibil cu 641, deci reciproca afirmaţiei 1) de mai sus este falsă. Se ştie că F_n este compus dacă $5 \leq n \leq 32$. Nu se stie dacă există o infinitate de numere Fermat prime, respectiv compuse.

2) Numerele prime de forma $M_p = 2^p - 1$, unde p prim, se numesc *numere prime ale lui Mersenne*. Avem că $M_{11} = 2^{11} - 1 = 23 \cdot 89$ nu e prim, deci reciproca afirmaţiei 2) de mai sus este falsă. Nu se ştie care din numerele M_p sunt prime şi de asemenea, nu se ştie dacă există o infinitate de numere prime ale lui Mersenne.

7.3.4 Congruenţe. Inelul $\mathbb{Z}_n$ al claselor de resturi modulo n

Definiţia 7.3.15 Fie $n \in \mathbb{N}$ un număr natural.

a) Congruenţa modulo n este relaţia pe $\mathbb{Z}$ definită astfel: dacă $a, b \in \mathbb{Z}$, atunci

$$a \equiv b \pmod{n} \overset{\text{def}}{\Leftrightarrow} n \mid b - a \Leftrightarrow b - a \in n\mathbb{Z} \Leftrightarrow \exists k \in \mathbb{Z} : b = a + nk \iff a \bmod n = b \bmod n.$$

Notaţie: $\hat{a} = [a]_n = \{a + nk \mid k \in \mathbb{Z}\} = a + n\mathbb{Z}$ este clasa lui a modulo n.

b) Considerăm, conform Definiţiei 4.4.4, mulţimea factor

$$\mathbb{Z}_n := \{\hat{a} \mid a \in \mathbb{Z}\};$$

atunci $\mathbb{Z}_n$ este un inel comutativ cu unitate, numit **inelul claselor de resturi modulo** n, unde operaţiile sunt definite astfel (vezi Teorema 8.3.3):

$$\hat{a} + \hat{b} \overset{\text{def}}{=} \widehat{a + b}, \qquad \hat{a}\hat{b} \overset{\text{def}}{=} \widehat{ab}.$$

Observaţii 7.3.16 1) În inelul $\mathbb{Z}_n$ elementul nul este $\hat{0} = n\mathbb{Z}$, iar elementul unitate este $\hat{1} = 1 + n\mathbb{Z}$.

2) Distingem următoarele cazuri particulare:

- $n = 0$: avem $a \equiv b \pmod 0 \Leftrightarrow b - a = 0 \Leftrightarrow b = a$; atunci $\hat{a} = [a]_n = \{a\}$, deci $\mathbb{Z}_0 = \{\{a\} \mid a \in \mathbb{Z}\} \simeq \mathbb{Z}$;
- $n = 1$: avem că $a \equiv b \pmod 1$ este adevărat pentru orice a, b, deci $\hat{a} = \mathbb{Z}$; rezultă că inelul $\mathbb{Z}_1 = \{\hat{0}\}$ are un singur element;

- $n \geq 2$: din teorema împărţirii cu rest 7.3.1 există unic $q, r \in \mathbb{Z}$ astfel încât

$$a = nq + r, \quad 0 \leq r < n$$

Aici $q = \left[\frac{a}{n}\right]$, $r = a - n\left[\frac{a}{n}\right] \equiv a \pmod n$; rezultă că $\hat{a} = \hat{r}$, deci $|\mathbb{Z}_n| \leq n$; dacă $0 \leq r < s < n - 1$, atunci $n \nmid s - r$, deci $|\mathbb{Z}_n| = n$.

Exerciţiul 135 Dacă $a \equiv b \pmod n$, atunci $(a, n) = (b, n)$.

Exerciţiul 136 (proprietăţile de bază ale congruenţelor) Fie $a, b, c, d \in \mathbb{Z}$ şi $m, m_1, m_2, k \in \mathbb{N}^*$. Să se arate că:
1) dacă $a \equiv b$ (mod m) şi $c \equiv d$ (mod m), atunci $a + c \equiv b + d$ (mod m) şi $ac \equiv bd$ (mod m);
2) dacă $f \in \mathbb{Z}[X]$ este un polinom şi $a \equiv b \pmod m$), atunci $f(a) \equiv f(b) \pmod m$;
3) dacă $a \equiv b \pmod m$ şi $d \mid a, b, m$, atunci $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$;
4) dacă $ac \equiv bc \pmod m$ şi $(c, m) = 1$, atunci $a \equiv b \pmod m$;
5) dacă $a \equiv b \pmod{m_1}$ şi $a \equiv b \pmod{m_2}$, atunci $a \equiv b \pmod{[m_1, m_2]}$).

Exerciţiul 137 (criterii de divizibilitate) Fie

$$N = \overline{a_k a_{k-1} \dots a_1 a_0} = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0$$

un număr scris în sistemul cu baza 10. Să se arate că:
1) $N \equiv a_0 \pmod 2$, $\pmod 5$, $\pmod{10}$.
2) $N \equiv \overline{a_1 a_0} \pmod 4$, $\pmod{25}$.
3) $N \equiv \overline{a_2 a_1 a_0} \pmod 8$, $\pmod{125}$.
4) $N \equiv a_0 + a_1 + \dots + a_k \pmod 3$, $\pmod 9$.
5) $N \equiv \sum_{i=0}^{k} (-1)^i a_i \pmod{11}$.
6) $N \equiv \overline{a_2 a_1 a_0} + \overline{a_k \dots a_3} \pmod{27}$, $\pmod{37}$. (Folosim faptul că $27 \cdot 37 = 999$.)
7) $N \equiv \overline{a_2 a_1 a_0} - \overline{a_k \dots a_3} \pmod 7$, $\pmod{11}$, $\pmod{13}$. (Folosim faptul că $7 \cdot 11 \cdot 37 = 1001$.)

7.3.5 Grupul $U(\mathbb{Z}_n)$. Teoremele lui Euler şi Fermat

Considerăm grupul multiplicativ $(U(\mathbb{Z}_n), \cdot)$ al elementelor inversabile din $\mathbb{Z}_n$.

Lema 7.3.17 *Fie $a \in \mathbb{Z}$. Următoarele afirmaţii sunt echivalente:*
(i) $\hat{a} \in U(\mathbb{Z}_n)$;
(ii) a *nu este divizor al lui* 0 *în* $\mathbb{Z}_n$ (*adică* $\hat{a}\hat{b} = \hat{0} \Rightarrow \hat{b} = \hat{0}$);
(iii) $(a, n) = 1$.

Demonstraţie. (i)⇒(ii). $\hat{a}\hat{b} = \hat{0}$. Înmulţind cu $\hat{a}^{-1}$ obţinem $\hat{b} = \hat{0}$.
(ii)⇒(iii) ⇔ $\overline{\text{(iii)}} \Rightarrow \overline{\text{(ii)}}$. Presupunem că $(a, n) = d > 1$. Fie $a = a'd$, $n = n'd$, deci $(a', n') = 1$. În acest caz $\hat{a}$ este divizor al lui 0. Într-adevăr,

$$\hat{a}\widehat{n'} = \widehat{an'} = \widehat{a'dn'} = \widehat{a'n} = \widehat{a'}\hat{n} = \hat{0}.$$

(iii)⇒(i). Dacă $(a, n) = 1$, atunci $\exists\, u, v \in \mathbb{Z}$ astfel ca $au + nv = 1$. De aici $\hat{1} = \hat{a}\hat{u} + \hat{n}\hat{v}$, deci $\hat{a}^{-1} = \hat{u}$. ■

Teorema 7.3.18 *Următoarele afirmaţii sunt echivalente:*
(i) $\mathbb{Z}_n$ *este corp (orice element nenul este inversabil);*
(ii) $\mathbb{Z}_n$ *este domeniu de integritate;*
(iii) n *este număr prim.*

Demonstraţie. (i)⇔(ii). Evident, orice corp comutativ este domeniu de integritate; invers, se arată uşor că orice domeniu de integritate finit este corp.
(i)⇔(iii). $\mathbb{Z}_n$ este corp ⇔ pentru orice $0 < a < n$ avem $(a, n) = 1$ ⇔ n este prim. ■

Observaţii 7.3.19 Considerăm grupul $(U(\mathbb{Z}_n, \cdot)$. Am văzut că

$$U(\mathbb{Z}_n) = \{\hat{a} \in \mathbb{Z}_n \mid (a, n) = 1\},$$

deci $|\, U(\mathbb{Z}_n) \,| = \varphi(n)$, unde $\varphi : \mathbb{N}^* \to \mathbb{C}$ este *funcţia aritmetică a lui Euler.*

Corolar 7.3.20 a) **(teorema lui Euler)** *Pentru orice* $a \in \mathbb{Z}$, $(a, n) = 1$ *avem* $a^{\varphi(n)} = 1$ *în* $U(\mathbb{Z}_n)$*, adică*

$$a^{\varphi(n)} \equiv 1 \pmod n.$$

b) **(mica teoremă a lui Fermat)** *Pentru orice* $a \in \mathbb{Z}$ *şi pentru orice număr prim* p*, avem* $a^p \equiv a \pmod p$.

Demonstraţie. a) Rezultă din Teorema lui Lagrange din teoria grupurilor.

b) Dacă $p \nmid a$ atunci $(p, a) = 1 \overset{a)}{\Rightarrow} a^{p-1} \equiv 1 \pmod p \Rightarrow a^{p-1} \equiv a \pmod p$. Dacă $p \mid a$, atunci $p \mid a^p$, deci $p \mid a^p - a$, de unde $a^p \equiv a \pmod p$. ■

Exerciţiul 138 Să se calculeze cel mai mic rest pozitiv:
a) $2^{1000000} \mod 77$; b) $3^{400} \mod 100$ c) $3^{100000} \mod 101$.

Exerciţiul 139 Să se arate că $42 \mid n^7 - n$ şi $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \mid n^{13} - n$ pentru orice $n \in \mathbb{N}$.

7.3.6 Rezolvarea congruenţelor şi a ecuaţiilor diofantice de gradul I

A. Congruenţa $ax \equiv b \pmod n$

Fie $a, b \in \mathbb{Z}$, $n \in \mathbb{N}^*$, $n \geq 2$ date şi fie $x \in \mathbb{Z}$ necunoscuta. Fie $d := (a, n)$, $a = a'd$, $n = n'd$, deci $(a', n') = 1$.

- Dacă x este soluţie $\Rightarrow b - ax = nk$ cu $k \in \mathbb{Z} \Rightarrow b = ax + nk$, este divizibil cu d, deoarece $a \vdots d$ şi $n \vdots d$. Deci dacă $d \nmid b$ atunci nu există soluţie.
- Presupunem că $d | b$ şi fie $b = b'd$. Atunci $ax \equiv b \pmod n \Leftrightarrow a'x \equiv b' \pmod{n'}$ (1).

Congruenţa (1) este echivalentă cu ecuaţia $\widehat{a'}\widehat{x} = \widehat{b'}$ în $\mathbb{Z}_n$. Din $(a', n') = 1 \Rightarrow \exists\ \widehat{a'}^{-1} \in U(\mathbb{Z}_{n'})$ ($\widehat{a'}^{-1}$ se determină cu algoritmul lui Euclid). Deci în $\mathbb{Z}_{n'}$ avem soluţie unică $\hat{x} = \widehat{b'}\widehat{a'}^{-1}$. Fie cel mai mică soluţie pozitivă x_0 a lui (1) ($0 \leq x_0 < n'$). Atunci cele d soluţii distincte (adică necongruente modulo n) ale congruenţei (A) sunt: $x_0,\ x_0 + n',\ \ldots,\ x_0 + (d-1)n'$ (mai exact, acestea sunt cele mai mici soluţii pozitive).

Exerciţiul 140 Să se rezolve congruenţele:
a) $x \equiv 2 \pmod 3$; b) $9x \equiv 12 \pmod{21}$; c) $27x \equiv 72 \pmod{900}$; d) $68x \equiv 16 \pmod{72}$.

Exerciţiul 141 Să se rezolve în $\mathbb{Z}_{18}$ ecuaţiile:
a) $\hat{7}x = \widehat{15}$; b) $\hat{8}x = \widehat{11}$; c) $\widehat{10}x = \widehat{16}$.

B. Ecuaţia diofantică $a_1x_1 + \cdots + a_nx_n = c$

1) Fie $n = 2$. Considerăm ecuaţia

$$ax + by = c,$$

unde $a, b, c \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$ sunt date, $x, y \in \mathbb{Z}$ sunt necunoscute.

Fie $d = (a, b)$. Dacă $\exists\,(x, y)$ soluţie, atunci $d \mid c$. Deci, dacă $d \nmid c$ atunci nu există soluţie.

Presupunem deci că $d \mid c$. Fie $a = a'd$, $b = b'd$. Căutăm o soluţie particulară. Fie $u, v \in \mathbb{Z}$ astfel încât $d = au + bv$ (folosim algoritmul lui Euclid). Înmulţim cu c': $\Longrightarrow c = ac'u + bc'v$. Fie $x_0 := c'u$, $y := c'v$, deci (x_0, y_0) este soluţie particulară.

Căutăm acum soluţa generală. Avem

$$ax + by = c \Longleftrightarrow ax + by = ax_0 + by_0 \Longleftrightarrow a\,(x - x_0) + b\,(y - y_0) = 0 \Longleftrightarrow a'(x - x_0) + b'(y - y_0) = 0.$$

Presupunem că $(x, y) \in \mathbb{Z}$ este soluţie. Rezultă, că $a' \mid b'\,(y - y_0)$, $b' \mid a'\,(x - x_0)$ Dar $(a', b') = 1$, deci $a' \mid y - y_0$, $b' \mid x - x_0$. Rezultă, că $y - y_0 = a't$, unde $t \in \mathbb{Z}$. De aici $a'\,(x - x_0) + b'a't = 0$, deci $x - x_0 = -b't$. Deci soluţia este:

$$\begin{cases} x = x_0 - b't \\ y = y_0 + a't \end{cases},$$

unde $t \in \mathbb{Z}$. Invers, este evident că pentru orice $t \in \mathbb{Z}$ avem că $(x = x_0 - b't, y = y_0 + a't)$ este într-adevăr soluţie a ecuaţiei $ax + by = c$.

2) În general, arătăm cěcuaţia $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ are soluţie dacă şi numai dacă $(a_1, \ldots, a_n) \mid c$.

Într-adevăr, dacă ecuaţia $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ are soluţie, atunci $(a_1, \ldots, a_n)$ divide membrul stâng, deci şi pe cel drept. Invers, presupunem că $c = (a_1, \ldots, a_n)c'$. Există numerele întregi $x'_1, \ldots, x'_n$ astfel ca

$$a_1x'_1 + a_2x'_2 + \ldots + a_nx'_n = (a_1, \ldots, a_n).$$

Înmulţim cu c' şia obţinem:

$$x_1 = c'x'_1,\ x_2 = c'x'_2,\ \ldots,\ x_n = c'x'_n.$$

Observaţii 7.3.21 Observăm că ecuaţia $ax + by = c$ este echivalentă cu congruenţa $ax \equiv c \pmod b$ sau cu $by \equiv c \pmod a$.

Fie $d = (a, b)$, atunci $a = a_1 d$, $b = b_1 d$ şi $c = c_1 d$, unde $(a_1, b_1) = 1$. Atunci în inelul$\mathbb{Z}_{b_1}$ avem

$$a_1 x + b_1 y = c_1 \Leftrightarrow a_1 x \mid c_1 \pmod{b_1} \Leftrightarrow \hat{a_1}\hat{x_1} = \hat{c_1}.$$

Dar $(a_1, b_1) = 1 \Rightarrow \exists \hat{a}_1^{-1}$ de underezultă că $\hat{x} = \hat{a}_1^{-1} c_1$ este unica soluţie.

Exemplul 7.3.22 Considerăm ecuaţia $18x + 28y = 10$. Deoarece $(18, 28) = 2 \mid 10$ rezultă că există soluţie. Considerăm ecuaţia redusă $9x + 14y = 5$. Rezolvăm congruenţa $9x \equiv 5 \pmod{14}$, adică ecuaţia $\hat{9}\hat{x} = \hat{5}$ în $\mathbb{Z}_{14}$. Avem $(9, 14) = 1 \Rightarrow \exists u\ ,v \in \mathbb{Z}$: $9u + 14v = 1$. Deoarece $14 = 9 \cdot 1 + 5$, $9 = 5 \cdot 1 + 4$, $5 = 4 \cdot 1 + 1$, obţinem $u = -3$, $v = 2$. Deci $\hat{x} = \hat{11} \cdot \hat{5}$ în inelul $\mathbb{Z}_{14}$, adică $x \equiv 13 \pmod{14}$.

Exemplul 7.3.23 (Rezolvarea prin micşorarea modulului coeficienţilor) 1) Considerăm ecuaţia $25x + 7y = 4$. Deoarece $|25| > |7|$, exprimăm pe y:

$$\begin{aligned}
&y = \frac{4 - 25x}{7} = \frac{4 + 3x}{7} - 4x \in \mathbb{Z} \Leftrightarrow 4 + 3x = 7z,\ |3| < |7| \\
&x = \frac{7z - 4}{3} = \frac{6z + z - 3 - 1}{3} = 2z - 1 + \frac{z - 1}{3} \in \mathbb{Z} \Leftrightarrow z - 1 = 3t \Leftrightarrow z = 3t + 1 \\
&\Rightarrow x = \frac{21t + 3}{3} = 7t + 1,\ y = \frac{4 - 175t - 25}{7} = -25t - 3, \quad t \in \mathbb{Z}.
\end{aligned}$$

2) Să se rezolve ecuaţia $16x - 23y + 9z = 15$. Este util să începem cu cel mai mic coeficient în modul:

$$z = \frac{15 - 16x + 23}{5} = 1 - 2x + 2y + \frac{6 + 2x + 5y}{9}.$$

Notăm $\frac{6+2x+5y}{9} = t$. De aici $2x + 5y - 9t = -6$. Continuăm ca mai sus:

$$x = \frac{-6 - 5y + 9t}{2} = -3 - 2y + 4t + \frac{-y + t}{2}.$$

Notăm $\frac{-y+t}{2} = u$, de unde $y = t - 2u$. Înlocuim în x, apoi în z. Atunci obţinem

$$x = -3 + 2t + 5u, \qquad y = t - 2u, \qquad z = 7 - t - 14u, \qquad t, u \in \mathbb{Z}.$$

Verificăm că acestea sunt soluţii:

$$16(-3 + 2t + 5u) - 23(t - 2u) + 9(7 - t - 14u) = 25 + (32 - 23 - 9)t + (80 + 46 - 126)u = 25.$$

Exerciţiul 142 Să se rezolve:

1) $12x + 31y = 23$; 2) $25x - 13y - 7z = 4$; 3) $\begin{cases} 25x - 13y + 7z = 4 \\ 7x + 4y - 2z + 3t = 2 \end{cases}$

7.3.7 Teorema chineză a resturilor. Sisteme de congruenţe

Teorema 7.3.24 (Teorema chineză a resturilor) *Fie* $n_1, \dots, n_r \in \mathbb{N}^*$, $(n_i, n_j) = 1$, $1 \le i, j \le r$, $i \ne j$. *Atunci*

$$\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r} \simeq \mathbb{Z}_{n_1 \cdots n_r}.$$

Demonstraţie. Fie funcţia $f : \mathbb{Z} \to \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}$ $f(a) = ([a]_{n_1}, \dots, [a]_{n_r})$. Arătăm că f este omomorfism de inele:

$$\begin{aligned}
f(a + b) &= ([a + b]_{n_1}, \dots, [a + b]_{n_r}) = ([a]_{n_1} + [b_{n_1}], \dots, [a]_{n_r} + [b]_{n_r}) = \\
&= ([a]_{n_1}, \dots, [a]_{n_r}) + ([b]_{n_1}, \dots, [b]_{n_r}) = f(a) + f(b) \\
f(ab) &= ([ab]_{n_1}, \dots, [ab]_{n_r}) = ([a]_{n_1}[b_{n_1}], \dots, [a]_{n_r}[b]_{n_r}) = \\
&= ([a]_{n_1}, \dots, [a]_{n_r})([b]_{n_1}, \dots, [b]_{n_r}) = f(a)f(b)
\end{aligned}$$

Determinăm pe $\operatorname{Ker} f$:

$$\begin{aligned}
\operatorname{Ker} f &= \{a \in \mathbb{Z} \mid f(a) = ([a]_{n_1}, \dots, [a]_{n_r}) = ([0]_{n_1}, \dots, [0]_{n_r})\} = \\
&= \{a \in \mathbb{Z} \mid n_i | b,\ i = 1, \dots, r\} = \\
&= \{a \in \mathbb{Z} \mid n_1 \dots n_r | a\} = n_1 \dots n_r \mathbb{Z}.
\end{aligned}$$

Din Teorema I de izomorfism 8.3.4 rezultă că avem izomorfismul de inele

$$\bar{f} : \mathbb{Z}/\operatorname{Ker} f \longrightarrow \operatorname{Im} f, \quad \bar{f}([a]_{n_1 \cdot \ldots \cdot n_r}) = f(a) = ([a]_{n_1}, \ldots, [a]_{n_r}),$$

unde $\mathbb{Z}/\operatorname{Ker} f = \mathbb{Z}_{n_1 \ldots n_r}$ şi $\operatorname{Im} f \subseteq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$. Arătăm prin două metode că $\bar{f}$ este surjectiv.

(1) Deoarece $|\mathbb{Z}_{n_1 \ldots n_r}| = n_1 \ldots n_r$ şi $\bar{f}$ este bijectiv, rezultă că $|\operatorname{Im} f| = n_1 \ldots n_r$. Dar $\operatorname{Im} f \subseteq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$, şi $|\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}| = n_1 \ldots n_r$, deci $\operatorname{Im} f = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$.

(2) Bijectivitatea lui $\bar{f}$ este echivalentă cu afirmaţia că pentru orice $a_1, \ldots, a_r \in \mathbb{Z}$ sistemul de congruenţe

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \quad\vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$

are soluţie în $\mathbb{Z}$ şi mai mult, orice două soluţii sunt congruente modulo $n_1 \cdots n_r$. Pentru exprimarea soluţiei introducem notaţiile: $N := n_1 \cdots n_r$, $M_i := \frac{N}{n_i}$. Aici $(M_i, n_i) = 1$ deoarece $(n_i, n_j) = 1$ pentru orice $i \neq j$. Rezultă că există $u_i \in \mathbb{Z}$ astfel încât

$$M_i u_i \equiv 1 \pmod{n_i}$$

(amintim că u_i se calculează cu algoritmul lui Euclid). Fie

$$x := \sum_{i=1}^{r} a_i M_i u_i.$$

Atunci $x \equiv a_i \pmod{n_i}$, deoarece $M_j \equiv 0 \pmod{n_i}$, dacă $j \neq i$. Deci x este unica soluţie modulo N. ■

Exerciţiul 143 Să se rezolve sistemele de congruenţe:

$$\text{a)} \begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 5 \pmod 7 \end{cases}; \qquad \text{b)} \begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 4 \pmod 5 \\ x \equiv 6 \pmod 7 \end{cases}; \qquad \text{c)} \begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 6 \pmod 7 \\ x \equiv 8 \pmod{16} \end{cases}.$$

Corolar 7.3.25 *Presupunem că $n_1, \ldots, n_r \in \mathbb{N}^*$ relativ prime două câte două. Atunci avem izomorfismul de grupuri*

$$U(\mathbb{Z}_{n_1 \cdot \ldots \cdot n_r}) \simeq U(\mathbb{Z}_{n_1}) \times \cdots \times U(\mathbb{Z}_{n_r}).$$

Demonstraţie. Din Teorema chineză a resturilor 7.3.24 rezultă că

$$(U(\mathbb{Z}_{n_1 \cdot \ldots \cdot n_r}), \cdot) \simeq (U(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}), \cdot) = (U(\mathbb{Z}_{n_1}) \times \cdots \times U(\mathbb{Z}_{n_r})). \qquad ■$$

Corolar 7.3.26 *Dacă $(m, n) = 1$, atunci $\varphi(mn) = \varphi(m)\varphi(n)$, adică funcţia φ a lui Euler este funcţie aritmetică multiplicativă. În general, dacă $(n_i, n_j) = 1, 1 \leq i < j \leq r$, atunci $\varphi(n_1 \cdot \cdots \cdot n_r) = \varphi(n_1) \cdots \varphi(n_r)$.*

Corolar 7.3.27 *Fie $n = p_1^{a_1} \ldots p_r^{a_r}$, unde p_i numere prime distincte şi $a_i \in \mathbb{N}^*$. Atunci*

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

Demonstraţie. Avem $\varphi(n) = \varphi(p_1^{a_1}) \cdot \cdots \cdot \varphi(p_r^{a_r})$. Conform definiţiei lui φ, trebuie să găsim numerele mai mici decât p^a şi relativ prime cu p^a. Dintre numerele $1, \ldots, p-1, p, p+1, \ldots, 2p-1, p, 2p+1, \ldots, p^a - 1, p^a$ fiecare al p-lea este divizibil cu p, iar celelalte sunt relativ prime cu p, deci

$$\varphi\left(p^a\right) = p^a - p^{a-1} = p^a \left(1 - \frac{1}{p}\right).$$

De aici afirmaţia rezultă imediat. ■

7.4 Mulţimea numerelor raţionale

Am văzut că $(\mathbb{Z}, +, \cdot, \leq)$ este domeniu de integritate total ordonat arhimedian. Vom extinde această structură pentru a obţine un corp comutativ total ordonat.

Definiţia 7.4.1 a) Pe mulţimea $\mathbb{Z} \times \mathbb{Z}^*$ definim relaţia omogenă

$$(a, b) \sim (c, d), \quad \text{dacă} \quad ad = bc,$$

şi se verifică uşor că este o relaţie de echivalenţă. Notăm prin $\widetilde{(a, b)}$ clasa de echivalenţă a perechii (a, b), deci

$$\widetilde{(a, b)} = \{(c, d) \in \mathbb{Z} \times \mathbb{Z}^* \mid (c, d) \sim (a, b)\}.$$

Mulţimea factor

$$\mathbb{Q} := \mathbb{Z} \times \mathbb{Z}^* / \sim = \{\widetilde{(a, b)} \mid (a, b) \in \mathbb{Z} \times \mathbb{Z}^*\}$$

se numeşte **mulţimea numere raţionale**. Un număr raţional se notează de obicei sub formă de **fracţie**, adică

$$\widetilde{(a, b)} = \frac{a}{b}.$$

Observăm că pentru $a \in \mathbb{Z}$ şi $b, c \in \mathbb{Z}^*$ avem $\frac{a}{b} = \frac{ac}{bc}$. În particular, $\frac{a}{b} = \frac{-a}{-b}$, deci putem întotdeauna alege un reprezentant cu numitor pozitiv, adică putem presupune că $b \in \mathbb{N}^*$.

b) Adunarea şi înmulţirea numerelor raţionale se definesc astfel:

$$\widetilde{(a, b)} + \widetilde{(c, d)} := (\widetilde{ad + bc, bd}), \qquad \widetilde{(a, b)}\widetilde{(c, d)} := (\widetilde{ac, bd}),$$

adică

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

Aceste definiţii nu depind de alegerea reprezentanţilor.

Teorema 7.4.2 *Structura algebrică $(\mathbb{Q}, +, \cdot)$ este un corp comutativ, în care elementul nul este*

$$0 := \widetilde{(0, 1)} = \{(0, b) \mid b \in \mathbb{Z}^*\} = \frac{0}{a}, \quad a \in \mathbb{Z}^*,$$

elementul unitate este

$$1 := \widetilde{(1, 1)} = \{(a, a) \mid a \in \mathbb{Z}^*\} = \frac{a}{a}, \quad a \in \mathbb{Z}^*,$$

opusul numărului raţional $\widetilde{(a, b)}$ este

$$-\widetilde{(a, b)} := \widetilde{(-a, b)} = \widetilde{(a, -b)}, \quad \text{adică} \quad -\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b},$$

şi dacă $a, b \in \mathbb{Z}^*$, atunci inversul lui $\widetilde{(a, b)}$ este

$$\widetilde{(a, b)}^{-1} = \widetilde{(b, a)}, \quad \text{adică} \quad \left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

Exerciţiul 144 a) Să se arate că relaţia „~" este o relaţie de echivalenţă.

b) Să se arate că definiţiile adunării şi înmulţirii nu depind de alegerea reprezentanţilor.

c) Să se demonstreze Teorema 7.4.2.

Definiţia 7.4.3 Numerele raţionale se ordonează prin relaţia:

$$\frac{a}{b} \leq \frac{c}{d}, \quad \text{dacă} \quad (bc - ad)bd \geq 0.$$

b) **Valoarea absolută (modulul)** numărului raţional $a \in \mathbb{Q}$ este $|a| := \begin{cases} a, & \text{dacă } a \geq 0, \\ -a, & \text{dacă } a < 0 \end{cases}.$

Teorema de mai jos spune că structura $(\mathbb{Q}, +, \cdot, \leq)$ este un **corp comutativ total ordonat arhimedian**, în care se scufundă domeniul de integritate total ordonat al numerelor întregi.

Teorema 7.4.4 1) *Definiţia relaţiei ,,$\leq$" nu depinde de alegerea reprezentanţilor.*

2) $(\mathbb{Q}, \leq)$ *este total ordonat.*

3) *Funcţia* $\alpha : \mathbb{Z} \to \mathbb{Q}$, $\alpha(a) = \widetilde{(a, 1)} = \frac{a}{1}$ *este bine definită, strict crescătoare (deci injectivă) şi este morfism unital de inele.*

4) *Ordonarea numerelor raţionale este compatibilă cu adunarea şi înmulţirea, adică dacă* $x, y, z, t \in \mathbb{Q}$, *atunci*

$$x < y, z \leq t \Rightarrow x + z < y + t, \qquad x < y, z > 0 \Rightarrow xz < yz, \qquad x < y, z < 0 \Rightarrow xz > yz.$$

5) **(Axioma lui Arhimede)** $\forall x \in \mathbb{Q}_+^*$, $\forall y \in \mathbb{Q}$, $\exists n \in \mathbb{N}$ *astfel ca* $nx > y$.

Observaţii 7.4.5 Vom identifica numărul întreg a cu $\alpha(a) = \frac{a}{1}$ şi astfel $\mathbb{Z} \subset \mathbb{Q}$. Observăm că $\frac{a}{b} = \alpha(a)\alpha(b)^{-1}$.

Exerciţiul 145 Să se demonstreze Teorema 7.4.4.

Exerciţiul 146 Să se arate că pentru orice $x, y \in \mathbb{Q}$

$$|x| = |-x|, \qquad |xy| = |x||y|, \qquad |x + y| \leq |x| + |y|, \qquad ||x| - |y|| \leq |x - y|.$$

7.5 Mulţimea numerelor reale

7.5.1 Fie K un corp comutativ total ordonat. Din analiza matematică ştim că umătoarele afirmaţii sunt echivalente:

(i) Orice şir monoton şi mărginit de elemente din K este convergent.

(ii) Orice submulţime nevidă şi mărginită inferior (superior) a lui K are infimum (supremum).

(iii) Corpul K satisface axioma lui Arhimede şi orice şir Cauchy de elemente din K este convergent.

(iv) Corpul K satisface axioma lui Dedekind (adică orice tăietură Dedekind a lui K este generată de un element al lui K).

Nu este greu de văzut că numerele raţionale fomează un corp comutativ total ordonat care nu este complet în sensul de mai sus. Pornind de la corpul $\mathbb{Q}$ al numerelor raţionale, vom construi o extindere a sa care este un corp comutativ total ordonat şi complet, numit corpul numerelor reale.

Definiţia 7.5.2 a) Considerăm mulţimea şirurilor de numere raţionale, pe care o notăm

$$\mathbb{Q}^{\mathbb{N}} = \{(a_n) \mid a_n \in \mathbb{Q}\};$$

acesta este un inel comutativ cu operaţiile $(a_n) + (b_n) = (a_n + b_n)$, respectiv $(a_n)(b_n) = (a_n b_n)$; elementul nul este şirul constant (0), iar elementul unitate este şirul constant (1). În general notăm prin (a) şirul constant în care fiecare termen este egal cu a. Considerăm următoarele submulţimi ale lui $\mathbb{Q}^{\mathbb{N}}$:

b) mulţimea şirurilor mărginite

$$\mathcal{B} = \{(a_n) \in \mathbb{Q}^{\mathbb{N}} \mid \exists b \in \mathbb{Q}_+^* \text{ astfel ca } \forall n \in \mathbb{N} : |a_n| < b\}.$$

c) mulţimea şirurilor Cauchy

$$\mathcal{C} = \{(a_n) \in \mathbb{Q}^{\mathbb{N}} \mid \forall \epsilon \in \mathbb{Q}_+^* \ \exists n_\epsilon \in \mathbb{N} \text{ astfel ca } \forall m, n > n_\epsilon : |a_m - a_n| < \epsilon\}.$$

d) mulţimea şirurilor convergente la zero

$$\mathcal{N} = \{(a_n) \in \mathbb{Q}^{\mathbb{N}} \mid \forall \epsilon \in \mathbb{Q}_+^* \ \exists n_\epsilon \in \mathbb{N} \text{ astfel ca } \forall n > n_\epsilon : |a_n| < \epsilon\}.$$

Se arată uşor că $\mathcal{N} \subseteq \mathcal{C} \subseteq \mathcal{B}$, mai mult, $\mathcal{C}$ este subinel unital al lui $\mathbb{Q}^{\mathbb{N}}$-nek, iar $\mathcal{N}$ este ideal al lui $\mathcal{B}$ (deci şi al lui $\mathcal{C}$.

e) Considerăm relaţia de echivalenţă ,,$\sim$" pe $\mathcal{C}$ definită prin

$$(a_n) \sim (b_n) \text{ dacă } (a_n - b_n) \in \mathcal{N},$$

Notăm prin $\widetilde{(a_n)}$ clasa de echivalenţă a şirului $(a_n) \in \mathcal{C}$, deci

$$\widetilde{(a_n)} = (a_n) + \mathcal{N} = \{(a_n + b_n) \mid (b_n) \in \mathcal{N}\}.$$

f) Mulţimea factor $\mathbb{R} := \mathcal{C}/\sim = \{\widetilde{(a_n)} = (a_n) + \mathcal{N} \mid (a_n) \in \mathcal{C}\}$ se numeşte **mulţimea numerelor reale**.

g) Adunarea şi înmulţirea numerelor reale se definesc astfel:

$$\widetilde{(a_n)} + \widetilde{(b_n)} := \widetilde{(a_n + b_n)}, \qquad \widetilde{(a_n)}\widetilde{(b_n)} := \widetilde{(a_n b_n)}.$$

Teorema 7.5.3 $(\mathbb{R},+,\cdot)$ *este un corp comutativ în care elementul nul este* $0 := \widetilde{(0)} = (0)+\mathcal{N}$, *iar elementul unitate este* $1 := \widetilde{(1)} = (1)+\mathcal{N}$.

Exerciţiul 147 a) Să se arate că $(\mathbb{Q}^{\mathbb{N}},+,\cdot)$ este un inel comutativ, $\mathcal{N}\subseteq\mathcal{C}\subseteq\mathcal{B}$, $\mathcal{C}$ şi $\mathcal{B}$ sunt subinele unitale ale lui $\mathbb{Q}^{\mathbb{N}}$, iar $\mathcal{N}$ este un ideal al lui $\mathcal{B}$.

b) Să se arate că ,,$\sim$" este relaţie de echivalenţă pe $\mathcal{C}$.

c) Să se arate că definiţiile operaţiilor ,,$+$" şi ,,$\cdot$" nu depind de alegerea reprezentanţilor.

d) Să se demonstreze Teorema 7.5.3.

Definiţia 7.5.4 a) Introducem submulţimile:

$$\mathbb{R}_+^* := \{\widetilde{(a_n)}\in\mathbb{R} \mid \exists r\in\mathbb{Q}_+^*\ \exists N\in\mathbb{N} \text{ astfel ca } \forall n>N: a_n>r\},$$

$$\mathbb{R}_-^* := \{\widetilde{(a_n)}\in\mathbb{R} \mid \exists r\in\mathbb{Q}_+^*\ \exists N\in\mathbb{N} \text{ astfel ca } \forall n>N: a_n<-r\}.$$

b) Spunem că $\alpha<\beta$, dacă $\beta-\alpha\in\mathbb{R}_+^*$. Ordonăm numerele reale prin relaţia

$$\alpha\le\beta \text{ dacă } \alpha<\beta \text{ sau } \alpha=\beta.$$

Teorema 7.5.5 1) $\alpha\in\mathbb{R}_+^* \iff -\alpha\in\mathbb{R}_-^*$.

2) *Submulţimile* $\mathbb{R}_+^*$, $\{0\}$, $\mathbb{R}_-^*$ *formează o partiţie a lui* $\mathbb{Z}$ *(adică sunt disjuncte două câte două şi avem* $\mathbb{R} = \mathbb{R}_+^*\cup\{0\}\cup\mathbb{R}_-^*$*).*

3) $(\mathbb{R},\le)$ *este o mulţime total ordonată.*

4) *Funcţia* $\varphi:\mathbb{Q}\to\mathbb{R}$, $\varphi(a)=\widetilde{(a)}=(a)+\mathcal{N}$ *este strict crescătoare (deci injectivă) şi este morfism de corpuri. Vom identifica numărul raţional* a *cu* $\varphi(a)$ *şi astfel* $\mathbb{Q}\subset\mathbb{R}$.

5) *Ordonarea numere reale este compatibilă cu adunarea şi înmulţirea, adică dacă* $\alpha,\beta,\gamma,\delta\in\mathbb{R}$, *atunci*

$$\alpha<\beta,\gamma\le\delta\Rightarrow\alpha+\gamma<\beta+\delta,\qquad \alpha<\beta,\gamma>0\Rightarrow\alpha\gamma<\beta\gamma,\qquad \alpha<\beta,\gamma<0\Rightarrow\alpha\gamma>\beta\gamma.$$

6) **(Axioma lui Arhimede)** $\forall\alpha\in\mathbb{R}_+^*$, $\forall\beta\in\mathbb{R}$, $\exists n\in\mathbb{N}$ *astfel ca* $n\alpha>\beta$.

7) *Dacă* $\alpha,\beta\in\mathbb{R}$ *şi* $\alpha<\beta$, *atunci* $\exists r\in\mathbb{Q}$ *astfel ca* $\alpha<r<\beta$. (Spunem că $\mathbb{Q}$ este submulţime **densă** a lui $\mathbb{R}$)

8) *Dacă* $(\alpha_n)\in\mathbb{R}^{\mathbb{N}}$ *este un şir Cauchy de numere reale, atunci* $\exists\lim_{n\to\infty}\alpha_n\in\mathbb{R}$. *În particular, dacă* $(a_n)\in\mathcal{C}$, *atunci* $\lim_{n\to\infty}a_n=(a_n)+\mathcal{N}$.

Exerciţiul 148 a) Să se arate că definiţia relaţiei ,,$\le$" nu depinde de alegerea reprezentanţilor.

b) Să se demonstreze Teorema 7.5.5.

Teorema 7.5.5 spune că $(\mathbb{R},+,\cdot,\le)$ este un corp comutativ total ordonat arhimedian şi complet în sensul lui Cauchy (sau echivalent, conform 7.5.1, corp comutativ total ordonat complet în sensul lui Dedekind. Aceste proprietăţi determină unic corpul numerelor reale pâna la un (unic) izomorfism.

Teorema 7.5.6 (unicitatea corpului numerelor reale) *Dacă* K *este un corp comutativ total ordonat complet, atunci există un unic izomorfism de corpuri ordonate de la* K *la* $\mathbb{R}$.

Exerciţiul 149 Să se demonstreze Teorema 7.5.6.

Capitolul 8

ALGEBRE UNIVERSALE

O *structură* matematică este o mulţime (sau mai multe mulţimi) dotată cu operaţi (de obicei finitare), relaţii, topologii etc. care satisfac anumite condiţii de compatibilitate. O structură algebrică este o mulţime dotată cu operaţii ce satisfac a listă de *axiome*, care de obicei se scriu sub forma unor identităţi polinomiale (sau legi ecuaţionale). Exemplele cele mai cunoscute sunt axiomele de asociativitate şi comutativitate pentru o operaţie binară. O clasă de structuri algebrice definită prin identităţi se numeşte *varietate* sau *clasă ecuaţională*. Exemplele uzuale de structuri algebrice formează varietăţi: grupuri, inele, latice. Clasa corpurilor nu este o varietate deoarece nu toate axiomele corpului pot fi exprimate ca ecuaţii. Exemple mai complexe de structuri algebrice sunt spaţiile vectoriale peste un corp, modulele peste un inel şi algebrele peste un inel comutativ. Uneori sunt permise şi operaţii infinitare, astfel putând fi inclus aici şi studiul laticelor complete. Corpurile ordonate sau grupurile topologice sunt exemple de structuri mixte. Alte exemple de structuri sunt grafurile (sau reţelele), bazele de date relaţionale şi universurile din teoria mulţimilor.

În cadrul algebrei abstracte se studiază proprietăţile unor structuri particulare, punctul de vedere fiind acela că structurile izomorfe sunt considerate identice. Algebra universală este studiul structurilor algebrice generale.

Teoria categoriilor studiază legăturile dintre diferite structuri. De exemplu, teoria lui Galois stabileşte o conexiune între anumite corpuri comutative şi grupuri. Structurile algebrice pot fi definite în orice categorie ce are produse directe finite. De exemplu, un grup topologic este un grup în categoria spaţiilor topologice. Într-o categorie, noţiunile pot fi dualizate, obţinându-se astfel noi structuri, cum ar fi cogrupurile sau coalgebrele peste un inel comutativ.

Teoria modelelor, ca domeniu interdisciplinar ce leagă matematica, logica, filosofia şi informatica, este investigarea claselor de structuri matematice din perspectiva logicii matematice. Ca obiecte de studiu sunt modelele teoriilor într-un limbaj formal. O teorie este o mulţime de propoziţii într-un limbaj formal (de exemplu, logica de ordinul I); un model al teoriei este o structură (adică o interpretare) ce satisface propoziţiile (axiomele) teoriei. Teoria modelelor examinează semantica (semnificaţie şi adevăr) prin intermediul sintaxei limbajului respectiv (formule şi demonstraţii).

8.1 Ω-algebre şi omomorfisme

Definiţia 8.1.1 a) Fie A o mulţime şi $n \in \mathbb{N}$. O funcţie $\omega : A^n \to A$ se numeşte **operaţie** pe mulţimea A. Spunem că $n = \tau(\omega)$ este **tipul** sau **aritatea** lui ω.

b) Fie Ω o mulţime de operaţii pe mulţimea A. Perechea (A, Ω) se numeşte **algebră universală** sau Ω-algebră.

Algebra universală (A, Ω) determină o funcţie $\tau : \Omega \to \mathbb{N}$, unde $\tau(\omega)$ este tipul lui ω. Spunem că τ este **tipul** lui (A, Ω).

Exemplul 8.1.2 1) Dacă $n = 0$, atunci $A^n = \{\emptyset\}$, deci $\omega : A^0 \to A$ este unic determinat, dacă se dă u elementul $\omega(\emptyset) \in A$. De exemplu, în $\mathbb{R}$, elementele 0 şi 1 pot fi cosiderate operaţii nulare.

2) Dacă $n = 1$, atunci $A^n = A$, deci orice funcţie $\omega : A \to A$ este operaţie unară. De exemplu, $\omega : \mathbb{R} \to \mathbb{R}$, $\omega(x) = -x$ este operaţie unară pe $\mathbb{R}$.

3) Dacă M este o mulţime, atunci $(\mathcal{P}(M), \cup, \cap, \complement, \emptyset, M)$ este algebră universală de tip $\tau = \begin{pmatrix} \cup & \cap & \complement & \emptyset & M \\ 2 & 2 & 1 & 0 & 0 \end{pmatrix}$.

4) Dacă $\mathcal{R}_2(M) = \{\rho = (M, M, R) \mid R \subseteq M \times M\}$ este mulţimea relaţiilor binnare pe mulţimea M, atunci $(\mathcal{R}_2(M), \cup, \cap, \circ, \complement, ^{-1})$ este algebră universală de tip $\tau = \begin{pmatrix} \cup & \cap & \circ & \complement & ^{-1} \\ 2 & 2 & 2 & 1 & 1 \end{pmatrix}$.

Exerciţiul 150 Fie A o mulţime cu m elemente şi fie $n \in \mathbb{N}$. Câte operaţii n-are există pe A?

Definiţia 8.1.3 Fie (A, Ω), (A', Ω') algebre universale şi $\theta : \Omega \to \Omega'$ o funcţie astfel încât $\tau'(\theta(\omega)) = \tau(\omega)$.

a) Funcţia $f : A \to A'$ se numeşte **θ-omomorfism**, dacă pentru orice $\omega \in \Omega$ şi pentru orice $a_1, \dots, a_n \in A$ (unde $n = \tau(\omega)$) avem

$$f(\omega(a_1, \dots, a_n)) = \theta(\omega)(f(a_1), \dots, f(a_n)).$$

b) Spunem că f este θ-izomorfism, dacă f şi θ sunt funcţii bijective, f θ-omomorfism şi f^{-1} este θ^{-1}-izomorfism.

c) Dacă $(A, \Omega) = (A', \Omega')$ şi $\theta = 1_\Omega$, atunci f se numeşte **endomorfism**, respectiv **automorfism**.

Observaţii 8.1.4 1) Funcţia identică $1_A : (A, \Omega) \to (A, \Omega)$ este automorfism al lui (A, Ω).

2) În general, pentru simplificare, vom nota pe Ω' prin Ω-val şi pe $\theta(\omega)$ prin ω.

3) $f : (A, \Omega) \to (A', \Omega)$ este izomorfism dacă şi numai dacă f omomorfism bijectiv.

Într-adevăr, presupunem că f omomorfism bijectiv h şi arătăm că şi f^{-1} este omomorfism. Fie $\omega \in \Omega$, $\tau(\omega) = n$, $b_1, \dots, b_n \in A'$ şi $a_i = f^{-1}(b_i)$, $i = 1, \dots, n$. Atunci

$$\begin{aligned} f^{-1}(\omega(b_1, \dots, b_n)) &= f^{-1}(\omega(f(a_1), \dots, f(a_n))) = f^{-1}(f(\omega(a_1, \dots, a_n))) = \\ &= \omega(a_1, \dots, a_n) = \omega(f^{-1}(b_1), \dots, f^{-1}(b_n)). \end{aligned}$$

Exerciţiul 151 Să se arate că $f : (A, \Omega) \to (A', \Omega)$ este θ-omomorfism dacă şi numai dacă pentru orice $\omega \in \Omega$, notând $f^{\tau(\omega)} := f \times \cdots \times f : A^{\tau(\omega)} \to {A'}^{\tau(\omega)}$, următoarea diagramă este comutativă:

$$\begin{array}{ccc} A^{\tau(\omega)} & \xrightarrow{f^{\tau(\omega)}} & {A'}^{\tau(\omega)} \\ {\scriptstyle\omega}\downarrow & & \downarrow{\scriptstyle\theta(\omega)} \\ A & \xrightarrow{f} & A' \end{array}$$

Exemplul 8.1.5 (Produs direct de algebre universale) Fie $(A_i, \Omega)_{i \in I}$ o familie de Ω-algebre şi considerăm a produsul direct $(\prod_{i \in I} A_i, (p_i)_{i \in I})$.

Fie τ tip algebrelor. Dacă $\omega \in \Omega$ şi $(a_i^k)_{i \in I} \in P$, $k = 1, \dots, n$, $n = \tau(\omega)$, atunci fie

$$\omega((a_i^1)_{i \in I}, \dots, (a_i^n)_{i \in I}) = (\omega(a_i^1, \dots, a_i^n))_{i \in I}.$$

Astfel am definit pe $\prod_{i \in I} A_i$ o structură de Ω-algebră, iar proiecţia canonică $p_j : P \to A_j$ este omomorfism surjectiv pentru orice $j \in I$. Într-adevăr,

$$\begin{aligned} p_j(\omega((a_i^1)_{i \in I}, \dots, (a_i^n)_{i \in I})) &= p_j((\omega(a_i^1, \dots, a_i^n))_{i \in I}) = \omega(a_j^1, \dots, a_j^n) = \\ &= \omega(p_j((a_i^1)_{i \in I}), \dots, p_j((a_i^n)_{i \in I})). \end{aligned}$$

Dacă ω' este o altă operaţie de tip $\tau(\omega)$ definită pe P astfel încât

$$p_j(\omega'((a_i^1)_{i \in I}, \dots, (a_i^{\tau(\omega)})_{i \in I})) = \omega(p_j((a_i^1)_{i \in I}), \dots, p_j((a_i^{\tau(\omega)})_{i \in I})),$$

atunci $\omega = \omega'$, deoarece avem că

$$\omega((a_i^1)_{i \in I}, \dots, (a_i^{\tau(\omega)})_{i \in I}) = \omega'((a_i^1)_{i \in I}, \dots, (a_i^{\tau(\omega)})_{i \in I}).$$

Mai departe, dacă $f_i : (A_i, \Omega) \to (A_i', \Omega)$ sunt omomorfisme, $i \in I$, atunci

$$\prod_{i \in I} f_i : \prod_{i \in I} A_i \to \prod_{i \in I} A_i', \quad \prod_{i \in I} f_i((a_i)_{i \in I}) = (f_i(a_i))_{i \in I}$$

este de asemenea omomorfism.

8.2 Subalgebre

Definiţia 8.2.1 Fie (A, Ω) o algebră universală şi $B \subseteq A$. Spunem că B este *subalgebră* a lui A (notaţie: $B \leq (A, \Omega)$), dacă

$$\forall\ \omega \in \Omega,\ \tau(\omega) = n,\ \forall\ a_1, \dots, a_n \in B, \quad \omega(a_1, \dots, a_n) \in B.$$

Vom nota mulţimea subalgebrelor lui A prin $\mathcal{S}(A, \Omega)$.

Observaţii 8.2.2 1) Dacă $B \in \mathcal{S}(A,\Omega)$, atunci orice $\omega \in \Omega$ induce o operaţie pe submulţimea B, deci şi (B,Ω) este algebră universală.

2) Mulţimea vidă $\emptyset$ este subalgebră dacă şi numai dacă Ω nu conţine operaţii nulare.

Exemplul 8.2.3 1) Fie M o mulţime şi $N \subseteq M$. Atunci $\mathcal{P}(N)$ este subalgebră a algebrei $(\mathcal{P},\cup,\cap)$ dar nu şi a lui $(\mathcal{P},\cup,\cap,\complement)$.

3) Fie $\mathcal{F}(M)=\{f \mid f: M\to M\}$, $\mathcal{F}_i(M)=\{f: M\to M \mid\ f\ \text{injectivă}\}$, $\mathcal{F}_s(M)=\{f: M\to M \mid f\ \text{surjectiv}\}$, $\mathcal{F}_b(M)=\{f: M\to M \mid f\ \text{bijectiv}\}$. Atunci $\mathcal{F}_i(M), \mathcal{F}_s(M)$ şi $\mathcal{F}_b(M)$ sunt subalgebre ale lui $(\mathcal{F}(M),\circ)$.

Exerciţiul 152 Fie (A,Ω), (B,Ω), (C,Ω) algebre universale. Spunem că $\rho=(A,B,R)$ este **relaţie omomorfă**, dacă R este subalgebră a produsului direct $(A\times B,\Omega)$.

Să se arate că :

a) Dacă $f=(A,B,F)$ egy funcţie, atunci f omomorfism $\Leftrightarrow f$ este relaţie omomorfă;

b) Dacă $\rho=(A,B,R)$ şi $\sigma=(B,C,S)$ sunt relaţii omomorfe, atunci şi $\sigma\circ\rho$ şi ρ^{-1} sunt relaţii omomorfe;

c) Dacă $\rho=(A,B,R)$ este relaţie omomorfă şi $X\in\mathcal{S}(A,\Omega)$, atunci $\rho(X)\in\mathcal{S}(B,\Omega)$. (În particular, dacă $f: A\to B$ este omomorfism, atunci $f(X)\in\mathcal{S}(B,\Omega)$.)

Lema 8.2.4 *Dacă* (A,Ω) *este o algebră universală şi* $\mathcal{S}\subseteq\mathcal{S}(A,\Omega)$*, atunci*

$$\bigcap_{B\in\mathcal{S}} B \in \mathcal{S}(A,\Omega).$$

Demonstraţie. Fie $\omega\in\Omega$, $n=\tau(\omega)$ şi $b_1,\ldots,b_n\in\bigcap_{B\in\mathcal{S}}B$; rezultă că pentru orice $B\in\mathcal{S}$, $b_1,\ldots,b_n\in B$, deci $\omega(b_1,\ldots,b_n)\in\bigcap_{B\in\mathcal{S}}B$; rezultă că $\omega(b_1,\ldots,b_n)\in\bigcap_{B\in\mathcal{S}}B$. ■

Corolar 8.2.5 $(\mathcal{S}(A,\Omega),\subseteq)$ *este latice completă. Dacă* $\mathcal{S}\subseteq\mathcal{S}(A,\Omega)$*, atunci*

$$\inf_{\mathcal{S}(A,\Omega)}\mathcal{S}=\bigcap\{B\mid B\in\mathcal{S}\},\qquad \sup_{\mathcal{S}(A,\Omega)}\mathcal{S}=\bigcap\{C\in\mathcal{S}(A,\Omega)\mid C\supseteq B\ \forall\ B\in\mathcal{S}\}.$$

Demonstraţie. Rezultă din lema şi din Teorema 5.2.5 de caracterizare a laticilor complete. ■

Definiţia 8.2.6 Fie (A,Ω) algebră universală şi $X\subseteq A$. Din Lema 8.2.4 rezultă că

$$\langle X\rangle := \bigcap\{B\in\mathcal{S}(A,\Omega)\mid X\subseteq B\}\in\mathcal{S}(A,\Omega).$$

Spunem că $\langle X\rangle$ este **subalgebra generată** de submulţimea X.

Observaţii 8.2.7 Evident, $\langle X\rangle$ este cea mai mică subalgebră de conţine pe X, deci următoarele proprietăţi caracterizează pe $\langle X\rangle$:

(1) $X\subseteq\langle X\rangle$;

(2) $\langle X\rangle\in\mathcal{S}(A,\Omega)$;

(3) Dacă $X\subseteq B$ şi $B\in\mathcal{S}(A,\Omega)$, atunci $\langle X\rangle\subseteq B$.

Observăm că $\langle\langle X\rangle\rangle=\langle X\rangle$, şi $X\in\mathcal{S}(A,\Omega)\Leftrightarrow X=\langle X\rangle$.

Teorema 8.2.8 (caracterizarea subalgebrei generate) *Fie* (A,Ω) *o algebră universală şi* $X\subseteq A$*. Atunci*

$$\langle X\rangle=\bigcup_{i\in\mathbb{N}}X_i,$$

unde $X_0=X, X_{i+1}=X_i\cup\{\omega(x_1,\ldots,x_{\tau(\omega)})\mid \omega\in\Omega,\ x_1,\ldots,x_{\tau(\omega)}\in X_i\}$.

Demonstraţie. Fie $Y=\bigcup_{i\in\mathbb{N}}X_i$. Se vede uşor că

(1) $X\subseteq Y$;

(2) $Y\in\mathcal{S}(A,\Omega)$;

(3) Dacă $B\in\mathcal{S}(A,\Omega)$ şi $X\subseteq B$, atunci $Y\subseteq B$. ■

Exerciţiul 153 a) Fie M o mulţime şi $A\subseteq M$. Să se determine subalgebra lui $(\mathcal{P}(M),\cup,\cap,\complement)$ generată de $\{A\}$.

b) Fie $\mathcal{R}_2(M)$ mulţimea relaţiilor binare pe M şi fie $\rho\in\mathcal{R}_2(M)$ o relaţie reflexiv a şi simetrică. Să se determine subalgebra lui $(\mathcal{R}_2(M),\cup,\cap,\circ,{}^{-1})$ generată de $\{\rho\}$. Cine este aceată subalgebră dacă ρ este tranzitiv?

Exerciţiul 154 Fie A o Ω-algebra şi $X_0=\{\omega(\emptyset)\mid\omega\in\Omega,\ \tau(\omega)=0\}$. Să se arate că $\langle X_0\rangle=\langle\emptyset\rangle$ şi $\langle X_0\rangle$ este cel mai mic element al lui az $(\mathcal{S}(A,\Omega),\subseteq)$.

Exerciţiul 155 Fie A şi B două Ω-algebre şi fie $f : A \to B$ un omomorfism. Să se arate că:
a) Dacă $X \subseteq A$, atunci $f(\langle X \rangle) = \langle f(X) \rangle$.
b) Dacă $g : A \to B$ este un omomorfism, $\langle X \rangle = A$ şi $g_{|X} = f_{|X}$, atunci $g = f$.

Exerciţiul 156 Fie A o Ω-algebra. Elementul $a \in A$ se numeşte **non-generator**, dacă pentru orice $X \subseteq A$ avem

$$\langle X \cup \{a\} \rangle = A \Longrightarrow \langle X \rangle = A.$$

Subalgebra $M \leq (A, \Omega)$ se numeşte **maximală**, dacă $M \neq A$ şi pentru orice subalgebra B a lui A avem

$$M \subseteq B \Longrightarrow B = M \text{ sau } B = A.$$

Să se arate că :
a) Submulţimea $N(A) := \{a \in a \mid a \text{ non-generator}\}$ este subalgebră a lui (A, Ω);
b) Pentru orice automorfism $f : A \to A$ avem $f(N(A)) \subseteq N(A)$;
c) $N(A)$ coincide cu **subalgebra Frattini** $\Phi(A) := \bigcap_{M \text{ subalgebra maximală}} M$ a lui A.

8.3 Congruenţe. Algebre factor. Teoreme de izomorfism

Definiţia 8.3.1 Fie (A, Ω) o algebră universală şi $\rho = (A, A, R)$ o relaţie pe A. Spunem că ρ este **congruenţă** pe (A, Ω) (notaţie: $\rho \in \mathcal{C}(A, \Omega)$), dacă ρ este relaţie de echivalenţă şi este **compatibilă** cu operaţiile, adică: $\forall\ \omega \in \Omega$, $\forall\ a_1, \dots, a_{\tau(\omega)}, b_1, \dots, b_{\tau(\omega)} \in A$

$$a_i \ \rho \ b_i, \ i = 1, \dots, \tau(\omega) \Longrightarrow \omega(a_1, \dots, a_{\tau(\omega)}) \ \rho \ \omega(b_1, \dots, b_{\tau(\omega)}).$$

Exemplul 8.3.2 1) Relaţia $\equiv \pmod n$ definită pe $\mathbb{Z}$ este relaţie de congruenţă pe algebra $(\mathbb{Z}, +, \cdot, 0, 1, -)$.
2) Relaţia diagonală $1_A = (A, A, \Delta_A)$ şi relaţia universală $(A, A, A \times A)$ sunt congruenţe pe A.

Teorema 8.3.3 *Fie (A, Ω) o algebră universală şi $\rho \in \mathcal{C}(A, \Omega)$ o congruenţă. Pe mulţimea factor*

$$A/\rho = \{\rho\langle x \rangle \mid x \in A\}$$

există o unică structură de Ω-algebră astfel încât proiecţia canonică $p_\rho : A \to A/\rho$ să fie omomorfism.

Demonstraţie. Fie $\omega \in \Omega$ şi $\rho\langle x_1 \rangle, \dots, \rho\langle x_n \rangle$, unde $n = \tau(\omega)$. Definim

$$\omega(\rho\langle x_1 \rangle, \dots, \rho\langle x_n \rangle) = \rho\langle \omega(x_1, \dots, x_n) \rangle.$$

Arătăm că definiţia nu depinde de alegerea reprezentanţilor. Într-adevăr, fie $x_i' \in \rho\langle x_i \rangle$, $i = 1, \dots, n$. Atunci $x_i \rho x_i'$, $i = 1, \dots, n$, deci $\omega(x_1, \dots, x_n) \ \rho \ \omega(x_1', \dots, x_n')$, deoarece ρ este congruenţă.
Arătăm că p_ρ este omomorfism. Pentru orice $\omega \in \Omega$ şi $x_1, \dots, x_n \in A$ avem

$$p_\rho(\omega(x_1, \dots, x_n)) = \rho\langle \omega(x_1, \dots, x_n) \rangle = \omega(\rho\langle x_1 \rangle, \dots, \rho\langle x_n \rangle) = \omega(p_\rho(x_1), \dots, p_\rho(x_n)).$$

Presupunem acum că ω' este o operaţie n-ară pe mulţimea factor A/ρ astfel încât

$$p_\rho(\omega(x_1, \dots, x_n)) = \omega'(p_\rho(x_1), \dots, p_\rho(x_n))$$

pentru orice $x_1, \dots, x_n \in A$. Atunci

$$\begin{aligned}\omega(\rho\langle x_1 \rangle, \dots, \rho\langle x_n \rangle) &= \omega(p_\rho(x_1), \dots, p_\rho(x_n)) = p_\rho(\omega(x_1, \dots, x_n)) = \\ &= \omega'(p_\rho(x_1), \dots, p_\rho(x_n)) = \omega'(\rho\langle x_1 \rangle, \dots, \rho\langle x_n \rangle),\end{aligned}$$

deci $\omega = \omega'$. ∎

Exerciţiul 157 Fie A o Ω-algebră. Să se arate că Δ_A şi $A \times A$ sunt congruenţe pe (A, Ω) şi algebra factor $(A/\Delta_A, \Omega)$ este izomorfă cu (A, Ω). Câte elemente are algebra factor $A/A \times A$?

Teorema 8.3.4 (teorema I de izomorfism) *Fie* $: (A, \Omega) \to (B, \Omega)$ *un omomorfism. Atunci:*
a) $\ker f = \{(x_1, x_2) \in A \times A \mid f(x_1) = f(x_2)\}$ *congruenţă pe algebra* (A, Ω).
b) $\operatorname{Im} f = f(A) \in \mathcal{S}(B, \Omega)$.
c) $A/\ker f \simeq \operatorname{Im} f$.

Demonstraţie. a) Fie $\omega \in \Omega$, $\tau(\omega) = n$ şi fie $x_1, \dots, x_n, x'_1, \dots, x'_n \in A$ astfel ca $x_i \ \ker f \ x'_i$, pentru $i = 1, \dots, n$; rezultă că $f(x_i) = f(x'_i)$, $i = 1, \dots, n$, deci

$$\omega(f(x_1), \dots, f(x_n)) = \omega(f(x'_1), \dots, f(x'_n)).$$

Deoarece f este omomorfism, $f(\omega(x_1, \dots, x_n)) = f(\omega(x'_1, \dots, x'_n))$, adică $\omega(x_1, \dots, x_n) \ \ker f \ \omega(x'_1, \dots, x'_n)$.

b) Fie $\omega \in \Omega$, $\tau(\omega) = n$ şi $y_1 = f(x_1), \dots, y_n = f(x_n) \in f(A)$. Atunci

$$\omega(y_1, \dots, y_n) = \omega(f(x_1), \dots, f(x_n)) = f(\omega(x_1, \dots, x_n)) \in f(A).$$

c) Din teorema I de factorizare 4.5.5 rezultă că

$$\bar{f} : A/\ker f \to \operatorname{Im} f, \quad \bar{f}(\rho\langle x\rangle) = f(x)$$

este funcţie bijectivă. Arătăm că $\bar{f}$ este omomorfism. Într-adevăr, pentru orice $\omega \in \Omega$ avem

$$\begin{aligned}\bar{f}(\omega(\rho\langle x_1\rangle, \dots, \rho\langle x_n\rangle)) &= \bar{f}(\rho\langle\omega(x_1, \dots, x_n)\rangle) = f(\omega(x_1, \dots, x_n)) = \\ &= \omega(f(x_1), \dots, f(x_n)) = \omega(\bar{f}(\rho\langle x_1\rangle), \dots, \bar{f}(\rho\langle x_n\rangle)).\end{aligned}$$ ■

Teorema 8.3.5 (teorema II de izomorfism) *Fie* (A, Ω) *o algebră universală,* $B \in \mathcal{S}(A, \Omega)$ *şi* $\rho \in \mathcal{C}(A, \Omega)$. *Atunci:*

a) $\rho(B) \in \mathcal{S}(A, \Omega)$;

b) $\sigma := \rho \cap (B \times B) \in \mathcal{C}(B, \Omega)$ *şi* $\tau := \rho \cap (\rho(B) \times \rho(B)) \in \mathcal{C}(\rho(B), \Omega)$;

c) $(B/\sigma, \Omega) \simeq (\rho(B)/\tau, \Omega)$.

Demonstraţie. a) Fie $\omega \in \Omega$, $\tau(\omega) = n$ şi $y_1, \dots, y_n \in \rho(B)$, deci există $b_1, \dots, b_n \in B$ astfel încât $n_i \rho y_i$, $i = 1, \dots, n$. Deoarece $\rho \in \mathcal{C}(A, \Omega))$, rezultă că $\omega(b_1, \dots, b_n)\rho\omega(y_1, \dots, y_n)$, şi deoarece $B \in \mathcal{S}(A, \Omega)$, rezultă că $\omega(b_1, \dots, b_n) \in B$, deci $\omega(y_1, \dots, y_n) \in \rho(B)$.

b) Fie $\omega \in \Omega$, $\tau(\omega) = n$ şi $b_1, \dots, b_n, b'_1, \dots, b'_n \in B$ astfel încât $b_i \sigma b'_i$, $i = 1, \dots, n$; rezultă că $b_i \rho b'_i$, $i = 1, \dots, n$, deci $\omega(b_1, \dots, b_n)\rho\omega(b'_1, \dots, b'_n)$. Deoarece $B \in \mathcal{S}(A, \Omega)$, rezultă că $\omega(b_1, \dots, b_n), \omega(b'_1, \dots, b'_n) \in B$, deci $\omega(b_1, \dots, b_n) \ \sigma \ \omega(b'_1, \dots, b'_n)$. La fel se arată că $\tau \in \mathcal{C}(\rho(B), \Omega)$.

c) Din Teorema II de factorizare 4.5.6 rezultă că $\bar{f} : B/\sigma \to \rho(B)/\tau$, $\bar{f}(\sigma\langle b\rangle) = \tau(\langle b\rangle)$ este funcţie bijectivă. Deoarece f este omomorfism, se vede uşor că $\bar{f}$ este de asemenea omomorfism. ■

Teorema 8.3.6 (teorema III de izomorfism) *Fie* (A, Ω) *o algebră universală şi fie* $\rho, \sigma \in \mathcal{C}(A, \Omega)$, $\rho \subseteq \sigma$. *Atunci există* $\sigma/\rho \in \mathcal{C}(A/\rho, \Omega)$ *astfel încât*

$$\frac{A/\rho}{\sigma/\rho} \simeq A/\sigma.$$

Demonstraţie. Din Teorema III de factorizare 4.5.7 rezultă că

$$g : A/\rho \to A/\sigma, \quad g(\rho\langle a\rangle) = \sigma\langle a\rangle$$

este funcţie surjectivă şi se verifică uşor că g este omomorfism. Din Teorema I de izomorfism 8.3.4 rezultă că $\sigma/\rho := \ker g$ este congruenţă pe algebra $(A/\rho, \Omega)$ şi are loc izomorfismul $\frac{A/\rho}{\sigma/\rho} \simeq A/\sigma$. ■

Exerciţiul 158 (laticea congruenţelor) Fie (A, Ω) o algebră universală şi $\rho \in \mathcal{E}(A)$ o relaţie de echivalenţă pe A.

a) Să se arate că ρ este congruenţă $\Leftrightarrow$ ρ este relaţie omomorfă.

b) Să se arate că mulţimea $(\mathcal{C}(A, \Omega), \subseteq)$ a congruenţelor pe A este latice completă.

c) Fie $\mathcal{C} \subseteq \mathcal{E}(A)$. Să se arate că

$$\sup_{\mathcal{E}(A)} \mathcal{C} = \bigcup_{n \in \mathbb{N}, \ \rho_1, \dots, \rho_n \in \mathcal{C}} \rho_1 \circ \cdots \circ \rho_n$$

(adică, dacă $q = \sup_{\mathcal{E}(A)} \mathcal{C}$, atunci $xqy \Leftrightarrow \exists x = x_0, x_1, \dots, x_n = y \in A$ şi $\exists \rho_1, \dots, \rho_n \in \mathcal{E}(A)$ astfel încât $x_0 \rho_1 x_1, \dots, x_{n-1} \rho_n x_n$.)

d) Dacă $\mathcal{C} \subseteq \mathcal{C}(A, \Omega)$, atunci $\sup_{\mathcal{E}(A)} \mathcal{C} = \sup_{\mathcal{C}(A,\Omega)} \mathcal{C}$.

e) Fie $\rho_1, \rho_2 \in \mathcal{C}(A, \Omega)$. Să se arate că

$$\rho_1 \circ \rho_2 \in \mathcal{C}(A, \Omega) \Longleftrightarrow \rho_1 \circ \rho_2 = \rho_2 \circ \rho_1$$

şi în acest caz $\sup_{\mathcal{C}(A,\Omega)}\{\rho_1, \rho_2\} = \rho_1 \circ \rho_2$.

f) Presupunem că pentru orice $\rho_1, \rho_2 \in \mathcal{C}(A, \Omega)$ avem $\rho_1 \circ \rho_2 = \rho_2 \circ \rho_1$. Să se arate că pentru orice $\rho_1, \rho_2, \rho_3 \in \mathcal{C}(A, \Omega)$ avem $\rho_1 \subseteq \rho_3 \Longrightarrow \rho_1 \circ (\rho_2 \cap \rho_3) = (\rho_1 \circ \rho_2) \cap \rho_3$. (În acest caz spunem că $\mathcal{C}(A, \Omega)$ este **latice modulară**.)

Capitolul 9

NUMERE CARDINALE

Rezultatele prezentate în următoarele două capitole au fost descoperite de matematicianul german Georg Cantor (1845 – 1918). El este creatorul teoriei mulţimilor şi a arătat importanţa funcţiilor bijective. Cantor a definit mulţimile infinite şi mulţimile bine ordonate, şi a arătat că există o ,,ierarhie" a mulţimilor infinite. Tot el a introdus numerele cardinale şi numerele ordinale şi a studiat aritmetica acestora.

9.1 Număr cardinal. Operaţii cu numere cardinale

Definiţia 9.1.1 Spunem că mulţimile A şi B sunt **echipotente** (notaţie: $A \sim B$), dacă există o funcţie bijectivă $f : A \to B$.

Observaţii 9.1.2 ,,$\sim$" este o relaţie de echivalenţă pe clasa mulţimilor, deci obţinem o partiţie a acestei clase.

Într-adevăr, dacă A o mulţime, atunci $1_A : A \to A$ este bijectiv, deci ,,$\sim$" este reflexiv. Dacă $A \sim B$ şi $B \sim C$ atunci există funcţiile bijective $f : A \to B$ şi $g : B \to C$. Deoarece $g \circ f : A \to C$ este bijectiv, rezultă că $A \sim C$ deci ,,$\sim$" este tranzitiv. Dacă $f : A \to B$ este bijectiv, atunci si $f^{-1} : B \to A$ este bijectiv, deci ,,$\sim$" este simetric.

Definiţia 9.1.3 a) **Cardinalul** mulţimii A este clasa de echipotenţă A. Notaţie: $|A|$, deci $A \sim B$ dacă şi numai dacă $|A| = |B|$, şi spunem că mulţimea A este **reprezentant** al numărului cardinal $\alpha = |A|$. (Deoarece construcţia axiomatică precisă a lui $|A|$ este dificilă, o vom face doar după introducerea şi a numerelor ordinale în capitolul următor.)

b) Adunarea, înmulţirea şi exponenţierea numerelor cardinale de definesc astfel:

1. $\sum_{i\in I} \alpha_i = |\coprod_{i\in I} A_i|$;
2. $\prod_{i\in I} \alpha_i = |\prod_{i\in I} A_i|$;
3. $\beta^\alpha = |B^A| = |\mathrm{Hom}(A, B)|$.

Observaţii 9.1.4 Definiţiile de mai sus nu depind de alegerea reprezentanţilor. Într-adevăr, dacă $\alpha_i = |A_i| = |A'_i|$, şi $f_i : A \to A'_i$ este bijectiv pentru orice $i \in I$, atunci $\coprod_{i\in I} f_i : \coprod A_i \to \coprod_{i\in I} A'_i$ şi $\prod_{i\in I} f_i : \prod_{i\in I} A_i \to \prod_{i\in I} A'_i$ sunt funcţii bijective. Dacă $f : A' \to A$ şi $g : B \to B'$ sunt bijective, atunci şi $\mathrm{Hom}(f, g) : \mathrm{Hom}(A, B) \to \mathrm{Hom}(A', B')$ este bijectiv.

Teorema 9.1.5 *Fie* $(A_i)_{i\in I}$ *o familie de mulţimi.*

a) $\phi : \coprod_{i\in I} A_i \to \bigcup_{i\in I} A_i$, $\phi(a_i, i) = a_i$ *este funcţie surjectivă, şi* ϕ *este injectivă dacă şi numai dacă* $A_i \cap A_j = \emptyset$ *pentru orice* $i, j \in I$, $i \neq j$.

b) $|A_1 \cup A_2| + |A_1 \cap A_2| = |A_1| + |A_2|$.

Demonstraţie. a) Dacă $a \in \bigcup_{i\in I} A_i$, atunci există $i \in I$ astfel încât $a \in A_i$ şi $\phi(a, i) = a$, deci ϕ este surjectivă.

Presupunem că ϕ este injectivă şi că există $i, j \in I$ şi $a \in A_i \cap A_j$. Deoarece $\phi(a, i) = \phi(a, j) = a$, rezultă că $(a, i) = (a, j)$, deci $i = j$.

Invers, presupunem că pentru orice $i \neq j$, $A_i \cap A_j = \emptyset$, şi fie $(a_i, i), (a_j, j) \in \coprod_{i\in I} A_i$ astfel încât $\phi(a_i, i) = \phi(a_j, j)$; rezultă că $a_i = a_j \in A_i \cap A_j$, deci $i = j$ şi $(a_i, i) = (a_j, j)$.

b) Dacă $A_1 \cap A_2 = \emptyset$, atunci din a) rezultă că $A_1 \cup A_2 \sim A_1 \coprod A_2$, deci $|A_1 \cup A_2| = |A_1| + |A_2|$.

În general, $A_1 \cup A_2 = A_1 \cup (A_2 \setminus A_1)$ şi $A_2 = (A_2 \setminus A_1) \cup (A_1 \cap A_2)$, unde $A_1 \cap (A_2 \setminus A_1) = \emptyset$ şi $(A_2 \setminus A_1) \cap A_1 \cap A_2) = \emptyset$; rezultă că

$$|A_1 \cup A_2| + |A_1 \cap A_2| = |A_1| + |A_1 \setminus A_2| + |A_1 \cap A_2| = |A_1| + |A_2|.$$

Teorema 9.1.6 *Au loc următoarele identităţi cu numere cardinale:*
a) $\alpha_1 + \alpha_2 = \alpha_2 + \alpha_1$; $\alpha_1\alpha_2 = \alpha_2\alpha_1$;
b) $(\alpha_1 + \alpha_2) + \alpha_3 = \alpha_1 + (\alpha_2 + \alpha_3)$; $(\alpha_1\alpha_2)\alpha_3 = \alpha_1(\alpha_2\alpha_3)$;
c) $(\sum_{i\in I}\alpha_i)(\sum_{j\in J}\beta_j) = \sum_{(i,j)\in I\times J}\alpha_i\beta_j$;
d) $\beta^{\sum_{i\in I}\alpha_i} = \prod_{i\in I}\beta^{\alpha_i}$;
e) $(\prod_{i\in I}\alpha_i)^\beta = \prod_{i\in I}\alpha_i^\beta$;
f) $\gamma^{\alpha\beta} = (\gamma^\beta)^\alpha$.

Demonstraţie. a) Fie $\alpha_1 = |A_1|$, $\alpha_2 = |A_2|$ şi să observăm că funcţiile

$$\phi : A_1 \coprod A_2 \to A_2 \coprod A_1,\quad \phi(a_1,1) = (a_1,2),\ \phi(a_2,2) = (a_2,1),$$
$$\psi : A_1 \times A_2 \to A_2 \times A_1,\quad \psi(a_1,a_2) = (a_2,a_1)$$

sunt bijective.
b) Observăm că mulţimile $(A_1 \coprod A_2) \coprod A_3 = \{((a_1,1),1'),((a_2,2),1'),(a_3,2') \mid a_i \in A_i\}$ şi $A_1 \coprod(A_2 \coprod A_3) = \{(a_1,1'),((a_2,1),2'),((a_3,2),2') \mid a_i \in A_i\}$ sunt echipotente.
c) Dacă $\alpha_i = |A_i|$ şi $\beta_j = |B_j|$, atunci

$$\phi : (\coprod_{i\in I} A_i) \times (\coprod_{j\in J} B_j) \to \coprod_{(i,j)\in I\times J}(A_i \times B_j),\qquad ((a_i,i),(b_j,j)) \mapsto ((a_i,b_i),(i,j))$$

este funcţie bijectivă.
d) Fie $\alpha_i = |A_i|$, $i \in I$ şi $\beta = |B|$. Atunci

$$\phi : \mathrm{Hom}(\coprod_{i\in I} A_i, B) \to \prod_{i\in I}\mathrm{Hom}(A_i,B),\qquad \phi(\alpha) = (\alpha\circ q_i)_{i\in I}$$

este funcţie bijectivă, unde $q_i : A_i \to \coprod_{i\in I} A_i$ este injecţia canonică a sumei directe.
e) Cu notaţiile de mai sus avem că funcţia

$$\psi : \mathrm{Hom}(B, \prod_{i\in I} A_i) \to \prod_{i\in I}\mathrm{Hom}(B,A_i),\qquad \psi(\alpha) = (p_i\circ\alpha)_{i\in I}$$

este bijectivă, unde $p_i : \prod_{i\in I} A_i \to A_i$ este proiecţia canonică a produsului direct.
f) Fie $\alpha = |A|$, $\beta = |B|$, $\gamma = |C|$ şi considerăm funcţiile

$$\phi : \mathrm{Hom}(A\times B, C) \to \mathrm{Hom}(A,\mathrm{Hom}(B,C)),\qquad \phi(f)(a)(b) = f(a,b),$$

$$\psi : \mathrm{Hom}(A,\mathrm{Hom}(B,C)) \to \mathrm{Hom}(A\times B, C),\qquad \psi(g)(a,b) = g(a)(b),$$

unde $a \in A$ şi $b \in B$. Se arată uşor că $\psi = \phi^{-1}$. ■

Teorema 9.1.7 (Cantor) *Pentru orice mulţime* A *are loc* $|\mathcal{P}(A)| = 2^{|A|}$.

Demonstraţie. Fie $\varphi_A : \mathcal{P}(A) \to \mathrm{Hom}(A,\{0,1\})$, $\varphi_A(X) = \chi_X$, unde

$$\chi_X : A \to \{0,1\},\qquad \chi_X(a) = \begin{cases} 1, & \text{dacă } a \in X \\ 0, & \text{dacă } a \notin X \end{cases}$$

este **funcţia caracteristică** a submulţimii X. Observăm că φ_A este bijectivă, pentru că

$$\varphi_A^{-1}(\chi) = \chi^{-1}(1),\qquad \forall\, \chi : A \to \{0,1\}$$

este inversa lui φ_A. ■

9.2 Ordonarea numerelor cardinale

Definiţia 9.2.1 Fie $\alpha = |A|$ şi $\beta = |B|$ două numere cardinale. Spunem că $\alpha \le \beta$ dacă există o funcţie injectivă $\phi : A \to B$.

Să arătăm că definiţia nu depinde de alegerea reprezentanţilor. Într-adevăr, dacă $\alpha = |A| = |A'|$, $f : A' \to A$ bijectiv, $\beta = |B| = |B'|$, $g : B \to B'$ bijectiv, atunci $\mathrm{Hom}(f,g)(\phi) = g\circ\phi\circ f : A' \to B'$ este funcţie injectivă.

Exerciţiul 159 Dacă $\alpha_i \leq \beta_i$, $\forall\ i \in I$, atunci:
a) $\sum_{i\in I} \alpha_i \leq \sum_{i\in I} \beta_i$;
b) $\prod_{i\in I} \alpha_i \leq \prod_{i\in I} \beta_i$;
c) dacă $0 \neq \alpha \leq \alpha'$ şi $\beta \leq \beta'$, atunci $\beta^\alpha \leq {\beta'}^{\alpha'}$.

Pentru a arăta că „$\leq$" este relaţie de ordine, avem nevoie de următoarea lemă.

Lema 9.2.2 (Cantor–Bernstein–Schröder) *Dacă $A_2 \subseteq A_1 \subseteq A_0$ şi $A_0 \sim A_2$, atunci $A_0 \sim A_1$.*

Demonstraţie. Fie $f : A_0 \to A_2$ o funcţie bijectivă şi definim familia de mulţimi $(A_n)_{n\geq 0}$ prin formula de recurenţă $A_{n+2} = f(A_n)$. Deoarece $A_2 \subseteq A_1 \subseteq A_0$, se arată prin inducţie că $A_n \supseteq A_{n+1}$ pentru orice $n \geq 0$.

Fie $B = \bigcap_{n\in\mathbb{N}} A_n$; atunci $A = B \cup \bigcup_{n\in\mathbb{N}}(A_n \setminus A_{n+1})$ şi $(A_i \setminus A_{i+1}) \cap (A_j \setminus A_{j+1}) = \emptyset$ dacă $i \neq j$. Deoarece $A_{n+2} = f(A_n)$, rezultă că funcţia

$$f_n : (A_n \setminus A_{n+1}) \to (A_{n+2} \setminus A_{n+3}), \qquad f_n(x) = f(x)$$

este bijectivă pentru orice $n \geq 0$. Funcţia bijectivă căutată $g : A_0 \to A_1$ se defineşte astfel:

$$g(x) = \begin{cases} x, & \text{dacă } x \in B, \\ f(x), & \text{dacă } x \in A_{2n} \setminus A_{2n+1},\ n \in \mathbb{N}, \\ x, & \text{dacă } x \in A_{2n-1} \setminus A_{2n},\ n \in \mathbb{N}. \end{cases} \quad \blacksquare$$

Teorema 9.2.3 *Relaţia „$\leq$" este relaţie de ordine totală. (În particular, are loc trihotomia: dacă α şi β sunt numere cardinale, atunci sau $\alpha < \beta$ sau $\alpha = \beta$ sau $\alpha > \beta$.)*

Demonstraţie. Dacă $\alpha = |A|$, atunci $\alpha \leq \alpha$, pentru că $1_A : A \to A$ este functie injectivă.

Dacă $\alpha = |A|$, $\beta = |B|$, $\gamma = |C|$ şi $\alpha \leq \beta$, $\beta \leq \gamma$, atunci există funcţiile injective $f : A \to B$ şi $g : B \to C$; deoarece şi $g \circ f : A \to C$ este injectivă, rezultă că $\alpha \leq \gamma$.

Fie acum $\alpha = |A|$, $\beta = |B|$ astfel încât $\alpha \leq \beta$ şi $\beta \leq \alpha$, deci există funcţiile injective $f : A \to B$ şi $g : B \to A$. Fie $A_0 = A$, $A_1 = g(B)$, $B_1 = f(A)$ şi $A_2 = g(B_1)$. Deoarece $B_1 \subseteq B$, rezultă că $A_2 \subseteq A_1 \subseteq A_0$. Mai departe, $g\circ f$ este funcţie injectivă şi $(g\circ f)(A_0) = g(f(A)) = g(B_1) = A_2$, deci $A_0 \sim A_2$. Din Lema Cantor–Bernstein–Schröder rezultă că $A_0 \sim A_1$, deci $A \sim B$ pentru că $A_1 \sim B$.

Fie $\alpha = |A|$, $\beta = |B|$ şi pentru orice $X \subseteq A$, $Y \subseteq B$, fie

$$\mathcal{B}(X, Y) = \{f : X \to Y \mid f \text{ bijectiv}\},$$
$$\mathcal{B} = \bigcup_{(X,Y)\in\mathcal{P}(A)\times\mathcal{P}(B)} \mathcal{B}(X, Y).$$

Pe mulţimea $\mathcal{B}$-n definim relaţia „$\leq$" astfel: dacă $f : X \to Y$ şi $f' : X' \to Y'$, atunci $f \leq f'$ dacă şi numai dacă $X \subseteq X'$ şi f este restricţia lui f' la X. Se verifică uşor că $(\mathcal{B}, \leq)$ este o mulţime nevidă ordonată.

Fie $\mathcal{L} = \{f_i : X_i \to Y_i \mid i \in I\} \subseteq \mathcal{B}$ o submulţime total ordonată, şi arătăm că $\mathcal{L}$ are majorantă în $\mathcal{B}$. Întradevăr, fie $X = \bigcup_{i\in I} X_i$, $Y = \bigcup_{i\in I} Y_i$ şi fie $f : X \to Y$, $f(x) = f_i(x)$ dacă $x \in X_i$. Este uşor de arătat că f este funcţie bine definită, bijectivă, şi $f_i \leq f$ pentru orice $i \in I$.

Din lema lui Zorn rezultă că în $\mathcal{B}$ există un element maximal $f_0 : X_0 \to Y_0$, deci este suficient de demonstrat că $X_0 = A$ sau $Y_0 = B$. Presupunem că $X_0 \neq A$, $Y_0 \neq B$ şi fie $a_0 \in A \setminus X_0$ şi $b_0 \in B \setminus Y_0$. Observăm că funcţia

$$f' : X_0 \cup \{a_0\} \to Y_0 \cup \{b_0\}, \quad f'(x) = \begin{cases} f_0(x), & \text{dacă } x \in X_0, \\ b_0, & \text{dacă } x = a_0 \end{cases}$$

este bijectivă si $f_0 \leq f'$, ceea ce contrazice maximalitatea lui f_0. $\blacksquare$

Teorema 9.2.4 (Cantor) *Pentru orice număr cardinal α avem $\alpha < 2^\alpha$.*

Demonstraţie. Fie $\alpha = |A|$. Deoarece $A \to \mathcal{P}(A)$, $a \mapsto \{a\}$ este funcţie injectivă, rezultă că $\alpha \leq 2^\alpha$. Presupunem că $\phi : A \to \mathcal{P}(A)$ este bijectiv, şi fie

$$X = \{a \in A \mid a \notin \phi(a)\}.$$

Atunci există $x \in A$ astfel încât $\phi(x) = X$. Dacă $x \in X$, atunci $x \in \phi(x)$, deci $x \notin X$; dacă $x \notin X$, atunci $x \notin \phi(x)$, deci $x \in X$. În ambele cazuri ajungem la o contradicţie, deci $\alpha < 2^\alpha$. $\blacksquare$

9.3 Mulţimi finite, infinite şi numărabile

Definiţia 9.3.1 a) Spunem că A este mulţime **finită**, dacă este echipotentă cu un număr natural, adică $\exists n \in \mathbb{N}$ astfel ca $A \sim n$. Mulţimea A este **infinită**, dacă nu este finită.

b) Spunem că A este mulţime **infinită numărabilă**, dacă este echipotentă cu mulţimea numerelor naturale, adică $A \sim \mathbb{N}$. Notăm cu $\aleph_0$ cardinalul lui $\mathbb{N}$.

c) Spunem că A este mulţime **numărabilă** (sau **cel mult numărabilă**), dacă este finită sau infinit numărabilă.

d) Notăm cu $\mathfrak{c}$ cardinalul mulţimii $\mathbb{R}$ a numerelor reale, şi spunem că $\mathbb{R}$ are **puterea continuului**.

Teorema 9.3.2 a) *Orice submulţime a unei mulţimi finite este finită.*

b) *Dacă $n, m \in \mathbb{N}$ şi există $f : n \to m$ funcţie injectivă, atunci $n \subseteq m$. În particular, dacă $n \sim m$, atunci $n = m$, adică orice mulţime finită este echipotentă cu un singur număr natural.*

Demonstraţie. a) Este suficient de arătat că pentru orice număr natural n, orice submulţime a lui n este finită. Deoarece mulţimea

$$S := \{n \in \mathbb{N} \mid \text{ orice submulţime a lui } n \text{ este finită}\}$$

satisface $\emptyset \in S$ şi $n \in S \Rightarrow n^+ \in S$, din principiul inducţiei matematice obţinem $S = \mathbb{N}$.

b) Considerăm mulţimea

$$T = \{n \in \mathbb{N} \mid \text{ pentru orice } m \in \mathbb{N}, \text{ dacă există } f : n \to m \text{ injectivă, atunci } n \subseteq m\}.$$

Este evident că $\emptyset \in T$. Fie $n \in T$, şi presupunem că $f : n^+ \to m$ este o funcţie injectivă, unde $m \in \mathbb{N}$. Deoarece $n^+ \neq \emptyset$, rezultă că $m \neq \emptyset$, şi conform axiomelor lui Peano există $p \in \mathbb{N}$ astfel încât $m = p^+$, deci avem $f : n^+ = n \cup \{n\} \to m = p^+ = p \cup \{p\}$. Dacă $p \notin f(n)$, atunci $g : n \to p$, $g(x) = f(x)$ este funcţie bine definită şi injectivă. Dacă $p \in f(n)$, atunci fie $p = f(u)$, $f(n) = v$, unde $u \in n$ şi $v \in p$ (într-adevăr, deoarece dacă $v \notin p$, atunci $f(n) = p = f(u)$, deci $n = u \in n$, contradicţie). Atunci funcţia

$$g : n \to p, \quad g(x) = \begin{cases} f(x), & \text{dacă } x \neq u, \\ v, & \text{dacă } x = u \end{cases}$$

este injectivă. Deci în ambele cazuri avem o funcţie injectivă $g : n \to p$. Deoarece $n \in T$, rezultă că $n \subseteq p$. Dacă $n \subset p$, atunci $n \in p$, deci $n^+ \subseteq p^+ = m$. Dacă $n = p$, atunci avem $n^+ = p^+ = m$. Deci în orice caz $n^+ \in m$, adică $n^+ \in T$. Din principiul inducţiei rezultă $T = \mathbb{N}$. ∎

Observaţii 9.3.3 a) În capitolul următor vom da definiţia axiomatică a numărului cardinal. Vom vedea că dacă A este mulţime finită, adică există unic $n \in \mathbb{N}$ astfel ca $A \sim n$, atunci $|A| = |n| = n$. Deci orice număr natural este şi număr cardinal (este chiar propriul cardinal).

b) Adunarea numerelor naturale definită în capitolul anterior coincide cu adunarea lor ca numere cardinale. Într-adevăr, dacă notăm pentru moment cu $\bar{+}$ adunarea numerelor cardinale, atunci avem $n^+ = |n^+| = |n \cup \{n\}| = |n| \bar{+} |\{n\}| = n \bar{+} 1$.

Teorema 9.3.4 *Fie A o mulţime. Următoarele afirmaţii sunt echivalente:*

(1) *A este mulţime infinită;*

(2) *Există o funcţie injectivă $f : \mathbb{N} \to A$;*

(3) *A are o submulţime proprie echipotentă cu A.*

Demonstraţie. (1)⇒(2) Observăm că dacă A infinit şi $a \in A$, atunci şi $A \setminus \{a\}$ este infinit (pentru că dacă $A \setminus \{a\} \sim n$, atunci $A \sim n^+ = n + 1$). Demonstraţia ,,naivă” decurge astfel. Prin inducţie definim un şir $(A_n)_{n \in \mathbb{N}}$, unde $a_n \in A$ şi o familie de mulţimi $(A_n)_{n \in \mathbb{N}}$, unde $A_n \subseteq A$. Deoarece A este infinit, este evident nevid (căci altfel am avea $A \sim 0$), deci există $a_0 \in A$. Fie $A_0 = A \setminus \{a_0\}$, care este de asemenea infinit. Presupunem că a_n şi A_n sunt definite. Atunci A_n este infinit, deci există $a_{n+1} \in A_n$, şi dacă $A_{n+1} = A_n \setminus \{a_{n+1}\}$, atunci şi A_{n+1} este infinit. Fie $f : \mathbb{N} \to A$, $f(n) = a_n$, deci f este funcţie injectivă.

Mai exact, trebuie să folosim axioma alegerii. Fie $\mathbb{N}_n = \{0, 1, \dots, n-1\}$. Prin inducţie (ca mai sus) se arată că pentru orice $n \in \mathbb{N}$, există o funcţie injectivă $\phi : \mathbb{N}_n \to A$. Dacă $n \in \mathbb{N}$, fie

$$M_n = \{\phi : \mathbb{N}_n \to A \mid \phi \text{ injectivă}\},$$

deci $M_n \neq \emptyset$, şi avem $M_n \cap M_m = \emptyset$, dacă $m \neq n$. Din axioma alegerii rezultă că există o mulţime M astfel încât pentru orice $n \in \mathbb{N}$, $M_n \cap M$ are exact un element. Vedem că dacă definim mulţimea $B := \bigcup_{\phi \in M} \operatorname{Im} \phi$, atunci există o funcţie bijectivă $f : \mathbb{N} \to B$.

(2)⇒(1) Presupunem că A este finită. Deoarece $f : \mathbb{N} \to A$ este injectiv, rezultă că $\mathbb{N} \sim f(\mathbb{N}) \subseteq A$. Dar atunci $\mathbb{N}$ este finită, adică există $n \in \mathbb{N}$ şi o funcţie bijectivă $g : \mathbb{N} \to n$. Fie $h = g|_{n^+} : n^+ \to n$ restricţia funcţiei g la $n^+ \subseteq \mathbb{N}$. Evident h este injectiv, deci $n^+ = n \cup \{n\} \subseteq n$, contradicţie.

(3)⇒(2) Fie $B \subset A$ şi fie $f : A \to B$ o funcţie bijectivă. Mai departe, fie $a_0 \in A \setminus B$, şi prin inducţie definim şirul $(a_n)_{n\in\mathbb{N}}$, $a_{n+1} = f(a_n)$. Fie $\phi : \mathbb{N} \to A$, $\phi(n) = a_n$, şi prin inducţie după n arătăm că din $n \neq m$ rezultă $\phi(n) \neq \phi(m)$. Într-adevăr, dacă $n = 1$, atunci $m \neq 1$, de unde $\phi(1) = a_1$ şi $\phi(m) = f(a_{m-1}) \in B$; deoarece $a_1 \notin B$, rezultă că $\phi(1) \neq \phi(m)$. Presupunem că afirmaţia este adevărată pentru n, şi fie $m \neq n+1$. Dacă $m = 1$, atunci $\phi(m) = a_1 \notin B$ şi $\phi(n+1) = f(a_n) \in B$, deci $\phi(n+1) \neq \phi(m)$. Dacă $m \neq 1$, atunci $\phi(m) = f(a_{m-1})$ şi $\phi(n+1) = f(a_n)$. Deoarece $m - 1 \neq n$, rezultă că $a_{m-1} \neq a_n$, şi deoarece f este injectivă, rezultă că $f(a_{m-1}) \neq f(a_n)$, deci $\phi(m) \neq \phi(n+1)$.

(2)⇒(3) Considerăm funcţia

$$\phi : A \to A \setminus \{f(0)\}, \qquad \phi(a) = \begin{cases} a, & \text{dacă } x \notin f(\mathbb{N}), \\ f(n+1), & \text{dacă } x = f(n) \end{cases},$$

şi aratăm că ϕ este bijectivă. Într-adevăr, fie $a, b \in A$ astfel încât $\phi(a) = \phi(b)$. Atunci sau $a, b \in f(\mathbb{N})$, sau $a, b \in A \setminus f(\mathbb{N})$. Dacă $a, b \notin f(\mathbb{N})$, atunci este evident că $a = b$. Dacă $a, b \in f(\mathbb{N})$, atunci $\phi(a) = f(k+1)$ şi $\phi(b) = f(l+1)$, unde $a = f(k)$ şi $b = f(l)$. Deoarece f este injectivă, rezultă că $k+1 = l+1$, de unde $k = l$ şi $a = b$. Deci ϕ este injectivă. Fie acum $b \in A \setminus \{f(0)\}$. Dacă $b = f(n) \in f(\mathbb{N})$, atunci $n \neq 0$ şi $b = f(n-1+1) = \phi(f(n-1))$; dacă $b \notin f(\mathbb{N})$, atunci $b = f(b)$, deci ϕ este surjectivă. ■

Corolar 9.3.5 a) *Mulţimea $\mathbb{N}$ a numerelor naturale este infinită, mai mult, $|\mathbb{N}| =: \aleph_0$ este cel mai mic număr cardinal infinit (sau* **transfinit***).*

b) *Fie A o mulţime. Următoarele afirmaţii sunt echivalente:*

(1) *A este finită;*

(2) *Dacă $f : \mathbb{N} \to A$, atunci f nu este injectiv;*

(3) *Dacă $B \subseteq A$ şi $|B| = |A|$, atunci $B = A$.*

c) *Reuniunea a două mulţimi finite este finită.*

Demonstraţie. c) Fie A şi B două mulţimi finite. Deoarece $|A \coprod B| = |A| + |B|$ şi suma a două numere naturale este număr natural, rezultă că $A \coprod B$ este finită. Deoarece există o funcţie injectivă $f : A \cup B \to A \coprod B$, rezultă că $A \cup B$ este finită. ■

Exerciţiul 160 Fie A o mulţime. Să se arate că următoarele afirmaţii sunt echivalente:

(i) A este mulţime finită;

(ii) Dacă $f : A \to A$ este injectiv, atunci f este surjectiv;

(iii) Dacă $f : A \to A$ este surjectiv, atunci f este injectiv.

Exerciţiul 161 Fie A o mulţime infinită. Să se arate că :

a) $|A| + n = |A|$, $\forall\, n \in \mathbb{N}$;

b) $|A| + \aleph_0 = |A|$.

Exerciţiul 162 Să se demonstreze :

a) $\aleph_0 + \aleph_0 = \aleph_0$; $\aleph_0 \cdot \aleph_0 = \aleph_0$;

b) Dacă $A_n \sim \mathbb{N}$ pentru orice $n \in \mathbb{N}$, atunci $\bigcup_{n\in\,\mathbb{N}} A_n \sim \mathbb{N}$ (adică, o reuniune numărabilă de mulţimi numărabile este numărabilă);

c) Mulţimea $\mathcal{P}_f(\mathbb{N}) = \{X \subset \mathbb{N} \mid X \text{ este finită}\}$ a părţilor finite ale lui $\mathbb{N}$ este numărabilă;

d) Mulţimea numerelor raţionale este numărabilă;

e) Mulţimea $\mathbb{Q}[X]$ a polinoamelor cu coeficienţi raţionali este numărabilă;

f) Mulţimea $\mathbb{A} := \{z \in \mathbb{C} \mid (\exists)P \in \mathbb{Q}[X] \setminus \{0\},\ P(z) = 0\}$ a **numerelor algebrice** este numărabilă.

Teorema 9.3.6 a) *Mulţimea $\mathbb{R}$ a numerelor reale este nenumărabilă, adică $\mathfrak{c} > \aleph_0$;*

b) $\mathfrak{c} = 2^{\aleph_0}$.

Demonstraţie. a) Folosim **metoda diagonală a lui Cantor**. Fie o funcţie

$$f : \mathbb{N}^* \to [0,1), \qquad f(n) = 0, a_{n1}a_{n2}\dots a_{nn}\dots,$$

unde $a_{ni} \in \{0, \dots, 9\}$. Fie $a_n \in \{0, \dots, 9\}$ astfel încât $a_n \notin \{0, 9, a_{nn}\}$, şi $a = 0, a_1, a_2, \dots a_n \dots$. Atunci evident $f(n) \neq a$ pentru orice $n \in \mathbb{N}$, deci funcţia f nu este surjectivă. Astfel am arătat că nu există o funcţie bijectivă $f : \mathbb{N}^* \to \mathbb{R}$.

b) Ştim că are loc egalitatea

$$2^{\aleph_0} = |\mathrm{Hom}(\mathbb{N}^*, \{0,1\})|,$$

de aceea vom folosi reprezentarea numerelor reale ca fracţii binare infinite. Fie $a \in [0,1)$, $a = 0, a_1 a_2 \ldots$ (în baza de numeraţie 2), unde $a_n \in \{0,1\}$. Presupunem că 1 nu este perioadă a fracţiei. Fie funcţia

$$\phi : [0,1) \to \mathrm{Hom}(\mathbb{N}^*, \{0,1\}), \qquad \phi(a) = f, \text{ unde } f(n) = a_n \ \ \forall\, n \geq 1.$$

Atunci funţia ϕ este injectivă, pentru că exprimarea numărului real a ca fracţii binare infinită fără perioada 1 este unică. În plus, avem că

$$\complement(\mathrm{Im}\,\phi) = \{f : \mathbb{N}^* \to \{0,1\} \mid \exists\, n_0 \text{ astfel încât } \ f(n) = 1 \ \ \forall\, n > n_0\}.$$

Dar un număr real de forma $0, b_1 b_2 \ldots b_{n_0} 111\ldots$ este raţional, deci $\complement(\mathrm{Im}\,\phi)$ (adică mulţimea numerelor ce pot fi reprezentate cu perioada 1) este o mulţime numărabilă. Deoarece avem

$$\mathrm{Hom}(\mathbb{N}^*, \{0,1\}) = \mathrm{Im}\,\phi \cup \complement(\mathrm{Im}\,\phi),$$

rezultă că $2^{\aleph_0} = \mathfrak{c} + \aleph_0$, deci $\mathfrak{c} = 2^{\aleph_0}$. ■

Exerciţiul 163 Să se demonstreze :

a) Orice interval de numere reale are puterea continuului, adică $\mathbb{R} \sim (0,1) \sim (a,b) \sim [a,b) \sim [a,b] \sim (a,b]$ pentru orice $a, b \in \mathbb{R}$ astfel ca $a < b$;

b) Mulţimea $\mathbb{R} \setminus \mathbb{Q}$ a numerelor iraţionale are puterea continuului (adică $\mathbb{R} \sim \mathbb{R} \setminus \mathbb{Q}$).

Exerciţiul 164 Să se demonstreze :

a) $\mathfrak{c}^2 = \mathfrak{c}^{\aleph_0} = \mathfrak{c}$;

b) $\mathfrak{c} + \mathfrak{c} = \mathfrak{c} \cdot \aleph_0 = {\aleph_0}^{\aleph_0} = \mathfrak{c}$.

Teorema 9.3.7 *Dacă α este un număr cardinal infinit, atunci $\alpha^2 = \alpha = \alpha\alpha'$ pentru orice α', unde $0 \neq \alpha' \leq \alpha$.*

Demonstraţie. Fie $\alpha = |A|$ şi arătăm că există o funcţie bijectivă $f : A \to A \times A$. Pentru aceasta vom folosi Lema lui Zorn. Fie

$$\mathcal{R} = \{(M, f) \mid M \subseteq A, \ M \text{ este infinit şi } f : M \to M \times M \text{ este bijectiv}\}.$$

Deoarece A este infinit, există $M \subseteq A$ astfel încât $M \sim \mathbb{N}$. Atunci $M \sim M \times M$, deci $\mathcal{R} \neq \emptyset$. Pe mulţimea $\mathcal{R}$ definim relaţia de ordine

$$(M, f) \leq (M', f') \iff M \subseteq M' \text{ és } f'|_M = f.$$

Arătăm că în $\mathcal{R}$ orice lanţ are majorantă. Într-adevăr, fie $\mathcal{L} \subseteq \mathcal{R}$ un lanţ, şi fie perechea (M_0, f_0), unde $M_0 = \bigcup_{(M,f)\in\mathcal{L}} M$ şi $f_0 : M_0 \to M_0 \times M_0$, $f_0(x) = f(x)$, dacă $(M, f) \in \mathcal{L}$ şi $x \in M$. Atunci f_0 este bine definită, pentru că $\mathcal{L}$ este lanţ, şi f_0 este injectivă, pentru că dacă $(M, f) \in \mathcal{L}$, atunci f injectivă. Din egalitatea $M_0 \times M_0 = \bigcup_{(M,f)\in\mathcal{L}} (M \times M)$ rezultă că f_0 este surjectivă, deci $(M_0, f_0) \in \mathcal{R}$. Evident că (M_0, f_0) este majorantă pentru $\mathcal{L}$.

Conform lemei lui Zorn, există un element maximal $(B, f) \in \mathcal{R}$, şi fie $\beta = |B|$, deci $\beta^2 = \beta$. Dacă $\beta = \alpha$, atunci $\alpha^2 = \alpha$, deci putem presupune că $\beta < \alpha$. Deoarece $\beta \leq \beta + \beta = 2\beta \leq \beta^2$, rezultă că $2\beta = \beta$, şi prin inducţie, $n\beta = \beta$ pentru orice $n \in \mathbb{N}$.

Dacă $|A \setminus B| \leq \beta$, atunci deoarece $A = (A \setminus B) \cup B$, rezultă că $\alpha = |A \setminus B| + \beta \leq \beta + \beta = \beta$, contradicţie. Rezultă că $\beta < |A \setminus B|$, şi există o mulţime $C \subseteq A \setminus B$ astfel încât $|C| = \beta$, deci $B \sim C$. Atunci

$$(B \cup C) \times (B \cup C) = (B \times B) \cup (B \times C) \cup (C \times B) \cup (C \times C),$$

şi avem

$$|(B \times C) \cup (C \times B) \cup (C \times C)| = \beta^2 + \beta^2 + \beta^2 = 3\beta = \beta.$$

Rezultă că există o funcţie bijectivă $g : (B \times C) \cup (C \times B) \cup (C \times C) \to C$. Considerăm funcţia

$$h : B \cup C \to (B \cup C) \times (B \cup C), \quad h(x) = \begin{cases} f(x), & \text{dacă } x \in B, \\ g(x), & \text{dacă } x \in C \end{cases}.$$

Atunci h este bijectivă, deci $(B \cup C, h) \in \mathcal{R}$, contradicţie, pentru că $(B, f) < (B \cup C, h)$. Rezultă că ipoteza $\beta < \alpha$ este falsă, deci $\beta = \alpha$ şi $\alpha^2 = \alpha$. ■

9.4 Elemente de combinatorică

Discutăm câteva aspecte privind calculul numărului de elemente al unor mulţimi finite.

9.4.1 Aranjamente, permutări, combinări

Definiţia 9.4.1 Fie A şi B două mulţimi finite, $|A| = k$ şi $|B| = n$. Fixăm câte o ordonare totală a acestor mulţimi astfel: $A = \{a_1 < a_2 < \cdots < a_k\}$ şi $B = \{b_1 < b_2 < \cdots < b_n\}$.

a) Un şir de lungime k de elemente din B se numeşte k-**aranjament cu repetiţie** de n elemente. Numărul k-aranjamentelor cu repetiţie de n elemente se notează $\bar{A}_n^k$.

b) Un şir de lungime k de elemente din B, în care fiecare element apare cel mult o dată, se numeşte k-**aranjament** de n elemente. Numărul k-aranjamentelor de n elemente se notează A_n^k.

c) Un şir de lungime n de elemente din B, în care fiecare element apare exact o dată, se numeşte **permutare** de n elemente. Numărul permutărilor de n elemente se notează P_n.

d) O submulţime cu k elemente a lui B (unde $k \le n$) se numeşte k-**combinare** de n elemente. Numărul k-combinărilor de n elemente se notează $\binom{n}{k}$ sau C_n^k.

e) Un şir crescător de lungime k de elemente din B se numeşte k-**combinare cu repetiţie** de n elemente. (Un astfel de şir se mai numeşte *multiset* cu k elemente, adică elementele se pot repeta, dar nu contează ordinea lor.) Numărul k-combinărilor cu repetiţie de n elemente se notează $\left(\binom{n}{k}\right)$ sau $\bar{C}_n^k$.

Observaţii 9.4.2 Deoarece şirurile sunt de fapt funcţii, definiţiile de mai sus se pot reformula astfel:

a) Numărul k-aranjamentelor cu repetiţie de n elemente este egal cu numărul funcţiilor $f : A \to B$.

b) Numărul k-aranjamentelor de n elemente este egal cu numărul funcţiilor injective $f : A \to B$.

c) Numărul permutărilor de n elemente este egal cu numărul funcţiilor bijective $f : A \to B$.

d) Numărul k-combinărilor de n elemente este egal cu numărul funcţiilor strict crescătoare $f : A \to B$, sau altfel spus, cu numărul şirurilor strict crescătoare de lungime k de elemente din B.

e) Numărul k-combinărilor cu repetiţie de n elemente este egal cu numărul funcţiilor crescătoare $f : A \to B$.

Exerciţiul 165 Pentru $n = 5$ şi $k = 2$ să se enumere toate

a) k-aranjamentele cu repetiţie de n elemente.

b) k-aranjamentele de n elemente.

c) permutările de n elemente.

d) k-combinările de n elemente.

e) k-combinările cu repetiţie de n elemente.

Exerciţiul 166 Să se demonstreze :

a) $\bar{A}_n^k = n^k$.

b) Dacă $k \le n$, atunci $A_n^k = \frac{n!}{(n-k)!}$.

c) $P_n = n!$.

d) Dacă $k \le n$, atunci $C_n^k = \binom{n}{k} = \frac{n!}{k!(n-k)!}$.

e) $\bar{C}_n^k = \left(\binom{n}{k}\right) = \frac{(n+k-1)!}{(n-1)!k!}$.

Exerciţiul 167 Să se demonstreze :

a) $C_n^k = C_n^{n-k}$; $C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$.

b) $(X + Y)^n = \sum_{k=0}^n C_n^k X^{n-k} Y^k$ (*formula binomului*).

c) $\sum_{k=0}^n C_n^k = 2^n$ (în două moduri!).

Exerciţiul 168 a) În câte moduri poate fi scris n ca sumă de k numere naturale nenule, dacă ţinem cont de ordinea termenilor?

b) În câte moduri poate fi scris n ca sumă de k numere naturale, dacă ţinem cont de ordinea termenilor?

Exerciţiul 169 Fie $|A| = k$, $|B| = n$ şi fie $f : A \to B$.

a) Dacă f este injectiv, câte inverse la stânga are f?

b) Dacă f este surjectiv, câte inverse la dreapta are f?

9.4.2 Principiul includerii şi al excluderii

Propoziţia 9.4.3 (Principiul includerii şi al excluderii) *Dacă $A_1, \dots, A_n$ sunt mulţimi finite, atunci cardinalul reuniunii lor este dat de formula*

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{1\le i_1<i_2\le n} |A_{i_1} \cap A_{i_2}| + \sum_{1\le i_1<i_2<i_3\le n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| -$$
$$- \cdots + (-1)^{k+1} \sum_{1\le i_1<\cdots<i_k\le n} |A_{i_1} \cap \cdots \cap A_{i_k}| + \cdots + (-1)^{n+1} |\bigcap_{i=1}^{n} A_i|.$$

Demonstraţie. 1. Dacă $A \cap B = \varnothing$, atunci $|A \cup B| = |A| + |B|$. În general, $|A_1 \cup A_2| = |A_1| + |A_2 \setminus A_1|$ şi $|A_2| = |A_2 \setminus A_1| + |A_1 \cap A_2 |$, deci

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Continuăm prin inducţie. Presupunem că afirmaţia este adevărată pentru n mulţimi, şi fie $A_1, \dots, A_n, A_{n+1}$ mulţimi finite. Atunci

$$|\bigcup_{i=1}^{n+1} A_i| = |\bigcup_{i=1}^{n} A_i \cup A_{n+1}| = |\bigcup_{i=1}^{n} A_i| + |A_{n+1}| - |\bigcup_{i=1}^{n} A_i \cap A_{n+1}| =$$
$$= \sum_{i=1}^{n+1} |A_i| - \sum_{1\le i_1<i_2\le n} |A_{i_1} \cap A_{i_2}| + \cdots + (-1)^{n+1} |\bigcap_{i=1}^{n} A_i| + \bigcup_{i=1}^{n} (A_i \cap A_{n+1})| =$$
$$= \sum_{i=1}^{n+1} |A_i| - \sum_{1\le i_1<i_2\le n+1} |A_{i_1} \cap A_{i_2}| + \cdots + (-1)^{n+2} | \bigcap_{i=1}^{n+1} A_i|,$$

deci formula are loc pe baza principiului inducţiei matematice. ■

Demonstraţie. 2. A doua demonstraţie se bazează pe proprietăţile funcţiei caracteristice, date în Exerciţiul 66. Presupunem că $A_1, \dots, A_n \subseteq A$. Observăm în plus că pentru o submulţime finită $X \subseteq A$, avem

$$|X| = \sum_{x\in A} \chi_X(x).$$

Avem $A_1 \cup \cdots \cup A_n = \complement(\complement A_1 \cap \cdots \cap \complement A_n)$ (De Morgan), deci

$$\chi_{A_1\cup\cdots\cup A_n} = 1 - (1 - \chi_{A_1}) \dots (1 - \chi_{A_n}) =$$
$$= \sum_{i=1}^{n} \chi_{A_i} - \sum_{i_1<i_2} \chi_{A_{i_1}} \chi_{A_{i_2}} + \cdots + (-1)^{k+1} \sum_{i_1<\cdots<i_k} \chi_{A_{i_1}} \dots \chi_{A_{i_k}} + \cdots + (-1)^{n+1} \prod_{i=1}^{n} \chi_{A_i} =$$
$$= \sum_{i=1}^{n} \chi_{A_i} - \sum_{i_1<i_2} \chi_{A_{i_1}\cap A_{i_2}} + \cdots + (-1)^{k+1} \sum_{i_1<\cdots<i_k} \chi_{A_{i_1}\cap\cdots\cap A_{i_k}} + \cdots + (-1)^{n+1} \chi_{\bigcap_{i=1}^{n} A_i}.$$

Însumând după valorile în $x \in A$ ale funcţiilor din ambii membri, obţinem formula din enunţ. ■

Exerciţiul 170 *Aplicaţii ale principiului includerii şi al excluderii.*

a) Fie $m = p_1^{k_1} \dots p_n^{k_n} \in \mathbb{N}$. Să se calculeze **numărul lui Euler** $\phi(m)$, unde prin definiţie,

$$\phi(m) := |\{a \in \mathbb{N} \mid 1 \le a \le m,\ (a, m) = 1\}|.$$

b) Fie $\sigma \in S_n$ o permutare de grad n. Spunem că elementul $i \in \{1, \dots, n\}$ este **punct fix** al lui σ, dacă $\sigma(i) = i$. Câte permutări de grad n nu au puncte fixe? (Astfel de permutări se mai numesc *deranjamente*.)

Exerciţiul 171 Fie A şi B două mulţimi finite, $|A| = k$ şi $|B| = n$. Dacă $k \ge n$, atunci **numărul funcţiilor surjective** $f : A \to B$ este notat $s(k, n)$ şi să se arate că are loc egalitatea

$$s(k, n) = n^k - C_n^1 (n - 1)^k + C_n^2 (n - 2)^k + \cdots + (-1)^{n-1} C_n^{n-1} 1^k.$$

9.4.3 Partiţii. Numerele lui Stirling şi Bell. Permutări cu repetiţie

Am întâlnit relaţiile de echivalenţă şi partiţiile în Secţiunea 4.4.2. Determinăm numărul lor în cazul mulţimilor finite.

Definiţia 9.4.4 Notăm cu $\mathcal{E}(A)$ mulţimea tuturor relaţiilor de echivalenţă pe A. Dacă $1 \le n \le k$, unde $|A| = k$ atunci notăm cu $\mathcal{E}_n(A) = \{\rho \in \mathcal{E}(A) \mid |A/\rho| = n\}$ mulţimea relaţiilor de echivalenţă pe A pentru care mulţimea factor (adică partiţia corespunzătoare) are n clase.

a) Numărul $|\mathcal{E}_n(A)|$ se numeşte **numărul Stirling de speţa a II-a** şi se notează $\{{k \atop n}\}$ sau $S(k,n)$.

b) Numărul $|\mathcal{E}(A)|$ al relaţiilor de echivalenţă pe A se numeşte **numărul lui Bell**, notat B_k.

Exerciţiul 172 Să se enumere toate partiţiile mulţimii $A = \{a_1, a_2, a_3, a_4, a_5\}$.

Exerciţiul 173 Folosind legătura dintre funcţii surjective şi relaţii de echivalenţă, să se arate că:

a) $S(k,n) = \{{k \atop n}\} = \frac{s(k,n)}{n!}$.

b) Numărul partiţiilor mulţimii A coincide cu numărul lui Bell B_k şi mai mult, avem $B_k = \sum_{n=1}^{k} S(k,n)$.

Definiţia 9.4.5 Fie $A = \{a_1, \dots, a_k\}$ şi $B = \{b_1, \dots, b_n\}$ două mulţimi ca mai sus, şi fie $f : A \to B$ o funcţie. Fie $(k_1, \dots, k_n) \in \mathbb{N}^n$ astfel încât $\sum_{i=1}^{n} k_i = k$.

a) Dacă $|f^{-1}(b_i)| = k_i$, pentru $1 \le i \le n$, atunci spunem că $(f^{-1}(b_1), \dots, f^{-1}(b_n))$ este o **partiţie ordonată de tip** $(k_1, \dots, k_n)$ a mulţimii A. (Să observăm că este permis aici ca unele din clasele partiţiei să fie vide.)

b) O **permutare cu repetiţie de tip** $(k_1, \dots, k_n)$ a celor n elemente ale mulţimii B este un şir de lungime k de elemente din B astfel încât elementul b_i apare exact de k_i ori, pentru $1 \le i \le n$. Numărul permutărilor cu repetiţie de tip $(k_1, \dots, k_n)$ se notează cu $P_k^{k_1,\dots,k_n}$ sau $\binom{k}{k_1 \dots k_n}$.

Exerciţiul 174 a) Să se enumere toate partiţiile ordonate de tip $(2,1,2)$ ale mulţimii $A = \{a_1, a_2, a_3, a_4, a_5\}$.

b) Să se enumere toate 5-permutările cu repetiţie de tip $(2,1,2)$ ale elementelor mulţimii $B = \{b_1, b_2, b_3\}$.

Exerciţiul 175 a) Să se demonstreze că numărul partiţiilor ordonate de tip $(k_1, \dots, k_n)$ ale mulţimii A coincide cu numărul $P_k^{k_1,\dots,k_n}$ al permutărilor cu repetiţie de tip $(k_1, \dots, k_n)$ ale elementelor lui B; mai mult, are loc egalitatea

$$\binom{k}{k_1 \dots k_n} = \frac{k!}{k_1! \dots k_n!}.$$

b) Să se interpreteze aranjamentele, permutările şi combinările în termeni de permutări cu repetiţie.

Exerciţiul 176 Să se demonstreze *formula polinomului*:

$$(X_1 + \dots + X_n)^k = \sum_{\substack{(k_1,\dots,k_n) \in \mathbb{N}^n \\ (k_1+\dots+k_n=k}} \binom{k}{k_1 \dots k_n} X_1^{k_1} \dots X_n^{k_n}.$$

Capitolul 10

NUMERE ORDINALE

Numerele ordinale, introduse de Georg Cantor în 1883, reprezintă clase de izomorfism de mulţimi bine ordonate şi sunt o generalizare a numerelor naturale. Ele pot fi privite ca nişte etichete sau indici pe care le folosim când vrem să punem în ordine (enumerăm) elementele unei mulţimi nu neapărat finite.

10.1 Noţiunea de număr ordinal

Definiţia 10.1.1 a) Spunem că mulţimile ordonate $(A, \leq)$ şi $(B, \leq)$ sunt **asemenea** (notaţie: $A \simeq B$), dacă există o funcţie crescătoare, bijectivă $f : A \to B$ astfel ca f^{-1} este crescătoare. (Asemănarea se mai numeşte **izomorfism de ordine**.)

b) O mulţime α se numeşte **număr ordinal** dacă satisface următoarele proprietăţi:

1. $u, v \in \alpha \Rightarrow u \in v$ sau $v \in u$ sau $u = v$;
2. $u \in \alpha \Rightarrow u \subseteq \alpha$

c) Dacă α este un număr ordinal, atunci definim pe α relaţia "$\preceq$" astfel:

$u \preceq v$ dacă $u \in v$ sau $u = v$

Exerciţiul 177 Să se arate că:
1) Asemănarea este relaţie de echivalenţă pe clasa mulţimilor ordonate.
2) Dacă $(A, \leq)$ este bine ordonată şi $(B, \leq)$ este asemenea cu A, atunci şi B este bine ordonată.
3) Dacă α este un număr ordinal, atunci relaţia "$\preceq$" este o relaţie de bună ordonare pe α.

Definiţia 10.1.2 a) Fie $(A, \leq)$ o mulţime bine ordonată. Se poate arăta că există unic număr ordinal α astfel ca $(A, \leq)$ este asemenea cu $(\alpha, \preceq)$. În acest caz α se numeşte **numărul ordinal al mulţimii bine ordonate** $(A, \leq)$ şi notăm $\alpha = \overline{(A, \leq)}$. (De multe ori vom nota doar prin $\bar{A}$ numărul ordinal al mulţimii bine ordonate $(A, \leq)$.)

b) Din 7.1.3 e) şi 7.1.10 1),2) rezultă că numerele naturale, respectiv mulţimea (bine ordonată) $\mathbb{N}$ a numerelor naturale sunt numere ordinale. În acest context vom nota

$$\bar{\mathbb{N}} = \mathbb{N} =: \omega$$

c) Număr ordinal al unei mulţimi bine ordonate infinite se numeşte număr ordinal **transfinit**. În particular, $\mathbb{N} = \omega$ este număr ordinal transfinit.

Exerciţiul 178 Să se arate că:
1) Dacă A, B sunt mulţimi bine ordonate, atunci $A \simeq B$ dacă şu numai dacă $\bar{A} = \bar{B}$.
2) Dacă α este un număr ordinal şi $a \in \alpha$, atunci şi a este număr ordinal.

Definiţia 10.1.3 (ordonarea numerelor ordinale) Fie $\alpha = \bar{A}$ şi $\beta = \bar{B}$ numere ordinale.

a) Spunem că α este mai mic decât β (notaţie: $\alpha < \beta$), dacă există $b \in B$, astfel încât $A \simeq B_b$, unde submulţimea

$$B_b := \{y \in B \mid y < b\}$$

se numeşte **segment iniţial** al lui B.

b) Spunem că $\alpha \leq \beta$ dacă $\alpha < \beta$ sau $\alpha = \beta$.

Teorema 10.1.4 *Definiţiile relaţiilor „$<$" şi „$\leq$" nu depind de alegerea reprezentanţilor şi sunt adevărate următoarele afirmaţii:*
1) *Dacă* α, β *sunt numere ordinale, atunci* $\alpha \leq \beta \Leftrightarrow \alpha \preceq \beta \Leftrightarrow \alpha \subseteq \beta$;
2) *Dacă* β *este un număr ordinal, atunci* $\beta = \{\alpha \mid \alpha < \beta\}$*;*
3) $\alpha \not< \alpha$ *pentru orice număr ordinal* α*;*
4) *Dacă* $\alpha < \beta$*, atunci* $\beta \not< \alpha$*;*
5) *Relaţia „$<$" este tranzitivă;*
6) *„$\leq$" este relaţie de ordine;*
7) *Dacă* M *este o mulţime ale cărei elemente sunt numere ordinale, atunci* $(M, \leq)$ *este bine ordonată;*
8) *Dacă* α *şi* β *sunt numere ordinale, atunci din următoarele trei afirmaţii exact una este adevărată:*
(a) $\alpha = \beta$*;* (b) $\alpha < \beta$*;* (c) $\beta < \alpha$.

Demonstraţie. Fie $\alpha = \bar{A}$, $\beta = \bar{B}$ şi presupunem că $A \simeq B_b$. Dacă A' şi B' sunt mulţimi bine ordonate astfe ca $A \simeq A'$ şi $B \simeq B'$, atunci există o asemănare $g : B \to B'$. Fie $b' = g(b)$; atunci $B_b \simeq B'_{b'}$, deci $A' \simeq B'_{b'}$, deci definiţia lui „$<$" nu depinde de alegerea reprezentanţiloe.

3), 4) Este suficient de arătat că dacă A este bine ordonată şi $a \in A$, atunci $A \not\simeq A_a$.

Într-adevăr, presupunem că $f : A \to A_a$ este o asemănare. Atunci $f(a) < a$, deci mulţimea

$$C := \{x \in A \mid f(x) < x\}$$

este nevidă. Fie $a_0 = \min C$; rezultă că $f(a_0) < a_0$, şi $f(f(a_0)) < f(a_0)$, deci $f(a_0) \in C$. Dar $f(a_0) < a_0$, deci avem o contradicţie.

5) (*Tranzitivitea*) Fie $\alpha = \bar{A}$, $\beta = \bar{B}$ şi $\gamma = \bar{C}$. Deoarece $\alpha < \beta$ şi $\beta < \gamma$, există $b \in B$ şi $c \in C$ astfel încât $A \simeq B_b$ şi $B \simeq C_c$. Mai departe, fie $g : B \to C_c$ o asemănare, şi fie $c' = g(b)$. Atunci $B_b \simeq C_{c'}$, deci $A \simeq C_{c'}$ şi $\alpha < \gamma$. ■

Exerciţiul 179 Să se arate că:
a) Dacă A este o mulţime bine ordonată şi $a, a' \in A$, $a \neq a'$, atunci $A_a \not\simeq A_{a'}$;
b) Dacă A şi B sunt mulţimi bine ordonate şi $f, g : A \to B$ sunt două asemănări, atunci $f = g$.

Exerciţiul 180 Să se completeze demonstraţia Teoremei 10.1.4.

Definiţia 10.1.5 Din definiţia numărului ordinal rezultă că dacă α este un număr ordinal, atunci **succesorul**

$$\alpha^+ := \alpha \cup \{\alpha\}$$

al lui α este de asemenea număr ordinal.

a) Un număr ordinal β se numeşte **de speţa I**, dacă există un număr ordinal α astfel încât $\beta = \alpha^+$.

b) Un număr ordinal β se numeşte **de speţa II** sau **ordinal limită**, dacă nu este de speţa I şi scriem

$$\beta = \lim_{\alpha < \beta} \alpha.$$

Observaţii 10.1.6 Vedem că număr ordinal β eset de speţa I dacă $\beta = \overline{A}$, unde A este o mulţime bine ordonată care are cel mai mare element (adică există $\max A$). În particular, ω este de speţa II.

Din Corolarul 5.3.4 obţinem următoarea teoremă.

Teorema 10.1.7 (Principiul inducţiei transfinite) *Fie* P *un predicat de o variabilă definit pe numerele ordinale. Presupunem că dacă pentru orice* $\alpha < \beta$ *propoziţia* $P(\alpha)$ *este adevărată, atunci şi* $P(\beta)$ *este adevărată. Atunci* $P(\alpha)$ *este propoziţie adevărată pentru orice număr ordinal* α.

Pentru a generaliza Teorema 7.1.4, cu scopul de a da definiţii prin recurenţă transfinită, avem nevoie de câteva noţiuni.

Definiţia 10.1.8 Fie A bine ordonată şi fie X o mulţime oarecare.

a) Fie $a \in A$. Un **şir de tip** a **din** X este o funcţie $h : A_a = \{x \in A \mid x < a\} \to X$.

De exemplu, un şir de tip ω este chiar un şir obişnuit $h : \mathbb{N} \to X$ de elemente din X. Evident, dacă $g : A \to X$ este o funţie oarecare, atunci restricţia $g|_{A_a} : A_a \to X$ funcţiei g la A_a este un şir de tip a din X.

b) Un **şir de tip** A **din** X este o funcţie

$$f : \{g \mid g \text{ este şir de tip } a \text{ din } X,\ a \in A\} \to X.$$

Teorema 10.1.9 (teorema recurenţei transfinite) *Dacă* A *bine ordonată şi* f *este un şir de tip* A *din* X*, atunci există o unică funcţie* $g : A \to X$ *astfel încât* $g(a) = f(g|_{A_a})$ *pentru orice* $a \in A$.

10.2 Operaţii cu numere ordinale

Definiţia 10.2.1 (adunarea numerelor ordinale) *a) Fie A_1 şi A_2 două mulţimi bine ordonate. Pe reuniunea disjunctă*

$$A_1 \coprod A_2 = (A_1 \times \{1\}) \cup (A_1 \times \{2\})$$

definim următoarea relaţie:

- $(a_1, 1) \leq (a_1', 1)$ *dacă* $a_1 \leq a_1'$*;*
- $(a_2, 2) \leq (a_2', 2)$ *dacă* $a_2 \leq a_2'$*;*
- $(a_1, 1) \leq (a_2, 2)$ *pentru orice* $a_1 \in A_1$, $a_2 \in A_2$.

Atunci $(A_1 \coprod A_2, \leq)$ *mulţime bine ordonată şi se numeşte* **reuniunea disjunctă ordonată** *a lui* A_1 *şi* A_2 .

b) Dacă $\alpha_1 = \bar{A}_1$ *şi* $\alpha_2 = \bar{A}_2$ *sunt numere ordinale, atunci prin definiţie,*

$$\alpha_1 + \alpha_2 = \overline{A_1 \coprod A_2}.$$

În general, fie $(\alpha_i)_{i\in I}$ *o familie de numere ordinale, unde* I *eset o mulţime bine ordonată şi* $\alpha_i = \overline{A}_i$. **Suma** *familiei* $(\alpha_i)_{i\in I}$ *este numărul ordinal* $\sum_{i\in I} \alpha_i = \overline{\coprod_{i\in I}^{\circ} A_i}$.

Se arată uşor că $\sum_{i\in I} \alpha_i$ *nu depinde de alegerea reprezentanţilor* A_i*, unde* $\overline{A}_i = \alpha_i$.

Teorema 10.2.2 *Adunarea numerelor ordinale are următoarele proprietăţi:*

a) (asociativitatea) $(\alpha_1 + \alpha_2) + \alpha_3 = \alpha_1 + (\alpha_2 + \alpha_3)$*;*

b) *Dacă* $\alpha_1 \leq \beta_1$ *şi* $\alpha_2 \leq \beta_2$*, atunci* $\alpha_1 + \alpha_2 \leq \beta_1 + \beta_2$*. În general, dacă* $\alpha_i \leqslant \beta_i$*, pentru orice* $i \in I$*, atunci*

$$\sum_{i\in I} \alpha_i \leq \sum_{i\in I} \beta_i;$$

c) $\alpha \leq \beta$ *dacă şi numai dacă există un număr ordinal* $\gamma \neq 0$ *astfel încât* $\beta = \alpha + \gamma$*;*

d) *Dacă* $\alpha < \beta$*, atunci pentru orice număr ordinal* γ *avem*

1. $\gamma + \alpha < \gamma + \beta$*;*
2. $\alpha + \gamma \leq \beta + \gamma$*;*

e) *Dacă* α *este un număr ordinal, atunci* $\alpha^+ = \alpha + 1$*. În particular, adunarea numerelor naturale ca numere ordinale coincide cu adunarea definită recursiv.*

Demonstraţie. b) Fie $\alpha_i = \bar{A}_i$ şi $\beta_i = \bar{B}_i$, $i = 1, 2$. Deoarece $\alpha_i \leq \beta_i$, există funcţiile injective crescătoare $f_i : A_i \to B_i$ astfel încât $f(A_i)$ este egal cu B_i sau cu un segment al lui B_i. Atunci funcţia

$$f_1 \coprod f_2 : A_1 \coprod A_2 \to B_1 \coprod B_2$$

este injectivă crescătoare şi $\mathrm{Im}\,(f_1 \coprod f_2)$ este egal cu $B_1 \coprod B_2$ sau cu un segment al lui $B_1 \coprod B_2$; rezultă că $\alpha_2 + \alpha_2 \leq \beta_1 + \beta_2$.

c) Fie $\alpha = \bar{A}$ şi $\beta = \bar{B}$. Deoarece $\alpha < \beta$, există $b \in B$ astfel încât $A \simeq B_b$. Fie $\gamma = \overline{B \setminus B_b}$; deoarece $B_b \cap B \setminus B_b = \emptyset$ şi fiecare element al lui B_b este mai mic decât fiecare element al lui $B \setminus B_b$, rezultă că $B \simeq B_b \coprod (B \setminus B_b)$, deci $\beta = \alpha + \gamma$.

Invers, fie $\beta = \alpha + \gamma$, unde $\alpha = \bar{A}$, $\beta = \bar{B}$ şi $\gamma = \bar{C}$. Putem presupune că $A \cap C = \emptyset$ şi $B = A \cup C$, deci fiecare element al lui A este mai mic decât fiecare element al lui C. Dacă $c_o := \min C$, atunci $A = B_{c_o}$, deci $\alpha < \beta$.

d) (1) Din c) rezultă că $\beta = \alpha + \delta$, unde $\delta \neq 0$; atunci $\gamma + \beta = \gamma + (\alpha + \delta) = (\gamma + \alpha) + \delta$, deci $\gamma + \alpha < \gamma + \beta$.
(2) este caz particular al lui b).

e) Fie $\alpha = \overline{A}$ şi a_0 un element astfel încât $a_0 \notin A$. Ca reprezentant al lui $\alpha + 1$ putem alege mulţimea bine ordonată $C := A \cup \{a_0\}$ ordonată astfel: dacă x, $y \in C$, atunci $x \leqslant y$ dacă $x \leqslant y$ şi $x, y \in A$, şi $x \leq a_0$ pentru orice $x \in C$.

Atunci $A = C_{a_0}$ şi deci $\alpha < \alpha + 1$. Dacă $\alpha < \beta$, unde $\beta = \overline{B}$, atunci $A \simeq B_b$ $(b \in B)$.

Dacă $b := \max B$, atunci $C \simeq B$; în caz contrar există un succesor b' al lui b. În acest caz $C \simeq B_{b'}$. În consecinţă $\alpha + 1 \leqslant \beta$, deci $\alpha + 1$ este succesor al lui α. ■

Exercițiul 181 Să se arate că:
a) dacă $(A_1, \leq)$ şi $(A_2, \leq)$ sunt mulţimi bine ordonate, atunci şi $(A_1 \coprod A_2, \leq)$ este mulţime bine ordonată;
b) definiţia sumei $\alpha_2 + \alpha_2$ nu depinde de alegerea reprezentanţilor;
c) adunareaa numerelor ordinale este asociativă;
d) dacă $n \neq 0$ este un număr natural, atunci $n + \omega = \omega$ şi $\omega < \omega + n$ (în particular, adunarea numerelor ordinale nu e comutativă);
e) dacă A_1, A_2, B_1, B_2 sunt mulţimi bine ordonate şi $f_1 : A_1 \to B_1$ şi $f_2 : A_2 \to B_2$ sunt funcţii crescătoare, atunci şi funcţia $f_1 \coprod f_2 : A_1 \coprod A_2 \to B_1 \coprod B_2$ este crescătoare.

Exercițiul 182 Fie $\alpha, \beta, \gamma, \delta$ numere ordinale. Să se arate că:
(1) dacă $\gamma + \alpha < \gamma + \beta$ sau $\alpha + \gamma < \beta + \gamma$, atunci $\alpha < \beta$;
(2) dacă $\gamma + \alpha = \gamma + \beta$, atunci $\alpha = \beta$;
(3) dacă $\gamma + \alpha = \delta + \beta$ şi $\alpha < \beta$, atunci $\gamma > \delta$.

Definiția 10.2.3 (înmulţirea numerelor ordinale) a) Fie A şi B două mulţimi bine ordonate. Pe produsul cartezian

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}$$

definim relaţia:

$$(a, b) \leq (a', b') \iff (a < a' \text{ sau } (a = a' \text{ şi } b \leq b')).$$

Atunci $(A \times B, \leq)$ este mulţime bine ordonată, şi relaţia „$\leq$" se numeşte **ordonarea lexicografică**. Notaţie: $A \overset{\circ}{\times} B$.
b) Dacă $\alpha = \bar{A}$ şi $\beta = \bar{B}$ sunt numere ordinale, atunci prin definiţie

$$\alpha\beta = \overline{B \overset{\circ}{\times} A}.$$

Observații 10.2.4 Verificăm că $(A \times B, \leq)$ este mulţime bine ordonată.
Reflexivitatea şi antisimetria sunt evidente. Mai departe, fie (a, b), (a', b'), $(a'', b'') \in A \times B$ astfel încât $(a, b) \leq (a', b')$ şi $(a', b') \leq (a'', b'')$.
Cazul I. $a < a'$ şi $a' < a''$. Atunci $a < a''$, deci $(a, b) \leq (a'', b'')$.
Cazul II. $a < a'$ şi $a' = a''$. Atunci $a < a''$, deci $(a, b) \leq (a'', b'')$.
La fel tratăm *Cazul II'.* $a = a'$ şi $a' < a''$.
Cazul III. $a = a'$ şi $a' = a''$. Atunci $b \leq b'$ şi $b' \leq b''$, deci $b \leq b''$ şi $(a, b) \leq (a'', b'')$.
Fie $M \subseteq A \times B$, $M \neq \emptyset$, şi fie $p_A : A \times B \to A$, $p_B : A \times B \to B$ proiecţiile canonice. Atunci $p_A(M) \neq \emptyset$, şi fie $a_0 = \min p_A(M)$. Mai departe, fie $B' = \{b \in B \mid (a_0, b) \in M\}$; deoarece $B' \neq \emptyset$, există $b_0 = \min B'$. Atunci e evident că $(a_0, b_0) = \min M$.

Exercițiul 183 **4.** Să se arate că dacă $f : A \to A'$ şi $g : B \to B'$ sunt asemănări, atunci şi funţia

$$f \times g : A \times B \to A' \times B', \quad (a, b) \mapsto (f(a), g(b))$$

este asemănare. (În particular, definiţia produsului $\alpha\beta$ nu depinde de alegerea reprezentanţilor.)

Teorema 10.2.5 *Înmulţirea numerelor ordinale are următoarele proprietăţi:*
a) (asociativitate) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$*;*
b) (distributivitate la stânga) $\alpha(\beta_1 + \beta_2) = \alpha\beta_1 + \alpha\beta_2$. *În general, dacă* $(\beta_i)_{i\in I}$ *este o familie de numere ordinale, atunci* $\alpha(\sum_{i\in I} \beta_i) = \sum_{i\in I} \alpha\beta_i$*;*
c) *Dacă* $\alpha < \beta$*, şi* $\gamma \neq 0$*, atunci* $\gamma\alpha < \gamma\beta$*;*
d) *Dacă* $\alpha \leq \beta$*, atunci* $\alpha\gamma \leq \beta\gamma$.

Demonstrație. a) Considerăm funcţia bijectivă

$$\phi : (A \times B) \times C \to A \times (B \times C), \quad ((a, b), c) \mapsto (a, (b, c)).$$

Este suficient de arătat că

$$((a, b), c) \leq ((a', b'), c') \iff (a, (b, c)) \leq (a', (b', c')).$$

Într-adevăr,

$$((a, b), c) \leq ((a', b'), c') \iff (a < a') \vee (a = a',\ b < b') \vee (a = a',\ b = b',\ c \leq c') \iff$$
$$\iff (a, (b, c)) \leq (a', (b', c')).$$

b) Fie

$$\psi : (A_1 \coprod A_2) \times B \to (A_1 \times B) \coprod (A_2 \times B), \quad ((a, i), b) \mapsto ((a, b), i),$$

unde $a \in A_i$, $i \in \{1, 2\}$, şi $b \in B$. Evidentcă ψ este bijectiv, şi este suficient de arătat că

$$((a, i), b) \le ((a', i'), b') \iff ((a, b), i) \le ((a', b'), i').$$

Într-adevăr,

$$\begin{aligned} ((a, i), b) \le ((a', i'), b') &\iff ((a, i) < (a', i)) \vee ((a, i) = (a', i'),\ b \le b') \iff \\ &\iff (a < a', i = i') \vee (i < i') \vee \\ &\vee (a = a',\ b \le b',\ i = i') \iff \\ &\iff ((a, b) \le (a', b'),\ i = i') \vee (i < i') \iff \\ &\iff ((a, b), i)) \le ((a', b'), i'). \end{aligned}$$

c) Fie $\beta = \alpha + \delta$, unde $\delta \neq 0$. Atunci $\gamma\beta = \gamma(\alpha + \delta) = \gamma\alpha + \gamma\delta$, şi deoarece $\gamma\delta \neq 0$, rezultă că $\gamma\alpha < \gamma\beta$.
d) Rezultă din definiţii. ■

Observaţii 10.2.6 a) Înmulţirea numerelor ordinale nu e comutativă. De exemplu, să aratăm că $2 \cdot \omega \neq \omega \cdot 2$.
Avem $2 \cdot \omega = \overline{\mathbb{N} \times \{1, 2\}}$, unde

$$\mathbb{N} \times \{1, 2\} = \{(0, 1) < (0, 2) < (1, 1) < (1, 2) < \cdots < (n, 1) < (n, 2) < \cdots\}.$$

Se verifică uşor că funţia

$$f : \mathbb{N} \to \mathbb{N} \times \{1, 2\}, \quad f(n) = \begin{cases} (\frac{n+1}{2}, 1), & \text{dacă } n \text{ este impar}, \\ (\frac{n}{2}, 2), & \text{dacă } n \text{ este par} \end{cases}$$

este asemănare, deci $2 \cdot \omega = \omega$.
Pe de altă parte, $\omega \cdot 2 = \omega \cdot (1 + 1) = \omega + \omega > \omega$, deci $2 \cdot \omega \neq \omega \cdot 2$.
b) Distributivitatea la dreapta nu are loc în general, deoarece de exemplu,

$$\begin{aligned} (\omega + 1)2 &= (\omega + 1)(1 + 1) = \\ &= (\omega + 1) + (\omega + 1) = \\ &= \omega + (1 + \omega) + 1 = \\ &= \omega + \omega + 1 = \omega \cdot 2 + 1 = \\ &\neq \omega \cdot 2 + 2. \end{aligned}$$

Exerciţiul 184 Fie $\alpha, \beta, \gamma, \delta$ numere ordinale. Să se arate că :
a) dacă $\gamma\alpha < \gamma\beta$, atunci $\alpha < \beta$;
b) dacă $\gamma\alpha = \gamma\beta$, atunci $\alpha = \beta$;
c) dacă $\gamma\alpha = \delta\beta \neq 0$ şi $\alpha < \beta$, atunci $\gamma > \delta$.

Definiţia 10.2.7 (Exponenţierea numerelor ordinale) Fie α şi β două numere ordinale şi definim numărul ordinal α^β. Prin recursie transfinită definim funcţia f pe mulţimea $\{\lambda \mid \lambda < \beta + 1\}$ astfel:

1. $f(0) = 1$;
2. Presupunem că $f(\rho)$ este definită pentru orice $\rho < \lambda$, $(\lambda < \beta + 1)$, şi fie

$$f(\lambda) = \begin{cases} f(\lambda - 1) \cdot \alpha, & \text{dacă } \lambda \text{ este de speţa I}, \\ \lim\limits_{\rho < \lambda} f(\rho), & \text{dacă } \lambda \text{ este de speţa II}. \end{cases}$$

Prin definiţie, $\alpha^\beta = f(\beta)$.

De exemplu, dacă $\beta = \omega$, atunci $\alpha^\omega = \lim\limits_{n<\omega} \alpha^n$.

Teorema 10.2.8 *Dacă* α, β, γ *sunt numer ordinale, atunci*
1) $\alpha^\beta \cdot \alpha^\gamma = \alpha^{\beta+\gamma}$;
2) $(\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}$.

Demonstraţie. Arătăm 1) şi 2) prin inducţie transfinită după γ. Dacă $\gamma = 0$, atunci 1) şi 2) au loc. Presupunem că 1) şi 2) au loc pentru orice număr ordinalr $\rho < \gamma$. Avem două cazuri:

a) γ este de speţa I. Atunci din definiţie avem

$$\begin{aligned}\alpha^{\beta} \cdot \alpha^{\gamma} &= \alpha(\alpha^{\gamma-1} \cdot \alpha) = (\alpha^{\beta} \cdot \alpha^{\gamma-1}) \cdot \alpha = \alpha^{\beta+\gamma-1} \cdot \alpha = \alpha^{\beta+\gamma},\\ (\alpha^{\beta})^{\gamma} &= (\alpha^{\beta})^{\gamma-1} \cdot \alpha^{\beta} = \alpha^{\beta(\gamma-1)\cdot\alpha^{\beta}} = \alpha^{\beta\gamma-\beta} \cdot \alpha^{\beta} = \alpha^{\beta\gamma}.\end{aligned}$$

b) γ este de speţa II. Atunci

$$\begin{aligned}\alpha^{\beta} \cdot \alpha^{\gamma} &= \alpha^{\beta} \lim_{\mu<\gamma} \alpha^{\mu} = \lim_{\mu<\gamma} (\alpha^{\beta} \cdot \alpha^{\mu}) =\\ &= \lim_{\mu<\gamma} a(\alpha^{\beta+\mu}) = \lim_{\mu<\beta+\gamma} (\alpha^{\mu}) = \alpha^{\beta+\gamma},\\ (\alpha^{\beta})^{\gamma} &= \lim_{\mu<\gamma} (\alpha^{\beta})^{\mu} = \lim_{\mu<\gamma} (\alpha^{\beta\cdot\mu}) = \lim_{\nu<\beta\cdot\gamma} (\alpha^{\nu}) = \alpha^{\beta\cdot\gamma}.\end{aligned}$$

Deci 1) şi 2) unt adevărate. ■

Observaţii 10.2.9 În general, $(\alpha\cdot\beta)^{\gamma} \neq \alpha^{\gamma}\cdot\beta^{\gamma}$. Într-adevăr, fie $\beta = \gamma = 3$ şi $\alpha = \omega$. În acest caz $\alpha^{\gamma}\cdot\beta^{\gamma} = \omega^3\cdot 27$, şi

$$\begin{aligned}(\alpha \cdot \beta)^{\gamma} &= (\omega \cdot 3)^3 = (\omega \cdot 3)(\omega \cdot 3)(\omega \cdot 3) = \omega(3 \cdot \omega)(3 \cdot \omega) \cdot 3 =\\ &= \omega \cdot \omega \cdot \omega \cdot 3 = \omega^3 \cdot 3 \neq \omega^3 \cdot 27.\end{aligned}$$

10.3 Definiţia axiomatică a numărului cardinal

Fie A o mulţime. Conform teoremei lui Zermelo 5.4.2. 7), A se poate bine ordona (nu în mod unic), deci mulţimea

$$N(A) = \{\alpha \mid \alpha \text{ număr ordinal şi } \alpha \sim A\}$$

este nevidă. Atunci din 10.1.4 rezultă că $N(A)$ are cel mai mic element relativ la ordonarea numerelor ordinale.

Definiţia 10.3.1 (von Neumann) Cel mai mic număr ordinal din $N(A)$ se numeşte **cardinalul** mulţimii A. Notaţie: $|A|$.

Observaţii 10.3.2 1) Definiţia clasică numărului cardinal dată de Cantor şi pe care am utilizat-o în capitolul anterior nu funţionează în sistemele axomatice uzuale ale teoriei mulţimilor, cum ar fi Zermelo–Fraenkel sau von Neumann–Bernays–Gödel. Vedem că definiţia de mai sus presupune că acceptăm axioma alegerii.

2) Tot din 10.1.4 rezultă că $|A| = \cap N(A)$.

3) Este evident că $|A| = |B|$ dacă şi numai dacă $A \sim B$. Într-adevăr, dacă $|A| = |B|$, atunci $A \sim |A| = |B| \sim B$, deci $A \sim B$. Invers, dacă presupunem că $A \sim B$, atunci $|A| \sim B$, deci $|A| \in N(B)$, de unde $|A| \leq |B|$ (relativ la la ordonarea numerelor ordinale). Analog se arată că $|A| \geq |B|$.

4) Dacă A este o mulţime finită, atunci am văzut că există unic $n \in \mathbb{N}$ astfel ca $A \sim n$. De aici şi din definiţia de mai sus deducem că $|A| = n$. Afirmaţia reciprocă este de asemenea adevărată: dacă $|A| = n$, atunci evident $A \sim n$, deci A este finită.

10.4 Alefuri şi problema continuului

Definiţia 10.4.1 a) Cardinalul unei mulţimi bine ordonate se numeşte **alef**. Dacă $\alpha = \overline{A}$ este un număr ordinal (unde A este bine ordonată), atunci notăm $|\alpha| = |A|$. Evident, număr cardinal $|\alpha|$ nu depinde de alegerea reprezentantului A al numărului ordinal α.

b) Dacă mulţimea este infinită, atunci aleful se numeşte **transfinit**.

Din Teorema lui Zermelo 5.4.2. 7) rezultă imediat:

Teorema 10.4.2 *Orice număr cardinal este un alef.*

Teorema 10.4.3 *Fie α şi β două numere ordinale.*

1) *Dacă $|\alpha| < |\beta|$, atunci $\alpha < \beta$;*

2) *Dacă $\alpha < \beta$, atunci $|\alpha| \leqslant |\beta|$.*

Demonstraţie. 1) Fie $\alpha = \overline{A}$ şi $\beta = \overline{B}$. Dacă $A \simeq B$, atunci $A \sim B$, deci $|\alpha| = |\beta|$, contradicţie.

Dacă $B \simeq A_a$, unde $a \in A$, atunci $|B| \leqslant |A|$, adică $|\beta| \leqslant |\alpha|$, contradicţie. Deci $A \simeq B_b$, unde $b \in B$, deci $\alpha < \beta$. ■

Teorema 10.4.4 1) *Dacă* $(\alpha_i)_{i\in I}$ *este o familie de numere ordinale, atunci* $|\sum_{i\in I} \alpha_i| = \sum_{i\in I} |\alpha_i|$.

2) *Dacă* α, β *sunt două numere ordinale, atunci* $|\alpha \cdot \beta| = |\alpha| \cdot |\beta|$.

Observaţii 10.4.5 Dacă $(\alpha_i)_{i\in I}$ este o familie de numere ordinale, unde mulţimea de indici I este bine ordonată, atunci în general $|\prod_{i\in I} \alpha_i| \neq \prod_{i\in I} |\alpha_i|$.

De exemplu, fie $I = N$ şi $\alpha_i = 2$, pentru orice $i \in I$. Deoarece $\prod_{i\in I} \alpha_i = \omega$, rezultă că $\prod_{i\in I} \alpha_i = \aleph_0$. Pe de altă parte, $\prod_{i\in I} |\alpha|_i = 2^{\aleph_0} = \mathfrak{c} > \aleph_0$.

Folosind recursia transfinită, stabilim un sistem de notaţii pentru alefii transfiniţi.

Definiţia 10.4.6 a) Fie $\aleph_0$ cardinalul unei mulţimi bine ordonate numărabile.

b) Fie acum α un număr ordinal arbitrar şi presupunem că pentru orice $\beta < \alpha$, este definit numărul cardinal $\aleph_\beta$.

- Dacă α este de speţa I, atunci $\aleph_\alpha$ este succesorul numărului cardinal $\aleph_{\alpha-1}$.
- Dacă α este de speţa II, atunci $\aleph_\alpha$ este succesorul mulţimii bine ordonate $W = \{\aleph_\beta \mid \beta < \alpha\}$.

Observaţii 10.4.7 1) $\aleph_1$ este succesorul lui $\aleph_0$, $\aleph_2$ este succesorul lui $\aleph_1$ etc; $\aleph_\omega$ este succesorul mulţimii bine ordonate $\{\aleph_n \mid n$ număr natural$\}$.

2) Evident, dacă $\alpha < \beta$, atunci $\aleph_\alpha < \aleph_\beta$.

Teorema 10.4.8 *Orice cardinal transfinit este de forma* $\aleph_\alpha$*, pentru un un număr* α.

Demonstraţie. Fie m un cardinal transfinit şi fie

$$M := \{x \mid x \text{ cardinal transfinit, } x < m\}.$$

Mulţimea M este bine ordonată şi fie $\alpha := \overline{M}$. Arătăm prin inducţie transfinită după α că $m = \aleph_\alpha$.

Dacă $\alpha = 0$, atunci $M = \emptyset$, deci $m = \aleph_0$. Presupunem că pentru orice $\beta < \alpha$, afirmaţia are loc.

Dacă α este de speţa I, adică $\alpha = \beta + 1$, atunci avem $\aleph_\beta = n$, unde $\beta = \overline{N}$ şi $N = \{x \mid x < n,\ x \text{ transfinit}\}$. Evident că $n < m$ şi $N = M_n$. Deoarece $\alpha = \beta + 1$, rezultă că m este succesorul lui n, adică m este succesorul lui $\aleph_\beta$; rezultă că $m = \aleph_\alpha$.

Presupunem că α este de speţa II. Pentru orice $\beta < \alpha$ avem că $\aleph_\beta = n_\beta$, unde $\beta = \overline{N}$ şi $N_\beta = \{x \mid x < n_\beta,\ x \text{ transzfinit}\}$. Evident că pentru orice $\beta < \alpha$ avem $n_\beta < m$. Deoarece $\alpha = \lim_{\beta<\alpha} \beta$, rezultă că m este succesorul mulţimii $\{n_\beta\}_{\beta<\alpha}$, adică m este succesorul mulţimii $\{\aleph_\beta\}_{\beta<\alpha}$. ■

Fie $\mathfrak{c} = 2^{\aleph_0}$ cardinalul mulţimii $\mathbb{R}$ a numerelor reale. Din teorema de mai sus rezultă că putem scrie $\mathfrak{c} = \aleph_\alpha$, unde α este un număr ordinal. Problema determinării numărului ordinal α se numeşte **problema continuului.**

Ipoteza continuului, formulată de Georg Cantor, afirmă că $\alpha = 1$.

În 1938, Kurt Gödel a construit un model al teoriei mulţimilor în care ipoteza continuului este adevărată. Deci ipoteza continuului este compatibilă cu sistemul axiomatic NBG. Se pune mai departe întrebarea dacă nu cumva ipoteza continuului rezultă din axiomele NBG. În 1963, Paul Cohen a dat un răspuns negativ, construind un alt model al teoriei mulţimilor în care ipoteza continuului nu este adevărată. Aceasta arată că ipoteza continuului este independentă de axiomele NBG, la fel ca axioma alegerii.

Capitolul 11

INDICAŢII ŞI SOLUŢII

1. Logica propoziţiilor

Exerciţiul 1. Tabelul de adevăr este:

p	q	$p \oplus q$	$p \mid q$	$p \downarrow q$
0	0	0	1	1
0	1	1	1	0
1	0	1	1	0
1	1	0	0	0

Exerciţiul 11. b) Considerăm şirul de formule $(A_m)_{m\geq 1}$ definit prin $A_{nk+i} = A_i$ pentru orice $k \in \mathbb{N}$ şi orice $i = 1, \ldots, n$. Vedem că acest şir este periodic şi are perioada n. Este suficient să arătăm că $A_i \models A_{i+k}$ pentru orice $i, k \in \mathbb{N}^*$. Folosim inducţie după k. Cazul $k = 1$ este adevărat conform ipotezei. Presupunem că avem $A_i \models A_{i+k}$; din ipoteză avem $A_{i+k} \models A_{i+k+1}$; din proprietatea de tranzitivitate deducem că $A_i \models A_{i+k+1}$.

2. Logica de ordinul întâi

Exerciţiul 19. a) $A = \forall x(S \to P)$; $E = \forall x(S \to \neg P)$; $I = \exists x(S \wedge P)$; $O = \exists x(S \wedge \neg P)$; $U = A \vee E$; $Y = I \wedge O$.

b) Următoarele 15 relaţii se verifică uşor folosind tautologiile 2.3.9, precum şi ipoteza, care spune că propoziţia $\exists x S$ este adevărată:

- $A \Rightarrow I$; $E \Rightarrow O$; $A \Rightarrow U$; $E \Rightarrow U$; $Y \Rightarrow I$; $Y \Rightarrow O$ (spunem că aceste perechi sunt *subalterne*).
- $A \Leftrightarrow \neg O$; $E \Leftrightarrow \neg I$; $U \Leftrightarrow \neg Y$ (spunem că ceste perechi sunt *contradictorii*).
- $A \Rightarrow \neg E$ (sau echivalent, $E \Rightarrow \neg A$, adică $A \wedge E \Leftrightarrow 0$); $Y \Rightarrow \neg A$; $Y \Rightarrow \neg E$ (spunem că aceste perechi sunt *contrare*, adică nu pot fi ambele adevărate, dar pot fi ambele false).
- $\neg I \Rightarrow O$ (sau echivalent, $\neg O \Rightarrow I$, adică $I \vee O \Leftrightarrow 1$); $\neg U \Rightarrow I$; $\neg U \Rightarrow O$ (spunem că aceste perechi sunt *subcontrare*, adică nu pot fi ambele false, dar pot fi ambele adevărate).

3. Mulţimi

Exerciţiul 21. Arătăm că orice element al membrului stâng aparţine membrului drept şi invers. De exemplu:

a) Pentru orice $x \in U$ avem

$$\begin{aligned} x \in A \cap (B \cup C) &\Leftrightarrow x \in A \wedge x \in B \cup C \Leftrightarrow x \in A \wedge (x \in B \vee x \in C) \Leftrightarrow \\ &\Leftrightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \Leftrightarrow \\ &\Leftrightarrow x \in A \cap B \vee x \in A \cap C \Leftrightarrow x \in (A \cap B) \cup (A \cap C); \end{aligned}$$

d) Pentru orice $x \in U$ avem

$$\begin{aligned} x \in A \setminus (B \cap C) &\Leftrightarrow x \in A \wedge x \notin (B \cap C) \Leftrightarrow x \in A \wedge (x \notin B \vee x \notin C) \Leftrightarrow \\ &\Leftrightarrow (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C) \Leftrightarrow \\ &\Leftrightarrow x \in A \setminus B \vee x \in A \setminus C \Leftrightarrow x \in (A \setminus B) \cup (A \setminus C). \end{aligned}$$

Exercițiul 22. a) Deoarece $A \setminus A = B \setminus B = \varnothing$, și $A \setminus B = A \cap \complement B,\ B \setminus A = B \cap \complement A$, obținem că

$$\begin{aligned} A \triangle B &= (A \cup B) \setminus (A \cap B) = (A \setminus (A \cap B)) \cup (B \setminus (A \cap B)) = \\ &= ((A \setminus A) \cup (A \setminus B)) \cup ((B \setminus A) \cup (B \setminus B)) = (A \setminus B) \cup (B \setminus A) = (A \cap \complement B) \cup (B \cap \complement A). \end{aligned}$$

b) $A \triangle B = (A \setminus B) \cup (B \setminus A) = (B \setminus A) \cup (A \setminus B) = B \triangle A$;
c) Arătăm întâi că $\complement(A \setminus B) = \complement A \cup B$: pentru orice $x \in U$ avem

$$x \in \complement(A \setminus B) \Leftrightarrow x \notin A \setminus B \Leftrightarrow (x \notin A \vee x \in B) \Leftrightarrow x \in \complement A \vee x \in B \Leftrightarrow x \in \complement A \cup B;$$

revenim la afirmația de demonstrat:

$$\begin{aligned} (A \triangle B) \triangle C &= ((A \triangle B) \cap \complement C) \cup (C \cap \complement(A \triangle B)) = \\ &= (((A \cap \complement B) \cup (B \cap \complement A)) \cap \complement C) \cup (C \cap (\complement(A \cup B) \cup (A \cap B))) = \\ &= (A \cap \complement B \cap \complement C) \cup (B \cap \complement A \cap \complement C) \cup (C \cap \complement A \cap \complement B) \cup (A \cap B \cap C); \end{aligned}$$

deoarece ultima expresie este simetrică în A, B, C, din b) rezultă că

$$(A \triangle B) \triangle C = (B \triangle C) \triangle A = A \triangle (B \triangle C).$$

d) $A \triangle \varnothing = (A \setminus \varnothing) \cup (\varnothing \setminus A) = A \cup \varnothing = A$, $A \triangle A = (A \cup A) \setminus (A \cap A) = A \setminus A = \varnothing$;
e) $A \cap (B \triangle C) = A \cap ((B \setminus C) \cup (C \setminus B)) = (A \cap (B \setminus C)) \cup (A \cap (C \setminus B)) = ((A \cap B) \setminus C) \cup ((A \cap C) \setminus B) = ((A \cap B) \setminus (A \cap C)) \cup ((A \cap C) \setminus (A \cap B)) = (A \cap B) \triangle (A \cap C)$.

Exercițiul 23. $A = ((A \cup C) \setminus C) \cup (A \cap C) = ((B \cup C) \setminus C) \cup (B \cap C) = B$.

Exercițiul 24. a) Folosind exercițiul anterior, avem $X = ((A \cup X) \setminus A) \cup (A \cap X) = (C \setminus A) \cup B$;
b) $A \cap X = A \setminus (A \setminus X) = A \setminus B \Rightarrow X = (X \setminus A) \cup (A \cap X) = C \cup (A \setminus B)$.

Exercițiul 25. a) Din definiții rezultă că

$$\begin{aligned} (A \cap B) \times (C \cap D) &= \{(x, y) \mid x \in (A \cap B) \text{ și } y \in (C \cap D)\} = \\ &= \{(x, y) \mid x \in A \text{ și } x \in B \wedge y \in C \text{ și } y \in D\} = \\ &= \{(x, y) \mid x \in A \text{ și } y \in C\} \cap \{(x, y) \mid x \in B \text{ și } y \in D\} \\ &= (A \times C) \cap (B \times D). \end{aligned}$$

b) Dacă presupunem că $A \setminus B \neq \varnothing$, $D \setminus C \neq \varnothing$, $x \in A \setminus B$, $y \in D \setminus C$, atunci $(x, y) \in (A \cup B) \times (C \cup D)$ de $(x, y) \notin (A \times C) \cup (B \times D)$, deoarece $(x, y) \notin (A \times C)(y \notin C)$ și $(x, y) \notin (B \times D)(x \notin B)$; deci incluziunea $(A \times C) \cup (B \times D) \subseteq (A \cup B) \times (C \cup D)$ nu e în general egalitate.

Exercițiul 26. Notăm $A_0 = \emptyset$ și $A_n = \{\ldots\{\emptyset\}\ldots\}$ (n perechi de acolade) pentru $n \in \mathbb{N}^*$. Avem deci relația de recurență $A_{k+1} = \{A_k\}$ pentru orice $k \in \mathbb{N}$.

Evident, $A_0 \neq A_n$ pentru orice $n \in \mathbb{N}^*$. Fie $0 < m < n$ și presupunem prin absurd că $A_m = A_n$. Atunci este evident că $A_{m-1} = A_{n-1}$. Prin inductie obținem $A_0 = A_{n-k}$, contradicție.

Observație. Se poate da și o demonstrație directă. Fie $n \in \mathbb{N}^*$. Din $A_0 \neq A_n$ rezultă $A_1 = \{A_0\} \neq \{A_n\} = A_{n+1}$. Prin inducție obținem $A_k \neq A_{n+k}$ pentru orice $k \in \mathbb{N}$.

Exercițiul 27. Presupunem că $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$.

Cazul 1. Presupunem $\{a\} = \{c\}$. Atunci $a = c$, deci $\{\{a\}, \{a, b\}\} = \{\{a\}, \{a, d\}\}$.

Cazul 1.1. Presupunem $a = b$. Atunci $\{\{a\}\} = \{\{a\}, \{a, d\}\}$, de unde rezultă $a = d$. În acest caz avem $(a, b) = \{\{a\}\}$.

Cazul 1.2. Presupunem $a \neq b$. Atunci avem și $a \neq d$, de unde rezultă $\{a, b\}\} = \{a, d\}$, deci $b = d$.

Implicația inversă este evidentă.

4. Relații și funcții

Exercițiul 28. $R_2 \circ R_1 = \{(a, c) \mid \exists b \in B : (a, b) \in R_1, (b, c) \in R_2\} = \{(1, 1), (1, 4), (2, 1), (2, 4)\}$;
$R_1 \circ R_2 = \{(b_1, b_2) \in B \times B \mid \exists a \in A \cap C : (b_1, a) \in R_2, (a, b_2) \in R_1\} = \{(3, 2), (3, 3)\}$;
$R_1^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R_1\} = \{(2, 1), (3, 1), (3, 2)\}$;
$R_2^{-1} = \{(c, b) \in C \times B \mid (b, c) \in R_2\} = \{(1, 3), (4, 1), (4, 3)\}$;
$(R_1 \circ R_2)^{-1} = \{(b_2, b_1) \in B \times B \mid (b_1, b_2) \in R_1 \circ R_2\} = \{(2, 3), (3, 3)\}$;
$R_2^{-1} \circ R_1^{-1} = \{(b_1, b_2) \in B \times B \mid \exists a \in A \cap C : (b_1, a) \in R_1^{-1}, (a, b_2) \in R_2^{-1}\} = \{(2, 3), (3, 3)\} = (R_1 \circ R_2)^{-1}$.

Exercițiul 29. $x <^2 y \Leftrightarrow\ \exists\, z \in \mathbb{N} : x < z \text{ și } z < y \Leftrightarrow x + 1 < y \quad (z = x + 1)$;

$x <^3 y \Leftrightarrow x < \circ <^2 y \Leftrightarrow\ \exists\, z \in \mathbb{N} : x+1 < z$ şi $z < y \Leftrightarrow x+2 < y$;

$x < \circ > y \Leftrightarrow\ \exists\, z \in \mathbb{N} : x > z$ şi $z < y \Leftrightarrow\ \exists\, z \in \mathbb{N} : z < \min(x,y)$, deci graficul relaţiei $< \circ >$ este $(\mathbb{N}\setminus\{0\}) \times (\mathbb{N}\setminus\{0\})$;

$x > \circ < y \Leftrightarrow\ \exists\, z \in \mathbb{N} : x < z$ şi $z > y \Leftrightarrow\ \exists\, z \in \mathbb{N} : z > \max(x,y)$, deci graficul relaţiei $> \circ <$ estea $\mathbb{N} \times \mathbb{N}$.

Exerciţiul 30. $(S \cap S') \circ R = \varnothing$; $(S \circ R) \cap (S' \circ R) = \{(1,4),(2,4),(4,1),(4,4)\} \cap \{(1,4),(4,4)\} = \{(1,4),(4,4)\} \neq \varnothing$, deci $(S \cap S') \subset (S \circ R) \cap (S' \circ R)$; $R \circ (S \cap S') = \varnothing$; $(R \circ S) \cap (R \circ S') = \{(1,2),(1,4),(2,1),(2,3),(3,1),(3,3)\} \cap \{(1,1),(1,3),(4,1),(4,3)\} = \varnothing$, deci $R \circ (S \cap S') = (R \circ S) \cap (R \circ S')$.

Exerciţiul 31. b) $(\sigma \circ \rho)^{-1} = (D, A, (S \circ R)^{-1})$ şi $\rho^{-1} \circ \sigma^{-1} = (D, A, R^{-1} \circ S^{-1})$, deci mai este de demonstrat egalitatea $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$: pentru orice $(z,x) \in D \times A$ avem

$$\begin{aligned}(z,x) \in (S \circ R)^{-1} &\Leftrightarrow z(\sigma \circ \rho)^{-1}x \Leftrightarrow x\sigma \circ \rho z \ \Leftrightarrow\ \exists\, y \in B \cap C:\ x\rho y \text{ şi } y\sigma z \Leftrightarrow \\ &\Leftrightarrow\ \exists\, y \in B \cap C:\ z\sigma^{-1}y \text{ şi } y\rho^{-1}x \ \Leftrightarrow\ z\rho^{-1} \circ \sigma^{-1}x \Leftrightarrow (z,x) \in R^{-1} \circ S^{-1};\end{aligned}$$

c) $(\tau \circ \sigma) \circ \rho = (A, F, (T \circ S) \circ R)$ şi $\tau \circ (\sigma \circ \rho) = (A, F, T \circ (S \circ R))$, deci mai este de demonstrat egalitatea $(T \circ S) \circ R = T \circ (S \circ R)$: pentru orice $(x,t) \in A \times F$ avem

$$\begin{aligned}(x,t) \in (T \circ S) \circ R &\Leftrightarrow x(\tau \circ \sigma) \circ \rho t \Leftrightarrow\ \exists\, y \in B \cap C : x\rho y \text{ şi } y\tau \circ \sigma t \Leftrightarrow \\ &\Leftrightarrow\ \exists\, y \in B \cap C:\ x\rho y \text{ şi } \exists\, z \in E \cap D:\ y\sigma z \text{ şi } z\tau t \Leftrightarrow \\ &\Leftrightarrow\ \exists\, y \in B \cap C \text{ şi } \exists\, z \in E \cap D:\ x\rho y \text{ şi } y\sigma z \wedge z\tau t \Leftrightarrow \\ &\Leftrightarrow\ \exists\, z \in E \cap D:\ z\tau t \text{ şi } \exists\, y \in B \cap C:\ x\rho y \text{ şi } y\sigma z \Leftrightarrow \\ &\Leftrightarrow\ \exists\, z \in E \cap D:\ z\tau t \text{ şi } x\sigma \circ \rho z \Leftrightarrow\ \exists\, z \in E \cap D:\ x\sigma \circ \rho z \text{ şi } z\tau t \Leftrightarrow \\ &\Leftrightarrow x\tau \circ (\sigma \circ \rho)t \Leftrightarrow (x,t) \in T \circ (S \circ R);\end{aligned}$$

e) Avem $\sigma \circ (\rho \cap \rho') = (A, D, S \circ (R \cap R'))$ şi $(\sigma \circ \rho) \cap (\sigma \circ \rho') = (A, D, (S \circ R) \cap (S \circ R'))$. Trebuie să arătăm incluziunea $S \circ (R \cap R') \subseteq (S \circ R) \cap (S \circ R')$: pentru orice $(x,z) \in A \times D$ avem

$$\begin{aligned}(x,z) \in S \circ (R \cap R') &\Leftrightarrow x\sigma \circ (\rho \cap \rho')z \Leftrightarrow\ \exists\, y \in B \cap C:\ x\rho \cap \rho' y \text{ şi } y\sigma z \Leftrightarrow \\ &\Leftrightarrow\ \exists\, y \in B \cap C:\ x\rho y \text{ şi } x\rho' y \text{ şi } y\sigma z \Leftrightarrow \\ &\Leftrightarrow\ \exists\, y \in B \cap C:\ (x\rho y \text{ şi } y\sigma z) \wedge (x\rho' y \text{ şi } y\sigma z) \Rightarrow \\ &\Rightarrow \exists\, y_1(=y) \in B \cap C:\ x\rho y_1 \text{ şi } y_1\sigma z \text{ şi } \exists\, y_2(=y) \in B \cap C:\ x\rho' y_2 \text{ şi } y_2\sigma z \Leftrightarrow \\ &\Leftrightarrow x\sigma \circ \rho z \text{ şi } x\sigma \circ \rho' z \Leftrightarrow x(\sigma \circ \rho) \cap (\sigma \circ \rho')z \Leftrightarrow (x,z) \in (S \circ R) \cap (S \circ R').\end{aligned}$$

Exerciţiul 32. $R(X) = \{b_4\}$; $R\langle a_2 \rangle = \{b_4\}$; $R^{-1}(Y) = \{a_1, a_2, a_3\}$; $R^{-1}\langle b_5 \rangle = \{a_3\}$; $R^{-1}(B) = \{a_1, a_2, a_3\}$; $R(A) = \{b_2, b_3, b_4, b_5\}$.

Exerciţiul 33. $\delta\langle 1 \rangle = \{$numere naturale divizibile cu 1$\} = \mathbb{N}$;

$\delta^{-1}(\{4,9\}) = \{$numere naturale ce divid pe 4 sau 9 $\} = \{1,2,3,4,9\}$;

$\delta^{-1}(\mathbb{N}) = \mathbb{N}^*$; $\delta(\mathbb{N}) = \mathbb{N}$.

Exerciţiul 35. c) Pentru orice $b \in B$ avem

$$\begin{aligned}b \in \rho(X \cap X') &\Leftrightarrow\ \exists\, a \in X \cap X':\ a\rho b \Leftrightarrow\ \exists\, a \in X \text{ şi } a \in X':\ a\rho b \Rightarrow \\ &\Rightarrow\ \exists\, a_1(=a) \in X:\ a_1\rho b \text{ şi } \exists\, a_2(=a) \in X':\ a_2\rho b \Leftrightarrow b \in \rho(X) \cap \rho(X');\end{aligned}$$

Pentru orice $b \in B$ avem

$$\begin{aligned}b \in (\rho \cap \rho')(X) &\Leftrightarrow\ \exists\, a \in X:\ a\rho \cap \rho' b \Leftrightarrow\ \exists\, a \in X:\ a\rho b \text{ şi } a\rho' b \Rightarrow \\ &\Rightarrow\ \exists\, a_1(=a) \in X : a_1\rho b\ \exists\, a_2(=a) \in X:\ a_2\rho' b \Leftrightarrow b \in \rho(X) \cap \rho'(X);\end{aligned}$$

d) Pentru orice $d \in D$ avem

$$\begin{aligned}d \in (\sigma \circ \rho)(X) &\Leftrightarrow\ \exists\, a \in X : a\sigma \circ \rho d \Leftrightarrow\ \exists\, a \in X:\ \exists\, b \in B \cap C : a\rho b \text{ şi } b\sigma d \Leftrightarrow \\ &\Leftrightarrow\ \exists\, b \in B \cap C:\ (\ \exists\, a \in X : a\rho b) \text{ şi } b\sigma d \Leftrightarrow\ \exists\, b \in B \cap C:\ b \in \rho(X) \text{ şi } b\sigma d \Leftrightarrow \\ &\Leftrightarrow\ \exists\, b \in \rho(X) \cap C:\ b\sigma d \Leftrightarrow d \in \sigma(\rho(X) \cap C).\end{aligned}$$

Exerciţiul 36. (i)$\Rightarrow$(ii) $\forall\, (x,x) \in \Delta_A$ avem $x \in A \Rightarrow R\langle x \rangle \neq \varnothing \Rightarrow\ \exists\, y \in B : xRy \Rightarrow\ \exists\, y \in B :\ xRy$ şi $yR^{-1}x \Rightarrow (x,x) \in R^{-1} \circ R$;

(ii)$\Rightarrow$(iii) $\forall\, x \in A \Rightarrow (x,x) \in \Delta_A \Rightarrow (x,x) \in R^{-1} \circ R \Rightarrow\ \exists\, y \in B :\ xRy \Rightarrow x \in R^{-1}(B)$, deci $A \subseteq R^{-1}(B)$, şi de aici rezultă că $A = R^{-1}(B)$, deoarece $R^{-1}(B) \subseteq A$;

(iii)⇒(iv) implicaţia din (iv) este echivalentă cu implicaţia $P_1 \cap P_2 \neq \varnothing \Rightarrow (R \circ P_1) \cap (R \circ P_2) \neq \varnothing$, pe care o demonstrăm în continuare: $P_1 \cap P_2 \neq \varnothing \Rightarrow \ \exists\, (x_1, x_2) \in P_1 \cap P_2 \subseteq A' \times A \Rightarrow x_2 \in A$ (conform (iii)) $\Rightarrow \ \exists\, x \in A:\ (x_2, x) \in R \Rightarrow \ \exists\, x_2 \in A:\ (x_1, x_2) \in P_1$ şi $(x_2, x) \in R$ şi $\exists\, x_2 \in A:\ (x_1, x_2) \in P_2$ şi $(x_2, x) \in R \Rightarrow (x_1, x) \in R \circ P_1$ şi $(x_1, x) \in R \circ P_2 \Rightarrow (x_1, x) \in (R \circ P_1) \cap (R \circ P_2) \Rightarrow (R \circ P_1) \cap (R \circ P_2) \neq \varnothing$;

(iv)⇒(v) în (iv) fie $P_1 = P_2 = P$;

(v)⇒(vi) Deoarece $R(X_1 \cap X_2) \subseteq R(X_1) \cap R(X_2)$ rezultă că $(R(X_1) \cap R(X_2) = \varnothing \Rightarrow R(X_1 \cap X_2) = \varnothing)$, deci dacă $P = \{(x, x) \mid x \in X_1 \cap X_2\}$, atunci $R \circ P = \varnothing$ (din (v)) $\Rightarrow P = \varnothing \Rightarrow X_1 \cap X_2 = \varnothing$;

(vi)⇒(vii) în (vi) fie $X_1 = X_2 = X$;

(vii)⇒(i) considerăm mulţimea $X = \{x\}$, unde $x \in A$. Dacă $R(X) = R\langle x\rangle = \varnothing$, atunci din (vii) rezultă că $X = \varnothing$, ceea ce este o contradicţie (deoarece $X = \{x\}$); deci $\ \forall\, x \in A\ R\langle x\rangle \neq \varnothing$.

Exerciţiul 37. (i)⇒(ii) $\forall\, (y_1, y_2) \in R \circ R^{-1}\ \ \exists\, x \in A:\ y_1 R^{-1} x$ şi $xRy_2 \Rightarrow \ \exists\, x \in A:\ xRy_1$ şi $xRy_2 \Rightarrow \ \exists\, x \in A:\ \{y_1, y_2\} \subseteq R\langle x\rangle$ (din (i)) $\Rightarrow y_1 = y_2 \Rightarrow (y_1, y_2) \in \Delta_B$;

(ii)⇒(iii) Deoarece în general $(S_1 \cap S_2) \circ R \subseteq (S_1 \circ R) \cap (S_2 \circ R)$, este suficient de demonstrat incluziunea $(S_1 \circ R) \cap (S_2 \circ R) \subseteq (S_1 \cap S_2) \circ R$: pentru orice (x, z) avem $(x, z) \in (S_1 \circ R) \cap (S_2 \circ R) \Rightarrow (x, z) \in S_1 \circ R$ şi $(x, z) \in S_2 \circ R \Rightarrow \ \exists\, y \in B (x, y) \in R$ şi $(y, z) \in S_1$ şi $\exists\, y' \in B:\ (x, y') \in R$ şi $(y', z) \in S_2 \Rightarrow \ \exists\, x \in A\ (y, x) \in R^{-1}$ şi $(x, y') \in R \Rightarrow (y, y') \in R \circ R^{-1}$ (din (ii)) $\Rightarrow (y, y') \in \Delta_B \Rightarrow y = y' \Rightarrow \ \exists\, y \in B: (x, y) \in R$ şi $(y, z) \in S_1$ şi $(y, z) \in S_2 \Rightarrow \ \exists\, y \in B: (x, y) \in R$ şi $(y, z) \in S_1 \cap S_2 \Rightarrow (x, z) \in (S_1 \cap S_2) \circ R$;

(iii)⇒(iv) $S_1 \cap S_2 = \varnothing \Rightarrow (S_1 \cap S_2) \circ R = \varnothing \circ R = \varnothing$ (din (iii)) $\Rightarrow (S_1 \circ R) \cap (S_2 \circ R) = (S_1 \cap S_2) \circ R = \varnothing$;

(iv)⇒(v) în (iv) fie $S_1 = S$ şi $S_2 = \complement(S)$;

(v)⇒(vi) arătăm că ¬(vi)⇒ ¬(v): ¬(vi)⇒ $\exists\, Y_1, Y_2 \subseteq B: Y_1 \cap Y_2 = \varnothing \wedge R^{-1}(Y_1) \cap R^{-1}(Y_2) \neq \varnothing \Rightarrow \ \exists\, x \in R^{-1}(Y_1) \cap R^{-1}(Y_2) \Rightarrow \ \exists\, y_1 \in Y_1: xRy_1$ şi $\exists\, y_2 \in Y_2:\ xRy_2$ (deoarece $Y_1 \cap Y_2 = \varnothing$) $\Rightarrow y_1 \neq y_2 \Rightarrow$ dacă $S = \{(y_1, y_2)\}$, atunci $(y_2, y_2) \in \complement(S) \Rightarrow \ \exists\, y_1 \in Y_1: (x, y_1) \in R$ şi $(y_1, y_2) \in S \wedge \ \exists\, y_2 \in Y_2: (x, y_2) \in R$ şi $(y_2, y_2) \in \complement(S) \Rightarrow (x, y_2) \in S \circ R \wedge (x, y_2) \in \complement(S) \Rightarrow (S \circ R) \cap (\complement(S) \circ R) \neq \varnothing \Rightarrow \neg$(v);

(vi)⇒(vii) în (vi) fie $Y_1 = Y$ şi $Y_2 = \complement(Y)$;

(vii)⇒(viii) $R^{-1}(Y) \cup R^{-1}(\complement(Y)) = R^{-1}(Y \cup \complement(Y)) = R^{-1}(B) = R^{-1}(B)$ şi (din (vii)) $R^{-1}(Y) \cap R^{-1}(\complement(Y)) = \varnothing \Longrightarrow R^{-1}(B) \setminus R^{-1}(Y) = (R^{-1}(Y) \cup R^{-1}(\complement(Y)) \setminus R^{-1}(Y) = R^{-1}(\complement(Y))$;

(viii)⇒(vii) deoarece $R^{-1}(B) = R^{-1}(Y) \cup R^{-1}(\complement(Y))$ şi din (viii) avem $R^{-1}(B) \setminus R^{-1}(Y) = R^{-1}(\complement(Y)) \Longrightarrow R^{-1}(Y) \cap R^{-1}(\complement(Y)) = \varnothing$;

(vii)⇒(i) aratăm că ¬(i)⇒ ¬(vii): ¬(i)⇒ $\exists\, x \in A:\ |R\langle x\rangle| \geq 2 \Rightarrow \exists\, y_1, y_2 \in B: y_1 \neq y_2$ şi $(x, y_1) \in R$ şi $(x, y_2) \in R \Rightarrow x \in R^{-1}\langle y_1\rangle$ şi $x \in R^{-1}\langle y_2\rangle \Rightarrow R^{-1}\langle y_1\rangle \cap R^{-1}\langle y_2\rangle \neq \varnothing \Rightarrow$ dacă $Y = \{y_1\}$, atunci $y_2 \in \complement(Y)$ (deoarece $y_1 \neq y_2$) $\Rightarrow \varnothing \neq R^{-1}\langle y_1\rangle \cap R^{-1}\langle y_2\rangle = R^{-1}(Y) \cap R^{-1}\langle y_2\rangle \subseteq R^{-1}(Y) \cap R^{-1}(\complement(Y)) \Rightarrow \ \exists\, Y \subseteq B: R^{-1}(Y) \cap R^{-1}(\complement(Y)) \neq \varnothing \Rightarrow \neg$(vii).

Exerciţiul 38. (i)⇒(ii) Presupunem $S \circ R_1 = S \circ R_2$; atunci $\forall\, x \in A:\ (S \circ R_1)\langle x\rangle = (S \circ R_2)\langle x\rangle \Rightarrow S(R_1\langle x\rangle) = S(R_2\langle x\rangle)$; din ipoteza (i) rezultă că $\forall\, x \in A$ avem $R_1\langle x\rangle = R_2\langle x\rangle$, deci $R_1 = R_2$;

(ii)⇒(i) Fie $Y_1, Y_2 \subseteq B$ astfel ca $S(Y_1) = S(Y_2)$; alegem $R_1 = \{(x, y_1) \mid x \in A,\ y_1 \in Y_1\} = A \times Y_1$ şi $R_2 = \{(x', y_2) \mid x' \in A,\ y_2 \in Y_2\} = A \times Y_2$; atunci $S(Y_1) = S(Y_2) \Rightarrow \ \forall\, x \in A:\ S(R_1\langle y\rangle) = S(R_2\langle y\rangle) \Rightarrow \ \forall\, x \in A: (S \circ R_1)\langle y\rangle = (S \circ R_2)\langle y\rangle \Rightarrow S \circ R_1 = S \circ R_2 \Rightarrow R_1 = R_2 \Rightarrow Y_1 = Y_2$.

Exerciţiul 39. Rezultă imediat din Exerciţiul 38, schimbând pur şi simplu notaţiile: scriem R^{-1} în loc de S, A în loc de C, C în loc de A, S_i^{-1} în loc de R_i $(i = 1, 2)$ şi tinând cont că $(S_i \circ R)^{-1} = R^{-1} \circ S_i^{-1}$ respectiv $S_1 = S_1 \Leftrightarrow S_1^{-1} = S_2^{-1}$. Dăm totuşi şi o demonstraţie independentă de Exerciţiul 38 .

¬(ii)⇒¬(i) Presupunem că există $S_1, S_2 \subseteq B \times C$ astfel ca $S_1 \circ R = S_2 \circ R$ şi $S_1 \neq S_2$. Arătăm că există $Y_1, Y_2 \subseteq B$ astfel ca $Y_1 \neq Y_2$ şi $R^{-1}(Y_1) = R^{-1}(Y_2)$.

Din $S_1 \neq S_2$ rezultă că există $y \in B$ astfel ca $S_1\langle y\rangle = S_2\langle y\rangle$, deci putem presupune că există $z \in C$ astfel ca yS_1z şi $y \not{S}_2 z$.

Fie $Y_1 := B$ şi $Y_2 := B \setminus \{y\}$, deci $Y_2 \subsetneq Y_1$. Evident, $R^{-1}(Y_2) \subseteq R^{-1}(Y_1)$. Invers, fie $x \in R^{-1}(Y_1) = R^{-1}(B)$; trebuie analizat cazul $x \in R^{-1}\langle y\rangle$, adică xRy; atunci din xRy şi yS_1z obţinem $xS_1 \circ Rz$. Din ipoteză avem $xS_2 \circ Rz$, deci există $y_1 \in B$ astfel ca xRy_1 şi y_1S_2z, deci $y_1 \neq y$. Obţinem $x \in R^{-1}\langle y_1\rangle \subseteq R^{-1}(B \setminus \{y\}) = R^{-1}(Y_2)$.

¬(i)⇒¬(ii) Presupunem că există $Y_1, Y_2 \subseteq B$ astfel ca $Y_1 \neq Y_2$ şi $R^{-1}(Y_1) = R^{-1}(Y_2) =: X$. Arătăm că există $S_1, S_2 \subseteq B \times C$ astfel ca $S_1 \circ R = S_2 \circ R$ şi $S_1 \neq S_2$.

Fie $C := A$, $S_1 := Y_1 \times X$, $S_2 := Y_2 \times X$, deci $S_1 \neq S_2$. Arătăm că $S_1 \circ R = S_2 \circ R$.

Fie $(a, c) \in A \times A$. Aven $aS_1 \circ R$, deci există $y_1 \in B$ astfel ca aRy_1 şi y_1S_1c; atunci $c \in X = R^{-1}(Y_1) = R^{-1}(Y_2)$ şi $y_1 \in Y_1$. Mai mult, $a \in R^{-1}(Y_1) = R^{-1}(Y_2)$, deci există $y_2 \in Y_2$ astfel ca aRy_2; atunci $(y_2, c) \in Y_2 \times X = S_2$, deci avem aRy_2 şi y_2S_2c, adică $aS_2 \circ Rc$.

Am obţinut astfel că $S_1 \circ R \subseteq S_2 \circ R$. Analog se arată că $S_2 \circ R \subseteq S_1 \circ R$.

Exerciţiul 41. Dacă relaţia $\rho = (A, B, R)$ este funcţie, atunci: $\ \forall\, x \in A \Rightarrow (\exists!) y \in B: x\rho y \Rightarrow \ \exists\, y \in B: x\rho y$ şi $y\rho^{-1}x \Rightarrow x\rho^{-1} \circ \rho y \Longrightarrow \mathbf{1}_A \subseteq \rho^{-1} \circ \rho$ şi $\ \forall\, y_1, y_2 \in B:\ y_1\rho \circ \rho^{-1}y_2 \Rightarrow \ \exists\, x \in A:\ y_1\rho^{-1}x$ şi $dx\rho y_2 \Rightarrow \exists\, x \in A:\ x\rho y_1$ şi $x\rho y_2$ (dar ρ este funcţie) $\Rightarrow y_1 = y_2 \Longrightarrow \rho \circ \rho^{-1} \subseteq \mathbf{1}_B$.

Dacă $\mathbf{1}_A \subseteq \rho^{-1}\circ\rho$ şi $\rho\circ\rho^{-1} \subseteq \mathbf{1}_B$, atunci: $\forall\, x \in A \Rightarrow x\rho^{-1}\circ\rho x$ (deoarece $\mathbf{1}_A \subseteq \rho^{-1}\circ\rho$)$\Rightarrow\ \exists\, y \in B:\ x\rho y$ şi dacă $\exists\, x \in A,\ \exists\, y_1, y_2 \in B : x\rho y_1$ şi $x\rho y_2 \Rightarrow\ \exists\, x \in A:\ y_1\rho^{-1}x$ şi $x\rho y_2 \Rightarrow y_1\rho\circ\rho^{-1}y_2 \Rightarrow y_1 = y_2$ (deoarece $\rho\circ\rho^{-1} \subseteq \mathbf{1}_B$); deci $\forall\, x \in A \Rightarrow (\exists!) y \in B : x\rho y \Longrightarrow \rho = (A, B, R)$ este funcţie.

Exerciţiul 42. a), b) Deoarece $f : A \to B$ este funcţie, din Exerciţiul 41 avem: $\mathbf{1}_A \subseteq f^{-1}\circ f$ şi $f\circ f^{-1} \subseteq \mathbf{1}_B \Rightarrow \forall\, X \subseteq A,\ \forall\, Y \subseteq B \Rightarrow X = \mathbf{1}_A(X) \subseteq (f^{-1}\circ f)(X)$ şi $(f\circ f^{-1})(Y) \subseteq \mathbf{1}_B = Y \Rightarrow X \subseteq f^{-1}(f(X)), f(f^{-1}(Y)) \subseteq Y$.

c) Deoarece $f : A \to B$ este funcţie, din Exerciţiul 41. avem: $\mathbf{1}_A \subseteq f^{-1}\circ f$ şi $f\circ f^{-1} \subseteq \mathbf{1}_B \Rightarrow f\circ\mathbf{1}_A \subseteq f\circ(f^{-1}\circ f)$ şi $(f\circ f^{-1})\circ f \subseteq \mathbf{1}_B\circ f \Rightarrow f \subseteq f\circ(f^{-1}\circ f)$ şi $(f\circ f^{-1})\circ f \subseteq f \Rightarrow f = f\circ(f^{-1}\circ f) = f\circ f^{-1}\circ f$.

La toate punctele se poate argumenta şi independent de Exerciţiul 41.

Exerciţiul 43. f) Pentru orice $x \in U$ avem:

$$x \in \bigcup_{j\in J}(A\cap B_j) \Leftrightarrow\ \exists\, j \in J:\ x \in A\cap B_j \Leftrightarrow\ \exists\, j \in J:\ x \in A \text{ şi } dx \in B_j \Leftrightarrow$$

$$\Leftrightarrow x \in A \text{ şi } \exists\, j \in J:\ x \in B_j \Leftrightarrow x \in A \text{ şi } x \in \bigcup_{j\in J} B_j \Leftrightarrow\ x \in A\cap(\bigcup_{j\in J} B_j).$$

h) Pentru orice $x \in U$ avem:

$$x \in \bigcup_{i\in I}(\bigcap_{j\in J}(A_{ij})) \Leftrightarrow\ \exists\, i \in I : x \in \bigcap_{j\in J}(A_{ij}) \Leftrightarrow\ \exists\, i \in I:\ \forall\, j \in J : x \in A_{ij}\ \Rightarrow$$

$$\Rightarrow\ \forall\, j \in J\ \ x \in \bigcup_{i\in I} A_{ij} \Leftrightarrow x \in \bigcap_{j\in J}(\bigcup_{i\in I} A_{ij}).$$

Exerciţiul 44. a) Pentru orice (x, y) avem: $(x, y) \in (\bigcap_{i\in I} X_i)\times(\bigcap_{i\in I} Y_i) \Leftrightarrow x \in \bigcap_{i\in I} X_i$ şi $y \in \bigcap_{i\in I} Y_i \Leftrightarrow\ \forall\, i \in I : x \in X_i$ şi $y \in Y_i \Leftrightarrow\ \forall\, i \in I:\ (x, y) \in (X_i \times Y_i) \Leftrightarrow\ (x, y) \in \bigcap_{i\in I}(X_i \times Y_i)$;

b) Pentru orice (x, y) avem: $(x, y) \in (\bigcup_{i\in I} X_i)\times(\bigcup_{j\in J} Y_j) \Leftrightarrow x \in \bigcup_{i\in I} X_i$ şi $y \in \bigcup_{j\in J} Y_j \Leftrightarrow\ \exists\, i \in I:\ x \in X_i$ şi $\exists\, j \in J:\ y \in Y_j \Leftrightarrow\ \exists\, (i, j) \in I\times J : (x, y) \in X_i \times Y_j \Leftrightarrow (x, y) \in \bigcup_{(i,j)\in I\times J}(X_i \times Y_j)$.

Exerciţiul 45. Pentru $n \in \mathbb{N}^*$ fixat avem: $B_n = A_n \setminus (\bigcap_{i=0}^{n-1} A_i) = \bigcup_{i=0}^{n-1}(A_n \setminus A_i)$; rezultă că:

$$\begin{aligned}\bigcup_{n\in\mathbb{N}} B_n &= A_0 \cup \bigcup_{n\in\mathbb{N}^*}(\bigcup_{i=0}^{n-1}(A_n \setminus A_i)) = \\ &= A_0 \cup (A_1 \setminus A_0) \cup \cdots \cup (A_n \setminus A_0) \cup (A_n \setminus A_1) \cup \cdots \cup (A_n \setminus A_{n-1}) \cup \cdots = \\ &= A_0 \cup A_1 \cup A_2 \cup \cdots \cup A_n \cup \cdots = \bigcup_{n\in\mathbb{N}} A_n\end{aligned}$$

(am folosit faptul că $A\cup(B\setminus A) = A\cup B$); dacă presupunem că $\exists\, m, n \in \mathbb{N}, m \neq n$, astfel încât, de exemplu, $m < n$ şi $B_m \cap B_n \neq \varnothing$, atunci $\exists x \in U$ astfel încât $x \in B_m$ és $x \in B_n$; rezultă că $\exists x \in U:\ x \in A_m \setminus (\bigcap_{i=0}^{m-1} A_i)$ şi $x \in A_n \setminus (\bigcap_{i=0}^{n-1})A_i) = \bigcup_{i=0}^{n-1}(A_n \setminus A_i)$, deci deoarece $m < n,\ \exists\, x \in U:\ x \in A_m$ şi $x \in A_n \setminus A_m$, contradicţie.

Exerciţiul 46. b) Considerăm mulţimile $X_n = \left(-\frac{1}{n}, \frac{1}{n}\right), n \in \mathbb{N}^*$ şi funcţia sgn; atunci $\operatorname{sgn}(\bigcap_{n\in\mathbb{N}^*} X_n) = \{0\} \subset \bigcap_{n\in\mathbb{N}^*} \operatorname{sgn} X_n = \{-1, 0, +1\}$;

d) Pentru orice $x \in A$ avem:

$$x \in f^{-1}(\bigcap_{i\in I} Y_i) \Leftrightarrow f(x) \in \bigcap_{i\in I} Y_i \Leftrightarrow\ \forall\, i \in I:\ f(x) \in Y_i \Leftrightarrow\ \forall\, i \in I : x \in f^{-1}(Y_i) \Leftrightarrow x \in \bigcap_{i\in I} f^{-1}(Y_i).$$

Exerciţiul 47. Pentru orice X avem:

$$X \in \mathcal{P}(\bigcap_{i\in I} A_i) \Leftrightarrow X \subseteq \bigcap_{i\in I} A_i \Leftrightarrow\ \forall\, i \in I:\ X \subseteq A_i \Leftrightarrow\ \forall\, i \in I:\ X \in \mathcal{P}(A_i) \Leftrightarrow X \in \bigcap_{i\in I} \mathcal{P}(A_i).$$

Exerciţiul 48. a) Pentru orice $(x, z) \in A\times D$ avem:

$$x\sigma\circ(\bigcup_{i\in I}\rho_i)z \Leftrightarrow\ \exists\, y \in B\cap C:\ x\bigcup_{i\in I}\rho_i y \text{ şi } y\sigma z \Leftrightarrow\ \exists\, y \in B\cap C:\ \exists\, i \in I:\ x\rho_i y \text{ şi } y\sigma z \Leftrightarrow$$

$$\Leftrightarrow\ \exists\, i \in I:\ \ \exists\, y \in B\cap C:\ x\rho_i y \text{ şi } y\sigma z \Leftrightarrow\ \exists\, i \in I:\ x\sigma\circ\rho_i z \Leftrightarrow x\bigcup_{i\in I}(\sigma\circ\rho_i)z.$$

c) Pentru orice $(x, z) \in A \times D$ avem:

$$x\sigma \circ (\bigcap_{i\in I} \rho_i)z \Leftrightarrow \ \exists\, y \in B \cap C:\ x \bigcap_{i\in I} \rho_i y \text{ şi } y\sigma z \Leftrightarrow \ \exists\, y \in B \cap C:\ \ \forall\, i \in I: x\rho_i y \text{ şi } y\sigma z \Rightarrow$$
$$\Rightarrow \ \forall\, i \in I:\ \ \exists\, y \in B \cap C:\ x\rho_i y \text{ şi } y\sigma z \Leftrightarrow \ \forall\, i \in I:\ x\sigma \circ \rho_i z \Leftrightarrow x \bigcap_{i\in I} (\sigma \circ \rho_i)z.$$

Exerciţiul 49. a) Injectivitatea: deoarece $\forall\, x_1, x_2 \in A$ avem $(g \circ f)(x_1) = (g \circ f)(x_2) \Rightarrow g(f(x_1)) = g(f(x_2))$ (deoarece g este injectiv)$\Rightarrow f(x_1) = f(x_2)$ (deoarece f este injectiv) $\Rightarrow x_1 = x_2 \Longrightarrow g \circ f$ este injectiv;

surjectivitatea: $\forall\, z \in C:\ \exists\, y \in B: g(y) = z$ (deoarece g este surjectiv) şi $\forall\, y\ \ \exists\, x \in A:\ f(x) = y$ (deoarece f este surjectiv)$\Rightarrow\ \forall\, z \in C:\ \exists\, x \in A: g(f(x)) = z$ deci $g \circ f$ este surjectiv;

b) dacă $g \circ f$ este injectiv, atunci $\forall\, x_1, x_2 \in A$ avem $f(x_1) = f(x_2) \Rightarrow g(f(x_1)) = g(f(x_2)) \Rightarrow (g \circ f)(x_1) = (g \circ f)(x_2) \Rightarrow x = y$, deci f într-adevăr este injectiv;

dacă $g \circ f$ este surjectiv, atunci $\forall\, z \in C$ avem $\exists\, x \in A: (g \circ f)(x) = z \Rightarrow\ \exists\, x \in A: g(f(x)) = z \Rightarrow\ \exists\, y = f(x) \in B: g(y) = z$, deci g este într-adevăr surjectiv;

c) $\forall\, y_1, y_2 \in B: g(y_1) = g(y_2)$ (deoarece f este surjectiv) $\Rightarrow\ \exists\, x_1 \in A: f(x_1) = y_1$ şi $\exists\, x_2 \in A:\ f(x_2) = y_2 \Rightarrow\Rightarrow g(f(x_1)) = g(f(x_2)) \Rightarrow (g \circ f)(x_1) = (g \circ f)(x_2)$ ($g \circ f$ este injectiv)$\Rightarrow\ x_1 = x_2\ \Rightarrow\ y_1 = f(x_1) = f(x_2) = y_2$, deci g într-adevăr este injectiv;

d) $\forall\, y \in B$ ($g \circ f$ este surjectiv)$\Rightarrow g(y) \in C$-re $\ \exists\, x \in A: (g \circ f)(x) = g(y)\ \Rightarrow\ g(f(x)) = g(y)$ (deoarece g este injectiv)$\Rightarrow f(x) = y$, deci $\forall\, y \in B:\ \exists\, x \in A: f(x) = y$, adică f este surjectiv.

Observaţie: Putem demonstra proprietăţile de mai sus folosind inversele la stânga sau dreapta. De exemplu în d): $g \circ f$ este surjectiv, deci $g \circ f$ are inversă la drepta s, adică $(g \circ f) \circ s = 1_C$. Analog, deoarece g este injectiv, rezultă că $\exists$ inversă la stânga r, deci $r \circ g = 1_B \Rightarrow r \circ (g \circ f) = f \Rightarrow r \circ ((g \circ f) \circ s) = f \circ s \Rightarrow r = f \circ s \Rightarrow 1_B = r \circ g = f \circ (s \circ g) \Rightarrow s \circ g$ este inversă la drepta pentru f, deci f este surjectiv.

Exerciţiul 50. a) Pentru orice $x \in A$ avem:

$$x \in f^{-1}(Y_1 \setminus Y_2) \Leftrightarrow f(x) \in Y_1 \setminus Y_2 \Leftrightarrow f(x) \in Y_1 \wedge f(x) \notin Y_2 \Leftrightarrow$$
$$\Leftrightarrow x \in f^{-1}(Y_1) \wedge x \notin f^{-1}(Y_2) \Leftrightarrow\ x \in f^{-1}(Y_1) \setminus f^{-1}(Y_2).$$

b) Pentru orice $y \in B$ avem $y \in f(X_1 \setminus X_2)$ (deoarece f este injectiv) $\Leftrightarrow\ \exists\, !x \in X_1 \setminus X_2 : f(x) = y \Leftrightarrow y = f(x) \in f(X_1)$ şi $y = f(x) \notin f(X_2) \Leftrightarrow\ y \in f(X_1) \setminus f(X_2)$.

Deoarece $f(\bigcap_{i\in I} X_i) \subseteq \bigcap_{i\in I} f(X_i)$, este suficient de demonstrat incluziunea $\bigcap_{i\in I} f(X_i) \subseteq f(\bigcap_{i\in I} X_i)$: într-adevăr, pentru orice $y \in B$ avem: $y \in \bigcap_{i\in I} f(X_i) \Rightarrow\ \ \forall\, i \in I: y \in f(X_i)$ (deoarece f este injectiv) $\Rightarrow\ \exists\, !x:\ x \in X_i\ \ \forall\, i \in I$ şi $f(x) = y \Rightarrow\ \exists\, x \in \bigcap_{i\in I} X_i : f(x) = y \Rightarrow y \in f(\bigcap_{i\in I} X_i)$.

Exerciţiul 50. a) (i)$\Rightarrow$(ii) deoarece $1_A \subseteq f^{-1} \circ f$ (deoarece f este funcţie), este suficient de demonstrat incluziunea $f^{-1} \circ f \subseteq 1_A$: într-adevăr, pentru orice $x_1, x_2 \in A$ avem:

$$x_1 f^{-1} \circ f x_2 \Rightarrow\ \exists\, y \in B:\ x_1 f y \wedge y f^{-1} x_2 \Rightarrow\ \exists\, y \in B:\ f(x_1) = y \wedge f(x_2) = y \Rightarrow$$
$$\Rightarrow f(x_1) = f(x_2) = y \Rightarrow x_1 = x_2 \Rightarrow x_1 1_A x_2.$$

(ii)$\Rightarrow$(iii) Din (ii) rezultă că $f^{-1} \circ f = 1_A \Rightarrow\ \forall\, X \subseteq A: f^{-1}(f(X)) = 1_A(X) = X$;

(iii)$\Rightarrow$(iv) deoarece $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$, este suficient de demonstrat incluziunea $f(X_1) \cap f(X_2) \subseteq f(X_1 \cap X_2)$: într-adevăr, pentru orice $y \in B$ avem:

$$y \in f(X_1) \cap f(X_2) \Rightarrow\ \exists\, x_1 \in X_1:\ f(x_1) = y \text{ şi } \ \exists\, x_2 \in X_2:\ f(x_2) = y \Rightarrow$$
$$\Rightarrow f^{-1}(\{y\}) = f^{-1}(f(\{x_1\})) = \{x_1\} \text{ şi } \ f^{-1}(\{y\}) = f^{-1}(f(\{x_2\})) = \{x_2\} \Rightarrow$$
$$\Rightarrow x_1 = x_2 = x \in X_1 \cap X_2 \Rightarrow\ \exists\, x \in X_1 \cap X_2:\ f(x) = y \Rightarrow y \in f(X_1 \cap X_2).$$

(iv)$\Rightarrow$(v) în (iv) fie $X_1 = X$ şi $X_2 = \complement(X)$; rezultă că $f(X) \cap f(\complement(X)) = \varnothing$, deci $f(\complement(X)) \subseteq \complement(f(X))$.

(v)$\Rightarrow$(i) Pentru orice $x_1, x_2 \in A$, dacă $x_1 \neq x_2 \Rightarrow$ şi în (v) $X = \{x_1\}$, atunci $x_2 \in \complement(X) \Rightarrow f(x_2) \in \complement(f(x_1)) \Rightarrow f(x_1) \neq f(x_2)$, deci este injectiv;

b) (i)$\Rightarrow$(ii) deoarece $f \circ f^{-1} \subseteq 1_B$ (deoarece f funcţie), este suficient de demonstrat incluziunea $1_B \subseteq f \circ f^{-1}$; într-adevăr deoarece din (i) f este surjectiv, rezultă că pentru orice $\forall\, y \in B\ \ \exists\, x \in A:\ f(x) = y \Rightarrow\ \exists\, x \in A: xfy \Rightarrow\ \exists\ : yf^{-1}x \wedge xfy \Rightarrow yf \circ f^{-1}y$.

(ii)$\Rightarrow$(iii) deoarece din (ii) avem $f \circ f^{-1} = 1_B \Rightarrow\ \forall\, Y \subseteq B: (f \circ f^{-1})(Y) = 1_B(Y) = Y$ és $f(f^{-1}(Y)) = Y$.

(iii)$\Rightarrow$(i) deoarece din (iii) pentru orice $Y \subseteq B$ avem $f(f^{-1}(Y)) = Y$, rezultă că pentru orice $y \in B$ $f(f^{-1}(y)) = y \Rightarrow\ \forall\, y \in B: yf \circ f^{-1}y \Rightarrow\ \forall\, y \in B:\ \exists\, x \in A: xfy \Rightarrow\Rightarrow\ \forall\, y \in B:\ \exists\, x \in A: f(x) = y$, deci f este surjectiv.

(i)$\Rightarrow$(iv) $\forall\, y \in \complement(f(X)) \Rightarrow\ \forall\, x \in X: f(x) \neq y$, dar din (i) avem că f este surjectiv, deci $\exists\, x_y \in \complement(X): f(x_y) = y \Rightarrow y \in f(\complement(X))$.

(iv)⇒(i) fie în (iv) $X = A \Rightarrow \complement(f(A)) \subseteq f(\complement A) \Rightarrow \complement(f(A)) = \varnothing \Rightarrow B = f(A)$, deci f este surjectiv.

Exerciţiul 52. a) Presupunem că f este injectiv; dacă presupunem că există $s_1, s_2 : B \to A$ astfel încât $f \circ s_1 = f \circ s_2 = \mathbf{1}_B \Rightarrow \forall\, y \in B : f(s_1(y)) = f(s_2(y)) = y$ (deoarece f este injectiv) $\Rightarrow \Rightarrow \forall\, y \in B : s_1(y) = s_2(y) \Rightarrow s_1 = s_2 \Rightarrow (\exists!)\ s : B \to A$ astfel încât $f \circ s = \mathbf{1}_B$; presupunem că f are exact o inversă la dreapta: dacă presupunem că există $x_1 \neq x_2 \in A$ astfel încât $y = f(x_1) = f(x_2)$ (adică, f nu este injectiv), atunci putem construi două inverse la dreapta distincte $s_1, s_2 : B \to A$ pentru f, astfel încât $s_1(y) = x_1$ şi $s_2(y) = x_2$, contradicţie, deci f este injectiv;

b) Fie f surjectiv: dacă presupunem că există $r_1,\ r_2 : B \to A$ astfel încât $r_1 \circ f = r_2 \circ f = \mathbf{1}_A \Rightarrow \forall\, x \in A : (r_1 \circ f)(x) = (r_2 \circ f)(x) = x$, dar pentru orice $y \in B\ \ \exists\, x \in A : f(x) = y$ (deoarece f este surjectiv)⇒ $\forall\, y \in B : r_1(y) = r_2(y) \Rightarrow r_1 = r_2$, deci f într-adevăr are o inversă la stânga; reciproca într-adevăr nu e adevărată: dacă $f : \{1\} \to \{1, 2\}, f(1) = 2$, atunci f este injectiv, nu este surjectiv şi are exact o inversă la stânga $r : \{1, 2\} \to \{1\}, r(2) = 1, r(1) = 1$.

Exerciţiul 53. Fie $g = s \circ r$, unde s este inversă la drepta a funcţiei surjective $f' : A \to f(A)$, $\forall\, x \in A\ f'(x) = f(x)$, iar r este inversă la stânga a funcţiei injective canonice $i : f(A) \to B$, $i(y) = y\ \forall\, y \in f(A)$.

Exerciţiul 54. a) $\mathbf{1}_A \times \mathbf{1}_B : A \times B \to A \times B,\ \ (\mathbf{1}_A \times \mathbf{1}_B)(x, y) = (\mathbf{1}_A(x), \mathbf{1}_B(y)) = (x, y)$, deci $\mathbf{1}_A \times \mathbf{1}_B = \mathbf{1}_{A\times B}$;

b) $(f' \times g') \circ (f \times g) : A \times B \to A'' \times B'', (f' \circ f) \times (g' \circ g) : A \times B \to A'' \times B''$ şi pentru orice $(x, y) \in A \times B$ avem:

$$\begin{aligned}((f' \times g') \circ (f \times g))(x, y) &= (f' \times g')((f \times g)(x, y)) = (f' \times g')(f(x), g(y)) = (f'(f(x)), g'(g(y))) = \\ &= ((f' \circ f)(x), (g' \circ g)(y)) = ((f' \circ f) \times (g' \circ g))(x, y),\end{aligned}$$

deci $(f' \times g') \circ (f \times g) = (f' \circ f) \times (g' \circ g)$.

c) Pentru orice $X \subseteq A$ és $Y \subseteq B$ avem:

$$(f \times g)(X \times Y) = (f \times g)(\{(a, b) \mid a \in X,\ b \in Y\}) = \{(f(a), f(b)) \mid a \in X,\ b \in Y\} = f(X) \times f(Y).$$

d) Pentru orice $(x, y) \in X \times Y$ avem

$$\begin{aligned}(x, y) \in (f \times g)^{-1}(X' \times Y') &\Leftrightarrow (f \times g)(x, y) \in X' \times Y' \Leftrightarrow f(x), g(y)) \in X' \times Y' \Leftrightarrow \\ &\Leftrightarrow f(x) \in X',\ g(y) \in Y' \Leftrightarrow x \in f^{-1}(X'),\ y \in g^{-1}(Y') \Leftrightarrow \\ &\Leftrightarrow (x, y) \in f^{-1}(X') \times g^{-1}(Y').\end{aligned}$$

e) Contraexemplu: fie $A = B = A' = B' = \{1, 2\}$, $M = \{(1, 2), (2, 1)\}$ şi fie $\varphi : A \times B \to A' \times B'$, $\varphi((1, 1)) = (2, 1), \varphi((1, 2)) = (1, 2), \varphi((2, 1)) = (1, 1), \varphi((2, 2)) = (2, 2)$.

Exerciţiul 56. a) „⇒" este lăsat pe seama cititorului.

„⇐" *injectivitatea*: pentru orice $x_1, x_2 \in A$ avem $f(x_1) = f(x_2) \Rightarrow$ pentru un $b \in B$ fixat: $(f(x_1), g(b)) = (f(x_2), g(b)) \Rightarrow (f \times g)(x_1, b) = (f \times g)(x_2, b)$ (deoarece $f \times g$ este injectiv) rezultă că $(x_1, b) = (x_2, b) \Rightarrow x_1 = x_2$, deci f este într-adevăr injectiv (injectivitatea lui g se face analog);

surjectivitatea: deoarece $f \times g$ este surjectiv rezultă că pentru orice $(x', y') \in A' \times B'\ \ \exists\ (x, y) \in A \times B : (f \times g)(x, y) = (x', y') \Rightarrow\ \exists\, x \in A : f(x) = x' \wedge\ \exists\, y \in B : g(y) = y'$, deci f şi g sunt surjective.

Exerciţiul 57. a) $\mathbf{1}_A \coprod \mathbf{1}_B : A \coprod B \to A \coprod B,\ \ (\mathbf{1}_A \coprod \mathbf{1}_B)(1, x_1) = (1, \mathbf{1}_A(x_1)) = (1, x_1)\ \forall x_1 \in A$, şi $(\mathbf{1}_A \coprod \mathbf{1}_B)(2, x_2) = (2, \mathbf{1}_B(x_2)) = (2, x_2)\ \forall x_2 \in B$, deci $\mathbf{1}_A \coprod \mathbf{1}_B = \mathbf{1}_{A \coprod B}$;

b) $(f' \coprod g') \circ (f \coprod g), (f' \circ f) \coprod (g' \circ g) : A \coprod B \to A'' \coprod B''$ şi $\forall\ x_1 \in A$:

$$((f' \coprod g') \circ (f \coprod g))(1, x_1) = (f' \coprod g')(1, f(x_1)) = (1, (f' \circ f)(x_1)) = ((f' \circ f) \coprod (g' \circ g))(1, x_1),$$

respectiv analog pentru orice $x_2 \in B$ avem

$$((f' \coprod g') \circ (f \coprod g))(2, x_2) = ((f' \circ f) \coprod (g' \circ g))(2, x_2),$$

deci $(f' \coprod g') \circ (f \coprod g) = (f' \circ f) \coprod (g' \circ g)$.

Exerciţiul 58. a) Trebuie să arătăm că $(\coprod_{i\in I} f_i) \circ q_i = q_i' \circ f_i,\ \forall\ i \in I$; într-adevăr, pentru orice $i \in I$ avem $(\coprod_{i\in I} f_i) \circ q_i : A_i \to \coprod_{i\in I} A_i',\ q_i' \circ f_i : A_i \to \coprod_{i\in I} A_i'$ şi pentru orice $a_i \in A_i$ avem:

$$((\coprod_{i\in I} f_i) \circ q_i)(a_i) = (\coprod_{i\in I} f_i)(q_i(a_i)) = (\coprod_{i\in I} f_i)(i, a_i) = (i, f_i(a_i)) = q_i'(f_i(a_i)) = (q_i' \circ f_i)(a_i).$$

b) Avem $\coprod_{i\in I} \mathbf{1}_{A_i} : \coprod_{i\in I} A_i \to \coprod_{i\in I} A_i,\ \ (\coprod_{i\in I} \mathbf{1}_{A_i})(i, a_i) = (i, \mathbf{1}_{A_i}(a_i)) = (i, a_i)$, deci $\coprod_{i\in I} \mathbf{1}_{A_i} = \mathbf{1}_{\coprod_{i\in I} A_i}$;

c) Avem $(\coprod_{i\in I} f_i') \circ (\coprod_{i\in I} f_i) : \coprod_{i\in I} A_i \to \coprod_{i\in I} A_i''$, $\coprod_{i\in I}(f_i' \circ f_i) : \coprod_{i\in I} A_i \to \coprod_{i\in I} A_i''$ şi pentru orice $(i, a_i) \in \coprod_{i\in I} A_i$ avem

$$(\coprod_{i\in I} f_i') \circ (\coprod_{i\in I} f_i)(i, a_i) = (\coprod_{i\in I} f_i')(i, f_i(a_i)) = (i, (f_i' \circ f_i)(a_i)) = (\coprod_{i\in I}(f_i' \circ f_i))(i, a_i),$$

deci $(\coprod_{i\in I} f_i') \circ (\coprod_{i\in I} f_i) = \coprod_{i\in I}(f_i' \circ f_i)$.

Exerciţiul 59. b) ştim că o funcţie $f : A \to B$ este injectiv$\Leftrightarrow$ $\exists\, r : B \to A$ funcţie astfel încât $r \circ f = \mathbf{1}_A$; în cazul nostru $\forall\, i \in I : f_i$ este injectiv$\Rightarrow$ $\forall\, i \in I :$ $\exists\, r_i : A_i' \to A_i : r_i \circ f_i = \mathbf{1}_A \Rightarrow (\coprod_{i\in I} r_i) \circ (\coprod_{i\in I} f_i) = \coprod_{i\in I}(r_i \circ f_i) = \coprod_{i\in I} \mathbf{1}_{A_i} = \mathbf{1}_{\coprod_{i\in I} A_i}$, deci există $\coprod_{i\in I} r_i : \coprod_{i\in I} A_i' \to \coprod_{i\in I} A_i$ astfel încât $(\coprod_{i\in I} r_i) \circ (\coprod_{i\in I} f_i) = \mathbf{1}_{\coprod_{i\in I} A_i}$, adică $\coprod_{i\in I} f_i$ este injectiv.

Analog demonstrăm surjectivitatea lui $\coprod_{i\in I} f_i$.

Exerciţiul 60. a) Avem $\mathrm{Hom}(f, g) : \mathrm{Hom}(A, B) \to \mathrm{Hom}(A', B')$ $\mathrm{Hom}(f, g)(\alpha) = g\circ\alpha\circ f$, şi $|\mathrm{Hom}(A, B)| = \left|B^A\right| = |B|^{|A|} = 2^2 = 4$, deci $\mathrm{Hom}(A, B) = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$, unde: $\alpha_1(1) = 1, \alpha_1(2) = 1, \alpha_2(1) = 1, \alpha_2(2) = 2, \alpha_3(1) = 2, \alpha_3(2) = 1, \alpha_4(1) = 2, \alpha_4(2) = 2$; notăm $\beta_k := \mathrm{Hom}(f, g)(\alpha_k), k = 1, 2, 3, 4$; atunci $\beta_1(1) = 2, \beta_1(2) = 2, \beta_1(3) = 2, \beta_2(1) = 2,\ \beta_2(2) = 2, \beta_2(3) = 3,\ \beta_3(1) = 3, \beta_3(2) = 3, \beta_3(3) = 2, \beta_4(1) = 3, \beta_4(2) = 3, \beta_4(3) = 3.$

b) $\mathrm{Hom}(\mathbf{1}_A, \mathbf{1}_B) : \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, B)$, $\mathrm{Hom}(\mathbf{1}_A, \mathbf{1}_B)(\alpha) = \mathbf{1}_B \circ \alpha \circ \mathbf{1}_A = \alpha$, deci $\mathrm{Hom}(\mathbf{1}_A, \mathbf{1}_B) = \mathbf{1}_{\mathrm{Hom}(A,B)}$.

c) $\mathrm{Hom}(f \circ f', g' \circ g), \mathrm{Hom}(f', g') \circ \mathrm{Hom}(f, g) : \mathrm{Hom}(A, B) \to \mathrm{Hom}(A'', B'')$, şi pentru orice $\alpha \in \mathrm{Hom}(A, B)$ avem:

$$\begin{aligned}\mathrm{Hom}(f \circ f', g' \circ g)(\alpha) &= g' \circ g \circ \alpha \circ f \circ f' = g' \circ (g \circ \alpha \circ f) \circ f' = g' \circ \mathrm{Hom}(f, g)(\alpha) \circ f' = \\ &= \mathrm{Hom}(f', g')(\mathrm{Hom}(f, g)(\alpha)) = (\mathrm{Hom}(f', g') \circ \mathrm{Hom}(f, g))(\alpha)\end{aligned}$$

deci $\mathrm{Hom}(f \circ f', g' \circ g) = \mathrm{Hom}(f', g') \circ \mathrm{Hom}(f, g)$.

Exerciţiul 61. a) Dacă f este surjectiv şi g este injectiv, atunci $\exists\, s : A \to A'$ astfel încât $f\circ s = \mathbf{1}_A$ şi $\exists\, r : B' \to B$ astfel încât $r \circ g = \mathbf{1}_B$; rezultă că $\mathrm{Hom}(s, r) \circ \mathrm{Hom}(f, g) = \mathrm{Hom}(f \circ s, r \circ g) = \mathrm{Hom}(\mathbf{1}_A, \mathbf{1}_B) = \mathbf{1}_{\mathrm{Hom}(A,B)}$, deci există $\mathrm{Hom}(s, r) : \mathrm{Hom}(A', B') \to \mathrm{Hom}(A, B)$ astfel încât $\mathrm{Hom}(s, r) \circ \mathrm{Hom}(f, g) = \mathbf{1}_{\mathrm{Hom}(A,B)}$, deci $\mathrm{Hom}(f, g)$ este injectiv;

b) este analog cu a);

c) „$\Rightarrow$" deoarece $\mathbf{1}_A$ este surjectiv şi g este injectiv, din a) rezultă că $\mathrm{Hom}(\mathbf{1}_A, g)$ este injectiv;

„$\Leftarrow$" deoarece $\mathrm{Hom}(\mathbf{1}_A, g)$ este injectiv, rezultă că pentru orice $\alpha_1, \alpha_2 \in \mathrm{Hom}(A, B)$ avem $g \circ \alpha_1 = g \circ \alpha_2 \Rightarrow \alpha_1 = \alpha_2$, adică putem simplifica cu $g$la stânga$\Longrightarrow$ g este injectiv;

d) este analog cu c).

Exerciţiul 62. a) Deoarece $\mathbf{1}_{A*} : \mathcal{P}(A) \to \mathcal{P}(A)$, $\mathbf{1}_{A*}(X) = \mathbf{1}_A(X) = X$ pentru orice $X \in \mathcal{P}(A)$, şi $\mathbf{1}_A{}^* : \mathcal{P}(A) \to \mathcal{P}(A)$, $\mathbf{1}_A{}^*(Y) = \mathbf{1}_A(Y) = Y$, rezultă că $\mathbf{1}_{A*} = \mathbf{1}_A{}^* = \mathbf{1}_{\mathcal{P}}(A)$;

b) Pentru orice $X \subseteq A$ avem

$$(g \circ f)_*(X) = (g \circ f)(X) = g(f(X)) = g(f_*(X)) = g_*(f_*(X)) = (g_* \circ f_*)(X),$$

deci $(g \circ f)_* = g_* \circ f_*$.

Pentru orice $Z \in C$ avem

$$(g \circ f)^*(Z) = (g \circ f)^{-1}(Z) = (f^{-1} \circ g^{-1})(Z) = f^{-1}(g^{-1}(Z)) = f^{-1}(g^*(Z)) = f^*(g^*(Z)) = (f^* \circ g^*)(Z),$$

deci $(g \circ f)^* = f^* \circ g^*$.

c) Pentru orice $Y \subseteq B$ avem

$$(f^* \circ f_* \circ f^*)(Y) = f^{-1}(f(f^{-1}(Y))) = f^{-1}((f \circ f^{-1})(Y)) = (f^{-1} \circ f)(f^{-1}(Y))$$

şi, deoarece $f : A \to B$ este funcţie, dintr-un exerciţiu anterior rezultă că $\mathbf{1}_A \subseteq f^{-1} \circ f$ şi $f \circ f^{-1} \subseteq \mathbf{1}_B$; obţinem că pentru orice $Y \subseteq B$ avem $f^{-1}(Y) \subseteq (f^{-1}\circ f)(f^{-1}(Y)) = (f^*\circ f_*\circ f^*)(Y)$ şi $(f^*\circ f_*\circ f^*)(Y) = f^{-1}((f\circ f^{-1})(Y)) \subseteq f^{-1}(Y)$, deci $(f^* \circ f_* \circ f^*)(Y) = f^{-1}(Y) = f^*(Y) \Rightarrow f^* \circ f_* \circ f^* = f^*$.

d) $\varphi\circ\varphi = (f^*\circ f_*)\circ(f^*\circ f_*) = (f^*\circ f_*\circ f^*)\circ f_* = f^*\circ f_* = \varphi$; $\psi\circ\psi = (f_*\circ f^*)\circ(f_*\circ f^*) = f_*\circ(f^*\circ f_*\circ f^*) = f_*\circ f^* = \psi$.

Exerciţiul 63. a) (i)$\Rightarrow$(ii) deoarece f este injectiv, există $r : B \to A$ astfel încât $r \circ f = \mathbf{1}_A$; atunci $r_* \circ f_* = (r \circ f)_* = \mathbf{1}_{A*} = \mathbf{1}_{\mathcal{P}(A)}$, deci există $r_* : \mathcal{P}(B) \to \mathcal{P}(A)$ astfel încât $r_* \circ f_* = \mathbf{1}_{\mathcal{P}(A)}$, deci f_* este injectiv;

(ii)$\Rightarrow$(iii) deoarece f este funcţie, avem $\mathbf{1}_A \subseteq f^{-1} \circ f$, deci pentru orice $X \subseteq A$ avem $X \subseteq (f^{-1} \circ f)(X) = f^{-1}(f(X)) = f^*(f_*(X)) = (f^* \circ f_*)(X)$; fie $X \subseteq A$; atunci pentru orice $x \in A$ avem

$$\begin{aligned}x \in (f^* \circ f_*)(X) = f^{-1}(f(X)) &\Rightarrow f(x) \in f(X) \Rightarrow \\ &\Rightarrow \exists\, x' \in X :\ f(x) = f(x') \Rightarrow \\ &\Rightarrow f_*(\{x\}) = f_*(\{x'\}) \Rightarrow \{x\} = \{x'\} \Rightarrow \\ &\Rightarrow x = x' \Rightarrow x \in X,\end{aligned}$$

deci pentru orice $X \subseteq A$ avem $(f^* \circ f_*)(X) \subseteq X$.

(iii)⇒(i) deoarece $f^* \circ f_* = \mathbf{1}_{\mathcal{P}(A)}$, există $r := f^* : \mathcal{P}(B) \to \mathcal{P}(A)$ astfel încât $r \circ f_* = \mathbf{1}_A$, deci f_* este injectiv, deci pentru orice $x, x' \in A$, din $\{f(x)\} = f_*(\{x\}) = f_*(\{x'\}) = \{f(x')\}$ rezultă $x = x'$, de unde obţinem că f este injectiv;

(iii)⇒(iv) din ipoteză avem că există $s := f_* : \mathcal{P}(A) \to \mathcal{P}(B)$ astfel încât $f^* \circ s = \mathbf{1}_{\mathcal{P}(A)}$, deci f^* este surjectiv;

(iv)⇒(iii) $f^* \circ f_* \circ f^* = f^*$ şi din surjectivitatea lui f^* $\exists\ s : \mathcal{P}(A) \to \mathcal{P}(B)$ astfel încât $f^* \circ s = \mathbf{1}_{\mathcal{P}(A)}$; atunci rezultă că $f^* \circ f_* \circ f^* \circ s = f^* \circ s \Rightarrow f^* \circ f_* = \mathbf{1}_{\mathcal{P}(A)}$.

b) este analog cu a).

Exerciţiul 67. a) Deoarece ρ reflexiv$\Rightarrow \mathbf{1}_A \subseteq \rho$; este trebuie demonstrată incluziunea $\rho \subseteq \mathbf{1}_A$: dacă $x\rho y$ (din simetrie)$\Rightarrow x\rho y \wedge y\rho x$ (din antisimetrie)$\Rightarrow x = y$ adică $x\mathbf{1}_A y$;

b) dacă $x\rho y$ (adin reflexivitate)$\Rightarrow x\rho y \wedge y\rho y \Rightarrow x\rho^2 y$, deci $\rho \subseteq \rho^2$; invers, dacă $x\rho^2 y \Rightarrow\ \exists\ z \in A : x\rho z \wedge z\rho y$ (din tranzitivitate)$\Rightarrow x\rho y$, deci $\rho^2 \subseteq \rho$.

Exerciţiul 68. a) $\pi_\rho = \{\{1,2,3\},\{4\}\}$; b) $\rho_\pi = \{(1,1),\ (2,2),\ (3,3),\ (4,4),\ (1,2),\ (2,1)\}$.

Exerciţiul 69. Întâi determinăm toate partiţiile, apoi scriem relaţiile de echivalenţă corespunzătoare. De exemplu pentru $A = \{1,2,3\}$ partiţiile sunt: $\pi_1 = \{\{1,2,3\}\}$, $\pi_2 = \{\{1,2\},\{3\}\}$, $\pi_3 = \{\{1,3\},\{2\}\}$, $\pi_4 = \{\{2,3\},\ \{1\}\}$ şi $\pi_5 = \{\{1\},\{2\},\{3\}\}$. Acestora corespund relaţiile de echivalenţă $\rho_1 = \{(1,1),\ (2,2),\ (3,3),\ (1,2),\ (2,1),\ (1,3),\ (3,1),\ (2,3),\ (3,2)\}$, $\rho_2 = \{(1,1),\ (2,2),\ (3,3),\ (1,2),\ (2,1)\}$, $\rho_3 = \{(1,1),(2,2),(3,3),(1,3),(3,1)\}$, $\rho_4 = \{(1,1),(2,2),(3,3),\ (2,3),\ (3,2)\}$ şi $\rho_2 = \{(1,1),(2,2),(3,3)\}$.

Exerciţiul 70. a) „|” nu e simetric, deoarece de exemplu $2|4$, dar invers nu e adevărat; „|” nu e antisimetric, deoarece de exemplu $2|-2$, $-2|2$, dar $2 \neq -2$;

c) $\mathbb{Z}/_{\equiv\ (\mathrm{mod}\ n)} = \mathbb{Z}_n = \{\hat{a} \mid a \in \mathbb{Z}\}$, unde $\hat{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\} = n\mathbb{Z} + a$.

Exerciţiul 71. $\mathbb{C}/\rho_1 = \{\mathbb{C}(0,|z|) \mid z \in \mathbb{C}\}$, deci clasele se reprezintă grafic în planul complex ca cercuri cu centrul în orgine; clasele din $\mathbb{C}/\rho_2$ sunt semidrepte deschise ce pornesc din originea O.

Exerciţiul 72. b) Deoarece $\mathbf{1}_A \subseteq \rho_1$, rezultă că $\mathbf{1}_A \cap \complement\rho_1 = \varnothing$, deci $\complement\rho_1$ nu e reflexiv, deci $\complement\rho_1$ nu e relaţie de echivalenţă; $\rho_1 \cup \rho_2$ în general nu e tranzitiv. De exemplu, dacă $A = \{1,2,3\}$, $\rho_1 = \{(1,1),(2,2),(3,3),(1,2),(2,1)\}$ şi $\rho_2 = \{(1,1),(2,2),(3,3),(1,3),(3,1)\}$ sunt două relaţii de echivalenţă pe A, atunci relaţia $\rho_1 \cup \rho_2 = \{(1,1),(2,2),(3,3),(1,2),\ (2,1),(1,3),(3,1)\}$ nu e tranzitivă, deoarece nu conţine perechile $(2,3)$ şi $(3,2)$;

c) imediat se vede că pentr relaţia ρ pe A avem: ρ este echivalenţă $\Longleftrightarrow \mathbf{1}_A \subseteq \rho$ şi $\rho = \rho^{-1} = \rho^2$. De aici demonstrăm uşor c):

„⇒” dacă $\rho_1 \circ \rho_2$ echivalenţă, atunci$\Rightarrow \rho_1 \circ \rho_2 = (\rho_1 \circ \rho_2)^{-1} = \rho_2^{-1} \circ \rho_1^{-1} = \rho_2 \circ \rho_1$;

„⇐” folosind $\rho_1 \circ \rho_2 = \rho_2 \circ \rho_1$ arătăm că: (1) $\mathbf{1}_A \subseteq \rho_1 \circ \rho_2$ şi (2) $\rho_1 \circ \rho_2 = (\rho_1 \circ \rho_2)^{-1} = (\rho_1 \circ \rho_2)^2$;

(1) deoarece $\mathbf{1}_A \subseteq \rho_1 \wedge \mathbf{1}_A \subseteq \rho_2 \Rightarrow \mathbf{1}_A = \mathbf{1}_A \circ \mathbf{1}_A \subseteq \rho_1 \circ \rho_2$;

(2) $(\rho_1 \circ \rho_2)^{-1} = \rho_2^{-1} \circ \rho_1^{-1} = \rho_2 \circ \rho_1 = \rho_1 \circ \rho_2$ şi $(\rho_1 \circ \rho_2)^2 = (\rho_1 \circ \rho_2) \circ (\rho_1 \circ \rho_2) = \rho_1 \circ (\rho_2 \circ \rho_1) \circ \rho_2 = \rho_1 \circ (\rho_1 \circ \rho_2) \circ \rho_2 = \rho_1^2 \circ \rho_2^2 = \rho_1 \circ \rho_2$.

Exerciţiul 73. b) „⇒” dacă $\rho_1 \cup \rho_2$ echivalenţă, atunci

$$\rho_1 \cup \rho_2 = (\rho_1 \cup \rho_2)^2 = \rho_1^2 \cup \rho_2^2 \cup (\rho_1 \circ \rho_2) \cup (\rho_2 \circ \rho_1)$$

deci $\rho_1 \circ \rho_2$ şi $\rho_2 \circ \rho_1$ este subrelaţie a lui $\rho_1 \cup \rho_2$;

„⇐” deoarece ρ_1 şi ρ_2 sunt relaţii de echivalenţă rezultă că $\rho_1 \cup \rho_2$ reflexiv şi simetric; deoarece $\rho_1 \circ \rho_2$, $\rho_2 \circ \rho_1$ şi $\rho_1^2 \cup \rho_2^2 = \rho_1 \circ \rho_2$ sunt subrelaţii ale lui $\rho_1 \cup \rho_2$, rezultă că $(\rho_1 \cup \rho_2)^2 = \rho_1^2 \cup \rho_2^2 \cup (\rho_1 \circ \rho_2) \cup (\rho_2 \circ \rho_1) \subseteq \rho_1 \cup \rho_2 \Rightarrow \rho_1 \cup \rho_2$ este tranzitiv.

Exerciţiul 74. a) Demonstrăm că $\bigcup_{n \geq 1} \rho^n$ este tranzitivă: pentru orice $x, y, z \in A$ avem $x \bigcup_{n \geq 1} \rho^n y \wedge y \bigcup_{n \geq 1} \rho^n z \Rightarrow\ \exists\ m, n \in \mathbb{N}^* : x\rho^m y \wedge y\rho^n z \Rightarrow x\rho^n \circ \rho^m z \Rightarrow x\rho^{n+m} z \Rightarrow \Rightarrow x \bigcup_{n \geq 1} \rho^n z$.

Fie acum σ o relaţie ce include pe ρ. Deoarece $\rho \subseteq \sigma \Rightarrow \rho^2 \subseteq \sigma^2$, dar σ tranzitiv$\Rightarrow \sigma^2 \subseteq \sigma$. Deci $\rho^2 \subseteq \sigma$ şi deoarece $\rho \subseteq \sigma$ respectiv $\sigma^2 \subseteq \sigma \Rightarrow \rho^3 \subseteq \sigma$. Prin inducţie se arată că $\forall\ n \in \mathbb{N}^*$ avem $\rho^n \subseteq \sigma$, de aici evident rezultă că $\bigcup_{n \geq 1} \rho^n \subseteq \sigma$. Deci într-adevăr, $\bigcup_{n \geq 1} \rho^n$ este cea mai mică relaţie tranzitivă ce include pe ρ.

b) Arătăm că relaţia $\bigcup_{n \geq 1} \bar{\rho}^n$ este echivalenţă. Verificăm următoarele:

1) $\mathbf{1}_A \subseteq \bigcup_{n \geq 1} \bar{\rho}^n$ (evident);

2) $\bigcup_{n \geq 1} \bar{\rho}^n = \left(\bigcup_{n \geq 1} \bar{\rho}^n\right)^{-1} = \left(\bigcup_{n \geq 1} \bar{\rho}^n\right)^2$.

Într-adevăr, $\left(\bigcup_{n \geq 1} \bar{\rho}^n\right)^{-1} = \left(\bigcup_{n \in \mathbb{Z}} \rho^n\right)^{-1} = \bigcup_{n \in \mathbb{Z}} \rho^{-n} = \bigcup_{n \in \mathbb{Z}} \rho^n = \bigcup_{n \geq 1} \bar{\rho}^n$ şi $\left(\bigcup_{n \geq 1} \bar{\rho}^n\right)^2 = \left(\bigcup_{n \in \mathbb{Z}} \rho^n\right)^2 = \left(\bigcup_{n \in \mathbb{Z}} \rho^n\right)$.

Fie acum σ o relaţie de echivalenţă ce include pe ρ. Deoarece σ este relaţie de echivalenţă $\Rightarrow \sigma$ este tranzitiv. Din a) rezultă că $\bigcup_{n \geq 1} \rho^n \subseteq \sigma$ (deoarece $\bigcup_{n \geq 1} \rho^n$ este cea mai mică relaţie de echivalenţă ce include pe ρ. Deoarece $\rho \subseteq \sigma$ şi σ relaţie de echivalenţă $\Rightarrow \rho^{-1} \subseteq \sigma^{-1} = \sigma \Rightarrow \sigma$ tranzitiv şi conţine pe $\rho^{-1} \Rightarrow \bigcup_{n \geq 1} (\rho^{-1})^n \subseteq$

σ. Deci: $\bigcup_{n\geq 1}\rho^n \subseteq \sigma$ şi $\bigcup_{n\geq 1}(\rho^{-1})^n \subseteq \sigma$, de evident $\mathbf{1}_A \subseteq \sigma$(deoarece σ reflexiv); din acestea rezultă că $\bigcup_{n\geq 1}\bar{\rho}^n \subseteq \sigma$, ceea ce arată că într-adevăr $\bigcup_{n\geq 1}\bar{\rho}^n$ este cea mai mică relaţie de echivalenţă ce include pe ρ.

Exerciţiul 75. 1) Este uşor de arătat că $\ker f$ este reflexiv, simetric şi tranzitiv, pentru că şi relaţia „=" este aşa. Mai departe,

$$\begin{aligned} a_1 \ker f a_2 &\Leftrightarrow \exists b \in B : f(a_1) = f(a_2) = b \Leftrightarrow \\ &\Leftrightarrow \exists b \in B : a_1 f b \text{ şi } a_2 f b \Leftrightarrow \\ &\Leftrightarrow \exists b \in B : a_1 f b \text{ şi } b f^{-1} a_2 \Leftrightarrow a_1 (f^{-1} \circ f) a_2. \end{aligned}$$

2) Avem $f^{-1}(b) = \{a' \in A \mid f(a') = b\}$ şi $A/\ker f = \{\ker f\langle a\rangle \mid a \in A\}$, unde $\ker f\langle a\rangle = \{a' \in A \mid f(a') = f(a)\} = f^{-1}(f(a))$. Deoarece $f(a) \in \operatorname{Im} f$, rezultă că $A/\ker f \subseteq \{f^{-1}(b) \mid b \in \operatorname{Im} f\}$.

Invers, pentru orice $b \in \operatorname{Im} f$, există $a \in A$ astfel încât $b = f(a)$, deci $f^{-1}(b) = f^{-1}(f(a)) = \{a' \in A \mid f(a') = f(a)\} = \ker f\langle a\rangle \in A/\ker f$.

3) Dacă $f : A \to B$ este o funcţie, atunci $\mathbf{1}_A \subseteq \ker f$, pentru că $\ker f$ este reflexiv. Mai departe,

$$\begin{aligned} \ker f \subseteq \mathbf{1}_A &\Leftrightarrow (\forall x_1, x_2 \in A : x_1 \ker f x_2 \Rightarrow x_1 \mathbf{1}_A x_2) \Leftrightarrow \\ &\Leftrightarrow (\forall x_1, x_2 \in A : f(x_1) = f(x_2) \Rightarrow x_1 = x_2) \Leftrightarrow \\ &\Leftrightarrow f \text{ injectiv}. \end{aligned}$$

4) Rezultă uşor din definiţii.

Exerciţiul 76. Surjectivitatea rezultă din definiţii: $\forall \rho\langle x\rangle \in A/\rho$, unde $x \in A \Rightarrow p_\rho(x) = \rho\langle x\rangle$. Mai departe, dacă $x_1, x_2 \in A$, atunci

$$x_1 \ker p_\rho x_2 \Leftrightarrow p_\rho(x_1) = p_\rho(x_2) \Leftrightarrow \rho\langle x_1\rangle = \rho\langle x_2\rangle \Leftrightarrow x_1 \rho x_2.$$

conform Lemei 4.4.6.

Exerciţiul 77. a) Deoarece g este surjectiv şi $x_1^2 = x_2^2 \Rightarrow \cos x_1 = \cos x_2$, adică $\ker g \subseteq \ker f$, rezultă că $(\exists!)h : \mathbb{R}_+ \to \mathbb{R}$ o funcţie astfel încât $f = h \circ g$. Determinăm această funcţie. Fie $s : \mathbb{R}_+ \to \mathbb{R}$, $s(x) = \sqrt{x}$ funcţie o inversă la dreapta a lui g. Atunci, deoarece $f = h \circ g \Rightarrow f \circ s = (h \circ g) \circ s = h \circ (g \circ s) = h$, deci $h : \mathbb{R}_+ \to \mathbb{R}$, $h(x) = (f \circ s)(x) = \cos(\sqrt{x})$.

b) Vedem că g este surjectiv, dar $\ker g \not\subseteq \ker f \Longrightarrow$ în acest caz nu există o funcţie h ce satisface cerinţele.

Exerciţiul 78. a) Deoarece g este injectiv şi $[-1, 1] = \operatorname{Im} f \subseteq \operatorname{Im} g = [-3, +\infty)$, rezultă ą $(\exists!)h : \mathbb{R} \to [-2, \infty)$ funcţie astfel încât $f = g \circ h$. Determinăm această funcţie. Fie

$$r : \mathbb{R} \to [-2, +\infty), \quad r(x) = \begin{cases} \frac{x-1}{2}, & x \in [-3, +\infty) \\ x_0 \in [-2, +\infty), & x \notin [-3, +\infty) \end{cases}$$

o inversă la stânga a lui g. Atunci, deoarece $f = g \circ h$, rezultă că $r \circ f = r \circ (g \circ h) = (r \circ g) \circ h = h$, deci a $h : \mathbb{R} \to [-2, +\infty)$, $h(x) = (r \circ f)(x) = \frac{\cos x - 1}{2}$.

b) Vedem ą g este injectiv, dar $[-1, 1] = \operatorname{Im} f \not\subseteq \operatorname{Im} g = [1, +\infty) \Longrightarrow$ în acest caz nu există o funcţie h ce satisface cerinţele.

Exerciţiul 79. a) Dacă $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$: $\ker f\langle x\rangle = \{x, -x\}$, $\mathbb{R}/\ker f = \{\{x, -x\} \mid x \in \mathbb{R}\}$, şi $\bar{f} : \mathbb{R}/\ker f \to \mathbb{R}_+$ $\bar{f}(\{x, -x\}) = x^2$ este bijectiv.

Dacă $g : \mathbb{R} \to \mathbb{R}$, $g(x) = x^4$: $\ker g\langle x\rangle = \{x, -x\}$, $\mathbb{R}/\ker g = \{\{x, -x\} \mid x \in \mathbb{R}\}$, şi $\bar{g} : \mathbb{R}/\ker g \to \mathbb{R}_+$ $\bar{g}(\{x, -x\}) = x^4$ este bijectiv.

b) Dacă $f : \mathbb{C} \to \mathbb{C}$, $f(z) = z^2$: $\ker f\langle z\rangle = \{z, -z\}$, $\mathbb{C}/\ker f = \{\{z, -z\} \mid z \in \mathbb{C}\}$, şi $\bar{f} : \mathbb{C}/\ker f \to \mathbb{C}$, $\bar{f}(\{z, -z\}) = z^2$ este bijectiv.

Dacă $g : \mathbb{C} \to \mathbb{C}$, $g(z) = z^4$, atunci $(\ker g)\langle z\rangle = \{z, -z, iz, -iz\}$, mai departe $\mathbb{C}/\ker g = \{\{z, -z, iz, -iz\} \mid x \in \mathbb{C}\}$, şi $\bar{g} : \mathbb{C}/\ker g \to \mathbb{C}$, $\bar{g}(\{z, -z, iz, -iz\}) = z^4$ este bijectiv.

Exerciţiul 80. a) Fie $\varphi : A \times B/\rho \times \sigma \to A/\rho \times B/\sigma$, $\varphi(\rho \times \sigma\langle(a, b)\rangle) = (\rho\langle a\rangle, \sigma\langle b\rangle)$. Această funcţie este evident bine definită şi bijectivă, deoarece se verifică imediat că $\varphi^{-1} : A/\rho \times B/\sigma \to A \times B/\rho \times \sigma$, $\varphi^{-1}(\rho\langle a\rangle, \sigma\langle b\rangle) = \rho \times \sigma\langle(a, b)\rangle$ este inversa lui φ.

Exerciţiul 81. Fie $\varphi : \mathcal{P}(A)/\rho \to \mathcal{P}(B)$, $\varphi(\rho\langle X\rangle) = X \cap B$. Această funcţie este evident bine definită şi bijectivă; se verifică imediat că are inversa $\varphi^{-1} : \mathcal{P}(B) \to \mathcal{P}(A)/\rho$, $\varphi^{-1}(Y) = \rho\langle Y\rangle$.

Exerciţiul 82. a) Fie $\varphi : \operatorname{Hom}(A, B)/\rho \to B$, $\varphi(\rho\langle f\rangle) = f(a_0)$. Această funcţie este evident bine definită şi bijectivă; se verifică imediat că are inversa $\varphi^{-1} : B \to \operatorname{Hom}(A, B)/\rho$, $\varphi^{-1}(b) = \rho\langle f_b\rangle$, unde $f_b \in \operatorname{Hom}(A, B)$, $f_b(a) = b \;\; \forall\, a \in A$.

b) Fie $\psi : \mathrm{Hom}(A,B)/\sigma \to \mathrm{Hom}(A',B)$, $\psi(\rho\langle f\rangle) = f|_{A'}$. Această funcţie este evident bine definită şi bijectivă; se verifică imediat că are inversa $\varphi^{-1} : \mathrm{Hom}(A',B) \to \mathrm{Hom}(A,B)/\sigma$, $\varphi^{-1}(f') = \rho\langle f\rangle$, unde $f \in \mathrm{Hom}(A,B)$, $f(a) = f'(a)\ \ \forall\ a \in A'$ şi $f(a) = b_0 \in B$ (fixat) $\forall\ a \in A \setminus A'$.

c) Dacă în b) luăm $A' = \{a_0\}$, atunci o funcţie $f : \{a_0\} \to B$ este determinată B de elementul $f(a_0) \in B$; deci $\mathrm{Hom}(A',B)$ se identifică cu B.

Exerciţiul 83. a) „$\Rightarrow$” $f \ker \varphi g \Rightarrow \varphi(f) = \ker f = \ker g = \varphi(g)$. Deoarece $\ker f = \ker g$, f şi g sunt surjectiv, din Teoremă 4.5.3 rezultă că există funcţia $\alpha : B \to B$, $g = \alpha \circ f$, care este surjectivă (deoarece f este surjectiv) şi este injectiv (deoarece $\ker f = \ker g$);

„$\Leftarrow$” este suficient de arătat că $\ker f = \ker g$. Într-adevăr, pentru orice $x_1, x_2 \in A$ avem $x_1 \ker f x_2 \Leftrightarrow f(x_1) = f(x_2) \Leftrightarrow g(x_1) = \alpha \circ f(x_1) = \alpha \circ f(x_2) = g(x_2)$ (deoarece $\alpha : B \to B$, $g = \alpha \circ f$ este bijectiv)$\Leftrightarrow x_1 \ker g x_2$.

b) $\mathrm{Im}\,\varphi \subseteq \{\rho \in \mathcal{E}(A) \mid\ \exists\ \alpha : A/\rho \to B$ bijectiv$\}$, deoarece $\forall\ f \in \mathrm{Hom}_s(A,B)$ avem $\varphi(f) = \ker f \in \mathcal{E}(A)$ şi

$$\alpha : A/\ker f \to B,\ \ \alpha(\ker f\langle x\rangle) = f(x)$$

este funcţie bijectivă.

$\{\rho \in \mathcal{E}(A) \mid\ \exists\ \alpha : A/\rho \to B$ bijectiv $\} \subseteq \mathrm{Im}\,\varphi$, deoarece pentru $\rho \in \mathcal{E}(A)$ din mulţimea de mai sus, există $f = \alpha \circ p_\rho \in \mathrm{Hom}_s(A,B)$ astfel încât $\ker f = \rho$, unde $p_\rho : A \to A/\rho$, $p_\rho(x) = \rho\langle x\rangle$.

Exerciţiul 84. Fie $\sigma = \rho \cap B \times B$, $\tau = \rho \cap (\rho(B) \times \rho(B))$, unde $\rho(B) = \{z \in \mathbb{C} \mid |z| > 1\}$. Dacă $x \in B$, atunci $\sigma\langle x\rangle = \{x, -x\}$; dacă $z \in \rho(B)$, atunci $\tau\langle z\rangle = \mathbb{C}(O, |z|)$.

Exerciţiul 85. a) $A/\rho_1 = \{\{1,2\},\{3\},\{4\},\{5\}\}$, $\ker h = \{(\{1,2\},\{1,2\}),\ (\{1,2\},\{3\}),\ (\{3\},\{1,2\}),\ (\{3\},\{3\}),\ (\{4\},\{4\}),\ (\{4\},\{5\}),\ (\{5\},\{4\}),\ (\{5\},\{5\})\}$, $\frac{A/\rho_1}{\ker h} = \{\{\{1,2\},\{3\}\},\{\{4\},\{5\}\}\}$, $A/\rho_2 = \{\{1,2,3\},\{4,5\}$. între ultimele două mulţimi există o bijecţie canonică.

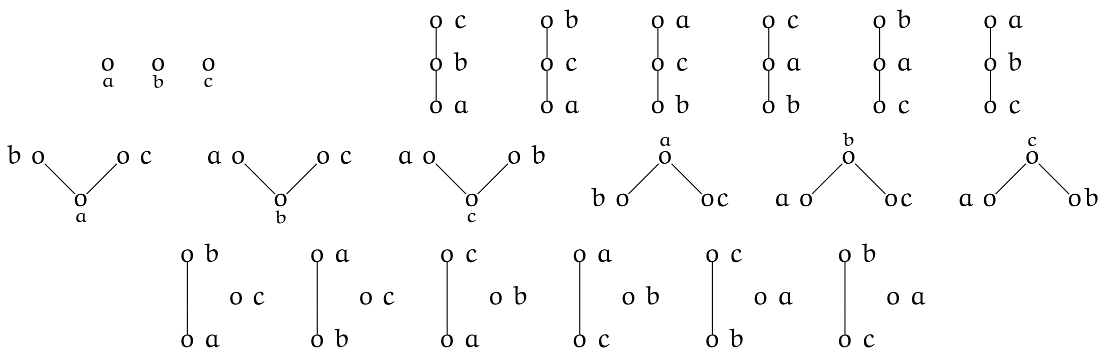
b) $A/\rho_1 = \mathbb{Z}_4 = \{\bar{0},\bar{1},\bar{2},\bar{3}\}$, $\ker h = \{(\bar{0},\bar{0}),\ (\bar{0},\bar{2}),\ (\bar{2},\bar{2}),\ (\bar{1},\bar{1}),\ (\bar{1},\bar{3}),\ (\bar{3},\bar{3})\}$, $\frac{A/\rho_1}{\ker h} = \{\{\bar{0},\bar{2}\},\{\bar{1},\bar{3}\}\}$, $A/\rho_2 = \{\hat{0},\hat{1}\}$. între ultimele două mulţimi există o bijecţie canonică.

5. Mulţimi ordonate

Exerciţiul 86. b) Se vede imediat că relaţia $\complement\rho$ nu e reflexivă (deoarece ρ este reflexivă);

c) fie $A = \{1,2,3\}$, $\rho = \{(1,1),(2,2),(3,3),(1,2)\}$, $\sigma = \{(1,1),(2,2),(3,3),(3,1)\}$; evident $\rho \cup \sigma \notin \mathcal{O}(A)$, deoarece această relaţie nu este tranzitivă (căci $(3,2) \notin \rho \cup \sigma$).

Exerciţiul 88. Relaţiile de ordine pe $A = \{a,b,c\}$ sunt cele reprezentate de următoarele diagrame Hasse (prima este relaţia de egalitate pe A):



Exerciţiul 89. a) Dacă f şi g sunt crescătoare, atunci pentru orice $a, a' \in A$ avem $a \le a' \Rightarrow f(a) \le f(a') \Rightarrow g(f(a)) \le g(f(a')) \Rightarrow g \circ f(a) \le g \circ f(a')$, deci $g \circ f$ este crescător; dacă f şi g sunt descrescătoare, atunci pentru orice $a, a' \in A$ avem $a \le a' \Rightarrow f(a') \le f(a) \Rightarrow g(f(a)) \le g(f(a')) \Rightarrow (g \circ f)(a) \le (g \circ f)(a')$, deci $g \circ f$ este crescător;

b) vezi punctul anterior.

Exerciţiul 90. Fie $b, b' \in B$ astfel încât $b \le b'$. Deoarece $f : A \to B$ este bijectiv, rezultă $(\exists!) a, a' \in A$ astfel încât $f(a) = b$ şi $f(a') = b'$. Ştiind că $(A, \le)$ este total ordonată, $\Rightarrow a \le a'$ sau $a' \le a$. Dacă presupunem că $a' \le a$, deoarece f crescător, avem $f(a') = b' \le b = f(a)$, de $b \le b' \Rightarrow b = b' \Rightarrow f^{-1}(b) = a = a' = f^{-1}(b')$. Deci $\forall\ b, b' \in B$ astfel încât $b \le b'$, avem $a = f^{-1}(b) \le f^{-1}(b') = a'$, adică f^{-1} este crescător;

$f := 1_{\mathbb{N}} : (\mathbb{N}, |) \to (\mathbb{N}, \le)$ este o funcţie evident bijectivă şi crescătoare. Nu este izomorfism, deoarece f^{-1} nu e crescător. De exemplu $2 \le 3$, dar $f^{-1}(2) = 2 \nmid 3 = f^{-1}(3)$.

Exerciţiul 93. Fie a_1 un element minimal al mulţimii ordonate $(A, \le)$. Atunci pentru orice $x \in A$ avem $x \le a_1 \Rightarrow x = a_1$. Deoarece $a = \min A \Rightarrow\ \forall\ x \in A :\ a \le x \Rightarrow a \le a_1 \Rightarrow a = a_1$, deci într-adevăr există un singur element minimal, care este cel mai mic element.

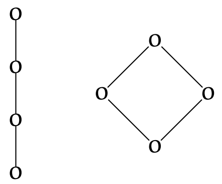
Reciproca în general nu e adevărată: considerăm relaţia de ordine

$$\rho \subseteq \mathbb{R} \times \mathbb{R}, \quad x\rho y \Longleftrightarrow (x \neq 0 \neq y \wedge x \leq y) \vee x = 0 = y.$$

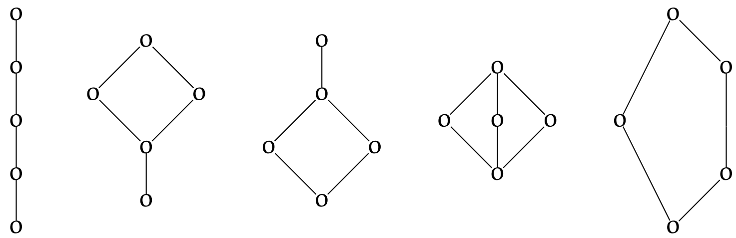
În mulţimea ordonată $(\mathbb{R}, \rho)$, 0 este unicul element minimal (maximal), dar nu există cel mai mic (cel mai mare) element.

Exerciţiul 94. Este suficient de observat că $\inf_B X \in \{a \in A \mid \forall x \in X, \ a \leq x\}$ şi $\sup_B X \in \{a \in A \mid \forall x \in \in X, \ a \geq x\}$.

Exerciţiul 95. Există, abstracţie făcând de izomorfisme, câte o latice cu 1, 2 respectiv 3 elemente şi 16 cu 6 elemente. Laticile neizomorfe cu 4 elemente sunt cele reprezentate de următoarele diagrame Hasse.



Laticile neizomorfe cu 5 elemente sunt cele reprezentate de următoarele diagrame Hasse:



Exerciţiul 97. Considerăm mulţimea $B = \{a \in A \mid a \leq f(a)\}$. Deoarece în orice latice completă există cel mai mare ($\sup_A A$) şi cel mai mic element ($\inf_A A$) vedem că B este submulţime nevidă a lui A, deoarece evident $\inf_A A \in B$. Deoarece $B \subseteq A \Rightarrow \ \exists \ a_0 := \sup_A B$. Arătăm că a_0 este punct fix al lui f.

Deoarece $a_0 = \sup_A B \Rightarrow \ \forall \ a \in B$ avem $a \leq a_0$, dar f este crescător şi $a \leq f(a)$ (deoarece $a \in B$) $\Rightarrow a \leq f(a) \leq f(a_0) \Rightarrow f(a_0)$ este majorantă a lui B. Ştim că a_0 este cea mai mică majorantă a lui B, deci $a_0 \leq f(a_0)$, şi de aici avem că $a_0 = \sup_A B \in B$, adică a_0 este cel mai mare element al lui B. Deoarece f este crescător şi $a_0 \leq f(a_0) \Rightarrow f(a_0) \leq f(f(a_0))$, deci $f(a_0) \in B$, dar a_0 este cel mai mare element al lui B, deci $f(a_0) \leq a_0$. Deducem că $a_0 \in B$, adică $a_0 \leq f(a_0)$, şi $f(a_0) \leq a_0$. De aici rezultă că $a_0 = f(a_0)$, adică a_0 este într-adevăr punct fix al lui f.

Exerciţiul 98. a) Dacă există $a \in A$ astfel ca $a > f(a)$, atunci obţinem un şir strict descrescător infinit $a > f(a) > f(f(a)) > \ldots$, contradicţie.

b) Fie A şi B două mulţimi bine ordonate. Dacă $f, g : A \to B$ sunt două izomorfisme distincte, atunci există $a \in A$ astfel ca $f(a) < g(a)$ sau $g(a) < f(a)$, de unde $g^{-1}(f(a)) < a$ sau $f^{-1}(g(a)) < a$, ceea ce contrazice a).

Exerciţiul 99. a) Fie ρ un element maximal ce aparţine lui $\mathcal{O}(A)$. Arătăm că ρ este ordine totală. Fie $c, d \in A$ astfel încât $c \neq d$. Arătăm că perechea (c, d) sau (d, c) aparţine graficului R al relaţiei ρ. Presupunem că $(c, d), (d, c) \notin R$. Considerăm relaţia

$$\sigma = \rho \cup \{(c, d)\} \cup (\rho^{-1}\langle c\rangle \times \rho\langle d\rangle).$$

Vedem uşor că σ este o relaţie de ordine ce conţine strict pe ρ, ceea ce contrazice maximalitatea lui ρ în mulţimea ordonată $(\mathcal{O}(A), \subseteq)$.

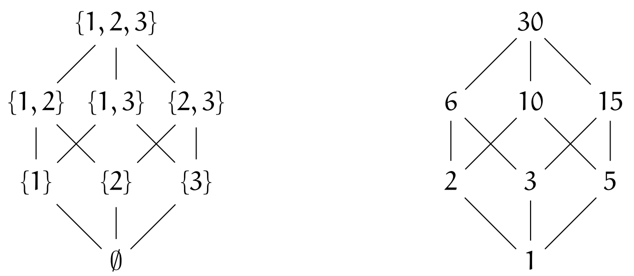
Fie ρ o relaţie de ordonare totală pa A. Aratăm că ρ este element maximal al lui $\mathcal{O}(A)$. Presupunem că $\exists \ \sigma \in \mathcal{O}(A)$ astfel încât $\rho \subset \sigma \Rightarrow \ \exists \ (c, d) \ c \neq d$ în graficul lui σ astfel încât $(c, d) \notin R$ (unde R este graficul lui ρ). Deoarece ρ este ordonare totală şi $(c, d) \notin R \Rightarrow (d, c) \in R$, dar $\rho \subset \sigma \Rightarrow \ (d, c)$ şi (c, d) sunt elemente ale lui σ, rezultă că $=d$ (din antisimmetrie), contradicţie cu ipoteza $c \neq d$.

b) Arătăm întâi că mulţimea ordonată $(\mathcal{O}(A), \subseteq)$ satisface ipotezele lemei lui Zorn. Într-adevăr, pentru orice lanţ $\mathcal{L} = \{\rho_\alpha \in \mathcal{O}(A) \mid \alpha \in \Lambda\} \subseteq \mathcal{O}(A)$ avem că $\bigcup_{\alpha \in \Lambda} \rho_\alpha$ este majorantă a lui $\mathcal{L}$ în $(\mathcal{O}(A), \subseteq)$.

Din lema lui Zorn rezultă că pentru orice $\rho \in \mathcal{O}(A)$ există un element maximal $\bar{\rho}$ în $\mathcal{O}(A)$ astfel încât $\rho \subseteq \bar{\rho}$. Din punctul a) rezultăcă $\bar{\rho}$ este relaţie de ordine totală.

6. Latici şi algebre Boole

Exerciţiul 102. Diagramele Hasse ale laticilor $(\mathcal{P}(A), \subseteq)$şi $(B, |)$ sunt:



Un izomorfism de ordine $f : \mathcal{P}(A) \to B$ păstrează diagramele, adică $f(\{1,2,3\}) = 30$, $f(\{\{1,2\},\{1,3\},\{2,3\}\}) = \{6,10,15\}$, $f(\{\{1\},\{2\},\{3\}\}) = \{2,3,5\}$, $f(\emptyset) = 1$. Avem $\{1,2\} = \{1\}\cup\{2\}$, $\{1,3\} = \{1\}\cup\{3\}$, $\{2,3\} = \{2\}\cup\{3\}$. Rezultă că restricţia lui f la $\{\{1,2\},\{1,3\},\{2,3\}\}$ este determinată de restricţia lui f la $\{\{1\},\{2\},\{3\}\}$; deci există 6 izomorfisme între $(\mathcal{P}(A),\subseteq)$ pe $(B,|)$, determinate de bijecţiile dintre $\{\{1\},\{2\},\{3\}\}$ şi $\{2,3,5\}$.

Exerciţiul 103. a) pentru orice $a, a' \in A$ avem $a \le a' \Rightarrow a = a \wedge a' = \inf\{a,a'\} \Rightarrow f(a) \wedge f(a') = f(a \wedge a') = f(a) \Rightarrow f(a) \le f(a')$, deci într-adevăr f este crescător;

b) Reciproca în general nu e adevărată. Contraexemplu: fie $\rho = (A,B,R)$ $R \subseteq A \times B$ o relaţie; considerăm laticea $(\mathcal{P}(A),\subseteq,\cup,\cap)$, $(\mathcal{P}(B),\subseteq,\cup,\cap)$. Definim funcţia f astfel: $f : \mathcal{P}(A) \to \mathcal{P}(B)$, $f(X) = \rho\langle X\rangle$. Deoarece pentru orice $X_1, X_2 \in \mathcal{P}(A)$ avem $X_1 \subseteq X_2 \Rightarrow f(X_1) = \rho\langle X_1\rangle = \rho\langle X_2\rangle = f(X_2)$ rezultă că f este crescător. Dacă presupunem că ρ nu este funcţie injectivă, rezultă că $\rho\langle X_1\cap X_2\rangle \subset \rho\langle X_1\rangle\cap\rho\langle X_2\rangle$, deci $f(X_1\cap X_2) \ne f(X_1)\cap f(X_2) \Rightarrow$ f nu este morfism de latici.

c) Deoarece $(A,\le)$ este mulţime total ordonată, rezultă că pentru orice $a, a' \in A$ avem $a \le a'$ sau $a' \le a$. Presupunem, de exemplu, că $a \le a'$. Atunci $a \wedge a' = \inf\{a,a'\} = a$, $a \vee a' = \sup\{a,a'\} = a'$, $f(a) \le f(a')$ (deoarece f este crescător), $f(a) \wedge f(a') = f(a)$ şi în fine, $f(a) \vee f(a') = f(a')$.

Rezultă că $f(a) = f(a \wedge a') = f(a) \wedge f(a')$ şi $f(a') = f(a \vee a') = f(a) \vee f(a')$. Cazul $a' \le a$ se trateaza asemănător, şi obţinem că f este morfism de latici.

Exerciţiul 105. a) Vedem că pentru orice $m, n \in \mathbb{N}$ avem $m \wedge n = \inf\{m,n\} = (m,n)$ (cmmdc), $m \vee n = \sup\{m,n\} = [m,n]$ (cmmmc). Deoarece pentru orice $m, n, p \in \mathbb{N}$ avem

$$m \vee (n \wedge p) = [m,(n,p)] = (\langle m,n],[m,p]) = (m \vee n) \wedge (m \vee p),$$

rezultă a $(\mathbb{N},|)$ este latice distributivă.

b) Pentru orice $a, b \in A$ avem $a\wedge b = \inf\{a,b\} = \min\{a,b\}$ şi $a\vee b = \sup\{a,b\} = \max\{a,b\}$. Dacă presupunem, de exemplu, că $a, b, c \in A$ şi $a \le b \le c$, atunci $a \vee (b \wedge c) = a \vee b = b = b \wedge c = (a \vee b) \wedge (a \vee c)$. Analog tratăm cazurile $a \le c \le b$, $b \le a \le c$, $b \le c \le a$, $c \le a \le b$, $c \le b \le a$.

Exerciţiul 107. b) $a \le b \iff a\vee b = b \iff (a\vee b)' = b' \iff a'\wedge b' = b' \iff b' \le a'$. În acest caz, deoarece $a \wedge b' \le a \wedge a' = 0$ şi $a' \vee b' \ge b' \vee b = 1$, rezultă că $a \wedge b' = 0$ és $a' \vee b = 1$ etc.

Exerciţiul 109. a) Avem funcţia bijectivă $\phi : \mathcal{P}(M) \to \mathbb{Z}_2^M$, $\phi(X) = \chi_X$ (unde $\chi_X : M \to \mathbb{Z}_2$, $\chi_X(a) = \hat{1}$ $\Leftrightarrow a \in X$). Arătăm că $\chi_{X\triangle Y} = \chi_X + \chi_Y$ és $\chi_{X\cap Y} = \chi_X \cdot \chi_Y$. Dacă $x \in M$, atunci trebuie să analizăm următoarele cazuri: (i) $x \notin X \cup Y$; (ii) $x \in X \cap Y$; (iii) $x \in X \setminus Y$; (iv) $x \in Y \setminus X$.

b) $\mathcal{P}(M \cup N) \simeq \prod_{x\in M\cup N} \mathbb{Z}_2 \simeq \prod_{x\in M} \mathbb{Z}_2 \times \prod_{x\in N} \mathbb{Z}_2 \simeq \mathcal{P}(M) \times \mathcal{P}(N)$.

c) rezultă din b). Altfel, fie $\phi : \mathcal{P}(M) \to \mathcal{P}(\complement N)$, $\phi(X) = X \cap \complement N = X \setminus N$. Atunci ϕ este morfism surjectiv, şi $\phi(X) = \varnothing \Leftrightarrow X \subseteq N$, deci $\mathrm{Ker}(\phi) = \mathcal{P}(N)$.

Exerciţiul 110. a) Observăm că $(e \oplus f)^2 = e \oplus f$.

b) $\mathrm{Id}(\mathbb{Z}_{24}) = \{\hat{0}, \hat{1}, \hat{9}\}$ és $\mathrm{Id}(\mathbb{Z}_{180}) = \{\hat{0}, \hat{1}, \widehat{36}, \widehat{45}, \widehat{81}, \widehat{100}, \widehat{136}, \widehat{145}\}$.

7. Mulţimi de numere

Exerciţiul 115. În Teorema recurenţei 7.1.4 luăm $X := N'$, $a := 0'$ şi $f := s'$ şi obţinem o unică funcţie $u : \mathbb{N} \to N'$ care satisface (1) şi (2). Vom arăta că u este bijecţie, construind o inversă a lui u.

Deoarece şi tripletul $(N', 0', s')$ satisface axiomele lui Peano, obţinem o unică funcţie $u' : N' \to \mathbb{N}$ care satisface (1) şi (2). Arătăm prin inducţie că $(u' \circ u)(n) = n$ şi $(u \circ u')(n') = n'$ pentru orice $n \in \mathbb{N}$ şi $n' \in N'$. Evident, $(u' \circ u)(0) = 0$. Presupunem că $(u' \circ u)(n) = n$. Atunci $(u' \circ u)(s(n)) = (u' \circ u \circ s)(n) = (u' \circ s' \circ u)(n) = (s \circ u' \circ u)(n) = s((u' \circ u)(n)) = s(n)$. Analog se arată că $u \circ u' = 1_{N'}$.

Exerciţiul 126. a) Deoarece $(a,b)|a$ şi $(a,b)|b$, rezultă că $(a,b)x|ax$ şi $(a,b)x|bx$; de aici obţinem $(a,b)x|(ax,bx)$, deci $(ax,bx) = (a,b)xy$, unde $y \in \mathbb{Z}$. Mai departe

$$ax = (ax,bx)y' = (a,b)xyy',$$

adică $a = (a, b)yy'$, şi

$$bx = (ax, bx)y'' = (a, b)xyy'',$$

adică $b = (a, b)yy''$; rezultă că $(a, b)y \mid a, b$, adică $(a, b)y \mid (a, b)$. Obţinem că $y \sim 1$, adică $(ax, bx) = (a, b)x$.

b) În particular, dacă $d = (a, b) = (a'd, b'd) = d(a', b')$, atunci $(a', b') = 1$.

c) Aplicând cele de mai sus avem

$$(a, x) = (a, 1 \cdot c) = (a, (a, b)c) = (a, (ac, bc)) = ((a, ac), bc)) = (a, bc).$$

d) Fie $d = (a, b), x_1 = da', b = db'$ şi $m = da'b'$. Deoarece

$$m = da'b' = ab' = a'b,$$

rezultă că $a, b|m$, adică m este multiplu comun.

Presupunem că $a, b|m'$; rezultă că $m' = au = bv$, adică $m' = da'u = da'v$. Atunci $m'b' = da'b'u = mu$ şi $m'a' = da'b'v = mv$, adică $m|m'xa'$, $m|m'b'$; rezultă că $m|(m'a', m'b')$, dar $(m'a', m'b') = m'(a', b') = m'$, deci $m|m'$.

Am arătat că $m = [a, b]$ şi $ab = dda'b' = dm = (a, b)[a, b]$.

Exerciţiul 127. a) Fie $d = (x_1, x_2, x_3)$ şi $d' = ((x_1, x_2), x_3)$. Atunci $d|x_1, x_2, x_3 \iff d|x_1x_2$ şi $d|x_3 \iff d|(x_1, x_2)$ şi $d|x_3 \iff d|((x_1, x_2), x_3)$, adică $d|d'$. Invers rezultă că $d'|(x_1, x_2)$ şi $d'|x_3 \iff d'|x_1, d'|x_2$ şi $d'|x_3 \implies d'|(x_1, x_2, x_3)$, adică $d'|d$. Pentru cazul general folosim inducţie după n.

Exerciţiul 135. Fie $a - b = kn$, unde $k \in \mathbb{Z}$. Deoarece $(a, n)|a$ şi $(a, n) \mid m$, rezultă că $(a, m) \mid b$. Deci (a, m) este comun divizor al lui b şi m, de unde $(a, m) \mid (b, m)$. Asemănător obţinem $(b, m) \mid (a, m)$, deci $(a, m) = (b, m)$.

8. Algebre universale

Exerciţiul 150. O operaţie n-ară pe A este o funcţie $\omega : A^n \to A$, deci numărul căutat este $|A^{(A^n)}| = m^{(m^n)}$.

Exerciţiul 152. a) Fie $\omega \in \Omega$, $\tau(\omega) = n$. Dacă $(a_1, b_1), \dots, (a_n, b_n) \in F$, atunci $b_1 = f(a_1), \dots, b_n = f(a_n)$ şi

$$\begin{aligned} \omega((a_1, b_1), \dots, (a_n, b_n)) &= (\omega(a_1, \dots, a_n), \omega(b_1, \dots, b_n)) \\ &= (\omega(a_1, \dots, a_n), \omega(f(a_1), \dots, f(a_n)) \\ &= (\omega(a_1, \dots, a_n), f(\omega(a_1, \dots, a_n))) \in F. \end{aligned}$$

Invers, dacă $a_1, \dots, a_n \in A$, atunci $(a_1, f(a_1)), \dots, (a_n, f(a_n)) \in F$, şi

$$(\omega(a_1, \dots, a_n), \omega(f(a_1), \dots, f(a_n))) = \omega((a_1, f(a_1)), \dots, (a_n, f(a_n))) \in F,$$

deci $f(\omega(a_1, \dots, a_n)) = \omega(f(a_1), \dots, f(a_n))$.

b) Fie $\omega \in \Omega$, $\tau(\omega) = n$ şi $(a_1, c_1), \dots, (a_n, c_n) \in S \circ R$; rezultă că există $b_1, \dots, b_n \in B$ astfel încât $(a_1, b_1), \dots, (a_n, b_n) \in R$ şi $(b_1, c_1), \dots, (b_n, c_n) \in S$. Deoarece R şi S sunt subalgebre, obţinem că

$$(\omega(a_1, \dots, a_n), \omega(b_1, \dots, b_n)) = \omega((a_1, b_1), \dots, (a_n, b_n)) \in R$$

şi

$$(\omega(b_1, \dots, b_n), \omega(c_1, \dots, c_n)) = (\omega(b_1, c_1), \dots, (b_n, c_n)) \in S,$$

deci

$$\omega((a_1, c_1), \dots, (a_n, c_n)) = (\omega(a_1, \dots, a_n), \omega(c_1, \dots, c_n)) \in S \circ R.$$

Dacă $(b_1, a_1), \dots, (b_n, a_n) \in R^{-1}$, atunci $(a_1, b_1), \dots, (a_n, b_n) \in R$ şi

$$(\omega(a_1, \dots, a_n), \omega(b_1, \dots, b_n)) = \omega((a_1, b_1), \dots, (a_n, b_n)) \in R,$$

deci $\omega((b_1, a_1), \dots, (b_n, a_n)) = (\omega(b_1, \dots, b_n), \omega(a_1, \dots, a_n)) \in R^{-1}$.

c) Fie $\omega \in \Omega$, $\tau(\omega) = n$, $y_1, \dots, y_n \in \rho(X)$. Există $x_1, \dots, x_n \in X$ astfel încât $(x_1, y_1), \dots, (x_n, y_n) \in R$, deci $(\omega(x_1, \dots, x_n), \omega(y_1, \dots, y_n)) = \omega((x_1, y_1), \dots, (x_n, y_n)) \in R$. Deoarece X este subalgebră, rezultă că $\omega(x_1, \dots, x_n) \in X$ şi $\omega(y_1, \dots, y_n) \in \rho(X)$.

Exerciţiul 153. a) Fie $X = \{A\}$ şi aplicăm teorema de caracterizare a subalgebrei subalgebrei generate: $X_0 = X, X_1 = \{A, \complement_M A\}, X_2 = \{A, \complement_M A, M, \emptyset\}, X_3 = X_4 = \dots$, deci $\langle X\rangle = \bigcup_{k=1}^{\infty} X_k = \{A, \complement_M A, M, \emptyset\}$.

b) $\langle\{\rho\}\rangle = \{\rho^n \mid n \in \mathbb{N}^*\}$; dacă ρ este tranzitiv, atunci $\langle\{\rho\}\rangle = \{\rho\}$.

Exerciţiul 155. a) Dacă $X_0 = X$ şi $Y_0 = f(X)$, atunci

$$X_{k+1} = X_k \cup \{\omega(x_1, \dots, x_{\tau}(\omega)) \mid \omega \in \Omega \text{ şi } x_i \in X_k\,;\ i = 1, \dots, \tau(\omega)\}$$

şi Y_{k+1} este definit analog, atunci $\langle X\rangle = \bigcup_{k=0}^{\infty} X_k$, $\langle f(X)\rangle = \bigcup_{k=0}^{\infty} Y_k$. Prin inducţie se arată că $f(X_k) = Y_k$, $k \geq 0$.

Exerciţiul 156. a) Fie τ tipul algebrei (A, Ω), $\omega \in \Omega$, $n = \tau(\omega)$ şi $a_i \in N(A)$, $i = 1, \dots, n$. Dacă $\langle X \cup \{\omega(a_1, \dots, a_n)\}\rangle = A$, atunci, deoarece $\langle X \cup \{\omega(a_1, \dots, a_n)\}\rangle \subseteq \langle X \cup \{a_1, \dots, a_n\}\rangle$, deci $\langle X \cup \{a_1, \dots, a_n\}\rangle = A$. Deoarece $a_1 \in N(A)$, rezultă că $\langle X \cup \{a_2, \dots, a_n\}\rangle = A$. Prin inducţie obţinem că $\langle X\rangle = A$, deci $\omega(a_1, \dots, a_n) \in N(A)$, şi $N(A)$ este subalgebra.

b) Fie $a \in N(A)$ şi $f : A \to A$ un automorfism. Dacă $\langle X \cup \{f(a)\}\rangle = A$, atunci $A = f^{-1}(A) = \langle f^{-1}(X) \cup \{a\}\rangle$. Deoarece $a \in N(A)$, rezultă că $\langle f^{-1}(X)\rangle = A$ şi $A = f(A) = \langle X\rangle$. Deci $f(a) \in N(A)$, adică $f(N(A)) \subseteq N(A)$.

c) Fie $\{M_i \mid i \in I\}$ mulţimea subalgebrelor maximale şi $\Phi(A) = \bigcap_{i\in I} M_i$. Atunci $a \notin \Phi(A) \Longrightarrow \exists i_0 \in I, a \notin M_{i_0} \Longrightarrow \langle M_{i_0} \cup \{a\}\rangle = A$ şi $\langle M_{i_0}\rangle = M_{i_0} \neq A \Longrightarrow a \notin N(A)$, deci $N(A) \subseteq \Phi(A)$.

Dacă $a \notin N(A)$, atunci $\exists X \subseteq A$ astfel încât $\langle X \cup \{a\}\rangle = A$ şi $\langle X\rangle = A$. Fie

$$\mathcal{S} = \{B \leq (A, \Omega) \mid X \subseteq B,\ a \notin B\}.$$

Evident, $\langle X\rangle \in \mathcal{S}$, deci $\mathcal{S} \neq \emptyset$. Mulţimea $(\mathcal{S}, \subseteq)$ ordonată satisface condiţiile lemei lui Zorn 5.4.2, deci există un element maximal $M' \in (\mathcal{S}, \subseteq)$; vedem uşor că M' este subalgebră maximală a lui(A, Ω). Deoarece $M' \in \mathcal{S}$, rezultă că $a \notin M'$, deci $a \notin \Phi(A)$. Am arătat că $a \notin N(A) \Longrightarrow a \notin \Phi(A)$, adică $\Phi(A) \subseteq N(A)$.

Exerciţiul 158. a) Fie $\omega \in \Omega$, $\tau(\omega) = n$. Presupunem că ρ este congruenţă şi fie $(a_1, b_1), \dots, (a_n, b_n) \in R$; atunci $a_1 \rho b_1, \dots, a_n \rho b_n$, deci $\omega(a_1, \dots, a_n)\rho(b_1, \dots, b_n)$, şi

$$\omega((a_1, b_1), \dots, a_n, b_n)) = (\omega(a_1, \dots, a_n), \omega(b_1, \dots, b_n)) \in R.$$

Invers, dacă ρ eset relaţie omomorfă şi $a_1\rho b_1, \dots, a_n\rho b_n$, atunci $(a_i, b_i) \in R$, $(\omega(a_1, \dots, a_n), \omega(b_1, \dots, b_n)) = \omega((a_1, b_1), \dots, a_n, b_n)) \in R$, şi $\omega(a_1, \dots, a_n)\rho\omega(b_1, \dots, b_n)$.

b) Arătăm întâi că intersecţia relaţiilor de congruenţă este congruenţă şi apoi aplicăm teorema 5.2.5 de caracterizare a laticilor complete.

c) Fie $\sigma = \bigcup_{n\in\mathbb{N},\ \rho_1,\dots,\rho_n\in\mathbb{C}} \rho_1 \circ \dots \circ \rho_n$. Arătăm că $\sigma \in \mathcal{E}(A)$, $\forall \rho \in \mathbb{C}\ \rho \subseteq \sigma$, şi dacă $\sigma' \in \mathcal{E}(A)$ astfel încât $\forall \rho \in \mathbb{C}\ \rho \subseteq \sigma'$, atunci $\sigma \subseteq \sigma'$.

d) Arătăm că dacă $\mathbb{C} \subseteq \mathbb{C}(A, \Omega)$, atunci $\sigma := \bigcup_{n\in\mathbb{N},\ \rho_1,\dots,\rho_n\in\mathbb{C}}$ este congruenţă.

e) Implicaţia „$\Longrightarrow$” este cunoscută. Implicaţia inversă rezultă din a) şi din Exerciţiul 152. b).

f) Deoarece $\rho_1 \subseteq \rho_1 \circ \rho_2$, $\rho_1 \subseteq \rho_3$ $\rho_2 \cap \rho_3 \subseteq \rho_1 \circ \rho_3$ şi $\rho_2 \cap \rho_3 \subseteq \rho_3$, rezultă că $\rho_1 \subseteq \rho_3 \Longrightarrow \rho_1 \circ (\rho_2 \cap \rho_3) \subseteq (\rho_1 \circ \rho_2) \cap \rho_3$.

Dacă $x(\rho_1 \circ \rho_2) \cap \rho_3 y$, atunci $x\rho_3 y$ şi $\exists z \in A$ astfel încât $x\rho_2 z$ şi $z\rho_1 y$; rezultă că $z\rho_3 y$, mai departe $x\rho_3 z$, deci $x(\rho_2 \cap \rho_3)z$ şi în final, $x\ \rho_1 \circ (\rho_2 \cap \rho_3)\ y$.

9. Numere cardinale

Exerciţiul 159. a), b) Fie $\alpha_i = |A_i|$, $\beta_i = |B_i|$, $i \in I$. Dacă $f_i : A_i \to B_i$ este injectiv $\forall\ i \in I$, atunci $\coprod_{i\in I} f_i : \coprod_{i\in I} A_i \to \coprod_{i\in I} B_i$ şi $\prod_{i\in I} f_i : \prod_{i\in I} A_i \to \prod_{i\in I} B_i$ sunt injective.

c) Fie $\alpha = |A|$, $A \neq \varnothing$, $\alpha' = |A'|$, $\beta = |B|$ şi $\beta' = |B'|$. Există $f : A' \to A$ surjectiv şi $g : B \to B'$ injectiv; atunci şi $\mathrm{Hom}(f, g) : \mathrm{Hom}(A, B) \to \mathrm{Hom}(A', B')$ este injectiv, deci $\beta^{\alpha} \leq \beta'^{\alpha'}$.

Exerciţiul 160. (i)⇒(ii) Dacă f injectiv, $A \sim f(A)$; deoarece A este finită şi $f(A) \subseteq A$, rezultă că $f(A) = A$, deci f este surjectiv.

(i)⇒(iii) Dacă f este surjectiv, există $s : A \to A$ astfel încât $f \circ s = 1_A$; s este injectiv, deci bijectiv, deci şi $f = s^{-1}$ este bijectiv.

(ii)⇒(i) Presupunem că A este infinit, şi arătăm că există $f : A \to A$ injectiv, nesurjectiv. Fie $\phi : \mathbb{N} \to A$ o funcţie injectivă, şi notăm $\phi(n) = a_n \in A$, $n \in \mathbb{N}$. Atunci $f : A \to A$, $f(a) = a$ dacă $a \notin \phi(\mathbb{N})$ şi $f(a) = a_{n+1}$ dacă $a = a_n \in \phi(\mathbb{N})$ este funcţia căutată.

(iii)⇒(i) Presupunem că A este mulţime infinită, şi fie $g : A \to A$, $g(a) = a$ dacă $a \notin \phi(\mathbb{N})$, $g(a_n) = a_{n-1}$ dacă $n \geq 1$, şi $g(a_0) = a_0$, unde ϕ este funcţia injectivă de mai sus. Atunci g este surjectiv şi nu eeste injectiv, căci $g(a_1) = g(a_0) = a_0$.

Observăm că $f \circ g = 1_A$ şi $g \circ f \neq 1_A$.

Exercițiul 161. Dacă A este infinit, există o funcție injectivă $\phi : \mathbb{N} \to A,\ n \mapsto a_n$.

a) Fie $B = \{b_0, \dots, b_{n-1}\}$, $A \cap B = \varnothing$. Atunci $f : A \cup B \to A,\ f(a) = a$ dacă $a \notin \phi(\mathbb{N})$, $f(a_k) = a_{k+n},\ f(b_k) = a_k$ este funcție bijectivă.

b) Fie $C = \{c_k \mid k \in \mathbb{N}\} \sim \mathbb{N},\ A \cap C = \varnothing$, și $g : A \cup C \to A,\ g(a) = a$ dacă $a \notin \phi(\mathbb{N}),\ g(a_n) = a_{2n+1},\ g(c_n) = a_{2n}$. Atunci g este bijectiv, deci $|A| + |C| = |A|$.

Exercițiul 162. a) Fie $2\mathbb{N}$ (respectiv $2\mathbb{N}+1$) mulțimea numerelor pare (respectiv impare). Atunci $2\mathbb{N} \sim 2\mathbb{N}+1 \sim \mathbb{N}$, $2\mathbb{N} \cap (2\mathbb{N}+1) = \varnothing$ și $2\mathbb{N} \cup (2\mathbb{N}+1) = \mathbb{N}$, deci $\aleph_0 + \aleph_0 = \aleph_0$.

Funcția $f : \mathbb{N}^* \times \mathbb{N}^* \to \mathbb{N}^*,\ f(m,n) = 2^{n-1}(2n-1)$ este bijectivă, deci $\aleph_0 \cdot \aleph_0 = \aleph_0$.

b) Putem presupune că $A_n = \mathbb{N} \times \{n\},\ \forall\, n \in \mathbb{N}$. Atunci $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.

Mai în detaliu, fie familia de mulțimi $(A_n)_{n\in I}$, unde $I = \{1, 2, \dots, k\}$ este finită sau $I = \mathbb{N}$ infinita numărabilă și fie $A_n = \{a_{n1}, a_{n2}, \dots, a_{nm}, \dots\}$ pentru orice $n \in I$.

Definim funcția $f : \bigcup_{n\in I} A_n \to \mathbb{N} \times \mathbb{N}$. $\forall\ x \in \bigcup_{n\in I} A_n$ fie n a cel mai mic număr astfel încât $x = a_{nm}$ și fie $f(x) = (n, m)$. Atunci f este injectiv, deci există o bijectie între $\bigcup_{n\in I} A_n$ și o submulțime a lui $\mathbb{N} \times \mathbb{N}$, deci $\bigcup_{n\in I} A_n$ este numărabilă.

c) Pentru $k \in \mathbb{N}$, fie $\mathcal{P}_k(\mathbb{N}) = \{X \subseteq \mathbb{N} \mid |X| = k\}$. Definim funcția $\phi : \mathcal{P}_k(\mathbb{N}) \to \mathbb{N}^k$ astfel: dacă $X = \{a_1, \dots, a_k\},\ a_1 < \cdots < a_k$, atunci $\phi_k(X) = (a_1, \dots, a_k) \in \mathbb{N}^k$. Vedem că ϕ_k este injectiv, deci $|\mathcal{P}_k(\mathbb{N})| \le |\mathbb{N}^k| = \aleph_0$; din b) rezultă că $\mathcal{P}_f(\mathbb{N}) = \bigcup_{k\in\mathbb{N}} \mathcal{P}_k(\mathbb{N})$ este numărabil.

d) $\mathbb{Q} = \mathbb{Q}^*_- \cup \{0\} \cup \mathbb{Q}^*_+$ și $f : \mathbb{Q}^*_+ \to \mathbb{N} \times \mathbb{N},\ f(\frac{m}{n}) = (m, n)$ este funcție injectivă, unde $\frac{m}{n} \in \mathbb{Q}^*_+$ este fracție ireducibilă, deci $\mathbb{Q}^*_+ \sim \mathbb{N}$.

e) Fie $\mathbb{Q}_k[X] = \{P \in \mathbb{Q}[X] \mid \deg(P) = k\}$. Atunci $\mathbb{Q}_k[X] \sim \mathbb{Q}^{k+1} \sim \mathbb{Q} \sim \mathbb{N}$ și $\mathbb{Q}[X] = \bigcup_{k\in\mathbb{N}} \mathbb{Q}_k[X] \sim \mathbb{N}$.

Exercițiul 163. a) $f : (0,1) \to (a,b),\ f(x) = (b-a)x + a$ și $g : (-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R},\ g(x) = \tan x$ sunt funcții bijective. Echipotențele $(a,b) \sim [a,b) \sim [a,b] \sim (a,b]$ rezultă dintr-un exercițiu anterior.

b) Dacă $\mathbb{R} \setminus \mathbb{Q} \sim \mathbb{N}$, atunci $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q}) \sim \mathbb{N}$, contradicție, deci $\mathbb{R} \setminus \mathbb{Q} \nsim \mathbb{N}$

Exercițiul 164. a) $\mathfrak{c}^2 = (2^{\aleph_0})^2 = 2^{2\aleph_0} = 2^{\aleph_0} = \mathfrak{c}$; $\mathfrak{c}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = \mathfrak{c}$.

b) $\mathfrak{c} \le \mathfrak{c} + \mathfrak{c} = 2\mathfrak{c} \le \mathfrak{c}^2 = \mathfrak{c}$; $\mathfrak{c} \le \mathfrak{c} \cdot \aleph_0 \le \mathfrak{c}^2 = \mathfrak{c}$; $\mathfrak{c} = 2^{\aleph_0} \le \aleph_0^{\aleph_0} \le \mathfrak{c}^{\aleph_0} = \mathfrak{c}$.

Exercițiul 166. a) Dacă $A = \{a_1\}$, atunci $|\mathrm{Hom}(A, B)| = n$. Aplicăm inducția matematică, observând că: $|\mathrm{Hom}(\{a_1, \dots, a_k, a_{k+1}\}, B)| = |\mathrm{Hom}(\{a_1, \dots, a_k\}, B)| \cdot n = n^{k+1}$.

b) Argumentul e analog. Dacă $A = \{a_1\}$, atunci există n funcții injective; dacă $f(a_1), \dots, f(a_k) \in B$ sunt date, atunci, din injectivitatea lui f rezultă că pentru $f(a_{k+1})$ există $(n-k)$ posibilități.

c) Dacă $k = n$ și $f : A \to B$ este injectiv, atunci f este și bijectiv, deci numărul funcțiilor bijective este $n!$.

d) Fie $A = \{a_1, \dots, a_k\},\ \ a_1 < \cdots < a_k$ și $B = \{b_1, \dots, b_n\}$. Între mulțimea submulțmilor cu k elemente ale lui B și mulțimea $\{f : A \to B \mid f \text{ strict crescător}\}$ există o funcție bijectivă ϕ definită astfel: dacă $B' \subseteq B$, $B' = \{b_{i_1}, \dots, b_{i_k}\}$, atunci fie $\phi(B) = (f : A \to B),\ f(a_{i_j}) = b_{i_j}$; rezultă că numărul funcțiilor strict crescătoare este C_n^k. Deoarece o mulțime cu k elemente se poate ordona în $k!$ moduri, deducem egalitatea $C_n^k = A_n^k/k!$.

e) Fie $\mathbb{N}^*_n = \{1, 2, \dots, n\}$, $\mathcal{F} = \{f : \mathbb{N}^*_k \to \mathbb{N}^*_{n+k-1} \mid f \text{ strict crescător}\}$ și $\bar{\mathcal{F}} = \{\bar{f} : \mathbb{N}^*_k \to \mathbb{N}^*_n \mid f \text{ crescător}\}$; atunci $|\mathcal{F}| = C^k_{n+k-1}$ și $|\bar{\mathcal{F}}| = \bar{C}^k_n$. Fie $\phi : \bar{\mathcal{F}} \to \mathcal{F},\ \phi(\bar{f})(i) = \bar{f}(i) + (i-1)$ și $\psi : \mathcal{F} \to \bar{\mathcal{F}},\ \psi(f) = f(i) - (i-1)$, unde $i \in \mathbb{N}^*_k$. Vedem ușor că ϕ și ψ sunt funcții bine definite, $\psi \circ \phi = 1_{\bar{\mathcal{F}}}$ și $\phi \circ \psi = 1_{\mathcal{F}}$.

Exercițiul 168. a) Dacă $n = n_1 + n_2 + \cdots + n_k$ este o partiție a lui n, atunci fie $s_i = n_1 + \cdots + n_i \in \in \{1, \dots, n-1\}$. Partiția lui n respectiv șirul strict crescător $s_1, s_2, \dots, s_{k-1}$ se determină reciproc; rezultă că numărul partițiilor lui n este C^{k-1}_{n-1}.

b) Dacă $n = n_1 + n_2 + \cdots + n_k$ este o partiție a numărului natural n, fie $s_i = n_1 + \cdots + n_i \in \{0, \dots, n\}$. Partiția lui n respectiv șirul strict crescător $s_1, s_2, \dots, s_{k-1}$ se determină reciproc; rezultă că numărul partițiilor lui n este $\bar{C}^{k-1}_{n+1}$.

Exercițiul 169. a) Dacă $f : A \to B$ este injectiv și $r : B \to A$ este o inversă la stânga a lui f, atunci $r(b) = f^{-1}(b)$ dacă $b \in \mathrm{Im}\, f$ și $r(b) \in A$, dacă $b \notin \mathrm{Im}\, f$; rezultă că numărul inverselor la stânga ale lui f este $|\mathrm{Hom}(B \setminus \mathrm{Im}\, f, A)| = k^{n-k}$.

b) Presupunem că $B = \{b_1, \dots, b_n\}$ și $|f^{-1}(b_i)| = k_i$. Dacă $s : B \to A$ f este o inversă la drepta a lui f, atunci avem k_i posibilități de alegere pentru $s(b_i)$, deci f are $k_1 \cdots k_n$ inverse la drepta.

Exercițiul 170. a) Fie $A_i = \{a \in \mathbb{N} \mid 1 \le a \le m,\ p_i | a\}$, $1 \le i \le n$. Atunci $|A_i| = \frac{m}{p_i}$ și $\phi(m) = m \setminus |\bigcup_{i=1}^n A_i|$; mai departe

$$|A_{i_1} \cap \cdots \cap A_{i_k}| = \{a \in \mathbb{N} \mid 1 \le a \le m,\ p_{i_1} \cdots p_{i_k} | a\}| = \frac{m}{p_{i_1} \cdots p_{i_k}},$$

deci

$$\begin{aligned}\phi(m) &= m\left(1 - \sum_{i=1}^{n} \frac{1}{p_i} + \sum_{1 \le i_1 < i_2 \le n} \frac{1}{p_{i_1} p_{i_2}} - \cdots + (-1)^n \frac{1}{p_{i_1} \dots p_{i_n}}\right) = \\ &= m\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_n}\right).\end{aligned}$$

b) Fie $A_i = \{\sigma \in S_n \mid \sigma(i) = i\}$, şi că observăm că $|A_{i_1} \cap \cdots \cap A_{i_k}| = |\{\sigma \in S_n \mid \sigma(i_j) = i_j,\ 1 \le j \le k\}| = (n-k)!$; rezultă că numărul căutat este

$$n! - |\bigcup_{i=1}^{n} A_i| = n! - C_n^1(n-1)! + C_n^2(n-2_! + \cdots + (-1)^n C_n^n(n-n)! =$$
$$= n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}\right).$$

Exerciţiul 171. Pentru $1 \le i \le n$ fie $A_i = \{f : A \to B \mid b_i \notin \operatorname{Im} f\} \sim \operatorname{Hom}(A, B \setminus \{b_i\})$, deci $|A_i| = (n-1)^k$. Vedem că $\bigcup_{i=1}^n A_i$ este mulţimea funcţiilor nesurjective; rezultă că numărul funcţiilor surjective este $n^k - |\bigcup_{i=1}^n A_i|$. Deoarece $|A_{i_1} \cap \cdots \cap A_{i_l}| = (n-l)^k$, afirmaţia rezultă din principiul includerii şi al excluderii.

Exerciţiul 173. a) Fie $|B| = n$ şi $\phi : \operatorname{Hom}_{sz}(A, B) \to \mathcal{E}_n(A)$, $\phi(f) = \ker f$. Dacă $\rho \in \mathcal{E}_n(A)$, atunci există o funcţie bijectivă $g : A/\rho \to B$, şi dacă $g = g \circ p_\rho$, atunci $\phi(f) = \ker f = \rho$, deci ϕ este surjectiv; dacă $f, f' : A \to B$ sunt două funcţii surjective, atunci $\ker f = \ker f' \Leftrightarrow$ există $g : B \to B$ astfel încât $f' = g \circ f$, deci $|(\ker \phi)\langle f\rangle| = n!$; de aici rezultă că $S(k, n) = |\mathcal{E}_n(A)| = \frac{s(k,n)}{n!}$.

b) Numărul partiţiilor este egal cu numărul relaţiiilor de echivalenţă.

Exerciţiul 175. În prima clasă alegem k_1 elemente din k elemente – numărul posibilităţilor este $C_k^{k_1} = \binom{k}{k_1}$; în a doua clasă alegem k_2 elemente din $k - k_1$ elemente – numărul posibilităţilor este $\binom{k-k_1}{k_2}$. Continuând, în clasa r alegem k_r elemente din $k-(k_1+\cdots+k_{r-1})$ elemente, deci numărul posibilităţilor este $\binom{k-(k_1+\cdots+k_{r-1})}{k_r}$. La al n-lea pas numărul posibilităţilor este 1; rezultă că numărul partiţiilor este $\frac{k!}{k_1!(k-k_1)!} \cdots \binom{k-(k_1+\cdots+k_{n-1})}{k_n} = \frac{k!}{k_1! \ldots k_n!}$.

10. Numere ordinale

Exerciţiul 179. a) Deoarece $A_a \ne A_{a'}$, rezultă că $a \ne a'$, şi deoarece A total ordonată, rezultă că $a < a'$ sau $a' < a$.

Presupunem că există o asemănare $f : A_a \to A_{a'}$. Dacă $a' < a$, atunci $a' \in A_a$, deci $f(a') < a'$; dacă $a < a'$, atunci $a \in A_{a'}$ şi $f^{-1}(a) < a$. În ambele cazuri avem contradicţie (vezi demonstraţia teoremei 10.1.4).

b) Presupunem că $f \ne g$, deci există $a \in A$ astfel încât $f(a) \ne g(a)$; rezultă că

$$A_0 = \{x \in A \mid f(x) \ne g(x)\}$$

este mulţime nevidă, şi fie $a_0 = \min A_0$. Mai departe, fie $b = f(a_0)$ şi $b' = g(a_0)$; rezultă că $A_{a_0} \simeq B_b$ şi $A_{A_0} \simeq B_{b'}$ deci $B_b \simeq B_{b'}$, contradicţie.

Bibliografie

[1] Adamson, I.: *A Set Theory Workbook*. Birkhäuser, Boston, 1998.

[2] Bilaniuk, S.: *A Problem Course in Mathematical Logic*. http://euclid.trentu.ca/math/sb/pcml/pcml-16.pdf. Trent University, Ontario, 2003.

[3] Breaz, S., Covaci, R.: *Elemente de logică, teoria mulţimilor şi aritmetică*. Ed. Fundaţiei pentru Studii Europene, Cluj-Napoca, 2006.

[4] Bloch, E.D.: *Proofs and Fundamentals*. 2nd ed. Springer, New York, 2011.

[5] Bloch, E.D.: *The Real Numbers and Real Analysis*. Springer, New York, 2011.

[6] Epp, S.: *Discrete Mathematics with Applications*. 4th ed. Brooks/Cole, Boston, 2011.

[7] Gallier, J.: *Discrete Mathematics*. 2nd ed. Springer Verlag, New York, 2011.

[8] Grätzer, G.: *Universal Algebra*. 2nd ed. Springer Verlag, Berlin, 2008.

[9] Grätzer, G.: *Lattice Theory: Foundation*. Birkhäuser, Basel, 2010.

[10] Halmos, P.: *Naive Set Theory*. D. Van Nostrand Company Inc., Princeton, 1974.

[11] Kneale, W., Kneale, M.: *The Development of Logic*. Oxford University Press, London, 1985.

[12] Krantz, S. G.: *Discrete Mathematics Demystified*. McGraw-Hill, New York, 2009.

[13] Krantz, S. G.: *The Proof is in the Pudding. The Changing Nature of Mathematical Proof*. Springer Verlag, New York, 2011.

[14] Lavrov, I.A., Maksimova, L.L.: *Probleme de teoria mulţimilor şi logică matematică*. Ed. Tehnică, Bucureşti, 1974.

[15] Levy, A.: *Basic Set Theory*. Dover Publications, New York, 1979.

[16] Lidl, R., Pilz, G.: *Applied Abstract Algebra*. Springer-Verlag, Berlin, 1998.

[17] Manin, Yu. I.: *A Course in Mathematical Logic for Mathematicians*. 2nd ed. Springer-Verlag, New York, 2010.

[18] Mărcuş, A., Szántó Cs., Tóth L.: *Logika és halmazelmélet*. Scientia, Cluj-Napoca, 2005.

[19] Năstăsescu, C.: *Introducere în teoria mulţimilor*. Ed. Didactică şi Pedagogică, Bucureşti, 1981.

[20] Purdea, I., Pic, Gh.: *Tratat de algebră modernă I*. Ed. Academiei, Bucureşti, 1977.

[21] Purdea, I.: *Culegere de probleme de algebră. Relaţii, funcţii şi algebre universale*. Litografia Univ. Babeş-Bolyai, Cluj-Napoca, 1996.

[22] Ross, K. A., Wright Ch., *Discrete Mathematics*. Pearson Education, New Jersey, 2003.

Resurse online:

- http://en.wikipedia.org/wiki/Set_theory
- http://en.wikipedia.org/wiki/Logic
- http://en.wikipedia.org/wiki/Foundations_of_mathematics
- http://en.wikipedia.org/wiki/Philosophy_of_mathematics
- http://en.wikipedia.org/wiki/History_of_mathematics
- http://en.wikipedia.org/wiki/History_of_logic

Glosar