

# Introducere în Logica matematică și teoria mulțimilor

Andrei Mărcuș

14 septembrie 2020

# Cuprins

<b>0</b>	<b>Descrierea cursului</b>	<b>4</b>
0.1	Tematica . . . . .	4
0.2	Evaluare . . . . .	4
<b>1</b>	<b>Logica propozițiilor</b>	<b>5</b>
1.1	Formulele logicii propozițiilor . . . . .	5
1.2	Interpretarea formulelor propoziționale . . . . .	6
1.3	Problema deciziei . . . . .	8
1.3.1	Metoda tabelului de adevăr . . . . .	8
1.3.2	Metoda formelor normale . . . . .	9
1.3.3	Scheme de deducție . . . . .	10
1.3.4	Deducție formală . . . . .	12
<b>2</b>	<b>Logica de ordinul întâi</b>	<b>14</b>
2.1	Noțiunea de predicat . . . . .	14
2.2	Limbaje de ordinul întâi . . . . .	14
2.3	Structura unui limbaj de ordinul întâi. Modele . . . . .	16
2.4	Problema deciziei în logica de ordinul întâi . . . . .	19
2.4.1	Deducția formală în logica de ordinul întâi . . . . .	19
2.4.2	Teoremele principale ale teoriei modelelor . . . . .	20
2.4.3	Teorii formale . . . . .	20
2.5	Logică clasică și logici neclasice . . . . .	21
<b>3</b>	<b>Mulțimi</b>	<b>22</b>
3.1	Teoria naivă și teoria axiomatică a mulțimilor . . . . .	22
3.2	Sistemul axiomatice von Neumann–Bernays–Gödel . . . . .	23
<b>4</b>	<b>Relații și funcții</b>	<b>26</b>
4.1	Relații binare . . . . .	26
4.1.1	Operații cu relații . . . . .	26
4.2	Funcții . . . . .	29
4.2.1	Diagrame comutative . . . . .	30
4.2.2	Familie de elemente și familie de mulțimi . . . . .	30
4.3	Funcții injective, surjective și bijective . . . . .	31
4.3.1	Produsul direct al unei familii de mulțimi și al unei familii de funcții . . . . .	33
4.3.2	Suma directă a unei familii de mulțimi și a unei familii de funcții . . . . .	34
4.3.3	Mulțimea $\text{Hom}(A, B)$ și funcția $\text{Hom}(f, g)$ . . . . .	35
4.3.4	Mulțimea părților și funcția caracteristică a unei submulțimi . . . . .	35
4.4	Relații de echivalență . . . . .	36
4.4.1	Clase importante de relații omogene . . . . .	36
4.4.2	Echivalențe și partiții . . . . .	37
4.5	Teoreme de factorizare a funcțiilor . . . . .	39
<b>5</b>	<b>Mulțimi ordonate</b>	<b>43</b>
5.1	Relații de ordine . . . . .	43
5.2	Latici . . . . .	45
5.3	Mulțimi bine ordonate și mulțimi artiniene . . . . .	46
5.4	Axioma alegerii . . . . .	48

<b>6</b>	<b>Latici și algebre Boole</b>	<b>50</b>
6.1	Latticea ca structură algebrică . . . . .	50
6.2	Latici Boole și inele Boole . . . . .	52
6.3	Algebra Lyndenbaum–Tarski . . . . .	54
6.4	Formule și funcții Boole. Forme normale . . . . .	54
<b>7</b>	<b>Mulțimi de numere</b>	<b>57</b>
7.1	Mulțimea numerelor naturale . . . . .	57
7.1.1	Axiomele lui Peano . . . . .	57
7.1.2	Operații și relația de ordine pe mulțimea numerelor naturale . . . . .	58
7.1.3	Sistemul formal al aritmeticii. Teorema lui Gödel de incompletitudine . . . . .	60
7.2	Mulțimea numerelor întregi . . . . .	60
7.3	Elemente de aritmetica numerelor întregi . . . . .	61
7.3.1	Teorema împărțirii cu rest . . . . .	61
7.3.2	Divizibilitate. Cel mai mare divizor comun . . . . .	62
7.3.3	Numere prime. Teorema fundamentală a aritmeticii . . . . .	64
7.3.4	Congruențe. Inelul $\mathbb{Z}_n$ al claselor de resturi modulo $n$ . . . . .	65
7.3.5	Grupul $U(\mathbb{Z}_n)$ . Teoremele lui Euler și Fermat . . . . .	66
7.3.6	Rezolvarea congruențelor și a ecuațiilor diofantice de gradul I . . . . .	67
7.3.7	Teorema chineză a resturilor. Sisteme de congruențe . . . . .	68
7.4	Mulțimea numerelor raționale . . . . .	70
7.5	Mulțimea numerelor reale . . . . .	71
<b>8</b>	<b>Algebre universale</b>	<b>73</b>
8.1	$\Omega$ -algebre și omomorfisme . . . . .	73
8.2	Subalgebre . . . . .	74
8.3	Congruențe. Algebre factor. Teoreme de izomorfism . . . . .	76
<b>9</b>	<b>Numere cardinale</b>	<b>78</b>
9.1	Număr cardinal. Operații cu numere cardinale . . . . .	78
9.2	Ordonarea numerelor cardinale . . . . .	79
9.3	Mulțimi finite, infinite și numărabile . . . . .	81
9.4	Elemente de combinatorică . . . . .	84
9.4.1	Aranjamente, permutări, combinări . . . . .	84
9.4.2	Principiul includerii și al excluderii . . . . .	85
9.4.3	Partiții. Numerele lui Stirling și Bell. Permutări cu repetiție . . . . .	86
<b>10</b>	<b>Numere ordinale</b>	<b>87</b>
10.1	Noțiunea de număr ordinal . . . . .	87
10.2	Operații cu numere ordinale . . . . .	89
10.3	Definiția axiomatică a numărului cardinal . . . . .	92
10.4	Alefuri și problema continuului . . . . .	92
<b>11</b>	<b>Indicații și soluții</b>	<b>94</b>

# Capitolul 0

## Descrierea cursului

### 0.1 Tematica

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

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

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

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

- teoria mulțimilor, care studiază colecții abstracte de obiecte și corespondențele între ele, având rol important pentru fundamentele matematicii;
- teoria demonstrației, care în esență înseamnă analiza formală a demonstrațiilor matematice.
- teoria modelelor, care este studiul formal al structurilor matematice, având strânsă legătură cu algebra abstractă;
- teoria recursiei (sau teoria calculabilității), care studiază calculabilitatea efectivă a funcțiilor definite pe mulțimea numerelor naturale, având rol important pentru fundamentele informaticii;

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

### 0.2 Evaluare

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

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

unde N=nota, N1, N2, N3, N4=notele obținute pe fiecare subiect de lucrare scrisă, S=puncte acordate pe evaluarea activității de la seminar.

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

# Capitolul 1

## LOGICA PROPOZIȚIILOR

În limbajul comun, prin propoziție înțelegem o afirmație despre care putem decide dacă e adevărată sau falsă. Putem forma propoziții compuse, cărora de asemenea le asociem o valoare de adevăr, folosind cuvinte precum și, sau, nu, dacă și numai dacă etc. Din punct de vedere matematic, o astfel de definiție nu este satisfăcătoare, fiind necesară o abordare formală.

### 1.1 Formulele logicii propozițiilor

**Definiția 1.1.1** a) Simbolurile logicii propozițiilor sunt:

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

b) O **formulă propozițională** este un șir finit de simboluri ce satisface următoarele reguli:

1. Formulele atomice sunt formule.
2. Dacă  $A$  și  $B$  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.

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

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

**Exemplul 1.1.3** 1) Următoarele șiruri de simboluri sunt formule:

$$\begin{aligned} & (p \vee q) \rightarrow (r \leftrightarrow (\neg s)), \\ & ((p \vee (\neg q)) \vee r) \rightarrow (s \wedge (\neg s)), \\ & ((p \rightarrow q) \rightarrow r) \vee (s \wedge r), \\ & (\neg((p \wedge q) \vee (\neg r))) \rightarrow (t \vee p), \\ & ((p \vee q) \rightarrow (p \vee r)) \leftrightarrow ((\neg q) \wedge (\neg p)). \end{aligned}$$

2) Următoarele șiruri de simboluri nu sunt formule:

$$p \wedge \rightarrow q, p \rightarrow, pq \wedge t, p \wedge q \vee r p \wedge (q \rightarrow \wedge r), (pq \wedge (r \wedge p \neg q).$$

**Definiția 1.1.4** a) Spunem că  $B$  **subformulă** a formulei  $A$  dacă  $B$  este obținut în cursul construcției lui  $A$ .

b) Vorbim de **substituție**, dacă în formula  $A$  o formulă atomică  $p$  sau o subformulă  $B$  este înlocuită cu formula  $C$  (notație  $A(C/p)$  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  $A(C/p) = (\neg(((r \wedge s) \wedge q) \vee (\neg r))) \rightarrow (t \vee (r \wedge s))$  și  $A(C, p \wedge q) = (\neg((r \wedge s) \vee (\neg r))) \rightarrow (t \vee p)$ .

## 1.2 Interpretarea formulelor propoziționale

**Definiția 1.2.1** Fie  $V = \{0, 1\}$  mulțimea **valorilor de adevăr**. Aici 0 corespunde *falsului*, iar 1 corespunde *adevărului*. O funcție de  $n$  variabile  $f : V^n \rightarrow V$  se numește **funcție de adevăr**.

O funcție de adevăr de  $n$  variabile poate fi dată printr-un **tabel de adevăr**, care are  $n + 1$  coloane și  $2^n$  linii. Primele  $n$  coloane conțin toate combinațiile posibile ale variabilelor, iar ultima coloană conține valorile corespunzătoare ale funcției.

De asemenea, o funcție de adevăr poate fi vizualizată cu ajutorul diagramelor Euler-Venn sau cu ajutorul schemelor (circuitelor) cu contacte și rele.

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

a) **Negația („non”)**:  $\neg p$ , definită prin

p	$\neg p$
0	1
1	0

b) **Conjunția („și”)**:  $p \wedge q$ , definită prin

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

c) **Disjuncția („sau”)**:  $p \vee q$ , definită prin

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

d) **Implicația („dacă ... atunci”)**:  $p \rightarrow q$ , definită prin

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

e) **Echivalența („dacă și numai dacă”)**:  $p \leftrightarrow q$ , definită prin

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

**Definiția 1.2.3** Dacă  $A$  este o formulă și  $\mathcal{A}$  este mulțimea formulelor atomice din  $A$ , atunci o **interpretare** a lui  $A$  este o funcție  $v : \mathcal{A} \rightarrow V = \{0, 1\}$ . Elementul  $v(p) \in V$  se numește **valoarea de adevăr** a formulei atomice  $p$ .

Fie  $A = A(p_1, \dots, p_n)$  o formulă ce conține atomii  $p_1, \dots, p_n$ , și fie  $v$  o interpretare a lui  $A$ . Notăm cu  $\tilde{A} : V^n \rightarrow V$  funcția de adevăr corespunzătoare lui  $A$ , obținută folosind funcțiile logice fundamentale. Atunci **valoarea de adevăr a formulei  $A$**  corespunzătoare interpretării  $v$  este dată de:

$$H_v(A) := \tilde{A}(v(p_1), \dots, v(p_n)).$$

**Exemplul 1.2.4** în tabelul de mai jos avem interpretările și valorile de adevăr corespunzătoare pentru formula  $A = A(p, q) = ((p \vee q) \wedge \neg p) \rightarrow q$  (punând în evidență și 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 exercițiile de mai jos.

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

**Exemplul 1.2.6** În afară de operațiile logice fundamentale, menționăm și următoarele funcții de adevăr:

- 1) **Adunarea și înmulțirea modulo 2**, notate prin simbolurile  $\oplus$  respectiv  $\odot$ .
- 2) **Funcția lui Sheffer (non și; not and)**:  $p \mid q = \neg(p \wedge q)$ . Este adevărat, dacă cel mult unul din  $p$  sau  $q$  este adevărat.
- 3) **Funcția lui Webb–Peirce (nici-nici; neither-nor; non sau; not or)**:  $p \downarrow q = (\neg p) \wedge (\neg q)$ . Este adevărat, dacă niciunul din  $p$  și  $q$  nu este adevărat.
- 4) **Disjuncția exclusivă (sau-sau; xor)**:  $p \oplus q = \neg(p \leftrightarrow q)$ . Este adevărat, dacă exact unul din  $p$  sau  $q$  este adevărat.

**Exercițiul 1** Să se întocmească tabelele de adevăr pentru funcțiile din exemplul de mai sus.

**Exercițiul 2** Să se verifice cu ajutorul tabelor de adevăr următoarele egalități între funcții:

- 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)  $p \rightarrow q = 1 \oplus p \oplus p \odot q$ .
- 5)  $p \leftrightarrow q = 1 \oplus p \oplus q$ .

**Exercițiul 3** 1) Să se scrie toate funcțiile de adevăr de 1 respectiv 2 variabile.

- 2) Câte funcții de adevăr de  $n$  variabile există?

**Exercițiul 4** Să se arate că orice funcție de adevăr de  $n \geq 1$  variabile poate fi exprimată numai cu ajutorul negației și conjuncției (sau numai cu ajutorul negației și disjuncției). Mai exact, să se verifice următoarele egalități:

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

**Exercițiul 5** Să se arate că orice funcție de adevăr de  $n \geq 1$  variabile poate fi exprimată numai cu ajutorul negației și implicației. Mai exact, să se scrie conjuncția, disjuncția și echivalența cu folosind doar negația și implicația.

**Exercițiul 6** Să se arate că orice funcție de adevăr de  $n \geq 1$  variabile poate fi exprimată numai cu ajutorul funcției lui Sheffer. Mai exact, să se verifice următoarele egalități:

- 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)  $p \rightarrow q = p \mid (q \mid q) = p \mid (p \mid q)$ .

**Exercițiul 7** Să se arate că orice funcție de adevăr poate fi exprimată numai cu ajutorul funcției lui Webb–Peirce. Mai exact, să se verifice următoarele egalități:

- 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)  $p \rightarrow q = ((p \downarrow p) \downarrow q) \downarrow ((p \downarrow p) \downarrow q)$ .

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

b) Dacă nu există o astfel de interpretare formula se numește **contradicție (identic falsă)** și o notăm cu **0**.

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

**Definiția 1.2.8** Introducem două *relații* între formule:

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

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

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

În teoremele din matematică folosim următoarele exprimări:  *$A$  este condiție necesară și suficientă pentru  $B$ ;  $B$  dacă și 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 și  $(\neg A) \wedge A$  contradicție.

2)  $A$  este contradicție dacă și numai dacă  $\neg A$  este tautologie.

3)  $A$  este tautologie dacă și numai dacă  $\neg A$  este contradicție.

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

**Observații 1.2.10** Fie  $A$  o tautologie,  $p$  o formulă atomică și  $B$  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 propoziționale.

- 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)  $A \wedge (A \vee B) \Leftrightarrow A$ ,  $A \vee (A \wedge B) \Leftrightarrow A$  (absorbție),
- 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)  $A \wedge A \Leftrightarrow A$ ,  $A \vee A \Leftrightarrow A$  (idempotență),
- 6)  $A \wedge 1 \Leftrightarrow A$ ,  $A \vee 0 \Leftrightarrow A$ ,
- 7)  $A \wedge 0 \Leftrightarrow 0$ ,  $A \vee 1 \Leftrightarrow 1$ ,
- 8)  $\neg(\neg A) \Leftrightarrow A$  (legea dublei negații),
- 9)  $A \vee (\neg A) \Leftrightarrow 1$  (legea terțului exclus),  $A \wedge (\neg A) \Leftrightarrow 0$  (legea contradicției),
- 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 <sup>1</sup>)
- 11)  $A \leftrightarrow B \Leftrightarrow (A \rightarrow B) \wedge (B \rightarrow A)$  (legea echivalenței),
- 12)  $A \rightarrow B \Leftrightarrow (\neg A) \vee B$  (legea implicației),
- 13)  $A \rightarrow B \Leftrightarrow (\neg B) \rightarrow (\neg A)$  (legea contrapozității),
- 14)  $(A \wedge B) \rightarrow C \Leftrightarrow A \rightarrow (B \rightarrow C)$  (legea separării/reunirii premiselor),
- 15)  $A \rightarrow (B \rightarrow C) \Leftrightarrow B \rightarrow (A \rightarrow C)$  (legea permutării premiselor),

**Exercițiul 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 propozițiilor înseamnă găsirea unui algoritm care să stabilească dacă o formulă propozițională este *tautologie*, *contradicție*, sau *realizabilă* precum și găsirea metodelor corecte de deducție. Vom discuta trei metode, în principiu echivalente: a tabelelor de adevăr, a formelor normale și a deducției formale bazate pe scheme de deducție.

### 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.

<sup>1</sup>Augustus De Morgan (1806–1871), matematician și logician britanic.



### 1.3.2 Metoda formelor normale

**Definiția 1.3.1** Fie  $A = A(x_1, x_2, \dots, x_n)$  o formulă propozițională.

- $A$  este o **conjuncție elementară** dacă este o conjuncție ce are ca factori atomi sau negații de atomi.
- $A$  este o **disjuncție elementară** dacă este o disjuncție ce are ca termeni atomi sau negații 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 conjuncții elementare.

- 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 disjuncții elementare.

**Definiția 1.3.3** a) Formula  $A = A(x_1, x_2, \dots, x_n)$  are **formă normală conjunctivă (FNC)**, dacă este o conjuncție de disjuncții elementare, adică:

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

unde subformula  $A_i = A_i(x_1, x_2, \dots, x_n)$  este o disjuncție elementară, pentru orice  $i = 1, 2, \dots, m$ .

b) Spunem că formula  $B = B(x_1, x_2, \dots, x_n)$  are **formă normală disjunctivă (FND)**, dacă este o disjuncție de conjuncții elementare, adică:

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

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

**Observații 1.3.4** Orice formulă propozițională  $A$  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 șir finit de echivalențe logice, utilizând legile fundamentale ale logicii propozițiilor, prezentate în Teorema 1.2.11, astfel:

- Se exprimă formula  $A$  numai cu conectorii  $\neg$ ,  $\wedge$ ,  $\vee$ , folosind legea implicației și legea echivalenței.
- Se trece negația numai asupra atomilor, utilizând legile lui De Morgan și legea dublei negații.
- Se obțin conjuncții de disjuncții (pentru FNC), respectiv disjuncții de conjuncții (pentru FND), folosindu-se distributivitatea, absorbția, idempotența, comutativitatea sau asociativitatea.

**Exemplul 1.3.5** Fie  $A = \neg x \rightarrow x \wedge y$ . Aplicând cele de mai sus, obținem

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

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

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

și obținem o FNC. Folosind acum idempotența avem:

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

și obținem o altă FNC. Aplicând absorbția, avem:

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

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

**Observații 1.3.6** Metoda formelor normale se aplică astfel. Fie  $C = C(x_1, x_2, \dots, x_n)$  o formulă propozițională și fie  $A = A_1 \wedge A_2 \wedge \dots \wedge A_m$  o FNC respectiv  $B = B_1 \vee B_2 \vee \dots \vee B_m$  o FND cu care  $C$  este logic echivalentă. Atunci:

- $C$  este tautologie dacă și numai dacă în FNC  $A$ , pentru orice  $i = 1, 2, \dots, m$ ,  $A_i$  conține cel puțin un atom împreună cu negația sa;
- $C$  este o contradicție dacă și numai dacă în FND  $B$ , pentru orice  $i = 1, 2, \dots, m$ ,  $B_i$  conține cel puțin un atom împreună cu negația sa.

**Exemplul 1.3.7** Să rezolvăm problema deciziei prin metoda formelor normale.

- Fie  $C = x \wedge \neg y \rightarrow x$ . Aducem pe  $C$  la o formă normală:

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

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

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

$$\begin{aligned} C &= \neg x \wedge (\neg x \vee y \rightarrow x) \Leftrightarrow \neg x \wedge (\neg(\neg x \vee y) \vee x) \Leftrightarrow \neg x \wedge ((\neg\neg x \wedge \neg y) \vee x) \Leftrightarrow \\ &\Leftrightarrow \neg x \wedge ((x \wedge \neg y) \vee x) \Leftrightarrow (\neg x \wedge x \wedge \neg y) \vee (\neg x \wedge x) \end{aligned}$$

Am obținut 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 negația sa  $\neg x$ , deci  $C$  este o contradicție.

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

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

Am obținut FNC  $A = (\neg x \vee y) \wedge (\neg y \vee z)$ , și vedem că  $C$  nu este tautologie. Determinăm și 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 obținut 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 contradicție, deci  $C$  este o formulă realizabilă.

**Exercițiul 9** Să se aducă la formă normală conjunctivă și la formă normală disjunctivă și să se rezolve problema deciziei pentru formulele:

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

### 1.3.3 Scheme de deducție

**Definiția 1.3.8** Spunem că formula propozițională  $B$  este **consecință** a mulțimii de formule  $\Sigma = \{A_1, \dots, A_n\}$  (unde  $n \geq 0$ ), dacă orice interpretare care face  $A_1, \dots, A_n$  adevărate, face și formula  $B$  adevărată.

Notăm aceasta prin

$$A_1, \dots, A_n \models B \quad \text{sau} \quad \Sigma \models B \quad \text{sau} \quad \frac{A_1, \dots, A_n}{B}$$

și o numim **schemă de deducție (inferență)**. Formulele  $A_1, \dots, A_n$  se numesc **premise**, iar  $B$  se numește **concluzie**.

Este evident din definiție că avem  $A_1, \dots, A_n \models B$  exact când formula

$$A_1 \wedge \dots \wedge A_n \rightarrow B$$

este tautologie, adică are loc relația  $A_1 \wedge \dots \wedge A_n \Rightarrow B$ .

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

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

2) Are loc  $\Sigma \models \Gamma$  dacă și numai dacă formula  $(A_1 \wedge \dots \wedge A_n) \rightarrow (B_1 \wedge \dots \wedge B_m)$  este tautologie.

3) Are loc proprietatea de *reflexivitate*  $A \models A$ , deoarece formula  $A \rightarrow A$  este tautologie, pe baza legii implicației și a legii tertului exclus. Mai general, dacă  $\Gamma \subseteq \Sigma$  sunt mulțimi de formule, atunci  $\Sigma \models \Gamma$ .

**Exemplul 1.3.10** Prezentăm mai jos câteva scheme de deducție ale logicii clasice (aristotelice<sup>2</sup>). Ele pot fi verificate ușor cu ajutorul tabelor de adevăr și sunt frecvent utilizate în demonstrarea teoremelor din matematică. Să observăm că unele variante se obțin din altele înlocuind o formulă cu negația ei.

#### 1. Moduri clasice de argumentare.

$$(a) \quad \frac{A, A \rightarrow B}{B} \quad (\text{modus ponendo ponens sau pe scurt modus ponens (MP)})^3$$

<sup>2</sup>Aristotel (384–322 BC), filosof grec. Contribuțiile sale la Logică sunt colectate în *Organon*.

<sup>3</sup>modul de a afirma prin afirmare

- (b)  $\frac{\neg A, \neg A \rightarrow \neg B}{\neg B}$  (modus tollendo tollens) <sup>4</sup>
- (c)  $\frac{\neg A, \neg A \rightarrow B}{B}$  (modus tollendo ponens)
- (d)  $\frac{A, A \rightarrow \neg B}{\neg B}$  (modus ponendo tollens)

## 2. Reductio ad absurdum.

- (a)  $\frac{B, \neg A \rightarrow \neg B}{A}; \quad \frac{\neg B, \neg A \rightarrow B}{A}; \quad \frac{B, A \rightarrow \neg B}{\neg A}; \quad \frac{\neg B, A \rightarrow B}{\neg A}.$
- (b)  $\frac{(\neg A) \rightarrow B, (\neg A) \rightarrow (\neg B)}{A}; \quad \frac{A \rightarrow B, A \rightarrow (\neg B)}{\neg A}.$

## 3. Contrapozitie.

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

## 4. Silogism ipotetic.

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

## 5. Silogism disjunctiv.

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

## 6. Metoda analizei cazurilor.

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

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

**Observații 1.3.11** Prezentăm câteva proprietăți generale ale schemelor de deducție, care sunt utile în demonstrarea teoremelor din matematică:

1. Dacă  $A_1, \dots, A_n \models B_j$  (pentru orice  $j = 1, \dots, m$ ) și  $B_1, \dots, B_m \models C$ , atunci  $A_1, \dots, A_n \models C$  (aceasta este proprietatea de *transitivitate*, care generalizează silogismul ipotetic).
2. Dacă  $A_1 \models A_2, \dots, A_{n-1} \models A_n$ , și  $A_n \models A_1$ , atunci formulele  $A_1, \dots, A_n$  sunt echivalente (aceasta este **metoda demonstrației ciclice**).
3.  $\Sigma \cup \{A\} \models B$  dacă și numai dacă  $\Sigma \models A \rightarrow B$ .

**Exercițiul 11** Să se demonstreze proprietățile de mai sus.

**Observații 1.3.12** Multe demonstrații din matematică devin mai ușoare dacă înlocuim o schemă dată cu una echivalentă.

1. **Demonstrație directă:** înlocuim  $\frac{A}{B \rightarrow C}$  cu  $\frac{A, B}{C}$  (adică *reunim premisele*).
2. **Demonstrație prin contrapozitie:** înlocuim  $\frac{A, B}{C}$  cu  $\frac{A, \neg C}{\neg B}$ .
3. **Demonstrație indirectă (reducere la absurd):** în loc de  $\frac{A}{B}$  arătăm că  $A \wedge (\neg B)$  este contradicție.

**Exercițiul 12** Să se demonstreze echivalența schemelor de deducție de mai sus.

<sup>4</sup>modul de a nega prin negare

### 1.3.4 Deducție formală

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

**1.3.13** Prezentăm aici pe scurt *calculul lui Hilbert*.<sup>5</sup> (Există și alte abordări, cum ar fi *calculul secvențial al lui Gentzen*.) Această metodă pornește cu următoarele date:

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

**A1:**  $A \rightarrow (B \rightarrow A)$

**A2:**  $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$

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

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

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

**Definiția 1.3.14** Fie acum  $A_1, \dots, A_n$  ( $n \geq 0$ ) formule propoziționale. O **deducție** din formulele  $A_1, \dots, A_n$  (numite **premise** sau **ipoteze**) este un șir 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 obține din  $E_j, E_l$  ( $j, l < i$ ) folosind schema (MP).

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

Definiția se generalizează imediat la cazul a două mulțimi de formule  $\Sigma$  și  $\Gamma$ ; notăm  $\Sigma \vdash \Gamma$  dacă  $\Sigma \vdash B$  pentru orice  $B \in \Gamma$ .

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

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

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

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

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

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

1.  $\neg A$  Ipoteză

<sup>5</sup>David Hilbert (1862–1943), matematician german. Între multele sale contribuții, a fost unul din fondatorii teoriei demonstrației și un susținător al teoriei mulțimilor create de Georg Cantor.

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

Vedem că această metodă nu e foarte ușor de aplicat. Următoarele observații simplifică oarecum lucrurile.

**Observații 1.3.17** a) Dacă  $\Sigma \vdash B$  și  $\Sigma \vdash B \rightarrow C$ , atunci  $\Sigma \rightarrow C$ .

b) Dacă  $\Sigma \subseteq \Delta$  și  $\Sigma \vdash B$ , atunci  $\Delta \vdash B$ .

c) Dacă  $\Sigma \vdash \Gamma$  și  $\Gamma \vdash B$ , atunci  $\Sigma \vdash B$ .

d) Dacă  $\Sigma \vdash B \wedge \neg B$ , atunci  $\Sigma \vdash C$  pentru orice formulă  $C$ .

e) (*Teorema lui Herbrand*<sup>6</sup>, 1930):  $\Sigma \vdash B \rightarrow C$  dacă și numai dacă  $\Sigma \cup \{B\} \vdash C$ .

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

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

Următoarea teoremă spune că metoda de deducție bazată pe valorile de adevăr („rezultă”  $\Rightarrow, \models$ ) este echivalentă cu deducția formală ( $\vdash$ ). Prima implicație este mai ușor de demonstrat, a doua este dificilă.

**Teorema 1.3.19 (Frege–Łukasiewicz, de completitudine)** *Are loc  $\Sigma \vdash B$  dacă și numai dacă  $\Sigma \models B$ .*<sup>7 8</sup>

<sup>6</sup>Jacques Herbrand (1908–1931), matematician francez.

<sup>7</sup>Gottlob Frege (1848–1925), matematician, logician și filosof german, unul din fondatorii logicii moderne.

<sup>8</sup>Jan Łukasiewicz (1878–1956), matematician, logician și filosof polonez.

## Capitolul 2

# LOGICA DE ORDINUL ÎNTÂI

Am văzut că logica propozițiilor formalizează utilizarea operațiilor logice *non, și, sau, dacă ... atunci, dacă și numai dacă*). Logica de ordinul întâi merge mai departe introducând *cuantificatori*, pentru a formaliza noțiunile de *pentru orice și 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 și predicatele (sau mulțimile) etc.

### 2.1 Noțiunea de predicat

**Definiția 2.1.1** Fie  $M$  o mulțime nevidă și fie  $n \in \mathbb{N}^*$ . Un **predicat  $n$ -ar pe mulțimea  $M$**  este o submulțime a mulțimii  $M^n$  (adică o relație  $n$ -ară pe  $M$ ).

**Observații 2.1.2** În limbajul comun, un predicat  $n$ -ar pe mulțimea  $M$  este o afirmație „deschisă”  $P(x_1, \dots, x_n)$ , în care putem înlocui variabilele  $x_1, \dots, x_n$  cu elementele  $a_1, \dots, a_n \in M$  pentru a obține propoziția  $P(a_1, \dots, a_n)$ . În acest caz,

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

este o relație  $n$ -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 și regulile de formare a formulilor date mai jos formează **limbajul ordinul întâi**.

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

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

Presupunem în plus că pentru fiecare funcție și fiecare predicat se dă **aritatea**  $\geq 1$  (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 mulțimilor folosește un singur predicat binar  $\in$  („aparține”).

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

3) *Limbajul*  $\mathcal{L}_\mathbb{N}$  al teoriei numerelor naturale folosește constanta 0 și trei operații  $s, +, \cdot$ : funcția succesor  $s$  este unară, adunarea și înmulțirea sunt binare.

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

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

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

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

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

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

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

Spunem că variabila  $x$  este **legată**, dacă nu e liberă. O formulă în care orice variabilă este legată se numește **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  $\forall x((x = y) \wedge (P(x) \rightarrow Q(y)))$ ; atunci  $x = y$ ,  $P(x) \rightarrow Q(y)$ ,  $P(x)$  sunt subformule, dar  $\forall x(x = y)$  nu este.

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

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

1. Dacă  $\varphi$  este formulă atomică.
2. Dacă  $\varphi$  are forma  $(\neg\alpha)$  sau  $(\alpha \wedge \beta)$  sau  $(\alpha \vee \beta)$  sau  $(\alpha \rightarrow \beta)$  sau  $(\alpha \leftrightarrow \beta)$  și substituția lui  $x$  cu  $t$  în  $\alpha$  și  $\beta$  este permisă.
3. Dacă  $\varphi$  are forma  $\forall y\alpha$  sau  $\exists y\alpha$  și suntem în una din următoarele cazuri:
  - (i)  $x$  nu este liberă în  $\varphi$ .
  - (ii)  $y$  nu apare în  $t$  și substituția lui  $x$  cu  $t$  în  $\alpha$  este permisă.

c) Printr-o **generalizare** a formulei  $\varphi$  înțelegem 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  $\forall y(x = y)$  substituția lui  $x$  cu  $y$  nu e permisă.

**Exercițiul 14** Fie  $f, g, h$  simboluri de funcții de 1, 2 respectiv 3 variabile, și 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)  $(P(x) \rightarrow (\forall y)(Q(x, y, z) \wedge P(g(x, y))))$ .
- (c)  $Q(P(x), f(y), z)$ .
- (d)  $f(h(x, y, z))$ .

**Exercițiul 15** Să se scrie toate subformulele formulei:

- a)  $Q(f(x), g(x, y))$ ;
- b)  $\exists x Q(x, y) \rightarrow \neg(P(g(x, y)) \wedge \forall x P(z))$ .

**Exercițiul 16** Să se descrie mulțimea termenilor (expresiilor) unui limbaj de ordinul I, dacă se dau:

- a) o variabilă  $x$  și un simbol de funcție unară (de o variabilă)  $f$ ;
- b) o variabilă  $x$  și un simbol de funcție binară (de două variabile)  $f$ ;

## 2.3 Structura unui limbaj de ordinul întâi. Modele

Acum dăm semnificație și valori de adevăr formulelor unui limbaj de ordinul întâi.

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

1. O mulțime nevidă  $M$ , pe care o numim **univers** și o notăm cu  $|\mathcal{M}|$ .
2. Fiecărei constante  $a$  îi corespunde un element  $\tilde{a} \in M$ .
3. Fiecărui simbol de funcție  $n$ -ară  $f$  îi corespunde o funcție  $\tilde{f} : M^n \rightarrow M$ .
4. Fiecărui simbol de predicat  $n$ -ar  $P$  îi corespunde un predicat  $n$ -ar  $\tilde{P}$  pe mulțimea  $M$  (adică o submulțime  $\tilde{P} \subseteq M^n$ ).
5. Simbolului de egalitate îi corespunde relația de egalitate pe  $M$ .

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

**Definiția 2.3.2** a) Dacă  $\mathcal{V}$  este mulțimea variabilelor lui  $\mathcal{L}$ , atunci o funcție  $s : \mathcal{V} \rightarrow M$  se numește **interpretare** a structurii  $\mathcal{M}$ .

b) Definim inductiv **valoarea**  $H_s^{\mathcal{M}}(t) \in M$  a expresiei  $t$ , corespunzătoare interpretării  $s$ , o definim inductiv astfel:

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

$$H_s^{\mathcal{M}}(f(t_1, \dots, t_n)) = \tilde{f}(H_s^{\mathcal{M}}(t_1), \dots, H_s^{\mathcal{M}}(t_n)).$$

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

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



2.  $H_s^M(t_1 = t_2) = 1$ , dacă  $H_s^M(t_1) = H_s^M(t_2)$ , altfel  $H_s^M(t_1 = t_2) = 0$ .
3.  $H_s^M(\neg\varphi) = 1$ , dacă  $H_s^M(\varphi) = 0$ , altfel  $H_s^M(\neg\varphi) = 0$ .  
 $H_s^M(\varphi \vee \psi) = 1$ , dacă  $H_s^M(\varphi) = 1$  sau  $H_s^M(\psi) = 1$ , altfel  $H_s^M(\varphi \vee \psi) = 0$ .  
 $H_s^M(\varphi \wedge \psi) = 1$ , dacă  $H_s^M(\varphi) = H_s^M(\psi) = 1$ , altfel  $H_s^M(\varphi \wedge \psi) = 0$ .  
 $H_s^M(\varphi \rightarrow \psi) = 0$ , dacă  $H_s^M(\varphi) = 1$  și  $H_s^M(\psi) = 0$ , altfel  $H_s^M(\varphi \rightarrow \psi) = 1$ .  
 $H_s^M(\varphi \leftrightarrow \psi) = 1$ , dacă  $H_s^M(\varphi) = H_s^M(\psi)$ , altfel  $H_s^M(\varphi \leftrightarrow \psi) = 0$ .

4. Considerăm funcția (interpretarea)

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

Atunci:

$$H_s^M(\forall x\varphi) = 1 \text{ dacă și numai dacă pentru orice } m \in M \text{ avem } H_{s(x|m)}^M(\varphi) = 1.$$

$$H_s^M(\exists x\varphi) = 1 \text{ dacă și numai dacă există } m \in M \text{ astfel încât } H_{s(x|m)}^M(\varphi) = 1.$$

**Definiția 2.3.3** a) Spunem că  $M$  este **model** al lui  $\varphi$  (sau că  $M$  **satisfacă**  $\varphi$ ), dacă  $H_s^M(\varphi) = 1$  pentru orice interpretare  $s$  a lui  $M$ . Notăție:  $M \models \varphi$ .

Spunem că  $M$  este **model** pentru mulțimea de formule  $\Gamma$  (sau că  $M$  **satisfacă** pe  $\Gamma$ ), dacă  $M \models \gamma$  pentru orice  $\gamma \in \Gamma$ . Notăție:  $M \models \Gamma$ .

Prin inducție se arată:

**Teorema 2.3.4** 1) Dacă interpretările  $s$  și  $r$  coincid pe variabilele ce apar în expresia  $t$ , atunci  $H_s^M(t) = H_r^M(t)$ .

2) Dacă  $s$  și  $r$  coincid pe variabilele libere ce apar în formula  $\varphi$ , atunci  $H_s^M(\varphi) = H_r^M(\varphi)$ .

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

**Definiția 2.3.6** a) O formulă  $\varphi$  este **tautologie (identic adevărată)**, dacă orice structură  $M$  este model al lui  $\varphi$ . Formula  $\varphi$  se numește **contradicție**, dacă  $\neg\varphi$  este tautologie.

b) Dacă formula  $\varphi \rightarrow \psi$  este tautologie, atunci spunem că  $\psi$  **rezultă** din  $\varphi$  și notăm  $\varphi \Rightarrow \psi$ .

c) Dacă formula  $\varphi \leftrightarrow \psi$  este tautologie, atunci spunem că  $\varphi$  este **echivalent** cu  $\psi$  și notăm  $\varphi \Leftrightarrow \psi$ .

**Exemplul 2.3.7** 1) Pentru orice formulă  $\varphi$  avem că  $\varphi \rightarrow \varphi$  tautologie, iar  $\neg(\varphi \rightarrow \varphi)$  este contradicție.

2)  $\forall y(y = y)$  este tautologie, în timp ce  $\exists y(\neg(y = y))$  este contradicție.

3) Dacă  $\varphi$  este tautologie, atunci orice generalizare  $\forall x_1 \dots \forall x_n \varphi$  este tautologie.

**Observații 2.3.8** a)  $\varphi$  este contradicție dacă și numai dacă pentru orice structură  $M$  și interpretare  $s : \mathcal{V} \rightarrow |M|$ , avem  $H_s^M(\varphi) = 0$ .

b) Dacă  $\varphi$  este contradicție, atunci nu are model. Afirmăția inversă are loc doar pentru formule închise.

c)  $\varphi \Rightarrow \psi$  dacă și numai dacă pentru orice structură  $M$  și pentru orice interpretare  $s : \mathcal{V} \rightarrow |M|$ , dacă  $s$  satisfacă pe  $\varphi$ , atunci satisfacă și pe  $\psi$ .

d) Dacă  $\varphi \Rightarrow \psi$ , atunci orice model  $M$  al lui  $\varphi$  este și model al lui  $\psi$ . Afirmăția inversă are loc doar pentru formule închise.

e)  $\varphi \Leftrightarrow \psi$  dacă și numai dacă pentru orice structură  $M$  și pentru orice interpretare  $s : \mathcal{V} \rightarrow |M|$ ,  $s$  satisfacă pe  $\varphi$  dacă și numai dacă satisfacă pe  $\psi$ .

f) Dacă  $\varphi \Leftrightarrow \psi$ , atunci are  $\varphi$  exact aceleași modele ca și  $\psi$ . Afirmăția inversă are loc doar pentru formule închise.

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

$$(1) \forall x \forall y A \Leftrightarrow \forall y \forall x A, \exists x \exists y A \Leftrightarrow \exists y \exists x A$$

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

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

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

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

- (6)  $\exists x(A \wedge B) \Rightarrow \exists xA \wedge \exists xB$
- (7)  $\neg\forall xA \Leftrightarrow \exists x(\neg A), \quad \neg\exists xA \Leftrightarrow \forall x(\neg A)$  (legile lui De Morgan)
- (8)  $C \wedge \forall xA \Leftrightarrow \forall x(C \wedge A),$   
 $C \vee \forall xA \Leftrightarrow \forall x(C \vee A),$   
 $C \wedge \exists xA \Leftrightarrow \exists x(C \wedge A),$   
 $C \vee \exists xA \Leftrightarrow \exists x(C \vee A).$
- (9)  $C \rightarrow \forall xA \Leftrightarrow \forall x(C \rightarrow A),$   
 $C \rightarrow \exists xA \Leftrightarrow \exists x(C \rightarrow A),$   
 $\forall xA \rightarrow C \Leftrightarrow \exists x(A \rightarrow C),$   
 $\exists xA \rightarrow C \Leftrightarrow \forall x(A \rightarrow C).$
- (10)  $\forall x\varphi \Rightarrow \varphi_t^x$  și  $\varphi_t^x \Rightarrow \exists x\varphi$  (dacă în formula  $\varphi$  înlocuirea variabilei libere  $x$  cu expresia  $t$  este permisă).

**Exercițiul 17** a) Să se arate că în (2), (5) și (6) implicațiile inverse nu sunt adevărate (dând contraexemple).  
 b) Să se demonstreze (9) folosind (8) și (7).

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

- Să se scrie o formulă cu o variabilă liberă  $x$ , adevărată dacă și numai dacă:
  - $x = 0$ ;
  - $x = 1$ ;
  - $x = 2$ ;
  - $x$  este număr par;
  - $x$  este număr impar;
  - $x$  este număr prim.
- Să se scrie o formulă cu două variabile libere  $x, y$ , adevărată dacă și numai dacă:
  - $x = y$ ;
  - $x \leq y$ ;
  - $x < y$ ;
  - $x$  divide  $y$ ;
  - $x$  și  $y$  sunt numere prime gemene (diferența lor e 2).
- Să se scrie o formulă cu trei variabile libere  $x, y, z$ , adevărată dacă și numai dacă:
  - $z$  este cel mai mic multiplu comun al lui  $x$  și  $y$ ;
  - $z$  este cel mai mare divizor comun al lui  $x$  și  $y$ ;
- Să se scrie propoziția (formula închisă) care exprimă:
  - comutativitatea adunării;
  - asociativitatea adunării;
  - comutativitatea înmulțirii;
  - asociativitatea înmulțirii;
  - distributivitatea adunării față de înmulțire;
  - pentru orice număr natural există unul strict mai mare;
  - infinitatea mulțimii numerelor prime;
  - infinitatea mulțimii perechilor de numere prime gemene;
  - orice număr natural este suma a 4 pătrate perfecte;
  - existența celui mai mic multiplu comun și a celui mai mare divizor comun;
  - orice număr par  $> 2$  este suma a două numere prime.

**Exercițiul 19 (Hexagonul opozițiilor din logica aristotelică)** Fie  $S$  și  $P$  două proprietăți referitoare la elementele unei mulțimi  $M$ , astfel ca  $S$  corespunde unei submulțimi nevide a lui  $M$ . Considerăm următoarele afirmații în limbaj natural:

- A: toți  $S$  sunt  $P$ ;
- E: niciun  $S$  nu e  $P$  (altfel formulat: toți  $S$  nu sunt  $P$ );
- I: unii  $S$  sunt  $P$ ;
- O: unii  $S$  nu sunt  $P$ ;
- U: toți  $S$  sunt  $P$  sau niciun  $S$  nu e  $P$ ;
- Y: unii  $S$  sunt  $P$  și unii  $S$  nu sunt  $P$ .

- a) Să se scrie aceste afirmații ca formule închise ale unui limbaj de ordinul I.
- b) Să se găsească cele  $C_g^2 = 15$  relații între propozițiile A, E, I, O, U și Y (sau negațiile acestora).

## 2.4 Problema deciziei în logica de ordinul întâi

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

**Definiția 2.4.1** a) Spunem că a formula  $\psi$  este **consecință** a formulelor  $\varphi_1, \dots, \varphi_n$  dacă pentru orice structură  $\mathcal{M}$  și pentru orice interpretare  $s : V \rightarrow |\mathcal{M}|$ , dacă  $s$  satisface toate formulele  $\varphi_1, \dots, \varphi_n$ , atunci satisface și formula  $\psi$ .

Notăție:  $\varphi_1, \dots, \varphi_n \models B$  sau  $\frac{\varphi_1, \dots, \varphi_n}{\psi}$ , și numim aceasta **schema de deducție**. Formulele  $\varphi_1, \dots, \varphi_n$  se numesc **premize (ipoteze)**, iar  $\psi$  este **concluzie (consecință)**.

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

Mai general, pentru mulțimile de formule  $\Sigma, \Gamma$  e clar ce se înțelege prin notațiile  $\Sigma \Rightarrow \Gamma$  sau  $\Sigma \models \Gamma$ .

**Observații 2.4.2** a) Vedem că  $\psi$  este consecință a lui  $\varphi_1, \dots, \varphi_n$  (adică  $\varphi_1, \dots, \varphi_n \models \psi$ ), dacă și numai dacă  $\psi$  rezultă din  $\varphi_1 \wedge \dots \wedge \varphi_n$  (adică  $\varphi_1 \wedge \dots \wedge \varphi_n \rightarrow \psi$  este tautologie, adică  $\varphi_1 \wedge \dots \wedge \varphi_n \Rightarrow \psi$ ).

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 Deducția formală în logica de ordinul întâi

Ca și în logica propozițiilor, și în logica de ordinul întâi se poate introduce o noțiune de deducție formală independentă de structuri, interpretări și modele. Vom vedea în paragraful următor că în cazul formulelor închise cele două abordări sunt echivalente.

**2.4.3** Pentru a defini noțiunea de deducție avem nevoie de:

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

$$(A1) \quad \varphi \rightarrow (\psi \rightarrow \varphi).$$

$$(A2) \quad (\varphi \rightarrow (\psi \rightarrow \sigma)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \sigma))$$

$$(A3) \quad ((\neg\psi) \rightarrow (\neg\varphi)) \rightarrow (((\neg\psi) \rightarrow \varphi) \rightarrow \psi), \text{ unde } \varphi, \psi, \sigma \text{ sunt formule arbitrare.}$$

$$(A4) \quad \forall x \varphi \rightarrow \varphi_t^x, \text{ dacă în } \varphi \text{ înlocuirea lui } x \text{ cu } t \text{ este permisă.}$$

$$(A5) \quad \forall x(\varphi \rightarrow \psi) \rightarrow (\forall x\varphi \rightarrow \forall x\psi), \text{ unde } \varphi, \psi \text{ sunt formule arbitrare.}$$

$$(A6) \quad \varphi \rightarrow \forall x\varphi, \text{ dacă } x \text{ este variabilă legată în } \varphi.$$

$$(A7) \quad x = x$$

$$(A8) \quad (x = y) \rightarrow (y = x)$$

$$(A9) \quad ((x = y) \wedge (y = z)) \rightarrow (x = z), \text{ unde } x, y, z \text{ sunt variabile arbitrare.}$$

$$(A10) \quad ((x_1 = y_1) \wedge \dots \wedge (x_n = y_n)) \rightarrow (P(x_1, \dots, x_n) \rightarrow P(y_1, \dots, y_n)), \text{ unde } P \text{ este un predicat } n\text{-ar.}$$

$$(A11) \quad ((x_1 = y_1) \wedge \dots \wedge (x_n = y_n)) \rightarrow (f(x_1, \dots, x_n) = f(y_1, \dots, y_n)), \text{ unde } f \text{ este o funcție } n\text{-ară.}$$

- 2) schema de deducție **Modus Ponens (MP)**, adică  $\frac{\varphi, \varphi \rightarrow \psi}{\psi}$ .

**Definiția 2.4.4** Fie formulele  $\varphi_1, \dots, \varphi_n$  ( $n \geq 0$ ).

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

1.  $\delta_i$  este axiomă logică, sau
2.  $\delta_i = \varphi_l$  pentru un  $l = 1, \dots, n$ , sau
3.  $\delta_i$  se obține din  $\delta_j, \delta_l$  (unde  $j, l < i$ ) aplicând schema Modus Ponens (MP).

b) Spunem că formula  $\psi$  este **deductibilă** din formulele  $\varphi_1, \dots, \varphi_n$  (notație:  $\varphi_1, \dots, \varphi_n \vdash \psi$ ), dacă  $\psi$  este ultimul termen al unei deducții din  $\varphi_1, \dots, \varphi_n$ . Formulele  $\varphi_1, \dots, \varphi_n$  sunt **premisele** (**ipotezele** deducției).

Dacă  $n = 0$ , atunci notăm  $\vdash \psi$ . Mai general, pentru mulțimile de formule  $\Sigma, \Gamma$  folosim notația  $\Sigma \vdash \Gamma$ .

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

**Teorema 2.4.5** a) Dacă  $\delta_1, \dots, \delta_k$  este o deducție, atunci și  $\delta_1, \dots, \delta_i$  este o deducție pentru orice  $i = 1, \dots, k$ .

b) Dacă  $\Sigma \vdash \psi$  și  $\Sigma \vdash \psi \rightarrow \sigma$ , atunci  $\Sigma \vdash \sigma$ .

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

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

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

f) Teorema deducției (Herbrand, 1930):  $\Sigma \vdash \psi \rightarrow \sigma$  dacă și numai dacă  $\Sigma \cup \{\psi\} \vdash \sigma$ .

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

h) Generalizare pe constante: Fie  $\Gamma$  o mulțime de formule unde constanta  $c$  nu apare. Dacă  $\Gamma \vdash \varphi$ , atunci există o variabilă  $x$  care nu apare în  $\varphi$  astfel ca  $\Gamma \vdash \forall x\varphi_x^c$ . Mai mult, există o deducție a lui  $\forall x\varphi_x^c$  din  $\Gamma$ , 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. $\forall x\forall y\varphi \rightarrow \forall y\varphi$	A4
3. $\forall y\varphi$	1,2 MP
4. $\forall y\varphi \rightarrow \varphi$	A4
5. $\varphi$	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  $\Sigma$  o mulțime de formule închise. Mulțimea formulor deducibile din  $\Sigma$  se numește **teorie**, iar formulele din  $\Sigma$  sunt **axiome** ale teoriei.

**Teorema 2.4.7** (Teorema lui Gödel de completitudine)<sup>1</sup> Fie  $\varphi$  o formulă închisă. Are loc  $\Sigma \models \varphi$  dacă și numai dacă  $\Sigma \vdash \varphi$ .

**Teorema 2.4.8** (Teorema lui Gödel de completitudine, varianta model-teoretică) Mulțimea  $\Sigma$  de formule nu este contradictorie dacă și numai dacă are model.

**Teorema 2.4.9** (Teorema de compactitate)  $\Sigma$  are model dacă și numai dacă orice submulțime finită a sa are.

## 2.4.3 Teorii formale

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

Șirul de formule deduse care conduce la o teoremă se numește demonstrație formală. *Teoria demonstrației* este ramura Logicii matematice care studiază demonstrațiile formale. Teoremele despre un sistem formal sunt numite de obicei *metateoreme*.

<sup>1</sup>Kurt Gödel (1906–1978), logician, matematician și filosof austriac, cunoscut mai ales pentru teoremele sale de *incompletitudine*.

Sistemul formal se numește **complet** dacă pentru fiecare formulă  $\phi$ ,  $\phi$  sau  $\neg\phi$  este deductibil. Sistemul formal se numește **necontradictoriu** dacă odată cu o formulă nu poate fi dedusă și negația ei. Spunem că avem de a face cu un sistem logic, dacă sistemului formal i se asociază și o **semantică** (semnificație), de obicei sub forma unei interpretări model-teoretice, prin care fiecărei formule închise (propoziții) i se dă o valoare de adevăr. Sistemul se numește **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 demonstrației 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 (și chiar ar fi o pedanterie inutilă). Demonstrațiile matematice obișnuite pot fi privite ca niște schițe pe baza cărora pot fi construite, în principiu, demonstrații formale.

La formalizarea logicii au contribuit în mare măsură Richard Dedekind, Gottlob Frege, Giuseppe Peano și Bertrand Russell, iar teoria demonstrației 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 demonstrații formale finite a consistenței tuturor teoriilor formale). Teoremele de completitudine menționate mai sus au dat inițial suport acestui program. Mai târziu însă, teoremele de incompletitudine ale lui Gödel au arătat că o teorie formală suficient de largă încât să conțină aritmetica lui Peano (pe care o vom discuta în Secțiunea 7.1) nu poate fi concomitent completă și consistentă, și astfel, programul lui Hilbert nu poate fi dus până la capăt. Totuși, programul formalist a contribuit din plin la dezvoltarea nu doar a logicii, ci și a bazelor teoretice ale calculatoarelor de către Alonzo Church și Alan Turing.

## 2.5 Logică clasică și logici neclasice

Teoria discutată în cele două capitole de mai sus aparține Logicii clasice, inițiată de Aristotel în *Organon*, unde a introdus silogismul. Aceasta se caracterizează prin: legea terțului exclus, legea dublei negații, legea necontradicției, monotonia și idempotența implicației, comutativitatea conjuncției, dualitatea De Morgan etc. Din punct de vedere semantic, logica clasică este bivalentă, propozițiile având două valori de adevăr (mai general, valorile de adevăr sunt elemente ale unei *algebre Boole*). Reformularea algebrică a logicii a fost făcută de George Boole, iar logica predicatelor de ordinul I a fost introdusă de Gottlob Frege.

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

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

**Logica intuiționistă** înlocuiește conceptul tradițional de adevăr cu cel de *demonstrabilitate constructivă*. Altfel spus, o afirmație este considerată adevărată doar dacă avem o demonstrație efectivă a ei, și este falsă dacă din ea se poate deduce o contradicție. O afirmație nedemonstrată nu are valoare de adevăr. Demonstrația constructivă existenței unui obiect poate fi transformată într-un algoritm prin care se generează un exemplu concret. Legea terțului exclus, legea dublei negații și legile lui De Morgan nu sunt admise ca axiome, dar pot fi demonstrate de la caz la caz. Logica intuiționistă a fost formalizată de Arend Heyting pornind de la programul intuiționist al lui L.E.J. Brouwer de fundamentare a matematicii. Semantica logicii intuiționiste folosește fie așa-numitele *algebre Heyting* în locul algebrelor Boole din logica clasică, fie *modelele Kripke*, dezvoltate în anii 1950-1960 de Saul Kripke și André Joyal. Logica liniară este o variantă a logicii intuiționiste în care se renunță și la idempotența implicației, adică la regula  $\frac{\Gamma, C, C \vdash B}{\Gamma, C \vdash B}$ . Are aplicații importante în domenii precum limbaje de programare, mecanica cuantică și lingvistică. Există și 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 atașeze unei afirmații expresia unei atitudini, credințe, obligații etc. De exemplu, avem modalități *alelice* (p este posibil, este necesar, este imposibil), *temporale* (a fost p, a fost întotdeauna p, va fi p, va fi întotdeauna p), *deontice* (p este obligatoriu, notat Op, p este permis, notat Pp), *epistemice* (se știe că p), *ale credinței* (se crede că p). Operatorii modali se reprezintă prin simboluri cum ar fi  $\Box$  pentru *este necesar* sau  $\Diamond$  pentru *este posibil*. Astfel, de exemplu, au loc tautologiile  $\Diamond p \leftrightarrow \neg\Box\neg p$ ;  $\Box p \leftrightarrow \neg\Diamond\neg p$ ;  $Pp \rightarrow \neg O\neg p$  (în limbaj natural spunem, de exemplu, „este posibil să ningă azi dacă și numai dacă nu este necesar să nu ningă azi”; „este necesar să ningă azi dacă și numai dacă nu este posibil să nu ningă azi”; „dacă p is permis, atunci non p nu este obligatoriu”). Logica modală este folosită în științe umaniste precum teoria literară, estetica, istoria.

# Capitolul 3

## MULȚIMI

### 3.1 Teoria naivă și teoria axiomatică a mulțimilor

Începem cu o recapitulare a cunoștințelor dobândite în liceu.

**3.1.1** Prin **mulțime** înțegem o colecție de lucruri (obiecte, noțiuni) bine determinate, numite **elementele** sale. Faptul că elementul  $a$  **aparține** mulțimii  $A$  se notează  $a \in A$ ; notația  $b \notin A$  înseamnă:  $b$  nu aparține lui  $A$ . Aceste noțiuni sunt primare, adică nu le definim.

O mulțime 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  $A = \{x \mid x \in \mathbb{R} \text{ și } 0 \leq x \leq 3\}$ .

Mulțimile  $A$  și  $B$  sunt **egale**,  $A = B$ , dacă au aceleași elemente.

**Mulțimea vidă** este unica mulțime care nu are niciun element. Notăție:  $\emptyset$ .

**Definiția 3.1.2** a) O mulțime  $A$  este **submulțime** a mulțimii  $B$ , dacă orice element al lui  $A$  este element al lui  $B$ ; notație:  $A \subseteq B$ . Orice mulțime nevidă  $A$  are două submulțimi **triviale**:  $\emptyset$  și  $A$ .

Să reținem că  $A = B$  dacă și numai dacă  $A \subseteq B$  și  $B \subseteq A$ . Dacă  $A \subseteq B$  și există  $x \in B$  astfel încât  $x \notin A$ , atunci spunem că  $A$  este **submulțime proprie** a lui  $B$ . Notăție:  $A \subset B$ .

b) Submulțimile unei mulțimi  $U$  formează **mulțimea părților (mulțimea putere)** a lui  $U$ :

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

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

**Definiția 3.1.3** **Intersecția** mulțimilor  $A$  și  $B$  este mulțimea elementelor comune, adică

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

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

**Reuniunea** mulțimilor  $A$  și  $B$  este mulțimea

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

**Diferența** mulțimilor  $A \setminus B$  este mulțimea

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

Dacă  $B \subseteq A$ , atunci  $A \setminus B$  este **complementara** mulțimii  $A$  relativ la  $B$ . Notăție:  $\mathcal{C}_A(B)$ .

**Diferența simetrică** a mulțimilor  $A$  și  $B$  este mulțimea

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

**Produsul cartezian** al mulțimilor  $A_1, A_2, \dots, A_n$  este mulțimea

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

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

**Exercițiul 20** Fie  $A, B, C$  mulțimi incluse în universul  $U$ . Să se demonstreze următoarele proprietăți de bază:

- $A \subseteq A$  (*reflexivitate*);
- dacă  $A \subseteq B$  și  $B \subseteq C$ , atunci  $A \subseteq C$  (*tranzitivitate*);
- dacă  $A \subseteq B$  și  $B \subseteq A$ , atunci  $A = B$  (*antisimetrie*);
- $A \cup B = B \cup A$ ,  $A \cap B = B \cap A$  (*comutativitate*);
- $(A \cup B) \cup C = A \cup (B \cup C)$ ,  $(A \cap B) \cap C = A \cap (B \cap C)$  (*asociativitate*);
- $A \cap A = A$ ,  $A \cup A = A$  (*idempotență*);
- $A \cup (A \cap B) = A$ ;  $A \cap (B \cup A) = A$  (*absorbție*);
- $A \cup \emptyset = A$ ;  $A \cap \emptyset = \emptyset$ ;
- $A \cup \complement A = U$ ;  $A \cap \complement A = \emptyset$ ;
- $\complement \complement A = A$ ;

**Exercițiul 21** Fie  $A, B, C$  mulțimi. Să se demonstreze:

- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ;  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$  (*distributivitate*);
- $A \setminus B = A \cap \complement B$ ;
- $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C) = (A \setminus B) \setminus C$ ;
- $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$ ;
- $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$ ;
- $(A \cap B) \setminus C = A \cap (B \setminus C) = (A \setminus C) \cap B$ ;
- $\complement(A \cup B) = \complement A \cap \complement B$ ;  $\complement(A \cap B) = \complement A \cup \complement B$  (*formulele lui De Morgan*).

**Exercițiul 22** Să se arate că pentru orice mulțimi  $A, B, C$  avem:

- $A \Delta B = (A \cap \complement B) \cup (B \cap \complement A)$ ;
- $A \Delta B = B \Delta A$ ;
- $(A \Delta B) \Delta C = A \Delta (B \Delta C)$ ;
- $A \Delta \emptyset = A$ ;  $\complement A = A \Delta U$ ;  $A \Delta A = \emptyset$ ;
- $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$ ;
- $A \cup B = A \Delta B \Delta (A \cap B)$ .

**Exercițiul 23** Să se arate că pentru orice mulțimi  $A, B, C$ , dacă  $A \cap C = B \cap C$  și  $A \cup C = B \cup C$  atunci  $A = B$ .

**Exercițiul 24** Fie  $A, B, C$  mulțimi date. Să se determine mulțimea  $X$  care satisface:

- $A \cap X = B$ ,  $A \cup X = C$ ;
- $A \setminus X = B$ ,  $X \setminus A = C$ .

**Exercițiul 25** Dacă  $A, B, C, D$  sunt mulțimi, atunci:

- $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$ ;
- afirmația  $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D)$  nu e adevărată în general;
- $(A \cup B) \times C = (A \times C) \cup (B \times C)$ ;
- $(A \cap B) \times C = (A \times C) \cap (B \times C)$ ;
- $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$ .

**3.1.4** Abordarea din acest paragraf ține de așa-numita **teorie naivă a mulțimilor**, dezvoltată de matematicianul german Georg Cantor după 1870. S-a arătat mai târziu că această teorie duce la contradicții, din cauza faptului că permite formarea de mulțimi „mari”, fără restricții. Paradoxul lui Bertrand Russel (1902) este printre cele mai cunoscute: considerăm mulțimea  $R$  a tuturor mulțimilor care nu se conțin 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 contradicție care vine din faptul că teoria permite ca  $R$  să fie considerată mulțime.

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

Din punctul de vedere al logicii predicatelor, axiomele ambelor teorii pot fi date prin formule închise în limbajul de ordinul întâi  $\mathcal{L}_S$ , menționat în capitolul anterior, care folosește un singur predicat binar  $\in$  („aparține”). 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 totuși o formalizare completă, iar *axioma alegerii* va fi enunțată doar în capitolele următoare.

**Definiția 3.2.1** a) Limbajul  $\mathcal{L}_S$  al teoriei axiomatice NBG folosește pe lângă simbolurile logice în singur predicat de două variabile notat  $\in$ . Deci formulele atomice ale teoriei sunt  $x = y$  și  $x \in y$ . Simbolurile de variabile  $x, y, z, \dots$  notează **clase**. Formula  $x \in y$  se citește **clasa  $x$  aparține clasei  $y$**  (sau  **$y$  conține pe  $x$** ), iar  $x = y$  se citește: clasa  $x$  este egală cu clasa  $y$ . Noțiunile de **clasă**, respectiv **aparține** sunt considerate primare, nu se definesc.

b) O clasă  $x$  se numește **mulțime**, dacă există o clasă  $y$ , careia îi aparține (adică există  $y$  astfel încât  $x \in y$ ). Dacă o clasă nu e mulțime, atunci se numește **clasă proprie**.

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

**3.2.2** Prezentăm în continuare axiomele.

**1. Axioma extensionalității.** Două clase sunt egale exact când au aceleași 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 conține exact elementele satisfăcând  $P(x)$ . 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 egalității rezultă că clasa de mai sus este unică și o notăm

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

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

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

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

**3. Axioma perechii.** Dacă  $x$  și  $y$  sunt mulțimi, atunci clasa  $\{z \mid (z = x) \vee (z = y)\}$  este mulțime.

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

**Definiția 3.2.3** a) Fie  $A$  și  $B$  clase. **Reuniunea claselor  $A$  și  $B$**  este

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

iar **intersecția claselor  $A$  și  $B$**  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 **intersecția clasei  $A$**  este clasa

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

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

c) **Complementara clasei  $A$**  este clasa

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

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

d) **Diferența claselor  $A$  și  $B$**  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 și  $x \in B$ . Notăție:  $A \subseteq B$ . Dacă  $A$  este mulțime și  $A \subseteq B$ , atunci spunem că  $A$  este **submulțime** a clasei  $B$ .

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

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



**4. Axioma mulțimii putere.** Pentru orice mulțime  $x$  există o mulțime  $y$ , care conține exact subclasele mulțimii  $x$ .

**Observații 3.2.4** 1) Rezultă ca subclasele unei mulțimi sunt mulțimi, iar clasa putere a unei mulțimi este mulțime.

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 mulțime. Evident, dacă  $R \in R$ , atunci  $R$  este mulțime și  $R \notin R$ ; invers, dacă presupunem că  $R$  este mulțime, atunci din  $R \notin R$  rezultă că  $R \in R$ . Deci avem contradicție în ambele cazuri, adică  $R$  nu e mulțime.

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

4) Intersecția și diferența mulțimilor sunt mulțimi. Într-adevăr, fie  $A$  o clasă nevidă. Atunci  $\cap A$  este mulțime, deoarece dacă  $a \in A$ , atunci evident  $\cap A \subseteq a$ ; dar  $a$  este mulțime (deoarece  $a \in A$ ), deci și  $\cap A$  este mulțime (fiind subclasă a unei mulțimi). În consecință,  $A \cap B = \cap\{A, B\}$  și  $A \setminus B = A \cap \complement B$  sunt mulțimi.

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

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

(În particular, dacă  $A$  și  $B$  sunt mulțimi, atunci  $A \cup B = \cup\{A, B\}$  este mulțime.)

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

(Această axiomă elimină „anomalia”  $a \in a$  pentru mulțimi. În consecință, clasa Russell  $R$  coincide cu universul  $U$ .)

**Definiția 3.2.5** Fie  $x$  o mulțime. Atunci mulțimea  $x^+ = x \cup \{x\}$  se numește **succesorul** lui  $x$ .

**7. Axioma infinitului.** Există o mulțime  $y$  pentru care  $\emptyset \in y$  și pentru orice  $x \in y$  avem  $x^+ \in y$ .

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

Pe baza axiomei infinitului se introduce mulțimea  $\mathbb{N}$  a numerelor naturale. Vom face această discuție în Secțiunea 7.1.

**Exercițiul 26** Să se arate că mulțimile  $\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \dots$  sunt distincte două câte două. (Indicație: folosim inducția matematică.)

**Definiția 3.2.6** a) Fie  $a$  și  $b$  mulțimi. Atunci mulțimea  $\{\{a\}, \{a, b\}\}$  se notează prin  $(a, b)$  și se numește **perche ordonată** cu **prima componentă**  $a$  și **a doua componentă**  $b$ .

b) **Produsul cartezian** al claselor  $A$  și  $B$  este clasa

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

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

**Exercițiul 27** Dacă  $a, b, c, d$  sunt mulțimi, atunci  $(a, b) = (c, d)$  dacă și numai dacă  $a = c$  și  $b = d$ .

**Observații 3.2.7** 1) Dacă  $P(x, y)$  este o formulă în care  $x$  și  $y$  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  $A$  și  $B$  sunt mulțimi, atunci și  $A \times B$  este mulțime. Într-adevăr, dacă  $a \in A$  și  $b \in B$ , 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 mulțime, deci și  $A \times B$  este mulțime.

# Capitolul 4

## RELAȚII ȘI FUNCȚII

O relație binară sau corespondență între elementele mulțimilor  $A$  și  $B$  este o mulțime de perechi din  $A \times B$ . Acest concept formalizează și generalizează noțiuni precum *mai mare ca*, *egal cu*, *divide pe*, *aparține lui*, *este inclus în*, *paralel cu*, *perpendicular pe*, *congruent cu*, *adiacent lui* etc. Conceptul de funcție este caz particular al celui de relație.

### 4.1 Relații binare

**Definiția 4.1.1** Fie  $n \in \mathbb{N}^*$  și fie  $A_1, A_2, \dots, A_n$  mulțimi.

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

Dacă  $n = 2$ , atunci  $\rho = (A_1, A_2, R)$  este **relație binară** (sau **corespondență**) între elementele mulțimilor  $A_1$  și  $A_2$ , unde  $R \subseteq A_1 \times A_2$ . În continuare ne ocupăm doar de relații binare, numite pe scurt relații. De multe ori identificăm relația cu graficul său.

b) Fie  $\rho = (A, B, R)$ ,  $R \subseteq A \times B$  o relație. Mulțimea  $R$  se numește **graficul** lui  $\rho$  și **notăm**:

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

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

c) Spunem că  $\rho$  este **relație omogenă**, dacă  $A = B$ .

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

e) Pe mulțimea  $A$  definim **relația diagonală**

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

(unde  $a1_A b \Leftrightarrow a = b$ ).

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

2) Relația de asemănare pe mulțimea triunghiurilor din plan.

3) Relația de divizibilitate pe  $\mathbb{Z}$  este următoarea relație 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 relație  $\rho = (A, B, R)$ , și anume relația vidă, cu graficul  $R = \emptyset$ .

#### 4.1.1 Operații cu relații

**Definiția 4.1.3** a) Spunem că  $\rho = (A, B, R)$  este **subrelație** relației  $\sigma = (A, B, S)$ , notație  $\rho \subseteq \sigma$ , dacă  $R \subseteq S$ , adică, dacă pentru orice  $(a, b) \in A \times B$  avem  $a\rho b \Rightarrow a\sigma b$ .

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

b) **Intersecția relațiilor**  $\rho$  și  $\rho'$  este relația  $\rho \cap \rho' = (A, B, R \cap R')$ , deci  $a(\rho \cap \rho')b \Leftrightarrow a\rho b \wedge a\rho'b$ .

c) **Reuniunea relațiilor**  $\rho$  și  $\rho'$  este relația  $\rho \cup \rho' = (A, B, R \cup R')$ , deci  $a(\rho \cup \rho')b \Leftrightarrow a\rho b \vee a\rho'b$ .

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

e) **Inversa relației**  $\rho$  este relația  $\rho^{-1} = (B, A, R^{-1})$  relație, 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 relațiilor**  $\rho$  și  $\sigma$  este relația  $\sigma \circ \rho = (A, D, S \circ R)$ , 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  $a(\sigma \circ \rho)b \Leftrightarrow \exists x \in B \cap C : a\rho x$  și  $x\rho d$ . Notăm  $\rho \circ \rho = \rho^2$ .

**Exemplul 4.1.4** 1) Pe mulțimea  $\mathbb{Z}$ , relația de egalitate „=” este subrelație a relației  $\leq$ . Relația de divizibilitate | nu este subrelație a lui  $\leq$ , pentru că de exemplu  $2 \mid -6$  și  $2 \not\leq -6$ .

2) Pe  $\mathbb{R}$ , intersecția lui  $\leq$  și  $\geq$  este relația de egalitate =; reuniunea relațiilor „=” și „<” este relația „ $\leq$ —”; complementara lui  $<$  este  $\geq$ ; inversa lui  $<$  este relația  $>$ .

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

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

- 1)  $(\tau \circ \sigma) \circ \rho = \tau \circ (\sigma \circ \rho)$  (compunerea relațiilor este asociativă),
- 2)  $\rho \circ \mathbf{1}_A = \mathbf{1}_B \circ \rho = \rho$  (relația de egalitate este element neutru față de compunere).

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

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

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

**Exercițiul 28** Fie mulțimile  $A = \{1, 2\}$ ,  $B = \{1, 2, 3\}$ ,  $C = \{1, 2, 3, 4\}$ ,  $R_1 = \{(1, 2), (1, 3), (2, 3)\} \subseteq A \times B$ ,  $R_2 = \{(1, 4), (3, 1), (3, 4)\} \subseteq B \times C$ ,  $\rho_1 = (A, B, R_1)$ ,  $\rho_2 = (B, C, R_2)$ . Să se determine relațiile:  $\rho_2 \circ \rho_1$ ,  $\rho_1 \circ \rho_2$ ,  $\rho_1^{-1}$ ,  $\rho_1^{-1}$ ,  $(\rho_1 \circ \rho_2)^{-1}$ ,  $\rho_2^{-1} \circ \rho_1^{-1}$ .

**Exercițiul 29** Fie  $\rho = (\mathbb{N}, \mathbb{N}, <)$ . Să se determine relațiile  $<^2$ ,  $<^3$ ,  $< \circ >$  și  $> \circ <$ .

**Exercițiul 30** Fie  $A = \{1, 2, 3, 4\}$  și  $R$ ,  $S$ ,  $S' \subseteq A \times A$ , 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 relațiile  $(S \cap S') \circ R$ ,  $(S \circ R) \cap (S' \circ R)$ ,  $R \circ (S \cap S')$  și  $(R \circ S) \cap (R \circ S')$ .

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

- a)  $(\rho^{-1})^{-1} = \rho$ ;  $(\mathbb{C}\rho)^{-1} = \mathbb{C}\rho^{-1}$ ;
- 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  $\sigma \circ \rho \subseteq \sigma' \circ \rho'$ .

**Definiția 4.1.6** Fie  $\rho = (A, B, R)$  o relație și fie  $X \subseteq A$ . Mulțimea

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

se numește **secțiunea relației  $\rho$  după submulțimea  $X$** . Dacă submulțimea  $X = \{x\}$  are un singur element, atunci notăm:

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

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

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

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

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

**Demonstrație.** Pentru orice  $d \in D$  avem:

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

deci afirmația e demonstrată. ■

**Exercițiul 32** Fie mulțimile  $A = \{a_1, a_2, a_3, a_4\}$ ,  $B = \{b_1, b_2, b_3, b_4, b_5\}$ ,  $X = \{a_2, a_4\}$ ,  $Y = \{b_1, b_2, b_4, b_5\}$  și considerăm relația  $R = \{(a_1, b_2), (a_3, b_5), (a_1, b_3), (a_2, b_4)\} \subseteq A \times B$ . Să se determine mulțimile  $R(X)$ ,  $R(a_2)$ ,  $R^{-1}(Y)$ ,  $R^{-1}\{b_5\}$ ,  $R^{-1}(B)$  și  $R(A)$ .

**Exercițiul 33** Fie  $\delta = (\mathbb{N}, \mathbb{N}, |)$  relația de divizibilitate. Să se determine mulțimile  $\delta\langle 1 \rangle$ ,  $\delta^{-1}(\{4, 9\})$ ,  $\delta^{-1}(\mathbb{N})$  și  $\delta(\mathbb{N})$ .

**Exercițiul 34** Fie  $\rho = (A, B, R)$  și  $\rho' = (A, B, R')$  relații. Să se arate că următoarele afirmații sunt echivalente:

- (i)  $\rho \subseteq \rho'$ ;
- (ii)  $(\forall x \in A) \rho(x) \subseteq \rho'(x)$ ;
- (iii)  $(\forall X \subseteq A) \rho(X) \subseteq \rho'(X)$ .

**Exercițiul 35** Fie  $\rho = (A, B, R)$  și  $\rho' = (A, B, R')$  relații și fie  $X, X' \subseteq A$ . Să se demonstreze (specificându-se tautologiile din lista 2.3.9 care au fost utilizate):

- a) dacă  $X \subseteq X'$  și  $\rho \subseteq \rho'$ , 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)  $\rho(X \cap X') \subseteq \rho(X) \cap \rho(X')$ ;  $(\rho \cap \rho')(X) \subseteq \rho(X) \cap \rho'(X)$ ;

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

**Exercițiul 36** Fie  $\rho = (A, B, R)$  o relație. Să se arate că următoarele afirmații sunt echivalente:

- (i)  $\forall x \in A, R(x) \neq \emptyset$ ;
- (ii)  $\Delta_A \subseteq R^{-1} \circ R$ ;
- (iii)  $R^{-1}(B) = A$ ;
- (iv)  $\forall A'$  mulțime,  $\forall P_1, P_2 \subseteq A' \times A$ , dacă  $(R \circ P_1) \cap (R \circ P_2) = \emptyset$ , atunci  $P_1 \cap P_2 = \emptyset$ ;
- (v)  $\forall A'$  mulțime,  $\forall P \subseteq A' \times A$  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  $R(X) = \emptyset \Rightarrow X = \emptyset$ .

**Exercițiul 37** Fie  $\rho = (A, B, R)$  o relație. Să se arate că următoarele afirmații sunt echivalente:

- (i) Pentru orice  $x \in A$ ,  $|R(x)| \leq 1$ ;
- (ii)  $R \circ R^{-1} \subseteq \Delta_B$ ;
- (iii) Pentru orice mulțime  $B'$  și pentru orice relații  $S_1, S_2 \subseteq B \times B'$  avem  $(S_1 \cap S_2) \circ R = (S_1 \circ R) \cap (S_2 \circ R)$ ;
- (iv) Pentru orice mulțime  $B'$  și pentru orice relații  $S_1, S_2 \subseteq B \times B'$  avem  $S_1 \cap S_2 = \emptyset \Rightarrow (S_1 \circ R) \cap (S_2 \circ R) = \emptyset$ ;
- (v) Pentru orice mulțime  $B'$  și pentru orice  $S \subseteq B \times B'$  avem  $(S \circ R) \cap (\overline{S} \circ R) = \emptyset$ ;
- (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  $R^{-1}(Y) \cap R^{-1}(\overline{Y}) = \emptyset$ ;
- (viii) Pentru orice  $Y \subseteq B$  avem  $R^{-1}(B) \setminus R^{-1}(Y) = R^{-1}(\overline{Y})$ .

**Exercițiul 38** Fie  $S \subseteq B \times C$ . Următoarele afirmații sunt echivalente:

- (i)  $\forall Y_1, Y_2 \subseteq B, Y_1 \neq Y_2 \Rightarrow S(Y_1) \neq S(Y_2)$ ;
- (ii)  $\forall A$  mulțime,  $\forall R_1, R_2 \subseteq A \times B, S \circ R_1 = S \circ R_2 \Rightarrow R_1 = R_2$ .

**Exercițiul 39** Fie  $R \subseteq A \times B$ . Următoarele afirmații 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)  $\forall C$  mulțime,  $\forall S_1, S_2 \subseteq B \times C, S_1 \circ R = S_2 \circ R \Rightarrow S_1 = S_2$ .

**Exercițiul 40 (Matricea booleană (de adiacență) a unei relații binare)** Fie  $\mathbb{B} = \{0, 1\}$ . Definim următoarele operații cu matrice booleene:

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

Fie relația  $\rho = (A, B, R)$ , unde  $A = \{a_1, \dots, a_m\}$ ,  $B = \{b_1, \dots, b_n\}$ . Asociem relației  $\rho$  matricea  $M_\rho \in M_{m,n}(\mathbb{B})$  care are pe 1 pe poziția  $(i, j)$  dacă și numai dacă  $(a_i, b_j) \in R$ .

Fie  $\rho = (A, B, R)$ ,  $\rho' = (A, B, R')$  și  $\sigma = (B, C, S)$ , unde  $A, B, C$  sunt mulțimi finite. Să se demonstreze:

- a)  $M_{\rho \cup \rho'} = M_\rho \vee M_{\rho'}$ ,  $M_{\rho \cap \rho'} = M_\rho \wedge M_{\rho'}$ ,  $M_{\rho^c} = \neg M_\rho$ ;
- b)  $M_{\rho^{-1}} = M_\rho^t$ ,  $M_{\sigma \circ \rho} = M_\sigma \circ M_\rho$ .

## 4.2 Funcții

**Definiția 4.2.1** a) Relația  $f = (A, B, F)$ , unde  $F \subseteq A \times B$ , se numește **funcție (relație funcțională)**, dacă pentru orice  $a \in A$ , secțiunea  $f\langle a \rangle$  are exact un element.

b) Dacă  $f = (A, B, F)$  este o funcție, atunci  $A$  se numește **domeniul de definiție** al lui  $f$ , notație  $A = \text{dom } f$ .

c) Mulțimea  $B$  este **codomeniul** lui  $f$ , notație  $B = \text{codom } f$ , iar secțiunea  $f(A)$  este **domeniul valorilor** sau **imaginea** lui  $f$ , notație  $f(A) = \text{Im } f$ .

d) Mulțimea  $F \subseteq A \times B$  este **graficul** funcției  $f$ .

Dacă  $f = (A, B, F)$  este funcție, atunci folosim următoarea notație:

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

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

**Observații 4.2.2** a) Funcțiile  $f: A \rightarrow B$  și  $f': A' \rightarrow B'$  sunt egale ( $f = f'$ ) dacă și numai dacă,  $A = A'$ ,  $B = B'$  și  $f(a) = f'(a')$  pentru orice  $a \in A$ .

b) Dacă  $A = \emptyset$ , atunci unica relație  $\rho = (A, B, R)$  este relația vidă ( $R = \emptyset$ ); aceasta este funcție pentru orice mulțime  $B$ .

Dacă  $A \neq \emptyset$  și  $B = \emptyset$ , atunci relația vidă  $\rho = (A, \emptyset, \emptyset)$  nu e funcție.

c) Dacă  $f: A \rightarrow B$  este o funcție și  $X \subseteq A, Y \subseteq B, y \in Y$ , atunci

$$f(X) = \{b \in B \mid \exists x \in X: f(x) = b\} = \{f(x) \mid x \in X\},$$

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

și

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

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

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

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

Relația compusă  $g \circ f = (A, D, G \circ F)$  este funcție dacă și numai dacă  $f(A) \subseteq C$ , adică  $\text{Im } f \subseteq \text{Dom } g$ , și atunci  $(g \circ f)(a) = g(f(a))$  pentru orice  $a \in A$ .

2) Dacă  $f: A \rightarrow B, g: B \rightarrow C, h: C \rightarrow D$  sunt funcții, atunci  $f \circ \mathbf{1}_A = \mathbf{1}_B \circ f = f$  și  $(h \circ g) \circ f = h \circ (g \circ f)$ .

**Demonstrație.** 1) „ $\Rightarrow$ ” Presupunem că  $g \circ f$  este funcție și 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 funcție), adică  $a(g \circ f)d$ , de unde rezultă că există  $c \in B \cap C$  astfel încât  $afc$  și  $cgd$ . De aici  $afc$  și  $afb$ , deoarece  $f$  este funcție, deci  $b = c \in B \cap C$ .

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

Avem

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

deci  $g \circ f$  este funcție și  $(g \circ f)(a) = g(f(a))$ .

2) Rezultă din proprietatea referitoare la relații, sau poate fi ușor demonstrată direct. ■

**Exercițiul 41** Fie  $\rho = (A, B, R)$  o relație. Să se arate că  $\rho$  este funcție dacă și numai dacă

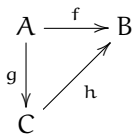
$$1_A \subseteq \rho^{-1} \circ \rho \quad \text{și} \quad \rho \circ \rho^{-1} \subseteq 1_B.$$

**Exercițiul 42** Fie  $f : A \rightarrow B$  o funcție. Să se arate că:

- Pentru orice  $X \subseteq A$  avem  $X \subseteq f^{-1}(f(X))$ ;
- Pentru orice  $Y \subseteq B$  avem  $Y \supseteq f(f^{-1}(Y))$ ;
- $f \circ f^{-1} \circ f = f$ .

### 4.2.1 Diagrame comutative

Considerăm funcțiile  $f : A \rightarrow B$ ,  $g : B \rightarrow C$  și  $h : A \rightarrow C$ , reprezentate prin următoarea diagramă:



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

$$\begin{array}{ccc} A & \xrightarrow{k} & D \\ f \downarrow & & \downarrow h \\ B & \xrightarrow{g} & C \end{array} \quad \begin{array}{ccc} A & \xrightarrow{k} & D \\ f \downarrow & & \uparrow h \\ B & \xrightarrow{g} & C \end{array}$$

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

### 4.2.2 Familie de elemente și familie de mulțimi

**Definiția 4.2.5** a) Fie  $f : I \rightarrow A$  o funcție, și fie  $F = \{(i, f(i)) \mid i \in I\}$  graficul lui  $f$ . Identificăm de multe ori funcția  $f$  cu  $F$  și 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 **mulțimea de indici**.

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

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

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

c) **Intersecția familiei de mulțimi**  $(A_i)_{i \in I}$  este mulțimea

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

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  $\exists i \in I : a \in A_i$ , și  $\bigcap_{i \in I} A_i = A$ , pentru că afirmația  $\exists i \in I : a \notin A_i$  este falsă pentru orice  $a \in A$ , deci negația ei  $\forall i \in I : a \in A_i$  este adevărată pentru orice  $a \in A$ .

**Exercițiul 43** Să se demonstreze următoarele identități (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  $i \in I, j \in J$ :

- $\bigcup_{i \in I} \bigcup_{j \in J} A_{ij} = \bigcup_{j \in J} \bigcup_{i \in I} A_{ij}$ ;
- $\bigcap_{i \in I} \bigcap_{j \in J} A_{ij} = \bigcap_{j \in J} \bigcap_{i \in I} A_{ij}$ ;
- $\mathcal{C}(\bigcup_{i \in I} A_i) = \bigcap_{i \in I} \mathcal{C}(A_i)$ ;
- $\mathcal{C}(\bigcap_{i \in I} A_i) = \bigcup_{i \in I} \mathcal{C}(A_i)$ ;
- $(\bigcup_{i \in I} A_i) \cup (\bigcup_{i \in I} B_i) = \bigcup_{i \in I} (A_i \cup B_i)$ ;
- $\bigcup_{j \in J} (A \cap B_j) = A \cap (\bigcup_{j \in J} B_j)$ ;
- $\bigcap_{j \in J} (A \cup B_j) = A \cup (\bigcap_{j \in J} B_j)$ ;
- $\bigcup_{i \in I} (\bigcap_{j \in J} A_{ij}) \subseteq \bigcap_{j \in J} (\bigcup_{i \in I} A_{ij})$ ;
- $(\bigcup_{i \in I} A_i) \cap (\bigcup_{j \in J} B_j) = \bigcup_{(i,j) \in I \times J} (A_i \cap B_j)$ ;
- $(\bigcap_{i \in I} A_i) \cup (\bigcap_{j \in J} B_j) = \bigcap_{(i,j) \in I \times J} (A_i \cup B_j)$ .

**Exercițiul 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)  $(\bigcup_{i \in I} X_i) \times (\bigcup_{j \in J} Y_j) = \bigcup_{(i,j) \in I \times J} (X_i \times Y_j)$ .

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

**Exercițiul 46** Fie  $f : A \rightarrow B$  o funcție și  $X_i \subseteq A$ ,  $Y_i \subseteq B \forall i \in I$ . 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)  $f^{-1}(\bigcap_{i \in I} Y_i) = \bigcap_{i \in I} f^{-1}(Y_i)$ .

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

**Exercițiul 48** Fie relațiile  $\rho_i = (A, B, R_i)$ ,  $i \in I$  și  $\sigma = (C, D, S)$ . 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 Funcții injective, surjective și bijective

**Definiția 4.3.1** Fie  $f : A \rightarrow B$  o funcție. 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 și surjectivă, sau echivalent, dacă  $\forall y \in B$  există unic  $x \in A$  astfel ca  $f(x) = y$ .

**Exemplul 4.3.2** 1) Funcția  $f : \mathbb{R} \rightarrow \mathbb{R}$ ,  $f(x) = x^2$  nu e injectivă, pentru că de exemplu  $-1 \neq 1$  și  $f(-1) = f(1) = 1$ ; nu e nici surjectivă, pentru că de exemplu  $y = -1 \in \mathbb{R}$ , dar nu există  $x \in \mathbb{R}$  astfel încât  $f(x) = x^2 = -1$ .

Funcția  $g : [0, \infty) \rightarrow \mathbb{R}$ ,  $g(x) = x^2$  este injectivă și nu e surjectivă, funcția  $h : [0, \infty) \rightarrow [0, \infty)$ ,  $h(x) = x^2$  este injectivă și surjectivă, deci bijectivă.

2) Pentru orice mulțime  $A$ , relația diagonală  $\mathbf{1}_A = (A, A, \Delta_A)$  este funcție bijectivă.

3) Proiecția canonică  $p_j : \prod_{i \in I} A_i \rightarrow A_j$  este surjectivă, și injecția canonică  $p_j : A_j \rightarrow \prod_{i \in I} A_i$  este funcție injectivă.

**Teorema 4.3.3 (caracterizarea funcțiilor injective)** Fie  $f : A \rightarrow B$  o funcție. Următoarele afirmații sunt echivalente:

- (i)  $f$  este injectivă  
 (ii) pentru orice mulțime  $A'$  și pentru orice funcții  $\alpha, \beta : A' \rightarrow A$ , 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 funcție  $r : B \rightarrow A$  astfel încât  $r \circ f = \mathbf{1}_A$ .

**Demonstrație.** (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 afirmația (ii) este adevărată și 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  $A' = \{x_1, x_2\}$  și  $\alpha, \beta : A' \rightarrow A, \alpha(x_1) = x_1, \alpha(x_2) = x_2, \beta(x_1) = x_1, \beta(x_2) = x_1$ . Atunci  $\alpha \neq \beta$ , dar  $f \circ \alpha = f \circ \beta$ , pentru că

$$\begin{aligned} (f \circ \alpha)(x_1) &= f(\alpha(x_1)) = f(x_1) = f(\beta(x_1)) = (f \circ \beta)(x_1), \\ (f \circ \alpha)(x_2) &= f(\alpha(x_2)) = f(x_2) = f(x_1) = f(\beta(x_2)) = (f \circ \beta)(x_2), \end{aligned}$$

deci avem o contradicție.

(i)  $\Rightarrow$  (iii) Presupunem că  $f$  injectiv și  $a_0 \in A$ . Considerăm funcția

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

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

(iii)  $\Rightarrow$  (i) Dacă există o funcție  $r : B \rightarrow A$  astfel încât  $r \circ f = \mathbf{1}_A$  și 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 funcțiilor surjective)** Fie  $f : A \rightarrow B$  o funcție. Următoarele afirmații sunt echivalente:

- (i)  $f$  este surjectivă;
- (ii) pentru orice mulțime  $B'$  și pentru orice funcții  $\alpha, \beta : B \rightarrow B'$  dacă  $\alpha \circ f = \beta \circ f$ , atunci  $\alpha = \beta$  (adică cu  $f$  se poate simplifica la dreapta);
- (iii)  $f$  are inversă la dreapta (secțiune), adică există o funcție  $s : B \rightarrow A$  pentru care  $f \circ s = \mathbf{1}_B$ .

**Demonstrație.** (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 afirmația (ii) este adevărată și că  $f$  nu e surjectiv, adică există  $b_0 \in B \setminus f(A)$ . Fie  $A \neq \emptyset, B' = B$  și considerăm funcțiile  $\alpha, \beta : B \rightarrow B$ , unde  $\alpha = \mathbf{1}_B$  și

$$\beta(b) = \begin{cases} b, & \text{dacă } b \neq b_0, \\ b'_0, & \text{dacă } b = b_0, \end{cases}$$

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 contradicție.

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

(i)  $\Rightarrow$  (iii) Presupunem că funcția  $f$  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 obținem o funcție  $s : B \rightarrow A$ ,  $s(b) = a$ , și avem

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

adică  $f \circ s = \mathbf{1}_B$ .

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

**Teorema 4.3.5 (caracterizarea funcțiilor bijective)** Fie  $f : A \rightarrow B$  o funcție. Următoarele afirmații sunt echivalente:

- (i)  $f$  este funcție bijectivă;
- (ii) relația inversă  $f^{-1}$  este funcție și avem  $f^{-1} \circ f = \mathbf{1}_A$ ,  $f \circ f^{-1} = \mathbf{1}_B$ ;
- (iii)  $f$  are inversă, adică există o funcție  $g : B \rightarrow A$ , astfel ca

$$g \circ f = \mathbf{1}_A, \quad f \circ g = \mathbf{1}_B.$$

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

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

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

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

**Observații 4.3.6** Dacă  $f$  este funcție bijectivă, atunci și funcția  $f^{-1}$  este bijectivă, deoarece  $(f^{-1})^{-1} = f$ .

**Exercițiul 49** Fie  $f : A \rightarrow B$  și  $g : B \rightarrow C$  două funcții. Să se arate că:

- a) Dacă  $f$  și  $g$  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 și  $f$  este surjectiv, atunci  $g$  este injectiv;
- d) Dacă  $g \circ f$  este surjectiv și  $g$  este injectiv, atunci  $f$  este surjectiv.

**Exercițiul 50** Fie  $f : A \rightarrow B$  o funcție,  $X_1, X_2 \subseteq A$ ,  $(X_i)_{i \in I}, X_i \subseteq A$ , și  $Y_1, Y_2 \subseteq B$ . 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)  $f(\bigcap_{i \in I} X_i) = \bigcap_{i \in I} f(X_i)$ .



**Exercițiul 51** Fie  $f : A \rightarrow B$  o funcție.

a) Să se arate că următoarele afirmații sunt echivalente:

- (i)  $f$  este injectiv;
- (ii)  $f^{-1} \circ f = \mathbf{1}_A$ ;
- (iii)  $\forall X \subseteq A \ f^{-1}(f(X)) = X$ ;
- (iv)  $\forall X \subseteq A \ f(\mathcal{C}(X)) \subseteq \mathcal{C}f(X)$ ;
- (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 afirmații sunt echivalente:

- (i)  $f$  este surjectiv;
- (ii)  $f \circ f^{-1} = \mathbf{1}_B$ ;
- (iii)  $\forall Y \subseteq B \ f(f^{-1}(Y)) = Y$ ;
- (iv)  $\forall X \subseteq A \ \mathcal{C}f(X) \subseteq f(\mathcal{C}(X))$ .

**Exercițiul 52** Fie  $f : A \rightarrow B$  o funcție.

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

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

**Exercițiul 53** Fie  $A \neq \emptyset$  și  $f : A \rightarrow B$  o funcție. Să se demonstreze că există  $g : B \rightarrow A$  astfel încât  $f \circ g \circ f = f$ .

### 4.3.1 Produsul direct al unei familii de mulțimi și al unei familii de funcții

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

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

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

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

se numește **proiecția canonică**, și 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  $(f_i : A_i \rightarrow A'_i)_{i \in I}$  este o familie de funcții, atunci

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

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

Observăm că  $\prod_{i \in I} A_i$  este nevidă dacă și numai dacă  $I \neq \emptyset$  și  $A_i \neq \emptyset$  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  $f_i : A_i \rightarrow A'_i$ ,  $i = 1, 2$ , atunci

$$f_1 \times f_2 : A_1 \times A_2 \rightarrow A'_1 \times A'_2, \quad (f_1 \times f_2)(a_1, a_2) = (f_1(a_1), f_2(a_2)).$$

**Exercițiul 54** Fie funcțiile  $f : A \rightarrow A'$ ,  $g : B \rightarrow B'$ ,  $f' : A' \rightarrow A''$  și  $g' : B' \rightarrow B''$ . Să se demonstreze:

- a)  $\mathbf{1}_A \times \mathbf{1}_B = \mathbf{1}_{A \times B}$ ;
- b)  $(f' \times g') \circ (f \times g) = (f' \circ f) \times (g' \circ g)$ ;
- c)  $\forall X \subseteq A$  și  $\forall Y \subseteq B \ (f \times g)(X \times Y) = f(X) \times g(Y)$ ;
- d)  $\forall X' \subseteq A'$  și  $\forall Y' \subseteq B' \ (f \times g)^{-1}(X' \times Y') = f^{-1}(X') \times g^{-1}(Y')$ ;
- e) nu orice submulțime  $M \subseteq A \times B$  este de forma  $X \times Y$ , unde  $X \subseteq A$  și  $Y \subseteq B$ , și nu orice funcție  $\varphi : A \times B \rightarrow A' \times B'$  este de forma  $f \times g$ .

**Exercițiul 55** Fie  $(A_i)_{i \in I}$ ,  $(A'_i)_{i \in I}$  și  $(A''_i)_{i \in I}$  familii de mulțimi,  $(f_i : A_i \rightarrow A'_i)_{i \in I}$  și  $(f'_i : A'_i \rightarrow A''_i)_{i \in I}$  familii de funcții. Să se demonstreze :

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

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

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

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

**Exercițiul 56** Fie  $f : A \rightarrow A'$ ,  $g : B \rightarrow B'$  funcții și  $(f_i : A_i \rightarrow A'_i)_{i \in I}$  o familie de funcții. Să se arate că:

a)  $f$  și  $g$  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 mulțimi și a unei familii de funcții

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

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

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

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

se numește **injectia 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  $(f_i : A_i \rightarrow A'_i)_{i \in I}$  este o familie de funcții, atunci

$$\prod_{i \in I} f_i : \prod_{i \in I} A_i \rightarrow \prod_{i \in I} A'_i, \quad (\prod_{i \in I} f_i)(a_i, i) = (f_i(a_i), i)$$

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

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

**Exercițiul 57** Fie funcțiile  $f : A \rightarrow A'$ ,  $g : B \rightarrow B'$ ,  $f' : A' \rightarrow A''$  și  $g' : B' \rightarrow B''$ . Să se demonstreze:

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

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

**Exercițiul 58** Fie  $(A_i)_{i \in I}$ ,  $(A'_i)_{i \in I}$  și  $(A''_i)_{i \in I}$  familii de mulțimi,  $(f_i : A_i \rightarrow A'_i)_{i \in I}$  și  $(f'_i : A'_i \rightarrow A''_i)_{i \in I}$  familii de funcții. Să se demonstreze :

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

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

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

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

**Exercițiul 59** Fie  $f : A \rightarrow A'$ ,  $g : B \rightarrow B'$  funcții și  $(f_i : A_i \rightarrow A'_i)_{i \in I}$  o familie de funcții. Să se arate că:

a) Dacă  $f$  și  $g$  sunt injective (surjective), atunci  $f \coprod g$  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 Mulțimea $\text{Hom}(A, B)$ și funcția $\text{Hom}(f, g)$

Dacă  $A$  și  $B$  mulțimi, atunci notăm  $\text{Hom}(A, B)$  mulțimea funcțiilor  $f : A \rightarrow B$ :

$$\text{Hom}(A, B) = \{f \mid f : A \rightarrow B\}.$$

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

Fie  $f : A' \rightarrow A$ ,  $g : B \rightarrow B'$  funcții; definim următoarea funcție:

$$\text{Hom}(f, g) : \text{Hom}(A, B) \rightarrow \text{Hom}(A', B'), \quad \text{Hom}(f, g)(\alpha) = g \circ \alpha \circ f,$$

deci următoarea diagramă este comutativă.

$$\begin{array}{ccc} A' & \xrightarrow{f} & A \\ (g^f)(\alpha) \downarrow & & \downarrow \alpha \\ B' & \xleftarrow{g} & B \end{array}$$

Folosim și notațiile  $\text{Hom}(A, B) = B^A$  și  $\text{Hom}(f, g) = g^f$ .

**Exercițiul 60** Fie funcțiile  $f : A' \rightarrow A$ ,  $g : B \rightarrow B'$ ,  $f' : A'' \rightarrow A'$  și  $g' : B' \rightarrow B''$ .

a) Dacă  $A' = B' = \{1, 2, 3\}$  și  $A = B = \{1, 2\}$ ,  $f(1) = f(2) = 1$ ,  $f(3) = 2$ ,  $g(1) = 2$  și  $g(2) = 3$ , să se determine funcția  $\text{Hom}(f, g)$ .

Să se demonstreze:

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

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

**Exercițiul 61** Fie  $f : A' \rightarrow A$  și  $g : B \rightarrow B'$  două funcții. Să se arate că:

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

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

c)  $g$  este injectiv dacă și numai dacă pentru orice mulțime  $A$ ,  $\text{Hom}(\mathbf{1}_A, g) : \text{Hom}(A, B) \rightarrow \text{Hom}(A, B')$  este injectiv;

d)  $f$  este surjectiv dacă și numai dacă pentru orice mulțime  $B$ ,  $\text{Hom}(f, \mathbf{1}_B) : \text{Hom}(A, B) \rightarrow \text{Hom}(A', B)$  este injectiv. •

### 4.3.4 Mulțimea părților și funcția caracteristică a unei submulțimi

Amintim că mulțimea părților unei mulțimi  $A$  este mulțimea  $\mathcal{P}(A) = \{X \mid X \subseteq A\}$ , adică avem  $X \in \mathcal{P}(A) \iff X \subseteq A$ . O funcție  $f : A \rightarrow B$  induce funcțiile

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

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

**Exercițiul 62** Fie  $f : A \rightarrow B$  și  $g : B \rightarrow C$  funcții. 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  $\varphi = f^* \circ f_*$  și  $\psi = f_* \circ f^*$ , atunci  $\varphi \circ \varphi = \varphi$  și  $\psi \circ \psi = \psi$ .

**Exercițiul 63** Fie  $f : A \rightarrow B$  o funcție.

a) Următoarele afirmații 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 afirmații sunt echivalente:

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

**Exercițiul 64** Fie  $A$  și  $B$  două mulțimi și definim funcția

$$\varphi_{A, B} : \mathcal{P}(A \times B) \rightarrow \text{Hom}(A, \mathcal{P}(B)), \quad \varphi_{A, B}(R)(a) = R\langle a \rangle,$$

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

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

b) Fie  $f : A \rightarrow A'$  și  $g : B \rightarrow B'$  două funcții. Să se arate că următoarea diagramă este comutativă:

$$\begin{array}{ccc} \mathcal{P}(A \times B) & \xrightarrow{\varphi_{A,B}} & \text{Hom}(A, \mathcal{P}(B)) \\ (f \times g)^* \uparrow & & \uparrow \text{Hom}(f, g^*) \\ \mathcal{P}(A' \times B') & \xrightarrow{\varphi_{A',B'}} & \text{Hom}(A', \mathcal{P}(B')) \end{array}$$

**Observație.** Acest exercițiu spune că o relație  $\rho = (A, B, R)$  se identifică în mod canonic cu o funcție multivocă  $f : A \rightarrow \mathcal{P}(B)$ .

**Definiția 4.3.7** Fie  $A$  o mulțime și  $X \subseteq A$ . Funcția

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

se numește **funcția caracteristică** a submulțimii  $X$ . Astfel am definit funcția

$$\varphi_A : \mathcal{P}(A) \rightarrow \text{Hom}(A, \{0, 1\}), \quad \varphi_A(X) = \chi_X$$

**Exercițiul 65** Fie  $A$  o mulțime. Să se arate că:

- Funcția  $\varphi_A$  este bijectivă și avem  $\varphi_A^{-1}(\chi) = \chi^{-1}(1)$ , pentru orice funcție  $\chi : A \rightarrow \{0, 1\}$ ;
- Fie  $f : A \rightarrow B$  o funcție. Să se arate că următoarea diagramă este comutativă:

$$\begin{array}{ccc} \mathcal{P}(A) & \xrightarrow{\varphi_A} & \text{Hom}(A, \{0, 1\}) \\ f^* \uparrow & & \uparrow \text{Hom}(f, \mathbf{1}_{\{0,1\}}) \\ \mathcal{P}(B) & \xrightarrow{\varphi_B} & \text{Hom}(B, \{0, 1\}) \end{array}$$

**Exercițiul 66** Dacă  $X, Y \subseteq A$ , atunci:

- $X \subseteq Y \Leftrightarrow \chi_X(x) \leq \chi_Y(x), \quad \forall x \in A,$
- $\chi_{\bar{X}}(x) = 1 - \chi_X(x), \quad \forall x \in A,$
- $\chi_{X \cap Y}(x) = \chi_X(x)\chi_Y(x), \quad \forall x \in A,$
- $\chi_{X \cup Y}(x) = \chi_X(x) + \chi_Y(x) - \chi_X(x)\chi_Y(x), \quad \forall x \in A,$
- $\chi_{X \setminus Y}(x) = \chi_X(x)(1 - \chi_Y(x)), \quad \forall x \in A,$
- $\chi_{X \Delta Y}(x) = \chi_X(x) + \chi_Y(x) - 2\chi_X(x)\chi_Y(x), \quad \forall x \in A.$

**Observații 4.3.8** Proprietățile de mai sus ale funcției caracteristice sunt utile la demonstrarea egalităților de mulțimi. De exemplu, să aratăm că  $(X \Delta Y) \Delta Z = X \Delta (Y \Delta Z)$ :

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

Calculând analog  $\chi_{X \Delta (Y \Delta Z)}$  obținem aceeași expresie (\*). Altfel, din comutativitatea lui  $\Delta$  și 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 Relații de echivalență

### 4.4.1 Clase importante de relații omogene

**Definiția 4.4.1** Fie  $\rho = (A, A, R)$  o relație omogenă. Spunem că

- $\rho$  este **reflexiv**, dacă pentru orice  $x \in A$ ,  $x\rho x$ , adică

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

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

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

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

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

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

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

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

$\rho$  este **asimetric**, dacă pentru orice  $x, y \in A$ ,  $x\rho y$  implică  $y \notin \rho x$ ;

e)  $\rho$  este **relație de preordine**, dacă  $\rho$  este reflexiv și tranzitiv. Atunci spunem că  $(A, \rho)$  este **mulțime preordonată**;

f)  $\rho$  este **relație de echivalență**, dacă  $\rho$  este reflexiv, tranzitiv și simetric. Notăm  $\mathcal{E}(A)$  mulțimea relațiilor de echivalență definite pe  $A$ ;

g)  $\rho$  este **relație de ordine**, dacă  $\rho$  este reflexiv, tranzitiv și antisimetric. Atunci spunem că  $(A, \rho)$  este **mulțime ordonată**;

h)  $\rho$  este **relație de ordine strictă**, dacă  $\rho$  este ireflexiv și tranzitiv.

**Observații 4.4.2** Sunt ușor de demonstrat următoarele afirmații:

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

**Exemplul 4.4.3** 1) Pe mulțimea numerelor întregi  $\mathbb{Z}$ , relația de divizibilitate este relație de preordine, nu e simetrică și nu e antisimetrică, pentru că de exemplu  $3|-3$  și  $-3|3$ , dar  $-3 \neq 3$ .

2) Pe mulțimea numerelor naturale  $\mathbb{N}$  relația de divizibilitate este relație de ordine, deci  $(\mathbb{N}, |)$  este mulțime ordonată.

3) Pe mulțimea numerelor întregi  $\mathbb{Z}$ , relația de congruență definită prin  $a \equiv b \pmod{n} \Leftrightarrow n|a - b$  este relație de echivalență.

4) Relația universală  $(A, A, A \times A)$  este relație de echivalență.

5) Restricția la o submulțime a unei relații de echivalență este relație de echivalență. Mai exact, dacă  $\rho = (A, A, R)$  este relație de echivalență pe  $A$ , iar  $B \subseteq A$ , atunci  $(B, B, R \cap (B \times B))$  este relație de echivalență pe  $B$ .

## 4.4.2 Echivalențe și partiții

**Definiția 4.4.4** Dacă  $\rho$  este relație de echivalență pe mulțimea  $A$ , atunci secțiunea

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

după elementul  $x \in A$  se numește **clasă de echivalență**. Mulțimea acestor clase se numește **mulțimea factor modulo  $\rho$** :

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

**Exemplul 4.4.5** 1) Pe mulțimea  $\mathbb{Z}$  relației de congruență  $a \equiv b \pmod{n}$  (unde  $n \neq 0$ ) îi corespunde mulțimea 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)  $A/1_A = \{\{x\} : x \in A\}$  și  $A/(A \times A) = \{A\}$ .

**Lema 4.4.6** Dacă  $\rho$  este o relație de echivalență mulțimea  $A$  și  $x, y \in A$ , atunci sunt echivalente următoarele afirmații:

$$(i) \ x\rho y; \quad (ii) \ y \in \rho(x); \quad (iii) \ \rho(x) = \rho(y).$$

**Demonstrație.** (i)  $\Leftrightarrow$  (ii) este evident din definiție.

(i)  $\Rightarrow$  (iii) Fie  $x\rho y$  și fie  $z \in \rho(x)$ . Atunci  $x\rho y$  și  $x\rho z \Rightarrow z\rho x$  și  $x\rho y$  (pentru că  $\rho$  simetric), deci  $z\rho y$  (pentru că  $\rho$  tranzitiv)  $\Rightarrow z \in \rho(y)$ , deci  $\rho(x) \subseteq \rho(y)$ . Analog,  $\rho(y) \subseteq \rho(x)$ , deci (iii) are loc.

(iii)  $\Rightarrow$  (i) Dacă  $\rho(x) = \rho(y)$ , atunci  $y \in \rho(y) = \rho(x) \Rightarrow y\rho x \Rightarrow x\rho y$ .

**Definiția 4.4.7** Fie  $A$  o mulțime nevidă și  $\pi \subseteq \mathcal{P}(A) \setminus \{\emptyset\}$ .

a) Spunem că  $\pi$  este o **partiție** a lui  $A$  dacă

$$(1) \ A = \bigcup_{B \in \pi} B \text{ și}$$

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

Dacă  $B \in \pi$  și  $b \in B$ , atunci spunem că  $b$  este un **reprezentant** al lui  $B$ . Notăm prin  $\mathcal{P}(A)$  mulțimea partițiilor lui  $A$ .

b) Dacă  $\pi_1, \pi_2 \in \mathcal{P}(A)$ , atunci  $\pi_1$  este **mai fin** ca  $\pi_2$  (notație:  $\pi_1 \leq \pi_2$ ) dacă

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

adică dacă a orice submulțime din partiția mai fină  $\pi_1$  este conținută de o submulțime din partiția  $\pi_2$ .

Relațiile de echivalență și partițiile se determină reciproc.

**Teorema 4.4.8** Fie  $A$  o mulțime nevidă .

1) Dacă  $\rho$  relație de echivalență pe  $A$ , atunci mulțimea factor

$$A/\rho = \{\rho(x) \mid x \in A\}$$

este partiție a lui  $A$ .

2) Fie  $\pi \subseteq \mathcal{P}(A) \setminus \{\emptyset\}$  partiție a lui  $A$  și definim relația

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

adică  $x\rho_\pi y \Leftrightarrow \exists B \in \pi : x, y \in B$ .

Atunci  $\rho_\pi$  este relație de echivalență pe  $A$ .

3) Considerăm funcțiile

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

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

Atunci  $\psi \circ \phi = \mathbf{1}_{\mathcal{E}(A)}$  și  $\phi \circ \psi = \mathbf{1}_{\mathcal{P}(A)}$ .

4) Dacă  $\rho_1 \subseteq \rho_2$ , atunci  $\phi(\rho_1) \subseteq \phi(\rho_2)$ . Invers, dacă  $\pi_1 \leq \pi_2$ , atunci  $\psi(\pi_1) \subseteq \psi(\pi_2)$ .

**Demonstrație.** 1) Arătăm că  $A = \bigcup_{x \in A} \rho(x)$ . Incluziunea „ $\supseteq$ ” este evidentă, pentru că  $\rho(x) \subseteq A$  pentru orice  $x \in A$ . Mai departe, pentru orice  $y \in A$ ,  $y \in \rho(y)$  (pentru că  $\rho$  este reflexiv), deci  $y \in \bigcup_{x \in A} \rho(x)$ , de unde rezultă incluziunea „ $\subseteq$ ”.

Presupunem acum că  $\rho(x) \cap \rho(y) \neq \emptyset$ , unde  $x, y \in A$ . Arătăm că atunci clasele  $\rho(x)$  și  $\rho(y)$  sunt egale. Într-adevăr, din ipoteză  $\exists u \in \rho(x) \cap \rho(y) \Rightarrow x\rho u$  și  $y\rho u \Rightarrow x\rho u$  și  $u\rho y$  (pentru că  $\rho$  este simetric)  $\Rightarrow x\rho y$  ( $\rho$  tranzitiv)  $\Rightarrow \rho(x) = \rho(y)$  conform Lemei 4.4.6.

2)  $\rho_\pi$  este reflexiv, pentru că  $\forall x \in A = \bigcup_{B \in \pi} B \Rightarrow \exists B \in \pi : x \in B \Rightarrow (x, x) \in B \times B \Rightarrow x\rho_\pi x$ .

$\rho_\pi$  este tranzitiv, pentru că  $\forall x, y, z \in A : x\rho_\pi y$  și  $y\rho_\pi z \Rightarrow \exists B, C \in \pi : x, y \in B$  și  $y, z \in C$ . Deci  $y \in B \cap C$ , și obținem  $B = C$  (pentru că  $B \neq C$ , conform definiției  $B \cap C = \emptyset$ , contradicție). Deci  $x, z \in B = C \Rightarrow x\rho_\pi z$ .

Mai departe,  $\rho_\pi$  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  $\rho$  este relație de echivalență.

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,

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

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

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

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

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

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

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

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

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

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

$$\begin{aligned} x\rho_{\pi_1} y &\Rightarrow \exists B_1 \in \pi_1 : x, y \in B_1 \Rightarrow \\ &\Rightarrow \exists B_2 \in \pi_2 : B_1 \subseteq B_2 \text{ și } x, y \in B_1 \subseteq B_2 \Rightarrow x\rho_{\pi_2} y. \end{aligned}$$

**Exercițiul 67** Fie  $\rho = (A, B, R)$  o relație. Să se demonstreze:

- Dacă  $\rho$  este reflexiv, simetric și antisimetric, atunci  $\rho = \mathbf{1}_A$ ;
- Dacă  $\rho$  este reflexiv și tranzitiv, atunci  $\rho^2 = \rho$ .

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

- Dacă  $\rho = \{(1, 1), \dots, (4, 4), (1, 2), (2, 1), (3, 2), (2, 3), (1, 3), (3, 1)\}$ , să se determine partiția corespunzătoare.
- Dacă  $\pi = \{\{1, 2\}, \{3\}, \{4\}\}$ , să se determine relația de echivalență corespunzătoare.

**Exercițiul 69** Să se determine toate relațiile de echivalență pe o mulțime cu 1, 2, 3, respectiv 4 elemente.

**Exercițiul 70** Să se arate că:

- $(\mathbb{Z}, |)$  este mulțime preordonată, „|” nu e simetric și nu e antisimetric;
- $(\mathbb{N}, |)$  este mulțime ordonată;

**Exercițiul 71** Pe mulțimea  $\mathbb{C}$  a numerelor complexe considerăm relațiile  $\rho_1$  și  $\rho_2$ , unde  $z\rho_1 w \Leftrightarrow |z| = |w|$  și  $z\rho_2 w \Leftrightarrow z = w = 0$  sau  $\arg z = \arg w$ . Să se arate că  $\rho_1$  și  $\rho_2$  sunt relații de echivalență și să se reprezinte grafic clasele din  $\mathbb{C}/\rho_1$  și  $\mathbb{C}/\rho_2$ .

**Exercițiul 72** Fie  $\rho_1$  și  $\rho_2$  două relații de echivalență pe mulțimea  $A$ . Să se demonstreze:

- $\rho_1^{-1}$  și  $\rho_1 \cap \rho_2$  sunt relații de echivalență. (Mai general, dacă  $(\rho_i)_{i \in I}$  sunt relații de echivalență pe  $A$ , atunci  $\bigcap_{i \in I} \rho_i$  este relație de echivalență pe mulțimea  $A$ .)
- $\mathcal{C}\rho_1$  și  $\rho_1 \cup \rho_2$  în general nu sunt relații de echivalență;
- $\rho_1 \circ \rho_2$  este relație de echivalență dacă și 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 relație de echivalență ce conține pe  $\rho_1$  și  $\rho_2$ .

**Exercițiul 73** Fie  $\rho_1$  și  $\rho_2$  două relații pe mulțimea  $A$ .

- Să se arate că  $(\rho_1 \cup \rho_2)^2 = \rho_1^2 \cup \rho_2^2 \cup (\rho_1 \circ \rho_2) \cup (\rho_2 \circ \rho_1)$ .
- Presupunem că  $\rho_1$  și  $\rho_2$  sunt relații de echivalență. Să se arate că  $\rho_1 \cup \rho_2$  relație de echivalență dacă și numai dacă  $\rho_1 \circ \rho_2$  și  $\rho_2 \circ \rho_1$  sunt subrelații ale lui  $\rho_1 \cup \rho_2$ .

**Exercițiul 74** Fie  $\rho = (A, A, R)$  o relație,  $\rho^0 = \mathbf{1}_A$ ,  $\rho^n = \rho \circ \dots \circ \rho$  (de  $n$  ori), și fie  $\bar{\rho} = \mathbf{1}_A \cup \rho \cup \rho^{-1}$ . Să se arate că:

- $\bigcup_{n \geq 1} \rho^n$  este cea mai mică relație tranzitivă ce conține pe  $\rho$ ;
- $\bigcup_{n \geq 1} \bar{\rho}^n$  este cea mai mică relație de echivalență ce conține pe  $\rho$ .

## 4.5 Teoreme de factorizare a funcțiilor

**Definiția 4.5.1** a) Fie  $f : A \rightarrow B$  o funcție. Relația  $\ker f$  pe mulțimea  $A$  definită prin

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

se numește **nucleul** lui  $f$ .

- Fie  $\rho$  o relație de echivalență pe mulțimea  $A$ . Funcția

$$p_\rho : A \rightarrow A/\rho, \quad p_\rho(x) = \rho(x)$$

se numește **proiecția canonică** a lui  $A$  în mulțimea factor  $A/\rho$ .

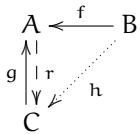
Este ușor de arătat că relația  $\ker f$  este relație de echivalență pe  $A$ , iar proiecția canonică  $p_\rho : A \rightarrow A/\rho$  este funcție surjectivă și avem  $\ker p_\rho = \rho$ .

**Exercițiul 75** Dacă  $f : A \rightarrow B$  este o funcție, atunci

- 1)  $\ker f$  este relație de echivalență pe  $A$  și  $\ker f = f^{-1} \circ f$ ,
- 2)  $A/\ker f = \{f^{-1}(b) \mid b \in \text{Im } f\}$ ,
- 3)  $f$  este injectiv  $\Leftrightarrow \ker f = \mathbf{1}_A$ ,
- 4)  $f$  este surjectiv  $\Leftrightarrow \text{Im } f = B$ .
- 5)  $f \circ f^{-1} = \Delta_{\text{Im } f}$ , unde  $\Delta_{\text{Im } f} = \{(b, b) \in \Delta \times \Delta \mid b \in \text{Im } f\}$ .

**Exercițiul 76** Dacă  $\rho$  este o relație de echivalență pe  $A$ , atunci proiecția canonică  $p_\rho : A \rightarrow A/\rho$  este surjectivă și avem  $\ker p_\rho = \rho$ .

**Teorema 4.5.2 (factorizare după o funcție injectivă)** Fie  $f : B \rightarrow A$  o funcție și  $g : C \rightarrow A$  o funcție injectivă.



- 1) Există o funcție  $h : B \rightarrow C$ , astfel încât  $f = g \circ h$  dacă și numai dacă  $\text{Im } f \subseteq \text{Im } g$ . Atunci:
- 2)  $h$  este unic determinat și dacă  $C \neq \emptyset$ , atunci  $h = r \circ f$ , unde  $r$  este o inversă la stânga a lui  $g$ ,
- 3)  $h$  este surjectiv dacă și numai dacă  $\text{Im } f = \text{Im } g$ ,
- 4)  $\ker h = \ker f$ . (În particular,  $h$  este injectiv  $\Leftrightarrow f$  este injectiv.)

**Demonstrație.** 1) Presupunem că există o funcție  $h : B \rightarrow C$  astfel încât  $f = g \circ h$ . Atunci pentru orice  $a \in A$ ,  $a \in \text{Im } f \Rightarrow \exists b \in B : a = f(b) = g(h(b)) \Rightarrow a \in \text{Im } g$ , deci  $\text{Im } f \subseteq \text{Im } g$ .

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

2) unicitatea lui  $h$ : dacă  $h, h' : B \rightarrow C$  sunt funcții, 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  $\Leftrightarrow \text{Im } g \subseteq \text{Im } f$ .

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

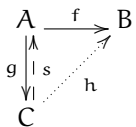
„ $\Leftarrow$ ” Pentru orice  $c \in C, g(c) \in \text{Im } g \subseteq \text{Im } f \Rightarrow \exists b \in B : g(c) = f(b) \Rightarrow \exists b \in B : h(b) = r(f(b)) = r(g(c)) = (r \circ g)(c) = c$ , deci  $h$  este surjectiv.

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

**Exercițiul 77** a) Fie  $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = \cos x, C = [-2, +\infty)$  și  $g : C \rightarrow \mathbb{R}, g(x) = 2x + 1$ . Să se determine o funcție  $h : \mathbb{R} \rightarrow C$  astfel încât  $f = g \circ h$ .

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

**Teorema 4.5.3 (factorizare după o funcție surjectivă)** Fie  $f : A \rightarrow B$  o funcție și  $g : A \rightarrow C$  o funcție surjectivă.



- 1) Există o funcție  $h : C \rightarrow B$  astfel încât  $f = h \circ g$ , dacă și numai dacă  $\ker g \subseteq \ker f$ . Atunci:
- 2)  $h$  este unic determinat și  $h = f \circ s$ , unde  $s$  este o inversă la dreapta a lui  $g$ ,
- 3)  $h$  este injectiv dacă și numai dacă  $\ker f = \ker g$ ,
- 4)  $\text{Im } h = \text{Im } f$ . (În particular,  $h$  este surjectiv  $\Leftrightarrow f$  este surjectiv.)



**Demonstrație.** 1) Presupunem că există o funcție  $h : C \rightarrow B$  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 dreapta a lui  $g$ , adică  $s : C \rightarrow A, g \circ s = \mathbf{1}_C$ , 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  $h, h' : C \rightarrow B$  sunt funcții 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  $x_1, x_2 \in A, x_1 \ker f \ x_2 \Rightarrow f(x_1) = f(x_2) \Rightarrow h(g(x_1)) = h(g(x_2)) \Rightarrow g(x_1) = g(x_2) \Rightarrow x_1 \ker g \ x_2$ .

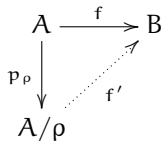
„ $\Leftarrow$ ” Presupunem acum că  $\ker f \subseteq \ker g$ . Atunci pentru orice  $z_1, z_2 \in C$ , din  $h(z_1) = h(z_2)$  rezultă că există  $x_1, x_2 \in A$  astfel încât  $z_1 = g(x_1), z_2 = g(x_2), \Rightarrow \exists x_1, x_2 \in A : f(x_1) = h(g(x_1)) = h(g(x_2)) = f(x_2)$ , deci  $g(x_1)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

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

**Exercițiul 78** a) Fie  $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = \cos x$  și  $g : \mathbb{R} \rightarrow \mathbb{R}_+, g(x) = x^2$ . Să se determine o funcție  $h : \mathbb{R}_+ \rightarrow \mathbb{R}$  astfel încât  $f = h \circ g$ .

b) Aceeași problemă dacă  $f(x) = \sin x$  și  $g(x) = x^2$ .

**Corolar 4.5.4 (factorizare după o proiecție canonică)** Fie  $f : A \rightarrow B$  o funcție și  $\rho$  o relație de echivalență pe mulțimea  $A$ .



1) Există o funcție  $f' : A/\rho \rightarrow B$  astfel încât  $f = f' \circ \text{p}_\rho$  dacă și numai dacă  $\rho \subseteq \ker f$ . Atunci:

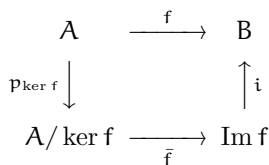
2)  $f'(\rho(x)) = f(x)$  pentru orice  $x \in A$ ,

3)  $f'$  este injectiv dacă și numai dacă  $\rho = \ker f$ ,

4)  $\text{Im } f' = \text{Im } f$ .

**Demonstrație.** În Teorema 4.5.3 fie  $g = \text{p}_\rho$ . ■

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



**Demonstrație.** Aplicăm Teorema 4.5.2 pentru funcția  $f : A \rightarrow B$  și funcția injectivă  $g = i : \text{Im } f \rightarrow B$ . Are loc condiția  $\text{Im } g = \text{Im } f$ , deci conform teoremei, există funcția  $h : A \rightarrow \text{Im } f$  astfel încât  $f = i \circ h$  și  $\ker h = \ker f$ .

Acum aplicăm Corolarul 4.5.4 pentru funcția  $h$  și relația  $\rho = \ker f \in \mathcal{E}(A)$ . Deoarece  $\ker f = \ker h$ , există o funcție  $\bar{f} : A/\ker f \rightarrow \text{Im } f$  astfel încât  $h = \bar{f} \circ \text{p}_{\ker f}$ ; dar  $\bar{f}$  este injectiv și  $\text{Im } \bar{f} = \text{Im } f$ , adică  $\bar{f}$  este surjectiv, deci este bijectiv.

Rezultă că  $f = i \circ \bar{f} \circ \text{p}_{\ker f}$  și  $\bar{f}(\ker f(x)) = f(x)$  pentru orice  $x \in A$ , de unde rezultă unicitatea lui  $\bar{f}$ . ■

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

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

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

**Exercițiul 80** Fie  $A$  și  $B$  mulțimi,  $\rho$  o relație de echivalență pe  $A$  și  $\sigma \in \mathcal{E}(B)$ . Pe produsul cartezian  $A \times B$  definim relația  $\rho \times \sigma$  astfel:  $(a, b)\rho \times \sigma(a', b') \Leftrightarrow a\rho a'$  și  $b\sigma b'$ .

a) Să se arate că  $\rho \times \sigma$  este relație de echivalență și există funcția bijectivă canonică

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

b) Dacă  $f : A \rightarrow A'$  și  $g : B \rightarrow B'$  sunt funcții, atunci  $\ker(f \times g) = \ker f \times \ker g$  și  $\text{Im}(f \times g) = \text{Im } f \times \text{Im } g$ .

**Exercițiul 81** Fie  $A$  o mulțime și fie  $B \subseteq A$ . Pe mulțimea părților  $\mathcal{P}(A)$  definim relația  $\rho$  astfel: pentru orice  $X, Y \in \mathcal{P}(A)$ ,  $X\rho Y \Leftrightarrow X \cap B = Y \cap B$ . Să se arate că  $\rho$  este relație de echivalență și există funcția bijectivă canonică  $\varphi : \mathcal{P}(A)/\rho \rightarrow \mathcal{P}(B)$ .

**Exercițiul 82** Fie  $A$  și  $B$  mulțimi,  $a_0 \in A$  și fie  $A' \subseteq A$ . Pe mulțimea  $\text{Hom}(A, B)$  definim următoarele relații: pentru orice  $f, g \in \text{Hom}(A, B)$ ,  $f\rho g \Leftrightarrow f(a_0) = g(a_0)$  și  $f\sigma g \Leftrightarrow f(x) = g(x) \forall x \in A'$ . Să se arate că:

- $\rho$  este relație de echivalență și există o funcție bijectivă  $\varphi : \text{Hom}(A, B)/\rho \rightarrow B$ ;
- $\sigma$  este relație de echivalență și există o funcție bijectivă  $\psi : \text{Hom}(A, B)/\sigma \rightarrow \text{Hom}(A', B)$ ;
- Să observăm că a) precum și exercițiul anterior sunt cazuri particulare ale lui b).

**Exercițiul 83** Fie  $A$  și  $B$  două mulțimi și fie  $\text{Hom}_{\text{surj}}(A, B) = \{f : A \rightarrow B \mid f \text{ este surjectiv}\}$ . Considerăm funcția  $\varphi : \text{Hom}_{\text{surj}}(A, B) \rightarrow \mathcal{E}(A)$ ,  $\varphi(f) = \ker f$ . Să se arate că:

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

**Teorema 4.5.6 (a doua teoremă de factorizare)** Fie o relație de echivalență pe  $A$ ,  $B \subseteq A$  și fie  $\sigma = (B \times B) \cap \rho$ ,  $\tau = (\rho(B) \times \rho(B)) \cap \rho$ , adică  $\sigma$  și  $\tau$  sunt restricțiile lui  $\rho$  la  $B$ , respectiv la  $\rho(B)$ .

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

$$\begin{array}{ccc} B & \xrightarrow{i} & \rho(B) \\ p_\sigma \downarrow & & \downarrow p_\tau \\ B/\sigma & \xrightarrow{F} & \rho(B)/\tau \end{array}$$

**Demonstrație.** Avem  $B \subseteq \rho(B)$  și  $i : B \rightarrow \rho(B)$ ,  $i(b) = b$ , pentru orice  $b \in B$ . Fie  $f : B \rightarrow \rho(B)/\tau$ ,  $f = p_\tau \circ i$ , deci  $f(x) = p_\tau(x) = \tau(x)$ ,  $\forall x \in B$ . Funcția  $f$  este surjectivă. Într-adevăr,  $\forall \tau(y) \in \rho(B)/\tau$ , unde  $y \in \rho(B) \Rightarrow \exists x \in B \subseteq \rho(B) : x\rho y \Rightarrow x\tau y$ , deci  $f(x) = \tau(x) = \tau(y)$ . Deci  $\text{Im } f = \rho(B)/\tau$ . Mai departe, pentru orice  $x, y \in B$  avem

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

Aplicăm Corolarul 4.5.4 funcției  $f$  și relației  $\sigma = \ker f$ . Rezultă că există o funcție injectivă

$$F : B/\sigma \rightarrow \rho(B)/\tau, \quad F(\sigma(x)) = \tau(x)$$

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

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

**Teorema 4.5.7 (a treia teoremă de factorizare)** Fie  $\rho$  și  $\sigma$  două relații de echivalență pe mulțimea  $A$  astfel încât  $\rho \subseteq \sigma$ . Atunci există o unică funcție surjectivă  $g : A/\rho \rightarrow A/\sigma$  și există o unică funcție bijectivă  $\bar{g} : (A/\rho)/(\sigma/\rho) \rightarrow A/\sigma$ , unde  $\sigma/\rho = \ker g$ , astfel încât a următoarea diagramă este comutativă:

$$\begin{array}{ccccc} A & \xrightarrow{p_\rho} & A/\rho & \xrightarrow{p_{\sigma/\rho}} & (A/\rho)/(\sigma/\rho) \\ & \searrow p_\sigma & \downarrow g & \swarrow \bar{g} & \\ & & A/\sigma & & \end{array}$$

**Demonstrație.** Aplicăm de două ori Corolarul 4.5.4 întâi pentru  $p_\sigma$ , apoi pentru  $g$ . ■

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

- $A = \{1, 2, 3, 4, 5\}$ ,  $\rho_1 = \Delta_A \cup \{(1, 2), (2, 1)\}$  și  $\rho_2 = \rho_1 \cup \{(1, 3), (3, 1), (2, 3), (3, 2), (4, 5), (5, 4)\}$ .
- $A = \mathbb{Z}$ ,  $\rho_1 = \equiv (\text{mod } 4)$  și  $\rho_2 = \equiv (\text{mod } 2)$ .
- $A = \mathbb{Z}$ ,  $\rho_1 = \equiv (\text{mod } 9)$  și  $\rho_2 = \equiv (\text{mod } 3)$ .

# Capitolul 5

## MULȚIMI ORDONATE

Noțiunea de mulțime ordonată formalizează și generalizează ideea intuitivă de ordonare, aranjare sau înșiruire a obiectelor unei colecții.

### 5.1 Relații de ordine

Fie  $\rho = (A, A, R)$  o relație omogenă. Amintim că  $\rho$  este **relație de ordine** și  $(A, \rho)$  este **mulțime ordonată** dacă  $\rho$  este reflexiv, tranzitiv și antisimetric. Dacă  $\rho$  este o relație de ordine, atunci în loc de  $x\rho y$  deseori notăm  $x \leq y$ . Notăm  $\mathcal{O}(A) = \{\rho = (A, A, R) \mid \rho \text{ relație de ordine}\}$  mulțimea relațiilor de ordine pe  $A$ .

Amintim că  $\rho$  este **relație de ordine strictă** dacă  $\rho$  este ireflexiv și tranzitiv. Notății:  $x < y$ , dacă  $x \leq y$  și  $x \neq y$  (strict mai mic);  $x > y$ , dacă  $y < x$  etc.

**Definiția 5.1.1** Spunem că  $(A, \rho)$  este **mulțime total ordonată** (sau **lanț**) dacă :

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

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

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

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

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

4) Dacă  $(A, \rho)$  este o mulțime ordonată (total ordonată) și  $B \subseteq A$ , atunci  $(B, \rho \cap (B \times B))$  este ordonată (total ordonată).

**Exercițiul 86** Fie  $A \neq \emptyset$  și 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  $\sigma$  este o relație de ordine strictă pe  $A$ , atunci  $\sigma$  este asimetric, iar  $\sigma \cup 1_A \in \mathcal{O}(A)$ .

e)  $\sigma := \rho \setminus 1_A$  este relație de ordine strictă pe  $A$ .

f) Relația de ordine  $\rho$  este totală  $\iff \rho$  satisface proprietatea de **trihotomie**, adică pentru orice  $x, y \in A$ , exact una din următoarele trei afirmații este adevărată: (1)  $a \sigma b$ ; (2)  $a = b$ ; (3)  $a \sigma^{-1} b$ .

O mulțime ordonată finită poate fi reprezentată grafic cu ajutorul unei **diagrame Hasse**, conform următoarei reguli: dacă  $x < y$  și dacă nu există  $z \in A$  astfel încât  $x < z < y$ , atunci așezăm punctul  $y$  mai sus decât punctul  $x$  și le unim cu un segment.

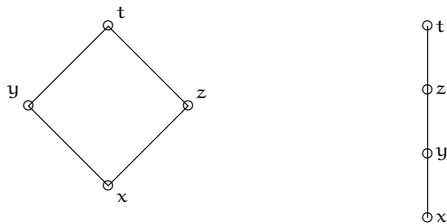
**Exemplul 5.1.3** Fie  $A = \{x, y, z, t\}$  și considerăm relațiile de ordine pe mulțimea  $A$  având graficele

$$R = \{(x, x), (y, y), (z, z), (t, t), (x, y), (x, z), (x, t), (y, t), (z, t)\},$$

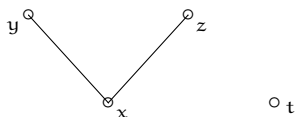
respectiv

$$R = \{(x, x), (y, y), (z, z), (t, t), (x, y), (x, z), (x, t), (y, z), (y, t), (z, t)\}.$$

Atunci diagramele Hasse sunt:



În următoarea diagramă  $x < y$ ,  $x < z$ ,  $y$  și  $z$  nu sunt comparabile, mai departe  $t$  nu e comparabil cu  $x, y, z$ .



**Exercițiul 87** Să se întocmească diagramele Hasse ale următoarelor mulțimi ordonate:

- $(\mathcal{P}(\{a, b, c, d\}), \subseteq)$ ;
- Mulțimea divizorilor lui 60, ordonată de relația de divizibilitate;
- Mulțimea partițiilor mulțimii  $\{a, b, c, d\}$ , ordonată de relația „mai fin”  $\preceq$ .

**Definiția 5.1.4** Fie  $(A, \leq)$  și  $(B, \leq)$  două mulțimi ordonate și  $f : A \rightarrow B$  o funcție.

- Spunem că  $f$  este **crescător** (**descrescător**), dacă pentru orice  $x, y \in A$ ,

$$x \leq y \Rightarrow f(x) \leq f(y) \quad (f(y) \leq f(x));$$

mai departe  $f$  este **izomorfism de ordine** (sau **asemănare**), dacă  $f$  este crescător, bijectiv și  $f^{-1}$  este crescător;

**Exemplul 5.1.5** 1) Mulțimile ordonate  $\mathbb{N} = \{1, 2, 3, \dots\}$  și  $2\mathbb{N} = \{2, 4, 6, \dots\}$  sunt asemenea, pentru că  $f : \mathbb{N} \rightarrow 2\mathbb{N}$ ,  $f(n) = 2n$  este o asemănare.

2) Mulțimile ordonate  $(\mathbb{N}, |)$  și  $(\mathbb{N}, \leq)$  nu sunt asemenea. Într-adevăr, dacă ar exista o asemănare  $f : (\mathbb{N}, |) \rightarrow (\mathbb{N}, \leq)$ , atunci fie  $f(2) = n$  și  $f(3) = m$ , 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 contradicție în ambele cazuri.

**Exercițiul 88** Să se determine toate relațiile de ordine pe mulțimea  $A = \{a, b, c\}$  (folosind diagrame Hasse). Să se împartă aceste ordonări în clase de asemănare.

**Exercițiul 89** Fie  $(A, \leq)$ ,  $(B, \leq)$  și  $(C, \leq)$  mulțimi ordonate și fie  $f : A \rightarrow B$ ,  $g : B \rightarrow C$  două funcții.

- Dacă  $f$  și  $g$  sunt crescătoare (descrescătoare), atunci  $g \circ f$  este funcție crescătoare.
- Dacă  $f$  este crescătoare (descrescătoare) și  $g$  este descrescătoare (crescătoare), atunci  $g \circ f$  este descrescătoare.

**Exercițiul 90** Fie  $(A, \leq)$  și  $(B, \leq)$  mulțimi ordonate și  $f : A \rightarrow B$  funcție bijectivă și crescătoare.

- Dacă  $A$  este total ordonată, atunci  $f^{-1}$  este crescătoare și  $B$  este total ordonată.
- Să se arate că  $1_{\mathbb{N}^*} : (\mathbb{N}^*, |) \rightarrow (\mathbb{N}^*, \leq)$  este bijectivă, crescătoare și nu e izomorfism de ordine.

**Exercițiul 91** Fie  $(A, \leq)$  și  $(B, \leq)$  mulțimi ordonate și fie  $f : A \rightarrow B$ ,  $g : B \rightarrow A$  funcții crescătoare. Fie  $M = \{a \in A \mid g(f(a)) = a\}$  și  $N = \{b \in B \mid f(g(b)) = b\}$ .

Să se arate că  $(M, \leq) \simeq (N, \leq)$ .

**Teorema 5.1.6 (preordine, echivalență și ordine)** Fie  $\rho = (A, A, R)$  o relație de preordine și fie  $\sigma = \rho \cap \rho^{-1}$ .

Atunci:

- $\sigma$  este relație de echivalență pe  $A$ ;
- pe mulțimea factor  $A/\sigma$  definim relația „ $\leq$ ” prin:  $\sigma\langle x \rangle \leq \sigma\langle y \rangle \Leftrightarrow x\rho y$ . Atunci  $(A/\sigma, \leq)$  mulțime ordonată.

**Demonstrație.** 1) Relația  $\sigma$  este reflexivă (evident), tranzitivă:  $\forall x, y, z \in A : x\sigma y$  și  $y\sigma z \Rightarrow x(\rho \cap \rho^{-1})y$  și  $y(\rho \cap \rho^{-1})z \Rightarrow (x\rho y$  și  $x\rho^{-1}y)$  și  $(y\rho z$  și  $y\rho^{-1}z) \Rightarrow (x\rho y$  și  $y\rho z)$  și  $(x\rho^{-1}y$  și  $y\rho^{-1}z) \Rightarrow x\rho z$  și  $x\rho^{-1}z$  (pentru că  $\rho$  și  $\rho^{-1}$  sunt tranzitive)  $\Rightarrow x(\rho \cap \rho^{-1})z \Rightarrow x\sigma z$ , și simetrică:  $\forall x, y \in A : x\sigma y \Rightarrow x(\rho \cap \rho^{-1})y \Rightarrow x\rho y$  și  $x\rho^{-1}y \Rightarrow y\rho x$  și  $y\rho^{-1}x \Rightarrow y(\rho \cap \rho^{-1})x \Rightarrow y\sigma x$ .

2) Definiția relației  $\leq$  nu depinde de alegerea reprezentanților  $x$  și  $y$ : dacă  $\sigma\langle x \rangle = \sigma\langle x' \rangle$ ,  $\sigma\langle y \rangle = \sigma\langle y' \rangle$  și dacă  $x\rho y$ , atunci  $x'\rho y'$ . Într-adevăr, pe baza ipotezelor avem:  $x\sigma x'$  și  $y\sigma y'$  și  $x\rho y \Rightarrow (x\rho x'$  și  $x\rho^{-1}x')$  și  $(y\rho y'$  și  $y\rho^{-1}y')$  și  $x\rho y \Rightarrow x'\rho x$  și  $x\rho y$  și  $y\rho y' \Rightarrow x'\rho y'$  (pentru că  $\rho$  este tranzitiv).

Relația  $\leq$  este reflexivă, tranzitivă și antisimetrică. Verificăm ultima proprietate. Pentru orice  $\sigma\langle x \rangle, \sigma\langle y \rangle \in A/\sigma$ ,  $\sigma\langle x \rangle \leq \sigma\langle y \rangle$  și  $\sigma\langle y \rangle \leq \sigma\langle x \rangle \Rightarrow x\rho y$  și  $y\rho x \Rightarrow x\rho y$  și  $x\rho^{-1}y \Rightarrow x(\rho \cap \rho^{-1})y \Rightarrow x\sigma y \Rightarrow \sigma\langle x \rangle = \sigma\langle y \rangle$ . ■

**Exercițiul 92** Să se aplice Teorema 5.1.6 în cazul mulțimii preordonate  $(\mathbb{Z}, |)$ .

**Definiția 5.1.7** Fie  $(A, \leq)$  o mulțime ordonată și 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  $a \in A$ ,  $a \leq x$ ).

Notăție:  $x = \min A$  (respectiv  $x = \max A$ ).

**Observații 5.1.8** Dacă există cel mai mic element (cel mai mare element), atunci el este unic. Într-adevăr, dacă de exemplu  $x$  și  $x'$  sunt ambele cele mai mic elemente, atunci  $x \leq x'$  (pentru că  $x$  este cel mai mic element) și  $x' \leq x$  (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 și nu există cel mai mare element.

2) În  $(\mathbb{N}, |)$   $1$  este cel mai mic element și  $0$  este cel mai mare element, pentru că  $1|a$  și  $a|0$  pentru orice  $a \in \mathbb{N}$ .

3) În  $(\mathbb{N} \setminus \{0, 1\}, |)$  nu există cel mai mic element și nu există cel mai mare element.

4) În  $(\mathcal{P}(A), \subseteq)$   $\min \mathcal{P}(A) = \emptyset$  și  $\max \mathcal{P}(A) = A$ .

**Definiția 5.1.10** În mulțimea 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 și nu există elemente maximale.

2) În  $(\mathbb{N}, |)$ , numărul  $1$  este element minimal și  $0$  este element maximal.

3) În  $(\mathbb{N} \setminus \{0, 1\}, |)$  numerele prime sunt elemente minimale și nu există elemente maximale.

4) Din definiții este evident că dacă există cel mai mic (cel mai mare) element, atunci el este unicul element minimal (maximal). Afirmatia reciprocă nu e adevărată; de exemplu dacă  $A = \{2^k \mid k \in \mathbb{N}\} \cup \{3, 9\}$ , atunci în mulțimea ordonată  $(A, |)$   $a = 9$  este unicul element maximal și nu există cel mai mare element.

5) Dacă  $(A, \leq)$  este o mulțime total ordonată, atunci noțiunile de element minimal (element maximal) și cel mai mic element (respectiv cel mai mare element) sunt echivalente.

**Exercițiul 93** Fie  $(A, \leq)$  o mulțime ordonată. Să se arate că dacă există  $a = \min A$ , atunci  $a$  este unicul element minimal al lui  $A$ , iar afirmația reciprocă nu e adevărată.

## 5.2 Latici

**Definiția 5.2.1** Fie  $(A, \leq)$  o mulțime ordonată,  $x \in A$  și 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  $B$ ). Notăție:  $x = \inf B$  sau  $x = \inf_A B$  (respectiv  $x = \sup B$  sau  $x = \sup_A B$ ).

**Exemplul 5.2.2** 1) În  $(\mathbb{N} \setminus \{0, 1\}, |)$ , submulțimea  $B = \{2k + 1 \mid k \in \mathbb{N}\}$  are un unic minorant, pe  $x = 1$ , deci  $\inf B = 1$ ; mai departe,  $B$  nu are majoranți și nu are supremum.

2) În  $(\mathbb{R}, \leq)$  intervalul  $B = (1, 3]$  are ca minorant orice  $x \leq 1$  și majorant orice  $x \geq 3$ ; mai departe,  $\inf B = 1 \notin B$ ,  $\sup B = 3 \in B$ .

3) Dacă  $(A, \leq)$  este o mulțime ordonată, atunci orice element al lui  $A$  este minorant și majorant al lui  $B = \emptyset$ . Mai departe  $\exists \inf \emptyset \Leftrightarrow \exists \max A \Leftrightarrow \exists \sup A$ ,  $\exists \sup \emptyset \Leftrightarrow \exists \min A \Leftrightarrow \exists \inf A$  și atunci  $\inf \emptyset = \max A = \sup A$ ,  $\sup \emptyset = \min A = \inf A$ .

4) Orice submulțime  $B \subseteq A$  are cel mult un infimum și cel mult un supremum; mai departe, dacă  $B$  are minorant  $x$  (majorant  $y$ ) ce aparține lui  $B$ , atunci  $x = \inf B$  (respectiv  $y = \sup B$ ).

**Exercițiul 94** Fie  $(A, \leq)$  o mulțime ordonată și fie  $X \subseteq B \subseteq A$ .

a) Dacă există  $\inf_B X$  și  $\inf_A X$ , atunci  $\inf_B X \geq \inf_A X$ .

b) Dacă există  $\sup_B X$  și  $\sup_A X$ , atunci  $\sup_B X \leq \sup_A X$ .

**Definiția 5.2.3** a) Mulțimea ordonată  $(A, \leq)$  se numește **latice**, dacă orice submulțime cu două elemente a lui  $A$  are infimum și supremum (pentru orice  $a, b \in A$ ,  $a \neq b$ ,  $\exists \inf\{a, b\}$  și  $\exists \sup\{a, b\}$ ).

b)  $(A, \leq)$  este **latice completă**, dacă orice submulțime a lui  $A$  are infimum și supremum (pentru orice  $B \subseteq A$ ,  $\exists \inf B$  și  $\exists \sup B$ ).

**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:  $\forall a, b \in A : \inf\{a, b\} = \min\{a, b\}$  și  $\sup\{a, b\} = \max\{a, b\}$ .

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  $\inf X = \bigcap_{i \in I} X_i$  și  $\sup X = \bigcup_{i \in I} X_i$ .

**Exercițiul 95** Să se determine, abstracție făcând de izomorfisme (asemănări), toate laticile cu 1, 2, 3, 4, 5 și respectiv 6 elemente (folosind diagrame Hasse).

**Exercițiul 96** Fie  $A$  o mulțime și  $(B, \leq)$  o mulțime ordonată. Pe mulțimea  $\text{Hom}(A, B)$  definim următoarea relație:  $f \leq g \iff f(a) \leq g(a)$  pentru orice  $a \in A$ .

Să se arate că:

a) „ $\leq$ ” este relație de ordine.

b) Dacă  $B$  este latice, atunci și  $\text{Hom}(A, B)$  este latice.

**Teorema 5.2.5 (caracterizarea laticilor complete)** Fie  $(A, \leq)$  o mulțime ordonată. Următoarele afirmații sunt echivalente:

(i)  $(A, \leq)$  este latice completă;

(ii) orice submulțime a lui  $A$  are infimum;

(iii) orice submulțime a lui  $A$  are supremum.

**Demonstrație.** (i)  $\Rightarrow$  (ii) și (i)  $\Rightarrow$  (iii) sunt evidente din definiție.

(ii)  $\Rightarrow$  (i) Trebuie să arătăm că orice submulțime  $B$  a lui  $A$  are supremum. Notăm cu  $C$  mulțimea majoranților 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  $b \in B$  și  $c \in C$  avem  $b \leq c$  (din definiția 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 definiției 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). ■

**Exercițiul 97** Fie  $(A, \leq)$  o latice completă și fie  $f : A \rightarrow A$  o funcție 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 Mulțimi bine ordonate și mulțimi artiniene

**Definiția 5.3.1** Fie  $(A, \leq)$  o mulțime ordonată. Spunem că  $A$  este **bine ordonată** dacă orice submulțime 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)  $(\mathbb{N}, \leq)$  mulțime 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 mulțime finită total ordonată bine ordonată.

Într-adevăr, trebuie să arătăm că  $\forall B \subseteq A, B \neq \emptyset, \exists \min B$ . Fie  $B \subseteq A, B \neq \emptyset$ . Deoarece  $A$  finită  $\Rightarrow B$  este finită, deci fie  $B = \{b_1, b_2, \dots, b_n\}$ . Deoarece  $(A, \leq)$  este total ordonată, rezultă că orice două elemente din  $A$  (deci și din  $B$ ) sunt comparabile. Comparăm primele două elemente ale lui  $B$ , păstrăm pe cel mai mic dintre ele, și apoi îl comparăm cu al treilea element al lui  $B$  și păstrăm pe cel mai mic dintre ele. Continuând, prin inducție, după  $n$  pași am găsit elementul  $\min B$ .

Următoarea teoremă arată că pe mulțimile bine ordonate se poate aplica metoda inducției matematice.

**Teorema 5.3.3 (caracterizarea mulțimilor bine ordonate)** Dacă  $(A, \leq)$  este o mulțime ordonată nevidă, atunci următoarele afirmații sunt echivalente:

(i)  $(A, \leq)$  este bine ordonată,

(ii)  $A$  este total ordonată, există  $a_0 = \min A$  și pentru orice  $B \subseteq A$ , dacă  $B$  satisface proprietățile:

a)  $a_0 \in B$ ,

b) pentru orice  $a \in A, \{x \in A \mid x < a\} \subseteq B \Rightarrow a \in B$ ,

atunci  $B = A$ .

**Demonstrație.** (i)  $\Rightarrow$  (ii) Presupunem că  $(A, \leq)$  este bine ordonată. Atunci  $A$  este total ordonată, și există  $a_0 = \min A$ . Presupunem că a doua condiție din (ii) nu e adevărată, adică există  $B \subseteq A$ , astfel încât au loc a) și b) și  $B \neq A$ .

Deci  $A \setminus B \neq \emptyset$  și 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 definiția lui  $x$ ), deci  $\{y \in A \mid y < x\} \subseteq B$ , și de aici  $x \in B$ , conform lui b), ceea ce e o contradicție.

(ii)  $\Rightarrow$  (i) Presupunem că (ii) este adevărat și 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

$\alpha$ )  $a_0 \in A \setminus B$ , pentru că dacă  $a_0 = \min A \in B$ , atunci  $a_0 = \min B$ , contradicție.

$\beta$ ) 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 așa, atunci  $a \in B$ , și deoarece  $A$  este total ordonată, elementele  $x$  mai mici ca  $a$  sunt în  $A \setminus B$ , deci obținem că  $a = \min B$ , contradicție.

Din  $\alpha$  și  $\beta$  deducem că submulțimea  $A \setminus B$  satisface ipotezele a) și b), și astfel  $A \setminus B = A$ , adică  $B = \emptyset$ , contradicție. ■

**Corolar 5.3.4** Fie  $(A, \leq)$  o mulțime nevidă bine ordonată,  $a_0 = \min A$  și 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  $a \in A$ .

**Demonstrație.** Fie

$$B = \{a \in A \mid P(a) \text{ este adevărat}\} \subseteq A,$$

care satisface ipotezele a) și b) ale teoremei precedente, deci  $B = A$ . ■

**Exercițiul 98** a) Să se arate că:

1) Dacă  $(A, \leq)$  este o mulțime bine ordonată și  $f : A \rightarrow A$  este o aplicație strict crescătoare, atunci pentru orice  $a \in A$  avem  $a \leq f(a)$ .

2) Între două mulțimi bine ordonate există cel mult un izomorfism.

Următoarea teoremă generalizează Teorema 5.3.3 la cazul mulțimilor care nu sunt total ordonate.

**Definiția 5.3.5** O mulțime ordonată  $(A, \leq)$  se numește **artiniană** sau **bine fondată** dacă satisface condițiile echivalente de mai jos.

Noțiunea duală este cea de **mulțime noetheriană**.

**Teorema 5.3.6 (caracterizarea mulțimilor artiniene)** Fie  $(A, \leq)$  o mulțime ordonată. Următoarele afirmații sunt echivalente:

(i) **(condiția minimalității)** Orice submulțime nevidă  $B \subseteq A$  are elemente minimale.

(ii) **(condiția inductivității)** Pentru orice  $B \subseteq A$ , dacă  $B$  satisface proprietățile:

(1)  $B$  conține toate elementele minimale ale lui  $A$ ;

(2) dacă  $a \in A$  și  $\{x \in A \mid x < a\} \subseteq B$ , atunci  $a \in B$ ,

atunci  $B = A$ .

(iii) **(condiția lanțurilor descrescătoare)** Orice șir strict descrescător  $a_1 > a_2 > \dots > a_n > \dots$  de elemente din  $A$  este finit.

**Demonstrație.** (i) $\Rightarrow$ (ii). Presupunem că  $B \subseteq A$  satisface condițiile (1) și (2), dar  $B \neq A$ . Fie  $x \in A \setminus B$  un element minimal. Atunci  $x$  nu e minimal în  $A$ , pentru că  $B$  conține 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  $x \in B$ , contradicție.

(ii) $\Rightarrow$ (iii). Considerăm mulțimea

$$B := \{a \in A \mid \text{pentru orice șir finit } a > a_1 > a_2 > \dots\}.$$

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  $x < b$  aparține lui  $B$ . Atunci avem  $b \in B$ , deci  $B = A$ .

(iii) $\Rightarrow$ (i). Presupunem că  $B \subseteq A$ ,  $B \neq \emptyset$ , și că  $B$  nu conține elemente minimale. Atunci pentru orice  $a_1 \in B$ , există  $a_2 \in B$ ,  $a_2 < a_1$ , și prin inducție construim un șir strict descrescător  $a_1 > a_2 > \dots > a_n > \dots$ , ceea ce contrazice ipoteza. ■

**Exemplul 5.3.7** O mulțime total ordonată artiniană este bine ordonată. Dăm câteva exemple de mulțimi artiniene care nu sunt bine ordonate.

1) Mulțimea  $(\mathbb{N}, |)$  a numerelor naturale ordonată de relația de divizibilitate.

2) Mulțimea  $(\mathcal{P}_f(M), \subseteq)$  a submulțimilor finite ale unei mulțimi  $M$ .

3) Mulțimea  $(\mathbb{N} \times \mathbb{N}, \leq)$  a perechilor de numere naturale, unde  $(a, b) \leq (a', b') \Leftrightarrow a \leq a'$  și  $b \leq b'$ .

4) Mulțimea  $M^{(\mathbb{N})}$  a șirurilor finite de elemente din mulțimea  $M$ , unde  $s \leq s' \Leftrightarrow s$  este subșir al șirului  $s'$ .

## 5.4 Axioma alegerii

De multe ori în matematică ne întâlnim cu propoziția: „alegem un element din mulțimea ...” sau mai precis:

(A<sub>0</sub>) Pentru orice mulțime  $X \neq \emptyset$  există un element  $x \in X$ , deci  $\{x\} \subseteq X$ .

Aceasta este cea mai simplă formulare a axiomei alegerii. La prima vedere, propoziția (A<sub>0</sub>) pare evidentă, pentru că  $X \neq \emptyset$  înseamnă că există cel puțin un element  $x \in X$ . Se pune însă întrebarea ce înseamnă expresia „există un element  $x \in X$ ”. Să dăm două exemple:

a) Fie  $f: [a, b] \rightarrow \mathbb{R}$  o funcție continuă astfel încât  $f(a) \cdot f(b) \leq 0$ . Definim mulțimea

$$X = \{x \in [a, b] \mid f(x) = 0\}.$$

Teorema lui Darboux arată că există  $x_0 \in [a, b]$  astfel încât  $f(x_0) = 0$ . Una din demonstrațiile 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 coeficienți complecși. Considerăm mulțimea

$$X = \{x \mid x \text{ număr complex astfel ca } P(x) = 0\}.$$

Teorema lui Gauss-d'Alembert afirmă că mulțimea  $X$  este nevidă și finită, dar nicio demonstrație nu dă o metodă de a găsi rădăcinile unui polinom arbitrar. Teorema este una de existență pură.

În aceste exemple, vedem că expresia „există un element  $x \in X$ ” are un sens restrâns (se dă o metodă pentru găsirea elementului  $x$ ) și un sens larg.

### 5.4.1 Forma generală a axiomei alegerii este următoarea:

(A) Fie  $F \neq \emptyset$  o mulțime de mulțimi nevide disjuncte două câte două. Atunci există o mulțime  $A$  cu următoarele proprietăți:

$$(1) A \subseteq \bigcup_{X \in F} X;$$

(2) pentru orice  $X \in F$ ,  $A \cap X$  conține exact un element.

Mulțimea  $A$  se numește **mulțime selectivă** pentru  $F$ . Observăm că (A<sub>0</sub>) este caz particular al lui (A).

Axioma alegerii a fost formulată de Ernst Zermelo în 1904. Ea este independentă de celelalte axiome, și are diferite formulări echivalente, după cum vom vedea mai jos. Considerând teoria mulțimilor fără axioma alegerii și privind această enunț ca o formulă închisă, Kurt Gödel a construit un model pentru teoria mulțimilor în care axioma alegerii este adevărată. Pe de altă parte, Paul Cohen a construit în 1963 un alt model pentru teoria mulțimilor în care axioma alegerii nu este adevărată. Altfel spus, teoria mulțimilor fără axioma alegerii este nedecidabilă.

Multe rezultate din matematică folosesc efectiv axioma alegerii, adică nu s-au descoperit demonstrații 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 afirmații sunt echivalente:

1) Axioma alegerii (A).

2) Pentru orice mulțime nevidă  $F$  de mulțimi nevide există o funcție  $f: F \rightarrow \bigcup_{X \in F} X$  astfel încât  $f(X) \in X$  pentru

orice  $X \in F$ .

3) Pentru orice mulțime  $X \neq \emptyset$  există o funcție  $f: \mathcal{P}(X) \setminus \{\emptyset\} \rightarrow X$  astfel încât pentru orice  $A \in \mathcal{P}(X) \setminus \{\emptyset\}$ ,  $f(A) \in A$  ( $f$  se numește **funcție selectivă**).

4) Dacă  $(X_i)_{i \in I}$  este o familie de mulțimi astfel încât  $I \neq \emptyset$  și  $X_i \neq \emptyset$  pentru orice  $i \in I$ , atunci produsul direct  $\prod_{i \in I} X_i$  este nevid (adică, există o funcție  $f: I \rightarrow \prod_{i \in I} X_i$  astfel încât pentru orice  $i \in I$  avem  $f(i) \in X_i$ ).

5) (**Lema lui Zorn**) Fie  $(A, \leq)$  o mulțime nevidă ordonată. Dacă orice lanț (submulțime 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 mulțime ordonată și  $L \subseteq A$  este un lanț, atunci există un lanț maximal  $L' \subseteq A$  astfel ca  $L \subseteq L'$ .

7) (**Teorema lui Zermelo**) Pentru orice mulțime  $A$ , există o relație de ordine „ $\leq$ ” astfel ca  $(A, \leq)$  este mulțime bine ordonată.

8) Orice funcție surjectivă are cel puțin o secțiune (inversă la dreapta).

**Exercițiul 99** Fie  $A$  o mulțime și considerăm mulțimea ordonată  $(\mathcal{O}(A), \subseteq)$  a relațiilor de ordine pe  $A$ . Folosind lema lui Zorn, să se demonstreze:

a)  $\rho$  este element maximal al lui  $\mathcal{O}(A)$  dacă și numai dacă  $\rho$  este ordonare totală.

b) Pentru orice  $\rho \in \mathcal{O}(A)$  există o ordonare totală  $\bar{\rho} \in \mathcal{O}(A)$  astfel încât  $\rho \subseteq \bar{\rho}$ .



**Exercițiul 100** Spunem că o mulțime  $\mathcal{F}$  de mulțimi *este de caracter finit* dacă satisface următoarea proprietate:

(\*) Dacă  $A$  este o mulțime, atunci  $A \in \mathcal{F}$ , dacă și numai dacă orice submulțime finită a lui  $A$  aparține lui  $\mathcal{F}$ .

Folosind lema lui Zorn, să se demonstreze:

a) Dacă  $\mathcal{F}$  este de caracter finit și  $A \in \mathcal{F}$ , atunci orice submulțime a lui  $A$  aparține lui  $\mathcal{F}$

b) (**Lema lui Tukey**) Orice mulțime nevidă  $\mathcal{F}$  de mulțimi de caracter finit are cel puțin un element maximal relativ la incluziune.

## Capitolul 6

# LATICI ȘI ALGEBRE BOOLE

### 6.1 Latticea ca structură algebrică

În capitolul anterior am definit latticea ca fiind o mulțime ordonată cu proprietăți adiționale. Existența infimumului și a supremumului a oricărei perechi de elemente permite definirea a două operații pe mulțimea respectivă.

**Definiția 6.1.1** a) Structura algebrică  $(A, \wedge, \vee)$  cu două operații binare „ $\wedge$ ” și „ $\vee$ ” se numește **lattice**, dacă sunt satisfăcute axiomele:

1. ambele operații sunt asociative,
2. ambele operații sunt comutative,
3. pentru orice  $x, y \in A$  avem  $x \wedge (x \vee y) = x$  și  $x \vee (x \wedge y) = x$  (**absorbție**).

b) Spunem ca  $A$  are **element unitate 1**, dacă  $1$  este element neutru față de  $\wedge$ , adică  $x \wedge 1 = x$  pentru orice  $x \in A$ . Spunem ca  $A$  are **element nul 0**, dacă  $0$  este element neutru față de  $\vee$ , adică  $x \vee 0 = x$  pentru orice  $x \in A$ .

b) Fie  $(A, \wedge, \vee)$  și  $(A', \wedge, \vee)$  latici. Funcția  $f : A \rightarrow A'$  se numește **morfism de latici** dacă pentru orice  $a, b \in A$  avem

$$f(a \vee b) = f(a) \vee f(b), \quad f(a \wedge b) = f(a) \wedge f(b).$$

Mai departe,  $f$  este **izomorfism de latici**, dacă este morfism bijectiv de latici.

**Teorema 6.1.2** a) Dacă mulțimea ordonată  $(A, \leq)$  este o lattice, atunci operațiile

$$a \wedge b = \inf\{a, b\}, \quad a \vee b = \sup\{a, b\}, \quad \forall a, b \in A$$

definesc pe mulțimea  $A$  o structură de lattice  $(A, \wedge, \vee)$ .

b) Invers, dacă structura algebrică  $(A, \wedge, \vee)$  este o lattice, atunci relația

$$a \leq b \iff a \wedge b = a, \quad \forall a, b \in A$$

definită pe mulțimea  $A$  este o relația de ordine astfel încât  $(A, \leq)$  este lattice; mai mult, pentru orice  $a, b \in A$  avem

$$a \vee b = \sup\{a, b\}, \quad a \wedge b = \inf\{a, b\}.$$

**Demonstrație.** a) Comutativitatea operațiilor  $\wedge$  și  $\vee$  este evidentă din definiție. Demonstrăm că  $\vee$  este asociativă: fie  $x = (a \vee b) \vee c, y = a \vee (b \vee c)$ . Avem  $a \vee b \leq x, c \leq x \implies a \leq x, b \leq x, c \leq x \implies a \leq x, b \vee c \leq x \implies a \vee (b \vee c) \leq x$ , de unde  $y \leq x$ . Analog obținem că  $x \leq y$ , deci  $x = y$ .

Fie acum  $v = a \vee (a \wedge b)$ . De aici  $a \leq v$ , pe de altă parte  $a \wedge b \leq a, a \leq a \implies a \vee (a \wedge b) \leq a \implies v \leq a \implies v = a$ .

b) Observăm că avem

$$(*) \quad a \vee b = b \iff a \wedge b = a.$$

Într-adevăr, pe baza proprietății de absorbție, avem  $a \vee b = b \implies a = a \wedge (a \vee b) = a \wedge b$ ; mai departe,  $a \wedge b = a \implies b = b \vee (b \wedge a) = b \vee (a \wedge b) = b \vee a = a \vee b$ .

Mai departe, să observăm că cele două operații sunt idempotente, adică avem

$$(**) \quad a \vee a = a \wedge a = a.$$

Într-adevăr, pe baza proprietății de absorbție, pentru orice  $a \in A$  avem  $a = a \wedge (a \vee a)$  și apoi  $a \vee a = a \vee (a \wedge (a \vee a)) = a$ . Analog se verifică proprietatea duală.

Arătăm că  $\leq$  este relație de ordine. Am văzut că  $a \vee a = a$ , de unde  $a \leq a$ , deci relația este reflexivă.

Antisimetria: fie  $a \leq b, b \leq a$ . Rezultă că  $a \vee b = b, b \vee a = a \implies a = b$ .

Tranzitivitatea: pentru orice  $a, b, c \in A$  avem  $a \leq b, b \leq c \implies a \vee b = b, b \vee c = c \implies a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c \implies a \leq c$ .

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  $a$  și  $b$ . Dacă  $c$  este o majorantă, adică  $a \leq c, b \leq c$ , atunci  $a \vee c = c, b \vee c = c \implies (a \vee b) \vee c = a \vee (b \vee c) = a \vee c \implies a \vee b \leq c$ , 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 lattice cu element nul și element unitate, unde  $x \wedge y = (x, y)$ , este cel mai mare divizor comun al lui  $x$  și  $y$ , iar  $x \vee y = [x, y]$  este cel mai mic multiplu comun al lui  $x$  și  $y$ . 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 lattice corespunde mulțimii ordonate  $(\mathbb{N}, |)$ .

2) Dacă  $M$  este o mulțime, atunci  $(\mathcal{P}(M), \cap, \cup)$  este o lattice cu element nul și element unitate. Elementul nul este mulțimea vidă  $\emptyset$ , iar elementul unitate este  $M$ . Această lattice corespunde mulțimii ordonate  $(\mathcal{P}(M), \subseteq)$ .

**Exercițiul 101** Să se arate că:

a) Dacă  $f : A \rightarrow B$ , atunci  $f^* : \mathcal{P}(B) \rightarrow \mathcal{P}(A)$ ,  $f^*(Y) = f^{-1}(Y)$  este morfism de latici.

b) Funcția  $f_* : \mathcal{P}(A) \rightarrow \mathcal{P}(B)$ ,  $f_*(X) = f(X)$  este morfism de latici dacă și numai dacă  $f$  este injectivă.

**Exercițiul 102** Fie mulțimile  $A = \{1, 2, 3\}$  și  $B = \{d > 0 \mid d|30\}$ . Să se determine toate izomorfismele de latici  $f : (\mathcal{P}(A), \subseteq) \rightarrow (B, |)$ .

**Exercițiul 103** Fie  $(A, \leq, \wedge, \vee)$  și  $(B, \leq, \wedge, \vee)$  două latici și fie  $f : A \rightarrow B$  o funcție. Să se arate că:

a) Dacă  $f$  este morfism de latici, atunci  $f$  este crescător.

b) Afirmatia reciprocă nu e adevărată, adică există funcții crescătoare care nu sunt morfisme de latici.

c) Dacă  $A$  este total ordonată și  $f$  este crescător, atunci  $f$  este morfism de latici.

d) Dacă  $f$  este morfism bijectiv de latici, atunci  $f^{-1} : B \rightarrow A$  este de asemenea morfism de latici.

e)  $f$  este izomorfism de latici  $\iff f$  este izomorfism de ordine.

**Definiția 6.1.4** a) Latticea  $(A, \wedge, \vee)$  este **distributivă**, dacă pentru orice  $a, b, c \in A$ ,

$$(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c).$$

b) Latticea  $(A, \wedge, \vee)$  este **modulară**, dacă pentru orice  $a, b, c \in A$ ,

$$a \leq c \implies a \vee (b \wedge c) = (a \vee b) \wedge c.$$

**Observații 6.1.5** 1) Se poate arăta că latticea  $(A, \wedge, \vee)$  este distributivă dacă și 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 lattice distributivă este modulară. Într-adevăr, pentru orice  $a, b, c \in A, a \leq c$ , avem  $a \vee c = c$  și  $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$ .

Afirmatia reciprocă nu este adevărată, există latici modulare, care nu sunt distributive.

**Exercițiul 104** Să se demonstreze :

a) În latticea  $(A, \wedge, \vee)$  avem  $a \leq a', b \leq b' \implies a \vee b \leq a' \vee b'$  și  $a \wedge b \leq a' \wedge b'$ .

b) Lattice  $(A, \wedge, \vee)$  este distributivă dacă și numai dacă pentru orice  $a, b, c \in A$  avem  $(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$ .

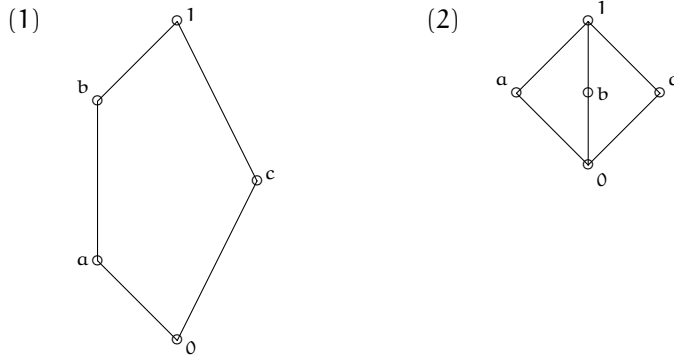
c) Dacă  $A$  este distributivă, atunci pentru orice  $a, b, c \in A$  avem

$$a \vee c = b \vee c, a \wedge c = b \wedge c \implies a = b.$$

d) Dacă  $A$  este modulară, atunci pentru orice  $a, b, c \in A$  avem

$$a \leq b, a \vee c = b \vee c, a \wedge c = b \wedge c \implies a = b.$$

e) Latticea (1) nu e modulară (deci nici distributivă); latticea (2) este modulară, dar nu e distributivă:



**Exercițiul 105** Să se arate că :

- Dacă  $(A, \leq)$  este total ordonată, atunci  $A$  este lattice distributivă.
- $(\mathbb{N}, |)$  este lattice distributivă.

## 6.2 Latici Boole și inele Boole

**Definiția 6.2.1** Latticea  $A$  se numește **lattice Boole** (sau **algebră Boole**) dacă  $A$  este distributivă, există cel mai mic element  $0 = \min A$ , există cel mai mare element  $1 = \max A$  și pentru orice  $a \in A$  există un **complement**  $a' \in A$  astfel încât  $a \wedge a' = 0$  și  $a \vee a' = 1$ . Vom nota această structură algebrică prin  $(A, \vee, \wedge, 0, 1, ')$ .

**Exemplul 6.2.2**  $(\mathcal{P}(M), \cap, \cup)$  este lattice 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 lattice Boole, atunci

- Pentru orice  $a \in A$  există un unic complement  $a' \in A$  astfel încât  $a \wedge a' = 0$  și  $a \vee a' = 1$ .
- $0' = 1$ ,  $1' = 0$ ,  $(a')' = a$ ,
- Pentru orice  $a, b \in A$ ,

$$(a \wedge b)' = a' \vee b', \quad (a \vee b)' = a' \wedge b'$$

(formulele lui de Morgan).

**Demonstrație.** a) Dacă  $a \vee a' = a \vee \bar{a} = 1$  și  $a \wedge a' = a \wedge \bar{a} = 0$ , 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  $0' = 1$  și  $1' = 0$ . Mai departe,  $a' \wedge a = 0$ ,  $a' \vee a = 1$ , deci  $(a')' = a$ .

c)  $(a \vee b) \vee (a' \wedge b') = (a \vee b \vee a') \wedge (a \vee b \vee b') = (1 \vee b) \wedge (1 \vee a) = 1 \wedge 1 = 1$  și  $(a \vee b) \wedge (a' \wedge b') = (a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') = 0 \vee 0 = 0$ , deci  $(a \vee b)' = a' \wedge b'$ ; analog se arată că  $(a \wedge b)' = a' \vee b'$ . ■

**Definiția 6.2.4** Inelul asociativ cu unitate  $(A, +, \cdot)$  se numește **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

- $1 + 1 = 0$  (deci  $x + x = 0$  pentru orice  $x \in A$ ).
- $A$  este comutativ.

**Demonstrație.** 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 noțiunile de lattice Boole și de inel Boole sunt echivalente.

**Teorema 6.2.6 (Stone)** a) Fie  $(A, \vee, \wedge, 0, 1, ')$  o latice Boole și definim operațiile:

$$\begin{aligned} a + b &= (a \wedge b') \vee (a' \wedge b) = (a \vee b) \wedge (a' \vee b') \\ a \cdot b &= a \wedge b. \end{aligned}$$

Atunci  $(A, +, \cdot)$  este inel Boole cu element nul 0 și element unitate 1.

b) Fie  $(A, +, \cdot, 0, 1)$  un inel Boole și definim operațiile:

$$a \vee b = a + b + ab, \quad a \wedge b = ab.$$

Atunci  $(A, \vee, \cdot)$  este latice Boole, în care  $a' = 1 + a$ ,  $\min A = 0$  și  $\max A = 1$ .

c) Corespondențele definite de a) și b) sunt inverse una alteia.

d) Dacă  $f : A \rightarrow A'$  este un morfism de latici Boole, atunci  $f$  este și morfism de inele Boole, iar dacă  $g : B \rightarrow B'$  este un morfism de inele Boole, atunci  $g$  este și morfism de latici Boole.

**Demonstrație.** 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  $a \in A$

Operația „·” este comutativă și 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 ușor că „ $\vee$ ” și „ $\wedge$ ” sunt comutative și asociative, au loc proprietățile de distributivitate și și absorbție, și pentru orice  $a \in A$ ,  $a \vee 0 = a + 0 + a \cdot 0 = a$ ;  $a \wedge 1 = a \cdot 1 = a$ ;  $a \wedge (1 + a) = a(1 + a) = a + a^2 = a + a = 0$  și  $a \vee (1 + a) = a + 1 + a + a(1 + a) = 1 + a + a^2 = 1$ .

c) Fie  $(A, \vee, \wedge, 0, 1, ')$  o latice Boole,  $(A, +, \cdot, 0, 1)$  inelul Boole corespunzător, și fie  $a \cup b = a + b + ab$ ,  $a \cap b = a \cdot b$ ,  $\bar{a} = a + 1$ . Atunci se arată că  $a \cup b = a \vee b$ ,  $a \cap b = a \wedge b$  și  $a' = \bar{a}$ .

Invers, fie  $(A, +, \cdot, 0, 1)$  un inel Boole,  $(A, \vee, \wedge, 0, 1, ')$  laticea Boole corespunzătoare, și fie  $a \oplus b = (a \wedge b') \vee (a' \wedge b)$ ,  $a \odot b = a \wedge b$ . Atunci  $a \oplus b = a + b$  și  $a \odot b = ab$ .

d) Afirmția 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

$\vee$	$\hat{0}$	$\hat{1}$
$\hat{0}$	$\hat{0}$	$\hat{1}$
$\hat{1}$	$\hat{1}$	$\hat{1}$

$\wedge$	$\hat{0}$	$\hat{1}$
$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$

$'$	$\hat{0}$	$\hat{1}$
$\hat{0}$	$\hat{1}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$

2)  $A(\mathcal{P}(M), \cup, \cap, \emptyset, M, \bar{\cdot})$  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 diferența simetrică a lui  $A$  și  $B$ .

**Exercițiul 106** a) Dacă  $B_1, \dots, B_n$  sunt inele Boole, atunci  $B_1 \times \dots \times B_n$  este inel Boole.

b) Dacă  $M$  o mulțime și  $B$  este un inel Boole, atunci  $B^M = \text{Hom}(M, B)$  este inel Boole.

**Exercițiul 107** a) Să se completeze demonstrația teoremei lui Stone.

b) Dacă  $A$  este o latice Boole și  $a, b \in A$ , atunci

$$a \leq b \iff b' \leq a' \iff a \wedge b' = 0 \iff a' \vee b = 1.$$

**Exercițiul 108** Folosind structura de inel Boole a lui  $\mathcal{P}(U)$ , să se rezolve următoarele sisteme de ecuații, unde  $A, B, C \in \mathcal{P}(U)$  sunt date, iar  $X \in \mathcal{P}(U)$  este necunoscută:

- a)  $A \cap X = B, A \cup X = C.$   
 b)  $A \setminus X = B, X \setminus A = C.$

**Exercițiul 109** Să se demonstreze că funcțiile de mai jos sunt izomorfisme de inele Boole:

- a)  $\mathcal{P}(M) \simeq \mathbb{Z}_2^M, X \mapsto \chi_X$  (unde  $\chi_X$  este funcția caracteristică a lui  $X$ ).  
 b)  $\mathcal{P}(M \cup N) \simeq \mathcal{P}(M) \times \mathcal{P}(N)$ , dacă  $M \cap N = \emptyset.$   
 c) Dacă  $N \subseteq M$ , atunci  $\mathcal{P}(N) \leq \mathcal{P}(M)$  și  $\mathcal{P}(M)/\mathcal{P}(N) \simeq \mathcal{P}(\mathbb{C}N).$

**Exercițiul 110** Fie  $A$  este un inel comutativ. Notăm  $\text{Idemp}(A) := \{e \in A \mid e^2 = e\}$  mulțimea idempotenților lui  $A$ . Pentru orice  $e, f \in \text{Idemp}(A)$  definim  $e \oplus f = e + f - 2ef$ .

- a) Să se arate că  $(\text{Idemp}(A), \oplus, \cdot)$  este un inel Boole.  
 b) Să se întocmească diagrama Hasse a laticii Boole  $(\text{Idemp}(A), \vee, \wedge)$ , dacă  $A = \mathbb{Z}_{24}$ , respectiv  $A = \mathbb{Z}_{180}.$

### 6.3 Algebra Lyndenbaum–Tarski

Logica propozițiilor furnizează un exemplu important de latice Boole.

**Definiția 6.3.1** a) Fie  $\mathcal{F}$  mulțimea formulelor propoziționale peste o mulțime dată de formule atomice. Considerăm structura algebrică  $(\mathcal{F}, \wedge, \vee, \bar{\phantom{x}})$ . În Capitolul 1 am definit pe  $\mathcal{F}$  relațiile „ $\Rightarrow$ ” (*rezultă*) respectiv „ $\Leftrightarrow$ ” (*echivalent*). Este evident că  $\Rightarrow$  este o relație de preordine, în timp ce  $\Leftrightarrow = (\Rightarrow \cap \Rightarrow^{-1})$  este o relație de echivalență pe  $\mathcal{F}$ , compatibilă cu operațiile  $\wedge, \vee$  și  $\bar{\phantom{x}}$ .

b) Construim mulțimea 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 mulțimea  $\hat{\mathcal{F}}$  definim operațiile

$$\hat{A} \wedge \hat{B} = \widehat{A \wedge B}, \quad \hat{A} \vee \hat{B} = \widehat{A \vee B}, \quad \bar{\hat{A}} = \widehat{\bar{A}}.$$

Aceste definiții nu depind de alegerea reprezentanților.

c) Clasa tautologiilor se notează cu  $1$ , iar clasa contradicțiilor cu  $0$ . Deci avem

$$1 = \{A \in \mathcal{F} \mid A \text{ tautologie}\}, \quad 0 = \{A \in \mathcal{F} \mid A \text{ contradicție}\}.$$

d) Conform Teoremei 5.1.6 pe mulțimea factor  $\hat{\mathcal{F}}$  se poate defini o relație de ordine prin  $\hat{A} \Rightarrow \hat{B}$  dacă și numai dacă  $A \Rightarrow B$ .

Demonstrația următoarei teoreme este lăsată cititorului.

**Teorema 6.3.2** a) Structura algebrică  $(\hat{\mathcal{F}}, \wedge, \vee, \bar{\phantom{x}}, 0, 1)$  este o latice Boole.

b) Următoarele afirmații 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  $(\hat{\mathcal{F}}, \wedge, \vee, \bar{\phantom{x}}, 0, 1)$  se numește *algebra Lyndenbaum–Tarski*. Teorema de mai sus dă posibilitatea utilizării metodelor algebrei în logica matematică.

**Exercițiul 111** a) Să se arate că relațiile „ $\Rightarrow$ ” și „ $\Leftrightarrow$ ” sunt compatibile cu operațiile  $\wedge, \vee$  și  $\bar{\phantom{x}}$ .

b) Să se demonstreze Teorema 6.3.2.

### 6.4 Formule și funcții Boole. Forme normale

Fie  $B$  o mulțime finită.

**Definiția 6.4.1** a) Numim **formule (polinoame) Boole** (peste  $B$ ) șirurile de simboluri construite astfel:

1. Dacă  $x \in B$ , atunci  $x$  este formulă Boole;

2. Dacă  $x, y$  sunt formule Boole, atunci următoarele șirurile de simboluri sunt formule Boole

$$(x \vee y), (x \wedge y), \text{ și } (\bar{x});$$

3. Nu există alte formule Boole în afara celor construite la (1) și (2).

b) Dacă  $x$  este o formulă Boole, atunci **duala** lui  $x$  (notație:  $x^*$ ) se obține schimbând între ele simbolurile „ $\wedge$ ” și „ $\vee$ ”.

c) Vom folosi uneori și simbolurile „ $\rightarrow$ ” și „ $\leftrightarrow$ ”, dar acestea se reduc la cele de mai sus conform formulelor cunoscute deja din logica propozițiilor.

**Observații 6.4.2** a) Presupunem că  $B$  este chiar o latică 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 dualității**:

(\*) Dacă  $x$  și  $y$  sunt formule Boole și  $x = y$  în  $B$ , atunci avem și 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 notații:

• 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

$$x_1^{\alpha_1} \wedge x_2^{\alpha_2} \wedge \dots \wedge x_n^{\alpha_n} \quad \text{și} \quad x_1^{\alpha_1} \vee x_2^{\alpha_2} \vee \dots \vee x_n^{\alpha_n}.$$

se numesc **conjunctii elementare**, respectiv **disjunctii elementare**.

**Definiția 6.4.3** a) Dacă  $c_1, \dots, c_m$  sunt conjuncții elementare, atunci formula  $\bigvee_{i=1}^m c_k$  se numește **formă normală disjunctivă**.

b) Dacă  $d_1, \dots, d_m$  disjuncții elementare, atunci formula  $\bigwedge_{i=1}^m d_k$  se numește **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  $\bar{x}_1 \rightarrow (x_1 \wedge x_2)$  și o aducem la formă normală disjunctivă respectiv conjunctivă:

$$\begin{aligned} \bar{x}_1 \rightarrow (x_1 \wedge x_2) &= \bar{\bar{x}_1} \vee (x_1 \wedge x_2) = x_1 \vee (x_1 \wedge x_2) = x_1 = \\ &= (x_1 \vee x_1) \wedge (x_1 \vee x_2) = x_1 \wedge (x_1 \vee x_2). \end{aligned}$$

**Definiția 6.4.5** a) Considerăm acum latică 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 funcție  $x : V^n \rightarrow V$ . O funcție obținută în acest fel se numește **funcție Boole**.

b) Fie  $f : V^n \rightarrow V$  o funcție și definim mulțimile  $T_f$  (*true*) și  $F_f$  (*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*. Obținem de asemenea că orice funcție  $f : V^n \rightarrow V$  este o funcție Boole.

**Teorema 6.4.6** Fie  $f : V^n \rightarrow V$  o funcție 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

$$f(x_1, \dots, x_n) = \bigwedge_{\alpha \in F_f} \bigvee_{i=1}^n x_i^{\bar{\alpha}_i}.$$

**Demonstrație.** 1) Dacă  $(\alpha_1, \dots, \alpha_n) \in T_f$ , atunci  $f(\alpha_1, \dots, \alpha_n) = 1$  și  $\bigwedge_{i=1}^n \alpha_i^{\alpha_i} = 1$ ; dacă  $(\beta_1, \dots, \beta_n) \neq (\alpha_1, \dots, \alpha_n)$ , 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  $i = 1, \dots, n$ . Rezultă că  $x_i = \alpha_i$ ,  $i = 1, \dots, n$ , deci  $(x_1, \dots, x_n) = (\alpha_1, \dots, \alpha_n) \in T_f$  și  $f(x_1, \dots, x_n) = 1$ .

Analog se demonstrează 2). ■

**Definiția 6.4.7** Formula de la punctul 1) (respectiv 2)) se numește **normală disjunctivă perfectă (FNDP)** (respectiv **normală conjunctivă perfectă (FNCP)**).

Să reținem că funcția constantă 0 nu are FNDP, iar funcția constantă 1 nu are FNCP.

**Exemplul 6.4.8** Fie  $f(x_1, x_2) = x_1 \rightarrow x_2$ ; atunci avem  $T_f = \{(0, 0), (0, 1), (1, 1)\}$  și  $F_f = \{(1, 0)\}$ , deci

$$f(x_1, x_2) = (x_1^0 \wedge x_2^0) \vee (x_1^0 \wedge x_2^1) \vee (x_1^1 \wedge x_2^1) = (\bar{x}_1 \wedge \bar{x}_2) \vee (\bar{x}_1 \wedge x_2) \vee (x_1 \wedge x_2); \quad (\text{FNDP})$$

$$f(x_1, x_2) = x_1^1 \vee x_2^0 = \bar{x}_1 \vee x_2. \quad (\text{FNCP})$$

**Exercițiul 112** Să se arate că  $f(x_1, x_2) = \overline{x_1 \wedge x_2} \rightarrow (\bar{x}_1 \vee \bar{x}_2)$  este egală cu funcția constantă 1, folosind:

a) tabele de adevăr ;    b) inele Boole.

**Exercițiul 113** Să se determine FNDP și FNCP pentru  $f(x_1, x_2, x_3) = \bar{x}_1 \rightarrow (x_2 \wedge \bar{x}_3)$ .

**Exercițiul 114** Fie  $f : V^3 \rightarrow V$  astfel încât  $T_f = \{(1, 1, 1), (1, 1, 0), (1, 0, 1), (1, 0, 0)\}$ .

a) Să se determine FNDP și 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

## MULȚIMI DE NUMERE

### 7.1 Mulțimea numerelor naturale

#### 7.1.1 Axiomele lui Peano

**Definiția 7.1.1** Axioma infinitului 3.1.2 spune că există o mulțime  $y$  astfel încât  $\emptyset \in y$  și  $x \in y$ ,  $x^+ \in y$ , unde  $x^+ = x \cup \{x\}$ .

Fie  $\mathcal{A}$  clasa mulților satisfăcând proprietatea de mai sus, numită clasa mulțimilor **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 mulțime, care se numește **mulțimea numerelor naturale**. Notății:  $\mathbb{N}$ ,  $0 := \emptyset$ ,  $1 := 0^+ = \{0\}$ ,  $2 := 1^+ = \{0, 1\}$ ,  $3 := 2^+ = \{0, 1, 2\}, \dots$ . Elementul  $s(n) = n^+$  se numește **succesorul** lui  $n$ . Notăm prin mai departe  $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ .

**Teorema 7.1.2 (Axiomele lui Peano)** *Tripletul format din mulțimea numerelor naturale  $\mathbb{N}$ , elementul 0 și funcția succesor  $s : \mathbb{N} \rightarrow \mathbb{N}$  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 inducției matematice)** *Dacă  $S \subseteq \mathbb{N}$ ,  $0 \in S$  și  $n \in S$ ,  $n^+ \in S$ , atunci  $S = \mathbb{N}$  (adică orice submulțime 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  $n = m$ .*

**Demonstrație.** 1), 2) și 3) sunt imediate din definiția 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 arătam că din  $y \in n$  rezultă  $y^+ \subseteq n$ , atunci am terminat. Fie

$$S = \{n \mid (n \in \mathbb{N}) \wedge \forall y((y \in n) \rightarrow (y^+ \subseteq n))\}.$$

Evident  $S \subseteq \mathbb{N}$ ,  $0 \in S$  și 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  $n \in S$  obținem  $y^+ \subseteq n \subseteq n^+$ , iar dacă  $y = n$ , atunci evident  $y^+ = n^+$ . Folosind 3) vedem că  $S = \mathbb{N}$ . ■

**Observații 7.1.3** a) Observăm că  $n \neq n^+$ , deoarece axioma regularității exclude anomalia  $n \in n$ .

b) Folosind principiul inducției matematice vedem ușor 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) și 5) respectiv observația de mai sus spun că **funcția succesor**

$$s : \mathbb{N} \rightarrow \mathbb{N}, \quad s(n) = n^+$$

este bine definită, este injectivă, dar nu este surjectivă, pentru că avem  $\text{Im } s = \mathbb{N}^*$ .

d) Am văzut că  $y \in n$  implică  $y^+ \subseteq n$ , adică  $y \subset n$ . Și invers este adevărat: dacă  $y \subset n$ , atunci  $y \in n$ . Într-adevăr, considerăm mulțimea

$$S = \{n \mid (n \in \mathbb{N}) \wedge \forall y((y \subset n) \rightarrow (y \in n))\}.$$

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  $n \in S$  și  $y \subset n^+ = n \cup \{n\}$ . 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  $n \in S$  obținem  $y \in n \subseteq n^+$ ; 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,  $0 \in S$  și dacă  $n \in S$ , atunci  $n^+ = n \cup \{n\} \in S$ .

Următoarea teoremă creează posibilitatea **definițiilor recursive (inductive)**.

**Teorema 7.1.4 (Teorema recurenței)** Dacă  $X$  este o mulțime,  $a \in X$  un element fixat și  $f : X \rightarrow X$  o funcție, atunci există o unică funcție  $u : \mathbb{N} \rightarrow X$  astfel încât  $u(0) = a$  și  $u(n^+) = f(u(n))$  pentru orice  $n \in \mathbb{N}$ .

**Demonstrație.** Considerăm relațiile  $\rho \in \mathbb{N} \times X$  și 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 relație satisfăcând proprietățile de mai sus. Este suficient de arătat că  $u$  este funcție, 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  $0 \in S$  și  $n \in S$ ,  $n^+ \in S$ , de unde din principiul inducției matematice rezultă că  $S = \mathbb{N}$ , adică  $u$  este funcție.

Dacă presupunem că  $0 \notin S$ , atunci ar exista  $b \neq a$  în  $X$  astfel încât  $(0, b) \in u$ . Dar atunci avem  $u \setminus \{(0, b)\} \in C$ , contradicție.

Fie acum  $n \in S$  și 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  $u \setminus \{(n^+, y)\} \in C$ , contradicție. 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, abstractie făcând de un unic izomorfism.

**Corolar 7.1.5** Dacă tripletul  $(\mathbb{N}', 0', s')$  satisface axiomele lui Peano, atunci este izomorf cu tripletul  $(\mathbb{N}, 0, s)$ , adică există o unică funcție  $u : \mathbb{N} \rightarrow \mathbb{N}'$  care satisface proprietățile:

$$(1) u(0) = 0', \quad (2) u \circ s = s' \circ u, \quad (3) u \text{ este bijectiv.}$$

**Exercițiul 115** Să se demonstreze Corolarul 7.1.5.

## 7.1.2 Operații și relația de ordine pe mulțimea numerelor naturale

**Definiția 7.1.6 (operații cu numere naturale)** a) Pe baza teoremei recurenței, pentru orice  $m \in \mathbb{N}$  există unic  $s_m : \mathbb{N} \rightarrow \mathbb{N}$  astfel încât  $s_m(0) = m$  și  $s_m(n^+) = s(s_m(n)) = (s_m(n))^+$  pentru orice  $n \in \mathbb{N}$ . Valoarea  $s_m(n)$  se numește **suma** lui  $m$  și  $n$ , și notăm  $s_m(n) =: m + n$ . Deci adunarea numerelor naturale se definește inductiv prin

$$m + 0 = m, \quad m + s(n) = s(m + n).$$

Să observăm că  $s(n) = n^+ = n + 1$ .

b) Pe baza teoremei recurenței, pentru orice  $m \in \mathbb{N}$  există unic  $p_m : \mathbb{N} \rightarrow \mathbb{N}$  astfel încât  $p_m(0) = 0$  și  $p_m(n^+) = p_m(n) + m$  pentru orice  $n \in \mathbb{N}$ . Valoarea  $p_m(n)$  se numește **produsul** lui  $m$  și  $n$ , și notăm  $p_m(n) =: mn$ . Deci înmulțirea numerelor naturale se definește inductiv prin

$$m \cdot 0 = 0, \quad ms(n) = mn + m.$$

Să observăm că  $n \cdot 1 = n$ .

**Teorema 7.1.7 (proprietățile de bază ale operațiilor)** 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 afirmații 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  $mp = np$  și  $p \neq 0$ , atunci  $m = n$ ;
- 15) Dacă  $mn = 1$ , atunci  $m = n = 1$ .

**Exercițiul 116** Să se demonstreze Teorema 7.1.7.

**Definiția 7.1.8 (ordonarea numerelor naturale)** Fie  $m, n \in \mathbb{N}$ . Spunem că  $m$  este mai mic decât  $n$ , notație  $m < n$ , 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  $n$  și notăm  $m \leq n$ .

**Propoziția 7.1.9 (caracterizarea relației „<”)** Pentru orice numere naturale  $m$  și  $n$  următoarele afirmații sunt echivalente:

- (i)  $m < n$ ;
- (ii)  $m \in n$ ;
- (iii)  $m \subset n$ .

**Demonstrație.** Am văzut că  $m \in n \Leftrightarrow m \subset n$ . Arătăm că  $m < n \Rightarrow m \in n$ . Fie

$$S = \{n \mid (n \in \mathbb{N}) \wedge \forall m((m < n) \rightarrow (m \in n))\}.$$

Evident  $0 \in S$ , deci prin inducție este suficient de arătat că  $n \in S \Rightarrow n' \in S$ . Într-adevăr, dacă  $n \in S$  și  $m < n'$ , 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

$$S = \{n \mid (n \in \mathbb{N}) \wedge \forall m((m \in n) \rightarrow (m < n))\}.$$

Evident  $0 \in S$ , deci prin inducție este suficient de arătat că  $n \in S \Rightarrow n' \in S$ . Într-adevăr, dacă  $n \in S$  și  $m \in n'$ , 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 (proprietățile de bază ale relației de ordine)** Fie  $m, n, p \in \mathbb{N}$ . Atunci

- 1) „ $\leq$ ” este relație de ordine totală;
- 2)  $0 \leq n$ ;
- 3) Dacă  $n \neq 0$ , atunci  $1 \leq n$ ;
- 4)  $m < n$  dacă și numai dacă  $m^+ \leq n$ ;
- 5)  $m \leq n$  dacă și 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 inducției matematice, varianta 2: inducție completă sau tare)** Dacă  $P(n)$  este un predicat pe mulțimea numerelor naturale astfel ca  $P(0)$  este adevărat și  $P(k)$  adevărat pentru orice  $k < n$ , atunci și  $P(n)$  este adevărat;

9) Dacă  $m < n$ , atunci  $m + p < n + p$ ;

10) Dacă  $m < n$  și  $p \neq 0$ , atunci  $mp < np$ ;

11) **(axioma lui Arhimede)** Dacă  $m \in \mathbb{N}$  și  $n \in \mathbb{N}^*$ , atunci există  $p \in \mathbb{N}$  astfel încât  $pn > m$ ;

12) **(teorema împărțirii cu rest)** Dacă  $m \in \mathbb{N}$  și  $n \in \mathbb{N}^*$ , atunci există unic  $q, r \in \mathbb{N}$  astfel încât  $m = nq + r$  și  $r < n$ .

**Demonstrație.** 7) Presupunem că  $(\mathbb{N}, \leq)$  nu e bine ordonată, adică există o submulțime  $A \neq \emptyset$  care nu are cel mai mic element. Fie  $S$  mulțimea minoranților stricti 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 inducție rezultă că  $S = \mathbb{N}$ , deci  $A = \emptyset$ , contradicție. ■

**Exercițiul 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 definițiile adunării și înmulțirii se pot scrie ca formule închise în limbajul  $\mathcal{L}_{\mathbb{N}}$  introdus în Exemplul 2.2.2. Amintim că limbajul  $\mathcal{L}_{\mathbb{N}}$  folosește, în afară de simbolurile logicii, simbolul de constantă 0 și trei simboluri de funcții:  $s$  de o variabilă, adunarea „+” de două variabile și înmulțirea „·” de două variabile. Axiomele lui Peano sunt:

(N1) Dacă  $\varphi$  este o formulă în  $\mathcal{L}_{\mathbb{N}}$ , atunci  $(\varphi_0^x \wedge \forall y(\varphi_y^x \rightarrow \varphi_{s(y)}^x)) \rightarrow \forall x\varphi$ .

Aici  $\varphi_0^x, \varphi_y^x, \varphi_{s(y)}^x$  înseamnă că în  $\varphi$ , variabila  $x$  se înlocuiește cu expresiile 0,  $y$ ,  $s(y)$ , respectiv.

(N2)  $\forall x(s(x) \neq 0)$

(N3)  $\forall x\forall y((s(x) = s(y)) \rightarrow (x = y))$

(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 definiției „teoriei” date în paragraful 2.4.2, putem spune că **teoria numerelor (aritmetica)** este mulțimea formulelor închise deductibile din axiomele lui Peano. Teorema 7.1.2 și definițiile ulterioare spun că mulțimea  $\mathbb{N}$  a numerelor naturale (cu elementul  $0 \in \mathbb{N}$ , funcția succesori  $s : \mathbb{N} \rightarrow \mathbb{N}$ , definițiile inductive ale adunării și înmulțirii) 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 și nici negația ei nu este deductibilă.*

*Mai general, dacă un sistem axiomatic necontradictoriu este suficient de larg încât să conțină teoria numerelor și este „suficient de regular”, atunci există o formulă închisă care nu este deductibilă și nici negația ei nu este deductibilă.*

## 7.2 Mulțimea numerelor întregi

Teoremele 7.1.7 și 7.1.10 spun că structura  $(\mathbb{N}, +, \cdot, \leq)$  este un semiinel asociativ, comutativ, cu unitate, fără divizori ai lui zero, bine ordonat și arhimedian. Una din probleme e că  $(\mathbb{N}, +)$  nu e grup. Rezolvăm asta prin lărgirea mulțimii  $\mathbb{N}$ . Vom construi mai jos mulțimea numerelor întregi pornind de la mulțimea numerelor naturale, respectiv definim adunarea, înmulțirea și ordonarea numerelor întregi.

**Definiția 7.2.1** a) Pe mulțimea  $\mathbb{N} \times \mathbb{N}$  definim relația omogenă

$$(m, n) \sim (p, q) \text{ dacă } m + q = n + p,$$

care este o relație de echivalență. Notăm prin  $\widetilde{(m, n)}$  clasă de echivalență a perechii  $(m, n)$ , deci

$$\widetilde{(m, n)} = \{(p, q) \in \mathbb{N} \times \mathbb{N} \mid (p, q) \sim (m, n)\}.$$

Mulțimea factor  $\mathbb{Z} := \mathbb{N} \times \mathbb{N} / \sim = \{\widetilde{(m, n)} \mid m, n \in \mathbb{N}\}$  se numește **mulțimea numerelor întregi**, iar clasele  $\widetilde{(m, n)}$  se numesc **numere întregi**.

b) Adunare și înmulțirea numerelor întregi se definesc astfel:

$$\widetilde{(m, n)} + \widetilde{(p, q)} := \widetilde{(m + p, n + q)}, \quad \widetilde{(m, n)} \widetilde{(p, q)} := \widetilde{(mp + nq, np + mq)}.$$

Aceste definiții nu depind de alegerea reprezentanților.

**Teorema 7.2.2**  $(\mathbb{Z}, +, \cdot)$  este domeniu de integritate, în care elementul nul este  $0 := \widetilde{(0, 0)} = \{\widetilde{(m, m)} \mid m \in \mathbb{N}\}$ , elementul unitate este  $1 := \widetilde{(1, 0)} = \{\widetilde{(m+1, m)} \mid m \in \mathbb{N}\}$  și opusul unui număr întreg  $\widetilde{(m, n)}$  este  $-(m, n) := \widetilde{(n, m)}$ .

**Exercițiul 118** a) Să se arate că relația „ $\sim$ ” este o relație de echivalență.

b) Să se arate că definițiile adunării și înmulțirii nu depind de alegerea reprezentanților.

c) Să se demonstreze Teorema 7.2.2.

**Definiția 7.2.3** Numerele întregi se ordonează prin relația:

$$\widetilde{(m, n)} < \widetilde{(p, q)} \text{ dacă și numai dacă } q + m < p + n.$$

**Teorema 7.2.4** 1) Definiția relației „ $\leq$ ” nu depinde de alegerea reprezentanților.

2)  $(\mathbb{Z}, \leq)$  este total ordonată.

3) Funcția  $\alpha: \mathbb{N} \rightarrow \mathbb{Z}_+$ ,  $\alpha(n) = \widetilde{(n, 0)}$  este bine definită, strict crescătoare și este izomorfism de semiinele.

4) Ordonarea numerelor întregi este compatibilă cu adunarea și înmulțirea, adică pentru orice  $a, b, c, d \in \mathbb{Z}$  avem

$$a < b, c \leq d \Rightarrow a + c < b + d, \quad a < b, c > 0 \Rightarrow ac < bc, \quad a < b, c < 0 \Rightarrow ac > bc.$$

5) (**Axioma lui Arhimede**) Pentru orice  $a \in \mathbb{Z}_+^*$  și  $b \in \mathbb{Z}$  există  $n \in \mathbb{N}$  astfel ca  $na > b$ .

**Observații 7.2.5** Vom identifica:  $\mathbb{N}$  cu  $\alpha(\mathbb{N}) = \widetilde{(n, 0)}$ ,  $\mathbb{N}$  cu  $\mathbb{Z}_+$ , unde

$$\mathbb{Z}_+ = \{a \in \mathbb{Z} \mid a \geq 0\} = \{\widetilde{(m, n)} \mid m \geq n\}.$$

Ținând cont de aceste identificări, pentru orice  $m, n \in \mathbb{N}$  avem

$$m - n = m + (-n) = \widetilde{(m, 0)} + (-\widetilde{(n, 0)}) = \widetilde{(m, 0)} + \widetilde{(0, n)} = \widetilde{(m, n)}.$$

**Exercițiul 119** Să se demonstreze Teorema 7.2.4.

## 7.3 Elemente de aritmetica numerelor întregi

Aritmetica este partea elementară a teoriei numerelor și studiază în special proprietățile operațiilor de bază. Cele mai vechi dovezi ale utilizării operațiilor aritmetice au aproape 400 de ani și provin de la egipteni și babilonieni. Sistemul de numerație al babilonienilor era în baza 60 și folosea notația pozițională. Civilizația 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 și rezolvarea ecuațiilor în numere întregi. Numerațiile hindu-arabe au început să fie folosite din secolul 6 e.n. Introducerea cifrei 0, notația pozițională și ideea de valoare dependentă de poziție au dus la dezvoltarea unor metode simple de calcul în baza 10.

### 7.3.1 Teorema împărțirii cu rest

Știm că inelul  $(\mathbb{Z}, +, \cdot)$  al numerelor întregi este domeniu de integritate. Vom formula teorema împărțirii cu rest în acest context. Am văzut 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  $n \in \mathbb{Z}$  și  $\varepsilon \in [0, 1)$ . Notăție:  $n =: [x]$  este *partea întreagă* a lui  $x$ , iar  $\varepsilon =: \{x\}$  este *partea fracționară* a lui  $x$ . Așadar,  $[x] \in \mathbb{Z}$ ,  $\{x\} = x - [x] \in [0, 1)$ , și  $[x] \leq x < [x] + 1$ .

**Teorema 7.3.1 (Teorema împărțirii 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.

**Demonstrație.** Fie  $r := \min(\{a - kb \mid k \in \mathbb{Z}\} \cap \mathbb{N})$ , și fie  $q := (a - r)/b$ , deci  $q$  și  $r$  există.

Dacă  $a = bq + r = bq_1 + r_1$ , unde  $0 \leq r_1 < |b|$ , atunci  $|b||q - q_1| = |r - r_1| < |b|$ , deci  $q - q_1 = 0$ , și de aici  $r = r_1$ . ■

**Corolar 7.3.2 (Teorema împărțirii 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,  $r \geq 0 \Leftrightarrow \left\{ \frac{a}{b} \right\} \leq \frac{1}{2}$ , și  $r < 0 \Leftrightarrow \left\{ \frac{a}{b} \right\} > \frac{1}{2}$ . Spunem că  $r$  az cel mai mic rest în modul.

De exemplu, dacă  $b \geq 3$  este un număr impar, atunci resturile sunt  $0, \pm 1, \pm 2, \dots, \pm \frac{b-1}{2}$ ; dacă  $b \geq 2$  este un număr par, atunci resturile sunt  $0, \pm 1, \pm 2, \dots, \pm(\frac{b}{2} - 1), \frac{b}{2}$ .

**Exercițiul 120** Să se arate că

- pătratul oricărui număr întreg este de forma  $3k$  sau  $3k + 1$ ;
- pătratul oricărui număr întreg este de forma  $5k$  sau  $5k + 1$  sau  $5k - 1$ ;
- pătratul oricărui număr întreg este de forma  $7k$  sau  $7k + 1$  sau  $7k - 1$ .

**Corolar 7.3.3 (sistem de numerație în baza  $b$ )** Fie  $b \in \mathbb{N}$ ,  $b > 1$ . Atunci orice număr  $n \in \mathbb{N}^*$  se scrie în mod unic sub forma

$$n = c_k b^k + c_{k-1} b^{k-1} + \dots + c_1 b + c_0,$$

unde  $c_i \in \mathbb{N}$ ,  $0 \leq c_i \leq b - 1$ ,  $i \in \{1, 2, \dots, k\}$ ,  $c_k \neq 0$ . (Numerele  $c_i$  sunt **cifrele** lui  $n$ .) Numărul cifrelor este  $k = \lceil \log_b n \rceil + 1$ .

**Demonstrație.** Conform Teoremei 7.3.1 avem

$$\begin{aligned} n &= bq_0 + c_0, & 0 \leq c_0 \leq b - 1 \\ q_0 &= bq_1 + c_1, & 0 \leq c_1 \leq b - 1, \\ q_1 &= bq_2 + c_2, & 0 \leq c_2 \leq b - 1, \\ &\dots \end{aligned}$$

și  $q_i, c_i$  în mod unic determinate. Aici  $q_0 > q_1 > q_2 > \dots$ , și dacă  $q_k = 0$  este primul cât nul, atunci  $q_{k-1} = c_k$ ,  $0 < c_k \leq b - 1$ . Înlocuind obținem

$$n = b(bq_1 + c_1) + c_0 = b(b(bq_2 + c_2) + c_1) + c_0 = \dots = c_k b^k + c_{k-1} b^{k-1} + \dots + c_1 b + c_0.$$

Observăm că deoarece  $0 < c_k < b$ , avem  $b^k \leq n < b^{k+1}$ , deci  $k \leq \log_b n < k + 1$ . ■

**Exercițiul 121** Să se scrie numărul:

- $309_{(10)}$  în bazele 7, 2, 16;
- $214_{(7)}$  în bazele 10, 2, 16;

**Exercițiul 122** Să se arate că pentru orice  $m > n$ , numărul

$$123 \dots (n-1)n(n-1) \dots 321$$

scris în baza  $m$  este pătrat perfect.

### 7.3.2 Divizibilitate. Cel mai mare divizor comun

**Definiția 7.3.4** Fie  $a$  și  $b$  numere întregi.

- Spunem că  $a$  **divide** pe  $b$ -nek (notație:  $a|b$ ) dacă există  $x \in \mathbb{Z}$  astfel încât  $b = ax$ .
- Un număr  $d \in \mathbb{N}$  este **cel mai mare divizor comun** al lui  $a$  și  $b$  (notație:  $d = (a, b)$ ) dacă

- $d|a$  și  $d|b$ ;
- dacă  $d' \in \mathbb{Z}$ ,  $d'|a$  și  $d'|b$ , atunci  $d'|d$ .

- Un număr  $m \in \mathbb{N}$  este **cel mai mic multiplu comun** al lui  $a$  și  $b$  (notație:  $m = [a, b]$ ) dacă

- $a|m$  și  $b|m$ ;
  - dacă  $m' \in \mathbb{Z}$ ,  $a|m'$  și  $b|m'$ , atunci  $m|m'$ .
- d)  $a$  și  $b$  sunt **relativ prime** dacă  $(a, b) = 1$ .

**Exercițiul 123** a) 0 este divizibil cu orice număr; orice număr este divizibil cu 1.

- $a|b, a|c \Rightarrow a|b \pm c$ .
- $a|b \Rightarrow ax|bx$  pentru orice  $x \in \mathbb{Z}$ . Invers, dacă  $ax|bx$ ,  $x \neq 0$ , atunci  $a|b$ .
- $x|y \iff (x, y) = x \iff [x, y] = y$ .

**Exercițiul 124** a) Fie  $a, b \in \mathbb{Z}$ . Să se arate că  $(a, b)$  există, și 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

$$d := \min\{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}$$

și să se arate că  $d = (a, b)$ .

b)  $(a, b) = 1 \Leftrightarrow$  există  $u, v \in \mathbb{Z}$  astfel încât  $au + bv = 1$ .

**Definiția 7.3.5** Următorul șir de calcule se numește **algoritmul lui Euclid** aplicat numerelor  $a$  și  $b$ .

$$\begin{aligned} a &= bq_0 + r_0, & 0 < r_0 < |b|; \\ b &= r_0q_1 + r_1, & 0 < r_1 < r_0; \\ r_0 &= r_1q_2 + r_2, & 0 < r_2 < r_1; \\ r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2; \\ &\dots \\ r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1}, & 0 < r_{n-1} < r_{n-2}; \\ r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1}; \\ r_{n-1} &= r_nq_{n+1} + r_{n+1}, & 0 < r_{n+1} < r_n; \\ r_n &= r_{n+1}q_{n+2} + r_{n+2}, & r_{n+2} = 0. \end{aligned}$$

Algoritmul se termină, deoarece șirul  $(r_k)_{k \geq 0}$  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  $a$  și  $b$  este egal cu ultimul rest nenul, adică  $d := (a, b) = r_{n+1}$ .*

2) *Știm că există  $u, v \in \mathbb{Z}$  astfel încât  $d = (a, b) = au + bv$ . Numerele  $u$  și  $v$  pot fi calculate folosind algoritmul lui Euclid.*

**Demonstrație.** 1) Se arată ușor că dacă  $a = bq + r$ , atunci  $(a, b) = (b, r)$ ; rezultă că

$$(a, b) = (b, r_0) = (r_0, r_1) = \dots = (r_{n-1}, r_n) = (r_n, r_{n+1}) = r_{n+1}.$$

2) Avem următorul șir de calcule ce *extinde* algoritmul lui Euclid:

$$\begin{aligned} (a, b) &= r_{n+1} = r_{n-1} - r_nq_{n+1} = \\ &= r_{n-1} - (r_{n-2} - r_{n-1}q_n)q_{n+1} = \\ &= r_{n-1}(1 + q_nq_{n+1}) - r_{n-2}q_{n+1} = \\ &= r_{n-1}u_{n-1} + r_{n-2}v_{n-1}, \end{aligned}$$

și continuăm prin inducție. ■

**Exercițiul 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)  $a = 2613, b = -2171$ .

**Exercițiul 126** a) Dacă  $x \in \mathbb{N}$ , atunci  $(ax, bx) = (a, b)x$ .

b) Dacă  $d = (a, b)$ ,  $a = da'$  și  $b = db'$ , 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)  $a|c$  și  $b|c \Rightarrow ab|c$ .

d) Dacă  $d = (a, b)$ ,  $a = da'$  și  $b = db'$ , atunci

$$[a, b] = a'b'd = \frac{ab}{d}.$$

**Definiția 7.3.7** Fie  $x_1, \dots, x_n$  numere întregi, unde  $n \in \mathbb{N}^*$ , și fie  $d, m \in \mathbb{N}$ . Prin definiție,

$$\begin{aligned} \text{a) } d = (x_1, \dots, x_n) &\Leftrightarrow \begin{cases} d|x_1, \dots, d|x_n, \\ \text{dacă } d'|x_1, \dots, d'|x_n, \text{ atunci } d'|d. \end{cases} \\ \text{b) } m = [x_1, \dots, x_n] &\Leftrightarrow \begin{cases} x_1|m, \dots, x_n|m, \\ \text{dacă } x_1|m', \dots, x_n|m', \text{ atunci } m|m'. \end{cases} \end{aligned}$$

**Exercițiul 127** Fie  $x_1, \dots, x_n$  numere întregi. Să se arate că:

- $(x_1, \dots, x_{n-1}, x_n) = ((x_1, \dots, x_{n-1}), x_n)$ ;  $[x_1, \dots, x_{n-1}, x_n] = [[x_1, \dots, x_{n-1}], x_n]$ .
- $(x_1, \dots, x_n) = \min\{x \in \mathbb{N}^* \mid \exists u_i \in \mathbb{Z} \text{ astfel încât } x = \sum_{i=1}^n u_i x_i\}$ . În particular,  $(x_1, \dots, x_n) = d \Rightarrow \exists u_i \in \mathbb{Z}$  astfel ca  $\sum_{i=1}^n u_i x_i = d$ .
- $(x_1, \dots, x_n) = 1 \Leftrightarrow \exists u_i \in \mathbb{Z}$  astfel încât  $\sum_{i=1}^n u_i x_i = 1$ .
- $(x_1 x, \dots, x_n x) = (x_1, \dots, x_n) x$  pentru orice  $x \in \mathbb{N}$ .
- Dacă  $(x, x_i) = 1$ ,  $i = 1, \dots, n$ , atunci  $(x, x_1 \dots x_n) = 1$ .
- 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*.)

**Exercițiul 128** Fie  $a, b \in \mathbb{Z}$  și  $n \in \mathbb{N}^*$ . Atunci

- $a - b \mid a^n - b^n$ ,
- dacă  $n$  este impar, atunci  $a + b \mid a^n + b^n$ ,
- dacă  $n$  este par, atunci  $a + b \mid a^n - b^n$ .

**Exercițiul 129** Să se arate că:

- pentru orice  $n \in \mathbb{N}$ ,  $n^5 - n$  este divizibil 30;
- $7 \mid 2^n - 1$  dacă și numai dacă  $3 \mid n$ , unde  $n \in \mathbb{N}$ ;
- pentru orice număr impar  $m \in \mathbb{N}^*$  avem  $240 \mid m^5 - m$ .

**Exercițiul 130** Fie  $a, b, c \in \mathbb{Z}$ . Să se arate că

- $(a, [b, c]) = [(a, b), (a, c)]$ ,  $[a, (b, c)] = ([a, b], [a, c])$ ;
- dacă  $(a, b) = (a, c)$  și  $[a, b] = [a, c]$ , atunci  $b = c$ .
- $[a, b, c](a, b)(b, c)(c, a) = abc(a, b, c)$ .

**Exercițiul 131** Fie  $a, m, n \in \mathbb{N}^*$ ,  $a \geq 2$ . Să se arate că

- $(a^m - 1, a^n - 1) = a^{(m, n)} - 1$ .
- Dacă  $(a, b) = 1$ , atunci  $(a^m - b^m, a^n - b^n) = a^d - b^d$ .
- Dacă  $m > n$ , atunci  $a^{2^n} + 1 \mid a^{2^m} - 1$ .

### 7.3.3 Numere prime. Teorema fundamentală a aritmeticii

**Definiția 7.3.8** Numărul  $p \in \mathbb{N}$  se numește **prim**, dacă  $p \neq 1$ , și dacă  $a \in \mathbb{Z}$ ,  $a \mid p$ , atunci  $a = \pm 1$  sau  $a = \pm p$  (adică  $p$  nu are divizori proprii).

**Observații 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). Pașii sunt următorii:

- Se scriu toate numerele de la 2 la  $n$ .
- Inițial, fie  $p := 2$ .
- Marcăm în listă toți multiplii lui  $p$  cu excepția lui  $p$  (adică pe  $2p, 3p, \dots$ ).
- Căutăm în listă primul număr nemarcat  $q > p$ . Dacă un astfel de  $q$  nu există, am terminat; altfel fie  $p := q$  și mergem din nou la pasul (3).

Algoritmul evident se termină, iar numerele nemarcate sunt toate numerele prime mai mici decât  $n$ .

**Exercițiul 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  $p \mid ab$ , atunci  $p \mid a$  sau  $p \mid b$ .

**Demonstrație.** Fie  $p \in \mathbb{N}$  prim. Atunci  $p \neq 0$ ,  $p \neq 1$ , și presupunem că  $p \mid ab$ ,  $p \nmid a$ . Trebuie să arătăm că  $p \mid b$ . Deoarece  $p \mid ab$ , 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  $p \mid b$ . Invers, presupunem că  $p = ab$ ; atunci  $p \mid ab$  și din ipoteză putem presupune că  $p \mid a$ ; dar  $a \mid p$ , 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 (abstracție 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 și  $k_i \in \mathbb{N}^*$ ,  $1 \leq i \leq r$ .



**Demonstrație.** *Existența 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  $a_1 | a$  și  $a_1 \neq a$ . Dacă  $a_1$  nu e prim, atunci  $a_1 = a_2 a_2'$  rezultă că  $a_2 | a_1$  și  $a_2 \neq a_1$  (adică  $a_2 < a_1$ ). Continuând procedura, am obține șirul 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 pași, 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  $p_1 | q_1 \dots q_m$  și  $p_1$  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 inducție, obținem că  $n = m$  și  $p_i = q_i$  pentru orice  $i \in \{1, \dots, n\}$ . ■

**Corolar 7.3.12** Dacă  $a = \pm p_1^{k_1} \dots p_r^{k_r}$  și  $b = \pm p_1^{l_1} \dots p_r^{l_r}$ , 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.

**Demonstrație.** Presupunem prin absurd că afirmația nu e adevărată și fie  $p_1, p_2, \dots, p_r$  toate numerele prime. Considerăm numărul  $N = p_1 p_2 \dots p_r + 1$ , care evidențiază nu e divizibil cu niciunul din numerele  $p_1, p_2, \dots, p_r$ . Dar  $N$  are un divizor prim  $q$  care nu e în șirul  $p_1, p_2, \dots, p_r$ , ceea ce este o contradicție. ■

**Exercițiul 133** Să se arate că dacă  $p$  număr prim, atunci  $p | C_p^k$ , pentru orice  $k$ ,  $1 \leq k \leq p - 1$ .

**Exercițiul 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.

**Observații 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 afirmației 1) de mai sus este falsă. Se știe că  $F_n$  este compus dacă  $5 \leq n \leq 32$ . Nu se știe 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 afirmației 2) de mai sus este falsă. Nu se știe care din numerele  $M_p$  sunt prime și de asemenea, nu se știe dacă există o infinitate de numere prime ale lui Mersenne.

### 7.3.4 Congruențe. Inelul $\mathbb{Z}_n$ al claselor de resturi modulo $n$

**Definiția 7.3.15** Fie  $n \in \mathbb{N}$  un număr natural.

a) Congruența modulo  $n$  este relația pe  $\mathbb{Z}$  definită astfel: dacă  $a, b \in \mathbb{Z}$ , atunci

$$a \equiv b \pmod{n} \stackrel{\text{def}}{\iff} n | b - a \iff b - a \in n\mathbb{Z} \iff \exists k \in \mathbb{Z} : b = a + nk \iff a \bmod n = b \bmod n.$$

Notăție:  $\hat{a} = [a]_n = \{a + nk \mid k \in \mathbb{Z}\} = a + n\mathbb{Z}$  este clasa lui  $a$  modulo  $n$ .

b) Considerăm, conform Definiției 4.4.4, mulțimea 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 operațiile sunt definite astfel (vezi Teorema 8.3.3):

$$\hat{a} + \hat{b} \stackrel{\text{def}}{=} \widehat{a + b}, \quad \hat{a}\hat{b} \stackrel{\text{def}}{=} \widehat{ab}.$$

**Observații 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  $a \equiv b \pmod{0} \iff b - a = 0 \iff b = a$ ; 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 împărțirii 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  $|\mathbb{Z}_n| = n$ .

**Exercițiul 135** Dacă  $a \equiv b \pmod{n}$ , atunci  $(a, n) = (b, n)$ .

**Exercițiul 136 (proprietățile de bază ale congruențelor)** Fie  $a, b, c, d \in \mathbb{Z}$  și  $m, m_1, m_2, k \in \mathbb{N}^*$ . Să se arate că:

- 1) dacă  $a \equiv b \pmod{m}$  și  $c \equiv d \pmod{m}$ , atunci  $a + c \equiv b + d \pmod{m}$  și  $ac \equiv bd \pmod{m}$ ;
- 2) dacă  $f \in \mathbb{Z}[X]$  este un polinom și  $a \equiv b \pmod{m}$ , atunci  $f(a) \equiv f(b) \pmod{m}$ ;
- 3) dacă  $a \equiv b \pmod{m}$  și  $d \mid a, b, m$ , atunci  $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ ;
- 4) dacă  $ac \equiv bc \pmod{m}$  și  $(c, m) = 1$ , atunci  $a \equiv b \pmod{m}$ ;
- 5) dacă  $a \equiv b \pmod{m_1}$  și  $a \equiv b \pmod{m_2}$ , atunci  $a \equiv b \pmod{[m_1, m_2]}$ .

**Exercițiul 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 și 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 afirmații 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)  $(a, n) = 1$ .

**Demonstrație.** (i) $\Rightarrow$ (ii).  $\hat{a}\hat{b} = \hat{0}$ . Înmulțind cu  $\hat{a}^{-1}$  obținem  $\hat{b} = \hat{0}$ .

(ii) $\Rightarrow$ (iii)  $\Leftrightarrow$  (iii)  $\Rightarrow$  (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,

$$\widehat{an'} = \widehat{an'} = \widehat{a'dn'} = \widehat{a'n} = \widehat{a'n} = \widehat{a'n} = \widehat{0}.$$

(iii) $\Rightarrow$ (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 afirmații 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.

**Demonstrație.** (i) $\Leftrightarrow$ (ii). Evident, orice corp comutativ este domeniu de integritate; invers, se arată ușor că orice domeniu de integritate finit este corp.

(i) $\Leftrightarrow$ (iii).  $\mathbb{Z}_n$  este corp  $\Leftrightarrow$  pentru orice  $0 < a < n$  avem  $(a, n) = 1 \Leftrightarrow n$  este prim. ■

**Observații 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  $\varphi: \mathbb{N}^* \rightarrow \mathbb{C}$  este funcția 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  $a \in \mathbb{Z}$  și pentru orice număr prim  $p$ , avem  $a^p \equiv a \pmod{p}$ .

**Demonstrație.** a) Rezultă din Teorema lui Lagrange din teoria grupurilor.

b) Dacă  $p \nmid a$  atunci  $(p, a) = 1 \stackrel{a)}{\Rightarrow} a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^{p-1} \equiv a \pmod{p}$ . Dacă  $p \mid a$ , atunci  $p \mid a^p$ , deci  $p \mid a^p - a$ , de unde  $a^p \equiv a \pmod{p}$ . ■

**Exercițiul 138** Să se calculeze cel mai mic rest pozitiv:

a)  $2^{1000000} \pmod{77}$ ;    b)  $3^{400} \pmod{100}$     c)  $3^{100000} \pmod{101}$ .

**Exercițiul 139** Să se arate că  $42 \mid n^7 - n$  și  $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \mid n^{13} - n$  pentru orice  $n \in \mathbb{N}$ .

### 7.3.6 Rezolvarea congruențelor și a ecuațiilor diofantice de gradul I

#### A. Congruența $ax \equiv b \pmod{n}$

Fie  $a, b \in \mathbb{Z}$ ,  $n \in \mathbb{N}^*$ ,  $n \geq 2$  date și fie  $x \in \mathbb{Z}$  necunoscută. Fie  $d := (a, n)$ ,  $a = a'd$ ,  $n = n'd$ , deci  $(a', n') = 1$ .

- Dacă  $x$  este soluție  $\Rightarrow b - ax = nk$  cu  $k \in \mathbb{Z} \Rightarrow b = ax + nk$ , este divizibil cu  $d$ , deoarece  $a \cdot d$  și  $n \cdot d$ . Deci dacă  $d \nmid b$  atunci nu există soluție.
- Presupunem că  $d \mid b$  și fie  $b = b'd$ . Atunci  $ax \equiv b \pmod{n} \Leftrightarrow a'x \equiv b' \pmod{n'} \quad (1)$ .

Congruența (1) este echivalentă cu ecuația  $\hat{a}'\hat{x} = \hat{b}'$  în  $\mathbb{Z}_{n'}$ . Din  $(a', n') = 1 \Rightarrow \exists \hat{a}'^{-1} \in U(\mathbb{Z}_{n'})$  ( $\hat{a}'^{-1}$  se determină cu algoritmul lui Euclid). Deci în  $\mathbb{Z}_{n'}$  avem soluție unică  $\hat{x} = \hat{b}'\hat{a}'^{-1}$ . Fie cel mai mică soluție pozitivă  $x_0$  a lui (1) ( $0 \leq x_0 < n'$ ). Atunci cele  $d$  soluții distincte (adică necongruente modulo  $n$ ) ale congruenței (A) sunt:  $x_0, x_0 + n', \dots, x_0 + (d-1)n'$  (mai exact, acestea sunt cele mai mici soluții pozitive).

**Exercițiul 140** Să se rezolve congruențele:

a)  $x \equiv 2 \pmod{3}$ ;    b)  $9x \equiv 12 \pmod{21}$ ;    c)  $27x \equiv 72 \pmod{900}$ ;    d)  $68x \equiv 16 \pmod{72}$ .

**Exercițiul 141** Să se rezolve în  $\mathbb{Z}_{18}$  ecuațiile:

a)  $7x = 15$ ;    b)  $8x = 11$ ;    c)  $10x = 16$ .

#### B. Ecuația diofantică $a_1x_1 + \dots + a_nx_n = c$

1) Fie  $n = 2$ . Considerăm ecuația

$$ax + by = c,$$

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  $\exists (x, y)$  soluție, atunci  $d \mid c$ . Deci, dacă  $d \nmid c$  atunci nu există soluție.

Presupunem deci că  $d \mid c$ . Fie  $a = a'd$ ,  $b = b'd$ . Căutăm o soluție particulară. Fie  $u, v \in \mathbb{Z}$  astfel încât  $d = au + bv$  (folosim algoritmul lui Euclid). Înmulțim cu  $c'$ :  $\Rightarrow c = ac'u + bc'v$ . Fie  $x_0 := c'u$ ,  $y := c'v$ , deci  $(x_0, y_0)$  este soluție particulară.

Căutăm acum soluția generală. Avem

$$ax + by = c \Leftrightarrow ax + by = ax_0 + by_0 \Leftrightarrow a(x - x_0) + b(y - y_0) = 0 \Leftrightarrow a'(x - x_0) + b'(y - y_0) = 0.$$

Presupunem că  $(x, y) \in \mathbb{Z}$  este soluție. 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 soluția 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 soluție a ecuației  $ax + by = c$ .

2) În general, arătăm că ecuația  $a_1x_1 + a_2x_2 + \dots + a_nx_n = c$  are soluție dacă și numai dacă  $(a_1, \dots, a_n) \mid c$ .

Într-adevăr, dacă ecuația  $a_1x_1 + a_2x_2 + \dots + a_nx_n = c$  are soluție, atunci  $(a_1, \dots, a_n)$  divide membrul stâng, deci și pe cel drept. Invers, presupunem că  $c = (a_1, \dots, a_n)c'$ . Există numerele întregi  $x'_1, \dots, x'_n$  astfel ca

$$a_1x'_1 + a_2x'_2 + \dots + a_nx'_n = (a_1, \dots, a_n)c'.$$

Înmulțim cu  $c'$  și obținem:

$$x_1 = c'x'_1, \quad x_2 = c'x'_2, \quad \dots, \quad x_n = c'x'_n.$$

**Observații 7.3.21** Observăm că ecuația  $ax + by = c$  este echivalentă cu congruența  $ax \equiv c \pmod{b}$  sau cu  $by \equiv c \pmod{a}$ .

Fie  $d = (a, b)$ , atunci  $a = a_1d$ ,  $b = b_1d$  și  $c = c_1d$ , unde  $(a_1, b_1) = 1$ . Atunci în inelul  $\mathbb{Z}_{b_1}$  avem

$$a_1x + b_1y = c_1 \Leftrightarrow a_1x \equiv c_1 \pmod{b_1} \Leftrightarrow \hat{a}_1 \hat{x}_1 = \hat{c}_1.$$

Dar  $(a_1, b_1) = 1 \Rightarrow \exists \hat{a}_1^{-1}$  de unde rezultă că  $\hat{x} = \hat{a}_1^{-1} \hat{c}_1$  este unica soluție.

**Exemplul 7.3.22** Considerăm ecuația  $18x + 28y = 10$ . Deoarece  $(18, 28) = 2 \mid 10$  rezultă că există soluție. Considerăm ecuația redusă  $9x + 14y = 5$ . Rezolvăm congruența  $9x \equiv 5 \pmod{14}$ , adică ecuația  $\hat{9}\hat{x} = \hat{5}$  în  $\mathbb{Z}_{14}$ . Avem  $(9, 14) = 1 \Rightarrow \exists u, v \in \mathbb{Z}: 9u + 14v = 1$ . Deoarece  $14 = 9 \cdot 1 + 5$ ,  $9 = 5 \cdot 1 + 4$ ,  $5 = 4 \cdot 1 + 1$ , obținem  $u = -3$ ,  $v = 2$ . Deci  $\hat{x} = \hat{1} \cdot \hat{5}$  în inelul  $\mathbb{Z}_{14}$ , adică  $x \equiv 13 \pmod{14}$ .

**Exemplul 7.3.23 (Rezolvarea prin micșorarea modului coeficienților)** 1) Considerăm ecuația  $25x + 7y = 4$ . Deoarece  $|25| > |7|$ , exprimăm pe  $y$ :

$$y = \frac{4 - 25x}{7} = \frac{4 + 3x}{7} - 4x \in \mathbb{Z} \Leftrightarrow 4 + 3x = 7z, \quad |3| < |7|$$

$$x = \frac{7z - 4}{3} = \frac{6z + z - 3 - 1}{3} = 2z - 1 + \frac{z - 1}{3} \in \mathbb{Z} \Leftrightarrow z - 1 = 3t \Leftrightarrow z = 3t + 1$$

$$\Rightarrow x = \frac{21t + 3}{3} = 7t + 1, \quad y = \frac{4 - 175t - 25}{7} = -25t - 3, \quad t \in \mathbb{Z}.$$

2) Să se rezolve ecuația  $16x - 23y + 9z = 15$ . Este util să începem cu cel mai mic coeficient în modul:

$$z = \frac{15 - 16x + 23y}{9} = 1 - 2x + 2y + \frac{6 + 2x + 5y}{9}.$$

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 obținem

$$x = -3 + 2t + 5u, \quad y = t - 2u, \quad z = 7 - t - 14u, \quad t, u \in \mathbb{Z}.$$

Verificăm că acestea sunt soluții:

$$16(-3 + 2t + 5u) - 23(t - 2u) + 9(7 - t - 14u) = 25 + (32 - 23 - 9)t + (80 + 46 - 126)u = 25.$$

**Exercițiul 142** Să se rezolve:

$$1) 12x + 31y = 23; \quad 2) 25x - 13y - 7z = 4; \quad 3) \begin{cases} 25x - 13y + 7z = 4 \\ 7x + 4y - 2z + 3t = 2 \end{cases}$$

### 7.3.7 Teorema chineză a resturilor. Sisteme de congruențe

**Teorema 7.3.24 (Teorema chineză a resturilor)** Fie  $n_1, \dots, n_r \in \mathbb{N}^*$ ,  $(n_i, n_j) = 1$ ,  $1 \leq i, j \leq r$ ,  $i \neq j$ . Atunci

$$\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r} \simeq \mathbb{Z}_{n_1 \dots n_r}.$$

**Demonstrație.** Fie funcția  $f: \mathbb{Z} \rightarrow \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}$   $f(a) = ([a]_{n_1}, \dots, [a]_{n_r})$ . 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  $\text{Ker } f$ :

$$\begin{aligned} \text{Ker } f &= \{a \in \mathbb{Z} \mid f(a) = ([a]_{n_1}, \dots, [a]_{n_r}) = ([0]_{n_1}, \dots, [0]_{n_r})\} = \\ &= \{a \in \mathbb{Z} \mid n_i \mid a, \quad i = 1, \dots, r\} = \\ &= \{a \in \mathbb{Z} \mid n_1 \dots n_r \mid a\} = n_1 \dots n_r \mathbb{Z}. \end{aligned}$$

Din Teorema I de izomorfism 8.3.4 rezultă că avem izomorfismul de inele

$$\bar{f}: \mathbb{Z}/\text{Ker } f \longrightarrow \text{Im } f, \quad \bar{f}([\mathbf{a}]_{n_1, \dots, n_r}) = f(\mathbf{a}) = ([\mathbf{a}]_{n_1}, \dots, [\mathbf{a}]_{n_r}),$$

unde  $\mathbb{Z}/\text{Ker } f = \mathbb{Z}_{n_1 \dots n_r}$  și  $\text{Im } f \subseteq \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}$ . Arătăm prin două metode că  $\bar{f}$  este surjectiv.

(1) Deoarece  $|\mathbb{Z}_{n_1 \dots n_r}| = n_1 \dots n_r$  și  $\bar{f}$  este bijectiv, rezultă că  $|\text{Im } f| = n_1 \dots n_r$ . Dar  $\text{Im } f \subseteq \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}$ , și  $|\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}| = n_1 \dots n_r$ , deci  $\text{Im } f = \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}$ .

(2) Bijectivitatea lui  $\bar{f}$  este echivalentă cu afirmația că pentru orice  $\mathbf{a}_1, \dots, \mathbf{a}_r \in \mathbb{Z}$  sistemul de congruențe

$$\begin{cases} x \equiv \mathbf{a}_1 \pmod{n_1} \\ \vdots \\ x \equiv \mathbf{a}_r \pmod{n_r} \end{cases}$$

are soluție în  $\mathbb{Z}$  și mai mult, orice două soluții sunt congruente modulo  $n_1 \dots n_r$ . Pentru exprimarea soluției introducem notațiile:  $N := n_1 \dots n_r$ ,  $M_i := \frac{N}{n_i}$ . 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 soluție modulo  $N$ . ■

**Exercițiul 143** Să se rezolve sistemele de congruențe:

$$\text{a) } \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases} ; \quad \text{b) } \begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \\ x \equiv 6 \pmod{7} \end{cases} ; \quad \text{c) } \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 6 \pmod{7} \\ x \equiv 8 \pmod{16} \end{cases} .$$

**Corolar 7.3.25** Presupunem că  $n_1, \dots, n_r \in \mathbb{N}^*$  relativ prime două câte două. Atunci avem izomorfismul de grupuri

$$\mathbf{U}(\mathbb{Z}_{n_1, \dots, n_r}) \simeq \mathbf{U}(\mathbb{Z}_{n_1}) \times \dots \times \mathbf{U}(\mathbb{Z}_{n_r}).$$

**Demonstrație.** Din Teorema chineză a resturilor 7.3.24 rezultă că

$$(\mathbf{U}(\mathbb{Z}_{n_1, \dots, n_r}), \cdot) \simeq (\mathbf{U}(\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}), \cdot) = (\mathbf{U}(\mathbb{Z}_{n_1}) \times \dots \times \mathbf{U}(\mathbb{Z}_{n_r})). \quad \blacksquare$$

**Corolar 7.3.26** Dacă  $(m, n) = 1$ , atunci  $\varphi(mn) = \varphi(m)\varphi(n)$ , adică funcția  $\varphi$  a lui Euler este funcție aritmetică multiplicativă. În general, dacă  $(n_i, n_j) = 1, 1 \leq i < j \leq r$ , atunci  $\varphi(n_1 \dots n_r) = \varphi(n_1) \dots \varphi(n_r)$ .

**Corolar 7.3.27** Fie  $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ , unde  $p_i$  numere prime distincte și  $\alpha_i \in \mathbb{N}^*$ . Atunci

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

**Demonstrație.** Avem  $\varphi(n) = \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r})$ . Conform definiției lui  $\varphi$ , trebuie să găsim numerele mai mici decât  $p^\alpha$  și relativ prime cu  $p^\alpha$ . Dintre numerele  $1, \dots, p-1, p, p+1, \dots, 2p-1, p, 2p+1, \dots, p^\alpha-1, p^\alpha$  fiecare al  $p$ -lea este divizibil cu  $p$ , iar celelalte sunt relativ prime cu  $p$ , deci

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right).$$

De aici afirmația rezultă imediat. ■

## 7.4 Mulțimea numerelor raționale

Am văzut că  $(\mathbb{Z}, +, \cdot, \leq)$  este domeniu de integritate total ordonat arhimedian. Vom extinde această structură pentru a obține un corp comutativ total ordonat.

**Definiția 7.4.1** a) Pe mulțimea  $\mathbb{Z} \times \mathbb{Z}^*$  definim relația omogenă

$$(a, b) \sim (c, d), \quad \text{dacă } ad = bc,$$

și se verifică ușor că este o relație de echivalență. Notăm prin  $\widetilde{(a, b)}$  clasa de echivalență a perechii  $(a, b)$ , deci

$$\widetilde{(a, b)} = \{(c, d) \in \mathbb{Z} \times \mathbb{Z}^* \mid (c, d) \sim (a, b)\}.$$

Mulțimea factor

$$\mathbb{Q} := \mathbb{Z} \times \mathbb{Z}^* / \sim = \{\widetilde{(a, b)} \mid (a, b) \in \mathbb{Z} \times \mathbb{Z}^*\}$$

se numește **mulțimea numere raționale**. Un număr rațional se notează de obicei sub formă de **fracție**, adică

$$\widetilde{(a, b)} = \frac{a}{b}.$$

Observăm că pentru  $a \in \mathbb{Z}$  și  $b, c \in \mathbb{Z}^*$  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 și înmulțirea numerelor raționale se definesc astfel:

$$\widetilde{(a, b)} + \widetilde{(c, d)} := \widetilde{(ad + bc, bd)}, \quad \widetilde{(a, b)} \widetilde{(c, d)} := \widetilde{(ac, bd)},$$

adică

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \frac{c}{d} = \frac{ac}{bd}.$$

Aceste definiții nu depind de alegerea reprezentanților.

**Teorema 7.4.2** Structura algebraică  $(\mathbb{Q}, +, \cdot)$  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 rațional  $\widetilde{(a, b)}$  este

$$-\widetilde{(a, b)} := \widetilde{(-a, b)} = \widetilde{(a, -b)}, \quad \text{adică } -\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b},$$

și dacă  $a, b \in \mathbb{Z}^*$ , atunci inversul lui  $\widetilde{(a, b)}$  este

$$\widetilde{(a, b)}^{-1} = \widetilde{(b, a)}, \quad \text{adică } \left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

**Exercițiul 144** a) Să se arate că relația „ $\sim$ ” este o relație de echivalență.

b) Să se arate că definițiile adunării și înmulțirii nu depind de alegerea reprezentanților.

c) Să se demonstreze Teorema 7.4.2.

**Definiția 7.4.3** Numerele raționale se ordonează prin relația:

$$\frac{a}{b} \leq \frac{c}{d}, \quad \text{dacă } (bc - ad)bd \geq 0.$$

b) **Valoarea absolută (modulul)** numărului rațional  $a \in \mathbb{Q}$  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) Definiția relației „ $\leq$ ” nu depinde de alegerea reprezentanților.

2)  $(\mathbb{Q}, \leq)$  este total ordonat.

3) Funcția  $\alpha : \mathbb{Z} \rightarrow \mathbb{Q}$ ,  $\alpha(a) = \widetilde{(a, 1)} = \frac{a}{1}$  este bine definită, strict crescătoare (deci injectivă) și este morfism unital de inele.

4) Ordonarea numerelor raționale este compatibilă cu adunarea și înmulțirea, adică dacă  $x, y, z, t \in \mathbb{Q}$ , atunci

$$x < y, z \leq t \Rightarrow x + z < y + t, \quad x < y, z > 0 \Rightarrow xz < yz, \quad x < y, z < 0 \Rightarrow xz > yz.$$

5) (**Axioma lui Arhimede**)  $\forall x \in \mathbb{Q}_+^*, \forall y \in \mathbb{Q}, \exists n \in \mathbb{N}$  astfel ca  $nx > y$ .

**Observații 7.4.5** Vom identifica numărul întreg  $a$  cu  $\alpha(a) = \frac{a}{1}$  și astfel  $\mathbb{Z} \subset \mathbb{Q}$ . Observăm că  $\frac{a}{b} = \alpha(a)\alpha(b)^{-1}$ .

**Exercițiul 145** Să se demonstreze Teorema 7.4.4.

**Exercițiul 146** Să se arate că pentru orice  $x, y \in \mathbb{Q}$

$$|x| = |-x|, \quad |xy| = |x||y|, \quad |x+y| \leq |x| + |y|, \quad ||x| - |y|| \leq |x - y|.$$

## 7.5 Mulțimea numerelor reale

**7.5.1** Fie  $K$  un corp comutativ total ordonat. Din analiza matematică știm că următoarele afirmații sunt echivalente:

(i) Orice șir monoton și mărginit de elemente din  $K$  este convergent.

(ii) Orice submulțime nevidă și mărginită inferior (superior) a lui  $K$  are infimum (supremum).

(iii) Corpul  $K$  satisface axioma lui Arhimede și orice șir 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 raționale formează un corp comutativ total ordonat care nu este complet în sensul de mai sus. Pornind de la corpul  $\mathbb{Q}$  al numerelor raționale, vom construi o extindere a sa care este un corp comutativ total ordonat și complet, numit corpul numerelor reale.

**Definiția 7.5.2** a) Considerăm mulțimea șirurilor de numere raționale, pe care o notăm

$$\mathbb{Q}^{\mathbb{N}} = \{(a_n) \mid a_n \in \mathbb{Q}\};$$

acesta este un inel comutativ cu operațiile  $(a_n) + (b_n) = (a_n + b_n)$ , respectiv  $(a_n)(b_n) = (a_n b_n)$ ; elementul nul este șirul constant  $(0)$ , iar elementul unitate este șirul constant  $(1)$ . În general notăm prin  $(a)$  șirul constant în care fiecare termen este egal cu  $a$ . Considerăm următoarele submulțimi ale lui  $\mathbb{Q}^{\mathbb{N}}$ :

b) mulțimea șirurilor 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) mulțimea șirurilor 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) mulțimea șirurilor 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 ușor 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 și al lui  $\mathcal{C}$ ).

e) Considerăm relația de echivalență „ $\sim$ ” 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 echivalență a șirului  $(a_n) \in \mathcal{C}$ , deci

$$\widetilde{(a_n)} = (a_n) + \mathcal{N} = \{(a_n + b_n) \mid (b_n) \in \mathcal{N}\}.$$

f) Mulțimea factor  $\mathbb{R} := \mathcal{C} / \sim = \{\widetilde{(a_n)} = (a_n) + \mathcal{N} \mid (a_n) \in \mathcal{C}\}$  se numește **mulțimea numerelor reale**.

g) Adunarea și înmulțirea numerelor reale se definesc astfel:

$$\widetilde{(a_n)} + \widetilde{(b_n)} := \widetilde{(a_n + b_n)}, \quad \widetilde{(a_n)}\widetilde{(b_n)} := \widetilde{(a_n b_n)}.$$

**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  $1 := \widetilde{(1)} = (1) + \mathcal{N}$ .

**Exercițiul 147** a) Să se arate că  $(\mathbb{Q}^{\mathbb{N}}, +, \cdot)$  este un inel comutativ,  $\mathcal{N} \subseteq \mathcal{C} \subseteq \mathcal{B}$ ,  $\mathcal{C}$  și  $\mathcal{B}$  sunt subinele unitale ale lui  $\mathbb{Q}^{\mathbb{N}}$ , iar  $\mathcal{N}$  este un ideal al lui  $\mathcal{B}$ .

- Să se arate că „ $\sim$ ” este relație de echivalență pe  $\mathcal{C}$ .
- Să se arate că definițiile operațiilor „+” și „ $\cdot$ ” nu depind de alegerea reprezentanților.
- Să se demonstreze Teorema 7.5.3.

**Definiția 7.5.4** a) Introducem submulțimile:

$$\mathbb{R}_+^* := \{(\mathbf{a}_n) \in \mathbb{R} \mid \exists r \in \mathbb{Q}_+^* \exists N \in \mathbb{N} \text{ astfel ca } \forall n > N : a_n > r\},$$

$$\mathbb{R}_-^* := \{(\mathbf{a}_n) \in \mathbb{R} \mid \exists r \in \mathbb{Q}_+^* \exists N \in \mathbb{N} \text{ astfel ca } \forall n > N : a_n < -r\}.$$

b) Spunem că  $\alpha < \beta$ , dacă  $\beta - \alpha \in \mathbb{R}_+^*$ . Ordonăm numerele reale prin relația

$$\alpha \leq \beta \text{ dacă } \alpha < \beta \text{ sau } \alpha = \beta.$$

**Teorema 7.5.5** 1)  $\alpha \in \mathbb{R}_+^* \iff -\alpha \in \mathbb{R}_-^*$ .

2) Submulțimile  $\mathbb{R}_+^*$ ,  $\{0\}$ ,  $\mathbb{R}_-^*$  formează o partiție a lui  $\mathbb{Z}$  (adică sunt disjuncte două câte două și avem  $\mathbb{R} = \mathbb{R}_+^* \cup \{0\} \cup \mathbb{R}_-^*$ ).

3)  $(\mathbb{R}, \leq)$  este o mulțime total ordonată.

4) Funcția  $\varphi : \mathbb{Q} \rightarrow \mathbb{R}$ ,  $\varphi(\mathbf{a}) = \widetilde{(\mathbf{a})} = (\mathbf{a}) + \mathcal{N}$  este strict crescătoare (deci injectivă) și este morfism de corpuri. Vom identifica numărul rațional  $\mathbf{a}$  cu  $\varphi(\mathbf{a})$  și astfel  $\mathbb{Q} \subset \mathbb{R}$ .

5) Ordonarea numere reale este compatibilă cu adunarea și înmulțirea, adică dacă  $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ , atunci

$$\alpha < \beta, \gamma \leq \delta \Rightarrow \alpha + \gamma < \beta + \delta, \quad \alpha < \beta, \gamma > 0 \Rightarrow \alpha\gamma < \beta\gamma, \quad \alpha < \beta, \gamma < 0 \Rightarrow \alpha\gamma > \beta\gamma.$$

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  $\alpha, \beta \in \mathbb{R}$  și  $\alpha < \beta$ , atunci  $\exists r \in \mathbb{Q}$  astfel ca  $\alpha < r < \beta$ . (Spunem că  $\mathbb{Q}$  este submulțime **densă** a lui  $\mathbb{R}$ )

8) Dacă  $(\alpha_n) \in \mathbb{R}^{\mathbb{N}}$  este un șir Cauchy de numere reale, atunci  $\exists \lim_{n \rightarrow \infty} \alpha_n \in \mathbb{R}$ . În particular, dacă  $(\mathbf{a}_n) \in \mathcal{C}$ , atunci  $\lim_{n \rightarrow \infty} \mathbf{a}_n = (\mathbf{a}_n) + \mathcal{N}$ .

**Exercițiul 148** a) Să se arate că definiția relației „ $\leq$ ” nu depinde de alegerea reprezentanților.

b) Să se demonstreze Teorema 7.5.5.

Teorema 7.5.5 spune că  $(\mathbb{R}, +, \cdot, \leq)$  este un corp comutativ total ordonat arhimedian și complet în sensul lui Cauchy (sau echivalent, conform 7.5.1, corp comutativ total ordonat complet în sensul lui Dedekind. Aceste proprietăți determină unic corpul numerelor reale până 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  $\mathbb{R}$ .

**Exercițiul 149** Să se demonstreze Teorema 7.5.6.



## Capitolul 8

# ALGEBRE UNIVERSALE

O *structură* matematică este o mulțime (sau mai multe mulțimi) dotată cu operații (de obicei finite), relații, topologii etc. care satisfac anumite condiții de compatibilitate. O structură algebrică este o mulțime dotată cu operații ce satisfac o listă de *axiome*, care de obicei se scriu sub forma unor identități polinomiale (sau legi ecuaționale). Exemplele cele mai cunoscute sunt axiomele de asociativitate și comutativitate pentru o operație binară. O clasă de structuri algebrice definită prin identități se numește *varietate* sau *clasă ecuațională*. Exemplele uzuale de structuri algebrice formează varietăți: grupuri, inele, latices. Clasa corpurilor nu este o varietate deoarece nu toate axiomele corpului pot fi exprimate ca ecuații. Exemple mai complexe de structuri algebrice sunt spațiile vectoriale peste un corp, modulele peste un inel și algebrele peste un inel comutativ. Uneori sunt permise și operații infinite, astfel putând fi inclus aici și studiul laticelor complete. Corpurile ordonate sau grupurile topologice sunt exemple de structuri mixte. Alte exemple de structuri sunt grafurile (sau rețelele), bazele de date relaționale și universurile din teoria mulțimilor.

În cadrul algebrei abstracte se studiază proprietățile 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 stabilește o conexiune între anumite corpuri comutative și grupuri. Structurile algebrice pot fi definite în orice categorie ce are produse directe finite. De exemplu, un grup topologic este un grup în categoria spațiilor topologice. Într-o categorie, noțiunile pot fi dualizate, obținându-se astfel noi structuri, cum ar fi cogrupurile sau coalgebrele peste un inel comutativ.

Teoria modelelor, ca domeniu interdisciplinar ce leagă matematica, logica, filosofia și 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 mulțime de propoziții într-un limbaj formal (de exemplu, logica de ordinul I); un model al teoriei este o structură (adică o interpretare) ce satisface propozițiile (axiomele) teoriei. Teoria modelelor examinează semantica (semnificație și adevăr) prin intermediul sintaxei limbajului respectiv (formule și demonstrații).

### 8.1 $\Omega$ -algebre și omomorfisme

**Definiția 8.1.1** a) Fie  $A$  o mulțime și  $n \in \mathbb{N}$ . O funcție  $\omega : A^n \rightarrow A$  se numește **operație** pe mulțimea  $A$ . Spunem că  $n = \tau(\omega)$  este **tipul** sau **aritatea** lui  $\omega$ .

b) Fie  $\Omega$  o mulțime de operații pe mulțimea  $A$ . Perechea  $(A, \Omega)$  se numește **algebră universală** sau  $\Omega$ -algebră.

Algebra universală  $(A, \Omega)$  determină o funcție  $\tau : \Omega \rightarrow \mathbb{N}$ , unde  $\tau(\omega)$  este tipul lui  $\omega$ . Spunem că  $\tau$  este **tipul** lui  $(A, \Omega)$ .

**Exemplul 8.1.2** 1) Dacă  $n = 0$ , atunci  $A^n = \{\emptyset\}$ , deci  $\omega : A^0 \rightarrow A$  este unic determinat, dacă se dă u elementul  $\omega(\emptyset) \in A$ . De exemplu, în  $\mathbb{R}$ , elementele 0 și 1 pot fi considerate operații nulare.

2) Dacă  $n = 1$ , atunci  $A^n = A$ , deci orice funcție  $\omega : A \rightarrow A$  este operație unară. De exemplu,  $\omega : \mathbb{R} \rightarrow \mathbb{R}$ ,  $\omega(x) = -x$  este operație unară pe  $\mathbb{R}$ .

3) Dacă  $M$  este o mulțime, atunci  $(\mathcal{P}(M), \cup, \cap, \mathcal{C}, \emptyset, M)$  este algebră universală de tip  $\tau = \begin{pmatrix} \cup & \cap & \mathcal{C} & \emptyset & M \\ 2 & 2 & 1 & 0 & 0 \end{pmatrix}$ .

4) Dacă  $\mathcal{R}_2(M) = \{\rho = (M, M, R) \mid R \subseteq M \times M\}$  este mulțimea relațiilor binnare pe mulțimea  $M$ , atunci  $(\mathcal{R}_2(M), \cup, \cap, \circ, \mathcal{C}, -1)$  este algebră universală de tip  $\tau = \begin{pmatrix} \cup & \cap & \circ & \mathcal{C} & -1 \\ 2 & 2 & 2 & 1 & 1 \end{pmatrix}$ .

**Exercițiul 150** Fie  $A$  o mulțime cu  $m$  elemente și fie  $n \in \mathbb{N}$ . Câte operații  $n$ -are există pe  $A$ ?

**Definiția 8.1.3** Fie  $(A, \Omega)$ ,  $(A', \Omega')$  algebre universale și  $\theta : \Omega \rightarrow \Omega'$  o funcție astfel încât  $\tau'(\theta(\omega)) = \tau(\omega)$ .

a) Funcția  $f : A \rightarrow A'$  se numește  **$\theta$ -omomorfism**, dacă pentru orice  $\omega \in \Omega$  și 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  **$\theta$ -izomorfism**, dacă  $f$  și  $\theta$  sunt funcții bijective,  $f$   $\theta$ -omomorfism și  $f^{-1}$  este  $\theta^{-1}$ -izomorfism.

c) Dacă  $(A, \Omega) = (A', \Omega')$  și  $\theta = \mathbf{1}_\Omega$ , atunci  $f$  se numește **endomorfism**, respectiv **automorfism**.

**Observații 8.1.4** 1) Funcția identică  $\mathbf{1}_A : (A, \Omega) \rightarrow (A, \Omega)$  este automorfism al lui  $(A, \Omega)$ .

2) În general, pentru simplificare, vom nota pe  $\Omega'$  prin  $\Omega$ -val și pe  $\theta(\omega)$  prin  $\omega$ .

3)  $f : (A, \Omega) \rightarrow (A', \Omega)$  este izomorfism dacă și numai dacă  $f$  omomorfism bijectiv.

Într-adevăr, presupunem că  $f$  omomorfism bijectiv și arătăm că și  $f^{-1}$  este omomorfism. Fie  $\omega \in \Omega$ ,  $\tau(\omega) = n$ ,  $b_1, \dots, b_n \in A'$  și  $a_i = f^{-1}(b_i)$ ,  $i = 1, \dots, n$ . Atunci

$$\begin{aligned} f^{-1}(\omega(b_1, \dots, b_n)) &= f^{-1}(\omega(f(a_1), \dots, f(a_n))) = f^{-1}(f(\omega(a_1, \dots, a_n))) = \\ &= \omega(a_1, \dots, a_n) = \omega(f^{-1}(b_1), \dots, f^{-1}(b_n)). \end{aligned}$$

**Exercițiul 151** Să se arate că  $f : (A, \Omega) \rightarrow (A', \Omega)$  este  $\theta$ -omomorfism dacă și numai dacă pentru orice  $\omega \in \Omega$ , notând  $f^{\tau(\omega)} := f \times \dots \times f : A^{\tau(\omega)} \rightarrow A'^{\tau(\omega)}$ , următoarea diagramă este comutativă:

$$\begin{array}{ccc} A^{\tau(\omega)} & \xrightarrow{f^{\tau(\omega)}} & A'^{\tau(\omega)} \\ \omega \downarrow & & \downarrow \theta(\omega) \\ A & \xrightarrow{f} & A' \end{array}$$

**Exemplul 8.1.5 (Produs direct de algebre universale)** Fie  $(A_i, \Omega)_{i \in I}$  o familie de  $\Omega$ -algebre și considerăm a produsul direct  $(\prod_{i \in I} A_i, (p_i)_{i \in I})$ .

Fie  $\tau$  tip algebrelor. Dacă  $\omega \in \Omega$  și  $(a_i^k)_{i \in I} \in P$ ,  $k = 1, \dots, n$ ,  $n = \tau(\omega)$ , 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  $\Omega$ -algebră, iar proiecția canonică  $p_j : P \rightarrow A_j$  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  $\omega'$  este o altă operație 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  $f_i : (A_i, \Omega) \rightarrow (A'_i, \Omega)$  sunt omomorfisme,  $i \in I$ , atunci

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

este de asemenea omomorfism.

## 8.2 Subalgebre

**Definiția 8.2.1** Fie  $(A, \Omega)$  o algebră universală și  $B \subseteq A$ . Spunem că  $B$  este *subalgebră* a lui  $A$  (notație:  $B \leq (A, \Omega)$ ), dacă

$$\forall \omega \in \Omega, \tau(\omega) = n, \forall a_1, \dots, a_n \in B, \omega(a_1, \dots, a_n) \in B.$$

Vom nota mulțimea subalgebrelor lui  $A$  prin  $\mathcal{S}(A, \Omega)$ .

**Observații 8.2.2** 1) Dacă  $B \in \mathcal{S}(A, \Omega)$ , atunci orice  $\omega \in \Omega$  induce o operație pe submulțimea  $B$ , deci și  $(B, \Omega)$  este algebră universală.

2) Mulțimea vidă  $\emptyset$  este subalgebră dacă și numai dacă  $\Omega$  nu conține operații nulare.

**Exemplul 8.2.3** 1) Fie  $M$  o mulțime și  $N \subseteq M$ . Atunci  $\mathcal{P}(N)$  este subalgebră a algebrei  $(\mathcal{P}, \cup, \cap)$  dar nu și a lui  $(\mathcal{P}, \cup, \cap, \mathbb{C})$ .

3) Fie  $\mathcal{F}(M) = \{f \mid f : M \rightarrow M\}$ ,  $\mathcal{F}_i(M) = \{f : M \rightarrow M \mid f \text{ injectivă}\}$ ,  $\mathcal{F}_s(M) = \{f : M \rightarrow M \mid f \text{ surjectiv}\}$ ,  $\mathcal{F}_b(M) = \{f : M \rightarrow M \mid f \text{ bijectiv}\}$ . Atunci  $\mathcal{F}_i(M)$ ,  $\mathcal{F}_s(M)$  și  $\mathcal{F}_b(M)$  sunt subalgebre ale lui  $(\mathcal{F}(M), \circ)$ .

**Exercițiul 152** Fie  $(A, \Omega)$ ,  $(B, \Omega)$ ,  $(C, \Omega)$  algebre universale. Spunem că  $\rho = (A, B, R)$  este **relație omomorfă**, dacă  $R$  este subalgebră a produsului direct  $(A \times B, \Omega)$ .

Să se arate că :

a) Dacă  $f = (A, B, F)$  egy funcție, atunci  $f$  omomorfism  $\Leftrightarrow f$  este relație omomorfă;

b) Dacă  $\rho = (A, B, R)$  și  $\sigma = (B, C, S)$  sunt relații omomorfe, atunci și  $\sigma \circ \rho$  și  $\rho^{-1}$  sunt relații omomorfe;

c) Dacă  $\rho = (A, B, R)$  este relație omomorfă și  $X \in \mathcal{S}(A, \Omega)$ , atunci  $\rho(X) \in \mathcal{S}(B, \Omega)$ . (În particular, dacă  $f : A \rightarrow B$  este omomorfism, atunci  $f(X) \in \mathcal{S}(B, \Omega)$ .)

**Lema 8.2.4** Dacă  $(A, \Omega)$  este o algebră universală și  $\mathcal{S} \subseteq \mathcal{S}(A, \Omega)$ , atunci

$$\bigcap_{B \in \mathcal{S}} B \in \mathcal{S}(A, \Omega).$$

**Demonstrație.** Fie  $\omega \in \Omega$ ,  $n = \tau(\omega)$  și  $b_1, \dots, b_n \in \bigcap_{B \in \mathcal{S}} B$ ; rezultă că pentru orice  $B \in \mathcal{S}$ ,  $b_1, \dots, b_n \in B$ , deci  $\omega(b_1, \dots, b_n) \in \bigcap_{B \in \mathcal{S}} B$ ; rezultă că  $\omega(b_1, \dots, b_n) \in \bigcap_{B \in \mathcal{S}} B$ . ■

**Corolar 8.2.5**  $(\mathcal{S}(A, \Omega), \subseteq)$  este latică completă. Dacă  $\mathcal{S} \subseteq \mathcal{S}(A, \Omega)$ , atunci

$$\inf_{\mathcal{S}(A, \Omega)} \mathcal{S} = \bigcap \{B \mid B \in \mathcal{S}\}, \quad \sup_{\mathcal{S}(A, \Omega)} \mathcal{S} = \bigcap \{C \in \mathcal{S}(A, \Omega) \mid C \supseteq B \forall B \in \mathcal{S}\}.$$

**Demonstrație.** Rezultă din lema și din Teorema 5.2.5 de caracterizare a laticilor complete. ■

**Definiția 8.2.6** Fie  $(A, \Omega)$  algebră universală și  $X \subseteq A$ . 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 submulțimea  $X$ .

**Observații 8.2.7** Evident,  $\langle X \rangle$  este cea mai mică subalgebră de conține pe  $X$ , deci următoarele proprietăți caracterizează pe  $\langle X \rangle$ :

(1)  $X \subseteq \langle X \rangle$ ;

(2)  $\langle X \rangle \in \mathcal{S}(A, \Omega)$ ;

(3) Dacă  $X \subseteq B$  și  $B \in \mathcal{S}(A, \Omega)$ , atunci  $\langle X \rangle \subseteq B$ .

Observăm că  $\langle \langle X \rangle \rangle = \langle X \rangle$ , și  $X \in \mathcal{S}(A, \Omega) \Leftrightarrow X = \langle X \rangle$ .

**Teorema 8.2.8 (caracterizarea subalgebrei generate)** Fie  $(A, \Omega)$  o algebră universală și  $X \subseteq A$ . Atunci

$$\langle X \rangle = \bigcup_{i \in \mathbb{N}} X_i,$$

unde  $X_0 = X$ ,  $X_{i+1} = X_i \cup \{\omega(x_1, \dots, x_{\tau(\omega)}) \mid \omega \in \Omega, x_1, \dots, x_{\tau(\omega)} \in X_i\}$ .

**Demonstrație.** Fie  $Y = \bigcup_{i \in \mathbb{N}} X_i$ . Se vede ușor că

(1)  $X \subseteq Y$ ;

(2)  $Y \in \mathcal{S}(A, \Omega)$ ;

(3) Dacă  $B \in \mathcal{S}(A, \Omega)$  și  $X \subseteq B$ , atunci  $Y \subseteq B$ . ■

**Exercițiul 153** a) Fie  $M$  o mulțime și  $A \subseteq M$ . Să se determine subalgebra lui  $(\mathcal{P}(M), \cup, \cap, \mathbb{C})$  generată de  $\{A\}$ .

b) Fie  $\mathcal{R}_2(M)$  mulțimea relațiilor binare pe  $M$  și fie  $\rho \in \mathcal{R}_2(M)$  o relație reflexivă și simetrică. Să se determine subalgebra lui  $(\mathcal{R}_2(M), \cup, \cap, \circ, {}^{-1})$  generată de  $\{\rho\}$ . Cine este această subalgebră dacă  $\rho$  este tranzitiv?

**Exercițiul 154** Fie  $A$  o  $\Omega$ -algebra și  $X_0 = \{\omega(\emptyset) \mid \omega \in \Omega, \tau(\omega) = 0\}$ . Să se arate că  $\langle X_0 \rangle = \langle \emptyset \rangle$  și  $\langle X_0 \rangle$  este cel mai mic element al lui  $\mathcal{S}(A, \Omega)$ .

**Exercițiul 155** Fie  $A$  și  $B$  două  $\Omega$ -algebre și fie  $f : A \rightarrow B$  un omomorfism. Să se arate că:

- Dacă  $X \subseteq A$ , atunci  $f(\langle X \rangle) = \langle f(X) \rangle$ .
- Dacă  $g : A \rightarrow B$  este un omomorfism,  $\langle X \rangle = A$  și  $g|_X = f|_X$ , atunci  $g = f$ .

**Exercițiul 156** Fie  $A$  o  $\Omega$ -algebra. Elementul  $a \in A$  se numește **non-generator**, dacă pentru orice  $X \subseteq A$  avem

$$\langle X \cup \{a\} \rangle = A \implies \langle X \rangle = A.$$

Subalgebra  $M \leq (A, \Omega)$  se numește **maximală**, dacă  $M \neq A$  și pentru orice subalgebra  $B$  a lui  $A$  avem

$$M \subseteq B \implies B = M \text{ sau } B = A.$$

Să se arate că :

- Submulțimea  $N(A) := \{a \in A \mid a \text{ non-generator}\}$  este subalgebră a lui  $(A, \Omega)$ ;
- Pentru orice automorfism  $f : A \rightarrow A$  avem  $f(N(A)) \subseteq N(A)$ ;
- $N(A)$  coincide cu **subalgebra Frattini**  $\Phi(A) := \bigcap_{M \text{ subalgebra maximală}} M$  a lui  $A$ .

### 8.3 Congruențe. Algebre factor. Teoreme de izomorfism

**Definiția 8.3.1** Fie  $(A, \Omega)$  o algebră universală și  $\rho = (A, A, R)$  o relație pe  $A$ . Spunem că  $\rho$  este **congruență** pe  $(A, \Omega)$  (notație:  $\rho \in \mathcal{C}(A, \Omega)$ ), dacă  $\rho$  este relație de echivalență și este **compatibilă** cu operațiile, adică:  $\forall \omega \in \Omega, \forall a_1, \dots, a_{\tau(\omega)}, b_1, \dots, b_{\tau(\omega)} \in A$

$$a_i \rho b_i, i = 1, \dots, \tau(\omega) \implies \omega(a_1, \dots, a_{\tau(\omega)}) \rho \omega(b_1, \dots, b_{\tau(\omega)}).$$

**Exemplul 8.3.2** 1) Relația  $\equiv (\text{mod } n)$  definită pe  $\mathbb{Z}$  este relație de congruență pe algebra  $(\mathbb{Z}, +, \cdot, 0, 1, -)$ .  
2) Relația diagonală  $\mathbf{1}_A = (A, A, \Delta_A)$  și relația universală  $(A, A, A \times A)$  sunt congruențe pe  $A$ .

**Teorema 8.3.3** Fie  $(A, \Omega)$  o algebră universală și  $\rho \in \mathcal{C}(A, \Omega)$  o congruență. Pe mulțimea factor

$$A/\rho = \{\rho(x) \mid x \in A\}$$

există o unică structură de  $\Omega$ -algebră astfel încât proiecția canonică  $p_\rho : A \rightarrow A/\rho$  să fie omomorfism.

**Demonstrație.** Fie  $\omega \in \Omega$  și  $\rho(x_1), \dots, \rho(x_n)$ , unde  $n = \tau(\omega)$ . Definim

$$\omega(\rho(x_1), \dots, \rho(x_n)) = \rho(\omega(x_1, \dots, x_n)).$$

Aratăm că definiția nu depinde de alegerea reprezentanților. Într-adevăr, fie  $x'_i \in \rho(x_i)$ ,  $i = 1, \dots, n$ . 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  $\rho$  este congruență.

Aratăm că  $p_\rho$  este omomorfism. Pentru orice  $\omega \in \Omega$  și  $x_1, \dots, x_n \in A$  avem

$$p_\rho(\omega(x_1, \dots, x_n)) = \rho(\omega(x_1, \dots, x_n)) = \omega(\rho(x_1), \dots, \rho(x_n)) = \omega(p_\rho(x_1), \dots, p_\rho(x_n)).$$

Presupunem acum că  $\omega'$  este o operație  $n$ -ară pe mulțimea factor  $A/\rho$  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

$$\begin{aligned} \omega(\rho(x_1), \dots, \rho(x_n)) &= \omega(p_\rho(x_1), \dots, p_\rho(x_n)) = p_\rho(\omega(x_1, \dots, x_n)) = \\ &= \omega'(p_\rho(x_1), \dots, p_\rho(x_n)) = \omega'(\rho(x_1), \dots, \rho(x_n)), \end{aligned}$$

deci  $\omega = \omega'$ . ■

**Exercițiul 157** Fie  $A$  o  $\Omega$ -algebră. Să se arate că  $\Delta_A$  și  $A \times A$  sunt congruențe pe  $(A, \Omega)$  și algebra factor  $(A/\Delta_A, \Omega)$  este izomorfă cu  $(A, \Omega)$ . Câte elemente are algebra factor  $A/A \times A$ ?

**Teorema 8.3.4 (teorema I de izomorfism)** Fie  $f : (A, \Omega) \rightarrow (B, \Omega)$  un omomorfism. Atunci:

- $\ker f = \{(x_1, x_2) \in A \times A \mid f(x_1) = f(x_2)\}$  congruență pe algebra  $(A, \Omega)$ .
- $\text{Im } f = f(A) \in \mathcal{S}(B, \Omega)$ .
- $A/\ker f \simeq \text{Im } f$ .

**Demonstrație.** a) Fie  $\omega \in \Omega$ ,  $\tau(\omega) = n$  și fie  $x_1, \dots, x_n, x'_1, \dots, x'_n \in A$  astfel ca  $x_i \in \ker f$ ,  $x'_i \in \ker f$ , 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  $\omega(x_1, \dots, x_n) \in \ker f = \omega(x'_1, \dots, x'_n)$ .

b) Fie  $\omega \in \Omega$ ,  $\tau(\omega) = n$  și  $y_1 = f(x_1), \dots, y_n = f(x_n) \in f(A)$ . 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

$$\bar{f}: A/\ker f \rightarrow \text{Im } f, \quad \bar{f}(\rho\langle x \rangle) = f(x)$$

este funcție bijectivă. Arătăm că  $\bar{f}$  este omomorfism. Într-adevăr, pentru orice  $\omega \in \Omega$  avem

$$\begin{aligned} \bar{f}(\omega(\rho\langle x_1 \rangle, \dots, \rho\langle x_n \rangle)) &= \bar{f}(\rho\langle \omega(x_1, \dots, x_n) \rangle) = f(\omega(x_1, \dots, x_n)) = \\ &= \omega(f(x_1), \dots, f(x_n)) = \omega(\bar{f}(\rho\langle x_1 \rangle), \dots, \bar{f}(\rho\langle x_n \rangle)). \quad \blacksquare \end{aligned}$$

**Teorema 8.3.5 (teorema II de izomorfism)** Fie  $(A, \Omega)$  o algebră universală,  $B \in \mathcal{S}(A, \Omega)$  și  $\rho \in \mathcal{C}(A, \Omega)$ . Atunci:

- $\rho(B) \in \mathcal{S}(A, \Omega)$ ;
- $\sigma := \rho \cap (B \times B) \in \mathcal{C}(B, \Omega)$  și  $\tau := \rho \cap (\rho(B) \times \rho(B)) \in \mathcal{C}(\rho(B), \Omega)$ ;
- $(B/\sigma, \Omega) \simeq (\rho(B)/\tau, \Omega)$ .

**Demonstrație.** a) Fie  $\omega \in \Omega$ ,  $\tau(\omega) = n$  și  $y_1, \dots, y_n \in \rho(B)$ , deci există  $b_1, \dots, b_n \in B$  astfel încât  $\rho y_i = b_i$ ,  $i = 1, \dots, n$ . Deoarece  $\rho \in \mathcal{C}(A, \Omega)$ , rezultă că  $\omega(b_1, \dots, b_n) \in \rho(B)$ , și 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  $\omega \in \Omega$ ,  $\tau(\omega) = n$  și  $b_1, \dots, b_n, b'_1, \dots, b'_n \in B$  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  $\bar{f}: B/\sigma \rightarrow \rho(B)/\tau$ ,  $\bar{f}(\sigma\langle b \rangle) = \tau(\langle b \rangle)$  este funcție bijectivă. Deoarece  $f$  este omomorfism, se vede ușor că  $\bar{f}$  este de asemenea omomorfism.  $\blacksquare$

**Teorema 8.3.6 (teorema III de izomorfism)** Fie  $(A, \Omega)$  o algebră universală și fie  $\rho, \sigma \in \mathcal{C}(A, \Omega)$ ,  $\rho \subseteq \sigma$ . Atunci există  $\sigma/\rho \in \mathcal{C}(A/\rho, \Omega)$  astfel încât

$$\frac{A/\rho}{\sigma/\rho} \simeq A/\sigma.$$

**Demonstrație.** Din Teorema III de factorizare 4.5.7 rezultă că

$$g: A/\rho \rightarrow A/\sigma, \quad g(\rho\langle a \rangle) = \sigma\langle a \rangle$$

este funcție surjectivă și se verifică ușor că  $g$  este omomorfism. Din Teorema I de izomorfism 8.3.4 rezultă că  $\sigma/\rho := \ker g$  este congruență pe algebra  $(A/\rho, \Omega)$  și are loc izomorfismul  $\frac{A/\rho}{\sigma/\rho} \simeq A/\sigma$ .  $\blacksquare$

**Exercițiul 158 (latticea congruențelor)** Fie  $(A, \Omega)$  o algebră universală și  $\rho \in \mathcal{E}(A)$  o relație de echivalență pe  $A$ .

- Să se arate că  $\rho$  este congruență  $\Leftrightarrow \rho$  este relație omomorfă.
- Să se arate că mulțimea  $(\mathcal{C}(A, \Omega), \subseteq)$  a congruențelor pe  $A$  este lattice completă.
- Fie  $\mathcal{C} \subseteq \mathcal{E}(A)$ . Să se arate că

$$\sup_{\mathcal{E}(A)} \mathcal{C} = \bigcup_{n \in \mathbb{N}, \rho_1, \dots, \rho_n \in \mathcal{C}} \rho_1 \circ \dots \circ \rho_n$$

(adică, dacă  $q = \sup_{\mathcal{E}(A)} \mathcal{C}$ , atunci  $xqy \Leftrightarrow \exists x = x_0, x_1, \dots, x_n = y \in A$  și  $\exists \rho_1, \dots, \rho_n \in \mathcal{E}(A)$  astfel încât  $x_0 \rho_1 x_1, \dots, x_{n-1} \rho_n x_n$ .)

- Dacă  $\mathcal{C} \subseteq \mathcal{C}(A, \Omega)$ , atunci  $\sup_{\mathcal{E}(A)} \mathcal{C} = \sup_{\mathcal{C}(A, \Omega)} \mathcal{C}$ .
- Fie  $\rho_1, \rho_2 \in \mathcal{C}(A, \Omega)$ . Să se arate că

$$\rho_1 \circ \rho_2 \in \mathcal{C}(A, \Omega) \Leftrightarrow \rho_1 \circ \rho_2 = \rho_2 \circ \rho_1$$

și 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  $\rho_1 \subseteq \rho_3 \Rightarrow \rho_1 \circ (\rho_2 \cap \rho_3) = (\rho_1 \circ \rho_2) \cap \rho_3$ . (În acest caz spunem că  $\mathcal{C}(A, \Omega)$  este **lattice 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 mulțimilor și a arătat importanța funcțiilor bijective. Cantor a definit mulțimile infinite și mulțimile bine ordonate, și a arătat că există o „ierarhie” a mulțimilor infinite. Tot el a introdus numerele cardinale și numerele ordinale și a studiat aritmetica acestora.

### 9.1 Număr cardinal. Operații cu numere cardinale

**Definiția 9.1.1** Spunem că mulțimile  $A$  și  $B$  sunt **echipotente** (notație:  $A \sim B$ ), dacă există o funcție bijectivă  $f : A \rightarrow B$ .

**Observații 9.1.2** „ $\sim$ ” este o relație de echivalență pe clasa mulțimilor, deci obținem o partiție a acestei clase.

Într-adevăr, dacă  $A$  o mulțime, atunci  $1_A : A \rightarrow A$  este bijectiv, deci „ $\sim$ ” este reflexiv. Dacă  $A \sim B$  și  $B \sim C$  atunci există funcțiile bijective  $f : A \rightarrow B$  și  $g : B \rightarrow C$ . Deoarece  $g \circ f : A \rightarrow C$  este bijectiv, rezultă că  $A \sim C$  deci „ $\sim$ ” este tranzitiv. Dacă  $f : A \rightarrow B$  este bijectiv, atunci și  $f^{-1} : B \rightarrow A$  este bijectiv, deci „ $\sim$ ” este simetric.

**Definiția 9.1.3** a) **Cardinalul** mulțimii  $A$  este clasa de echipotență  $A$ . Notație:  $|A|$ , deci  $A \sim B$  dacă și numai dacă  $|A| = |B|$ , și spunem că mulțimea  $A$  este **reprezentant** al numărului cardinal  $\alpha = |A|$ . (Deoarece construcția axiomatică precisă a lui  $|A|$  este dificilă, o vom face doar după introducerea și a numerelor ordinale în capitolul următor.)

b) Adunarea, înmulțirea și exponențierea 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.  $\beta^\alpha = |B^A| = |\text{Hom}(A, B)|$ .

**Observații 9.1.4** Definițiile de mai sus nu depind de alegerea reprezentanților. Într-adevăr, dacă  $\alpha_i = |A_i| = |A'_i|$ , și  $f_i : A \rightarrow A'_i$  este bijectiv pentru orice  $i \in I$ , atunci  $\prod_{i \in I} f_i : \prod_{i \in I} A_i \rightarrow \prod_{i \in I} A'_i$  și  $\prod_{i \in I} f_i : \prod_{i \in I} A_i \rightarrow \prod_{i \in I} A'_i$  sunt funcții bijective. Dacă  $f : A' \rightarrow A$  și  $g : B \rightarrow B'$  sunt bijective, atunci și  $\text{Hom}(f, g) : \text{Hom}(A, B) \rightarrow \text{Hom}(A', B')$  este bijectiv.

**Teorema 9.1.5** Fie  $(A_i)_{i \in I}$  o familie de mulțimi.

a)  $\phi : \prod_{i \in I} A_i \rightarrow \bigcup_{i \in I} A_i$ ,  $\phi(a_i, i) = a_i$  este funcție surjectivă, și  $\phi$  este injectivă dacă și numai dacă  $A_i \cap A_j = \emptyset$  pentru orice  $i, j \in I$ ,  $i \neq j$ .

b)  $|A_1 \cup A_2| + |A_1 \cap A_2| = |A_1| + |A_2|$ .

**Demonstrație.** a) Dacă  $a \in \bigcup_{i \in I} A_i$ , atunci există  $i \in I$  astfel încât  $a \in A_i$  și  $\phi(a, i) = a$ , deci  $\phi$  este surjectivă.

Presupunem că  $\phi$  este injectivă și că există  $i, j \in I$  și  $a \in A_i \cap A_j$ . Deoarece  $\phi(a, i) = \phi(a, j) = a$ , rezultă că  $(a, i) = (a, j)$ , deci  $i = j$ .

Invers, presupunem că pentru orice  $i \neq j$ ,  $A_i \cap A_j = \emptyset$ , și fie  $(a_i, i), (a_j, j) \in \prod_{i \in I} A_i$  astfel încât  $\phi(a_i, i) = \phi(a_j, j)$ ; rezultă că  $a_i = a_j \in A_i \cap A_j$ , deci  $i = j$  și  $(a_i, i) = (a_j, j)$ .

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,  $A_1 \cup A_2 = A_1 \cup (A_2 \setminus A_1)$  și  $A_2 = (A_2 \setminus A_1) \cup (A_1 \cap A_2)$ , unde  $A_1 \cap (A_2 \setminus A_1) = \emptyset$  și  $(A_2 \setminus A_1) \cap (A_1 \cap A_2) = \emptyset$ ; 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 identități 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)  $\gamma^{\alpha^\beta} = (\gamma^\beta)^\alpha$ .

**Demonstrație.** a) Fie  $\alpha_1 = |A_1|$ ,  $\alpha_2 = |A_2|$  și să observăm că funcțiile

$$\begin{aligned} \phi : A_1 \coprod A_2 &\rightarrow A_2 \coprod A_1, & \phi(a_1, 1) &= (a_1, 2), & \phi(a_2, 2) &= (a_2, 1), \\ \psi : A_1 \times A_2 &\rightarrow A_2 \times A_1, & \psi(a_1, a_2) &= (a_2, a_1) \end{aligned}$$

sunt bijective.

b) Observăm că mulțimile  $(A_1 \coprod A_2) \coprod A_3 = \{(a_1, 1), 1'), ((a_2, 2), 1'), (a_3, 2') \mid a_i \in A_i\}$  și  $A_1 \coprod (A_2 \coprod A_3) = \{(a_1, 1'), ((a_2, 1), 2'), ((a_3, 2), 2') \mid a_i \in A_i\}$  sunt echipotente.

c) Dacă  $\alpha_i = |A_i|$  și  $\beta_j = |B_j|$ , atunci

$$\phi : \left( \prod_{i \in I} A_i \right) \times \left( \prod_{j \in J} B_j \right) \rightarrow \prod_{(i,j) \in I \times J} (A_i \times B_j), \quad ((a_i, i), (b_j, j)) \mapsto ((a_i, b_i), (i, j))$$

este funcție bijectivă.

d) Fie  $\alpha_i = |A_i|$ ,  $i \in I$  și  $\beta = |B|$ . Atunci

$$\phi : \text{Hom}\left(\prod_{i \in I} A_i, B\right) \rightarrow \prod_{i \in I} \text{Hom}(A_i, B), \quad \phi(\alpha) = (\alpha \circ q_i)_{i \in I}$$

este funcție bijectivă, unde  $q_i : A_i \rightarrow \prod_{i \in I} A_i$  este injecția canonică a sumei directe.

e) Cu notațiile de mai sus avem că funcția

$$\psi : \text{Hom}(B, \prod_{i \in I} A_i) \rightarrow \prod_{i \in I} \text{Hom}(B, A_i), \quad \psi(\alpha) = (p_i \circ \alpha)_{i \in I}$$

este bijectivă, unde  $p_i : \prod_{i \in I} A_i \rightarrow A_i$  este proiecția canonică a produsului direct.

f) Fie  $\alpha = |A|$ ,  $\beta = |B|$ ,  $\gamma = |C|$  și considerăm funcțiile

$$\phi : \text{Hom}(A \times B, C) \rightarrow \text{Hom}(A, \text{Hom}(B, C)), \quad \phi(f)(a)(b) = f(a, b),$$

$$\psi : \text{Hom}(A, \text{Hom}(B, C)) \rightarrow \text{Hom}(A \times B, C), \quad \psi(g)(a, b) = g(a)(b),$$

unde  $a \in A$  și  $b \in B$ . Se arată ușor că  $\psi = \phi^{-1}$ . ■

**Teorema 9.1.7 (Cantor)** *Pentru orice mulțime  $A$  are loc  $|\mathcal{P}(A)| = 2^{|A|}$ .*

**Demonstrație.** Fie  $\varphi_A : \mathcal{P}(A) \rightarrow \text{Hom}(A, \{0, 1\})$ ,  $\varphi_A(X) = \chi_X$ , unde

$$\chi_X : A \rightarrow \{0, 1\}, \quad \chi_X(a) = \begin{cases} 1, & \text{dacă } a \in X \\ 0, & \text{dacă } a \notin X \end{cases}$$

este **funcția caracteristică** a submulțimii  $X$ . Observăm că  $\varphi_A$  este bijectivă, pentru că

$$\varphi_A^{-1}(\chi) = \chi^{-1}(1), \quad \forall \chi : A \rightarrow \{0, 1\}$$

este inversa lui  $\varphi_A$ . ■

## 9.2 Ordonarea numerelor cardinale

**Definiția 9.2.1** Fie  $\alpha = |A|$  și  $\beta = |B|$  două numere cardinale. Spunem că  $\alpha \leq \beta$  dacă există o funcție injectivă  $\phi : A \rightarrow B$ .

Să arătăm că definiția nu depinde de alegerea reprezentanților. Într-adevăr, dacă  $\alpha = |A| = |A'|$ ,  $f : A' \rightarrow A$  bijectiv,  $\beta = |B| = |B'|$ ,  $g : B \rightarrow B'$  bijectiv, atunci  $\text{Hom}(f, g)(\phi) = g \circ \phi \circ f : A' \rightarrow B'$  este funcție injectivă.

**Exercițiul 159** Dacă  $\alpha_i \leq \beta_i, \forall i \in I$ , atunci:

- $\sum_{i \in I} \alpha_i \leq \sum_{i \in I} \beta_i$ ;
- $\prod_{i \in I} \alpha_i \leq \prod_{i \in I} \beta_i$ ;
- dacă  $0 \neq \alpha \leq \alpha'$  și  $\beta \leq \beta'$ , atunci  $\beta^\alpha \leq \beta'^{\alpha'}$ .

Pentru a arăta că „ $\leq$ ” este relație de ordine, avem nevoie de următoarea lemă.

**Lema 9.2.2 (Cantor–Bernstein–Schröder)** Dacă  $A_2 \subseteq A_1 \subseteq A_0$  și  $A_0 \sim A_2$ , atunci  $A_0 \sim A_1$ .

**Demonstrație.** Fie  $f : A_0 \rightarrow A_2$  o funcție bijectivă și definim familia de mulțimi  $(A_n)_{n \geq 0}$  prin formula de recurență  $A_{n+2} = f(A_n)$ . Deoarece  $A_2 \subseteq A_1 \subseteq A_0$ , se arată prin inducție că  $A_n \supseteq A_{n+1}$  pentru orice  $n \geq 0$ .

Fie  $B = \bigcap_{n \in \mathbb{N}} A_n$ ; atunci  $A = B \cup \bigcup_{n \in \mathbb{N}} (A_n \setminus A_{n+1})$  și  $(A_i \setminus A_{i+1}) \cap (A_j \setminus A_{j+1}) = \emptyset$  dacă  $i \neq j$ . Deoarece  $A_{n+2} = f(A_n)$ , rezultă că funcția

$$f_n : (A_n \setminus A_{n+1}) \rightarrow (A_{n+2} \setminus A_{n+3}), \quad f_n(x) = f(x)$$

este bijectivă pentru orice  $n \geq 0$ . Funcția bijectivă căutată  $g : A_0 \rightarrow A_1$  se definește astfel:

$$g(x) = \begin{cases} x, & \text{dacă } x \in B, \\ f(x), & \text{dacă } x \in A_{2n} \setminus A_{2n+1}, n \in \mathbb{N}, \\ x, & \text{dacă } x \in A_{2n-1} \setminus A_{2n}, n \in \mathbb{N}. \quad \blacksquare \end{cases}$$

**Teorema 9.2.3** Relația „ $\leq$ ” este relație de ordine totală. (În particular, are loc trihotomia: dacă  $\alpha$  și  $\beta$  sunt numere cardinale, atunci sau  $\alpha < \beta$  sau  $\alpha = \beta$  sau  $\alpha > \beta$ .)

**Demonstrație.** Dacă  $\alpha = |A|$ , atunci  $\alpha \leq \alpha$ , pentru că  $1_A : A \rightarrow A$  este funcție injectivă.

Dacă  $\alpha = |A|, \beta = |B|, \gamma = |C|$  și  $\alpha \leq \beta, \beta \leq \gamma$ , atunci există funcțiile injective  $f : A \rightarrow B$  și  $g : B \rightarrow C$ ; deoarece și  $g \circ f : A \rightarrow C$  este injectivă, rezultă că  $\alpha \leq \gamma$ .

Fie acum  $\alpha = |A|, \beta = |B|$  astfel încât  $\alpha \leq \beta$  și  $\beta \leq \alpha$ , deci există funcțiile injective  $f : A \rightarrow B$  și  $g : B \rightarrow A$ . Fie  $A_0 = A, A_1 = g(B), B_1 = f(A)$  și  $A_2 = g(B_1)$ . Deoarece  $B_1 \subseteq B$ , rezultă că  $A_2 \subseteq A_1 \subseteq A_0$ . Mai departe,  $g \circ f$  este funcție injectivă și  $(g \circ f)(A_0) = g(f(A)) = g(B_1) = A_2$ , 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  $\alpha = |A|, \beta = |B|$  și pentru orice  $X \subseteq A, Y \subseteq B$ , fie

$$\mathcal{B}(X, Y) = \{f : X \rightarrow Y \mid f \text{ bijectiv}\}, \\ \mathcal{B} = \bigcup_{(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(B)} \mathcal{B}(X, Y).$$

Pe mulțimea  $\mathcal{B}$ -n definim relația „ $\leq$ ” astfel: dacă  $f : X \rightarrow Y$  și  $f' : X' \rightarrow Y'$ , atunci  $f \leq f'$  dacă și numai dacă  $X \subseteq X'$  și  $f$  este restricția lui  $f'$  la  $X$ . Se verifică ușor că  $(\mathcal{B}, \leq)$  este o mulțime nevidă ordonată.

Fie  $\mathcal{L} = \{f_i : X_i \rightarrow Y_i \mid i \in I\} \subseteq \mathcal{B}$  o submulțime total ordonată, și arătăm că  $\mathcal{L}$  are majorantă în  $\mathcal{B}$ . Într-adevăr, fie  $X = \bigcup_{i \in I} X_i, Y = \bigcup_{i \in I} Y_i$  și fie  $f : X \rightarrow Y, f(x) = f_i(x)$  dacă  $x \in X_i$ . Este ușor de arătat că  $f$  este funcție bine definită, bijectivă, și  $f_i \leq f$  pentru orice  $i \in I$ .

Din lema lui Zorn rezultă că în  $\mathcal{B}$  există un element maximal  $f_0 : X_0 \rightarrow Y_0$ , deci este suficient de demonstrat că  $X_0 = A$  sau  $Y_0 = B$ . Presupunem că  $X_0 \neq A, Y_0 \neq B$  și fie  $a_0 \in A \setminus X_0$  și  $b_0 \in B \setminus Y_0$ . Observăm că funcția

$$f' : X_0 \cup \{a_0\} \rightarrow Y_0 \cup \{b_0\}, \quad f'(x) = \begin{cases} f_0(x), & \text{dacă } x \in X_0, \\ b_0, & \text{dacă } x = a_0 \end{cases}$$

este bijectivă și  $f_0 \leq f'$ , ceea ce contrazice maximalitatea lui  $f_0$ . ■

**Teorema 9.2.4 (Cantor)** Pentru orice număr cardinal  $\alpha$  avem  $\alpha < 2^\alpha$ .

**Demonstrație.** Fie  $\alpha = |A|$ . Deoarece  $A \rightarrow \mathcal{P}(A), a \mapsto \{a\}$  este funcție injectivă, rezultă că  $\alpha \leq 2^\alpha$ . Presupunem că  $\phi : A \rightarrow \mathcal{P}(A)$  este bijectiv, și 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 contradicție, deci  $\alpha < 2^\alpha$ . ■



### 9.3 Mulțimi finite, infinite și numărabile

**Definiția 9.3.1** a) Spunem că  $A$  este mulțime **finită**, dacă este echipotentă cu un număr natural, adică  $\exists n \in \mathbb{N}$  astfel ca  $A \sim n$ . Mulțimea  $A$  este **infinită**, dacă nu este finită.

b) Spunem că  $A$  este mulțime **infinită numărabilă**, dacă este echipotentă cu mulțimea numerelor naturale, adică  $A \sim \mathbb{N}$ . Notăm cu  $\aleph_0$  cardinalul lui  $\mathbb{N}$ .

c) Spunem că  $A$  este mulțime **numărabilă** (sau **cel mult numărabilă**), dacă este finită sau infinit numărabilă.

d) Notăm cu  $\mathfrak{c}$  cardinalul mulțimii  $\mathbb{R}$  a numerelor reale, și spunem că  $\mathbb{R}$  are **puterea continuului**.

**Teorema 9.3.2** a) *Orice submulțime a unei mulțimi finite este finită.*

b) *Dacă  $n, m \in \mathbb{N}$  și există  $f : n \rightarrow m$  funcție injectivă, atunci  $n \subseteq m$ . În particular, dacă  $n \sim m$ , atunci  $n = m$ , adică orice mulțime finită este echipotentă cu un singur număr natural.*

**Demonstrație.** a) Este suficient de arătat că pentru orice număr natural  $n$ , orice submulțime a lui  $n$  este finită. Deoarece mulțimea

$$S := \{n \in \mathbb{N} \mid \text{orice submulțime a lui } n \text{ este finită}\}$$

satisfacă  $\emptyset \in S$  și  $n \in S \Rightarrow n^+ \in S$ , din principiul inducției matematice obținem  $S = \mathbb{N}$ .

b) Considerăm mulțimea

$$T = \{n \in \mathbb{N} \mid \text{pentru orice } m \in \mathbb{N}, \text{ dacă există } f : n \rightarrow m \text{ injectivă, atunci } n \subseteq m\}.$$

Este evident că  $\emptyset \in T$ . Fie  $n \in T$ , și presupunem că  $f : n^+ \rightarrow m$  este o funcție injectivă, unde  $m \in \mathbb{N}$ . Deoarece  $n^+ \neq \emptyset$ , rezultă că  $m \neq \emptyset$ , și conform axiomelor lui Peano există  $p \in \mathbb{N}$  astfel încât  $m = p^+$ , deci avem  $f : n^+ = n \cup \{n\} \rightarrow m = p^+ = p \cup \{p\}$ . Dacă  $p \notin f(n)$ , atunci  $g : n \rightarrow p$ ,  $g(x) = f(x)$  este funcție bine definită și injectivă. Dacă  $p \in f(n)$ , atunci fie  $p = f(u)$ ,  $f(n) = v$ , unde  $u \in n$  și  $v \in p$  (într-adevăr, deoarece dacă  $v \notin p$ , atunci  $f(n) = p = f(u)$ , deci  $n = u \in n$ , contradicție). Atunci funcția

$$g : n \rightarrow p, \quad g(x) = \begin{cases} f(x), & \text{dacă } x \neq u, \\ v, & \text{dacă } x = u \end{cases}$$

este injectivă. Deci în ambele cazuri avem o funcție injectivă  $g : n \rightarrow p$ . 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 inducției rezultă  $T = \mathbb{N}$ . ■

**Observații 9.3.3** a) În capitolul următor vom da definiția axiomatică a numărului cardinal. Vom vedea că dacă  $A$  este mulțime finită, adică există unic  $n \in \mathbb{N}$  astfel ca  $A \sim n$ , atunci  $|A| = |n| = n$ . Deci orice număr natural este și 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 mulțime. Următoarele afirmații sunt echivalente:*

- (1)  $A$  este mulțime infinită;
- (2) Există o funcție injectivă  $f : \mathbb{N} \rightarrow A$ ;
- (3)  $A$  are o submulțime proprie echipotentă cu  $A$ .

**Demonstrație.** (1) $\Rightarrow$ (2) Observăm că dacă  $A$  infinit și  $a \in A$ , atunci și  $A \setminus \{a\}$  este infinit (pentru că dacă  $A \setminus \{a\} \sim n$ , atunci  $A \sim n^+ = n + 1$ ). Demonstrația „naivă” decurge astfel. Prin inducție definim un șir  $(A_n)_{n \in \mathbb{N}}$ , unde  $a_n \in A$  și o familie de mulțimi  $(A_n)_{n \in \mathbb{N}}$ , 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  $a_n$  și  $A_n$  sunt definite. Atunci  $A_n$  este infinit, deci există  $a_{n+1} \in A_n$ , și dacă  $A_{n+1} = A_n \setminus \{a_{n+1}\}$ , atunci și  $A_{n+1}$  este infinit. Fie  $f : \mathbb{N} \rightarrow A$ ,  $f(n) = a_n$ , deci  $f$  este funcție injectivă.

Mai exact, trebuie să folosim axioma alegerii. Fie  $\mathbb{N}_n = \{0, 1, \dots, n-1\}$ . Prin inducție (ca mai sus) se arată că pentru orice  $n \in \mathbb{N}$ , există o funcție injectivă  $\phi : \mathbb{N}_n \rightarrow A$ . Dacă  $n \in \mathbb{N}$ , fie

$$M_n = \{\phi : \mathbb{N}_n \rightarrow A \mid \phi \text{ injectivă}\},$$

deci  $M_n \neq \emptyset$ , și avem  $M_n \cap M_m = \emptyset$ , dacă  $m \neq n$ . Din axioma alegerii rezultă că există o mulțime  $M$  astfel încât pentru orice  $n \in \mathbb{N}$ ,  $M_n \cap M$  are exact un element. Vedem că dacă definim mulțimea  $B := \bigcup_{\phi \in M} \text{Im } \phi$ , atunci există o funcție bijectivă  $f : \mathbb{N} \rightarrow B$ .

(2) $\Rightarrow$ (1) Presupunem că  $A$  este finită. Deoarece  $f : \mathbb{N} \rightarrow A$  este injectiv, rezultă că  $\mathbb{N} \sim f(\mathbb{N}) \subseteq A$ . Dar atunci  $\mathbb{N}$  este finită, adică există  $n \in \mathbb{N}$  și o funcție bijectivă  $g : \mathbb{N} \rightarrow n$ . Fie  $h = g|_{n^+} : n^+ \rightarrow n$  restricția funcției  $g$  la  $n^+ \subseteq \mathbb{N}$ . Evident  $h$  este injectiv, deci  $n^+ = n \cup \{n\} \subseteq n$ , contradicție.

(3) $\Rightarrow$ (2) Fie  $B \subset A$  și fie  $f : A \rightarrow B$  o funcție bijectivă. Mai departe, fie  $a_0 \in A \setminus B$ , și prin inducție definim șirul  $(a_n)_{n \in \mathbb{N}}$ ,  $a_{n+1} = f(a_n)$ . Fie  $\phi : \mathbb{N} \rightarrow A$ ,  $\phi(n) = a_n$ , și prin inducție 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  $\phi(1) = a_1$  și  $\phi(m) = f(a_{m-1}) \in B$ ; deoarece  $a_1 \notin B$ , rezultă că  $\phi(1) \neq \phi(m)$ . Presupunem că afirmația este adevărată pentru  $n$ , și fie  $m \neq n + 1$ . Dacă  $m = 1$ , atunci  $\phi(m) = a_1 \notin B$  și  $\phi(n + 1) = f(a_n) \in B$ , deci  $\phi(n + 1) \neq \phi(m)$ . Dacă  $m \neq 1$ , atunci  $\phi(m) = f(a_{m-1})$  și  $\phi(n + 1) = f(a_n)$ . Deoarece  $m - 1 \neq n$ , rezultă că  $a_{m-1} \neq a_n$ , și deoarece  $f$  este injectivă, rezultă că  $f(a_{m-1}) \neq f(a_n)$ , deci  $\phi(m) \neq \phi(n + 1)$ .

(2) $\Rightarrow$ (3) Considerăm funcția

$$\phi : A \rightarrow A \setminus \{f(0)\}, \quad \phi(a) = \begin{cases} a, & \text{dacă } a \notin f(\mathbb{N}), \\ f(n + 1), & \text{dacă } a = f(n) \end{cases},$$

și aratăm că  $\phi$  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  $\phi(a) = f(k + 1)$  și  $\phi(b) = f(l + 1)$ , unde  $a = f(k)$  și  $b = f(l)$ . Deoarece  $f$  este injectivă, rezultă că  $k + 1 = l + 1$ , de unde  $k = l$  și  $a = b$ . Deci  $\phi$  este injectivă. Fie acum  $b \in A \setminus \{f(0)\}$ . Dacă  $b = f(n) \in f(\mathbb{N})$ , atunci  $n \neq 0$  și  $b = f(n - 1 + 1) = \phi(f(n - 1))$ ; dacă  $b \notin f(\mathbb{N})$ , atunci  $b = f(b)$ , deci  $\phi$  este surjectivă. ■

**Corolar 9.3.5** a) Mulțimea  $\mathbb{N}$  a numerelor naturale este infinită, mai mult,  $|\mathbb{N}| =: \aleph_0$  este cel mai mic număr cardinal infinit (sau **transfinit**).

b) Fie  $A$  o mulțime. Următoarele afirmații sunt echivalente:

- (1)  $A$  este finită;
- (2) Dacă  $f : \mathbb{N} \rightarrow A$ , atunci  $f$  nu este injectiv;
- (3) Dacă  $B \subseteq A$  și  $|B| = |A|$ , atunci  $B = A$ .

c) Reuniunea a două mulțimi finite este finită.

**Demonstrație.** c) Fie  $A$  și  $B$  două mulțimi finite. Deoarece  $|A \amalg B| = |A| + |B|$  și suma a două numere naturale este număr natural, rezultă că  $A \amalg B$  este finită. Deoarece există o funcție injectivă  $f : A \cup B \rightarrow A \amalg B$ , rezultă că  $A \cup B$  este finită. ■

**Exercițiul 160** Fie  $A$  o mulțime. Să se arate că următoarele afirmații sunt echivalente:

- (i)  $A$  este mulțime finită;
- (ii) Dacă  $f : A \rightarrow A$  este injectiv, atunci  $f$  este surjectiv;
- (iii) Dacă  $f : A \rightarrow A$  este surjectiv, atunci  $f$  este injectiv.

**Exercițiul 161** Fie  $A$  o mulțime infinită. Să se arate că :

- a)  $|A| + n = |A|$ ,  $\forall n \in \mathbb{N}$ ;
- b)  $|A| + \aleph_0 = |A|$ .

**Exercițiul 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 mulțimi numărabile este numărabilă);
- c) Mulțimea  $\mathcal{P}_f(\mathbb{N}) = \{X \subset \mathbb{N} \mid X \text{ este finită}\}$  a părților finite ale lui  $\mathbb{N}$  este numărabilă;
- d) Mulțimea numerelor raționale este numărabilă;
- e) Mulțimea  $\mathbb{Q}[X]$  a polinoamelor cu coeficienți raționali este numărabilă;
- f) Mulțimea  $\mathbb{A} := \{z \in \mathbb{C} \mid (\exists) P \in \mathbb{Q}[X] \setminus \{0\}, P(z) = 0\}$  a **numerelor algebrice** este numărabilă.

**Teorema 9.3.6** a) Mulțimea  $\mathbb{R}$  a numerelor reale este nenumerabilă, adică  $c > \aleph_0$ ;

b)  $c = 2^{\aleph_0}$ .

**Demonstrație.** a) Folosim **metoda diagonală a lui Cantor**. Fie o funcție

$$f : \mathbb{N}^* \rightarrow [0, 1], \quad f(n) = 0, a_{n1} a_{n2} \dots a_{nn} \dots,$$

unde  $a_{ni} \in \{0, \dots, 9\}$ . Fie  $a_n \in \{0, \dots, 9\}$  astfel încât  $a_n \notin \{0, 9, a_{nn}\}$ , și  $a = 0, a_1, a_2, \dots, a_n, \dots$ . Atunci evident  $f(n) \neq a$  pentru orice  $n \in \mathbb{N}$ , deci funcția  $f$  nu este surjectivă. Astfel am arătat că nu există o funcție bijectivă  $f : \mathbb{N}^* \rightarrow \mathbb{R}$ .

b) Știm că are loc egalitatea

$$2^{\aleph_0} = |\text{Hom}(\mathbb{N}^*, \{0, 1\})|,$$

de aceea vom folosi reprezentarea numerelor reale ca fracții binare infinite. Fie  $\mathbf{a} \in [0, 1)$ ,  $\mathbf{a} = 0, \mathbf{a}_1 \mathbf{a}_2 \dots$  (în baza de numerație 2), unde  $\mathbf{a}_n \in \{0, 1\}$ . Presupunem că 1 nu este perioadă a fracției. Fie funcția

$$\phi : [0, 1) \rightarrow \text{Hom}(\mathbb{N}^*, \{0, 1\}), \quad \phi(\mathbf{a}) = f, \text{ unde } f(n) = \mathbf{a}_n \quad \forall n \geq 1.$$

Atunci funcția  $\phi$  este injectivă, pentru că exprimarea numărului real  $\mathbf{a}$  ca fracții binare infinită fără perioada 1 este unică. În plus, avem că

$$\mathcal{C}(\text{Im } \phi) = \{f : \mathbb{N}^* \rightarrow \{0, 1\} \mid \exists n_0 \text{ astfel încât } f(n) = 1 \quad \forall n > n_0\}.$$

Dar un număr real de forma  $0, \mathbf{b}_1 \mathbf{b}_2 \dots \mathbf{b}_{n_0} 111 \dots$  este rațional, deci  $\mathcal{C}(\text{Im } \phi)$  (adică mulțimea numerelor ce pot fi reprezentate cu perioada 1) este o mulțime numărabilă. Deoarece avem

$$\text{Hom}(\mathbb{N}^*, \{0, 1\}) = \text{Im } \phi \cup \mathcal{C}(\text{Im } \phi),$$

rezultă că  $2^{\aleph_0} = \mathfrak{c} + \aleph_0$ , deci  $\mathfrak{c} = 2^{\aleph_0}$ . ■

**Exercițiul 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) Mulțimea  $\mathbb{R} \setminus \mathbb{Q}$  a numerelor iraționale are puterea continuului (adică  $\mathbb{R} \sim \mathbb{R} \setminus \mathbb{Q}$ ).

**Exercițiul 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  $\alpha$  este un număr cardinal infinit, atunci  $\alpha^2 = \alpha = \alpha\alpha'$  pentru orice  $\alpha'$ , unde  $0 \neq \alpha' \leq \alpha$ .

**Demonstrație.** Fie  $\alpha = |A|$  și arătăm că există o funcție bijectivă  $f : A \rightarrow A \times A$ . Pentru aceasta vom folosi Lema lui Zorn. Fie

$$\mathcal{R} = \{(M, f) \mid M \subseteq A, M \text{ este infinit și } f : M \rightarrow M \times M \text{ este bijectiv}\}.$$

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 mulțimea  $\mathcal{R}$  definim relația de ordine

$$(M, f) \leq (M', f') \iff M \subseteq M' \text{ și } f'|_M = f.$$

Arătăm că în  $\mathcal{R}$  orice lanț are majorantă. Într-adevăr, fie  $\mathcal{L} \subseteq \mathcal{R}$  un lanț, și fie perechea  $(M_0, f_0)$ , unde  $M_0 = \bigcup_{(M, f) \in \mathcal{L}} M$  și  $f_0 : M_0 \rightarrow M_0 \times M_0$ ,  $f_0(x) = f(x)$ , dacă  $(M, f) \in \mathcal{L}$  și  $x \in M$ . Atunci  $f_0$  este bine definită, pentru că  $\mathcal{L}$  este lanț, și  $f_0$  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  $(B, f) \in \mathcal{R}$ , și 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  $2\beta = \beta$ , și prin inducție,  $n\beta = \beta$  pentru orice  $n \in \mathbb{N}$ .

Dacă  $|A \setminus B| \leq \beta$ , atunci deoarece  $A = (A \setminus B) \cup B$ , rezultă că  $\alpha = |A \setminus B| + \beta \leq \beta + \beta = \beta$ , contradicție. Rezultă că  $\beta < |A \setminus B|$ , și există o mulțime  $C \subseteq A \setminus B$  astfel încât  $|C| = \beta$ , deci  $B \sim C$ . Atunci

$$(B \cup C) \times (B \cup C) = (B \times B) \cup (B \times C) \cup (C \times B) \cup (C \times C),$$

și 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 funcție bijectivă  $g : (B \times C) \cup (C \times B) \cup (C \times C) \rightarrow C$ . Considerăm funcția

$$h : B \cup C \rightarrow (B \cup C) \times (B \cup C), \quad h(x) = \begin{cases} f(x), & \text{dacă } x \in B, \\ g(x), & \text{dacă } x \in C. \end{cases}$$

Atunci  $h$  este bijectivă, deci  $(B \cup C, h) \in \mathcal{R}$ , contradicție, pentru că  $(B, f) < (B \cup C, h)$ . Rezultă că ipoteza  $\beta < \alpha$  este falsă, deci  $\beta = \alpha$  și  $\alpha^2 = \alpha$ . ■

## 9.4 Elemente de combinatorică

Discutăm câteva aspecte privind calculul numărului de elemente al unor mulțimi finite.

### 9.4.1 Aranjamente, permutări, combinări

**Definiția 9.4.1** Fie  $A$  și  $B$  două mulțimi finite,  $|A| = k$  și  $|B| = n$ . Fixăm câte o ordonare totală a acestor mulțimi astfel:  $A = \{a_1 < a_2 < \dots < a_k\}$  și  $B = \{b_1 < b_2 < \dots < b_n\}$ .

a) Un șir de lungime  $k$  de elemente din  $B$  se numește **k-aranjament cu repetiție** de  $n$  elemente. Numărul  $k$ -aranjamentelor cu repetiție de  $n$  elemente se notează  $\bar{A}_n^k$ .

b) Un șir de lungime  $k$  de elemente din  $B$ , în care fiecare element apare cel mult o dată, se numește **k-aranjament** de  $n$  elemente. Numărul  $k$ -aranjamentelor de  $n$  elemente se notează  $A_n^k$ .

c) Un șir de lungime  $n$  de elemente din  $B$ , în care fiecare element apare exact o dată, se numește **permutare** de  $n$  elemente. Numărul permutărilor de  $n$  elemente se notează  $P_n$ .

d) O submulțime cu  $k$  elemente a lui  $B$  (unde  $k \leq n$ ) se numește **k-combinare** de  $n$  elemente. Numărul  $k$ -combinărilor de  $n$  elemente se notează  $\binom{n}{k}$  sau  $C_n^k$ .

e) Un șir crescător de lungime  $k$  de elemente din  $B$  se numește **k-combinare cu repetiție** de  $n$  elemente. (Un astfel de șir se mai numește *multiset* cu  $k$  elemente, adică elementele se pot repeta, dar nu contează ordinea lor.) Numărul  $k$ -combinărilor cu repetiție de  $n$  elemente se notează  $\left(\binom{n}{k}\right)$  sau  $\bar{C}_n^k$ .

**Observații 9.4.2** Deoarece șirurile sunt de fapt funcții, definițiile de mai sus se pot reformula astfel:

- Numărul  $k$ -aranjamentelor cu repetiție de  $n$  elemente este egal cu numărul funcțiilor  $f: A \rightarrow B$ .
- Numărul  $k$ -aranjamentelor de  $n$  elemente este egal cu numărul funcțiilor injective  $f: A \rightarrow B$ .
- Numărul permutărilor de  $n$  elemente este egal cu numărul funcțiilor bijective  $f: A \rightarrow B$ .
- Numărul  $k$ -combinărilor de  $n$  elemente este egal cu numărul funcțiilor strict crescătoare  $f: A \rightarrow B$ , sau altfel spus, cu numărul șirurilor strict crescătoare de lungime  $k$  de elemente din  $B$ .
- Numărul  $k$ -combinărilor cu repetiție de  $n$  elemente este egal cu numărul funcțiilor crescătoare  $f: A \rightarrow B$ .

**Exercițiul 165** Pentru  $n = 5$  și  $k = 2$  să se enumere toate

- $k$ -aranjamentele cu repetiție de  $n$  elemente.
- $k$ -aranjamentele de  $n$  elemente.
- permutările de  $n$  elemente.
- $k$ -combinările de  $n$  elemente.
- $k$ -combinările cu repetiție de  $n$  elemente.

**Exercițiul 166** Să se demonstreze :

- $\bar{A}_n^k = n^k$ .
- Dacă  $k \leq n$ , atunci  $A_n^k = \frac{n!}{(n-k)!}$ .
- $P_n = n!$ .
- Dacă  $k \leq n$ , atunci  $C_n^k = \binom{n}{k} = \frac{n!}{k!(n-k)!}$ .
- $\bar{C}_n^k = \left(\binom{n}{k}\right) = \frac{(n+k-1)!}{(n-1)!k!}$ .

**Exercițiul 167** Să se demonstreze :

- $C_n^k = C_n^{n-k}$ ;  $C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$ .
- $(X + Y)^n = \sum_{k=0}^n C_n^k X^{n-k} Y^k$  (*formula binomului*).
- $\sum_{k=0}^n C_n^k = 2^n$  (în două moduri!).

**Exercițiul 168** a) În câte moduri poate fi scris  $n$  ca sumă de  $k$  numere naturale nenule, dacă ținem cont de ordinea termenilor?

- În câte moduri poate fi scris  $n$  ca sumă de  $k$  numere naturale, dacă ținem cont de ordinea termenilor?

**Exercițiul 169** Fie  $|A| = k$ ,  $|B| = n$  și fie  $f: A \rightarrow B$ .

- Dacă  $f$  este injectiv, câte inverse la stânga are  $f$ ?
- Dacă  $f$  este surjectiv, câte inverse la dreapta are  $f$ ?

### 9.4.2 Principiul includerii și al excluderii

**Propoziția 9.4.3 (Principiul includerii și al excluderii)** Dacă  $A_1, \dots, A_n$  sunt mulțimi finite, atunci cardinalul reuniunii lor este dat de formula

$$\begin{aligned} \left| \bigcup_{i=1}^n A_i \right| &= \sum_{i=1}^n |A_i| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| + \sum_{1 \leq i_1 < i_2 < i_3 \leq n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| - \\ &\quad - \dots + (-1)^{k+1} \sum_{1 \leq i_1 < \dots < i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k}| + \dots + (-1)^{n+1} \left| \bigcap_{i=1}^n A_i \right|. \end{aligned}$$

**Demonstrație.** 1. Dacă  $A \cap B = \emptyset$ , atunci  $|A \cup B| = |A| + |B|$ . În general,  $|A_1 \cup A_2| = |A_1| + |A_2 \setminus A_1|$  și  $|A_2| = |A_2 \setminus A_1| + |A_1 \cap A_2|$ , deci

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Continuăm prin inducție. Presupunem că afirmația este adevărată pentru  $n$  mulțimi, și fie  $A_1, \dots, A_n, A_{n+1}$  mulțimi finite. Atunci

$$\begin{aligned} \left| \bigcup_{i=1}^{n+1} A_i \right| &= \left| \bigcup_{i=1}^n A_i \cup A_{n+1} \right| = \left| \bigcup_{i=1}^n A_i \right| + |A_{n+1}| - \left| \bigcup_{i=1}^n A_i \cap A_{n+1} \right| = \\ &= \sum_{i=1}^{n+1} |A_i| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| + \dots + (-1)^{n+1} \left| \bigcap_{i=1}^n A_i \right| + \left| \bigcup_{i=1}^n (A_i \cap A_{n+1}) \right| = \\ &= \sum_{i=1}^{n+1} |A_i| - \sum_{1 \leq i_1 < i_2 \leq n+1} |A_{i_1} \cap A_{i_2}| + \dots + (-1)^{n+2} \left| \bigcap_{i=1}^{n+1} A_i \right|, \end{aligned}$$

deci formula are loc pe baza principiului inducției matematice. ■

**Demonstrație.** 2. A doua demonstrație se bazează pe proprietățile funcției caracteristice, date în Exercițiul 66. Presupunem că  $A_1, \dots, A_n \subseteq A$ . Observăm în plus că pentru o submulțime finită  $X \subseteq A$ , avem

$$|X| = \sum_{x \in A} \chi_X(x).$$

Avem  $A_1 \cup \dots \cup A_n = \complement(\complement A_1 \cap \dots \cap \complement A_n)$  (De Morgan), deci

$$\begin{aligned} \chi_{A_1 \cup \dots \cup A_n} &= 1 - (1 - \chi_{A_1}) \dots (1 - \chi_{A_n}) = \\ &= \sum_{i=1}^n \chi_{A_i} - \sum_{i_1 < i_2} \chi_{A_{i_1}} \chi_{A_{i_2}} + \dots + (-1)^{k+1} \sum_{i_1 < \dots < i_k} \chi_{A_{i_1}} \dots \chi_{A_{i_k}} + \dots + (-1)^{n+1} \prod_{i=1}^n \chi_{A_i} = \\ &= \sum_{i=1}^n \chi_{A_i} - \sum_{i_1 < i_2} \chi_{A_{i_1} \cap A_{i_2}} + \dots + (-1)^{k+1} \sum_{i_1 < \dots < i_k} \chi_{A_{i_1} \cap \dots \cap A_{i_k}} + \dots + (-1)^{n+1} \chi_{\bigcap_{i=1}^n A_i}. \end{aligned}$$

Însumând după valorile în  $x \in A$  ale funcțiilor din ambii membri, obținem formula din enunț. ■

**Exercițiul 170** Aplicații ale principiului includerii și 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 definiție,

$$\phi(m) := |\{a \in \mathbb{N} \mid 1 \leq a \leq m, (a, m) = 1\}|.$$

b) Fie  $\sigma \in S_n$  o permutare de grad  $n$ . Spunem că elementul  $i \in \{1, \dots, n\}$  este **punct fix** al lui  $\sigma$ , dacă  $\sigma(i) = i$ . Câte permutări de grad  $n$  nu au puncte fixe? (Astfel de permutări se mai numesc *deranjamente*.)

**Exercițiul 171** Fie  $A$  și  $B$  două mulțimi finite,  $|A| = k$  și  $|B| = n$ . Dacă  $k \geq n$ , atunci numărul funcțiilor surjective  $f: A \rightarrow B$  este notat  $s(k, n)$  și să se arate că are loc egalitatea

$$s(k, n) = n^k - C_n^1(n-1)^k + C_n^2(n-2)^k + \dots + (-1)^{n-1} C_n^{n-1} 1^k.$$

### 9.4.3 Partiții. Numerele lui Stirling și Bell. Permutări cu repetiție

Am întâlnit relațiile de echivalență și partițiile în Secțiunea 4.4.2. Determinăm numărul lor în cazul mulțimilor finite.

**Definiția 9.4.4** Notăm cu  $\mathcal{E}(A)$  mulțimea tuturor relațiilor de echivalență pe  $A$ . Dacă  $1 \leq n \leq k$ , unde  $|A| = k$  atunci notăm cu  $\mathcal{E}_n(A) = \{\rho \in \mathcal{E}(A) \mid |A/\rho| = n\}$  mulțimea relațiilor de echivalență pe  $A$  pentru care mulțimea factor (adică partiția corespunzătoare) are  $n$  clase.

- Numărul  $|\mathcal{E}_n(A)|$  se numește **numărul Stirling de speța a II-a** și se notează  $\left\{ \begin{smallmatrix} k \\ n \end{smallmatrix} \right\}$  sau  $S(k, n)$ .
- Numărul  $|\mathcal{E}(A)|$  al relațiilor de echivalență pe  $A$  se numește **numărul lui Bell**, notat  $B_k$ .

**Exercițiul 172** Să se enumere toate partițiile mulțimii  $A = \{a_1, a_2, a_3, a_4, a_5\}$ .

**Exercițiul 173** Folosind legătura dintre funcții surjective și relații de echivalență, să se arate că:

- $S(k, n) = \left\{ \begin{smallmatrix} k \\ n \end{smallmatrix} \right\} = \frac{s(k, n)}{n!}$ .
- Numărul partițiilor mulțimii  $A$  coincide cu numărul lui Bell  $B_k$  și mai mult, avem  $B_k = \sum_{n=1}^k S(k, n)$ .

**Definiția 9.4.5** Fie  $A = \{a_1, \dots, a_k\}$  și  $B = \{b_1, \dots, b_n\}$  două mulțimi ca mai sus, și fie  $f: A \rightarrow B$  o funcție. 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  $1 \leq i \leq n$ , atunci spunem că  $(f^{-1}(b_1), \dots, f^{-1}(b_n))$  este o **partiție ordonată de tip**  $(k_1, \dots, k_n)$  a mulțimii  $A$ . (Să observăm că este permis aici ca unele din clasele partiției să fie vide.)

b) O **permutare cu repetiție de tip**  $(k_1, \dots, k_n)$  a celor  $n$  elemente ale mulțimii  $B$  este un șir de lungime  $k$  de elemente din  $B$  astfel încât elementul  $b_i$  apare exact de  $k_i$  ori, pentru  $1 \leq i \leq n$ . Numărul permutărilor cu repetiție de tip  $(k_1, \dots, k_n)$  se notează cu  $P_k^{k_1, \dots, k_n}$  sau  $\binom{k}{k_1 \dots k_n}$ .

**Exercițiul 174** a) Să se enumere toate partițiile ordonate de tip  $(2, 1, 2)$  ale mulțimii  $A = \{a_1, a_2, a_3, a_4, a_5\}$ .

- Să se enumere toate 5-permutările cu repetiție de tip  $(2, 1, 2)$  ale elementelor mulțimii  $B = \{b_1, b_2, b_3\}$ .

**Exercițiul 175** a) Să se demonstreze că numărul partițiilor ordonate de tip  $(k_1, \dots, k_n)$  ale mulțimii  $A$  coincide cu numărul  $P_k^{k_1, \dots, k_n}$  al permutărilor cu repetiție de tip  $(k_1, \dots, k_n)$  ale elementelor lui  $B$ ; mai mult, are loc egalitatea

$$\binom{k}{k_1 \dots k_n} = \frac{k!}{k_1! \dots k_n!}.$$

- Să se interpreteze aranjamentele, permutările și combinările în termeni de permutări cu repetiție.

**Exercițiul 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

Numeralele ordinale, introduse de Georg Cantor în 1883, reprezintă clase de izomorfism de mulțimi bine ordonate și sunt o generalizare a numerelor naturale. Ele pot fi privite ca niște etichete sau indici pe care le folosim când vrem să punem în ordine (enumerăm) elementele unei mulțimi nu neapărat finite.

### 10.1 Noțiunea de număr ordinal

**Definiția 10.1.1** a) Spunem că mulțimile ordonate  $(A, \leq)$  și  $(B, \leq)$  sunt **asemenea** (notație:  $A \simeq B$ ), dacă există o funcție crescătoare, bijectivă  $f : A \rightarrow B$  astfel ca  $f^{-1}$  este crescătoare. (Asemănarea se mai numește **izomorfism de ordine**.)

b) O mulțime  $\alpha$  se numește **număr ordinal** dacă satisface următoarele proprietăți:

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  $\alpha$  este un număr ordinal, atunci definim pe  $\alpha$  relația “ $\preceq$ ” astfel:

$$u \preceq v \text{ dacă } u \in v \text{ sau } u = v$$

**Exercițiul 177** Să se arate că:

- 1) Asemănarea este relație de echivalență pe clasa mulțimilor ordonate.
- 2) Dacă  $(A, \leq)$  este bine ordonată și  $(B, \leq)$  este asemenea cu  $A$ , atunci și  $B$  este bine ordonată.
- 3) Dacă  $\alpha$  este un număr ordinal, atunci relația “ $\preceq$ ” este o relație de bună ordonare pe  $\alpha$ .

**Definiția 10.1.2** a) Fie  $(A, \leq)$  o mulțime bine ordonată. Se poate arăta că există unic număr ordinal  $\alpha$  astfel ca  $(A, \leq)$  este asemenea cu  $(\alpha, \preceq)$ . În acest caz  $\alpha$  se numește **numărul ordinal al mulțimii bine ordonate**  $(A, \leq)$  și notăm  $\alpha = \overline{(A, \leq)}$ . (De multe ori vom nota doar prin  $\bar{A}$  numărul ordinal al mulțimii bine ordonate  $(A, \leq)$ .)

b) Din 7.1.3 e) și 7.1.10 1),2) rezultă că numerele naturale, respectiv mulțimea (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 mulțimi bine ordonate infinite se numește număr ordinal **transfinit**. În particular,  $\bar{\mathbb{N}} = \omega$  este număr ordinal transfinit.

**Exercițiul 178** Să se arate că:

- 1) Dacă  $A, B$  sunt mulțimi bine ordonate, atunci  $A \simeq B$  dacă și numai dacă  $\bar{A} = \bar{B}$ .
- 2) Dacă  $\alpha$  este un număr ordinal și  $a \in \alpha$ , atunci și  $a$  este număr ordinal.

**Definiția 10.1.3 (ordonarea numerelor ordinale)** Fie  $\alpha = \bar{A}$  și  $\beta = \bar{B}$  numere ordinale.

a) Spunem că  $\alpha$  este mai mic decât  $\beta$  (notație:  $\alpha < \beta$ ), dacă există  $b \in B$ , astfel încât  $A \simeq B_b$ , unde submulțimea

$$B_b := \{y \in B \mid y < b\}$$

se numește **segment inițial** al lui  $B$ .

- b) Spunem că  $\alpha \leq \beta$  dacă  $\alpha < \beta$  sau  $\alpha = \beta$ .

**Teorema 10.1.4** Definițiile relațiilor „ $<$ ” și „ $\leq$ ” nu depind de alegerea reprezentanților și sunt adevărate următoarele afirmații:

- 1) Dacă  $\alpha, \beta$  sunt numere ordinale, atunci  $\alpha \leq \beta \Leftrightarrow \alpha \preceq \beta \Leftrightarrow \alpha \subseteq \beta$ ;
- 2) Dacă  $\beta$  este un număr ordinal, atunci  $\beta = \{\alpha \mid \alpha < \beta\}$ ;
- 3)  $\alpha \not\subseteq \alpha$  pentru orice număr ordinal  $\alpha$ ;
- 4) Dacă  $\alpha < \beta$ , atunci  $\beta \not\subseteq \alpha$ ;
- 5) Relația „ $<$ ” este tranzitivă;
- 6) „ $\leq$ ” este relație de ordine;
- 7) Dacă  $M$  este o mulțime ale cărei elemente sunt numere ordinale, atunci  $(M, \leq)$  este bine ordonată;
- 8) Dacă  $\alpha$  și  $\beta$  sunt numere ordinale, atunci din următoarele trei afirmații exact una este adevărată:  
(a)  $\alpha = \beta$ ;    (b)  $\alpha < \beta$ ;    (c)  $\beta < \alpha$ .

**Demonstrație.** Fie  $\alpha = \bar{A}$ ,  $\beta = \bar{B}$  și presupunem că  $A \simeq B_b$ . Dacă  $A'$  și  $B'$  sunt mulțimi bine ordonate astfel ca  $A \simeq A'$  și  $B \simeq B'$ , atunci există o asemănare  $g : B \rightarrow B'$ . Fie  $b' = g(b)$ ; atunci  $B_b \simeq B'_{b'}$ , deci  $A' \simeq B'_{b'}$ , deci definiția lui „ $<$ ” nu depinde de alegerea reprezentanților.

3), 4) Este suficient de arătat că dacă  $A$  este bine ordonată și  $a \in A$ , atunci  $A \not\subseteq A_a$ .

Într-adevăr, presupunem că  $f : A \rightarrow A_a$  este o asemănare. Atunci  $f(a) < a$ , deci mulțimea

$$C := \{x \in A \mid f(x) < x\}$$

este nevidă. Fie  $a_0 = \min C$ ; rezultă că  $f(a_0) < a_0$ , și  $f(f(a_0)) < f(a_0)$ , deci  $f(a_0) \in C$ . Dar  $f(a_0) < a_0$ , deci avem o contradicție.

5) (*Tranzitivitatea*) Fie  $\alpha = \bar{A}$ ,  $\beta = \bar{B}$  și  $\gamma = \bar{C}$ . Deoarece  $\alpha < \beta$  și  $\beta < \gamma$ , există  $b \in B$  și  $c \in C$  astfel încât  $A \simeq B_b$  și  $B \simeq C_c$ . Mai departe, fie  $g : B \rightarrow C_c$  o asemănare, și fie  $c' = g(b)$ . Atunci  $B_b \simeq C_{c'}$ , deci  $A \simeq C_{c'}$  și  $\alpha < \gamma$ . ■

**Exercițiul 179** Să se arate că:

- a) Dacă  $A$  este o mulțime bine ordonată și  $a, a' \in A$ ,  $a \neq a'$ , atunci  $A_a \not\subseteq A_{a'}$ ;
- b) Dacă  $A$  și  $B$  sunt mulțimi bine ordonate și  $f, g : A \rightarrow B$  sunt două asemănări, atunci  $f = g$ .

**Exercițiul 180** Să se completeze demonstrația Teoremei 10.1.4.

**Definiția 10.1.5** Din definiția numărului ordinal rezultă că dacă  $\alpha$  este un număr ordinal, atunci **succesorul**

$$\alpha^+ := \alpha \cup \{\alpha\}$$

al lui  $\alpha$  este de asemenea număr ordinal.

- a) Un număr ordinal  $\beta$  se numește **de speța I**, dacă există un număr ordinal  $\alpha$  astfel încât  $\beta = \alpha^+$ .
- b) Un număr ordinal  $\beta$  se numește **de speța II** sau **ordinal limită**, dacă nu este de speța I și scriem

$$\beta = \lim_{\alpha < \beta} \alpha.$$

**Observații 10.1.6** Vedem că număr ordinal  $\beta$  este de speța I dacă  $\beta = \bar{A}$ , unde  $A$  este o mulțime bine ordonată care are cel mai mare element (adică există  $\max A$ ). În particular,  $\omega$  este de speța II.

Din Corolarul 5.3.4 obținem următoarea teoremă.

**Teorema 10.1.7 (Principiul inducției transfinite)** Fie  $P$  un predicat de o variabilă definit pe numerele ordinale. Presupunem că dacă pentru orice  $\alpha < \beta$  propoziția  $P(\alpha)$  este adevărată, atunci și  $P(\beta)$  este adevărată. Atunci  $P(\alpha)$  este propoziție adevărată pentru orice număr ordinal  $\alpha$ .

Pentru a generaliza Teorema 7.1.4, cu scopul de a da definiții prin recurență transfinite, avem nevoie de câteva noțiuni.

**Definiția 10.1.8** Fie  $A$  bine ordonată și fie  $X$  o mulțime oarecare.

- a) Fie  $a \in A$ . Un **șir de tip a din X** este o funcție  $h : A_a = \{x \in A \mid x < a\} \rightarrow X$ .

De exemplu, un șir de tip  $\omega$  este chiar un șir obișnuit  $h : \mathbb{N} \rightarrow X$  de elemente din  $X$ . Evident, dacă  $g : A \rightarrow X$  este o funcție oarecare, atunci restricția  $g|_{A_a} : A_a \rightarrow X$  funcției  $g$  la  $A_a$  este un șir de tip  $a$  din  $X$ .

- b) Un **șir de tip A din X** este o funcție

$$f : \{g \mid g \text{ este șir de tip } a \text{ din } X, a \in A\} \rightarrow X.$$

**Teorema 10.1.9 (teorema recurenței transfinite)** Dacă  $A$  bine ordonată și  $f$  este un șir de tip  $A$  din  $X$ , atunci există o unică funcție  $g : A \rightarrow X$  astfel încât  $g(a) = f(g|_{A_a})$  pentru orice  $a \in A$ .



## 10.2 Operații cu numere ordinale

**Definiția 10.2.1 (adunarea numerelor ordinale)** a) Fie  $A_1$  și  $A_2$  două mulțimi bine ordonate. Pe reuniunea disjunctă

$$A_1 \amalg A_2 = (A_1 \times \{1\}) \cup (A_2 \times \{2\})$$

definim următoarea relație:

- $(a_1, 1) \leq (a'_1, 1)$  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  $(A_1 \amalg A_2, \leq)$  mulțime bine ordonată și se numește **reuniunea disjunctă ordonată** a lui  $A_1$  și  $A_2$ .

b) Dacă  $\alpha_1 = \bar{A}_1$  și  $\alpha_2 = \bar{A}_2$  sunt numere ordinale, atunci prin definiție,

$$\alpha_1 + \alpha_2 = \overline{A_1 \amalg A_2}.$$

În general, fie  $(\alpha_i)_{i \in I}$  o familie de numere ordinale, unde  $I$  eset o mulțime bine ordonată și  $\alpha_i = \bar{A}_i$ . **Suma** familiei  $(\alpha_i)_{i \in I}$  este numărul ordinal  $\sum_{i \in I} \alpha_i = \overline{\prod_{i \in I} A_i}$ .

Se arată ușor că  $\sum_{i \in I} \alpha_i$  nu depinde de alegerea reprezentanților  $A_i$ , unde  $\bar{A}_i = \alpha_i$ .

**Teorema 10.2.2** Adunarea numerelor ordinale are următoarele proprietăți:

- a) (asociativitatea)  $(\alpha_1 + \alpha_2) + \alpha_3 = \alpha_1 + (\alpha_2 + \alpha_3)$ ;  
 b) Dacă  $\alpha_1 \leq \beta_1$  și  $\alpha_2 \leq \beta_2$ , atunci  $\alpha_1 + \alpha_2 \leq \beta_1 + \beta_2$ . În general, dacă  $\alpha_i \leq \beta_i$ , pentru orice  $i \in I$ , atunci

$$\sum_{i \in I} \alpha_i \leq \sum_{i \in I} \beta_i;$$

- c)  $\alpha \leq \beta$  dacă și numai dacă există un număr ordinal  $\gamma \neq 0$  astfel încât  $\beta = \alpha + \gamma$ ;  
 d) Dacă  $\alpha < \beta$ , atunci pentru orice număr ordinal  $\gamma$  avem

$$1. \gamma + \alpha < \gamma + \beta;$$

$$2. \alpha + \gamma \leq \beta + \gamma;$$

e) Dacă  $\alpha$  este un număr ordinal, atunci  $\alpha^+ = \alpha + 1$ . În particular, adunarea numerelor naturale ca numere ordinale coincide cu adunarea definită recursiv.

**Demonstrație.** b) Fie  $\alpha_i = \bar{A}_i$  și  $\beta_i = \bar{B}_i$ ,  $i = 1, 2$ . Deoarece  $\alpha_i \leq \beta_i$ , există funcțiile injective crescătoare  $f_i : A_i \rightarrow B_i$  astfel încât  $f(A_i)$  este egal cu  $B_i$  sau cu un segment al lui  $B_i$ . Atunci funcția

$$f_1 \amalg f_2 : A_1 \amalg A_2 \rightarrow B_1 \amalg B_2$$

este injectivă crescătoare și  $\text{Im}(f_1 \amalg f_2)$  este egal cu  $B_1 \amalg B_2$  sau cu un segment al lui  $B_1 \amalg B_2$ ; rezultă că  $\alpha_1 + \alpha_2 \leq \beta_1 + \beta_2$ .

c) Fie  $\alpha = \bar{A}$  și  $\beta = \bar{B}$ . Deoarece  $\alpha < \beta$ , există  $b \in B$  astfel încât  $A \simeq B_b$ . Fie  $\gamma = \overline{B \setminus B_b}$ ; deoarece  $B_b \cap B \setminus B_b = \emptyset$  și fiecare element al lui  $B_b$  este mai mic decât fiecare element al lui  $B \setminus B_b$ , rezultă că  $B \simeq B_b \amalg (B \setminus B_b)$ , deci  $\beta = \alpha + \gamma$ .

Invers, fie  $\beta = \alpha + \gamma$ , unde  $\alpha = \bar{A}$ ,  $\beta = \bar{B}$  și  $\gamma = \bar{C}$ . Putem presupune că  $A \cap C = \emptyset$  și  $B = A \cup C$ , deci fiecare element al lui  $A$  este mai mic decât fiecare element al lui  $C$ . Dacă  $c_0 := \min C$ , atunci  $A = B_{c_0}$ , 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  $\alpha = \bar{A}$  și  $a_0$  un element astfel încât  $a_0 \notin A$ . Ca reprezentant al lui  $\alpha + 1$  putem alege mulțimea bine ordonată  $C := A \cup \{a_0\}$  ordonată astfel: dacă  $x, y \in C$ , atunci  $x \leq y$  dacă  $x \leq y$  și  $x, y \in A$ , și  $x \leq a_0$  pentru orice  $x \in C$ .

Atunci  $A = C_{a_0}$  și deci  $\alpha < \alpha + 1$ . Dacă  $\alpha < \beta$ , unde  $\beta = \bar{B}$ , atunci  $A \simeq B_b$  ( $b \in B$ ).

Dacă  $b := \max B$ , atunci  $C \simeq B$ ; în caz contrar există un succesori  $b'$  al lui  $b$ . În acest caz  $C \simeq B_{b'}$ . În consecință  $\alpha + 1 \leq \beta$ , deci  $\alpha + 1$  este succesori al lui  $\alpha$ . ■

**Exercițiul 181** Să se arate că:

- dacă  $(A_1, \leq)$  și  $(A_2, \leq)$  sunt mulțimi bine ordonate, atunci și  $(A_1 \coprod A_2, \leq)$  este mulțime bine ordonată;
- definiția sumei  $\alpha_2 + \alpha_2$  nu depinde de alegerea reprezentanților;
- adunarea numerelor ordinale este asociativă;
- dacă  $n \neq 0$  este un număr natural, atunci  $n + \omega = \omega$  și  $\omega < \omega + n$  (în particular, adunarea numerelor ordinale nu e comutativă);
- dacă  $A_1, A_2, B_1, B_2$  sunt mulțimi bine ordonate și  $f_1 : A_1 \rightarrow B_1$  și  $f_2 : A_2 \rightarrow B_2$  sunt funcții crescătoare, atunci și funcția  $f_1 \coprod f_2 : A_1 \coprod A_2 \rightarrow B_1 \coprod B_2$  este crescătoare.

**Exercițiul 182** Fie  $\alpha, \beta, \gamma, \delta$  numere ordinale. Să se arate că:

- dacă  $\gamma + \alpha < \gamma + \beta$  sau  $\alpha + \gamma < \beta + \gamma$ , atunci  $\alpha < \beta$ ;
- dacă  $\gamma + \alpha = \gamma + \beta$ , atunci  $\alpha = \beta$ ;
- dacă  $\gamma + \alpha = \delta + \beta$  și  $\alpha < \beta$ , atunci  $\gamma > \delta$ .

**Definiția 10.2.3 (înmulțirea numerelor ordinale)** a) Fie  $A$  și  $B$  două mulțimi bine ordonate. Pe produsul cartezian

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

definim relația:

$$(a, b) \leq (a', b') \iff (a < a' \text{ sau } (a = a' \text{ și } b \leq b')).$$

Atunci  $(A \times B, \leq)$  este mulțime bine ordonată, și relația „ $\leq$ ” se numește **ordonarea lexicografică**. Notăție:  $A \times B$ .

- Dacă  $\alpha = \bar{A}$  și  $\beta = \bar{B}$  sunt numere ordinale, atunci prin definiție

$$\alpha\beta = \overline{B \times A}.$$

**Observații 10.2.4** Verificăm că  $(A \times B, \leq)$  este mulțime bine ordonată.

Reflexivitatea și antisimetria sunt evidente. Mai departe, fie  $(a, b), (a', b'), (a'', b'') \in A \times B$  astfel încât  $(a, b) \leq (a', b')$  și  $(a', b') \leq (a'', b'')$ .

*Cazul I.*  $a < a'$  și  $a' < a''$ . Atunci  $a < a''$ , deci  $(a, b) \leq (a'', b'')$ .

*Cazul II.*  $a < a'$  și  $a' = a''$ . Atunci  $a < a''$ , deci  $(a, b) \leq (a'', b'')$ .

La fel tratăm *Cazul III'*.  $a = a'$  și  $a' < a''$ .

*Cazul III.*  $a = a'$  și  $a' = a''$ . Atunci  $b \leq b'$  și  $b' \leq b''$ , deci  $b \leq b''$  și  $(a, b) \leq (a'', b'')$ .

Fie  $M \subseteq A \times B$ ,  $M \neq \emptyset$ , și fie  $p_A : A \times B \rightarrow A$ ,  $p_B : A \times B \rightarrow B$  proiecțiile canonice. Atunci  $p_A(M) \neq \emptyset$ , și fie  $\alpha_0 = \min p_A(M)$ . Mai departe, fie  $B' = \{b \in B \mid (\alpha_0, b) \in M\}$ ; deoarece  $B' \neq \emptyset$ , există  $b_0 = \min B'$ . Atunci e evident că  $(\alpha_0, b_0) = \min M$ .

**Exercițiul 183 4.** Să se arate că dacă  $f : A \rightarrow A'$  și  $g : B \rightarrow B'$  sunt asemănări, atunci și funcția

$$f \times g : A \times B \rightarrow A' \times B', \quad (a, b) \mapsto (f(a), g(b))$$

este asemănare. (În particular, definiția produsului  $\alpha\beta$  nu depinde de alegerea reprezentanților.)

**Teorema 10.2.5** *Înmulțirea numerelor ordinale are următoarele proprietăți:*

- (asociativitate)  $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ ;
- (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  $\alpha(\sum_{i \in I} \beta_i) = \sum_{i \in I} \alpha\beta_i$ ;
- Dacă  $\alpha < \beta$ , și  $\gamma \neq 0$ , atunci  $\gamma\alpha < \gamma\beta$ ;
- Dacă  $\alpha \leq \beta$ , atunci  $\alpha\gamma \leq \beta\gamma$ .

**Demonstrație.** a) Considerăm funcția bijectivă

$$\phi : (A \times B) \times C \rightarrow A \times (B \times C), \quad ((a, b), c) \mapsto (a, (b, c)).$$

Este suficient de arătat că

$$((a, b), c) \leq ((a', b'), c') \iff (a, (b, c)) \leq (a', (b', c')).$$

Într-adevăr,

$$\begin{aligned} ((a, b), c) \leq ((a', b'), c') &\iff (a < a') \vee (a = a', b < b') \vee (a = a', b = b', c \leq c') \iff \\ &\iff (a, (b, c)) \leq (a', (b', c')). \end{aligned}$$

b) Fie

$$\psi : (A_1 \coprod A_2) \times B \rightarrow (A_1 \times B) \coprod (A_2 \times B), \quad ((a, i), b) \mapsto ((a, b), i),$$

unde  $a \in A_i$ ,  $i \in \{1, 2\}$ , și  $b \in B$ . Evident că  $\psi$  este bijectiv, și este suficient de arătat că

$$((a, i), b) \leq ((a', i'), b') \iff ((a, b), i) \leq ((a', b'), i').$$

Într-adevăr,

$$\begin{aligned} ((a, i), b) \leq ((a', i'), b') &\iff ((a, i) < (a', i')) \vee ((a, i) = (a', i'), b \leq b') \iff \\ &\iff (a < a', i = i') \vee (i < i') \vee \\ &\vee (a = a', b \leq b', i = i') \iff \\ &\iff ((a, b) \leq (a', b'), i = i') \vee (i < i') \iff \\ &\iff ((a, b), i) \leq ((a', b'), i'). \end{aligned}$$

c) Fie  $\beta = \alpha + \delta$ , unde  $\delta \neq 0$ . Atunci  $\gamma\beta = \gamma(\alpha + \delta) = \gamma\alpha + \gamma\delta$ , și deoarece  $\gamma\delta \neq 0$ , rezultă că  $\gamma\alpha < \gamma\beta$ .

d) Rezultă din definiții. ■

**Observații 10.2.6** a) Înmulțirea numerelor ordinale nu e comutativă. De exemplu, să aratăm că  $2 \cdot \omega \neq \omega \cdot 2$ .

Avem  $2 \cdot \omega = \mathbb{N} \times \{1, 2\}$ , unde

$$\mathbb{N} \times \{1, 2\} = \{(0, 1) < (0, 2) < (1, 1) < (1, 2) < \dots < (n, 1) < (n, 2) < \dots\}.$$

Se verifică ușor că funcția

$$f : \mathbb{N} \rightarrow \mathbb{N} \times \{1, 2\}, \quad f(n) = \begin{cases} (\frac{n+1}{2}, 1), & \text{dacă } n \text{ este impar,} \\ (\frac{n}{2}, 2), & \text{dacă } n \text{ este par} \end{cases}$$

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,

$$\begin{aligned} (\omega + 1)2 &= (\omega + 1)(1 + 1) = \\ &= (\omega + 1) + (\omega + 1) = \\ &= \omega + (1 + \omega) + 1 = \\ &= \omega + \omega + 1 = \omega \cdot 2 + 1 = \\ &\neq \omega \cdot 2 + 2. \end{aligned}$$

**Exercițiul 184** Fie  $\alpha, \beta, \gamma, \delta$  numere ordinale. Să se arate că :

- dacă  $\gamma\alpha < \gamma\beta$ , atunci  $\alpha < \beta$ ;
- dacă  $\gamma\alpha = \gamma\beta$ , atunci  $\alpha = \beta$ ;
- dacă  $\gamma\alpha = \delta\beta \neq 0$  și  $\alpha < \beta$ , atunci  $\gamma > \delta$ .

**Definiția 10.2.7 (Exponențierea numerelor ordinale)** Fie  $\alpha$  și  $\beta$  două numere ordinale și definim numărul ordinal  $\alpha^\beta$ . Prin recursie transfinită definim funcția  $f$  pe mulțimea  $\{\lambda \mid \lambda < \beta + 1\}$  astfel:

- $f(0) = 1$ ;
- Presupunem că  $f(\rho)$  este definită pentru orice  $\rho < \lambda$ , ( $\lambda < \beta + 1$ ), și fie

$$f(\lambda) = \begin{cases} f(\lambda - 1) \cdot \alpha, & \text{dacă } \lambda \text{ este de speța I,} \\ \lim_{\rho < \lambda} f(\rho), & \text{dacă } \lambda \text{ este de speța II.} \end{cases}$$

Prin definiție,  $\alpha^\beta = f(\beta)$ .

De exemplu, dacă  $\beta = \omega$ , atunci  $\alpha^\omega = \lim_{n < \omega} \alpha^n$ .

**Teorema 10.2.8** Dacă  $\alpha, \beta, \gamma$  sunt numer ordinale, atunci

- $\alpha^\beta \cdot \alpha^\gamma = \alpha^{\beta+\gamma}$ ;
- $(\alpha^\beta)^\gamma = \alpha^{\beta \cdot \gamma}$ .

**Demonstrație.** Arătăm 1) și 2) prin inducție transfinită după  $\gamma$ . Dacă  $\gamma = 0$ , atunci 1) și 2) au loc. Presupunem că 1) și 2) au loc pentru orice număr ordinal  $\rho < \gamma$ . Avem două cazuri:

a)  $\gamma$  este de speța I. Atunci din definiție 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)  $\gamma$  este de speța II. Atunci

$$\begin{aligned}\alpha^\beta \cdot \alpha^\gamma &= \alpha^\beta \lim_{\mu < \gamma} \alpha^\mu = \lim_{\mu < \gamma} (\alpha^\beta \cdot \alpha^\mu) = \\ &= \lim_{\mu < \gamma} \alpha^{\beta+\mu} = \lim_{\mu < \beta+\gamma} (\alpha^\mu) = \alpha^{\beta+\gamma}, \\ (\alpha^\beta)^\gamma &= \lim_{\mu < \gamma} (\alpha^\beta)^\mu = \lim_{\mu < \gamma} (\alpha^{\beta \cdot \mu}) = \lim_{\nu < \beta \cdot \gamma} (\alpha^\nu) = \alpha^{\beta \cdot \gamma}.\end{aligned}$$

Deci 1) și 2) sunt adevărate. ■

**Observații 10.2.9** În general,  $(\alpha \cdot \beta)^\gamma \neq \alpha^\gamma \cdot \beta^\gamma$ . Într-adevăr, fie  $\beta = \gamma = 3$  și  $\alpha = \omega$ . În acest caz  $\alpha^\gamma \cdot \beta^\gamma = \omega^3 \cdot 27$ , și

$$\begin{aligned}(\alpha \cdot \beta)^\gamma &= (\omega \cdot 3)^3 = (\omega \cdot 3)(\omega \cdot 3)(\omega \cdot 3) = \omega(3 \cdot \omega)(3 \cdot \omega) \cdot 3 = \\ &= \omega \cdot \omega \cdot \omega \cdot 3 = \omega^3 \cdot 3 \neq \omega^3 \cdot 27.\end{aligned}$$

### 10.3 Definiția axiomatică a numărului cardinal

Fie  $A$  o mulțime. Conform teoremei lui Zermelo 5.4.2. 7),  $A$  se poate bine ordona (nu în mod unic), deci mulțimea

$$N(A) = \{\alpha \mid \alpha \text{ număr ordinal și } \alpha \sim A\}$$

este nevidă. Atunci din 10.1.4 rezultă că  $N(A)$  are cel mai mic element relativ la ordonarea numerelor ordinale.

**Definiția 10.3.1 (von Neumann)** Cel mai mic număr ordinal din  $N(A)$  se numește **cardinalul** mulțimii  $A$ . Notăție:  $|A|$ .

**Observații 10.3.2** 1) Definiția clasică numărului cardinal dată de Cantor și pe care am utilizat-o în capitolul anterior nu funcționează în sistemele axiomatiche uzuale ale teoriei mulțimilor, cum ar fi Zermelo–Fraenkel sau von Neumann–Bernays–Gödel. Vedem că definiția 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 și 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 ordonarea numerelor ordinale). Analog se arată că  $|A| \geq |B|$ .

4) Dacă  $A$  este o mulțime finită, atunci am văzut că există unic  $n \in \mathbb{N}$  astfel ca  $A \sim n$ . De aici și din definiția de mai sus deducem că  $|A| = n$ . Afirmăția reciprocă este de asemenea adevărată: dacă  $|A| = n$ , atunci evident  $A \sim n$ , deci  $A$  este finită.

### 10.4 Alefuri și problema continuului

**Definiția 10.4.1** a) Cardinalul unei mulțimi bine ordonate se numește **alef**. Dacă  $\alpha = \bar{A}$  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  $\alpha$ .

b) Dacă mulțimea este infinită, atunci aleful se numește **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  $\alpha$  și  $\beta$  două numere ordinale.

- 1) Dacă  $|\alpha| < |\beta|$ , atunci  $\alpha < \beta$ ;
- 2) Dacă  $\alpha < \beta$ , atunci  $|\alpha| \leq |\beta|$ .

**Demonstrație.** 1) Fie  $\alpha = \bar{A}$  și  $\beta = \bar{B}$ . Dacă  $A \simeq B$ , atunci  $A \sim B$ , deci  $|\alpha| = |\beta|$ , contradicție.

Dacă  $B \simeq A_a$ , unde  $a \in A$ , atunci  $|B| \leq |A|$ , adică  $|\beta| \leq |\alpha|$ , contradicție. 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  $\alpha, \beta$  sunt două numere ordinale, atunci  $|\alpha \cdot \beta| = |\alpha| \cdot |\beta|$ .

**Observații 10.4.5** Dacă  $(\alpha_i)_{i \in I}$  este o familie de numere ordinale, unde mulțimea 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  $I = \mathbb{N}$  și  $\alpha_i = 2$ , 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,  $\prod_{i \in I} |\alpha_i| = 2^{\aleph_0} = c > \aleph_0$ .

Folosind recursia transfinită, stabilim un sistem de notații pentru alefii transfiniți.

**Definiția 10.4.6** a) Fie  $\aleph_0$  cardinalul unei mulțimi bine ordonate numărabile.

b) Fie acum  $\alpha$  un număr ordinal arbitrar și presupunem că pentru orice  $\beta < \alpha$ , este definit numărul cardinal  $\aleph_\beta$ .

- Dacă  $\alpha$  este de speța I, atunci  $\aleph_\alpha$  este succesorul numărului cardinal  $\aleph_{\alpha-1}$ .
- Dacă  $\alpha$  este de speța II, atunci  $\aleph_\alpha$  este succesorul mulțimii bine ordonate  $W = \{\aleph_\beta \mid \beta < \alpha\}$ .

**Observații 10.4.7** 1)  $\aleph_1$  este succesorul lui  $\aleph_0$ ,  $\aleph_2$  este succesorul lui  $\aleph_1$  etc;  $\aleph_\omega$  este succesorul mulțimii bine ordonate  $\{\aleph_n \mid n \text{ număr natural}\}$ .

2) Evident, dacă  $\alpha < \beta$ , atunci  $\aleph_\alpha < \aleph_\beta$ .

**Teorema 10.4.8** Orice cardinal transfinit este de forma  $\aleph_\alpha$ , pentru un număr  $\alpha$ .

**Demonstrație.** Fie  $m$  un cardinal transfinit și fie

$$M := \{x \mid x \text{ cardinal transfinit, } x < m\}.$$

Mulțimea  $M$  este bine ordonată și fie  $\alpha := \overline{M}$ . Arătăm prin inducție transfinită după  $\alpha$  că  $m = \aleph_\alpha$ .

Dacă  $\alpha = 0$ , atunci  $M = \emptyset$ , deci  $m = \aleph_0$ . Presupunem că pentru orice  $\beta < \alpha$ , afirmația are loc.

Dacă  $\alpha$  este de speța I, adică  $\alpha = \beta + 1$ , atunci avem  $\aleph_\beta = n$ , unde  $\beta = \overline{N}$  și  $N = \{x \mid x < n, x \text{ transfinit}\}$ . Evident că  $n < m$  și  $N = M_n$ . 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  $\alpha$  este de speța II. Pentru orice  $\beta < \alpha$  avem că  $\aleph_\beta = n_\beta$ , unde  $\beta = \overline{N}$  și  $N_\beta = \{x \mid x < n_\beta, x \text{ transfinit}\}$ . Evident că pentru orice  $\beta < \alpha$  avem  $n_\beta < m$ . Deoarece  $\alpha = \lim_{\beta < \alpha} \beta$ , rezultă că  $m$  este succesorul mulțimii  $\{n_\beta\}_{\beta < \alpha}$ , adică  $m$  este succesorul mulțimii  $\{\aleph_\beta\}_{\beta < \alpha}$ . ■

Fie  $c = 2^{\aleph_0}$  cardinalul mulțimii  $\mathbb{R}$  a numerelor reale. Din teorema de mai sus rezultă că putem scrie  $c = \aleph_\alpha$ , unde  $\alpha$  este un număr ordinal. Problema determinării numărului ordinal  $\alpha$  se numește **problema continuului**.

**Ipoteza continuului**, formulată de Georg Cantor, afirmă că  $\alpha = 1$ .

În 1938, Kurt Gödel a construit un model al teoriei mulțimilor 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 mulțimilor în care ipoteza continuului nu este adevărată. Aceasta arată că ipoteza continuului este independentă de axiomele NBG, la fel ca axioma alegerii.

# Capitolul 11

## INDICAȚII ȘI SOLUȚII

### 1. Logica propozițiilor

**Exercițiul 1.** Tabelul de adevăr este:

p	q	$p \oplus q$	$p   q$	$p \downarrow q$
0	0	0	1	1
0	1	1	1	0
1	0	1	1	0
1	1	0	0	0

**Exercițiul 11.** b) Considerăm șirul de formule  $(A_m)_{m \geq 1}$  definit prin  $A_{n+k+i} = A_i$  pentru orice  $k \in \mathbb{N}$  și orice  $i = 1, \dots, n$ . Vedem că acest șir este periodic și are perioada  $n$ . Este suficient să arătăm că  $A_i \models A_{i+k}$  pentru orice  $i, k \in \mathbb{N}^*$ . Folosim inducție 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

**Exercițiul 19.** a)  $A = \forall x(S \rightarrow P)$ ;  $E = \forall x(S \rightarrow \neg P)$ ;  $I = \exists x(S \wedge P)$ ;  $O = \exists x(S \wedge \neg P)$ ;  $U = A \vee E$ ;  $Y = I \wedge O$ .

b) Următoarele 15 relații se verifică ușor folosind tautologiile 2.3.9, precum și ipoteza, care spune că propoziția  $\exists xS$  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 aceste 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. Mulțimi

**Exercițiul 21.** Arătăm că orice element al membrului stâng aparține membrului drept și 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  $A \setminus A = B \setminus B = \emptyset$ , și  $A \setminus B = A \cap \complement B$ ,  $B \setminus A = B \cap \complement A$ , obținem că

$$\begin{aligned} A \Delta B &= (A \cup B) \setminus (A \cap B) = (A \setminus (A \cap B)) \cup (B \setminus (A \cap B)) = \\ &= ((A \setminus A) \cup (A \setminus B)) \cup ((B \setminus A) \cup (B \setminus B)) = (A \setminus B) \cup (B \setminus A) = (A \cap \complement B) \cup (B \cap \complement A). \end{aligned}$$

b)  $A \Delta B = (A \setminus B) \cup (B \setminus A) = (B \setminus A) \cup (A \setminus B) = B \Delta A$ ;

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:

$$\begin{aligned} (A \Delta B) \Delta C &= ((A \Delta B) \cap \complement C) \cup (C \cap \complement(A \Delta B)) = \\ &= (((A \cap \complement B) \cup (B \cap \complement A)) \cap \complement C) \cup (C \cap (\complement(A \cup B) \cup (A \cap B))) = \\ &= (A \cap \complement B \cap \complement C) \cup (B \cap \complement A \cap \complement C) \cup (C \cap \complement A \cap \complement B) \cup (A \cap B \cap C); \end{aligned}$$

deoarece ultima expresie este simetrică în  $A, B, C$ , din b) rezultă că

$$(A \Delta B) \Delta C = (B \Delta C) \Delta A = A \Delta (B \Delta C).$$

d)  $A \Delta \emptyset = (A \setminus \emptyset) \cup (\emptyset \setminus A) = A \cup \emptyset = A$ ,  $A \Delta A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset$ ;

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

**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  $A \setminus B \neq \emptyset$ ,  $D \setminus C \neq \emptyset$ ,  $x \in A \setminus B$ ,  $y \in D \setminus C$ , 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  $A_n = \{\dots\{\emptyset\}\dots\}$  ( $n$  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 inducție 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.**  $x <^2 y \Leftrightarrow \exists z \in \mathbb{N} : x < z \text{ și } z < y \Leftrightarrow x + 1 < y \quad (z = x + 1)$ ;

$x <^3 y \Leftrightarrow x < \circ <^2 y \Leftrightarrow \exists z \in \mathbb{N} : x + 1 < z \text{ și } z < y \Leftrightarrow x + 2 < y;$   
 $x < \circ > y \Leftrightarrow \exists z \in \mathbb{N} : x > z \text{ și } z < y \Leftrightarrow \exists z \in \mathbb{N} : z < \min(x, y),$  deci graficul relației  $< \circ >$  este  $(\mathbb{N} \setminus \{0\}) \times (\mathbb{N} \setminus \{0\});$   
 $x > \circ < y \Leftrightarrow \exists z \in \mathbb{N} : x < z \text{ și } z > y \Leftrightarrow \exists z \in \mathbb{N} : z > \max(x, y),$  deci graficul relației  $> \circ <$  este  $\mathbb{N} \times \mathbb{N}.$

**Exercițiul 30.**  $(S \cap S') \circ R = \emptyset; (S \circ R) \cap (S' \circ R) = \{(1, 4), (2, 4), (4, 1), (4, 4)\} \cap \{(1, 4), (4, 4)\} = \{(1, 4), (4, 4)\} \neq \emptyset,$  deci  $(S \cap S') \subset (S \circ R) \cap (S' \circ R); R \circ (S \cap S') = \emptyset; (R \circ S) \cap (R \circ S') = \{(1, 2), (1, 4), (2, 1), (2, 3), (3, 1), (3, 3)\} \cap \{(1, 1), (1, 3), (4, 1), (4, 3)\} = \emptyset,$  deci  $R \circ (S \cap S') = (R \circ S) \cap (R \circ S').$

**Exercițiul 31.** b)  $(\sigma \circ \rho)^{-1} = (D, A, (S \circ R)^{-1})$  și  $\rho^{-1} \circ \sigma^{-1} = (D, A, R^{-1} \circ S^{-1}),$  deci mai este de demonstrat egalitatea  $(S \circ R)^{-1} = R^{-1} \circ S^{-1}:$  pentru orice  $(z, x) \in D \times A$  avem

$$\begin{aligned} (z, x) \in (S \circ R)^{-1} &\Leftrightarrow z(\sigma \circ \rho)^{-1}x \Leftrightarrow x\sigma \circ \rho z \Leftrightarrow \exists y \in B \cap C : x\rho y \text{ și } y\sigma z \Leftrightarrow \\ &\Leftrightarrow \exists y \in B \cap C : z\sigma^{-1}y \text{ și } y\rho^{-1}x \Leftrightarrow z\rho^{-1} \circ \sigma^{-1}x \Leftrightarrow (z, x) \in R^{-1} \circ S^{-1}; \end{aligned}$$

c)  $(\tau \circ \sigma) \circ \rho = (A, F, (T \circ S) \circ R)$  și  $\tau \circ (\sigma \circ \rho) = (A, F, T \circ (S \circ R)),$  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

$$\begin{aligned} (x, t) \in (T \circ S) \circ R &\Leftrightarrow x(\tau \circ \sigma) \circ \rho t \Leftrightarrow \exists y \in B \cap C : x\rho y \text{ și } y\tau \circ \sigma t \Leftrightarrow \\ &\Leftrightarrow \exists y \in B \cap C : x\rho y \text{ și } \exists z \in E \cap D : y\sigma z \text{ și } z\tau t \Leftrightarrow \\ &\Leftrightarrow \exists y \in B \cap C \text{ și } \exists z \in E \cap D : x\rho y \text{ și } y\sigma z \wedge z\tau t \Leftrightarrow \\ &\Leftrightarrow \exists z \in E \cap D : z\tau t \text{ și } \exists y \in B \cap C : x\rho y \text{ și } y\sigma z \Leftrightarrow \\ &\Leftrightarrow \exists z \in E \cap D : z\tau t \text{ și } x\sigma \circ \rho z \Leftrightarrow \exists z \in E \cap D : x\sigma \circ \rho z \text{ și } z\tau t \Leftrightarrow \\ &\Leftrightarrow x\tau \circ (\sigma \circ \rho)t \Leftrightarrow (x, t) \in T \circ (S \circ R); \end{aligned}$$

e) Avem  $\sigma \circ (\rho \cap \rho') = (A, D, S \circ (R \cap R'))$  și  $(\sigma \circ \rho) \cap (\sigma \circ \rho') = (A, D, (S \circ R) \cap (S \circ R')).$  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

$$\begin{aligned} (x, z) \in S \circ (R \cap R') &\Leftrightarrow x\sigma \circ (\rho \cap \rho')z \Leftrightarrow \exists y \in B \cap C : x\rho \cap \rho'y \text{ și } y\sigma z \Leftrightarrow \\ &\Leftrightarrow \exists y \in B \cap C : x\rho y \text{ și } x\rho'y \text{ și } y\sigma z \Leftrightarrow \\ &\Leftrightarrow \exists y \in B \cap C : (x\rho y \text{ și } y\sigma z) \wedge (x\rho'y \text{ și } y\sigma z) \Rightarrow \\ &\Rightarrow \exists y_1 (= y) \in B \cap C : x\rho y_1 \text{ și } y_1\sigma z \text{ și } \exists y_2 (= y) \in B \cap C : x\rho'y_2 \text{ și } y_2\sigma z \Leftrightarrow \\ &\Leftrightarrow x\sigma \circ \rho z \text{ și } x\sigma \circ \rho'z \Leftrightarrow x(\sigma \circ \rho) \cap (\sigma \circ \rho')z \Leftrightarrow (x, z) \in (S \circ R) \cap (S \circ R'). \end{aligned}$$

**Exercițiul 32.**  $R(X) = \{b_4\}; R(a_2) = \{b_4\}; R^{-1}(Y) = \{a_1, a_2, a_3\}; R^{-1}(b_5) = \{a_3\}; R^{-1}(B) = \{a_1, a_2, a_3\}; R(A) = \{b_2, b_3, b_4, b_5\}.$

**Exercițiul 33.**  $\delta\langle 1 \rangle = \{\text{numere naturale divizibile cu } 1\} = \mathbb{N};$   
 $\delta^{-1}(\{4, 9\}) = \{\text{numere naturale ce divid pe } 4 \text{ sau } 9\} = \{1, 2, 3, 4, 9\};$   
 $\delta^{-1}(\mathbb{N}) = \mathbb{N}^*; \delta(\mathbb{N}) = \mathbb{N}.$

**Exercițiul 35.** c) Pentru orice  $b \in B$  avem

$$\begin{aligned} b \in \rho(X \cap X') &\Leftrightarrow \exists a \in X \cap X' : a\rho b \Leftrightarrow \exists a \in X \text{ și } a \in X' : a\rho b \Rightarrow \\ &\Rightarrow \exists a_1 (= a) \in X : a_1\rho b \text{ și } \exists a_2 (= a) \in X' : a_2\rho b \Leftrightarrow b \in \rho(X) \cap \rho(X'); \end{aligned}$$

Pentru orice  $b \in B$  avem

$$\begin{aligned} b \in (\rho \cap \rho')(X) &\Leftrightarrow \exists a \in X : a\rho \cap \rho'b \Leftrightarrow \exists a \in X : a\rho b \text{ și } a\rho'b \Rightarrow \\ &\Rightarrow \exists a_1 (= a) \in X : a_1\rho b \text{ și } \exists a_2 (= a) \in X : a_2\rho'b \Leftrightarrow b \in \rho(X) \cap \rho'(X); \end{aligned}$$

d) Pentru orice  $d \in D$  avem

$$\begin{aligned} d \in (\sigma \circ \rho)(X) &\Leftrightarrow \exists a \in X : a\sigma \circ \rho d \Leftrightarrow \exists a \in X : \exists b \in B \cap C : a\rho b \text{ și } b\sigma d \Leftrightarrow \\ &\Leftrightarrow \exists b \in B \cap C : (\exists a \in X : a\rho b) \text{ și } b\sigma d \Leftrightarrow \exists b \in B \cap C : b \in \rho(X) \text{ și } b\sigma d \Leftrightarrow \\ &\Leftrightarrow \exists b \in \rho(X) \cap C : b\sigma d \Leftrightarrow d \in \sigma(\rho(X) \cap C). \end{aligned}$$

**Exercițiul 36.** (i)  $\Rightarrow$  (ii)  $\forall (x, x) \in \Delta_A$  avem  $x \in A \Rightarrow R\langle x \rangle \neq \emptyset \Rightarrow \exists y \in B : xRy \Rightarrow \exists y \in B : xRy \text{ și } yR^{-1}x \Rightarrow (x, x) \in R^{-1} \circ R;$

(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  $A \subseteq R^{-1}(B),$  și de aici rezultă că  $A = R^{-1}(B),$  deoarece  $R^{-1}(B) \subseteq A;$



(iii) $\Rightarrow$ (iv) implicația din (iv) este echivalentă cu implicația  $P_1 \cap P_2 \neq \emptyset \Rightarrow (R \circ P_1) \cap (R \circ P_2) \neq \emptyset$ , pe care o demonstrăm în continuare:  $P_1 \cap P_2 \neq \emptyset \Rightarrow \exists (x_1, x_2) \in P_1 \cap P_2 \subseteq A' \times A \Rightarrow x_2 \in A$  (conform (iii))  $\Rightarrow \exists x \in A : (x_2, x) \in R \Rightarrow \exists x_2 \in A : (x_1, x_2) \in P_1$  și  $(x_2, x) \in R$  și  $\exists x_2 \in A : (x_1, x_2) \in P_2$  și  $(x_2, x) \in R \Rightarrow (x_1, x) \in R \circ P_1$  și  $(x_1, x) \in R \circ P_2 \Rightarrow (x_1, x) \in (R \circ P_1) \cap (R \circ P_2) \Rightarrow (R \circ P_1) \cap (R \circ P_2) \neq \emptyset$ ;

(iv) $\Rightarrow$ (v) în (iv) fie  $P_1 = P_2 = P$ ;

(v) $\Rightarrow$ (vi) Deoarece  $R(X_1 \cap X_2) \subseteq R(X_1) \cap R(X_2)$  rezultă că  $(R(X_1) \cap R(X_2) = \emptyset \Rightarrow R(X_1 \cap X_2) = \emptyset)$ , deci dacă  $P = \{(x, x) \mid x \in X_1 \cap X_2\}$ , atunci  $R \circ P = \emptyset$  (din (v))  $\Rightarrow P = \emptyset \Rightarrow X_1 \cap X_2 = \emptyset$ ;

(vi) $\Rightarrow$ (vii) în (vi) fie  $X_1 = X_2 = X$ ;

(vii) $\Rightarrow$ (i) considerăm mulțimea  $X = \{x\}$ , unde  $x \in A$ . Dacă  $R(X) = R\langle x \rangle = \emptyset$ , atunci din (vii) rezultă că  $X = \emptyset$ , ceea ce este o contradicție (deoarece  $X = \{x\}$ ); deci  $\forall x \in A \ R\langle x \rangle \neq \emptyset$ .

**Exercițiul 37.** (i) $\Rightarrow$ (ii)  $\forall (y_1, y_2) \in R \circ R^{-1} \ \exists x \in A : y_1 R^{-1}x$  și  $xRy_2 \Rightarrow \exists x \in A : xRy_1$  și  $xRy_2 \Rightarrow \exists x \in A : \{y_1, y_2\} \subseteq R\langle x \rangle$  (din (i))  $\Rightarrow y_1 = y_2 \Rightarrow (y_1, y_2) \in \Delta_B$ ;

(ii) $\Rightarrow$ (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  $(x, z) \in (S_1 \circ R) \cap (S_2 \circ R) \Rightarrow (x, z) \in S_1 \circ R$  și  $(x, z) \in S_2 \circ R \Rightarrow \exists y \in B \ (x, y) \in R$  și  $(y, z) \in S_1$  și  $\exists y' \in B : (x, y') \in R$  și  $(y', z) \in S_2 \Rightarrow \exists x \in A \ (y, x) \in R^{-1}$  și  $(x, y') \in R \Rightarrow (y, y') \in R \circ R^{-1}$  (din (ii))  $\Rightarrow (y, y') \in \Delta_B \Rightarrow y = y' \Rightarrow \exists y \in B : (x, y) \in R$  și  $(y, z) \in S_1$  și  $(y, z) \in S_2 \Rightarrow \exists y \in B : (x, y) \in R$  și  $(y, z) \in S_1 \cap S_2 \Rightarrow (x, z) \in (S_1 \cap S_2) \circ R$ ;

(iii) $\Rightarrow$ (iv)  $S_1 \cap S_2 = \emptyset \Rightarrow (S_1 \cap S_2) \circ R = \emptyset \circ R = \emptyset$  (din (iii))  $\Rightarrow (S_1 \circ R) \cap (S_2 \circ R) = (S_1 \cap S_2) \circ R = \emptyset$ ;

(iv) $\Rightarrow$ (v) în (iv) fie  $S_1 = S$  și  $S_2 = \mathcal{C}(S)$ ;

(v) $\Rightarrow$ (vi) arătăm că  $\neg$ (vi) $\Rightarrow$  $\neg$ (v):  $\neg$ (vi) $\Rightarrow \exists Y_1, Y_2 \subseteq B : Y_1 \cap Y_2 = \emptyset \wedge R^{-1}(Y_1) \cap R^{-1}(Y_2) \neq \emptyset \Rightarrow \exists x \in R^{-1}(Y_1) \cap R^{-1}(Y_2) \Rightarrow \exists y_1 \in Y_1 : xRy_1$  și  $\exists y_2 \in Y_2 : xRy_2$  (deoarece  $Y_1 \cap Y_2 = \emptyset \Rightarrow y_1 \neq y_2 \Rightarrow$  dacă  $S = \{(y_1, y_2)\}$ , atunci  $(y_2, y_2) \in \mathcal{C}(S) \Rightarrow \exists y_1 \in Y_1 : (x, y_1) \in R$  și  $(y_1, y_2) \in S \wedge \exists y_2 \in Y_2 : (x, y_2) \in R$  și  $(y_2, y_2) \in \mathcal{C}(S) \Rightarrow (x, y_2) \in S \circ R \wedge (x, y_2) \in \mathcal{C}(S) \Rightarrow (S \circ R) \cap (\mathcal{C}(S) \circ R) \neq \emptyset \Rightarrow \neg$ (v));

(vi) $\Rightarrow$ (vii) în (vi) fie  $Y_1 = Y$  și  $Y_2 = \mathcal{C}(Y)$ ;

(vii) $\Rightarrow$ (viii)  $R^{-1}(Y) \cup R^{-1}(\mathcal{C}(Y)) = R^{-1}(Y \cup \mathcal{C}(Y)) = R^{-1}(B) = R^{-1}(B)$  și (din (vii))  $R^{-1}(Y) \cap R^{-1}(\mathcal{C}(Y)) = \emptyset \Rightarrow R^{-1}(B) \setminus R^{-1}(Y) = (R^{-1}(Y) \cup R^{-1}(\mathcal{C}(Y))) \setminus R^{-1}(Y) = R^{-1}(\mathcal{C}(Y))$ ;

(viii) $\Rightarrow$ (vii) deoarece  $R^{-1}(B) = R^{-1}(Y) \cup R^{-1}(\mathcal{C}(Y))$  și din (viii) avem  $R^{-1}(B) \setminus R^{-1}(Y) = R^{-1}(\mathcal{C}(Y)) \Rightarrow R^{-1}(Y) \cap R^{-1}(\mathcal{C}(Y)) = \emptyset$ ;

(vii) $\Rightarrow$ (i) arătăm că  $\neg$ (i) $\Rightarrow$  $\neg$ (vii):  $\neg$ (i) $\Rightarrow \exists x \in A : |R\langle x \rangle| \geq 2 \Rightarrow \exists y_1, y_2 \in B : y_1 \neq y_2$  și  $(x, y_1) \in R$  și  $(x, y_2) \in R \Rightarrow x \in R^{-1}\langle y_1 \rangle$  și  $x \in R^{-1}\langle y_2 \rangle \Rightarrow R^{-1}\langle y_1 \rangle \cap R^{-1}\langle y_2 \rangle \neq \emptyset \Rightarrow$  dacă  $Y = \{y_1\}$ , atunci  $y_2 \in \mathcal{C}(Y)$  (deoarece  $y_1 \neq y_2 \Rightarrow \emptyset \neq R^{-1}\langle y_1 \rangle \cap R^{-1}\langle y_2 \rangle = R^{-1}(Y) \cap R^{-1}\langle y_2 \rangle \subseteq R^{-1}(Y) \cap R^{-1}(\mathcal{C}(Y)) \Rightarrow \exists Y \subseteq B : R^{-1}(Y) \cap R^{-1}(\mathcal{C}(Y)) \neq \emptyset \Rightarrow \neg$ (vii)).

**Exercițiul 38.** (i) $\Rightarrow$ (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) $\Rightarrow$ (i) Fie  $Y_1, Y_2 \subseteq B$  astfel ca  $S(Y_1) = S(Y_2)$ ; alegem  $R_1 = \{(x, y_1) \mid x \in A, y_1 \in Y_1\} = A \times Y_1$  și  $R_2 = \{(x', y_2) \mid x' \in A, y_2 \in Y_2\} = A \times Y_2$ ; atunci  $S(Y_1) = S(Y_2) \Rightarrow \forall x \in A : S(R_1\langle y \rangle) = S(R_2\langle y \rangle) \Rightarrow \forall x \in A : (S \circ R_1)\langle y \rangle = (S \circ R_2)\langle y \rangle \Rightarrow S \circ R_1 = S \circ R_2 \Rightarrow R_1 = R_2 \Rightarrow Y_1 = Y_2$ .

**Exercițiul 39.** Rezultă imediat din Exercițiul 38, schimbând pur și simplu notațiile: scriem  $R^{-1}$  în loc de  $S$ ,  $A$  în loc de  $C$ ,  $C$  în loc de  $A$ ,  $S_i^{-1}$  în loc de  $R_i$  ( $i = 1, 2$ ) și ținând 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 totuși și o demonstrație independentă de Exercițiul 38.

$\neg$ (ii) $\Rightarrow$  $\neg$ (i) Presupunem că există  $S_1, S_2 \subseteq B \times C$  astfel ca  $S_1 \circ R = S_2 \circ R$  și  $S_1 \neq S_2$ . Arătăm că există  $Y_1, Y_2 \subseteq B$  astfel ca  $Y_1 \neq Y_2$  și  $R^{-1}(Y_1) = R^{-1}(Y_2)$ .

Din  $S_1 \neq S_2$  rezultă că există  $y \in B$  astfel ca  $S_1\langle y \rangle \neq S_2\langle y \rangle$ , deci putem presupune că există  $z \in C$  astfel ca  $yS_1z$  și  $y \notin S_2z$ .

Fie  $Y_1 := B$  și  $Y_2 := B \setminus \{y\}$ , 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  $xRy$  și  $yS_1z$  obținem  $xS_1 \circ Rz$ . Din ipoteză avem  $xS_2 \circ Rz$ , deci există  $y_1 \in B$  astfel ca  $xRy_1$  și  $y_1S_2z$ , deci  $y_1 \neq y$ . Obținem  $x \in R^{-1}\langle y_1 \rangle \subseteq R^{-1}(B \setminus \{y\}) = R^{-1}(Y_2)$ .

$\neg$ (i) $\Rightarrow$  $\neg$ (ii) Presupunem că există  $Y_1, Y_2 \subseteq B$  astfel ca  $Y_1 \neq Y_2$  și  $R^{-1}(Y_1) = R^{-1}(Y_2) =: X$ . Arătăm că există  $S_1, S_2 \subseteq B \times C$  astfel ca  $S_1 \circ R = S_2 \circ R$  și  $S_1 \neq S_2$ .

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  $aRy_1$  și  $y_1S_1c$ ; atunci  $c \in X = R^{-1}(Y_1) = R^{-1}(Y_2)$  și  $y_1 \in Y_1$ . 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  $aRy_2$  și  $y_2S_2c$ , adică  $aS_2 \circ Rc$ .

Am obținut astfel că  $S_1 \circ R \subseteq S_2 \circ R$ . Analog se arată că  $S_2 \circ R \subseteq S_1 \circ R$ .

**Exercițiul 41.** Dacă relația  $\rho = (A, B, R)$  este funcție, atunci:  $\forall x \in A \Rightarrow (\exists!)y \in B : x\rho y \Rightarrow \exists y \in B : x\rho y$  și  $y\rho^{-1}x \Rightarrow x\rho^{-1} \circ \rho y \Rightarrow \mathbf{1}_A \subseteq \rho^{-1} \circ \rho$  și  $\forall y_1, y_2 \in B : y_1\rho \circ \rho^{-1}y_2 \Rightarrow \exists x \in A : y_1\rho^{-1}x$  și  $x\rho y_2 \Rightarrow \exists x \in A : x\rho y_1$  și  $x\rho y_2$  (dar  $\rho$  este funcție)  $\Rightarrow y_1 = y_2 \Rightarrow \rho \circ \rho^{-1} \subseteq \mathbf{1}_B$ .

Dacă  $\mathbf{1}_A \subseteq \rho^{-1} \circ \rho$  și  $\rho \circ \rho^{-1} \subseteq \mathbf{1}_B$ , atunci:  $\forall x \in A \Rightarrow x\rho^{-1} \circ \rho x$  (deoarece  $\mathbf{1}_A \subseteq \rho^{-1} \circ \rho$ )  $\Rightarrow \exists y \in B : x\rho y$  și dacă  $\exists x \in A, \exists y_1, y_2 \in B : x\rho y_1$  și  $x\rho y_2 \Rightarrow \exists x \in A : y_1\rho^{-1}x$  și  $x\rho y_2 \Rightarrow y_1\rho \circ \rho^{-1}y_2 \Rightarrow y_1 = y_2$  (deoarece  $\rho \circ \rho^{-1} \subseteq \mathbf{1}_B$ ); deci  $\forall x \in A \Rightarrow (\exists!)y \in B : x\rho y \Rightarrow \rho = (A, B, R)$  este funcție.

**Exercițiul 42.** a), b) Deoarece  $f : A \rightarrow B$  este funcție, din Exercițiul 41 avem:  $\mathbf{1}_A \subseteq f^{-1} \circ f$  și  $f \circ f^{-1} \subseteq \mathbf{1}_B \Rightarrow \forall X \subseteq A, \forall Y \subseteq B \Rightarrow X = \mathbf{1}_A(X) \subseteq (f^{-1} \circ f)(X)$  și  $(f \circ f^{-1})(Y) \subseteq \mathbf{1}_B = Y \Rightarrow X \subseteq f^{-1}(f(X)), f(f^{-1}(Y)) \subseteq Y$ .

c) Deoarece  $f : A \rightarrow B$  este funcție, din Exercițiul 41. avem:  $\mathbf{1}_A \subseteq f^{-1} \circ f$  și  $f \circ f^{-1} \subseteq \mathbf{1}_B \Rightarrow f \circ \mathbf{1}_A \subseteq f \circ (f^{-1} \circ f)$  și  $(f \circ f^{-1}) \circ f \subseteq \mathbf{1}_B \circ f \Rightarrow f \subseteq f \circ (f^{-1} \circ f)$  și  $(f \circ f^{-1}) \circ f \subseteq f \Rightarrow f = f \circ (f^{-1} \circ f) = f \circ f^{-1} \circ f$ .

La toate punctele se poate argumenta și independent de Exercițiul 41.

**Exercițiul 43.** f) Pentru orice  $x \in U$  avem:

$$\begin{aligned} x \in \bigcup_{j \in J} (A \cap B_j) &\Leftrightarrow \exists j \in J : x \in A \cap B_j \Leftrightarrow \exists j \in J : x \in A \text{ și } x \in B_j \Leftrightarrow \\ &\Leftrightarrow x \in A \text{ și } \exists j \in J : x \in B_j \Leftrightarrow x \in A \text{ și } x \in \bigcup_{j \in J} B_j \Leftrightarrow x \in A \cap \left( \bigcup_{j \in J} B_j \right). \end{aligned}$$

h) Pentru orice  $x \in U$  avem:

$$\begin{aligned} x \in \bigcup_{i \in I} \left( \bigcap_{j \in J} (A_{ij}) \right) &\Leftrightarrow \exists i \in I : x \in \bigcap_{j \in J} (A_{ij}) \Leftrightarrow \exists i \in I : \forall j \in J : x \in A_{ij} \Rightarrow \\ &\Rightarrow \forall j \in J : x \in \bigcup_{i \in I} A_{ij} \Leftrightarrow x \in \bigcap_{j \in J} \left( \bigcup_{i \in I} A_{ij} \right). \end{aligned}$$

**Exercițiul 44.** a) Pentru orice  $(x, y)$  avem:  $(x, y) \in \left( \bigcap_{i \in I} X_i \right) \times \left( \bigcap_{i \in I} Y_i \right) \Leftrightarrow x \in \bigcap_{i \in I} X_i$  și  $y \in \bigcap_{i \in I} Y_i \Leftrightarrow \forall i \in I : x \in X_i$  și  $y \in Y_i \Leftrightarrow \forall i \in I : (x, y) \in (X_i \times Y_i) \Leftrightarrow (x, y) \in \bigcap_{i \in I} (X_i \times Y_i)$ ;

b) Pentru orice  $(x, y)$  avem:  $(x, y) \in \left( \bigcup_{i \in I} X_i \right) \times \left( \bigcup_{j \in J} Y_j \right) \Leftrightarrow x \in \bigcup_{i \in I} X_i$  și  $y \in \bigcup_{j \in J} Y_j \Leftrightarrow \exists i \in I : x \in X_i$  și  $\exists j \in J : y \in Y_j \Leftrightarrow \exists (i, j) \in I \times J : (x, y) \in X_i \times Y_j \Leftrightarrow (x, y) \in \bigcup_{(i, j) \in I \times J} (X_i \times Y_j)$ .

**Exercițiul 45.** Pentru  $n \in \mathbb{N}^*$  fixat avem:  $B_n = A_n \setminus \left( \bigcap_{i=0}^{n-1} A_i \right) = \bigcup_{i=0}^{n-1} (A_n \setminus A_i)$ ; rezultă că:

$$\begin{aligned} \bigcup_{n \in \mathbb{N}} B_n &= A_0 \cup \bigcup_{n \in \mathbb{N}^*} \left( \bigcup_{i=0}^{n-1} (A_n \setminus A_i) \right) = \\ &= A_0 \cup (A_1 \setminus A_0) \cup \dots \cup (A_n \setminus A_0) \cup (A_n \setminus A_1) \cup \dots \cup (A_n \setminus A_{n-1}) \cup \dots = \\ &= A_0 \cup A_1 \cup A_2 \cup \dots \cup A_n \cup \dots = \bigcup_{n \in \mathbb{N}} A_n \end{aligned}$$

(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,  $m < n$  și  $B_m \cap B_n \neq \emptyset$ , atunci  $\exists x \in U$  astfel încât  $x \in B_m$  és  $x \in B_n$ ; rezultă că  $\exists x \in U : x \in A_m \setminus \left( \bigcap_{i=0}^{m-1} A_i \right)$  și  $x \in A_n \setminus \left( \bigcap_{i=0}^{n-1} A_i \right) = \bigcup_{i=0}^{n-1} (A_n \setminus A_i)$ , deci deoarece  $m < n$ ,  $\exists x \in U : x \in A_m$  și  $x \in A_n \setminus A_m$ , contradicție.

**Exercițiul 46.** b) Considerăm mulțimile  $X_n = \left( -\frac{1}{n}, \frac{1}{n} \right)$ ,  $n \in \mathbb{N}^*$  și funcția  $\text{sgn}$ ; atunci  $\text{sgn} \left( \bigcap_{n \in \mathbb{N}^*} X_n \right) = \{0\} \subset \bigcap_{n \in \mathbb{N}^*} \text{sgn} X_n = \{-1, 0, +1\}$ ;

d) Pentru orice  $x \in A$  avem:

$$x \in f^{-1} \left( \bigcap_{i \in I} Y_i \right) \Leftrightarrow f(x) \in \bigcap_{i \in I} Y_i \Leftrightarrow \forall i \in I : f(x) \in Y_i \Leftrightarrow \forall i \in I : x \in f^{-1}(Y_i) \Leftrightarrow x \in \bigcap_{i \in I} f^{-1}(Y_i).$$

**Exercițiul 47.** Pentru orice  $X$  avem:

$$X \in \mathcal{P} \left( \bigcap_{i \in I} A_i \right) \Leftrightarrow X \subseteq \bigcap_{i \in I} A_i \Leftrightarrow \forall i \in I : X \subseteq A_i \Leftrightarrow \forall i \in I : X \in \mathcal{P}(A_i) \Leftrightarrow X \in \bigcap_{i \in I} \mathcal{P}(A_i).$$

**Exercițiul 48.** a) Pentru orice  $(x, z) \in A \times D$  avem:

$$\begin{aligned} x\sigma \circ \left( \bigcup_{i \in I} \rho_i \right) z &\Leftrightarrow \exists y \in B \cap C : x \bigcup_{i \in I} \rho_i y \text{ și } y\sigma z \Leftrightarrow \exists y \in B \cap C : \exists i \in I : x\rho_i y \text{ și } y\sigma z \Leftrightarrow \\ &\Leftrightarrow \exists i \in I : \exists y \in B \cap C : x\rho_i y \text{ și } y\sigma z \Leftrightarrow \exists i \in I : x\sigma \circ \rho_i z \Leftrightarrow x \bigcup_{i \in I} (\sigma \circ \rho_i) z. \end{aligned}$$

c) Pentru orice  $(x, z) \in A \times D$  avem:

$$\begin{aligned} x\sigma \circ \left(\bigcap_{i \in I} \rho_i\right)z &\Leftrightarrow \exists y \in B \cap C : x \bigcap_{i \in I} \rho_i y \text{ și } y\sigma z \Leftrightarrow \exists y \in B \cap C : \forall i \in I : x\rho_i y \text{ și } y\sigma z \Rightarrow \\ &\Rightarrow \forall i \in I : \exists y \in B \cap C : x\rho_i y \text{ și } y\sigma z \Leftrightarrow \forall i \in I : x\sigma \circ \rho_i z \Leftrightarrow x \bigcap_{i \in I} (\sigma \circ \rho_i)z. \end{aligned}$$

**Exercițiul 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)  $\Rightarrow x_1 = x_2 \Rightarrow g \circ f$  este injectiv;

surjectivitatea:  $\forall z \in C : \exists y \in B : g(y) = z$  (deoarece  $g$  este surjectiv) și  $\forall y \exists x \in A : f(x) = y$  (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)  $\Rightarrow \exists x_1 \in A : f(x_1) = y_1$  și  $\exists x_2 \in A : f(x_2) = y_2$   $\Rightarrow g(f(x_1)) = g(f(x_2)) \Rightarrow (g \circ f)(x_1) = (g \circ f)(x_2)$  ( $g \circ f$  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.

**Observație:** Putem demonstra proprietățile 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 dreapta  $s$ , adică  $(g \circ f) \circ s = \mathbf{1}_C$ . Analog, deoarece  $g$  este injectiv, rezultă că  $\exists$  inversă la stânga  $r$ , deci  $r \circ g = \mathbf{1}_B \Rightarrow r \circ (g \circ f) = f \Rightarrow r \circ ((g \circ f) \circ s) = f \circ s \Rightarrow r = f \circ s \Rightarrow \mathbf{1}_B = r \circ g = f \circ (s \circ g) \Rightarrow s \circ g$  este inversă la dreapta pentru  $f$ , deci  $f$  este surjectiv.

**Exercițiul 50.** a) Pentru orice  $x \in A$  avem:

$$\begin{aligned} x \in f^{-1}(Y_1 \setminus Y_2) &\Leftrightarrow f(x) \in Y_1 \setminus Y_2 \Leftrightarrow f(x) \in Y_1 \wedge f(x) \notin Y_2 \Leftrightarrow \\ &\Leftrightarrow x \in f^{-1}(Y_1) \wedge x \notin f^{-1}(Y_2) \Leftrightarrow x \in f^{-1}(Y_1) \setminus f^{-1}(Y_2). \end{aligned}$$

b) Pentru orice  $y \in B$  avem  $y \in f(X_1 \setminus X_2)$  (deoarece  $f$  este injectiv)  $\Leftrightarrow \exists ! x \in X_1 \setminus X_2 : f(x) = y \Leftrightarrow y = f(x) \in f(X_1)$  și  $y = f(x) \notin f(X_2) \Leftrightarrow y \in f(X_1) \setminus f(X_2)$ .

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)  $\Rightarrow \exists ! x : x \in X_i \forall i \in I$  și  $f(x) = y \Rightarrow \exists x \in \bigcap_{i \in I} X_i : f(x) = y \Rightarrow y \in f(\bigcap_{i \in I} X_i)$ .

**Exercițiul 50.** a) (i)  $\Rightarrow$  (ii) deoarece  $\mathbf{1}_A \subseteq f^{-1} \circ f$  (deoarece  $f$  este funcție), este suficient de demonstrat incluziunea  $f^{-1} \circ f \subseteq \mathbf{1}_A$ : într-adevăr, pentru orice  $x_1, x_2 \in A$  avem:

$$\begin{aligned} x_1 f^{-1} \circ f x_2 &\Rightarrow \exists y \in B : x_1 f y \wedge y f^{-1} x_2 \Rightarrow \exists y \in B : f(x_1) = y \wedge f(x_2) = y \Rightarrow \\ &\Rightarrow f(x_1) = f(x_2) = y \Rightarrow x_1 = x_2 \Rightarrow x_1 \mathbf{1}_A x_2. \end{aligned}$$

(ii)  $\Rightarrow$  (iii) Din (ii) rezultă că  $f^{-1} \circ f = \mathbf{1}_A \Rightarrow \forall X \subseteq A : f^{-1}(f(X)) = \mathbf{1}_A(X) = X$ ;

(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:

$$\begin{aligned} y \in f(X_1) \cap f(X_2) &\Rightarrow \exists x_1 \in X_1 : f(x_1) = y \text{ și } \exists x_2 \in X_2 : f(x_2) = y \Rightarrow \\ &\Rightarrow f^{-1}(\{y\}) = f^{-1}(f(\{x_1\})) = \{x_1\} \text{ și } f^{-1}(\{y\}) = f^{-1}(f(\{x_2\})) = \{x_2\} \Rightarrow \\ &\Rightarrow x_1 = x_2 = x \in X_1 \cap X_2 \Rightarrow \exists x \in X_1 \cap X_2 : f(x) = y \Rightarrow y \in f(X_1 \cap X_2). \end{aligned}$$

(iv)  $\Rightarrow$  (v) în (iv) fie  $X_1 = X$  și  $X_2 = \mathcal{C}(X)$ ; rezultă că  $f(X) \cap f(\mathcal{C}(X)) = \emptyset$ , deci  $f(\mathcal{C}(X)) \subseteq \mathcal{C}(f(X))$ .

(v)  $\Rightarrow$  (i) Pentru orice  $x_1, x_2 \in A$ , dacă  $x_1 \neq x_2 \Rightarrow$  și în (v)  $X = \{x_1\}$ , atunci  $x_2 \in \mathcal{C}(X) \Rightarrow f(x_2) \in \mathcal{C}(f(x_1)) \Rightarrow f(x_1) \neq f(x_2)$ , deci este injectiv;

b) (i)  $\Rightarrow$  (ii) deoarece  $f \circ f^{-1} \subseteq \mathbf{1}_B$  (deoarece  $f$  funcție), este suficient de demonstrat incluziunea  $\mathbf{1}_B \subseteq f \circ f^{-1}$ : într-adevăr deoarece din (i)  $f$  este surjectiv, rezultă că pentru orice  $y \in B \exists x \in A : f(x) = y \Rightarrow \exists x \in A : x f y \Rightarrow \exists : y f^{-1} x \wedge x f y \Rightarrow y f \circ f^{-1} y$ .

(ii)  $\Rightarrow$  (iii) deoarece din (ii) avem  $f \circ f^{-1} = \mathbf{1}_B \Rightarrow \forall Y \subseteq B : (f \circ f^{-1})(Y) = \mathbf{1}_B(Y) = Y$  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  $y \in B f(f^{-1}(y)) = y \Rightarrow \forall y \in B : y f \circ f^{-1} y \Rightarrow \forall y \in B : \exists x \in A : x f y \Rightarrow \forall y \in B : \exists x \in A : f(x) = y$ , deci  $f$  este surjectiv.

(i)  $\Rightarrow$  (iv)  $\forall y \in \mathcal{C}(f(X)) \Rightarrow \forall x \in X : f(x) \neq y$ , dar din (i) avem că  $f$  este surjectiv, deci  $\exists x_y \in \mathcal{C}(X) : f(x_y) = y \Rightarrow y \in f(\mathcal{C}(X))$ .

(iv) $\Rightarrow$ (i) fie în (iv)  $X = A \Rightarrow \mathcal{C}(f(A)) \subseteq f(\mathcal{C}A) \Rightarrow \mathcal{C}(f(A)) = \emptyset \Rightarrow B = f(A)$ , deci  $f$  este surjectiv.

**Exercițiul 52.** a) Presupunem că  $f$  este injectiv; dacă presupunem că există  $s_1, s_2 : B \rightarrow A$  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)  $\Rightarrow \forall y \in B : s_1(y) = s_2(y) \Rightarrow s_1 = s_2 \Rightarrow (\exists!) s : B \rightarrow A$  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  $s_1, s_2 : B \rightarrow A$  pentru  $f$ , astfel încât  $s_1(y) = x_1$  și  $s_2(y) = x_2$ , contradicție, deci  $f$  este injectiv;

b) Fie  $f$  surjectiv: dacă presupunem că există  $r_1, r_2 : B \rightarrow A$  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)  $\Rightarrow \forall y \in B : r_1(y) = r_2(y) \Rightarrow r_1 = r_2$ , deci  $f$  într-adevăr are o inversă la stânga; reciproca într-adevăr nu e adevărată: dacă  $f : \{1\} \rightarrow \{1, 2\}, f(1) = 2$ , atunci  $f$  este injectiv, nu este surjectiv și are exact o inversă la stânga  $r : \{1, 2\} \rightarrow \{1\}, r(2) = 1, r(1) = 1$ .

**Exercițiul 53.** Fie  $g = s \circ r$ , unde  $s$  este inversă la dreapta a funcției surjective  $f' : A \rightarrow f(A), \forall x \in A f'(x) = f(x)$ , iar  $r$  este inversă la stânga a funcției injective canonice  $i : f(A) \rightarrow B, i(y) = y \forall y \in f(A)$ .

**Exercițiul 54.** a)  $\mathbf{1}_A \times \mathbf{1}_B : A \times B \rightarrow A \times B, (\mathbf{1}_A \times \mathbf{1}_B)(x, y) = (\mathbf{1}_A(x), \mathbf{1}_B(y)) = (x, y)$ , deci  $\mathbf{1}_A \times \mathbf{1}_B = \mathbf{1}_{A \times B}$ ;

b)  $(f' \times g') \circ (f \times g) : A \times B \rightarrow A'' \times B'', (f' \circ f) \times (g' \circ g) : A \times B \rightarrow A'' \times B''$  și 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:

$$(f \times g)(X \times Y) = (f \times g)(\{(a, b) \mid a \in X, b \in Y\}) = \{(f(a), g(b)) \mid a \in X, b \in Y\} = f(X) \times g(Y).$$

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  $A = B = A' = B' = \{1, 2\}, M = \{(1, 2), (2, 1)\}$  și fie  $\varphi : A \times B \rightarrow A' \times B', \varphi((1, 1)) = (2, 1), \varphi((1, 2)) = (1, 2), \varphi((2, 1)) = (1, 1), \varphi((2, 2)) = (2, 2)$ .

**Exercițiul 56.** a) „ $\Rightarrow$ ” este lăsat pe seama cititorului.

„ $\Leftarrow$ ” *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  $f$  și  $g$  sunt surjective.

**Exercițiul 57.** a)  $\mathbf{1}_A \coprod \mathbf{1}_B : A \coprod B \rightarrow A \coprod B, (\mathbf{1}_A \coprod \mathbf{1}_B)(1, x_1) = (1, \mathbf{1}_A(x_1)) = (1, x_1) \forall x_1 \in A$ , și  $(\mathbf{1}_A \coprod \mathbf{1}_B)(2, x_2) = (2, \mathbf{1}_B(x_2)) = (2, x_2) \forall x_2 \in B$ , deci  $\mathbf{1}_A \coprod \mathbf{1}_B = \mathbf{1}_{A \coprod B}$ ;

b)  $(f' \coprod g') \circ (f \coprod g), (f' \circ f) \coprod (g' \circ g) : A \coprod B \rightarrow A'' \coprod B''$  și  $\forall x_1 \in A$ :

$$((f' \coprod g') \circ (f \coprod g))(1, x_1) = (f' \coprod g')(1, f(x_1)) = (1, (f' \circ f)(x_1)) = ((f' \circ f) \coprod (g' \circ g))(1, x_1),$$

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

**Exercițiul 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  $(\coprod_{i \in I} f_i) \circ q_i : A_i \rightarrow \coprod_{i \in I} A'_i, q'_i \circ f_i : A_i \rightarrow \coprod_{i \in I} A'_i$  și 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  $\coprod_{i \in I} \mathbf{1}_{A_i} : \coprod_{i \in I} A_i \rightarrow \coprod_{i \in I} A_i, (\coprod_{i \in I} \mathbf{1}_{A_i})(i, a_i) = (i, \mathbf{1}_{A_i}(a_i)) = (i, a_i)$ , deci  $\coprod_{i \in I} \mathbf{1}_{A_i} = \mathbf{1}_{\coprod_{i \in I} A_i}$ ;

c) Avem  $(\coprod_{i \in I} f'_i) \circ (\prod_{i \in I} f_i) : \prod_{i \in I} A_i \rightarrow \prod_{i \in I} A_i''$ ,  $\prod_{i \in I} (f'_i \circ f_i) : \prod_{i \in I} A_i \rightarrow \prod_{i \in I} A_i''$  și pentru orice  $(i, a_i) \in \prod_{i \in I} A_i$  avem

$$\left(\prod_{i \in I} f'_i\right) \circ \left(\prod_{i \in I} f_i\right)(i, a_i) = \left(\prod_{i \in I} f'_i\right)(i, f_i(a_i)) = (i, (f'_i \circ f_i)(a_i)) = \left(\prod_{i \in I} (f'_i \circ f_i)\right)(i, a_i),$$

deci  $(\coprod_{i \in I} f'_i) \circ (\prod_{i \in I} f_i) = \prod_{i \in I} (f'_i \circ f_i)$ .

**Exercițiul 59.** b) știm că o funcție  $f : A \rightarrow B$  este injectiv  $\Leftrightarrow \exists r : B \rightarrow A$  funcție astfel încât  $r \circ f = \mathbf{1}_A$ ; în cazul nostru  $\forall i \in I : f_i$  este injectiv  $\Rightarrow \forall i \in I : \exists r_i : A'_i \rightarrow A_i : r_i \circ f_i = \mathbf{1}_{A_i} \Rightarrow (\prod_{i \in I} r_i) \circ (\prod_{i \in I} f_i) = \prod_{i \in I} (r_i \circ f_i) = \prod_{i \in I} \mathbf{1}_{A_i} = \mathbf{1}_{\prod_{i \in I} A_i}$ , deci există  $\prod_{i \in I} r_i : \prod_{i \in I} A'_i \rightarrow \prod_{i \in I} A_i$  astfel încât  $(\prod_{i \in I} r_i) \circ (\prod_{i \in I} f_i) = \mathbf{1}_{\prod_{i \in I} A_i}$ , adică  $\prod_{i \in I} f_i$  este injectiv.

Analog demonstrăm surjectivitatea lui  $\prod_{i \in I} f_i$ .

**Exercițiul 60.** a) Avem  $\text{Hom}(f, g) : \text{Hom}(A, B) \rightarrow \text{Hom}(A', B')$   $\text{Hom}(f, g)(\alpha) = g \circ \alpha \circ f$ , și  $|\text{Hom}(A, B)| = |B^A| = |B|^{|A|} = 2^2 = 4$ , deci  $\text{Hom}(A, B) = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ , 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  $\beta_k := \text{Hom}(f, g)(\alpha_k), k = 1, 2, 3, 4$ ; 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)  $\text{Hom}(\mathbf{1}_A, \mathbf{1}_B) : \text{Hom}(A, B) \rightarrow \text{Hom}(A, B)$ ,  $\text{Hom}(\mathbf{1}_A, \mathbf{1}_B)(\alpha) = \mathbf{1}_B \circ \alpha \circ \mathbf{1}_A = \alpha$ , deci  $\text{Hom}(\mathbf{1}_A, \mathbf{1}_B) = \mathbf{1}_{\text{Hom}(A, B)}$ .

c)  $\text{Hom}(f \circ f', g' \circ g), \text{Hom}(f', g') \circ \text{Hom}(f, g) : \text{Hom}(A, B) \rightarrow \text{Hom}(A'', B'')$ , și pentru orice  $\alpha \in \text{Hom}(A, B)$  avem:

$$\begin{aligned} \text{Hom}(f \circ f', g' \circ g)(\alpha) &= g' \circ g \circ \alpha \circ f \circ f' = g' \circ (g \circ \alpha \circ f) \circ f' = g' \circ \text{Hom}(f, g)(\alpha) \circ f' = \\ &= \text{Hom}(f', g')(\text{Hom}(f, g)(\alpha)) = (\text{Hom}(f', g') \circ \text{Hom}(f, g))(\alpha) \end{aligned}$$

deci  $\text{Hom}(f \circ f', g' \circ g) = \text{Hom}(f', g') \circ \text{Hom}(f, g)$ .

**Exercițiul 61.** a) Dacă  $f$  este surjectiv și  $g$  este injectiv, atunci  $\exists s : A \rightarrow A'$  astfel încât  $f \circ s = \mathbf{1}_A$  și  $\exists r : B' \rightarrow B$  astfel încât  $r \circ g = \mathbf{1}_B$ ; rezultă că  $\text{Hom}(s, r) \circ \text{Hom}(f, g) = \text{Hom}(f \circ s, r \circ g) = \text{Hom}(\mathbf{1}_A, \mathbf{1}_B) = \mathbf{1}_{\text{Hom}(A, B)}$ , deci există  $\text{Hom}(s, r) : \text{Hom}(A', B') \rightarrow \text{Hom}(A, B)$  astfel încât  $\text{Hom}(s, r) \circ \text{Hom}(f, g) = \mathbf{1}_{\text{Hom}(A, B)}$ , deci  $\text{Hom}(f, g)$  este injectiv;

b) este analog cu a);

c) „ $\Rightarrow$ ” deoarece  $\mathbf{1}_A$  este surjectiv și  $g$  este injectiv, din a) rezultă că  $\text{Hom}(\mathbf{1}_A, g)$  este injectiv;

„ $\Leftarrow$ ” deoarece  $\text{Hom}(\mathbf{1}_A, g)$  este injectiv, rezultă că pentru orice  $\alpha_1, \alpha_2 \in \text{Hom}(A, B)$  avem  $g \circ \alpha_1 = g \circ \alpha_2 \Rightarrow \alpha_1 = \alpha_2$ , adică putem simplifica cu gla stânga  $\Rightarrow g$  este injectiv;

d) este analog cu c).

**Exercițiul 62.** a) Deoarece  $\mathbf{1}_{A_*} : \mathcal{P}(A) \rightarrow \mathcal{P}(A)$ ,  $\mathbf{1}_{A_*}(X) = \mathbf{1}_A(X) = X$  pentru orice  $X \in \mathcal{P}(A)$ , și  $\mathbf{1}_{A^*} : \mathcal{P}(A) \rightarrow \mathcal{P}(A)$ ,  $\mathbf{1}_{A^*}(Y) = \mathbf{1}_A(Y) = Y$ , 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  $Z \in \mathcal{C}$  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

$$(f^* \circ f_* \circ f^*)(Y) = f^{-1}(f(f^{-1}(Y))) = f^{-1}((f \circ f^{-1})(Y)) = (f^{-1} \circ f)(f^{-1}(Y))$$

și, deoarece  $f : A \rightarrow B$  este funcție, dintr-un exercițiu anterior rezultă că  $\mathbf{1}_A \subseteq f^{-1} \circ f$  și  $f \circ f^{-1} \subseteq \mathbf{1}_B$ ; obținem că pentru orice  $Y \subseteq B$  avem  $f^{-1}(Y) \subseteq (f^{-1} \circ f)(f^{-1}(Y)) = (f^* \circ f_* \circ f^*)(Y)$  și  $(f^* \circ f_* \circ f^*)(Y) = f^{-1}((f \circ f^{-1})(Y)) \subseteq f^{-1}(Y)$ , deci  $(f^* \circ f_* \circ f^*)(Y) = f^{-1}(Y) = f^*(Y) \Rightarrow f^* \circ f_* \circ f^* = f^*$ .

d)  $\varphi \circ \varphi = (f^* \circ f_*) \circ (f^* \circ f_*) = (f^* \circ f_* \circ f^*) \circ f_* = f^* \circ f_* = \varphi$ ;  $\psi \circ \psi = (f_* \circ f^*) \circ (f_* \circ f^*) = f_* \circ (f^* \circ f_* \circ f^*) = f_* \circ f^* = \psi$ .

**Exercițiul 63.** a) (i)  $\Rightarrow$  (ii) deoarece  $f$  este injectiv, există  $r : B \rightarrow A$  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  $r_* : \mathcal{P}(B) \rightarrow \mathcal{P}(A)$  astfel încât  $r_* \circ f_* = \mathbf{1}_{\mathcal{P}(A)}$ , deci  $f_*$  este injectiv;

(ii)  $\Rightarrow$  (iii) deoarece  $f$  este funcție, 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)  $\Rightarrow$  (i) deoarece  $f^* \circ f_* = \mathbf{1}_{\mathcal{P}(A)}$ , există  $r := f^* : \mathcal{P}(B) \rightarrow \mathcal{P}(A)$  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 obținem că  $f$  este injectiv;

(iii)  $\Rightarrow$  (iv) din ipoteză avem că există  $s := f_* : \mathcal{P}(A) \rightarrow \mathcal{P}(B)$  astfel încât  $f^* \circ s = \mathbf{1}_{\mathcal{P}(A)}$ , deci  $f^*$  este surjectiv;

(iv)  $\Rightarrow$  (iii)  $f^* \circ f_* \circ f^* = f^*$  și din surjectivitatea lui  $f^* \exists s : \mathcal{P}(A) \rightarrow \mathcal{P}(B)$  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).

**Exercițiul 67.** a) Deoarece  $\rho$  reflexiv  $\Rightarrow \mathbf{1}_A \subseteq \rho$ ; este trebuie demonstrată incluziunea  $\rho \subseteq \mathbf{1}_A$ : dacă  $xpy$  (din simetrie)  $\Rightarrow xpy \wedge ypx$  (din antisimetrie)  $\Rightarrow x = y$  adică  $x\mathbf{1}_A y$ ;

b) dacă  $xpy$  (din reflexivitate)  $\Rightarrow xpy \wedge ypy \Rightarrow xp^2y$ , deci  $\rho \subseteq \rho^2$ ; invers, dacă  $x\rho^2y \Rightarrow \exists z \in A : x\rho z \wedge z\rho y$  (din tranzitivitate)  $\Rightarrow xpy$ , deci  $\rho^2 \subseteq \rho$ .

**Exercițiul 68.** a)  $\rho_\pi = \{(1, 2, 3), \{4\}\}$ ; b)  $\rho_\pi = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 1)\}$ .

**Exercițiul 69.** Întâi determinăm toate partițiile, apoi scriem relațiile de echivalență corespunzătoare. De exemplu pentru  $A = \{1, 2, 3\}$  partițiile sunt:  $\pi_1 = \{\{1, 2, 3\}\}$ ,  $\pi_2 = \{\{1, 2\}, \{3\}\}$ ,  $\pi_3 = \{\{1, 3\}, \{2\}\}$ ,  $\pi_4 = \{\{2, 3\}, \{1\}\}$  și  $\pi_5 = \{\{1\}, \{2\}, \{3\}\}$ . Acestea corespund relațiile de echivalență  $\rho_1 = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 2)\}$ ,  $\rho_2 = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$ ,  $\rho_3 = \{(1, 1), (2, 2), (3, 3), (1, 3), (3, 1)\}$ ,  $\rho_4 = \{(1, 1), (2, 2), (3, 3), (2, 3), (3, 2)\}$  și  $\rho_5 = \{(1, 1), (2, 2), (3, 3)\}$ .

**Exercițiul 70.** a) „ $\mid$ ” nu e simetric, deoarece de exemplu  $2 \mid 4$ , dar invers nu e adevărat; „ $\parallel$ ” nu e antisimetric, deoarece de exemplu  $2 \parallel -2$ ,  $-2 \parallel 2$ , dar  $2 \neq -2$ ;

c)  $\mathbb{Z}/\equiv_{(\text{mod } n)} = \mathbb{Z}_n = \{\hat{a} \mid a \in \mathbb{Z}\}$ , unde  $\hat{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\} = n\mathbb{Z} + a$ .

**Exercițiul 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 origine; clasele din  $\mathbb{C}/\rho_2$  sunt semidrepte deschise ce pornesc din originea  $O$ .

**Exercițiul 72.** b) Deoarece  $\mathbf{1}_A \subseteq \rho_1$ , rezultă că  $\mathbf{1}_A \cap \mathbb{C}\rho_1 = \emptyset$ , deci  $\mathbb{C}\rho_1$  nu e reflexiv, deci  $\mathbb{C}\rho_1$  nu e relație de echivalență;  $\rho_1 \cup \rho_2$  în general nu e tranzitiv. De exemplu, dacă  $A = \{1, 2, 3\}$ ,  $\rho_1 = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$  și  $\rho_2 = \{(1, 1), (2, 2), (3, 3), (1, 3), (3, 1)\}$  sunt două relații de echivalență pe  $A$ , atunci relația  $\rho_1 \cup \rho_2 = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (1, 3), (3, 1)\}$  nu e tranzitivă, deoarece nu conține perechile  $(2, 3)$  și  $(3, 2)$ ;

c) imediat se vede că pentru relația  $\rho$  pe  $A$  avem:  $\rho$  este echivalență  $\iff \mathbf{1}_A \subseteq \rho$  și  $\rho = \rho^{-1} = \rho^2$ . De aici demonstrăm ușor c):

„ $\Rightarrow$ ” dacă  $\rho_1 \circ \rho_2$  echivalență, atunci  $\Rightarrow \rho_1 \circ \rho_2 = (\rho_1 \circ \rho_2)^{-1} = \rho_2^{-1} \circ \rho_1^{-1} = \rho_2 \circ \rho_1$ ;

„ $\Leftarrow$ ” folosind  $\rho_1 \circ \rho_2 = \rho_2 \circ \rho_1$  arătăm că: (1)  $\mathbf{1}_A \subseteq \rho_1 \circ \rho_2$  și (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)  $(\rho_1 \circ \rho_2)^{-1} = \rho_2^{-1} \circ \rho_1^{-1} = \rho_2 \circ \rho_1 = \rho_1 \circ \rho_2$  și  $(\rho_1 \circ \rho_2)^2 = (\rho_1 \circ \rho_2) \circ (\rho_1 \circ \rho_2) = \rho_1 \circ (\rho_2 \circ \rho_1) \circ \rho_2 = \rho_1 \circ (\rho_1 \circ \rho_2) \circ \rho_2 = \rho_1^2 \circ \rho_2^2 = \rho_1 \circ \rho_2$ .

**Exercițiul 73.** b) „ $\Rightarrow$ ” dacă  $\rho_1 \cup \rho_2$  echivalență, 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  $\rho_1 \circ \rho_2$  și  $\rho_2 \circ \rho_1$  este subrelație a lui  $\rho_1 \cup \rho_2$ ;

„ $\Leftarrow$ ” deoarece  $\rho_1$  și  $\rho_2$  sunt relații de echivalență rezultă că  $\rho_1 \cup \rho_2$  reflexiv și simetric; deoarece  $\rho_1 \circ \rho_2$ ,  $\rho_2 \circ \rho_1$  și  $\rho_1^2 \cup \rho_2^2 = \rho_1 \circ \rho_2$  sunt subrelații 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.

**Exercițiul 74.** a) Demonstrăm că  $\bigcup_{n \geq 1} \rho^n$  este tranzitivă: pentru orice  $x, y, z \in A$  avem  $x \bigcup_{n \geq 1} \rho^n y \wedge y \bigcup_{n \geq 1} \rho^n z \Rightarrow \exists m, n \in \mathbb{N}^* : x\rho^m y \wedge y\rho^n z \Rightarrow x\rho^m \circ \rho^n z \Rightarrow x\rho^{n+m} z \Rightarrow x \bigcup_{n \geq 1} \rho^n z$ .

Fie acum  $\sigma$  o relație ce include pe  $\rho$ . Deoarece  $\rho \subseteq \sigma \Rightarrow \rho^2 \subseteq \sigma^2$ , dar  $\sigma$  tranzitiv  $\Rightarrow \sigma^2 \subseteq \sigma$ . Deci  $\rho^2 \subseteq \sigma$  și deoarece  $\rho \subseteq \sigma$  respectiv  $\sigma^2 \subseteq \sigma \Rightarrow \rho^3 \subseteq \sigma$ . Prin inducție 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 relație tranzitivă ce include pe  $\rho$ .

b) Arătăm că relația  $\bigcup_{n \geq 1} \bar{\rho}^n$  este echivalență. 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,  $\left(\bigcup_{n \geq 1} \bar{\rho}^n\right)^{-1} = \left(\bigcup_{n \in \mathbb{Z}} \rho^n\right)^{-1} = \bigcup_{n \in \mathbb{Z}} \rho^{-n} = \bigcup_{n \in \mathbb{Z}} \rho^n = \bigcup_{n \geq 1} \bar{\rho}^n$  și  $\left(\bigcup_{n \geq 1} \bar{\rho}^n\right)^2 = \left(\bigcup_{n \in \mathbb{Z}} \rho^n\right)^2 = \left(\bigcup_{n \in \mathbb{Z}} \rho^n\right)$ .

Fie acum  $\sigma$  o relație de echivalență ce include pe  $\rho$ . Deoarece  $\sigma$  este relație de echivalență  $\Rightarrow \sigma$  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 relație de echivalență ce include pe  $\rho$ ). Deoarece  $\rho \subseteq \sigma$  și  $\sigma$  relație de echivalență  $\Rightarrow \rho^{-1} \subseteq \sigma^{-1} = \sigma \Rightarrow \sigma$  tranzitiv și conține pe  $\rho^{-1} \Rightarrow \bigcup_{n \geq 1} (\rho^{-1})^n \subseteq$

$\sigma$ . Deci:  $\bigcup_{n \geq 1} \rho^n \subseteq \sigma$  și  $\bigcup_{n \geq 1} (\rho^{-1})^n \subseteq \sigma$ , de evident  $\mathbf{1}_A \subseteq \sigma$  (deoarece  $\sigma$  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 relație de echivalență ce include pe  $\rho$ .

**Exercițiul 75.** 1) Este ușor de arătat că  $\ker f$  este reflexiv, simetric și tranzitiv, pentru că și relația „=” este așa. Mai departe,

$$\begin{aligned} a_1 \ker f a_2 &\Leftrightarrow \exists b \in B : f(a_1) = f(a_2) = b \Leftrightarrow \\ &\Leftrightarrow \exists b \in B : a_1 f b \text{ și } a_2 f b \Leftrightarrow \\ &\Leftrightarrow \exists b \in B : a_1 f b \text{ și } b f^{-1} a_2 \Leftrightarrow a_1 (f^{-1} \circ f) a_2. \end{aligned}$$

2) Avem  $f^{-1}(b) = \{a' \in A \mid f(a') = b\}$  și  $A/\ker f = \{\ker f \langle a \rangle \mid a \in A\}$ , unde  $\ker f \langle a \rangle = \{a' \in A \mid f(a') = f(a)\} = f^{-1}(f(a))$ . Deoarece  $f(a) \in \text{Im } f$ , rezultă că  $A/\ker f \subseteq \{f^{-1}(b) \mid b \in \text{Im } f\}$ .

Invers, pentru orice  $b \in \text{Im } f$ , 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  $f : A \rightarrow B$  este o funcție, 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 ușor din definiții.

**Exercițiul 76.** Surjectivitatea rezultă din definiții:  $\forall \rho \langle x \rangle \in A/\rho$ , 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.

**Exercițiul 77.** a) Deoarece  $g$  este surjectiv și  $x_1^2 = x_2^2 \Rightarrow \cos x_1 = \cos x_2$ , adică  $\ker g \subseteq \ker f$ , rezultă că  $(\exists!) h : \mathbb{R}_+ \rightarrow \mathbb{R}$  o funcție astfel încât  $f = h \circ g$ . Determinăm această funcție. Fie  $s : \mathbb{R}_+ \rightarrow \mathbb{R}$ ,  $s(x) = \sqrt{x}$  funcție 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  $h : \mathbb{R}_+ \rightarrow \mathbb{R}$ ,  $h(x) = (f \circ s)(x) = \cos(\sqrt{x})$ .

b) Vedem că  $g$  este surjectiv, dar  $\ker g \not\subseteq \ker f \Rightarrow$  în acest caz nu există o funcție  $h$  ce satisface cerințele.

**Exercițiul 78.** a) Deoarece  $g$  este injectiv și  $[-1, 1] = \text{Im } f \subseteq \text{Im } g = [-3, +\infty)$ , rezultă  $(\exists!) h : \mathbb{R} \rightarrow [-2, \infty)$  funcție astfel încât  $f = g \circ h$ . Determinăm această funcție. Fie

$$r : \mathbb{R} \rightarrow [-2, +\infty), \quad r(x) = \begin{cases} \frac{x-1}{2}, & x \in [-3, +\infty) \\ x_0 \in [-2, +\infty), & x \notin [-3, +\infty) \end{cases}$$

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  $h : \mathbb{R} \rightarrow [-2, +\infty)$ ,  $h(x) = (r \circ f)(x) = \frac{\cos x - 1}{2}$ .

b) Vedem că  $g$  este injectiv, dar  $[-1, 1] = \text{Im } f \not\subseteq \text{Im } g = [1, +\infty) \Rightarrow$  în acest caz nu există o funcție  $h$  ce satisface cerințele.

**Exercițiul 79.** a) Dacă  $f : \mathbb{R} \rightarrow \mathbb{R}$ ,  $f(x) = x^2 : \ker f \langle x \rangle = \{x, -x\}$ ,  $\mathbb{R}/\ker f = \{\{x, -x\} \mid x \in \mathbb{R}\}$ , și  $\bar{f} : \mathbb{R}/\ker f \rightarrow \mathbb{R}_+$   $\bar{f}(\{x, -x\}) = x^2$  este bijectiv.

Dacă  $g : \mathbb{R} \rightarrow \mathbb{R}$ ,  $g(x) = x^4 : \ker g \langle x \rangle = \{x, -x\}$ ,  $\mathbb{R}/\ker g = \{\{x, -x\} \mid x \in \mathbb{R}\}$ , și  $\bar{g} : \mathbb{R}/\ker g \rightarrow \mathbb{R}_+$   $\bar{g}(\{x, -x\}) = x^4$  este bijectiv.

b) Dacă  $f : \mathbb{C} \rightarrow \mathbb{C}$ ,  $f(z) = z^2 : \ker f \langle z \rangle = \{z, -z\}$ ,  $\mathbb{C}/\ker f = \{\{z, -z\} \mid z \in \mathbb{C}\}$ , și  $\bar{f} : \mathbb{C}/\ker f \rightarrow \mathbb{C}$ ,  $\bar{f}(\{z, -z\}) = z^2$  este bijectiv.

Dacă  $g : \mathbb{C} \rightarrow \mathbb{C}$ ,  $g(z) = z^4$ , atunci  $(\ker g) \langle z \rangle = \{z, -z, iz, -iz\}$ , mai departe  $\mathbb{C}/\ker g = \{\{z, -z, iz, -iz\} \mid z \in \mathbb{C}\}$ , și  $\bar{g} : \mathbb{C}/\ker g \rightarrow \mathbb{C}$ ,  $\bar{g}(\{z, -z, iz, -iz\}) = z^4$  este bijectiv.

**Exercițiul 80.** a) Fie  $\varphi : A \times B/\rho \times \sigma \rightarrow A/\rho \times B/\sigma$ ,  $\varphi(\rho \times \sigma \langle (a, b) \rangle) = (\rho \langle a \rangle, \sigma \langle b \rangle)$ . Această funcție este evident bine definită și bijectivă, deoarece se verifică imediat că  $\varphi^{-1} : A/\rho \times B/\sigma \rightarrow A \times B/\rho \times \sigma$ ,  $\varphi^{-1}(\rho \langle a \rangle, \sigma \langle b \rangle) = \rho \times \sigma \langle (a, b) \rangle$  este inversa lui  $\varphi$ .

**Exercițiul 81.** Fie  $\varphi : \mathcal{P}(A)/\rho \rightarrow \mathcal{P}(B)$ ,  $\varphi(\rho \langle X \rangle) = X \cap B$ . Această funcție este evident bine definită și bijectivă; se verifică imediat că are inversa  $\varphi^{-1} : \mathcal{P}(B) \rightarrow \mathcal{P}(A)/\rho$ ,  $\varphi^{-1}(Y) = \rho \langle Y \rangle$ .

**Exercițiul 82.** a) Fie  $\varphi : \text{Hom}(A, B)/\rho \rightarrow B$ ,  $\varphi(\rho \langle f \rangle) = f(a_0)$ . Această funcție este evident bine definită și bijectivă; se verifică imediat că are inversa  $\varphi^{-1} : B \rightarrow \text{Hom}(A, B)/\rho$ ,  $\varphi^{-1}(b) = \rho \langle f_b \rangle$ , unde  $f_b \in \text{Hom}(A, B)$ ,  $f_b(a) = b \quad \forall a \in A$ .

b) Fie  $\psi : \text{Hom}(A, B)/\sigma \rightarrow \text{Hom}(A', B)$ ,  $\psi(\rho\langle f \rangle) = f|_{A'}$ . Această funcție este evident bine definită și bijectivă; se verifică imediat că are inversa  $\varphi^{-1} : \text{Hom}(A', B) \rightarrow \text{Hom}(A, B)/\sigma$ ,  $\varphi^{-1}(f') = \rho\langle f \rangle$ , unde  $f \in \text{Hom}(A, B)$ ,  $f(a) = f'(a) \quad \forall a \in A'$  și  $f(a) = b_0 \in B$  (fixat)  $\forall a \in A \setminus A'$ .

c) Dacă în b) luăm  $A' = \{a_0\}$ , atunci o funcție  $f : \{a_0\} \rightarrow B$  este determinată de elementul  $f(a_0) \in B$ ; deci  $\text{Hom}(A', B)$  se identifică cu  $B$ .

**Exercițiul 83.** a) „ $\Rightarrow$ ”  $f \ker \varphi g \Rightarrow \varphi(f) = \ker f = \ker g = \varphi(g)$ . Deoarece  $\ker f = \ker g$ ,  $f$  și  $g$  sunt surjectiv, din Teoremă 4.5.3 rezultă că există funcția  $\alpha : B \rightarrow B$ ,  $g = \alpha \circ f$ , care este surjectivă (deoarece  $f$  este surjectiv) și 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  $\alpha : B \rightarrow B$ ,  $g = \alpha \circ f$  este bijectiv)  $\Leftrightarrow x_1 \ker g x_2$ .

b)  $\text{Im } \varphi \subseteq \{\rho \in \mathcal{E}(A) \mid \exists \alpha : A/\rho \rightarrow B \text{ bijectiv}\}$ , deoarece  $\forall f \in \text{Hom}_s(A, B)$  avem  $\varphi(f) = \ker f \in \mathcal{E}(A)$  și

$$\alpha : A/\ker f \rightarrow B, \quad \alpha(\ker f \langle x \rangle) = f(x)$$

este funcție bijectivă.

$\{\rho \in \mathcal{E}(A) \mid \exists \alpha : A/\rho \rightarrow B \text{ bijectiv}\} \subseteq \text{Im } \varphi$ , deoarece pentru  $\rho \in \mathcal{E}(A)$  din mulțimea de mai sus, există  $f = \alpha \circ p_\rho \in \text{Hom}_s(A, B)$  astfel încât  $\ker f = \rho$ , unde  $p_\rho : A \rightarrow A/\rho$ ,  $p_\rho(x) = \rho\langle x \rangle$ .

**Exercițiul 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  $\tau\langle z \rangle = \mathbb{C}(0, |z|)$ .

**Exercițiul 85.** a)  $A/\rho_1 = \{\{1, 2\}, \{3\}, \{4\}, \{5\}\}$ ,  $\ker h = \{\{1, 2\}, \{1, 2\}\}, \{1, 2\}, \{3\}, \{3\}, \{1, 2\}, \{3\}, \{3\}, \{4\}, \{4\}, \{4\}, \{5\}, \{5\}, \{4\}, \{5\}\}$ ,  $\frac{A/\rho_1}{\ker h} = \{\{1, 2, 3\}, \{4, 5\}\}$ ,  $A/\rho_2 = \{1, 2, 3, 4, 5\}$ . între ultimele două mulțimi există o bijecție canonică.

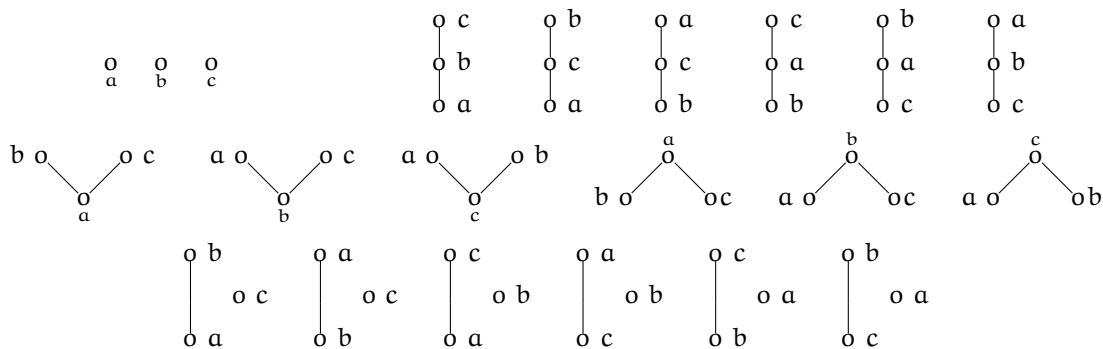
b)  $A/\rho_1 = \mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ ,  $\ker h = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{2}), (\bar{2}, \bar{2}), (\bar{1}, \bar{1}), (\bar{1}, \bar{3}), (\bar{3}, \bar{3})\}$ ,  $\frac{A/\rho_1}{\ker h} = \{\{\bar{0}, \bar{2}\}, \{\bar{1}, \bar{3}\}\}$ ,  $A/\rho_2 = \{\hat{0}, \hat{1}\}$ . între ultimele două mulțimi există o bijecție canonică.

## 5. Mulțimi ordonate

**Exercițiul 86.** b) Se vede imediat că relația  $\subset \rho$  nu e reflexivă (deoarece  $\rho$  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 relație nu este tranzitivă (căci  $(3, 2) \notin \rho \cup \sigma$ ).

**Exercițiul 88.** Relațiile de ordine pe  $A = \{a, b, c\}$  sunt cele reprezentate de următoarele diagrame Hasse (prima este relația de egalitate pe  $A$ ):



**Exercițiul 89.** a) Dacă  $f$  și  $g$  sunt crescătoare, atunci pentru orice  $a, a' \in A$  avem  $a \leq a' \Rightarrow f(a) \leq f(a') \Rightarrow g(f(a)) \leq g(f(a')) \Rightarrow g \circ f(a) \leq g \circ f(a')$ , deci  $g \circ f$  este crescător; dacă  $f$  și  $g$  sunt descrescătoare, atunci pentru orice  $a, a' \in A$  avem  $a \leq a' \Rightarrow f(a') \leq f(a) \Rightarrow g(f(a)) \leq g(f(a')) \Rightarrow (g \circ f)(a) \leq (g \circ f)(a')$ , deci  $g \circ f$  este crescător;

b) vezi punctul anterior.

**Exercițiul 90.** Fie  $b, b' \in B$  astfel încât  $b \leq b'$ . Deoarece  $f : A \rightarrow B$  este bijectiv, rezultă  $(\exists!) a, a' \in A$  astfel încât  $f(a) = b$  și  $f(a') = b'$ . Știind că  $(A, \leq)$  este total ordonată,  $\Rightarrow a \leq a'$  sau  $a' \leq a$ . Dacă presupunem că  $a' \leq a$ , deoarece  $f$  crescător, avem  $f(a') = b' \leq b = f(a)$ , de  $b \leq b' \Rightarrow b = b' \Rightarrow f^{-1}(b) = a = a' = f^{-1}(b')$ . Deci  $\forall b, b' \in B$  astfel încât  $b \leq b'$ , avem  $a = f^{-1}(b) \leq f^{-1}(b') = a'$ , adică  $f^{-1}$  este crescător;

$f := \mathbf{1}_{\mathbb{N}} : (\mathbb{N}, |) \rightarrow (\mathbb{N}, \leq)$  este o funcție evident bijectivă și crescătoare. Nu este izomorfism, deoarece  $f^{-1}$  nu e crescător. De exemplu  $2 \leq 3$ , dar  $f^{-1}(2) = 2 \nmid 3 = f^{-1}(3)$ .

**Exercițiul 93.** Fie  $a_1$  un element minimal al mulțimii ordonate  $(A, \leq)$ . Atunci pentru orice  $x \in A$  avem  $x \leq a_1 \Rightarrow x = a_1$ . Deoarece  $a = \min A \Rightarrow \forall x \in A : a \leq x \Rightarrow a \leq a_1 \Rightarrow a = a_1$ , deci într-adevăr există un singur element minimal, care este cel mai mic element.



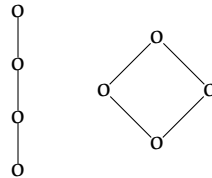
Reciproca în general nu e adevărată: considerăm relația de ordine

$$\rho \subseteq \mathbb{R} \times \mathbb{R}, \quad x\rho y \iff (x \neq 0 \neq y \wedge x \leq y) \vee x = 0 = y.$$

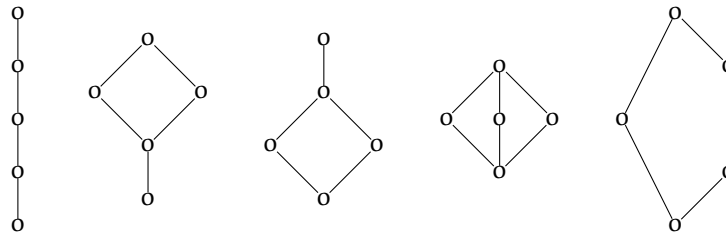
În mulțimea ordonată  $(\mathbb{R}, \rho)$ ,  $0$  este unicul element minimal (maximal), dar nu există cel mai mic (cel mai mare) element.

**Exercițiul 94.** Este suficient de observat că  $\inf_B X \in \{a \in A \mid \forall x \in X, a \leq x\}$  și  $\sup_B X \in \{a \in A \mid \forall x \in X, a \geq x\}$ .

**Exercițiul 95.** Există, abstractie făcând de izomorfisme, câte o latice cu 1, 2 respectiv 3 elemente și 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:



**Exercițiul 97.** Considerăm mulțimea  $B = \{a \in A \mid a \leq f(a)\}$ . Deoarece în orice latice completă există cel mai mare ( $\sup_A A$ ) și cel mai mic element ( $\inf_A A$ ) vedem că  $B$  este submulțime 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 și  $a \leq f(a)$  (deoarece  $a \in B$ )  $\Rightarrow a \leq f(a) \leq f(a_0) \Rightarrow f(a_0)$  este majorantă a lui  $B$ . Știm că  $a_0$  este cea mai mică majorantă a lui  $B$ , deci  $a_0 \leq f(a_0)$ , și 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 și  $a_0 \leq f(a_0) \Rightarrow f(a_0) \leq f(f(a_0))$ , 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  $a_0 \leq f(a_0)$ , și  $f(a_0) \leq a_0$ . De aici rezultă că  $a_0 = f(a_0)$ , adică  $a_0$  este într-adevăr punct fix al lui  $f$ .

**Exercițiul 98.** a) Dacă există  $a \in A$  astfel ca  $a > f(a)$ , atunci obținem un șir strict descrescător infinit  $a > f(a) > f(f(a)) > \dots$ , contradicție.

b) Fie  $A$  și  $B$  două mulțimi bine ordonate. Dacă  $f, g : A \rightarrow B$  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).

**Exercițiul 99.** a) Fie  $\rho$  un element maximal ce aparține lui  $\mathcal{O}(A)$ . Arătăm că  $\rho$  este ordine totală. Fie  $c, d \in A$  astfel încât  $c \neq d$ . Arătăm că perechea  $(c, d)$  sau  $(d, c)$  aparține graficului  $R$  al relației  $\rho$ . Presupunem că  $(c, d), (d, c) \notin R$ . Considerăm relația

$$\sigma = \rho \cup \{(c, d)\} \cup (\rho^{-1}\langle c \rangle \times \rho\langle d \rangle).$$

Vedem ușor că  $\sigma$  este o relație de ordine ce conține strict pe  $\rho$ , ceea ce contrazice maximalitatea lui  $\rho$  în mulțimea ordonată  $(\mathcal{O}(A), \subseteq)$ .

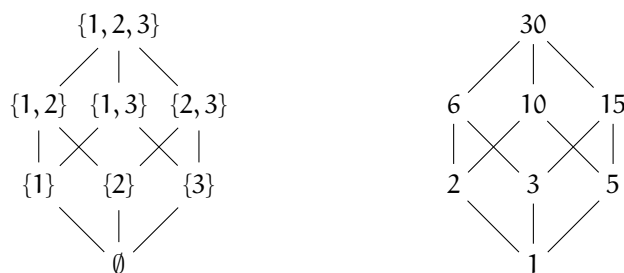
Fie  $\rho$  o relație de ordonare totală pe  $A$ . Aratăm că  $\rho$  este element maximal al lui  $\mathcal{O}(A)$ . Presupunem că  $\exists \sigma \in \mathcal{O}(A)$  astfel încât  $\rho \subset \sigma \Rightarrow \exists (c, d) \ c \neq d$  în graficul lui  $\sigma$  astfel încât  $(c, d) \notin R$  (unde  $R$  este graficul lui  $\rho$ ). Deoarece  $\rho$  este ordonare totală și  $(c, d) \notin R \Rightarrow (d, c) \in R$ , dar  $\rho \subset \sigma \Rightarrow (d, c)$  și  $(c, d)$  sunt elemente ale lui  $\sigma$ , rezultă că  $\neg d$  (din antisimetrie), contradicție cu ipoteza  $c \neq d$ .

b) Arătăm întâi că mulțimea ordonată  $(\mathcal{O}(A), \subseteq)$  satisface ipotezele lemei lui Zorn. Într-adevăr, pentru orice lanț  $\mathcal{L} = \{\rho_\alpha \in \mathcal{O}(A) \mid \alpha \in \Lambda\} \subseteq \mathcal{O}(A)$  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) rezultă că  $\bar{\rho}$  este relație de ordine totală.

## 6. Latici și algebre Boole

**Exercițiul 102.** Diagramele Hasse ale laticilor  $(\mathcal{P}(A), \subseteq)$  și  $(B, |)$  sunt:



Un izomorfism de ordine  $f : \mathcal{P}(A) \rightarrow B$  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 restricția lui  $f$  la  $\{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$  este determinată de restricția lui  $f$  la  $\{\{1\}, \{2\}, \{3\}\}$ ; deci există 6 izomorfisme între  $(\mathcal{P}(A), \subseteq)$  pe  $(B, |)$ , determinate de bijecțiile dintre  $\{\{1\}, \{2\}, \{3\}\}$  și  $\{2, 3, 5\}$ .

**Exercițiul 103.** a) pentru orice  $a, a' \in A$  avem  $a \leq a' \Rightarrow a = a \wedge a' = \inf\{a, a'\} \Rightarrow f(a) \wedge f(a') = f(a \wedge a') = f(a) \Rightarrow f(a) \leq f(a')$ , 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 relație; considerăm laticea  $(\mathcal{P}(A), \subseteq, \cup, \cap)$ ,  $(\mathcal{P}(B), \subseteq, \cup, \cap)$ . Definim funcția  $f$  astfel:  $f : \mathcal{P}(A) \rightarrow \mathcal{P}(B)$ ,  $f(X) = \rho\langle X \rangle$ . 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  $\rho$  nu este funcție injectivă, rezultă că  $\rho\langle X_1 \cap X_2 \rangle \subset \rho\langle X_1 \rangle \cap \rho\langle X_2 \rangle$ , deci  $f(X_1 \cap X_2) \neq f(X_1) \cap f(X_2) \Rightarrow f$  nu este morfism de latici.

c) Deoarece  $(A, \leq)$  este mulțime total ordonată, rezultă că pentru orice  $a, a' \in A$  avem  $a \leq a'$  sau  $a' \leq a$ . Presupunem, de exemplu, că  $a \leq a'$ . Atunci  $a \wedge a' = \inf\{a, a'\} = a$ ,  $a \vee a' = \sup\{a, a'\} = a'$ ,  $f(a) \leq f(a')$  (deoarece  $f$  este crescător),  $f(a) \wedge f(a') = f(a)$  și în fine,  $f(a) \vee f(a') = f(a')$ .

Rezultă că  $f(a) = f(a \wedge a') = f(a) \wedge f(a')$  și  $f(a') = f(a \vee a') = f(a) \vee f(a')$ . Cazul  $a' \leq a$  se tratează asemănător, și obținem că  $f$  este morfism de latici.

**Exercițiul 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

$$m \vee (n \wedge p) = [m, (n, p)] = ((m, n], [m, p]) = (m \vee n) \wedge (m \vee p),$$

rezultă a  $(\mathbb{N}, |)$  este latică distributivă.

b) Pentru orice  $a, b \in A$  avem  $a \wedge b = \inf\{a, b\} = \min\{a, b\}$  și  $a \vee b = \sup\{a, b\} = \max\{a, b\}$ . Dacă presupunem, de exemplu, că  $a, b, c \in A$  și  $a \leq b \leq c$ , atunci  $a \vee (b \wedge c) = a \vee b = b = b \wedge c = (a \vee b) \wedge (a \vee c)$ . Analog tratăm cazurile  $a \leq c \leq b$ ,  $b \leq a \leq c$ ,  $b \leq c \leq a$ ,  $c \leq a \leq b$ ,  $c \leq b \leq a$ .

**Exercițiul 107.** b)  $a \leq b \Leftrightarrow a \vee b = b \Leftrightarrow (a \vee b)' = b' \Leftrightarrow a' \wedge b' = b' \Leftrightarrow b' \leq a'$ . În acest caz, deoarece  $a \wedge b' \leq a \wedge a' = 0$  și  $a' \vee b' \geq b' \vee b = 1$ , rezultă că  $a \wedge b' = 0$  és  $a' \vee b = 1$  etc.

**Exercițiul 109.** a) Avem funcția bijectivă  $\phi : \mathcal{P}(M) \rightarrow \mathbb{Z}_2^M$ ,  $\phi(X) = \chi_X$  (unde  $\chi_X : M \rightarrow \mathbb{Z}_2$ ,  $\chi_X(a) = \hat{1} \Leftrightarrow a \in X$ ). Arătăm că  $\chi_{X \Delta Y} = \chi_X + \chi_Y$  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  $\phi : \mathcal{P}(M) \rightarrow \mathcal{P}(\mathbb{C}N)$ ,  $\phi(X) = X \cap \mathbb{C}N = X \setminus N$ . Atunci  $\phi$  este morfism surjectiv, și  $\phi(X) = \emptyset \Leftrightarrow X \subseteq N$ , deci  $\text{Ker}(\phi) = \mathcal{P}(N)$ .

**Exercițiul 110.** a) Observăm că  $(e \oplus f)^2 = e \oplus f$ .

b)  $\text{Id}(\mathbb{Z}_{24}) = \{\hat{0}, \hat{1}, \hat{9}\}$  és  $\text{Id}(\mathbb{Z}_{180}) = \{\hat{0}, \hat{1}, \hat{36}, \hat{45}, \hat{81}, \hat{100}, \hat{136}, \hat{145}\}$ .

## 7. Mulțimi de numere

**Exercițiul 115.** În Teorema recurenței 7.1.4 luăm  $X := \mathbb{N}'$ ,  $a := 0'$  și  $f := s'$  și obținem o unică funcție  $u : \mathbb{N} \rightarrow \mathbb{N}'$  care satisface (1) și (2). Vom arăta că  $u$  este bijecție, construind o inversă a lui  $u$ .

Deoarece și tripletul  $(\mathbb{N}', 0', s')$  satisface axiomele lui Peano, obținem o unică funcție  $u' : \mathbb{N}' \rightarrow \mathbb{N}$  care satisface (1) și (2). Arătăm prin inducție că  $(u' \circ u)(n) = n$  și  $(u \circ u')(n') = n'$  pentru orice  $n \in \mathbb{N}$  și  $n' \in \mathbb{N}'$ . 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  $u \circ u' = \mathbf{1}_{\mathbb{N}'}$ .

**Exercițiul 126.** a) Deoarece  $(a, b)|a$  și  $(a, b)|b$ , rezultă că  $(a, b)x|ax$  și  $(a, b)x|bx$ ; de aici obținem  $(a, b)x|(ax, bx)$ , deci  $(ax, bx) = (a, b)xy$ , unde  $y \in \mathbb{Z}$ . Mai departe

$$ax = (ax, bx)y' = (a, b)xyy',$$

adică  $\mathbf{a} = (\mathbf{a}, \mathbf{b})\mathbf{y}\mathbf{y}'$ , și

$$\mathbf{b}\mathbf{x} = (\mathbf{a}\mathbf{x}, \mathbf{b}\mathbf{x})\mathbf{y}'' = (\mathbf{a}, \mathbf{b})\mathbf{x}\mathbf{y}\mathbf{y}''$$

adică  $\mathbf{b} = (\mathbf{a}, \mathbf{b})\mathbf{y}\mathbf{y}''$ ; rezultă că  $(\mathbf{a}, \mathbf{b})\mathbf{y} \mid \mathbf{a}, \mathbf{b}$ , adică  $(\mathbf{a}, \mathbf{b})\mathbf{y} \mid (\mathbf{a}, \mathbf{b})$ . Obținem că  $\mathbf{y} \sim 1$ , adică  $(\mathbf{a}\mathbf{x}, \mathbf{b}\mathbf{x}) = (\mathbf{a}, \mathbf{b})\mathbf{x}$ .

b) În particular, dacă  $\mathbf{d} = (\mathbf{a}, \mathbf{b}) = (\mathbf{a}'\mathbf{d}, \mathbf{b}'\mathbf{d}) = \mathbf{d}(\mathbf{a}', \mathbf{b}')$ , atunci  $(\mathbf{a}', \mathbf{b}') = \mathbf{1}$ .

c) Aplicând cele de mai sus avem

$$(\mathbf{a}, \mathbf{x}) = (\mathbf{a}, \mathbf{1} \cdot \mathbf{c}) = (\mathbf{a}, (\mathbf{a}, \mathbf{b})\mathbf{c}) = (\mathbf{a}, (\mathbf{a}\mathbf{c}, \mathbf{b}\mathbf{c})) = ((\mathbf{a}, \mathbf{a}\mathbf{c}), \mathbf{b}\mathbf{c}) = (\mathbf{a}, \mathbf{b}\mathbf{c}).$$

d) Fie  $\mathbf{d} = (\mathbf{a}, \mathbf{b})$ ,  $\mathbf{x}_1 = \mathbf{d}\mathbf{a}'$ ,  $\mathbf{b} = \mathbf{d}\mathbf{b}'$  și  $\mathbf{m} = \mathbf{d}\mathbf{a}'\mathbf{b}'$ . Deoarece

$$\mathbf{m} = \mathbf{d}\mathbf{a}'\mathbf{b}' = \mathbf{a}\mathbf{b}' = \mathbf{a}'\mathbf{b},$$

rezultă că  $\mathbf{a}, \mathbf{b} \mid \mathbf{m}$ , adică  $\mathbf{m}$  este multiplu comun.

Presupunem că  $\mathbf{a}, \mathbf{b} \mid \mathbf{m}'$ ; rezultă că  $\mathbf{m}' = \mathbf{a}\mathbf{u} = \mathbf{b}\mathbf{v}$ , adică  $\mathbf{m}' = \mathbf{d}\mathbf{a}'\mathbf{u} = \mathbf{d}\mathbf{a}'\mathbf{v}$ . Atunci  $\mathbf{m}'\mathbf{b}' = \mathbf{d}\mathbf{a}'\mathbf{b}'\mathbf{u} = \mathbf{m}\mathbf{u}$  și  $\mathbf{m}'\mathbf{a}' = \mathbf{d}\mathbf{a}'\mathbf{b}'\mathbf{v} = \mathbf{m}\mathbf{v}$ , adică  $\mathbf{m} \mid \mathbf{m}'\mathbf{x}\mathbf{a}'$ ,  $\mathbf{m} \mid \mathbf{m}'\mathbf{b}'$ ; rezultă că  $\mathbf{m} \mid (\mathbf{m}'\mathbf{a}', \mathbf{m}'\mathbf{b}')$ , dar  $(\mathbf{m}'\mathbf{a}', \mathbf{m}'\mathbf{b}') = \mathbf{m}'(\mathbf{a}', \mathbf{b}') = \mathbf{m}'$ , deci  $\mathbf{m} \mid \mathbf{m}'$ .

Am arătat că  $\mathbf{m} = [\mathbf{a}, \mathbf{b}]$  și  $\mathbf{a}\mathbf{b} = \mathbf{d}\mathbf{d}\mathbf{a}'\mathbf{b}' = \mathbf{d}\mathbf{m} = (\mathbf{a}, \mathbf{b})[\mathbf{a}, \mathbf{b}]$ .

**Exercițiul 127.** a) Fie  $\mathbf{d} = (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3)$  și  $\mathbf{d}' = ((\mathbf{x}_1, \mathbf{x}_2), \mathbf{x}_3)$ . Atunci  $\mathbf{d} \mid \mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3 \iff \mathbf{d} \mid \mathbf{x}_1\mathbf{x}_2$  și  $\mathbf{d} \mid \mathbf{x}_3 \iff \mathbf{d} \mid (\mathbf{x}_1, \mathbf{x}_2)$  și  $\mathbf{d} \mid \mathbf{x}_3 \iff \mathbf{d} \mid ((\mathbf{x}_1, \mathbf{x}_2), \mathbf{x}_3)$ , adică  $\mathbf{d} \mid \mathbf{d}'$ . Invers rezultă că  $\mathbf{d}' \mid (\mathbf{x}_1, \mathbf{x}_2)$  și  $\mathbf{d}' \mid \mathbf{x}_3 \iff \mathbf{d}' \mid \mathbf{x}_1, \mathbf{d}' \mid \mathbf{x}_2$  și  $\mathbf{d}' \mid \mathbf{x}_3 \implies \mathbf{d}' \mid (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3)$ , adică  $\mathbf{d}' \mid \mathbf{d}$ . Pentru cazul general folosim inducție după  $n$ .

**Exercițiul 135.** Fie  $\mathbf{a} - \mathbf{b} = \mathbf{k}\mathbf{n}$ , unde  $\mathbf{k} \in \mathbb{Z}$ . Deoarece  $(\mathbf{a}, \mathbf{n}) \mid \mathbf{a}$  și  $(\mathbf{a}, \mathbf{n}) \mid \mathbf{m}$ , rezultă că  $(\mathbf{a}, \mathbf{m}) \mid \mathbf{b}$ . Deci  $(\mathbf{a}, \mathbf{m})$  este comun divizor al lui  $\mathbf{b}$  și  $\mathbf{m}$ , de unde  $(\mathbf{a}, \mathbf{m}) \mid (\mathbf{b}, \mathbf{m})$ . Asemănător obținem  $(\mathbf{b}, \mathbf{m}) \mid (\mathbf{a}, \mathbf{m})$ , deci  $(\mathbf{a}, \mathbf{m}) = (\mathbf{b}, \mathbf{m})$ .

## 8. Algebre universale

**Exercițiul 150.** O operație  $n$ -ară pe  $A$  este o funcție  $\omega : A^n \rightarrow A$ , deci numărul căutat este  $|A^{(A^n)}| = \mathbf{m}^{(\mathbf{m}^n)}$ .

**Exercițiul 152.** a) Fie  $\omega \in \Omega$ ,  $\tau(\omega) = n$ . Dacă  $(\mathbf{a}_1, \mathbf{b}_1), \dots, (\mathbf{a}_n, \mathbf{b}_n) \in F$ , atunci  $\mathbf{b}_1 = f(\mathbf{a}_1), \dots, \mathbf{b}_n = f(\mathbf{a}_n)$  și

$$\begin{aligned} \omega((\mathbf{a}_1, \mathbf{b}_1), \dots, (\mathbf{a}_n, \mathbf{b}_n)) &= (\omega(\mathbf{a}_1, \dots, \mathbf{a}_n), \omega(\mathbf{b}_1, \dots, \mathbf{b}_n)) \\ &= (\omega(\mathbf{a}_1, \dots, \mathbf{a}_n), \omega(f(\mathbf{a}_1), \dots, f(\mathbf{a}_n))) \\ &= (\omega(\mathbf{a}_1, \dots, \mathbf{a}_n), f(\omega(\mathbf{a}_1, \dots, \mathbf{a}_n))) \in F. \end{aligned}$$

Invers, dacă  $\mathbf{a}_1, \dots, \mathbf{a}_n \in A$ , atunci  $(\mathbf{a}_1, f(\mathbf{a}_1)), \dots, (\mathbf{a}_n, f(\mathbf{a}_n)) \in F$ , și

$$(\omega(\mathbf{a}_1, \dots, \mathbf{a}_n), \omega(f(\mathbf{a}_1), \dots, f(\mathbf{a}_n))) = \omega((\mathbf{a}_1, f(\mathbf{a}_1)), \dots, (\mathbf{a}_n, f(\mathbf{a}_n))) \in F,$$

deci  $f(\omega(\mathbf{a}_1, \dots, \mathbf{a}_n)) = \omega(f(\mathbf{a}_1), \dots, f(\mathbf{a}_n))$ .

b) Fie  $\omega \in \Omega$ ,  $\tau(\omega) = n$  și  $(\mathbf{a}_1, \mathbf{c}_1), \dots, (\mathbf{a}_n, \mathbf{c}_n) \in S \circ R$ ; rezultă că există  $\mathbf{b}_1, \dots, \mathbf{b}_n \in B$  astfel încât  $(\mathbf{a}_1, \mathbf{b}_1), \dots, (\mathbf{a}_n, \mathbf{b}_n) \in R$  și  $(\mathbf{b}_1, \mathbf{c}_1), \dots, (\mathbf{b}_n, \mathbf{c}_n) \in S$ . Deoarece  $R$  și  $S$  sunt subalgebre, obținem că

$$(\omega(\mathbf{a}_1, \dots, \mathbf{a}_n), \omega(\mathbf{b}_1, \dots, \mathbf{b}_n)) = \omega((\mathbf{a}_1, \mathbf{b}_1), \dots, (\mathbf{a}_n, \mathbf{b}_n)) \in R$$

și

$$(\omega(\mathbf{b}_1, \dots, \mathbf{b}_n), \omega(\mathbf{c}_1, \dots, \mathbf{c}_n)) = (\omega(\mathbf{b}_1, \mathbf{c}_1), \dots, (\mathbf{b}_n, \mathbf{c}_n)) \in S,$$

deci

$$\omega((\mathbf{a}_1, \mathbf{c}_1), \dots, (\mathbf{a}_n, \mathbf{c}_n)) = (\omega(\mathbf{a}_1, \dots, \mathbf{a}_n), \omega(\mathbf{c}_1, \dots, \mathbf{c}_n)) \in S \circ R.$$

Dacă  $(\mathbf{b}_1, \mathbf{a}_1), \dots, (\mathbf{b}_n, \mathbf{a}_n) \in R^{-1}$ , atunci  $(\mathbf{a}_1, \mathbf{b}_1), \dots, (\mathbf{a}_n, \mathbf{b}_n) \in R$  și

$$(\omega(\mathbf{a}_1, \dots, \mathbf{a}_n), \omega(\mathbf{b}_1, \dots, \mathbf{b}_n)) = \omega((\mathbf{a}_1, \mathbf{b}_1), \dots, (\mathbf{a}_n, \mathbf{b}_n)) \in R,$$

deci  $\omega((\mathbf{b}_1, \mathbf{a}_1), \dots, (\mathbf{b}_n, \mathbf{a}_n)) = (\omega(\mathbf{b}_1, \dots, \mathbf{b}_n), \omega(\mathbf{a}_1, \dots, \mathbf{a}_n)) \in R^{-1}$ .

c) Fie  $\omega \in \Omega$ ,  $\tau(\omega) = n$ ,  $\mathbf{y}_1, \dots, \mathbf{y}_n \in \rho(X)$ . Există  $\mathbf{x}_1, \dots, \mathbf{x}_n \in X$  astfel încât  $(\mathbf{x}_1, \mathbf{y}_1), \dots, (\mathbf{x}_n, \mathbf{y}_n) \in R$ , deci  $(\omega(\mathbf{x}_1, \dots, \mathbf{x}_n), \omega(\mathbf{y}_1, \dots, \mathbf{y}_n)) = \omega((\mathbf{x}_1, \mathbf{y}_1), \dots, (\mathbf{x}_n, \mathbf{y}_n)) \in R$ . Deoarece  $X$  este subalgebră, rezultă că  $\omega(\mathbf{x}_1, \dots, \mathbf{x}_n) \in X$  și  $\omega(\mathbf{y}_1, \dots, \mathbf{y}_n) \in \rho(X)$ .

**Exercițiul 153.** a) Fie  $X = \{A\}$  și aplicăm teorema de caracterizare a subalgebrei subalgebrei generate:  $X_0 = X$ ,  $X_1 = \{A, \mathcal{C}_M A\}$ ,  $X_2 = \{A, \mathcal{C}_M A, M, \emptyset\}$ ,  $X_3 = X_4 = \dots$ , deci  $\langle X \rangle = \bigcup_{k=1}^{\infty} X_k = \{A, \mathcal{C}_M A, M, \emptyset\}$ .

b)  $\langle \{\rho\} \rangle = \{\rho^n \mid n \in \mathbb{N}^*\}$ ; dacă  $\rho$  este tranzitiv, atunci  $\langle \{\rho\} \rangle = \{\rho\}$ .

**Exercițiul 155.** a) Dacă  $X_0 = X$  și  $Y_0 = f(X)$ , atunci

$$X_{k+1} = X_k \cup \{\omega(x_1, \dots, x_{\tau(\omega)}) \mid \omega \in \Omega \text{ și } x_i \in X_k; i = 1, \dots, \tau(\omega)\}$$

și  $Y_{k+1}$  este definit analog, atunci  $\langle X \rangle = \bigcup_{k=0}^{\infty} X_k$ ,  $\langle f(X) \rangle = \bigcup_{k=0}^{\infty} Y_k$ . Prin inducție se arată că  $f(X_k) = Y_k$ ,  $k \geq 0$ .

**Exercițiul 156.** a) Fie  $\tau$  tipul algebrei  $(A, \Omega)$ ,  $\omega \in \Omega$ ,  $n = \tau(\omega)$  și  $a_i \in N(A)$ ,  $i = 1, \dots, n$ . 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 inducție obținem că  $\langle X \rangle = A$ , deci  $\omega(a_1, \dots, a_n) \in N(A)$ , și  $N(A)$  este subalgebra.

b) Fie  $a \in N(A)$  și  $f : A \rightarrow A$  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  $\langle f^{-1}(X) \rangle = A$  și  $A = f(A) = \langle X \rangle$ . Deci  $f(a) \in N(A)$ , adică  $f(N(A)) \subseteq N(A)$ .

c) Fie  $\{M_i \mid i \in I\}$  mulțimea subalgebrelor maximale și  $\Phi(A) = \bigcap_{i \in I} M_i$ . Atunci  $a \notin \Phi(A) \implies \exists i_0 \in I$ ,  $a \notin M_{i_0} \implies \langle M_{i_0} \cup \{a\} \rangle = A$  și  $\langle M_{i_0} \rangle = M_{i_0} \neq A \implies a \notin N(A)$ , deci  $N(A) \subseteq \Phi(A)$ .

Dacă  $a \notin N(A)$ , atunci  $\exists X \subseteq A$  astfel încât  $\langle X \cup \{a\} \rangle = A$  și  $\langle X \rangle = A$ . Fie

$$\mathcal{S} = \{B \leq (A, \Omega) \mid X \subseteq B, a \notin B\}.$$

Evident,  $\langle X \rangle \in \mathcal{S}$ , deci  $\mathcal{S} \neq \emptyset$ . Mulțimea  $(\mathcal{S}, \subseteq)$  ordonată satisface condițiile lemei lui Zorn 5.4.2, deci există un element maximal  $M' \in (\mathcal{S}, \subseteq)$ ; vedem ușor că  $M'$  este subalgebră maximală a lui  $(A, \Omega)$ . Deoarece  $M' \in \mathcal{S}$ , rezultă că  $a \notin M'$ , deci  $a \notin \Phi(A)$ . Am arătat că  $a \notin N(A) \implies a \notin \Phi(A)$ , adică  $\Phi(A) \subseteq N(A)$ .

**Exercițiul 158.** a) Fie  $\omega \in \Omega$ ,  $\tau(\omega) = n$ . Presupunem că  $\rho$  este congruență și 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  $\omega(a_1, \dots, a_n) \rho (b_1, \dots, b_n)$ , și

$$\omega((a_1, b_1), \dots, (a_n, b_n)) = (\omega(a_1, \dots, a_n), \omega(b_1, \dots, b_n)) \in R.$$

Invers, dacă  $\rho$  este relație omomorfă și  $a_1 \rho b_1, \dots, a_n \rho b_n$ , atunci  $(a_i, b_i) \in R$ ,  $(\omega(a_1, \dots, a_n), \omega(b_1, \dots, b_n)) = \omega((a_1, b_1), \dots, (a_n, b_n)) \in R$ , și  $\omega(a_1, \dots, a_n) \rho \omega(b_1, \dots, b_n)$ .

b) Arătăm întâi că intersecția relațiilor de congruență este congruență și apoi aplicăm teorema 5.2.5 de caracterizare a laticilor complete.

c) Fie  $\sigma = \bigcup_{n \in \mathbb{N}, \rho_1, \dots, \rho_n \in \mathcal{C}} \rho_1 \circ \dots \circ \rho_n$ . Arătăm că  $\sigma \in \mathcal{E}(A)$ ,  $\forall \rho \in \mathcal{C} \rho \subseteq \sigma$ , și dacă  $\sigma' \in \mathcal{E}(A)$  astfel încât  $\forall \rho \in \mathcal{C} \rho \subseteq \sigma'$ , atunci  $\sigma \subseteq \sigma'$ .

d) Arătăm că dacă  $\mathcal{C} \subseteq \mathcal{C}(A, \Omega)$ , atunci  $\sigma := \bigcup_{n \in \mathbb{N}, \rho_1, \dots, \rho_n \in \mathcal{C}} \rho_1 \circ \dots \circ \rho_n$  este congruență.

e) Implicația „ $\implies$ ” este cunoscută. Implicația inversă rezultă din a) și din Exercițiul 152. b).

f) Deoarece  $\rho_1 \subseteq \rho_1 \circ \rho_2$ ,  $\rho_1 \subseteq \rho_3$ ,  $\rho_2 \cap \rho_3 \subseteq \rho_1 \circ \rho_3$  și  $\rho_2 \cap \rho_3 \subseteq \rho_3$ , rezultă că  $\rho_1 \subseteq \rho_3 \implies \rho_1 \circ (\rho_2 \cap \rho_3) \subseteq (\rho_1 \circ \rho_2) \cap \rho_3$ .

Dacă  $x(\rho_1 \circ \rho_2) \cap \rho_3 y$ , atunci  $x \rho_3 y$  și  $\exists z \in A$  astfel încât  $x \rho_2 z$  și  $z \rho_1 y$ ; rezultă că  $z \rho_3 y$ , mai departe  $x \rho_3 z$ , deci  $x(\rho_2 \cap \rho_3) z$  și în final,  $x \rho_1 \circ (\rho_2 \cap \rho_3) y$ .

## 9. Numere cardinale

**Exercițiul 159.** a), b) Fie  $\alpha_i = |A_i|$ ,  $\beta_i = |B_i|$ ,  $i \in I$ . Dacă  $f_i : A_i \rightarrow B_i$  este injectiv  $\forall i \in I$ , atunci  $\prod_{i \in I} f_i : \prod_{i \in I} A_i \rightarrow \prod_{i \in I} B_i$  și  $\prod_{i \in I} f_i : \prod_{i \in I} A_i \rightarrow \prod_{i \in I} B_i$  sunt injective.

c) Fie  $\alpha = |A|$ ,  $A \neq \emptyset$ ,  $\alpha' = |A'|$ ,  $\beta = |B|$  și  $\beta' = |B'|$ . Există  $f : A' \rightarrow A$  surjectiv și  $g : B \rightarrow B'$  injectiv; atunci și  $\text{Hom}(f, g) : \text{Hom}(A, B) \rightarrow \text{Hom}(A', B')$  este injectiv, deci  $\beta^\alpha \leq \beta'^{\alpha'}$ .

**Exercițiul 160.** (i) $\implies$ (ii) Dacă  $f$  injectiv,  $A \sim f(A)$ ; deoarece  $A$  este finită și  $f(A) \subseteq A$ , rezultă că  $f(A) = A$ , deci  $f$  este surjectiv.

(i) $\implies$ (iii) Dacă  $f$  este surjectiv, există  $s : A \rightarrow A$  astfel încât  $f \circ s = \mathbf{1}_A$ ;  $s$  este injectiv, deci bijectiv, deci și  $f = s^{-1}$  este bijectiv.

(ii) $\implies$ (i) Presupunem că  $A$  este infinit, și arătăm că există  $f : A \rightarrow A$  injectiv, nesurjectiv. Fie  $\phi : \mathbb{N} \rightarrow A$  o funcție injectivă, și notăm  $\phi(n) = a_n \in A$ ,  $n \in \mathbb{N}$ . Atunci  $f : A \rightarrow A$ ,  $f(a) = a$  dacă  $a \notin \phi(\mathbb{N})$  și  $f(a) = a_{n+1}$  dacă  $a = a_n \in \phi(\mathbb{N})$  este funcția căutată.

(iii) $\implies$ (i) Presupunem că  $A$  este mulțime infinită, și fie  $g : A \rightarrow A$ ,  $g(a) = a$  dacă  $a \notin \phi(\mathbb{N})$ ,  $g(a_n) = a_{n-1}$  dacă  $n \geq 1$ , și  $g(a_0) = a_0$ , unde  $\phi$  este funcția injectivă de mai sus. Atunci  $g$  este surjectiv și nu este injectiv, căci  $g(a_1) = g(a_0) = a_0$ .

Observăm că  $f \circ g = \mathbf{1}_A$  și  $g \circ f \neq \mathbf{1}_A$ .

**Exercițiul 161.** Dacă  $A$  este infinit, există o funcție injectivă  $\phi: \mathbb{N} \rightarrow A$ ,  $n \mapsto a_n$ .

a) Fie  $B = \{b_0, \dots, b_{n-1}\}$ ,  $A \cap B = \emptyset$ . Atunci  $f: A \cup B \rightarrow A$ ,  $f(a) = a$  dacă  $a \notin \phi(\mathbb{N})$ ,  $f(a_k) = a_{k+n}$ ,  $f(b_k) = a_k$  este funcție bijectivă.

b) Fie  $C = \{c_k \mid k \in \mathbb{N}\} \sim \mathbb{N}$ ,  $A \cap C = \emptyset$ , și  $g: A \cup C \rightarrow A$ ,  $g(a) = a$  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  $2\mathbb{N} \sim 2\mathbb{N}+1 \sim \mathbb{N}$ ,  $2\mathbb{N} \cap (2\mathbb{N}+1) = \emptyset$  și  $2\mathbb{N} \cup (2\mathbb{N}+1) = \mathbb{N}$ , deci  $\aleph_0 + \aleph_0 = \aleph_0$ .

Funcția  $f: \mathbb{N}^* \times \mathbb{N}^* \rightarrow \mathbb{N}^*$ ,  $f(m, n) = 2^{n-1}(2n-1)$  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  $f: \bigcup_{n \in I} A_n \rightarrow \mathbb{N} \times \mathbb{N}$ .  $\forall x \in \bigcup_{n \in I} A_n$  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  $\phi: \mathcal{P}_k(\mathbb{N}) \rightarrow \mathbb{N}^k$  astfel: dacă  $X = \{a_1, \dots, a_k\}$ ,  $a_1 < \dots < a_k$ , atunci  $\phi_k(X) = (a_1, \dots, a_k) \in \mathbb{N}^k$ . Vedem că  $\phi_k$  este injectiv, deci  $|\mathcal{P}_k(\mathbb{N})| \leq |\mathbb{N}^k| = \aleph_0$ ; 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  $f: \mathbb{Q}_+^* \rightarrow \mathbb{N} \times \mathbb{N}$ ,  $f(\frac{m}{n}) = (m, n)$  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)  $f: (0, 1) \rightarrow (a, b)$ ,  $f(x) = (b-a)x + a$  și  $g: (-\frac{\pi}{2}, \frac{\pi}{2}) \rightarrow \mathbb{R}$ ,  $g(x) = \tan x$  sunt funcții bijective. Echivalențele  $(a, b) \sim [a, b] \sim [a, b] \sim (a, b)$  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  $\mathbb{R} \setminus \mathbb{Q} \not\sim \mathbb{N}$ .

**Exercițiul 164.** a)  $c^2 = (2^{\aleph_0})^2 = 2^{2\aleph_0} = 2^{\aleph_0} = c$ ;  $c^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = c$ .

b)  $c \leq c + c = 2c \leq c^2 = c$ ;  $c \leq c \cdot \aleph_0 \leq c^2 = c$ ;  $c = 2^{\aleph_0} \leq \aleph_0^{\aleph_0} \leq c^{\aleph_0} = c$ .

**Exercițiul 166.** a) Dacă  $A = \{a_1\}$ , atunci  $|\text{Hom}(A, B)| = n$ . Aplicăm inducția matematică, observând că:  $|\text{Hom}(\{a_1, \dots, a_k, a_{k+1}\}, B)| = |\text{Hom}(\{a_1, \dots, a_k\}, B)| \cdot n = n^{k+1}$ .

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  $f: A \rightarrow B$  este injectiv, atunci  $f$  este și bijectiv, deci numărul funcțiilor bijective este  $n!$ .

d) Fie  $A = \{a_1, \dots, a_k\}$ ,  $a_1 < \dots < a_k$  și  $B = \{b_1, \dots, b_n\}$ . Între mulțimea submulțimilor cu  $k$  elemente ale lui  $B$  și mulțimea  $\{f: A \rightarrow B \mid f \text{ strict crescător}\}$  există o funcție bijectivă  $\phi$  definită astfel: dacă  $B' \subseteq B$ ,  $B' = \{b_{i_1}, \dots, b_{i_k}\}$ , atunci fie  $\phi(B) = (f: A \rightarrow B)$ ,  $f(a_{i_j}) = b_{i_j}$ ; 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  $\mathbb{N}_n^* = \{1, 2, \dots, n\}$ ,  $\mathcal{F} = \{f: \mathbb{N}_n^* \rightarrow \mathbb{N}_{n+k-1}^* \mid f \text{ strict crescător}\}$  și  $\bar{\mathcal{F}} = \{f: \mathbb{N}_n^* \rightarrow \mathbb{N}_n^* \mid f \text{ crescător}\}$ ; atunci  $|\mathcal{F}| = C_{n+k-1}^k$  și  $|\bar{\mathcal{F}}| = C_n^k$ . Fie  $\phi: \bar{\mathcal{F}} \rightarrow \mathcal{F}$ ,  $\phi(f)(i) = f(i) + (i-1)$  și  $\psi: \mathcal{F} \rightarrow \bar{\mathcal{F}}$ ,  $\psi(f) = f(i) - (i-1)$ , unde  $i \in \mathbb{N}_n^*$ . Vedem ușor că  $\phi$  și  $\psi$  sunt funcții bine definite,  $\psi \circ \phi = \mathbf{1}_{\bar{\mathcal{F}}}$  și  $\phi \circ \psi = \mathbf{1}_{\mathcal{F}}$ .

**Exercițiul 168.** a) Dacă  $n = n_1 + n_2 + \dots + n_k$  este o partiție a lui  $n$ , atunci fie  $s_i = n_1 + \dots + n_i \in \{1, \dots, n-1\}$ . 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  $C_{n-1}^{k-1}$ .

b) Dacă  $n = n_1 + n_2 + \dots + n_k$  este o partiție a numărului natural  $n$ , fie  $s_i = n_1 + \dots + n_i \in \{0, \dots, n\}$ . 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  $\bar{C}_{n+1}^{k-1}$ .

**Exercițiul 169.** a) Dacă  $f: A \rightarrow B$  este injectiv și  $r: B \rightarrow A$  este o inversă la stânga a lui  $f$ , atunci  $r(b) = f^{-1}(b)$  dacă  $b \in \text{Im } f$  și  $r(b) \in A$ , dacă  $b \notin \text{Im } f$ ; rezultă că numărul inverselor la stânga ale lui  $f$  este  $|\text{Hom}(B \setminus \text{Im } f, A)| = k^{n-k}$ .

b) Presupunem că  $B = \{b_1, \dots, b_n\}$  și  $|f^{-1}(b_i)| = k_i$ . Dacă  $s: B \rightarrow A$  este o inversă la dreapta a lui  $f$ , atunci avem  $k_i$  posibilități de alegere pentru  $s(b_i)$ , deci  $f$  are  $k_1 \cdots k_n$  inverse la dreapta.

**Exercițiul 170.** a) Fie  $A_i = \{a \in \mathbb{N} \mid 1 \leq a \leq m, p_i | a\}$ ,  $1 \leq i \leq n$ . Atunci  $|A_i| = \frac{m}{p_i}$  și  $\phi(m) = m \setminus |\bigcup_{i=1}^n A_i|$ ; mai departe

$$|A_{i_1} \cap \dots \cap A_{i_k}| = \{a \in \mathbb{N} \mid 1 \leq a \leq m, p_{i_1} \cdots p_{i_k} | a\} = \frac{m}{p_{i_1} \cdots p_{i_k}},$$

deci

$$\begin{aligned} \phi(m) &= m \left( 1 - \sum_{i=1}^n \frac{1}{p_i} + \sum_{1 \leq i_1 < i_2 \leq n} \frac{1}{p_{i_1} p_{i_2}} - \dots + (-1)^n \frac{1}{p_{i_1} \cdots p_{i_n}} \right) = \\ &= m \left( 1 - \frac{1}{p_1} \right) \cdots \left( 1 - \frac{1}{p_n} \right). \end{aligned}$$

b) Fie  $A_i = \{\sigma \in S_n \mid \sigma(i) = i\}$ , și că observăm că  $|A_{i_1} \cap \dots \cap A_{i_k}| = |\{\sigma \in S_n \mid \sigma(i_j) = i_j, 1 \leq j \leq k\}| = (n-k)!$ ; rezultă că numărul căutat este

$$\begin{aligned} n! - \left| \bigcup_{i=1}^n A_i \right| &= n! - C_n^1(n-1)! + C_n^2(n-2)! + \dots + (-1)^n C_n^n(n-n)! = \\ &= n! \left( 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!} \right). \end{aligned}$$

**Exercițiul 171.** Pentru  $1 \leq i \leq n$  fie  $A_i = \{f: A \rightarrow B \mid b_i \notin \text{Im } f\} \sim \text{Hom}(A, B \setminus \{b_i\})$ , deci  $|A_i| = (n-1)^k$ . Vedem că  $\bigcup_{i=1}^n A_i$  este mulțimea funcțiilor nesurjective; rezultă că numărul funcțiilor surjective este  $n^k - |\bigcup_{i=1}^n A_i|$ . Deoarece  $|A_{i_1} \cap \dots \cap A_{i_l}| = (n-l)^k$ , afirmația rezultă din principiul includerii și al excluderii.

**Exercițiul 173.** a) Fie  $|B| = n$  și  $\phi: \text{Hom}_{sz}(A, B) \rightarrow \mathcal{E}_n(A)$ ,  $\phi(f) = \ker f$ . Dacă  $\rho \in \mathcal{E}_n(A)$ , atunci există o funcție bijectivă  $g: A/\rho \rightarrow B$ , și dacă  $g = g \circ p_\rho$ , atunci  $\phi(f) = \ker f = \rho$ , deci  $\phi$  este surjectiv; dacă  $f, f': A \rightarrow B$  sunt două funcții surjective, atunci  $\ker f = \ker f' \Leftrightarrow$  există  $g: B \rightarrow B$  astfel încât  $f' = g \circ f$ , deci  $|(\ker \phi)(f)| = n!$ ; de aici rezultă că  $S(k, n) = |\mathcal{E}_n(A)| = \frac{s(k, n)}{n!}$ .

b) Numărul partițiilor este egal cu numărul relațiilor de echivalență.

**Exercițiul 175.** În prima clasă alegem  $k_1$  elemente din  $k$  elemente – numărul posibilităților este  $C_k^{k_1} = \binom{k}{k_1}$ ; în a doua clasă alegem  $k_2$  elemente din  $k - k_1$  elemente – numărul posibilităților este  $\binom{k-k_1}{k_2}$ . Continuând, în clasa  $r$  alegem  $k_r$  elemente din  $k - (k_1 + \dots + k_{r-1})$  elemente, deci numărul posibilităților este  $\binom{k - (k_1 + \dots + k_{r-1})}{k_r}$ . La al  $n$ -lea pas numărul posibilităților este 1; rezultă că numărul partițiilor este  $\frac{k!}{k_1!(k-k_1)!} \dots \binom{k - (k_1 + \dots + k_{n-1})}{k_n} = \frac{k!}{k_1! \dots k_n!}$ .

## 10. Numere ordinale

**Exercițiul 179.** a) Deoarece  $A_a \neq A_{a'}$ , rezultă că  $a \neq a'$ , și deoarece  $A$  total ordonată, rezultă că  $a < a'$  sau  $a' < a$ .

Presupunem că există o asemănare  $f: A_a \rightarrow A_{a'}$ . Dacă  $a' < a$ , atunci  $a' \in A_a$ , deci  $f(a') < a'$ ; dacă  $a < a'$ , atunci  $a \in A_{a'}$  și  $f^{-1}(a) < a$ . În ambele cazuri avem contradicție (vezi demonstrația teoremei 10.1.4).

b) Presupunem că  $f \neq g$ , deci există  $a \in A$  astfel încât  $f(a) \neq g(a)$ ; rezultă că

$$A_0 = \{x \in A \mid f(x) \neq g(x)\}$$

este mulțime nevidă, și fie  $a_0 = \min A_0$ . Mai departe, fie  $b = f(a_0)$  și  $b' = g(a_0)$ ; rezultă că  $A_{a_0} \simeq B_b$  și  $A_{a_0} \simeq B_{b'}$ , deci  $B_b \simeq B_{b'}$ , contradicție.

# 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 mulțimilor și aritmetică*. Ed. Fundației 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 mulțimilor și logică matematică*. Ed. Tehnică, București, 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] Mărcuș, A., Szántó Cs., Tóth L.: *Logika és halmazelmélet*. Scientia, Cluj-Napoca, 2005.
- [19] Năstăsescu, C.: *Introducere în teoria mulțimilor*. Ed. Didactică și Pedagogică, București, 1981.
- [20] Purdea, I., Pic, Gh.: *Tratat de algebră modernă I*. Ed. Academiei, București, 1977.
- [21] Purdea, I.: *Culegere de probleme de algebră. Relații, funcții și algebre universale*. Litografia Univ. Babeș-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/Set_theory)
- <http://en.wikipedia.org/wiki/Logic>
- [http://en.wikipedia.org/wiki/Foundations\\_of\\_mathematics](http://en.wikipedia.org/wiki/Foundations_of_mathematics)
- [http://en.wikipedia.org/wiki/Philosophy\\_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_mathematics)
- [http://en.wikipedia.org/wiki/History\\_of\\_logic](http://en.wikipedia.org/wiki/History_of_logic)

# Glosar

- alef, 92
  - transfinit, 92
- algoritmul lui Euclid, 63
- analiza cazurilor, 11
- aranjamente, 84
- aranjamente cu repetiție, 84
- asemănare, 44
- axioma lui Arhimede, 59
- axiomele lui Peano, 57
  
- clasă, 24
- clasă de echivalență, 37
- codomeniu, 29
- combinări, 84
- concluzie, 10
- condiția inductivității, 47
- condiția lanțurilor descrescătoare, 47
- condiția minimalității, 47
- conjunție, 6
  - elementară, 9
- consecință, 10
- continuum, 83
- contrapozitie, 11
- corp ordonat, 71
- criterii de divizibilitate, 66
- cuantificator, 14, 17
  
- diagramă comutativă, 30
- diagrame Hasse, 43
- disjuncție, 6
  - elementară, 9
- domeniu de definiție, 29
  
- echivalență, 6
- element maximal, 45
- element minimal, 45
  
- familie de elemente, 30
- familie de mulțimi, 30
- FNC, 9
- FND, 9
- formă normală
  - conjunctivă, 9
  - disjunctivă, 9
- formulă
  - atomică, 5
  - contradicție, 7
  - limbaj de ordinul întâi, 15
  - propozițională, 5
  - satisfiabilă, 7
  - tautologie, 7
- formulele lui de Morgan, 8
- funcția caracteristică, 36
  
- funcția lui Euler, 66
- funcție Boole, 55
- funcție de adevăr, 6
- funcție selectivă, 48
  
- grafic, 29
  
- imagine, 40
- implicație, 6
- infimum, 45
- ipoteza continuului, 93
  
- legea contrapozitiei, 8
- legea dublei negații, 8
- lema lui Zorn, 48
  
- maximum, 45
- metoda
  - formelor normale, 9
- metoda diagonală a lui Cantor, 82
- minimum, 45
- modus ponendo tollens, 11
- modus ponens, 10
- modus tollendo ponens, 11
- modus tollens, 11
- mulțime, 22
  - vidă, 22
- mulțime factor, 37
- mulțime selectivă, 48
- mulțime total ordonată, 43
- mulțimea părților, 22
- mulțimi artiniene, 47
  
- negație, 6
- nucleu, 40
- număr ordinal
  - de speța I, 88
- număr prim
  - Fermat, 65
  - Mersenne, 65
  
- paradox, 48
- partiție, 38
- permutare, 84
- premisă, 10
- prezintă, 10
- principiul dualității, 55
- problema deciziei, 8
- proiecția canonică, 33, 39
- propoziții
  - contrare, 94
  - contradictorii, 94
  - subalterne, 94



- subcontrare, 94
- reductio ad absurdum, 11
- relație
  - antisimetrică, 37
  - binară, 26
  - diagonală, 26
  - omogenă, 26
  - omomorfă, 75
  - reflexivă, 36
  - simetrică, 37
  - tranzitivă, 36
- retractă
  - a unei funcții injective, 31
- reuniunea disjunctă, 34
- secțiune
  - a unei funcții surjective, 32
  - a unei relații după o submulțime, 27
- silogism disjunctiv, 11
- silogism ipotetic, 11
- simbol
  - limbaj de ordinul întâi, 14
  - logica propozițiilor, 5
- sir Cauchy, 71
- sistem de numerație, 62
- subalgebra Frattini, 76
- subalgebra generată, 75
- subformulă, 5
- submulțime, 22
- substituție, 5
- supremum, 45
- tautologie, 17
- teorema
  - de compactitate, 20
  - Euler, 66
  - Fermat, 66
  - Frege-Lukasiewicz, 13
  - Gödel, 20
  - Herbrand, 13
- teorema de incompletitudine a lui Gödel, 60
- teorema lui Zermelo, 48
- teorema recurenței, 58
- variabilă, 15
  - legată, 15
  - liberă, 15