

Aurelian Claudiu VOLF

Logică și teoria mulțimilor

Partea a II-a

Universitatea „Al. I. Cuza” Iași

2016

Cuprins

Cuprins	2
Către cititor	3
I. Logică, mulțimi, axiome	4
I.1. Limbaj formal, logică	6
I.2. Axiomele teoriei mulțimilor	11
Exerciții.....	15
I.3. Clase, relații, funcții	15
Exerciții.....	24
I.4. Ordinale, axioma infinității și mulțimea numerelor naturale.....	25
I.5. Comentarii și completări privind axiomatica mulțimilor	35
I.6. Cardinali	38
Exerciții.....	39
II. Mulțimi factor și construcții de structuri numerice fundamentale	41
II.1. Relații de echivalență și mulțimi factor.....	41
II.2. Inelul numerelor întregi.....	43
II.3. Corpul numerelor raționale	45
Exerciții.....	47
II.4. Corpul numerelor reale.....	47
Exerciții.....	55
Index	57
Bibliografie	60

Către cititor

Parcurgerea unui text matematic este un proces *activ* prin excelență. În primul rând, toate definițiile nou introduse trebuie să capete rapid un suport intuitiv și să fie legate de noțiunile deja cunoscute prin căutarea de exemple (și contraexemple) de obiecte care să satisfacă definițiile. În plus, cititorul trebuie să *verifice* pe cazuri concrete și să *demonstreze* afirmațiile din text. În particular, toate aparițiile unor fraze de tipul „se verifică ușor că ...”, „evident, ...”, ... sînt o invitație la demonstrarea efectivă a afirmațiilor respective. Aceste exerciții intelectuale sînt un pas indispensabil spre asimilarea conceptelor și tehnicilor introduse și, totodată, o verificare a înțelegerii de către cititor a textului.

Paragrafele care au o bară la stînga sînt foarte importante pentru înțelegerea textului.

Paragrafele care au o linie ondulantă la dreapta pot fi omise și sînt destinate unui cititor avizat sau interesat de aspecte mai profunde ale teoriei.

Peste tot, în text:

- $|A|$ desemnează cardinalul mulțimii A (numărul elementelor lui A , dacă A este finită).
- $x := y$ înseamnă „ x este egal prin definiție cu y ” (unde y este deja definit) sau „notăm pe y cu x ”.
- \square marchează sfîrșitul sau absența unei demonstrații. Adesea, aceasta înseamnă că cititorul este invitat să facă el însuși demonstrația.

I. Logică, mulțimi, axiome

Studiul logicii matematice și al teoriei mulțimilor pornește de la premisa că un profesor de matematică nu se poate limita la punctul de vedere al unui manual de liceu, fiind necesară o viziune mai profundă asupra acestor tematici.

Mulțimile apar ca obiecte matematice foarte devreme în învățământul modern, sub o formă intuitivă (în varianta teoriei naive a mulțimilor). Este exclusă o tratare axiomatică a teoriei mulțimilor la nivel preuniversitar; totuși, un profesor de matematică trebuie să fie familiarizat cu conceptele de bază și să înțeleagă utilitatea, necesitatea și mecanismele teoriei axiomatică a mulțimilor.

De ce este important studiul teoriei mulțimilor? *Orice enunț matematic se poate reformula în termeni de mulțimi.* Așadar, dacă teoria mulțimilor este bine fundamentată, se obține o fundamentare a întregii matematici.

Teoria modernă a mulțimilor începe odată cu lucrarea „Teoria rațională a infinității” a lui Georg Cantor¹, în care se manevrează liber *mulțimile infinite* și se dezvoltă o tehnică de măsurare a lor (teoria cardinalelor). Pînă la Cantor, matematicienii adoptau punctul de vedere al filozofilor Greciei antice: există noțiunea de *infinit actual* (o infinitate de obiecte concepute ca existînd simultan) și cea de *infinit potențial* (o mulțime sau o mărime finită, dar care se poate mări oricît de mult). Filozoful Zenon, prin faimoasele sale aporii (paradoxuri) a atras atenția asupra consecințelor absurde care par să apară introducînd infinitul actual în raționamente. Se considera de aceea că infinitul actual nu este accesibil intuiției și doar infinitul potențial poate fi folosit în gîndirea matematică.

Cantor are meritul de a fi spart această barieră mentală și de a fi încercat să „numere infinitul”. El a avut ideea de a compara mulțimile (finite sau nu) cu ajutorul *funcțiilor bijective*: *două mulțimi sînt „la fel de mari” (echipotente) dacă există o bijecție între ele.* Cantor a obținut rezultate precum: \mathbb{N} este echipotent cu \mathbb{Q} și cu mulțimea numerelor algebrice (numerele complexe care sînt rădăcini ale unui polinom nenul cu coeficienți raționali). Deja aceste afirmații nu sînt în acord cu percepția obișnuită și arată că uneori „partea este la fel de mare ca și întregul”. A mai arătat că \mathbb{N} nu este echipotent cu \mathbb{R} ; în general, o mulțime A nu

¹ Georg Ferdinand Ludwig Philipp Cantor (1845-1918), matematician german.

este echipotentă cu mulțimea părților sale $\mathcal{P}(A)$. Există, deci, mai multe tipuri de infinitate. Alte rezultate contrazic și mai mult simțul comun: există tot atâtea puncte pe un segment câte sînt pe o dreaptă sau în întregul plan sau în întregul spațiu!

În cadrul teoriei lui Cantor a mulțimilor (astăzi numită „naivă”), prin *mulțime* se înțelege o colecție (un ansamblu, un set) de obiecte distincte (*elementele* mulțimii) bine determinată și considerată ca o entitate. Georg Cantor spunea „*Unter eine Menge verstehen wir jede Zusammenfassung M von bestimmten Wohlunterschiedenen Objekten m unseres Denkens zu einem Ganzen*”: „Prin *mulțime* înțelegem orice grupare într-un tot M a unor obiecte distincte și bine determinate m ale gândirii noastre”. Apare aici (deși nu e enunțată explicit) ideea că o „*proprietate*” determină o mulțime: *mulțimea obiectelor care satisfac proprietatea respectivă*.

Teoria mulțimilor în forma descrisă de Cantor conducea însă la *paradoxuri*, care provin din „definiția” foarte permisivă și vagă a conceptului de mulțime. Însuși Cantor în 1895 observă că nu se poate vorbi de „mulțimea tuturor ordinalelor” (paradox publicat de Burali-Forti în 1897); mai târziu, s-a constatat că există și alte „mulțimi contradictorii”: „mulțimea tuturor cardinalilor”, „mulțimea tuturor mulțimilor”, „mulțimea mulțimilor care nu se conțin ca element” (paradoxul lui Russel²). Prezentăm acest paradox: presupunem că există mulțimea mulțimilor care nu se conțin ca element și o notăm cu C (în notație modernă, $C = \{A \mid A \notin A\}$). Evident, are loc: sau $C \in C$, sau $C \notin C$. Dacă $C \in C$, atunci $C \notin C$ din definiția lui C , contradicție. Dacă $C \notin C$, atunci C nu satisface condiția de definiție a lui C , deci $C \in C$, contradicție.

Aceste paradoxuri au putut fi eliminate de *teoria axiomatică a mulțimilor*, care stabilește *reguli clare de construcție de mulțimi*. Printre altele, nu se permite considerarea mulțimilor „foarte mari”, care apar mai sus. O primă axiomatizare a fost dată de Zermelo³ în 1908. Una din axiomele sale (care evită apariția paradoxurilor de tipul de mai sus) este *Axioma selecției*, care în esență spune că, fiind date o „proprietate”⁴ P și o mulțime A , există „mulțimea elementelor *din* A care satisfac proprietatea P ”. Cu alte cuvinte, o proprietate nu determină o mulțime (ca în viziunea lui Cantor), ci, *dată o mulțime A* , se poate vorbi doar de existența *submulțimii* formată de elementele lui A care satisfac P .

În 1905 matematicianul francez Jules Richard construiește un paradox de alt tip (simplificat ulterior de Berry și publicat de Russel în 1906). Să considerăm următorul concept: „cel mai mic număr natural care nu poate fi definit cu mai puțin de 17 cuvinte”. Dacă acest număr ar exista, atunci el *poate fi definit cu 16 cuvinte*, chiar de enunțul anterior (care

² Bertrand Russel (1872-1970), matematician și filozof britanic.

³ Ernst Friedrich Ferdinand Zermelo (1871-1953), matematician german.

⁴ Mai precis, este vorba de un predicat cu o variabilă.

are 16 cuvinte, numărați). Contradicția obținută arată că nu există un astfel de număr. Pe de altă parte, mulțimea numerelor naturale care pot fi definite cu cel mult 16 cuvinte este finită (căci mulțimea frazelor cu cel mult 16 cuvinte care definesc un număr natural este finită) și deci *există* numere naturale care nu pot fi definite cu mai puțin de 17 cuvinte. Cel mai mic dintre acestea este un număr... care nu poate exista, conform celor de mai sus!

Paradoxul de mai sus are altă sursă, și anume *ambiguitatea limbajului* natural, obișnuit. Ce înseamnă exact *a defini* un număr natural?

Din cele spuse reiese că, pe lângă o axiomatizare a teoriei mulțimilor, trebuie *restrîns limbajul natural* la câteva modalități bine precizate și simple de exprimare. În același timp, posibilitățile trebuie să fie suficient de permissive pentru a putea formula orice enunț matematic. Aceste scopuri sînt realizate de un *limbaj formalizat*.

Vom prezenta intuitiv un astfel de limbaj (o prezentare riguroasă depășește cu mult cadrul și scopul acestei cărți). Cu această ocazie, vom sublinia anumite aspecte de logică matematică. În continuare vom descrie axiomele teoriei mulțimilor, aplicații (ordinale și numere naturale). Vom încerca să reliefăm și modul în care aceste axiome trebuie conștientizate în procesul didactic.

I.1. Limbaj formal, logică

În teoria axiomatică a mulțimilor⁵ *toate obiectele sînt mulțimi*. Altfel spus, *nu se face distincție între conceptele „element” și „mulțime”*. Acest punct de vedere este firesc, dacă ne gândim că o mulțime poate fi element al altei mulțimi; în plus, o teorie axiomatică trebuie să pornească de la un minim de noțiuni primare, iar distincția între element și mulțime ar complica lucrurile inutil.

Pentru a putea enunța axiomele teoriei mulțimilor, avem nevoie de prezentarea (intuitivă) a limbajului formal al acestei teorii. Subliniem că nu este vorba de o formalizare propriu-zisă. Un limbaj formal prezentat riguros ar ocupa zeci de pagini (un exemplu de formalizare, în cadrul axiomatizării von Neumann-Gödel-Bernays a teoriei mulțimilor, poate fi găsit în REGHIȘ [1981]). Mai întâi descriem *sintaxa limbajului* (regulile după care putem forma expresii corecte ale limbajului formal).

⁵ Axiomatizarea Zermelo-Fraenkel-Skolem, acceptată în aproape toată matematica modernă.

1.1 Definiție. Un *enunț* al limbajului formal (numit și *expresie* a limbajului formal) este un șir finit de *simboluri*, format după anumite reguli descrise mai jos. Intuitiv, un enunț exprimă un fapt bine determinat despre obiectele la care se referă (în cazul nostru, toate obiectele sînt mulțimi).

Descriem acum tipurile de simboluri și construcția expresiilor limbajului formal :

i) Există simboluri de tip nume, care denumesc *mulțimi* (acestea sînt singurele obiecte pe care le considerăm!). Numele sînt de două feluri: un *nume constant* (pe scurt, *o constantă*) se referă la un obiect bine precizat, iar un *nume variabil* (pe scurt, *o variabilă*) notează un obiect generic (arbitrar, neprecizat). Se presupune că avem la dispoziție o colecție suficient de mare de nume constante și variabile. Exemple de nume: $x, y, a, b, c, A, B, \dots$

ii) Simbolurile care notează relații:

- relația de *egalitate*, notată cu simbolul $=$,
- relația de *apartenență*, notată cu simbolul \in .

Dacă x, y sînt nume (constante sau variabile), atunci următoarele șiruri de simboluri sînt *expresii* ale limbajului formal:

$x = y$ (citit „ x este egal cu y ”);

$x \in y$ (citit „ x aparține lui y ” sau „ x este element al lui y ”).

iii) Parantezele rotunde (" $"$ și $"$ ") au rolul de a elimina ambiguitățile.

iv) Conectorii logici se folosesc pentru a exprima proprietăți mai complexe, pentru a combina mai multe expresii într-una nouă. Conectorii sînt: \wedge (conjuncția, „și”), \vee (disjuncția, „sau”), \neg (negația, „non”). Dacă E, F sînt expresii (deja construite), atunci sînt expresii și următoarele șiruri de simboluri:

$(E) \wedge (F)$ (citită „ E și F ”);

$(E) \vee (F)$ (citită „ E sau F ”);

$\neg(E)$ (citită „non E ”).

v) Cuantificatorii logici sînt: \forall (cuantificatorul universal, „oricare”), \exists (cuantificatorul existențial, „există”). Cu ajutorul cuantificatorilor (numiți uneori și *cuantori*) se precizează dacă, într-o expresie, o variabilă se referă la *toate obiectele* sau la *măcar un obiect*. Dacă E este o expresie a limbajului și x este o variabilă, atunci:

$(\forall x)(E)$ este expresie (citită „pentru orice x are loc E ” sau „pentru orice x, E este adevărată”);

$(\exists x)(E)$ este expresie (citită „există x astfel încît are loc E ” sau „există x astfel încît E este adevărată”).

vi) Pentru un plus de claritate, pe lîngă parantezele rotunde, se pot folosi și parantezele pătrate $[]$ sau acoladele $\{ \}$, după regulile uzuale.

Singurele expresii (enunțuri) admise ale limbajului formal sînt cele construite respectînd regulile de mai sus. În unele cazuri, se poate renunța la paranteze dacă nu este pericol de confuzie; astfel, se poate scrie de exemplu $x \in y \wedge a = b$ în loc de $(x \in y) \wedge (a = b)$ etc.

Variabilele unei expresii pot fi *libere* sau *legate*.

Spunem că *variabila x este liberă în expresia E* dacă x apare în E , dar E nu conține nici o cuantificare a lui x (adică nici $\forall x$, nici $\exists x$ nu apar în E).

Spunem că *variabila x este legată în E* dacă E conține un subșir de simboluri de forma $(\forall x)F$ sau $(\exists x)F$ (unde F este o expresie).

O expresie care nu conține variabile libere se numește *propoziție*.

Dacă expresia E conține variabilele *libere* x_1, \dots, x_n , vom sublinia uneori acest lucru scriind $E(x_1, \dots, x_n)$. Fiind date constantele c_1, \dots, c_n , prin înlocuirea peste tot în E a variabilei x_1 cu c_1 , a lui x_2 cu c_2 , ..., a lui x_n cu c_n se obține o nouă expresie (demonstrați!), notată cu $E(c_1, \dots, c_n)$. Dacă x_1, \dots, x_n sînt *toate* variabilele libere din E , atunci $E(c_1, \dots, c_n)$ este o *propoziție* (adică o expresie care nu are variabile libere). O expresie care are variabile libere se mai numește *predicat*.

Vom reveni asupra problemei variabilelor libere sau legate, care are o mare importanță în modul de scriere a enunțurilor matematice.

1.2 Exemple. Presupunem că x, y, z sînt variabile și a, b sînt constante. Arătați că următoarele șiruri de simboluri sînt expresii: $x \in y$; $(\forall x)(x \in y)$; $(a \in b) \wedge (x = y)$; $\neg((a \in b) \wedge (x = y))$; $(\forall z)(\exists y)(x \in y)$. Care sînt variabilele libere din fiecare? Șirurile de simboluri: $x(\forall y)$; $x = \in$; $\forall y$ nu sînt expresii corecte ale limbajului formal (de ce?).

Să trecem acum la **interpretarea sensului expresiilor (semantica limbajului)**. Reamintim că o expresie care nu conține variabile libere se numește *propoziție*. Oricărei *propoziții* îi asociem o unică *valoare de adevăr*. Valorile de adevăr sînt: 0 (sau *fals*), și 1 (sau *adevărat*). O propoziție cu valoarea de adevăr 0 se numește *propoziție falsă*; o propoziție cu valoarea de adevăr 1 se numește *propoziție adevărată*. O propoziție nu poate fi simultan falsă și adevărată.

Descriem acum *regulile prin care se determină valoarea de adevăr a unei propoziții date*. (Subliniem că doar *propozițiile* au valori de adevăr. Unei expresii cu variabile libere nu i se dă nici o valoare de adevăr.)

Fie a, b constante și x, y variabile.

- i) Propozițiile de forma $a = b$ sînt adevărate exact atunci cînd a și b denumesc același obiect (aceeași mulțime).
- ii) Valoarea de adevăr a propozițiilor de forma $a \in b$ nu poate fi precizată acum; acest lucru este descris de axiome (în paragraful următor). Evident, intuitiv, $a \in b$ este adevărată dacă și numai dacă mulțimea numită a este un element al mulțimii numită de b .
- iii) O propoziție de forma $(E) \wedge (F)$ (unde E și F sînt propoziții) este adevărată dacă și numai dacă E și F sînt *ambele* adevărate.

- iv) O propoziție de forma $(E) \vee (F)$ este adevărată dacă și numai dacă *măcar una* din propozițiile E și F este adevărată (adică sau E , sau F , sau atât E cât și F sînt adevărate).
- v) O propoziție de forma $\neg(E)$ este adevărată dacă și numai dacă propoziția E este *falsă*.
- vi) O propoziție de forma $(\forall x)(E(x))$ (unde variabila x este liberă în E) este adevărată dacă și numai dacă pentru *orice* obiect c propoziția $E(c)$ este adevărată.
- vii) O propoziție de forma $(\exists x)(E(x))$ (unde variabila x este liberă în E) este adevărată dacă și numai dacă *există măcar un obiect* c astfel încît propoziția $E(c)$ să fie adevărată.

1.3 Observație. Valoarea de adevăr a propozițiilor de tipul $E \wedge F$, $E \vee F$, $\neg E$ se poate defini prin *tabele de adevăr*. Iată tabelul de adevăr pentru $E \vee F$, construit după regula iv):

E	F	$E \vee F$
1	1	1
1	0	1
0	1	1
0	0	0

S-au scris pe linii toate combinațiile posibile de valori de adevăr pentru E și F . Tabelul se citește pe linii: de exemplu, linia 3 a tabelului spune, că, dacă E are valoarea de adevăr 0, iar F are valoarea de adevăr 1, atunci $E \vee F$ are valoarea de adevăr 1.

1.4 Definiție. a) Două propoziții E și F se numesc *echivalente* dacă au aceeași valoare de adevăr. Scriem aceasta sub forma $E \equiv F$.

b) Definiția se poate extinde la expresii oarecare. Două expresii E și F ce conțin aceleași constante și aceleași variabile (fie x_1, \dots, x_n variabilele din E și F) sînt numite *echivalente* dacă: orice variabilă care este liberă în E este liberă în F (și reciproc) și *propozițiile* $(\forall x_1)(\forall x_2)\dots(\forall x_n)E(x_1, \dots, x_n)$ și $(\forall x_1)(\forall x_2)\dots(\forall x_n)F(x_1, \dots, x_n)$ au aceeași valoare de adevăr. Scriem atunci $E \equiv F$, sau $E(x_1, \dots, x_n) \equiv F(x_1, \dots, x_n)$ dacă vrem să evidențiem variabilele libere.

1.5 Exercițiu. Dacă E , F și G sînt expresii, avem echivalențele :

$$\begin{aligned} \neg(E \wedge F) &\equiv (\neg E) \vee (\neg F); & \neg(E \vee F) &\equiv (\neg E) \wedge (\neg F); & & \text{(legile lui DeMorgan)} \\ (E \wedge F) \vee G &\equiv (E \vee G) \wedge (F \vee G); & & & & \text{(distributivitatea lui } \vee \text{ față de } \wedge) \\ (E \vee F) \wedge G &\equiv (E \wedge G) \vee (F \wedge G); & & & & \text{(distributivitatea lui } \wedge \text{ față de } \vee) \\ \neg((\forall x)E) &\equiv (\exists x)(\neg E); & \neg((\exists x)E) &\equiv (\forall x)(\neg E) & & \text{(legile de negare a cuantificatorilor).} \end{aligned}$$

De exemplu, $\neg(E \wedge F) \equiv (\neg E) \vee (\neg F)$ se poate demonstra cu următorul tabel de adevăr:

E	F	$E \wedge F$	$\neg(E \wedge F)$	$\neg E$	$\neg F$	$(\neg E) \vee (\neg F)$
1	1	1	0	0	0	0
1	0	0	1	0	1	1
0	1	0	1	1	0	1
0	0	0	1	1	1	1

Identitatea coloanelor $\neg(E \wedge F)$ și $(\neg E) \vee (\neg F)$ demonstrează echivalența cerută.

Legile lui DeMorgan arată că am fi putut reduce setul de conectori logici și cuantificatori, de exemplu la \forall, \neg, \wedge .

Introducem următoarele *prescurtări* uzuale. Fie E, F expresii. Atunci scriem:

$E \rightarrow F$ în loc de $(\neg E) \vee F$ și citim „ E implică F ” sau „dacă E , atunci F ”; \rightarrow se numește operatorul *implicație*.

$E \leftrightarrow F$ în loc de $(E \rightarrow F) \wedge (F \rightarrow E)$ și citim „ E este echivalent cu F ”.

1.6 Exercițiu. Scrieți tabelele de adevăr pentru operatorii \rightarrow și \leftrightarrow . Demonstrați că, dacă E și F sînt propoziții, $E \leftrightarrow F$ este adevărată dacă și numai dacă E și F au aceeași valoare de adevăr.

Insistăm asupra *implicației*, \rightarrow . Se justifică intuitiv că $E \rightarrow F$ este același lucru cu $(\neg E) \vee F$, astfel: " $E \rightarrow F$ " înseamnă "dacă E este adevărată, atunci F este adevărată". Altfel spus, sau E este falsă (adică are loc $\neg E$), sau E este adevărată și atunci automat F este adevărată (adică are loc F); pe scurt, $(\neg E) \vee F$. Este important de conștientizat această echivalență logică, utilă mai ales cînd trebuie negată o implicație (lucru care intervine frecvent, de exemplu în cazul demonstrațiilor prin reducere la absurd). Astfel, faptul că $E \rightarrow F$ este falsă înseamnă că are loc $(E \rightarrow F) \equiv \neg(\neg E) \vee F \equiv E \wedge (\neg F)$ (ipoteza este adevărată și totuși concluzia este falsă). Această interpretare este conformă cu intuiția („bunul-simț”). De altfel, concluziile bazate pe un calcul logic formal trebuie totdeauna interpretate intuitiv, proces absolut necesar în înțelegerea unor demonstrații (sau în găsirea unor soluții la o problemă dată).

Vom mai folosi și alte prescurtări, larg utilizate, de exemplu $x \neq y$ pentru $\neg(x = y)$ sau $x \notin y$ în loc de $\neg(x \in y)$.

Dacă propoziția $E \rightarrow F$ este adevărată, scriem atunci $E \Rightarrow F$. Analog, scrierea $E \Leftrightarrow F$ înseamnă că propoziția $E \leftrightarrow F$ este adevărată.

1.7 Observație. Orice teoremă matematică (propoziție, lemă etc.) poate fi scrisă în limbaj formal. Expresia obținută trebuie să fie din punct de vedere logic o *propoziție* (*nu trebuie să aibă variabile libere*). De exemplu, teorema împărțirii cu rest în \mathbb{N} se poate scrie formal:

$$(\forall a)(\forall b)[(a \in \mathbb{N} \wedge b \in \mathbb{N} \wedge b \neq 0) \Rightarrow (\exists q)(\exists r)(q \in \mathbb{N} \wedge r \in \mathbb{N} \wedge a = bq + r \wedge r < b)].$$

1.8 Observație. Se folosește foarte des în matematică simbolul $\exists!$ (citit *există și este unic*). Fie $P(x)$ predicat cu o variabilă. Expresia $(\exists!x)P(x)$ înseamnă că *există și este unic un x cu proprietatea $P(x)$* . Din punct de vedere formal, definiția este următoarea:

$(\exists!x)P(x)$ este o prescurtare pentru $((\exists x)P(x)) \wedge ((\forall y)(\forall z)((P(y) \wedge P(z)) \rightarrow y = z))$.

Proprietatea $(\forall y)(\forall z)((P(y) \wedge P(z)) \rightarrow y = z)$ se mai exprimă "există *cel mult* un x astfel încât $P(x)$ să fie adevărată".

În definiția formală, s-a exprimat faptul că x este unic punând condiția ca, de îndată ce y și z satisfac P , să rezulte că $y = z$. Aceasta este și o metodă de demonstrare a unicității în diverse situații.

De exemplu, $(\exists!x \in \mathbb{R})(x > 0 \wedge x^2 = 2)$ exprimă faptul că există un unic număr real pozitiv al cărui pătrat este 2. Aceasta este chiar definiția lui $\sqrt{2}$.

I.2. Axiomele teoriei mulțimilor

Prezentăm câteva elemente din teoria axiomatică Zermelo-Fraenkel-Skolem (ZFS) a mulțimilor. Pentru o tratare mai detaliată, incluzând multe teme interesante (ordinali, cardinali, axioma alegerii etc.), vezi SCORPAN [1996].

Nu putem *defini* un obiect fără a face referire la alte obiecte, presupuse cunoscute. Aceste obiecte "cunoscute" trebuie la rândul lor definite... Se vede că acest proces nu poate continua la infinit.

Trebuie să considerăm în cele din urmă *noțiuni care nu se definesc (noțiuni primare)*; cu ajutorul lor vom putea defini alte obiecte. Aceasta este un principiu de bază în orice teorie axiomatică.

În axiomatizarea teoriei mulțimilor, noțiunile de *mulțime* și de *relație de apartenență* se consideră *noțiuni primare* (nu se definesc) și *toate obiectele teoriei sînt mulțimi* (în particular, **toate elementele unei mulțimi sînt tot mulțimi!**). Aceste noțiuni satisfac un set de *axiome* (care, într-un anumit sens, *definesc* obiectele respective). Altfel spus, nu ne interesează *ce sînt* mulțimile, ci *cum se comportă* unele față de altele și față de relația de apartenență. Axiomele stabilesc regulile care se aplică obiectelor numite mulțimi și relației de apartenență.

Axiomele sînt *propoziții* (din limbajul formal construit anterior) care sînt *declarate și acceptate ca adevărate*. Orice altă afirmație despre mulțimi trebuie *demonstrată* pornind de la axiome. În acest mod se deduc toate proprietățile „uzuale” ale teoriei mulțimilor.

Deși, după cum am spus, în teoria axiomatică *elementele unei mulțimi sînt tot mulțimi*, vom adopta (pe cît posibil), pentru a nu crea confuzii cititorului, distincția tradițională în notație: în general, se notează *mulțimile cu majuscule* (A, B, \dots), iar *elementele mulțimilor cu minuscule*

(a, b, \dots). Dacă A este o mulțime și a este un element al lui A , atunci scriem $a \in A$ (citit „ a aparține lui A ” sau „ A conține pe a ”). Se mai poate scrie $A \ni a$). Dacă a nu este element al mulțimii A , scriem $a \notin A$.

2.1 Axioma extensibilității: Pentru orice două mulțimi A și B , avem :

$$[(\forall a) (a \in A \leftrightarrow a \in B)] \rightarrow A = B.$$

Mai riguros spus, propoziția următoare este adevărată:

$$(\forall A) (\forall B) \{[(\forall a) (a \in A \leftrightarrow a \in B)] \rightarrow A = B\}.$$

Această axiomă nu spune decât că o mulțime este determinată de elementele sale.⁶ O exprimare mai simplă, dar nu foarte precisă, este: *dacă două mulțimi au aceleași elemente, atunci mulțimile coincid.*

Observăm că are loc și implicația inversă: dacă $A = B$, atunci orice element care aparține lui A aparține și lui B . Acest fapt este evident: A și B denumesc același obiect, deci orice enunț referitor la A este adevărat și pentru B (și reciproc).

Dacă A și B sînt două mulțimi, vom scrie $A \subseteq B$ (și citim A inclus în B sau A este submulțime a lui B) dacă orice element al lui A aparține și lui B : $(\forall a) [(a \in A) \rightarrow (a \in B)]$. În caz contrar, notăm $A \not\subseteq B$.

Cu această notație, avem: $(\forall A) (\forall B) [(A = B) \leftrightarrow (A \subseteq B \wedge B \subseteq A)]$.

Pe această proprietate se bazează majoritatea demonstrațiilor de egalitate de mulțimi: pentru a demonstra că $A = B$, arătăm că orice element al lui A aparține și lui B (adică $A \subseteq B$) și reciproc ($B \subseteq A$).

Axiomele care urmează sînt toate de următorul tip: *fiind date una sau mai multe mulțimi, se garantează existența unei noi mulțimi cu anumite proprietăți* (construită cu ajutorul mulțimilor inițiale). Cu alte cuvinte, *axiomele descriu construcții permise în cadrul teoriei*. Se regăsește astfel motivul pentru care a fost construită teoria: evitarea paradoxurilor generate de construcții de mulțimi „prea mari”.

2.2 Axioma mulțimii părților unei mulțimi. $(\forall M) (\exists P) ((\forall a)(a \in P \leftrightarrow a \subseteq M))$.

În cuvinte: *fiind dată o mulțime M , există o mulțime P astfel încît elementele lui P sînt exact submulțimile lui M .*

Mulțimea P a cărei existență este garantată mai sus este unic determinată de mulțimea M . Într-adevăr, dacă și Q satisface condiția $(\forall A) (A \in Q \leftrightarrow A \subseteq M)$, atunci avem, pentru orice mulțime A : $A \in Q \leftrightarrow A \subseteq M \leftrightarrow A \in P$. Din axioma extensibilității obținem că $P = Q$.

Notația tradițională pentru P este $\mathcal{P}(M)$ (mulțimea părților lui M).

⁶ De aici provine și denumirea de "axioma extensibilității": două mulțimi sînt egale dacă au aceleași "întindere", "extensiune".

2.3 Axioma reuniunii. Pentru orice mulțime A (subînțeles: avînd ca elemente tot mulțimi), există o mulțime ale cărei elemente sînt elementele mulțimilor din A , adică:

$$(\forall A)(\exists U)(\forall x)[(x \in U) \leftrightarrow (\exists a)(a \in A \wedge x \in a)].$$

Pentru înțelegerea acestei axiome, este util să privim A ca pe o familie de mulțimi. Axioma de mai sus nu face decît să postuleze existența reuniunii acestei familii de mulțimi.

Mulțimea U – a cărei existență este garantată de axiomă – este unic determinată de A (demonstrați!) și se notează $\bigcup A$ sau $\bigcup_{x \in A} x$ sau $\bigcup \{x \mid x \in A\}$. A se remarca în acest context futilitatea distincției dintre element și mulțime.

2.4 Schema de axiome de substituție

Nu este vorba de o simplă axiomă, ci de o schemă de axiome. Mai precis, pentru orice expresie (de un anumit tip) a limbajului formal se obține o axiomă. Așadar, avem de a face cu o infinitate de axiome.

Pentru enunț, avem nevoie de o definiție. O expresie $E(x, y)$ cu exact două variabile libere x și y se numește *relație funcțională* dacă pentru orice x există cel mult un y astfel încît $E(x, y)$ să fie adevărată:

$$(\forall x)(\forall y)(\forall z)((E(x, y) \wedge E(x, z)) \rightarrow y = z).$$

Intuitiv, putem privi o relație funcțională ca pe o „funcție parțial definită”: pentru anumiți x există un unic y astfel încît $E(x, y)$ să aibă loc; se notează uneori chiar „funcțional”, $y = \tilde{E}(x)$ în loc de $E(x, y)$. Observăm că nu este neapărat adevărat că $(\forall x)(\exists y)E(x, y)$.

În termeni mai puțin formali, axioma-schemă a substituției afirmă că: *Pentru orice relație funcțională $E(x, y)$ și pentru orice mulțime a , există „imaginea prin E a mulțimii a ”.*

Evident, trebuie să definim formal conceptul de „imagine a unei mulțimi printr-o relație funcțională”. Spunem că mulțimea b este *imaginea mulțimii a prin relația funcțională $E(x, y)$* dacă „elementele lui b sînt de forma $\tilde{E}(x)$, cu $x \in a$ ”, adică:

$$(\forall y)[y \in b \leftrightarrow ((\exists x)(x \in a \wedge E(x, y)))].$$

Axioma-schemă a substituției este: *pentru orice relație funcțională $E(x, y)$, are loc:*

$$(\forall a)(\exists b)(\forall y)[y \in b \leftrightarrow ((\exists x)(x \in a \wedge E(x, y)))].$$

Subliniem din nou că se obține cîte o axiomă pentru fiecare alegere a unei relații funcționale E . Nu se pot condensa toate aceste enunțuri într-unul singur, de tipul

$$(\forall E \text{ relație funcțională})(\forall a)(\exists b)(\forall y)[y \in b \leftrightarrow ((\exists x)(x \in a \wedge E(x, y)))],$$

deoarece acesta nu este o expresie a limbajului formal: E nu denumește un obiect legitim (o mulțime), ci o expresie.

Folosind axioma extensionalității, se demonstrează imediat că *imaginea unei mulțimi printr-o relație funcțională este unic determinată* (mulțimea b a cărei existență este postulată de axioma schemă a substituției este unic determinată de E și a).

2.5 Consecință (Schema de comprehensiune, Axioma selecției). Pentru orice mulțime A și pentru orice expresie cu o variabilă liberă $P(x)$, există submulțimea elementelor din A pentru care P este adevărată. Formal, $(\forall A)(\exists B)(\forall x)[x \in B \leftrightarrow (x \in A \wedge P(x))]$.⁷

Demonstrație. Fie expresia $E(x,y) : "(x = y) \wedge P(y)"$. Afirmăm că E este o relație funcțională. Într-adevăr, fie x, y, z cu $E(x,y)$ și $E(x,z)$ adevărate. Atunci $x = y$ și $x = z$, deci $y = z$.

Conform axiomei substituției, pentru mulțimea A există o mulțime B astfel încât:

$$(\forall y)[y \in B \leftrightarrow (\exists x)(x \in A \wedge E(x, y))],$$

adică $y \in B \leftrightarrow (\exists x)(x \in A \wedge (x = y) \wedge P(y))$, ceea ce revine la a spune că

$$y \in B \leftrightarrow (y \in A \wedge P(y)),$$

ceea ce trebuia demonstrat. □

Iarăși, axioma extensionalității asigură că A și $P(x)$ determină *unic* mulțimea B din enunț. Această mulțime se notează tradițional:

$$\{x \in A \mid P(x)\} \text{ (citit „mulțimea elementelor din } A \text{ care satisfac } P\text{”).}$$

2.6 Observație. S-a eliminat paradoxul lui Russel: nu mai este permisă construirea mulțimii (și scrieri de tipul)

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

Există însă, pentru A mulțime dată, $\{x \in A \mid P(x)\}$.

2.7 Observație. Dacă se presupune că există măcar o mulțime⁸ A , rezultatul de mai sus asigură existența unei (unice) mulțimi ce nu conține nici un element, numită *mulțimea vidă* și notată cu \emptyset .⁹ Într-adevăr, fie $P(x) : "x \neq x"$. Din schema de comprehensiune, există $\emptyset := \{x \in A \mid x \neq x\}$. Pentru orice x , avem $x \notin \emptyset$ (dacă $x \in \emptyset$, atunci $x \neq x$, absurd). Unicitatea lui \emptyset este o consecință a axiomei extensionalității. Notăm deci:

$$\emptyset := \{x \in A \mid x \neq x\}.$$

Pentru orice mulțime M are loc $\emptyset \subseteq M$. Este instructiv să prezentăm în detaliu acest argument. Conform definiției, avem $\emptyset \subseteq M$ dacă și numai dacă $\forall x (x \in \emptyset \rightarrow x \in M)$. Dar expresia $x \in \emptyset \rightarrow x \in M$ este, conform definiției, o prescurtare pentru $\neg(x \in \emptyset) \vee (x \in M)$, care este adevărată, căci $\neg(x \in \emptyset)$ este adevărată.

Termenul de *comprehensiune* descrie modalitatea de a *preciza o mulțime prin enunțarea unei proprietăți pe care o au doar elementele mulțimii și numai ele*. S-a văzut că acest concept, care a stat la baza teoriei naive a mulțimilor, duce la paradoxuri; schema de

⁷ În axiomatizarea lui Zermelo din 1908, acest rezultat era enunțat ca axiomă și era numit *Axioma selecției*.

⁸ Axioma infinității, enunțată mai jos, asigură faptul că există o mulțime.

⁹ Nu este litera grecească majusculă ϕ , Φ , ci un simbol matematic derivat dintr-o literă norvegiană, \emptyset .

comprehensiune restrânge această modalitate doar la posibilitatea următoare: pentru orice mulțime dată M și orice „proprietate” P , există *submulțimea* elementelor lui M care satisfac P .

2.8 Observație. Putem acum defini și alte „operații cu mulțimi”. Astfel, pentru orice două mulțimi A și B , arătați că există mulțimile:

$$\{x \in A \mid x \in B\} \text{ (notată } A \cap B \text{ și numită } \textit{intersecția} \text{ lui } A \text{ și } B)$$

$$\{x \in A \mid x \notin B\} \text{ (notată } A \setminus B \text{ și numită } \textit{diferența} \text{ lui } A \text{ și } B).$$

Demonstrați că $A \cap B = B \cap A$.

Exerciții

1. Ce este o mulțime? Ce sînt axiomele? De ce sînt necesare axiomele și limbajul formal?
2. Scrieți măcar 5 expresii în limbaj formal folosind doar variabilele x și y .
3. Demonstrați că mulțimile a căror existență este garantată de axiome sînt unic determinate.
4. Folosind axiomele și existența mulțimii vide, construiți 4 mulțimi distincte.
5. Dați exemplu de mulțime $A \neq \emptyset$ astfel încît $\cup A = \emptyset$. Cîte astfel de mulțimi există?
6. Are loc întotdeauna $\cup A \subseteq A$? Dar $A \subseteq \cup A$?
7. Fie A, B mulțimi. Scrieți o expresie a limbajului formal care să semnifice că:
 - a) Mulțimea A nu este inclusă în mulțimea B .
 - b) $A \neq B$ (folosiți doar relația de apartenență).
 - c) A conține măcar un element.
 - d) A conține cel mult un element.
 - e) A este submulțime a oricărei mulțimi.
 - f) A este element al oricărei mulțimi.
 - g) $B \subseteq \cup A$.
 Pentru fiecare enunț de mai sus, scrieți negația sa în limbaj natural și formal.
8. Demonstrați că, pentru orice mulțime A , A este strict inclusă în $A \cup \{A\}$.

I.3. Clase, relații, funcții

Nu există o „mulțime a tuturor mulțimilor”, căci acest concept conduce la paradoxuri. Dacă ar exista mulțimea tuturor mulțimilor, fie aceasta A , atunci, conform schemei de comprehensiune, ar exista și mulțimea $C = \{B \in A \mid B \notin B\}$. Se vede că regăsim paradoxul lui

Russel. Astfel de colecții „foarte mari” de obiecte apar însă frecvent în matematică (dorim de exemplu să vorbim de o proprietate pe care o au „toate” grupurile) și este necesară precizarea unui cadru riguros pentru aceste situații. O rezolvare rezonabilă este dată de conceptul de *clasă*.

În cadrul teoriei Gödel-Bernays (GB), *clasa* este o noțiune primară (nu se definește clasa, ci este dat un set de axiome referitoare la clase; mulțimile vor fi un tip particular de clase – cele care sînt elemente ale altor clase). Teoria astfel dezvoltată este însă considerabil mai complicată decît ZFS¹⁰.

În teoria ZFS, prin *clasă* se înțelege o expresie cu o variabilă liberă (un predicat cu o variabilă)¹¹. Cu alte cuvinte, o proprietate nu mai definește o *mulțime* de obiecte, ci este privită ea însăși ca o entitate și o numim *clasă*. O clasă *nu* este însă un obiect al teoriei ZFS, ci este o expresie a limbajului formal (cf. comentariul de la axioma-schemă a substituției). De exemplu, predicatul $P(x) : „x = x”$ este evident satisfăcut de orice mulțime x ; acest predicat definește „clasa tuturor mulțimilor”. Abuzînd de limbajul de la mulțimi, fiind dată o clasă $P(x)$, în loc să se spună ca un anumit x satisface P sau „ $P(x)$ este adevărată”, se spune „ x aparține clasei P ” sau „ x este un element al clasei P ”.

Observăm că orice mulțime a definește o clasă, anume „ $x \in a$ ”. Reciproc, spunem că o clasă $P(x)$ *corespunde* unei mulțimi M dacă are loc $(\forall x)(P(x) \leftrightarrow x \in M)$, adică obiectele care satisfac P sînt exact elementele lui M . Uneori spunem în acest caz chiar că P *este* o mulțime.

În acest sens, *clasa tuturor mulțimilor nu corespunde unei mulțimi*. Demonstrația a fost dată chiar la începutul acestui paragraf!

Se pot defini și *operații cu clase*, prin analogie cu cele de la mulțimi. Astfel, dacă $P(x)$ și $Q(x)$ sînt clase, definim *reuniunea* claselor P și Q ca fiind clasa $P(x) \vee Q(x)$; *intersecția* lor este clasa $P(x) \wedge Q(x)$. Cum s-ar defini *diferența* lor? Dar faptul că clasa P este *inclusă* în clasa Q ?

În această terminologie, schema de comprehensiune nu spune altceva decît că *intersecția dintre o clasă și o mulțime este o mulțime*.

Apare acum destul de clar că exprimări de genul „mulțimea tuturor grupurilor” nu sînt legitime, o exprimare corectă fiind „clasa tuturor grupurilor”. Noțiunea de clasă este esențială în *teoria categoriilor*.

Să trecem la un alt concept fundamental, anume la cel de *funcție*. Pentru aceasta, avem nevoie de noțiunea de *cuplu (pereche ordonată)*. Începem cu un rezultat interesant și prin sine.

¹⁰ În plus, s-a arătat că orice enunț despre mulțimi demonstrabil în GB este demonstrabil în ZFS.

¹¹ Această interpretare pentru clase a fost prezentată de W. Quine în 1963.

3.1 Propoziție (Teorema perechii). Fie a și b două mulțimi. Atunci există o mulțime c care are ca elemente pe a și pe b și numai pe ele. Formal:

$$(\forall a)(\forall b)(\exists c)(\forall x) [(x \in c) \leftrightarrow (x = a \vee x = b)]$$

Mulțimea c de mai sus este unic determinată de a și b și se notează $\{a, b\}$.

Demonstrație. Ideea este de a construi o mulțime cu două elemente D și de a obține $\{a, b\}$ ca imaginea lui D printr-o relație funcțională bine aleasă (se aplică deci axioma substituției).

Știm că există mulțimea vidă \emptyset . Construim (cu axioma mulțimii părților) mulțimea $\mathcal{P}(\emptyset)$, care are un element (avem $\emptyset \subseteq \emptyset$, deci $\emptyset \in \mathcal{P}(\emptyset)$; \emptyset este chiar unicul element al lui $\mathcal{P}(\emptyset)$) deci $\mathcal{P}(\emptyset) = \{\emptyset\}$. Cum \emptyset nu are nici un element, deducem că $\mathcal{P}(\emptyset) \neq \emptyset$. Construim acum $\mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\})$. Unicele mulțimi incluse în $\{\emptyset\}$ sînt \emptyset și $\{\emptyset\}$, deci $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$ are două elemente (cum am dorit).

Fie $E(x, y)$: " $(x = \emptyset \wedge y = a) \vee (x = \{\emptyset\} \wedge y = b)$ " (verificați că este o relație funcțională). Imaginea prin E a lui $\mathcal{P}(\{\emptyset\})$ este chiar mulțimea căutată c .

Unicitatea lui c rezultă din axioma extensionalității. □

Se poate arăta că, fiind date x_1, \dots, x_n distincte, există mulțimea X ale cărei elemente sînt x_1, \dots, x_n (și numai ele). Scrierea $X = \{x_1, \dots, x_n\}$ este o prescurtare a scrierii $(\forall x)(x \in X \leftrightarrow (x = x_1 \vee x = x_2 \vee \dots \vee x = x_n))$.

Această modalitate de a da o mulțime (prin enumerarea tuturor elementelor sale) se numește definire prin *extensiune*.

3.2 Exercițiu. Fie a și b mulțimi. Demonstrați că există reuniunea lor $a \cup b$ (adică unica mulțime cu proprietatea $\forall x[(x \in a \cup b) \leftrightarrow (x \in a \vee x \in b)]$).

Intuitiv, noțiunea de *cuplu (pereche ordonată)* format de elementele a și b diferă de $\{a, b\}$, prin faptul că avem o „ordine”: a este primul, iar b este al doilea. Această distincție între a și b se realizează prin:

3.3 Definiție. Fie a și b mulțimi. Aplicînd teorema perechii mulțimilor a și a , există mulțimea $\{a\}$; există și $\{a, b\}$. Aplicînd din nou teorema perechii, există mulțimea $\{\{a\}, \{a, b\}\}$, care se notează cu (a, b) și se numește *perechea ordonată (cuplul)* format de a și b . Observați că, dacă $a = b$, atunci $(a, b) = \{\{a\}\}$.

Această idee de introducere a noțiunii de cuplu este atribuită lui Kuratowski. Are loc proprietatea fundamentală următoare (demonstrați!):

3.4 Propoziție. Fie a, b, a', b' mulțimi. Atunci are loc: $(a, b) = (a', b') \Leftrightarrow (a = a' \wedge b = b')$. □

Astfel, spre deosebire de mulțimea $\{a, b\}$, în cuplul (a, b) contează ordinea elementelor a și b ; dacă $a \neq b$, atunci $\{a, b\} = \{b, a\}$, însă $(a, b) \neq (b, a)$.

Avînd definită noțiunea de cuplu, definim noțiunea de *triplet*:

$$(a, b, c) := ((a, b), c)$$

și, prin recurență, n -uplu, $\forall n \geq 3$ (pentru o tratare riguroasă a inducției și recurenței, vezi **I.4.21**)

$$(a_1, \dots, a_n) := ((a_1, \dots, a_{n-1}), a_n).$$

$$\text{Are loc: } (a_1, \dots, a_n) = (b_1, \dots, b_n) \leftrightarrow a_1 = b_1 \wedge \dots \wedge a_n = b_n.$$

În manualele de liceu (și în multe alte cărți de matematică), o *funcție* definită pe o mulțime A cu valori într-o mulțime B este „definită” (mai bine spus descrisă) ca fiind „un procedeu (lege), prin care oricărui element din A i se asociază un unic element din B ”. Intuitiv, descrierea este corectă (dar vagă, deoarece folosește noțiunea nedefinită de *procedeu (lege)*); în plus, se subînțelege că pentru orice funcție se poate descrie un *procedeu (algoritm)* de obținere a imaginii oricărui element prin funcția dată. Acest lucru nu este necesar și în matematică se întâlnesc exemple de funcții pentru care acest fapt nu are loc.

Se observă însă că o funcție $f: A \rightarrow B$ este perfect determinată de *graficul* său, adică de mulțimea cuplurilor $\{(a, f(a)) \mid a \in A\}$. Aceasta este și ideea definiției conceptului de funcție în cadrul unei tratări riguroase. Începem cu alte două noțiuni, și ele fundamentale:

3.5 Definiție. Fie A și B mulțimi. Numim *produsul cartezian*¹² al mulțimilor A și B mulțimea $A \times B := \{(a, b) \mid a \in A \wedge b \in B\}$.

Avem dreptul de a defini o astfel de mulțime? Ar trebui să arătăm că ne încadrăm în schema de comprehensiune, adică să indicăm o mulțime a cărei existență este certă, care să conțină toate perechile de forma (a, b) cu $a \in A$ și $b \in B$. Dar $(a, b) = \{\{a\}, \{a, b\}\}$. Observăm că avem $\{a\} \in \mathcal{P}(A \cup B)$ și $\{a, b\} \in \mathcal{P}(A \cup B)$, deci $\{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$. Astfel, putem defini, respectând schema de comprehensiune:

$$A \times B := \{c \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid (\exists a)(\exists b)[c = (a, b) \wedge a \in A \wedge b \in B]\}.$$

Folosind produsul cartezian putem defini noțiunile de *relație* și de *funcție*:

3.6 Definiție. Fie A și B două mulțimi.

a) Numim *relație binară între A și B* (sau *de la A la B*) orice triplet de forma (A, B, ρ) , unde $\rho \subseteq A \times B$. Uneori vom exprima acest fapt sub forma „ ρ este o relație între A și B ”. Dacă $A = B$, scriem (A, ρ) și spunem că ρ este o *relație pe A* . Adeseori, în loc de $(x, y) \in \rho$ se scrie $x\rho y$. Dacă sînt subînțelese mulțimile A și B , se spune, simplu, „relația ρ ” în loc de (A, B, ρ) .

b) O relație binară f de la A la B se numește *funcție* (sau *aplicație*) *definită pe A cu valori în B* dacă pentru orice $a \in A$ există un unic $b \in B$ astfel încît $(a, b) \in f$. Formal, tripletul (A, B, f) este funcție de la A la B dacă:

¹² În onoarea lui René Descartes (1596-1650), al cărui nume latinizat era Cartesius.

$$(f \subseteq A \times B) \wedge (\forall a) \{ (a \in A) \rightarrow (\exists b) [(b \in B) \wedge (a, b) \in f] \} \wedge$$

$$(\forall a)(\forall b)(\forall b') \{ (a \in A) \wedge (b \in B) \wedge (b' \in B) \wedge (a, b) \in f \wedge (a, b') \in f \rightarrow (b = b') \} \quad (*)$$

Întrucît pentru orice $a \in A$ există *un unic* $b \in B$ astfel încît $(a, b) \in f$, se scrie:

$$„f(a) = b” \text{ în loc de } „(a, b) \in f”.$$

Se mai spune „ f este o funcție (aplicație) de la A la B ” și se notează aceasta prin $f: A \rightarrow B$ sau $A \xrightarrow{f} B$. Notăția $f: A \rightarrow B$ nu este decît o prescurtare a faptului că expresia (*) este propoziție adevărată.

Mulțimea A se numește *domeniul* funcției f și B se numește *codomeniul* lui f . Orice element a din domeniul lui f se numește *argument* al funcției f . Dacă $a \in A$ și $b \in B$ astfel încît $f(a) = b$, b se numește *valoarea funcției f în a* .

Pentru orice mulțime A , notăm cu $\mathbf{1}_A$ sau cu id_A *funcția identitate* a mulțimii A , anume: $id_A(a) = a, \forall a \in A$. Cum se definește $\mathbf{1}_A$ ca relație de la A la A ?

Dacă adoptăm punctul de vedere naiv: o funcție $f: A \rightarrow B$ este o „lege de corespondență” prin care oricărui element a din A i se asociază un unic element $f(a)$ din B , atunci mulțimea $\{(a, f(a)) \mid a \in A\} \subseteq A \times B$ se numește *graficul* lui f . Astfel, definiția 3.6.b) identifică o funcție cu graficul ei.

3.7 Observație. Condiția (*) se scrie, mai puțin formalizat:

$$(f \subseteq A \times B) \text{ și } \forall a \in A, \exists b \in B \text{ astfel încît } (a, b) \in f \text{ și}$$

$$\forall a \in A, \forall b, b' \in B, (a, b) \in f \text{ și } (a, b') \in f \text{ implică } b = b'.$$

Observăm că, în expresii, șirurile de forma “ $(\forall a)(a \in A)$ ” se scriu adesea prescurtat “ $\forall a \in A$ ”. Această convenție, larg răspîndită, ascunde o capcană: o implicație, de genul $(\forall a)[(a \in A) \rightarrow P(a)]$, se scrie adesea “ $\forall a \in A, P(a)$ ”, în care implicația \rightarrow nu apare explicit. Trebuie conștientizat acest fapt, mai ales cînd apare necesitatea negării unei astfel de expresii: negația ei este $(\exists a)\{(a \in A) \wedge \neg P(a)\}$, lucru care nu este clar din scrierea prescurtată (dar este destul de clar din punct de vedere intuitiv).

3.8 Observație. O expresie cu exact două variabile libere se numește *relație*. Pentru orice relație $R(x, y)$ putem defini “*domeniul*” D_R și “*imagea*” I_R ca fiind *clasele*:

$$D_R(x): “(\exists y)R(x, y)”$$

$$I_R(y): “(\exists x)R(x, y)”$$

Demonstrați că, dacă clasele D_R și I_R sînt mulțimi, atunci relației $R(x, y)$ i se asociază o relație ρ între D_R și I_R (în sensul definiției 3.6.a), $\rho := \{(x, y) \in D_R \times I_R \mid R(x, y) \text{ adevărată}\}$. Mai mult, această relație este *funcție* (în sensul definiției 3.6.b) dacă și numai dacă R este *relație funcțională*. Invers, unei funcții $f: A \rightarrow B$ i se asociază o relație funcțională $F(x, y): “x \in A \wedge y = f(x)”$.

Demonstrați că, dacă R este relație funcțională și D_R este mulțime, atunci I_R este mulțime. Reciproca este adevărată?

3.9 Exercițiu. Fie A o mulțime. Câte funcții $\varphi : \emptyset \rightarrow A$ (respectiv $\varphi : A \rightarrow \emptyset$) există?

3.10 Definiție. Fie $f : A \rightarrow B$ o funcție. Dacă $A' \subseteq A$, se definește *imaginea lui A' prin f* ca fiind imaginea mulțimii A' prin relația funcțională asociată lui f . Cu alte cuvinte, definim

$$f[A'] = \{y \in B \mid (\exists x)(x \in A' \wedge f(x) = y)\}$$

Notăția tradițională pentru imaginea lui A' prin f este $f(A')$; nu se poate folosi o astfel de notație în teoria axiomatice a mulțimilor, pentru că A' poate fi simultan submulțime a lui A și element al lui A (puteți da exemplu de un astfel de caz?) și este foarte posibil ca $f(A')$ (valoarea în A' a lui f) să difere de $f[A']$ (imaginea submulțimii A' prin f).

3.11 Definiție. Fie I o mulțime (interpretată ca mulțime de „indici”). O funcție $b : I \rightarrow M$, unde M este o mulțime, se numește *familie de mulțimi indexată după I* . Notații tradiționale pentru această noțiune: $(B_i)_{i \in I}$ (unde $B_i := b(i)$), sau $\{B_i \mid i \in I\}$.

Dacă $(B_i)_{i \in I}$ este o familie de mulțimi ca mai sus, *reuniunea familiei* $\{B_i\}_{i \in I}$ este reuniunea imaginii funcției b :

$$\bigcup A = \bigcup_{i \in I} B_i := \{x \in M \mid \exists i \in I \text{ astfel încât } x \in B_i\}.$$

Intersecția familiei $\{B_i\}_{i \in I}$ este, prin definiție

$$\bigcap_{i \in I} B_i := \{x \mid \forall i \in I, x \in B_i\}.$$

De exemplu, dacă $I = \{1, 2\}$ și $\{B_i\}_{i \in I} = \{B_1, B_2\}$,

$$\bigcup \{B_1, B_2\} = \bigcup_{i \in I} B_i = B_1 \cup B_2; \text{ la fel, } \bigcap \{B_1, B_2\} = \bigcap_{i \in I} B_i = B_1 \cap B_2.$$

Se spune că *reuniunea familiei* $\{B_i\}_{i \in I}$ este *disjunctă* dacă $\{B_i\}_{i \in I}$ sînt disjuncte două câte două: $B_i \cap B_j = \emptyset$ dacă $i \neq j$. În acest caz se mai scrie $\bigcup_{i \in I} B_i = \bigcup_{i \in I} B_i$.

3.12 Propoziție. Pentru orice mulțimi A, B, C , și orice familie de mulțimi $(B_i)_{i \in I}$ au loc egalitățile:

- i) $\emptyset \cap A = \emptyset, \emptyset \cup A = A, A \setminus \emptyset = A, A \setminus A = \emptyset$;
- ii) $A \cap B \subseteq A, A \cap B \subseteq B, A \subseteq A \cup B, B \subseteq A \cup B$;
- iii) $A \cap B = B \cap A, A \cup B = B \cup A$;
- iv) $A \cap (B \cap C) = (A \cap B) \cap C, A \cup (B \cup C) = (A \cup B) \cup C$;
- v) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
- vi) $A \cap (\bigcup_{i \in I} B_i) = \bigcup_{i \in I} (A \cap B_i); A \cup (\bigcap_{i \in I} B_i) = \bigcap_{i \in I} (A \cup B_i)$.
- vii) $A \cup A = A = A \cap A$. □

3.13 Definiție. Se numește *inversă a unei relații* (A, B, ρ) relația (B, A, ρ^{-1}) unde $\rho^{-1} = \{(b, a) \mid (a, b) \in \rho\} \subseteq B \times A$.

Fie relațiile (A, B, ρ) și (B, C, τ) . Relația $(A, C, \tau \circ \rho)$, unde

$$\tau \circ \rho = \{(a, c) \in A \times C \mid (\exists b)(b \in B \wedge a \rho b \wedge b \tau c)\}$$

este numită *compusa* (sau *compunerea*) *relațiilor* τ și ρ .

3.14 Propoziție. a) Fiind date funcțiile $u : A \rightarrow B$, $v : B \rightarrow C$, compusa $v \circ u$ este tot o funcție, $v \circ u : A \rightarrow C$, și, $\forall a \in A$, are loc:

$$(v \circ u)(a) = v(u(a)).$$

b) Pentru orice relații (A, B, ρ) , (B, C, τ) , (C, D, η) , avem $(\eta \circ \tau) \circ \rho = \eta \circ (\tau \circ \rho)$ (compunerea relațiilor este asociativă). În particular, compunerea funcțiilor este asociativă. \square

Se disting următoarele tipuri remarcabile de funcții:

3.15 Definiție. Fie $f : A \rightarrow B$ o funcție. Spunem că f este:

- i) funcție injectivă dacă $\forall x, y \in A, f(x) = f(y) \Rightarrow x = y$;
- ii) funcție surjectivă dacă $\forall y \in B, \exists x \in A$ astfel încât $f(x) = y$;
- iii) funcție bijectivă dacă este injectivă și surjectivă;
- iv) funcție inversabilă dacă $\exists g : B \rightarrow A$ (numită inversa lui f) astfel încât $(g \circ f)(x) = x$, $\forall x \in A$ și $(f \circ g)(y) = y$, $\forall y \in B$.

Notînd, pentru o mulțime M , prin $\mathbf{1}_M : M \rightarrow M$ funcția $\mathbf{1}_M(x) = x$, $\forall x \in M$ (numită și funcția identitate a lui M , notată și cu id_M sau id), condițiile ce definesc funcția inversabilă pot fi rescrise în modul următor: $g \circ f = \mathbf{1}_A, f \circ g = \mathbf{1}_B$. Dacă există, inversa lui f se notează f^{-1} .

3.16 Propoziție. Fie $f : A \rightarrow B$ și $g : B \rightarrow C$ funcții. Atunci:

- a) f este inversabilă $\Leftrightarrow f$ este bijectivă;
- b) $g \circ f$ este bijectivă $\Rightarrow g$ este surjectivă și f este injectivă;
- c) Compunerea a două funcții injective (surjective) este funcție injectivă (surjectivă). \square

Definiția produsului cartezian poate fi extinsă prin recurență la o familie de trei sau mai multe mulțimi, sau, mai general, la o familie oarecare de mulțimi:

3.17 Definiție. a) Fiind date mulțimile A_1, A_2, A_3 ¹³, definim produsul lor cartezian:

$$A_1 \times A_2 \times A_3 := (A_1 \times A_2) \times A_3.$$

Astfel, $\forall a_1 \in A_1, \forall a_2 \in A_2, \forall a_3 \in A_3$, notăm $((a_1, a_2), a_3)$, mai simplu, cu (a_1, a_2, a_3) .

b) Pentru orice $n \geq 3$ și orice familie de n mulțimi A_1, A_2, \dots, A_n , definim (prin recurență¹⁴):

$$A_1 \times A_2 \times \dots \times A_n := (A_1 \times A_2 \times \dots \times A_{n-1}) \times A_n.$$

$A_1 \times A_2 \times \dots \times A_n$ se mai notează cu $\prod_{i=1}^n A_i$ sau $\prod_{1 \leq i \leq n} A_i$. Dacă $\forall i \in \{1, 2, \dots, n\}, a_i \in A_i$, se notează $((a_1, a_2, \dots, a_{n-1}), a_n) \in \prod_{i=1}^n A_i$ cu (a_1, a_2, \dots, a_n) . Astfel,

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i, i = \overline{1, n}\}$$

În cazul $A_1 = A_2 = \dots = A_n = A$, $A \times A \times \dots \times A$ (de n ori) se notează cu A^n .

¹³ În această ordine! De fapt, se dă o familie de mulțimi indexată după $\{1, 2, 3\}$.

¹⁴ Folosim deocamdată o accepție intuitivă a noțiunii de definiție prin recurență. Pentru o tratare riguroasă, vezi 4.21 și următoarele.

c) Este necesară și o definiție în cazul general al unei familii de mulțimi $(A_i)_{i \in I}$ indexată după o mulțime de indici I . Se definește produsul cartezian $\prod_{i \in I} A_i$:

$$\prod_{i \in I} A_i := \{\varphi : I \rightarrow \bigcup_{i \in I} A_i \mid \varphi(i) \in A_i, \forall i \in I\}.$$

3.18 Observație. Produsul cartezian definit ca la c), în cazul unei familii finite de mulțimi, nu este același cu cel definit la a) și b) și la 3.5. Există însă o bijecție naturală între mulțimile obținute prin cele două definiții. De exemplu, dacă $I = \{1, 2\}$, avem funcția bijectivă β , definită pe $\{\varphi : \{1, 2\} \rightarrow A_1 \cup A_2 \mid \varphi(i) \in A_i, \forall i \in I\}$ cu valori în $A_1 \times A_2$, dată de $\beta(\varphi) = (\varphi(1), \varphi(2))$. Se pot astfel identifica noțiunile de produs cartezian definite mai sus.

Definim următoarele *tipuri remarcabile de relații pe o mulțime*:

3.19 Definiție. Fie o mulțime nevidă A și ρ o relație pe A . Spunem că ρ este:

- *reflexivă* dacă $a\rho a, \forall a \in A$. Formal: $(\forall a)(a \in A \rightarrow a\rho a)$;
- *ireflexivă* dacă $\forall a \in A$, nu are loc $a\rho a$;
- *simetrică* dacă $\forall a, b \in A, a\rho b \rightarrow b\rho a$;
- *asimetrică* dacă $\forall a, b \in A, a\rho b \rightarrow \neg b\rho a$;
- *antisimetrică* dacă $\forall a, b \in A, a\rho b$ și $b\rho a \rightarrow a = b$;
- *tranzitivă* dacă $\forall a, b, c \in A, a\rho b$ și $b\rho c \rightarrow a\rho c$;
- *relație de echivalență* dacă este reflexivă, simetrică și tranzitivă. Pentru relații de echivalență se folosesc notații de tipul $a \equiv b$, $a \sim b$ în loc de $a\rho b$.
- *relație de preordine* dacă este reflexivă și tranzitivă;
- *relație de ordine* dacă este reflexivă, tranzitivă și antisimetrică. Pentru relații de (pre)ordine se folosesc în general notații de tipul $a \leq b$ în loc de $a\rho b$.
- *relație de ordine strictă* dacă este ireflexivă și tranzitivă. Pentru relații de ordine strictă se folosesc în general notații de tipul $a < b$ în loc de $a\rho b$.

Relațiile de *ordine* și de *echivalență* sînt deosebit de importante în toată matematica și este esențială o bună cunoaștere a proprietăților lor.

3.20 Exercițiu. a) Scrieți formal condițiile de mai sus referitoare la o relație ρ .

b) Cum se generalizează definițiile anterioare la *relații* (în sensul de expresii cu două variabile libere)? De exemplu, o relație $R(x, y)$ se numește reflexivă dacă $(\forall x)R(x, x)$.

c) Exprimați definițiile de mai sus în termeni de incluziuni și compuneri de relații (și eventual de inverse). De exemplu, ρ este reflexivă înseamnă că $id_A \subseteq \rho$; ρ este simetrică înseamnă că $\rho^{-1} \subseteq \rho$.

Dacă \leq este o relație de ordine pe A , scriem (A, \leq) și spunem că (A, \leq) este *mulțime ordonată*. Dacă pentru orice $a, b \in A$ avem $a \leq b$ sau $b \leq a$, atunci (A, \leq) se numește mulțime *total ordonată* (sau *lanț*) și relația \leq se numește relație de *ordine totală*. Uneori, pentru a sublinia că o anumită relație de ordine nu este totală, se spune *relație de ordine parțială*. În

loc de $a \leq b$ se scrie și $b \geq a$. Se observă că, dacă \leq este o relație de ordine pe A , atunci \geq este tot o relație de ordine.

3.21 Observație. Dacă \leq este o relație de ordine pe A , atunci relația $<$ pe A , definită prin: $x < y \leftrightarrow (x \leq y \wedge x \neq y)$ este o relație de *ordine strictă* pe A . Reciproc, dacă $<$ este o ordine strictă pe A , atunci, definind $x \leq y \leftrightarrow (x < y \vee x = y)$ se obține o relație de ordine pe A . Verificați! Așadar, există o bijecție între relațiile de ordine pe A și relațiile de ordine strictă pe A . De aceea, orice definiție sau rezultat aplicabil unei relații de ordine se aplică și relației de ordine strictă asociate (și reciproc). Cum trebuie adaptate aceste considerații la *relațiile* văzute în sensul de la 3.8?

3.22 Definiție. Fie (A, \leq) o mulțime ordonată și B o submulțime a lui A . Un element $m \in A$ se numește *minorant* al lui B dacă $m \leq b, \forall b \in B$. Un element $M \in A$ se numește *majorant* al lui B dacă $b \leq M, \forall b \in B$. Submulțimea B se numește *minorată* (resp. *majorată*) dacă are un minorant (resp. majorant). Dacă B conține un minorant m pentru B , spunem că m este *cel mai mic element* (sau *primul element*) al lui B . Notăție: $m = \min(B)$.

Dacă B conține un majorant M pentru B , M se numește *cel mai mare element* (sau *ultimul element*) al lui B . Notăție: $M = \max(B)$.

Dacă B are un prim element $m \in B$, acesta este unic: $\forall m' \in B$ cu m' prim element, avem $m \leq m'$ (m este prim element) și $m' \leq m$ (m' este prim element), deci $m = m'$ din antisimetrie. La fel, *ultimul element al lui B este unic (dacă există)*.

3.23 Exemplu. Relația de divizibilitate " $|$ " pe \mathbb{N} , dată de:

$$\forall a, b \in \mathbb{N} \quad (a|b \leftrightarrow \exists c \in \mathbb{N} \text{ astfel încât } b = ac)$$

este o relație de ordine, care *nu este totală* (nu are loc nici $2|3$, nici $3|2$); 0 este *ultimul element* al lui $(\mathbb{N}, |)$ și 1 este *primul element* al lui $(\mathbb{N}, |)$. Relația uzuală de ordine " \leq " pe \mathbb{N} este *totală*, 0 este primul element al lui (\mathbb{N}, \leq) ; nu există ultimul element al lui (\mathbb{N}, \leq) .

O mulțime (A, \leq) cu proprietatea că orice submulțime nevidă B a lui A are un prim element se numește mulțime *bine ordonată* (caz în care relația \leq pe A se numește *relație de bună ordine*). Mulțimile bine ordonate sînt foarte importante: pe o mulțime bine ordonată se poate aplica un raționament prin *inducție*.

Orice mulțime bine ordonată este total ordonată (demonstrați!).

3.24 Definiție. Un element m al unei mulțimi ordonate (A, \leq) se numește *element maximal* al lui A dacă, $\forall b \in A$ cu $m \leq b$ rezultă $m = b$. Un element m se numește *element minimal* al lui A dacă, $\forall b \in A$ cu $b \leq m$ rezultă $m = b$. De exemplu, în mulțimea ordonată $\mathbb{N} \setminus \{0, 1\}$ cu divizibilitatea, 2 este element minimal. Care sînt toate elementele sale minimale? Există elemente maximale?

3.25 Definiție. Fie (A, \leq) o mulțime ordonată și B o submulțime a sa. Fie $Maj(B)$ mulțimea majoranților lui B . Dacă există cel mai mic element al lui $Maj(B)$, acest element se numește *supremumul* (sau *marginia superioară* a) lui B și se notează $\sup B$. Dacă există $\sup B = c$, atunci c este „*cel mai mic majorant al lui B*”, adică satisface condițiile:

- $\forall b \in B, b \leq c$ (c este majorant al lui B).
- $\forall c' \in A$ astfel încât $\forall b \in B, b \leq c'$, rezultă $c \leq c'$ (c este mai mic decât orice alt majorant c' al lui B).

„Dual” (considerînd relația de ordine \geq) se obține noțiunea de *infimum* (sau *marginie inferioară*) al submulțimii B a lui (A, \leq) , notat (dacă există!) cu $\inf B$.

O mulțime ordonată (A, \leq) cu proprietatea că orice submulțime cu două elemente a sa are supremum și infimum se numește *latice*. Dacă orice submulțime a lui A are \sup și \inf , A se numește *latice completă*.

De exemplu, pentru o mulțime nevidă oarecare M , mulțimea $\mathcal{P}(M)$ a părților lui M este ordonată de relația de incluziune; dacă $A, B \in \mathcal{P}(M)$, atunci

$$\sup\{A, B\} = A \cup B, \inf\{A, B\} = A \cap B.$$

$(\mathcal{P}(M), \subseteq)$ este chiar o latice completă (de ce?). La fel, $(\mathbb{N}, |)$ este o latice.

În \mathbb{R} , ordonat cu ordinea uzuală, orice submulțime nevidă majorată are supremum (aceasta este o proprietate fundamentală a lui \mathbb{R} , esențială în Analiză). În \mathbb{Q} , nu orice submulțime nevidă are supremum (justificați!).

Exerciții

1. Dacă $f: A \rightarrow B$ este o funcție, iar $C, D \subseteq A$, scrieți formal că $f[C] = f[D]$.

2. Fie $f: A \rightarrow B$ o funcție și $E \subseteq B$. Definem $f^{-1}(E) = \{a \in A \mid f(a) \in E\}$ (numită *contraimagea* lui E prin f). Definem $f^*: \mathcal{P}(B) \rightarrow \mathcal{P}(A), f^*(E) = f^{-1}(E), \forall E \in \mathcal{P}(B)$. Definem $f_*: \mathcal{P}(A) \rightarrow \mathcal{P}(B), f_*(D) = f[D], \forall D \in \mathcal{P}(A)$.

a) Demonstrați că următoarele afirmații sînt echivalente:

- (i) f este injectivă;
- (ii) f_* este injectivă;
- (iii) f^* este surjectivă;
- (iv) $f[X \cap Y] = f[X] \cap f[Y], \forall X, Y \in \mathcal{P}(A)$.

b) Demonstrați că următoarele afirmații sînt echivalente:

- (i) f este surjectivă;
- (ii) f_* este surjectivă;
- (iii) f^* este injectivă;

3. Fie $f: A \rightarrow B$ o funcție.

a) Demonstrați că f este injectivă dacă și numai dacă are loc: oricare ar fi o mulțime C și oricare ar fi $u, v: C \rightarrow A$ astfel încât $f \circ u = f \circ v$, rezultă $u = v$. (f este monomorfism în categoria *Set*).

b) Demonstrați că f este surjectivă dacă și numai dacă are loc: oricare ar fi o mulțime C și oricare ar fi $u, v: A \rightarrow C$ astfel încât $u \circ f = v \circ f$, rezultă $u = v$. (f este epimorfism în categoria *Set*).

4. Fie A, B mulțimi. Notăm $B^A = \{f \mid f: A \rightarrow B\}$.

a) Definiția de mai sus nu respectă Observația 2.6. Cum trebuie modificată încât să o respecte?

b) Demonstrați că există o bijecție între $\{0, 1\}^A$ și $\mathcal{P}(A)$. (aici 0 și 1 notează două mulțimi distincte oarecare, de exemplu $0 = \emptyset$, $1 = \{\emptyset\}$).

c) Demonstrați că există o bijecție între $(A \times B)^C$ și $A^C \times B^C$

5. Fie A, B mulțimi finite, cu m elemente, respectiv n elemente.

(a) Câte elemente are $A \times B$?

(b) Câte relații binare de la A la B există?

(c) Câte funcții definite pe A cu valori în B există?

(d) Câte funcții injective definite pe A cu valori în B există?

I.4. Ordinale, axioma infinității și mulțimea numerelor naturale

În toată matematica este esențială mulțimea numerelor naturale \mathbb{N} . Se pune problema unui mod de a construi această mulțime (sau, fiind vorba de un concept care poate apărea drept primar, de a axiomatiza \mathbb{N}). Vom arăta că, în cadrul teoriei axiomatice a mulțimilor, se poate da o construcție satisfăcătoare a lui \mathbb{N} . Mai mult, modul de construcție duce la o generalizare posibilă a mulțimii \mathbb{N} , sub forma *clasei ordinalelor*.

O modalitate de abordare a introducerii lui \mathbb{N} este dată de *axiomatica Dedekind-Peano*. *Noțiunile primare* sînt cele de *număr natural* și *funcție succesor*¹⁵. Limbajul acestei teorii axiomatice este format din:

¹⁵ Întrucît este vorba de o teorie axiomatică, funcția succesor nu este a priori o *funcție* în sensul teoriei mulțimilor (ci este o noțiune primară); este adevărat însă că în *modelul* pe care îl construim, rolul funcției succesor va fi jucat de o funcție în sens uzual.

- simbolul $=$ (notează egalitatea a două obiecte);
 - simbolul 0 (notează un număr natural privilegiat fixat);
 - nume variabile, constante, conectorii logici (ca la limbajul teoriei axiomatice a mulțimilor), cu deosebirea că numele denumesc acum obiectele acestei teorii, adică *numere naturale*.

Axiomele acestei teorii sînt:

1. Există un număr natural notat 0 .
2. Pentru orice număr natural n , există un număr natural unic determinat, numit *succesorul lui n* și notat $s(n)$ sau n^+ : $(\forall n)(\exists n^+)$.
3. Orice două numere naturale cu același succesori sînt egale: $(\forall m)(\forall n)(m^+ = n^+ \rightarrow m = n)$.
4. 0 nu este succesori nici unui număr natural: $(\forall n)(n^+ \neq 0)$.
5. (**Axioma inducției**) Pentru orice predicat cu o variabilă $A(n)$ are loc:

$$[A(0) \wedge (\forall n)(A(n) \rightarrow A(n^+))] \rightarrow (\forall m)A(m).$$

Observăm că axioma **5** (binecunoscutul *principiu de demonstrație prin inducție*) este de fapt o *schemă de axiome*.

Introducerea operațiilor cu numere naturale, a relației de ordine și deducerea principalelor proprietăți ale acestora folosind axiomatice Dedekind-Peano sînt interesante și instructive. Aceste aspecte fiind însă destul de cunoscute (vezi de ex. BECHEANU et al. [1983]), nu insistăm în această direcție. Vom arăta, în schimb, că se poate *modela* sistemul axiomatic de mai sus în cadrul teoriei mulțimilor, dacă mai introducem o axiomă (de fapt, acest *model* se expune în general, cînd se vorbește de axiomatice Peano). Mai precis, vom construi o *mulțime* \mathbb{N} , un *element* $0 \in \mathbb{N}$ și o *funcție* (în sens uzual) $s : \mathbb{N} \rightarrow \mathbb{N}$, $s(n) = n^+$, care să satisfacă axiomele de mai sus.

Începem cu o abordare intuitivă. Instrumentele oferite pînă acum de axiomele teoriei mulțimilor permit considerarea următorului „șir de mulțimi”:

$$\emptyset; \{\emptyset\}; \{\emptyset, \{\emptyset\}\}; \{\emptyset, \{\emptyset, \{\emptyset, \{\emptyset\}\}\}\}; \dots \quad (1)$$

Se observă că, pentru fiecare termen x al șirului, următorul termen este $x \cup \{x\}$. Primul termen are 0 elemente, al doilea are 1 element ș.a.m.d. Ar fi tentant să considerăm drept mulțime a numerelor naturale „mulțimea tuturor termenilor acestui șir”, \emptyset să joace rolul lui 0 , iar funcția succesori să fie $s(x) = x \cup \{x\}$. Apar două probleme: *definirea riguroasă* a „mulțimii tuturor termenilor șirului (1)” și garantarea *existenței* unei astfel de mulțimi. Faptul că există o mulțime care *include* toți termenii șirului (1) este asigurat de o nouă axiomă:

4.1 Axioma infinității. $(\exists M) [\emptyset \in M \wedge (\forall y)(y \in M \rightarrow y \cup \{y\} \in M)]$.

Intuitiv, este clar că axioma de mai sus garantează existența unei mulțimi M care să conțină toate mulțimile șirului (1); aceasta nu înseamnă că M conține *doar* aceste mulțimi. Vom adopta următoarea strategie: definim riguros *clasa* mulțimilor din șirul (1) (aceasta va fi clasa

ordinalelor finite, noțiune pe care o vom defini în cele ce urmează); atunci mulțimea \mathbb{N} a numerelor naturale va fi obținută prin comprehensiune, ca fiind mulțimea acelor elemente din M (dată de axioma infinității) care sînt în plus ordinale finite. Apoi demonstrăm că toate aceste obiecte satisfac axiomele Dedekind-Peano.

Într-o primă lectură, se pot omite paragrafele 4.2 pînă la 4.16.

4.2 Definiție. O mulțime α se numește *ordinal* dacă are următoarele proprietăți:

i) α este *tranzitivă*, adică $(\forall x)(x \in \alpha \rightarrow x \subseteq \alpha)$.

ii) relația de apartenență definește o relație de *ordine strictă* pe α , care este o *bună ordine* pe α . Detaliind, această condiție este echivalentă cu:

- $\forall x, y, z \in \alpha$, din $x \in y$ și $y \in z$ rezultă că $x \in z$ (*tranzitivitatea* relației \in);
- $\forall x, y \in \alpha$, din $x \in y$ rezultă că $y \notin x$ (*ireflexivitatea* relației \in);
- orice submulțime nevidă a lui α are un prim element (față de relația \in):

$$\forall \beta \{(\beta \subseteq \alpha \wedge \beta \neq \emptyset) \rightarrow \exists x [x \in \beta \wedge \forall y (y \in \beta \rightarrow (x = y \vee x \in y))]\}.$$

4.3 Exemplu. Orice element din șirul (1) este ordinal.

Clasa ordinalelor se notează cu On . Astfel, scrierea $On(\alpha)$ înseamnă „mulțimea α este un ordinal”.¹⁶

Înainte de a defini ordinalele *finite*, avem nevoie de unele pregătiri.

4.4 Definiție. Fie (A, \leq) o mulțime ordonată. O submulțime S a lui A se numește *segment inițial* al lui A dacă are proprietatea că, odată cu un element x , conține toate elementele mai mici decît x : $\forall x [x \in S \rightarrow (\forall y (y \in A \wedge y \leq x) \rightarrow y \in S)]$.

De exemplu, dacă fixăm $a \in A$, mulțimea $S_a(A) := \{x \in A \mid x < a\}$ este un segment inițial în A . Este remarcabil că în mulțimi *bine ordonate*, toate segmentele inițiale sînt de acest tip:

4.5 Propoziție. Fie (A, \leq) o mulțime *bine ordonată* și S un segment inițial al lui A . Atunci: sau $S = A$, sau există $a \in A$ astfel încît $S = S_a(A) := \{x \in A \mid x < a\}$.

Demonstrație. Presupunem că $S \neq A$. Atunci $A \setminus S$ este nevidă și (A fiind bine ordonată) are un prim element a . Afirmăm că $S_a(A) = S$. Într-adevăr, fie $x \in S$. Dacă $a \leq x$, atunci $a \in S$, din definiția segmentului inițial. Cum A este total ordonată, rezultă că $x < a$, adică $x \in S_a(A)$. Incluziunea cealaltă o lăsăm cititorului. \square

4.6 Propoziție. Fie α un ordinal și s un segment inițial în α . Atunci $s = \alpha$ sau există $\beta \in \alpha$ astfel încît $s = \beta = S_\beta(\alpha)$.

¹⁶ Ideea de a defini ordinalele în această manieră îi aparține lui John von Neumann. Un ordinal se poate defini și ca o *clasă de izomorfism de mulțimi bine ordonate*. În această abordare însă, clasa ordinalelor ar fi o "clasă de clase", o complicare tehnică evitată de prezentarea aleasă aici.

Demonstrație. Reamintim că relația de ordine strictă pe α este \in , față de care α este bine ordonată. Din propoziția precedentă rezultă că $s = \alpha$ sau există $\beta \in \alpha$ astfel încât $s = S_\beta(\alpha)$. Dar $S_\beta(\alpha) = \{x \in \alpha \mid x \in \beta\} = \alpha \cap \beta$. Cum α este ordinal, din $\beta \in \alpha$ rezultă $\beta \subseteq \alpha$, deci $\alpha \cap \beta = \beta$. \square

4.7 Propoziție. *Orice element al unui ordinal este tot un ordinal.*

Demonstrație. Fie α un ordinal și $\beta \in \alpha$. Atunci $\beta = S_\beta(\alpha)$, care este un segment inițial în α . În general, orice submulțime nevidă a unei mulțimi bine ordonate A este bine ordonată de relația de ordine de pe A (demonstrați!), deci $\beta = S_\beta(\alpha)$ este bine ordonat de \in . Avem și că β este tranzitivă: dacă $x \in \beta$, iar $y \in x$, atunci $x \in \alpha$ (căci $\beta \in \alpha$ și α este tranzitivă). Acum, din $x \in \alpha$ și $y \in x$ deducem că $y \in \alpha$. Am obținut că $y, x, \beta \in \alpha, y \in x$ și $x \in \beta$. Relația \in este tranzitivă pe α , deci $y \in \beta$. \square

4.8 Propoziție. *Dacă α este un ordinal, atunci $\alpha \notin \alpha$.*

Demonstrație. Relația de apartenență \in este de ordine strictă pe α , deci este ireflexivă: $\forall x \in \alpha$, avem $x \notin x$. Dacă presupunem că $\alpha \in \alpha$, obținem astfel că $\alpha \notin \alpha$, absurd. \square

4.9 Propoziție. *Pentru orice ordinale α și β , are loc una și numai una din afirmațiile: $\alpha \in \beta, \alpha = \beta$ sau $\beta \in \alpha$.*

Demonstrație. Fie $\gamma = \alpha \cap \beta = \{x \in \alpha \mid x \in \beta\}$. Se verifică imediat că γ este un segment inițial în mulțimea ordonată (α, \in) (vezi def. 4.4). Din 4.6 rezultă că $\gamma = \alpha$ sau $\gamma \in \alpha$. Simetric, avem $\gamma = \beta$ sau $\gamma \in \beta$. Analizăm toate posibilitățile: 1) $\gamma = \alpha$ și $\gamma = \beta$. Atunci $\alpha = \beta$. 2) $\gamma = \alpha$ și $\gamma \in \beta$. Atunci $\alpha \in \beta$. 3) $\gamma \in \alpha$ și $\gamma = \beta$. Atunci $\beta \in \alpha$. 4) $\gamma \in \alpha$ și $\gamma \in \beta$. Atunci $\gamma \in \alpha \cap \beta = \gamma$, imposibil: γ este ordinal și s-ar contrazice 4.8.

Cele trei situații din enunț sînt mutual incompatibile: dacă $\alpha \in \beta$, atunci $\alpha = \beta$ ar contrazice 4.8, iar $\beta \in \alpha$ implică (pentru că α este tranzitivă) $\alpha \in \alpha$, aceeași contradicție. \square

Putem enunța proprietatea de mai sus sub forma: *Clasa ordinalelor este total ordonată de relația de ordine strictă \in .*

Mai mult, *clasa ordinalelor este bine ordonată de relația de apartenență*. Acest enunț necesită precizări: nu am definit încă noțiunea de clasă bine ordonată. O analogie directă cu mulțimile bine ordonate ar conduce la următoarea „definiție”: o clasă $C(x)$ ordonată de o relație (în sensul de la 3.8) de ordine $R(x, y)$ este bine ordonată dacă *orice subclasă* nevidă a sa are un prim element. Sintagma „*orice subclasă*” inclusă în definiție conduce de fapt la a da o *schemă* de definiții, căci clasele nu sînt obiecte ale teoriei, ci expresii ale limbajului formal (cf. comentariul de la Axioma-schemă a substituției). Se adoptă următoarea definiție, mai restrictivă, dar care nu are dezavantajul descris anterior:

4.10 Definiție. O clasă $C(x)$ se numește *bine ordonată* de o relație de ordine strictă $R(x, y)$ dacă este total ordonată de R și orice segment inițial al lui C în raport cu relația R este o mulțime bine ordonată de R . Mai precis, au loc afirmațiile:

- R este o relație ireflexivă pe C : $\forall x(C(x) \rightarrow \neg R(x, x))$.
- R este o relație tranzitivă pe C : $\forall x \forall y \forall z(C(x) \wedge C(y) \wedge C(z) \wedge R(x, y) \wedge R(y, z) \rightarrow R(x, z))$.
- R este o relație totală pe C : $\forall x \forall y(C(x) \wedge C(y) \rightarrow (R(x, y) \vee R(y, x) \vee x = y))$.
- Pentru orice mulțime t , segmentul inițial al clasei C determinat de t în raport cu relația R , adică clasa $S_t(C)(\text{mod } R) := C(x) \wedge R(x, t)$, este o *mulțime* bine ordonată de R :

$$(\forall t)(\exists s)[(\forall x)(x \in s \leftrightarrow (C(x) \wedge R(x, t)))] \wedge (\forall u)[(u \neq \emptyset \wedge u \subseteq s) \rightarrow \exists p(p \text{ primul element al lui } u)]$$

Dacă C este bine ordonată de R în sensul definiției anterioare, atunci *orice clasă nevidă inclusă în C are prim element*. Într-adevăr, fie D o clasă nevidă inclusă în C și fie t un element din D (adică $D(t)$ adevărată). Dacă t este prim element în D în raport cu R , atunci am terminat. Dacă nu, există q în D mai mic strict decât t : $D(q) \wedge R(q, t)$. Dar segmentul inițial $S_t(C)(\text{mod } R)$ este o mulțime; deci intersecția clasei D cu $S_t(C)(\text{mod } R)$ (adică clasa $D(x) \wedge (x \in S_t(C)(\text{mod } R))$) este o submulțime S a lui $S_t(C)(\text{mod } R)$ (nevidă, căci conține q). Din buna ordonare a lui $S_t(C)(\text{mod } R)$ deducem că există primul element m al mulțimii S . Acesta este primul element al clasei D : dacă ar exista n în D , mai mic decât m , atunci n este mai mic decât t și deci $n \in S_t(C)(\text{mod } R)$. Astfel, $n \in S$ și obținem o contradicție cu faptul că m este primul element al lui S .

Să demonstrăm acum:

4.11 Propoziție. *Clasa ordinalelor On este bine ordonată de relația de apartenență.*

Demonstrație. Am văzut (4.9) că relația de apartenență este totală pe clasa ordinalelor. Fie α un ordinal și segmentul inițial $S_\alpha(On)(\text{mod } \in) = On(t) \wedge (t \in \alpha)$. Evident, această clasă este o mulțime, anume α (orice element t al lui α este ordinal). Din definiția ordinalelor, α este bine ordonat de apartenență. \square

Ordonarea „nestrictă” pe clasa On este *incluziunea*. Mai precis, pentru două ordinale α și β , ($\alpha \in \beta \vee \alpha = \beta$) este echivalent cu $\alpha \subseteq \beta$. Cel mai mic ordinal este \emptyset . Care este însă cel mai mic ordinal mai mare decât un ordinal α dat?

4.12 Propoziție. *Pentru orice ordinal α , $\alpha \cup \{\alpha\}$ este tot ordinal (numit succesorul lui α) și este cel mai mic ordinal, mai mare decât α .*

Demonstrație. Propunem spre demonstrație afirmația: α ordinal implică $\alpha \cup \{\alpha\}$ ordinal. Fie acum β un ordinal mai mare decât α . Atunci $\alpha \in \beta$ (adică $\{\alpha\} \subseteq \beta$). Deci $\alpha \subseteq \beta$ (căci β ordinal), și astfel $\alpha \cup \{\alpha\} \subseteq \beta$. Aceasta demonstrează că orice ordinal mai mare decât α este mai mare sau egal cu $\alpha \cup \{\alpha\}$. Pe de altă parte, este evident că $\alpha \in \alpha \cup \{\alpha\}$. \square

4.13 Definiție. Dacă pentru ordinalul β există α astfel încât $\beta = \alpha \cup \{\alpha\}$ (β este succesorul lui α), atunci α este ordinal, unic determinat de β (de ce?) și se numește *predecesorul* lui β . Un ordinal α se numește *ordinal finit* dacă: sau $\alpha = \emptyset$, sau orice element al lui α și α însuși au un predecesor. Un ordinal care nu este finit se numește *ordinal infinit*.

Se observă că toate mulțimile din șirul (1) sînt ordinale finite. De altfel, șirul a fost construit plecînd de la \emptyset și luînd succesorul fiecărui ordinal construit deja.

Dacă α este ordinal finit, atunci se verifică imediat că:

- orice ordinal $\beta \subseteq \alpha$ este ordinal finit.
- succesorul lui α , $\alpha \cup \{\alpha\}$, este ordinal finit.

4.14 Propoziție. *Axioma infinității este echivalentă cu afirmația:*

Ordinalele finite formează o mulțime (notată cu ω).

Demonstrație. Presupunem axioma infinității adevărată și considerăm mulțimea $\omega := \{\alpha \in M \mid \alpha \text{ ordinal finit}\}$, unde M este dată de 4.1. Să arătăm că ω conține orice ordinal finit. Dacă nu ar fi așa, ar exista un ordinal finit β , cu $\beta \notin M$. Cum clasa ordinarilor finite este bine ordonată, există cel mai mic ordinal finit μ cu proprietatea că $\mu \notin M$. Cum $\emptyset \in M$, $\mu \neq \emptyset$. Însă atunci μ are un predecesor λ , care (din modul de alegere al lui μ) este în M . Însă atunci succesorul lui λ (adică μ) aparține lui M , contradicție.

Invers, dacă ordinarile finite formează o mulțime ω , atunci ω satisface proprietățile din axioma 4.1: $\emptyset \in \omega$ și $\forall \alpha \in \omega$, avem $\alpha \cup \{\alpha\} \in \omega$. □

Acum se poate da următorul **model** (în cadrul teoriei axiomatice a mulțimilor) pentru axiomele Dedekind-Peano:

- numerele naturale sînt *ordinalele finite*;
- numărul natural 0 este *mulțimea vidă* \emptyset ;
- funcția succesor este funcția $s : \omega \rightarrow \omega$ care *asociază fiecărui ordinal finit α succesorul său $\alpha \cup \{\alpha\}$* .

Clar, axiomele 1-4 sînt verificate. Să verificăm și axioma inducției:

4.15 Propoziție. *(Teorema inducției pe mulțimea ordinarilor finite) Fie P o clasă de ordinale finite astfel încît $P(\emptyset)$ este adevărată și, $\forall \alpha$ ordinal finit cu $P(\alpha)$ adevărată, rezultă că $P(\alpha \cup \{\alpha\})$ adevărată. Atunci $P(\alpha)$ adevărată pentru orice ordinal finit α .*

Demonstrație. Clasa P corespunde unei submulțimi (notată tot P) a lui ω . Dacă $P \neq \omega$, atunci $\omega \setminus P \neq \emptyset$ și deci $\omega \setminus P$ are un prim element β , cu $\beta \neq \emptyset$ din ipoteza $P(\emptyset)$ adevărată. Fie α predecesorul lui β . Avem $\alpha \notin \omega \setminus P$, deci $P(\alpha)$ adevărată, de unde rezultă $P(\alpha \cup \{\alpha\}) = P(\beta)$ adevărată, adică $\beta \in P$, contradicție cu $\beta \in \omega \setminus P$. □

4.16 Observație. Mulțimea ω a ordinarilor finite este un ordinal (demonstrați!), care nu este finit.

Prin analogie cu \mathbb{N} , se notează cu $<$ relația de ordine strictă pe On (pentru orice ordinale α, β , $\alpha < \beta$ înseamnă deci $\alpha \in \beta$) și cu $\alpha + 1$ succesorul ordinalului α (deci $\alpha + 1 = \alpha \cup \{\alpha\}$).

Alte rezultate despre ordinale sînt propuse ca exerciții. Detalii și dezvoltări ale teoriei ordinalelor pot fi găsite de exemplu în SCORPAN [1996].

În continuare vom identifica mulțimea ordinalelor finite ω cu mulțimea numerelor naturale \mathbb{N} . Notăm cu \leq relația de ordine pe \mathbb{N} (numită relația de ordine uzuală) și cu $n + 1$ succesorul numărului natural (ordinalului finit) n . Prin această identificare, 0 corespunde lui \emptyset , 1 lui $\{\emptyset\}$, ș.a.m.d.; $n + 1$ corespunde lui $n \cup \{n\}$. Observăm că atunci $n = \{0, 1, \dots, n - 1\}$.

Este deosebit de important următorul enunț, care stă la baza raționamentelor prin inducție:

4.17 Teoremă. *Mulțimea numerelor naturale \mathbb{N} este bine ordonată în raport cu relația de ordine uzuală.*

Considerăm utile cîteva remarci și rezultate privind tehnica de *demonstrație prin inducție*, respectiv de *definiție prin recurență*. Mai întîi dăm un rezultat care este cunoscut uneori ca o „variantă a principiului de inducție”:

4.18 Propoziție. *Fie $P(x)$ o expresie cu proprietatea că, pentru orice număr natural n , dacă $P(k)$ este adevărată pentru orice $k < n$, rezultă că $P(n)$ este adevărată. Atunci $P(n)$ este adevărată pentru orice număr natural n . Mai precis, are loc (subînțelegem că toate variabilele sînt în \mathbb{N}):*

$$\{\forall n [(\forall k (k < n \rightarrow P(k)) \rightarrow P(n))\} \rightarrow (\forall n)(P(n)).$$

Demonstrație. Mai întîi observăm că, în condițiile din enunț, $P(0)$ este adevărată. Într-adevăr, pentru $n = 0$ are loc implicația: $[\forall k (k < 0 \rightarrow P(k)) \rightarrow P(0)$. Dar $\forall k (k < 0 \rightarrow P(k))$ este adevărată, deoarece $k < 0$ este falsă pentru orice $k \in \mathbb{N}$ (o expresie de forma $p \rightarrow q$ este adevărată dacă p este falsă!). Deci $P(0)$ adevărată.¹⁷

Presupunem prin absurd că există $n \in \mathbb{N}$ astfel încît $P(n)$ să fie falsă. Atunci mulțimea nevidă $\{n \in \mathbb{N} \mid P(n) \text{ falsă}\}$ are un prim element a . Deci $P(k)$ este adevărată, $\forall k < a$, din modul de alegere a lui a . Cum are loc implicația $(\forall k (k < a \rightarrow P(k)) \rightarrow P(a)$, rezultă că $P(a)$ este adevărată, absurd. \square

Este remarcabil faptul că acest rezultat are loc în *orice mulțime bine ordonată*. Propunem cititorului să reia ideea demonstrației de mai sus pentru a arăta :

4.19 Propoziție. *Fie (A, \leq) o mulțime bine ordonată și fie $P(x)$ o expresie cu proprietatea că, pentru orice $n \in A$, dacă $P(k)$ este adevărată pentru orice $k < n$, $k \in A$, rezultă că $P(n)$*

¹⁷ Așadar, nu are rost să se arate că $P(0)$ este adevărată cînd se folosește acest raționament prin inducție!

adevărată. Atunci $P(n)$ adevărată pentru orice $n \in A$. Mai precis, are loc (subînțelegem că toate variabilele sînt în A):

$$\{\forall n [(\forall k (k < n \rightarrow P(k)) \rightarrow P(n)]\} \rightarrow (\forall n)(P(n)). \quad \square$$

Un exemplu de aplicare a acestei propoziții este demonstrația teoremei polinoamelor simetrice (unde mulțimea bine ordonată este \mathbb{N}^n , cu ordinea lexicografică).

Mai mult, se poate face inducție pe *clase bine ordonate*. Dacă $R(x, y)$ este o relație de ordine, vom scrie, mai sugestiv, $x < y \pmod{R}$ în loc de $R(x, y) \wedge (x \neq y)$. Demonstrația rezultatului ce urmează este similară cu cea de la mulțimi bine ordonate.

4.20 Propoziție. Fie $A(x)$ o clasă bine ordonată de o relație $R(x, y)$ și fie $P(x)$ o expresie cu proprietatea că, pentru orice n din clasa A , dacă $P(k)$ este adevărată pentru orice k din A , cu $k < n \pmod{R}$, rezultă că $P(n)$ adevărată. Atunci $P(n)$ adevărată pentru orice n din A . Mai precis, dacă are loc:

$$\forall n \{ [A(n) \wedge (\forall k (A(k) \wedge k < n \pmod{R}) \rightarrow P(k)) \rightarrow P(n) \},$$

atunci are loc $(\forall n)(A(n) \rightarrow P(n))$. □

În general, astfel de raționamente se fac pe *clasa ordinalelor* On și se numesc raționamente prin *inducție transfinită*.

Strîns legat de principiul demonstrației prin inducție este *definirea șirurilor prin recurență* (numită uneori *definire prin inducție*, denumire improprie, căci inducția este o metodă de demonstrație). De exemplu, este clar că relațiile $x_0 = 1, x_{n+1} = 2x_n + 1, \forall n \in \mathbb{N}$, definesc unic șirul de numere naturale: $x_0 = 1, x_1 = 3, x_2 = 7, x_3 = 15, \dots$

4.21 Definiție. Fie A o mulțime nevidă. Se numește *șir* (indexat după ω)¹⁸, cu valori în A , orice funcție $s : \omega \rightarrow A$ (ω este ordinalul tuturor ordinalelor finite). Mai general, dacă α este un ordinal oarecare, vom numi *șir* (indexat după α) cu valori în A orice funcție definită pe α cu valori în A .

Pentru un șir $s : \alpha \rightarrow A$ se folosesc notații de tipul $(s_i)_{i \in \alpha}$ sau $\{s_i \mid i \in \alpha\}$. Pentru orice $\beta \in \alpha$ (β este deci ordinal!), notăm cu $s|_\beta$ restricția lui s la β ($s|_\beta$ este atunci șir indexat după β). De exemplu, dacă $(s_n)_{n \in \omega}$ este un șir indexat după ω , atunci:

$$s|_0 = s|_\emptyset = \emptyset; \quad s|_1 = s|_{\{0\}} = \{(0, s(0))\}; \quad s|_2 = s|_{\{0,1\}} = \{(0, s(0)), (1, s(1))\}, \dots, \\ s|_n = s|_{\{0,1, \dots, n-1\}} = \{(0, s(0)), (1, s(1)), \dots, (n-1, s(n-1))\}.$$

Ce înseamnă a *defini prin recurență* un șir $(s_n)_{n \in \omega}$? Intuitiv, pentru orice $n \in \omega$, termenul s_n „depinde de termenii precedenți s_0, \dots, s_{n-1} ”, adică este dată o „relație de recurență” de forma $s_n = f(s_0, \dots, s_{n-1})$. Observăm că putem rescrie aceasta sub forma $s_n = f(s|_n)$, folosind notațiile

¹⁸ Reamintim că am identificat \mathbb{N} cu ordinalul ω .

de mai sus. Deci f este o funcție cu domeniul format de mulțimea șirurilor (cu valori în A), indexate după un $n = \{0, 1, \dots, n-1\}$. Mai general, putem da următoarea:

4.22 Definiție. Fie A o mulțime nevidă și α un ordinal. Pentru fiecare $\beta \in \alpha$ notăm cu

$$S_\beta(A) = \{b \mid b : \beta \rightarrow A\}$$

mulțimea șirurilor cu valori în A , indexate după β . Fie

$$S(A, \alpha) = \bigcup_{\beta \in \alpha} S_\beta(A) = \{b \mid (\exists \beta) (\beta \in \alpha \text{ și } b \text{ este funcție de la } \beta \text{ la } A)\}$$

mulțimea șirurilor cu valori în A , indexate după ordinale din α . Dacă $s : \alpha \rightarrow A$ și $\beta \in \alpha$, atunci $s|_\beta \in S_\beta(A) \subseteq S(A, \alpha)$, deci există $f(s|_\beta) \in A$.

O relație de recurență este o funcție $f : S(A, \alpha) \rightarrow A$. Spunem că șirul $s : \alpha \rightarrow A$ este definit recurent de relația de recurență f dacă, $\forall \beta \in \alpha$, avem :

$$s(\beta) = f(s|_\beta).$$

4.23 Teoremă. Fie α un ordinal și A o mulțime. Pentru orice relație de recurență $f : S(A, \alpha) \rightarrow A$ există un unic șir $s : \alpha \rightarrow A$ care este definit recurent de f .

Demonstrație. Unicitatea: presupunem că există două șiruri $s : \alpha \rightarrow A$ și $t : \alpha \rightarrow A$, definite recurent de f , astfel încât $s \neq t$. Deci mulțimea $\{\beta \in \alpha \mid s(\beta) \neq t(\beta)\}$ este nevidă și are un prim element π . Atunci $s(\gamma) = t(\gamma)$, $\forall \gamma \in \pi$, adică $s|_\pi = t|_\pi$. Dar $s(\pi) = f(s|_\pi) = f(t|_\pi) = t(\pi)$, contradicție.

Existența: Notăm cu δ mulțimea ordinarilor β din α pentru care există un șir s_β indexat după β , definit recurent de f , adică: $\delta := \{\beta \in \alpha \mid \exists s_\beta : \beta \rightarrow A \wedge (\forall \gamma \in \beta \rightarrow s_\beta(\gamma) = f(s_\beta|_\gamma))\}$. Evident, $\delta \subseteq \alpha$. Avem de arătat că $\delta = \alpha$.

Afirmăm că δ este un ordinal. E suficient să demonstrăm că δ este segment inițial (vezi 4.6). Observăm că $\emptyset \in \delta$ (funcția $\emptyset : \emptyset \rightarrow A$ este definită recurent de f !), deci δ este nevidă. Fie $\beta \in \delta$. Vrem să arătăm că $\gamma \in \delta$, $\forall \gamma < \beta$. Cum $\beta \in \delta$, există $s : \beta \rightarrow A$ definit recurent de f . Pentru $s|_\gamma$ avem, $\forall \lambda \in \gamma$: $s|_\gamma(\lambda) = s(\lambda) = f(s|_\lambda) = f((s|_\gamma)|_\lambda)$, deci $s|_\gamma$ este definit pe γ și este definit recurent de f . Astfel, $\gamma \in \delta$.

Cum δ este ordinal și $\delta \subseteq \alpha$, avem $\delta = \alpha$ sau $\delta \in \alpha$. Dacă $\delta = \alpha$, am terminat. Presupunem prin absurd că $\delta \in \alpha$.

Observăm că, $\forall \beta \in \delta$, șirul s_β definit recurent de f este unic determinat, din prima parte a demonstrației. Mai mult, $\forall \beta \in \delta$ și $\forall \gamma \in \beta$, restricția lui s_β la γ coincide cu s_γ (tot din unicitate). Definim atunci $s : \delta \rightarrow A$ prin : $\forall \beta \in \delta$, $s(\beta) = f(s_\beta)$. Definiția are sens: s_β este un șir indexat după β (unicul șir definit recurent pe β de f) și există $f(s_\beta) \in A$.

Să demonstrăm că $s : \delta \rightarrow A$ este definit recurent pe δ de f , adică: $\forall \beta \in \delta$ are loc $s(\beta) = f(s|_\beta)$. Comparând cu definiția lui s , aceasta revine la a arăta că $\forall \beta \in \delta$, avem $s|_\beta = s_\beta$.

Fie $\beta \in \delta$ și fie $\gamma \in \beta$. Avem, din cele de mai sus: $s(\gamma) = f(s_\gamma) = f(s_\beta|_\gamma) = s_\beta(\gamma)$, $\forall \gamma \in \beta$. Deci $s|_\beta(\gamma) = s_\beta(\gamma)$, $\forall \gamma \in \beta$, adică $s|_\beta = s_\beta$.

Deci $\delta \in \alpha$ și există $s : \delta \rightarrow A$ definit recurent de f . Din definiția lui δ , avem $\delta \in \delta$, absurd. □

Definițiile prin recurență pe un ordinal oarecare sînt cunoscute ca definiții prin *recurență transfinită*. Acest tip de definiții se utilizează, între altele, în teoria dimensiunii laticelor și a modulelor (vezi de exemplu NĂSTĂSESCU [1983]).

Prezentăm o proprietate foarte importantă a lui \mathbb{N} , a cărei demonstrație ilustrează principiul de demonstrație prin inducție. Se presupun cunoscute operațiile de adunare și înmulțire în \mathbb{N} și proprietățile lor.

4.24 Teoremă (Teorema împărțirii cu rest în \mathbb{N}). *Pentru orice numere naturale a, b , cu $b \neq 0$, există $q, r \in \mathbb{N}$ astfel încît $a = bq + r$ și $r = 0$ sau $r < b$ (q se numește cîtul iar r restul împărțirii lui a la b). În plus, q și r sînt unic determinate cu aceste proprietăți.*

Demonstrație. Fie $b \neq 0$ fixat. Demonstrăm prin inducție după a , aplicînd 4.18. Mai precis, considerăm $P(a): \exists q \exists r (q \in \mathbb{N} \wedge r \in \mathbb{N} \wedge a = bq + r \wedge r < b)$.

Pentru orice $a < b$, $P(a)$ este adevărată, luînd $q = 0$, $r = a$. Presupunem acum că $a \geq b$ și $P(k)$ este adevărată, $\forall k \in \mathbb{N}$, $k < a$. Să demonstrăm $P(a)$. Cum $a \geq b$ avem $a - b \in \mathbb{N}$ și $a - b < a$. Deci are loc $P(a - b): \exists q, r$ astfel încît $a - b = bq + r$ și $r < b$, adică $a = b(q + 1) + r$, cu $r < b$.

Unicitatea: presupunem că $a = bq + r = bt + s$, cu $r < b$ și $s < b$. Pentru a face o alegere, fie $q \geq t$, adică $q - t \geq 0$. Atunci $b(q - t) = s - r$. Cum $s < b$, rezultă că $s - r < b$. Astfel, $b(q - t) < b$, de unde obținem $q - t = 0$ și $s - r = 0$. \square

Teorema împărțirii cu rest este de o importanță covîrșitoare în matematică. O primă aplicație a ei este reprezentarea numerelor naturale într-o bază dată (vezi Exerciții).

Un alt punct de vedere privind ordinalele este descris în continuare.

4.25 Definiție. Fie (A, \leq) și (B, \leq) mulțimi ordonate. O aplicație $\varphi: A \rightarrow B$ se numește *morfism de ordine* (sau *aplicație crescătoare*) dacă $\forall x, y \in A$, din $x \leq y$ rezultă $\varphi(x) \leq \varphi(y)$. Morfismul φ se numește *izomorfism de ordine* dacă φ este bijectivă și inversa sa φ^{-1} este tot morfism. Mulțimile ordonate (A, \leq) și (B, \leq) se numesc *izomorfe* dacă există măcar un izomorfism de ordine $\varphi: A \rightarrow B$, caz în care scriem $A \cong B$.

4.26 Observație. Dacă (A, \leq) și (B, \leq) sînt *total* ordonate, atunci orice morfism bijectiv $\varphi: A \rightarrow B$ este și izomorfism. Demonstrați! Pentru mulțimi ordonate în general, nu orice morfism bijectiv este izomorfism, după cum arată exemplul aplicației identitate $\text{id}: (\mathbb{N}^*, |) \rightarrow (\mathbb{N}^*, \leq)$, unde $(\mathbb{N}^*, |)$ este mulțimea numerelor naturale nenule înzestrată cu relația de ordine divizibilitatea, iar \leq este relația de ordine uzuală.

Comparați rezultatul următor cu 4.9:

4.27 Propoziție. *Fie A și B mulțimi bine ordonate. Atunci are loc exact una din situațiile: $A \cong B$; A izomorf cu un segment inițial al lui B ; B izomorf cu un segment inițial al lui A .* \square

Clasa mulțimilor ordonate izomorfe cu o mulțime ordonată dată (A, \leq) se numește *tipul de ordine* al lui (A, \leq) . Orice mulțime bine ordonată este izomorfă cu un unic ordinal:

4.28 Propoziție. *Fie (A, \leq) o mulțime bine ordonată. Atunci există un unic ordinal (α, \in) izomorf cu (A, \leq) . \square*

Astfel, pentru orice tip de *bună ordine*, există un unic ordinal în acel tip (și, evident, orice ordinal se află într-un unic tip de bună ordine). Din acest motiv, uneori prin *ordinal* se înțelege *un tip de ordine de mulțimi bine ordonate*. Rezultatele enunțate arată echivalența celor două abordări.

I.5. Comentarii și completări privind axiomatica mulțimilor

În această secțiune vom discuta cu titlu informativ anumite aspecte ale teoriei axiomatice a mulțimilor. Pentru detalii, se pot consulta lucrări precum SCORPAN [1996], MANIN [1977].

Sistemul ZF propriu-zis conține 4 axiome și o schemă de axiome: *axioma extensivității*, *axioma reuniunii*, *axioma mulțimii părților*, *schema de axiome a substituției* și *axioma infinității*.

Este de dorit ca orice teorie axiomatică (deci și ZF) să satisfacă următoarele proprietăți:

Consistența (sau *necontradictorialitatea*) teoriei: din axiomele teoriei nu se poate deduce simultan o propoziție și negația ei (adică nu se poate obține o *contradicție*). O teorie care nu este consistentă nu are nici o valoare științifică: *dacă există o propoziție p astfel încât p și $\neg p$ sînt adevărate, atunci orice propoziție q este adevărată* (ceea ce elimină orice interes în stabilirea adevărului unei propoziții). Într-adevăr, este clar că, dacă p și $p \rightarrow q$ sînt adevărate, atunci q este adevărată. Însă p e adevărată din ipoteză, iar $p \rightarrow q$ este $\neg p \vee q$, adevărată căci $\neg p$ este adevărată.

Independența axiomelor: nici o axiomă nu este o consecință a celorlalte. O teorie în care axiomele nu sînt independente nu este însă lipsită de interes (poate fi, cel mult, acuzată de redundanță).

Problemele stabilirii consistenței și independenței unui sistem axiomatic sînt dificile și profunde.

Strîns legată de problema consistenței este *modelarea* unui sistem axiomatic. Se numește *model* al unei teorii axiomatice o structură de obiecte care satisfac axiomele teoriei. Se pot da exemple numeroase: un model al axiomelor geometriei plane este $\mathbb{R} \times \mathbb{R}$, un model pentru axiomele inelului este $(\mathbb{Z}, +, \cdot)$ etc. Are loc următorul rezultat: *o teorie axiomatică este consistentă dacă și numai dacă are un model*.

Se observă că, în exemplele de mai sus, modelele teoriilor sînt obiecte construite în cadrul teoriei (axiomatică) a mulțimilor (care este mai largă decît teoriile respective). O teoremă a lui Gödel afirmă, într-o exprimare neriguroasă, că un model pentru o teorie axiomatice poate fi construit doar într-o teorie mai largă. Așadar, un eventual model pentru ZF (care i-ar demonstra consistența) nu ar putea fi construit decît într-o teorie mai largă. Însă ZF este suficient de cuprinzătoare pentru a putea servi drept fundament al întregii matematici; pe de altă parte, verificarea consistenței unei ipotetice teorii mai largi revine la construcția unei teorii și mai largi ș.a.m.d. Se vede că această cale nu conduce la o demonstrație a consistenței teoriei ZF. Se poate doar presupune că teoria ZF nu conduce la apariția de contradicții (de fapt, am văzut că a fost creată tocmai pentru a elimina contradicțiile apărute în teoria naivă a mulțimilor). În acest sens, este grăitor următorul citat din MANIN [1977], p. 102:

Problema consistenței formale a axiomelor Zermelo-Fraenkel trebuie să rămînă o chestiune de credință, cu excepția cazului cînd o eventuală inconsistență formală este demonstrată. Pînă acum toate demonstrațiile bazate pe aceste axiome nu au dus niciodată la o contradicție; dimpotrivă, au deschis în fața noastră bogata lume a matematicilor clasice și moderne. Această lume are o anumită realitate și o viață proprii, care depind în mică măsură de formalismele alese pentru a le descrie. O descoperire a unei contradicții în oricare din diversele formalisme, chiar dacă ar apărea, ar servi doar la clarificarea, rafinarea și poate reconstrucția unor anumite idei, dar nu ar conduce la falimentul lor, cum s-a întîmplat de mai multe ori în trecut.

Independența axiomelor are și ea legătură cu consistența. Să exemplificăm aceasta pe cazul unei noi axiome, *axioma fundării*.

Axioma fundării (AF). *Orice mulțime nevidă conține un element de care este disjunctă:*

$$(\forall a)[a \neq \emptyset \rightarrow (\exists b)(b \in a \wedge b \cap a = \emptyset)].$$

Acest enunț implică: *Nici o mulțime nu este element al ei însăși.* Într-adevăr, dacă avem o mulțime x astfel încît $x \in x$, atunci $\{x\}$ contrazice axioma fundării: singurul element al lui $\{x\}$ este x și avem $x \cap \{x\}$ nevidă, căci conține pe x . Mai mult, nu există „lanțuri de mulțimi” de forma $x_0 \in x_1 \in x_2 \in \dots \in x_n \in x_0$. Dacă ar exista un asemenea lanț, atunci mulțimea $\{x_0, x_1, \dots, x_n\}$ contrazice AF (de ce?). La fel, nu poate exista un șir $(x_n)_{n \in \omega}$ astfel încît $x_{n+1} \in x_n, \forall n \in \omega$. AF își datorează numele faptului că, pentru orice mulțime x , orice lanț de forma $x \ni x_0 \ni x_1 \ni \dots \ni x_n \ni \dots$ este finit și se termină cu \emptyset : $\exists n$ astfel încît $x \ni x_0 \ni x_1 \ni \dots \ni x_n \ni \emptyset$: orice șir descrescător (față de relația \in) este finit și „fundat” pe \emptyset .¹⁹

S-a demonstrat că, dacă acceptăm că ZF este consistentă, atunci ZF + AF (sistemul ZF la care se adaugă AF) nu conduce la contradicții. Această probare a *consistenței relative* a AF s-a realizat prin construirea unui model (în cadrul ZF) care satisface ZF + AF. În plus, s-a

¹⁹ Astfel, întregul univers descris de ZF și AF este "creat" pornind de la \emptyset (universul "von Neumann", vezi MANIN [1977], p. 95-102).

construit un alt model (tot în cadrul ZF) care satisface ZF și *negația AF*. Din aceste două rezultate se vede că AF este independentă de ZF (nu poate fi dedusă din axiomele ZF).

Un alt rezultat în această direcție este demonstrarea *independenței axiomei infinității față de restul axiomelor ZF*, printr-un procedeu principal asemănător cu cel de mai sus.

Axioma alegerii (AC)²⁰ este o nouă axiomă care joacă un rol deosebit în matematică, datorită faptului că, pe de o parte, are un enunț aparent „evident”; pe de altă parte, are un caracter neconstructiv care i-a atras multe critici. Există multe enunțuri echivalente cu această axiomă. În formularea lui Zermelo, AC se enunță:

*Pentru orice mulțime A în care elementele sînt disjuncte două cîte două*²¹, *există o mulțime care conține exact un element din fiecare mulțime nevidă din A :*

$$(\forall A)[(\forall x)(\forall y)(x \in A \wedge y \in A \wedge x \neq y) \rightarrow x \cap y = \emptyset] \rightarrow (\exists c)[(\forall x)(x \in A \wedge x \neq \emptyset) \rightarrow (\exists z)(c \cap x = \{z\})].$$

Altfel spus, putem „alege” cîte un element din fiecare mulțime nevidă din A și forma cu ele o nouă mulțime. Controversele privind această axiomă provin și din faptul că se postulează existența unei astfel de mulțimi și implicit a unui „procedeu de alegere” a unui element dintr-o mulțime nevidă. În 1963 s-a demonstrat că AC nu poate fi dedusă din ZF. În majoritatea matematicilor contemporane, AC este acceptată alături de ZF, în sistemul numit ZFC.

Există numeroase enunțuri echivalente cu Axioma Alegerii. Iată cîteva:

Principiul bunei ordonări (Zermelo 1904). *Orice mulțime nevidă A poate fi bine ordonată (există o relație de bună ordine pe A).*

Produsul cartezian al unei familii de mulțimi nevide este nevid.

*Pentru orice mulțime a, există o funcție de alegere $f: a \rightarrow \bigcup a$ (adică f are proprietatea că, $\forall x \in a, x \neq \emptyset \rightarrow f(x) \in x$).*²²

Pentru orice funcție surjectivă $\varphi: E \rightarrow F$ există $\psi: F \rightarrow E$ astfel încît $\varphi\psi = id_F$.

Lema lui Zorn. *Fie (A, \leq) o mulțime ordonată nevidă în care orice submulțime total ordonată este majorată (mulțime „inductiv ordonată”). Atunci A conține un element maximal.*

Lema lui Zorn este folosită în algebră în demonstrarea unor teoreme importante: existența unei baze într-un spațiu vectorial oarecare, existența idealelor maximale într-un inel, existența închiderii algebrice a unui corp comutativ.

²⁰ Acronimul expresiei Axiom of Choice.

²¹ Reamintim că elementele lui A sînt tot mulțimi.

²² Altfel spus, funcția f "alege" cîte un element f(x) din fiecare mulțime nevidă x ∈ a.

I.6. Cardinali

În continuare prezentăm câteva noțiuni de *teoria cardinalilor*. Pentru o tratare mai în detaliu, vezi MIRON, NĂSTĂSESCU [1974], SCORPAN.

6.29 Definiție. Fie A și B două mulțimi. Spunem că A și B sînt *echipotente* (sau că sînt *cardinal echivalente*, sau că *au același cardinal*) dacă există o bijecție $f: A \rightarrow B$. Scriem atunci $A \sim B$ sau $|A| = |B|$.

Pentru orice mulțimi A, B, C , au loc:

- $A \sim A$ (reflexivitate);
- Dacă $A \sim B$, atunci $B \sim A$ (simetrie);
- Dacă $A \sim B$ și $B \sim C$, atunci $A \sim C$ (tranzitivitate).

Astfel, putem spune că relația de echipotență " \sim " este o relație de echivalență pe clasa mulțimilor. Clasa²³ tuturor mulțimilor echipotente cu o mulțime dată A se numește *cardinalul mulțimii A* și se notează $\text{card } A$ sau $|A|$. Spunem că A este o mulțime *finită* cu n elemente ($n \in \mathbb{N}$) dacă $A \sim \{1, \dots, n\}$ și atunci notăm $|A| = |\{1, \dots, n\}| =: n$. O mulțime care nu este finită se numește *infinită*.

Se poate demonstra că: *mulțimea A este infinită* \Leftrightarrow *există o funcție injectivă $\varphi: A \rightarrow A$ care nu este surjectivă* \Leftrightarrow *există o funcție injectivă $\psi: \mathbb{N} \rightarrow A$* .

Dacă $|A| = |\mathbb{N}|$, spunem că A este o mulțime *numărabilă*.

Se introduce o *relație de ordine* între cardinali: spunem că $|A| \leq |B|$ dacă există o funcție injectivă $\varphi: A \rightarrow B$. Definiția este corectă: dacă $A \sim A'$, $B \sim B'$ și există o funcție injectivă $\varphi: A \rightarrow B$, atunci există o funcție injectivă $\varphi': A' \rightarrow B'$ (demonstrați!).

Se verifică imediat că, pentru orice mulțimi A, B, C are loc:

- $|A| \leq |A|$ (*reflexivitate*);
- $|A| \leq |B|$ și $|B| \leq |C|$ implică $|A| \leq |C|$ (*tranzitivitate*);

Are loc următoarea teoremă importantă, care arată că \leq este și *antisimetrică* (deci are într-adevăr aceleași proprietăți ca o relație de ordine).

6.30 Teoremă. (Cantor-Schröder-Bernstein) *Fie A și B două mulțimi. Dacă $|A| \leq |B|$ și $|B| \leq |A|$, atunci $|A| = |B|$.*

Demonstrație. Idee: să găsim $D \subseteq A$ astfel încît $A \setminus D \subseteq \text{Img}$ și $\alpha: A \rightarrow B$, dată de:

$$\alpha(a) = \begin{cases} f(a) & \text{dacă } a \in D \\ g^{-1}(a) & \text{dacă } a \notin D \end{cases}$$

să fie o bijecție (faceți un desen!). Trebuie să avem atunci $A \setminus D = g(B \setminus f(D))$, adică $D = A \setminus g(B \setminus f(D))$.

²³ Nu putem vorbi de "mulțimea tuturor mulțimilor echipotente cu A ".

Pentru a găsi D ca mai sus, definim $\varphi : \mathcal{P}(A) \rightarrow \mathcal{P}(A)$, $\varphi(E) := A \setminus g(B \setminus f(E))$, $\forall E \in \mathcal{P}(A)$. Noi căutăm un D cu $\varphi(D) = D$.

Se arată ușor că φ este crescătoare: dacă $E \subseteq F$, atunci $\varphi(E) \subseteq \varphi(F)$.

Definim $M := \{E \subseteq A \mid E \subseteq \varphi(E)\}$. Evident, M este nevidă căci, de exemplu, $\emptyset \in M$.

Fie $D := \bigcup \{E \mid E \in M\}$. Să arătăm că $\varphi(D) = D$. Avem $\varphi(D) = \varphi(\bigcup \{E \mid E \in M\}) = \bigcup \{\varphi(E) \mid E \in M\} \supseteq \bigcup \{E \mid E \in M\} = D$. Deci $D \subseteq \varphi(D)$. Aplicând φ acestei incluziuni, obținem $\varphi(D) \subseteq \varphi(\varphi(D))$ adică $\varphi(D) \in M$. De aici, $D = \bigcup \{E \mid E \in M\} \supseteq \varphi(D)$. Astfel, $\varphi(D) = D$. Lăsăm cititorului verificarea faptului că α este bijecție. \square

Relația de ordine \leq este și totală (demonstrația face apel la Axioma Alegerii):

6.31 Teoremă. Oricare ar fi două mulțimi A, B , are loc $|A| \leq |B|$ sau $|B| \leq |A|$. \square

Această ultimă proprietate este echivalentă cu Axioma Alegerii.

Exerciții

1. Demonstrați că axioma infinității este echivalentă cu enunțul: *Există un ordinal infinit.*
2. Demonstrați că clasa ordinalelor On nu este mulțime („paradoxul Burali-Forti”).
3. Demonstrați că reuniunea unei mulțimi A de ordinale este un ordinal și este marginea superioară a lui A în On .
4. Un ordinal se numește *ordinal limită* dacă nu are un predecesor. Arătați că ω este cel mai mic ordinal limită și că axioma infinității este echivalentă cu afirmația: *Există un ordinal limită.* Care este succesorul lui ω ?
5. Arătați că ordinalul α este ordinal limită dacă și numai dacă $\alpha = \sup \{\beta \mid \beta \in \alpha\}$ (margine superioară în On).
6. Inducția transfinită (pe clasa ordinalelor On) se face adesea distingând cazul ordinalelor limită. Mai precis, demonstrați că dacă o expresie $P(x)$ are proprietățile:
 - a) $P(\emptyset)$ adevărată;
 - b) $\forall \alpha [(On(\alpha) \wedge P(\alpha)) \rightarrow P(\alpha + 1)]$;
 - c) Pentru orice ordinal limită λ , dacă $P(\beta)$ adevărată, $\forall \beta < \lambda$, atunci $P(\lambda)$ adevărată,
 atunci $P(\alpha)$ adevărată pentru orice ordinal α .
7. Axioma infinității face referire la mulțimea vidă \emptyset , a cărei existență rezultă din existența măcar a unei mulțimi. Dar acest lucru este asigurat de axioma infinității. Cum se poate ieși din acest (aparent) cerc vicios?
8. Arătați că, pentru orice mulțime A , are loc $|\mathcal{P}(A)| > |A|$.

9. (Reprezentarea unui număr în baza b) Fie b un număr natural nenul fixat (numit *bază de numerație*). Demonstrați că, $\forall a \in \mathbb{N}$, există și sînt unice $n \in \mathbb{N}^*$ și $c_0, \dots, c_{n-1} \in \{0, 1, \dots, b-1\}$, astfel încît

$$a = c_{n-1}b^{n-1} + \dots + c_1b + c_0 \quad (R)$$

În cazul în care are loc egalitatea (R) de mai sus, se mai scrie $a = \overline{c_{n-1} \dots c_1 c_0}$, scriere numită *reprezentarea lui a în baza b* . Numerele naturale $0, 1, \dots, b-1$ se numesc *cifre*²⁴ în baza b (pentru scrierea concretă se dau b simboluri care reprezintă aceste cifre și nu se folosește bara superioară, scrisă aici pentru a evita confuzia cu produsul $c_{n-1} \dots c_1 c_0$). Uneori, în notație, se mai specifică baza b , ca indice. De exemplu, $105_7 = 54_{10}$. (Ind. Din teorema împărțirii cu rest aplicată lui a și b , $\exists! q, r \in \mathbb{N}$ astfel încît $a = bq + r$. Se pune $c_0 = r$ și se repetă procedeul pentru q – sau, mai riguros, se aplică o inducție după a . Pentru unicitate, se observă că c_0 este restul împărțirii lui a la b și se aplică o inducție după cel mai mic număr de cifre din ipoteticele reprezentări ale lui a în baza b).

10. Reprezentați în baza 10 numerele $1011_2, 1212_3$. Scrieți în bazele 2, 7, 16, numerele $129_{10}, 1152_{10}$.

²⁴ A se remarca distincția între *număr* și *cifră* (într-o bază fixată). De exemplu, cifrele în baza 16 (sistem *hexadecimal*) sînt 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, unde A reprezintă pe 10 [scris în baza zece], B pe 11, ...

II. Mulțimi factor și construcții de structuri numerice fundamentale

Presupunând cunoscută mulțimea \mathbb{N} a numerelor naturale, înzestrat cu operațiile de adunare și înmulțire (cu proprietățile cunoscute) și cu structura sa de ordine uzuală (\mathbb{N} este o mulțime *bine ordonată*), se pune problema *construirii celorlalte structuri numerice de bază*: \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} , la care putem adăuga inelele de clase de resturi \mathbb{Z}_n .

Se impune un comentariu privind noțiunea de „număr”. În multe cărți se pun întrebări (probleme) de genul „ce este *numărul* (eventual rațional sau real sau complex)”, urmînd ca autorul să dea un răspuns de natură filozofică sau matematică. Noțiunea de *număr* (privit ca element individual, izolat) nu are o semnificație deosebită în matematică, mult mai importantă fiind cea de *structură pe o mulțime numerică*. Astfel, de pildă mulțimea \mathbb{R} a numerelor reale este importantă prin *structurile* cu care este înzestrată: structura *algebrică* de corp comutativ, cea de *ordine* (este total ordonată și orice submulțime majorată are supremum), cea *topologică* derivată din acestea (este spațiu metric complet); un număr real, luat ca element individual al lui \mathbb{R} , nu poate fi pus nicidecum în legătură cu astfel de proprietăți. Insistăm asupra acestei distincții pentru că o conștientizare a ei își poate pune amprenta și asupra stilului de predare a acestor concepte fundamentale.

II.1. Relații de echivalență și mulțimi factor

Relațiile de echivalență sînt un instrument esențial în matematică, mai ales în problemele de *construcții* de obiecte (structuri) noi. Vom descrie un procedeu general, *construcția mulțimii factor (cît) în raport cu o relație de echivalență*, care, aplicat în diverse cazuri particulare, duce la construcții importante. Trebuie subliniat că mulțimea factor obținută se înzestreaază cu o structură care este de obicei legată de structura mulțimii inițiale (cea ce presupune o *compatibilitate între relația de echivalență și structura inițială*). Această metodă permite construcția unor structuri matematice importante: \mathbb{Z} (construit ca mulțime factor a lui $\mathbb{N} \times \mathbb{N}$), \mathbb{Q} (mulțime factor a lui $\mathbb{Z} \times \mathbb{Z}^*$; același procedeu dă în general inele și corpuri de fracții), \mathbb{R} (mulțime factor a mulțimii șirurilor Cauchy de numere raționale), \mathbb{C} (mulțime

factor a inelului de polinoame $\mathbb{R}[X]$). Remarcăm că majoritatea construcțiilor în matematică sînt mulțimi factor în raport cu o anumită relație de echivalență: produsul tensorial a două module, grupul liber pe o mulțime, spațiile proiective din geometrie, spațiile L^p din analiză, ... și lista este departe de a fi completă.

Fie A o mulțime și ρ o relație de echivalență pe A . Mulțimea

$$\{x \in A \mid x\rho a\}$$

poartă numele de *clasa de echivalență* a elementului a relativ la relația ρ și se notează cu \hat{a} . Se folosesc adesea multe alte notații, depinzînd de cazul particular ales și de dorința de a include sau nu relația ρ în notație. De exemplu, clasa lui a se mai notează $C_a, \bar{a}, \hat{a}_\rho, [a]_\rho$ etc.

Dacă pentru elementele a și b are loc $a\rho b$, mai spunem că a și b sînt *echivalente modulo* ρ .

1.1 Definiție. Mulțimea claselor de echivalență în raport cu relația ρ se numește *mulțimea cît* (sau *factor*) a lui A în raport cu ρ și se notează cu A/ρ . Deci $A/\rho := \{\hat{a} \mid a \in A\}$.

1.2 Propoziție. Fie ρ o relație de echivalență pe A . Atunci:

a) $\forall a \in A$ are loc $a \in \hat{a}$ (deci \hat{a} este nevidă).

b) $\forall a, b \in A$, avem: $\hat{a} = \hat{b} \Leftrightarrow a\rho b$.

c) $\forall a, b \in A$, are loc fie $\hat{a} = \hat{b}$, fie $\hat{a} \cap \hat{b} = \emptyset$.

d) $\bigcup_{a \in A} \hat{a} = A$. □

O mulțime P de submulțimi nevide ale lui A , disjuncte două cîte două, a căror reuniune este A , este numită *partiție* a lui A . Mai precis, P este *partiție a lui A* dacă:

a) $\forall B (B \in P) \rightarrow B \neq \emptyset$;

b) $\forall B [(B \in P) \wedge (C \in P) \wedge (B \neq C)] \rightarrow (B \cap C = \emptyset)$;

c) $\bigcup \{B \mid B \in P\} = A$.

Propoziția anterioară nu spune altceva decît că *mulțimea factor a lui A în raport cu o relație de echivalență este o partiție a lui A*. Reciproc, orice partiție poate fi obținută dintr-o relație de echivalență:

1.3 Propoziție. Fie P o partiție a mulțimii A . Atunci relația ρ definită prin:

$$\forall a, b \in A, a\rho b \Leftrightarrow \exists B \in P \text{ astfel încît } a \in B \text{ și } b \in B$$

este o relație de echivalență pe A și P este chiar mulțimea cît A/ρ . □

În aplicații, mulțimea inițială are de obicei o *structură* (algebrică, topologică, de ordine, ...), iar relația de echivalență este *compatibilă* cu structura dată (sensul precis al acestei compatibilități fiind definit în fiecare caz în parte; în general, definiția este „naturală”). Atunci mulțimea factor obținută va moșteni o structură de același tip ca mulțimea inițială. Vom prezenta exemple de aplicare în algebră a acestei construcții fundamentale (trecerea de la o mulțime la mulțimea factor în raport cu o relație de echivalență) în paragrafele următoare.

Un concept important este cel de *sistem de reprezentanți*.

1.4 Definiție. Fie ρ o relație de echivalență pe mulțimea A . Spunem că submulțimea $S \subseteq A$ este un *sistem de reprezentanți*²⁵ pentru clasele de echivalență (modulo ρ) dacă orice element din A este echivalent modulo ρ cu exact un element din S . Intuitiv, un sistem de reprezentanți se obține „alegînd” din fiecare clasă de echivalență cîte un element („reprezentantul” clasei respective). Astfel S este sistem de reprezentanți dacă și numai dacă:

$$(\forall a \in A)(\exists s \in S)(a \rho s) \wedge (\forall s, t \in S)(s \rho t \rightarrow s = t).$$

1.5 Exerciții. a) Fie relația de echivalență definită pe \mathbb{R}^2 (identificat cu un plan în care s-a ales un sistem de coordonate Oxy): $(x, y) \sim (z, t) \Leftrightarrow x = z$. Clasele de echivalență sînt dreptele paralele cu Oy . Un sistem de reprezentanți este (de exemplu) $\{(x, 0) \mid x \in \mathbb{R}\}$. Mulțimea factor \mathbb{R}^2 / \sim este în bijecție cu \mathbb{R} . Cum se poate defini o relație de echivalență pe \mathbb{R}^2 astfel încît clasele de echivalență să fie dreptele paralele cu o dreaptă fixată ce trece prin origine, de ecuație $y = \alpha x$?

b) Puteți defini o relație de echivalență pe \mathbb{R}^2 astfel încît clasele de echivalență să fie cercurile concentrice cu centrul în origine? Dar pătrate centrate în origine, cu laturile paralele cu axele? Dar pătrate centrate în origine, cu laturile paralele cu bisectoarele sistemului de axe?

c) Pe \mathbb{R} definim relația de „congruență modulo \mathbb{Z} ”: pentru $x, y \in \mathbb{R}$, spunem că $x \equiv y \pmod{\mathbb{Z}}$ dacă $x - y \in \mathbb{Z}$. Un sistem de reprezentanți este dat de intervalul $[0, 1)$. Acesta este un caz particular de grup factor (în cazul nostru \mathbb{R}/\mathbb{Z}).

d) *Închiderea tranzitivă a unei relații.* Fie ρ o relație pe mulțimea A . Definim o nouă relație τ_ρ pe A , astfel: $\forall a, b \in A, a \tau_\rho b \Leftrightarrow \exists n \in \mathbb{N}$ și $x_1, \dots, x_n \in A$ astfel încît $a = x_1, b = x_n$ și $x_i \rho x_{i+1}, i = 1, \dots, n - 1$. Atunci τ_ρ este o relație *tranzitivă* pe A . Mai mult, τ_ρ este cea mai mică (în sensul incluziunii) relație tranzitivă pe A care include relația ρ .

II.2. Inelul numerelor întregi

Necesitatea considerării numerelor negative apare din considerente practice, binecunoscute cititorilor (pentru a modela situații precum: temperaturi negative, datorii în conturi bancare etc.), dar și din considerente matematice: diferența a două numere naturale nu este întotdeauna definită ca un număr natural. Formulată altfel, nu pentru orice $a, b \in \mathbb{N}$ ecuația $x + a = b$ are soluții $x \in \mathbb{N}$.

De aici apare și ideea de a concepe un „număr întreg negativ” ca o *diferență* de numere naturale. Bineînțeles, pentru o „diferență” dată există mai multe (chiar o infinitate de) perechi de numere naturale care au aceeași diferență: de exemplu perechile $(0, 1), (1, 2), (2, 3), \dots$ au

²⁵ O denumire mai corectă, dar mai greu de manipulat, este *sistem complet și independent de reprezentanți*.

aceeași diferență (numărul întreg -1). Ar trebui deci să vedem un număr întreg ca pe o pereche de numere naturale (de forma (a, b)), cu convenția că „se consideră egale” două perechi (a, b) și (c, d) dacă $a - b = c - d$. Cum scăderea nu este definită pentru orice pereche de numere naturale, rescriem această condiție sub forma $a + d = b + c$. Exprimăm riguros aceste considerații euristice:

Pe mulțimea $\mathbb{N} \times \mathbb{N}$ se consideră relația \sim , definită prin:

$$\forall (a, b), (c, d) \in \mathbb{N} \times \mathbb{N} : (a, b) \sim (c, d) \Leftrightarrow a + d = b + c$$

Se demonstrează (verificați!) că aceasta este o relație de echivalență. O clasă de echivalență în raport cu această relație o numim *număr întreg*, iar mulțimea factor $\mathbb{N} \times \mathbb{N}/\sim$ se numește *mulțimea numerelor întregi* și se notează cu \mathbb{Z} .

Notăția \mathbb{Z} provine de la cuvântul german *zahl* (pronunțat *țal*, cu un *a* lung), care înseamnă *număr*. A se observa grafia (\mathbb{Z} și nu Z), litera \mathbb{Z} scrisă astfel fiind rezervată exclusiv notării mulțimii numerelor întregi (după cum \mathbb{N} este folosită exclusiv pentru mulțimea numerelor naturale).

Nu ne putem opri aici cu construcția. Trebuie arătat că obiectul pe care l-am construit (riguros) satisface toate proprietățile pe care ne-am aștepta să le aibă mulțimea numerelor întregi: „include” mulțimea \mathbb{N} , orice număr întreg este sau număr natural, sau opusul unui număr natural, este definită o adunare și o înmulțire în raport cu care este inel, este o mulțime total ordonată, iar ordinea este compatibilă cu adunarea și înmulțirea.

Mai întâi să determinăm un sistem de reprezentanți. Mulțimea

$$Z := \{(a, 0) \mid a \in \mathbb{N}\} \cup \{(0, a) \mid a \in \mathbb{N}^*\}$$

este sistem de reprezentanți: dacă $a \geq b$, atunci $(a, b) \sim (a - b, 0)$, iar dacă $a < b$, atunci $(a, b) \sim (0, b - a)$. Vom *identifica* numărul natural a cu clasa de echivalență a lui $(a, 0)$ (lucru permis de faptul că aplicația care duce a în $(a, 0)$ este injectivă de la \mathbb{N} la $\mathbb{N} \times \mathbb{N}/\sim$, demonstrați!) și vom nota cu $-a$ clasa de echivalență a lui $(0, a)$. Ce mai trebuie verificat pentru a demonstra că Z , definit mai sus, este sistem de reprezentanți?

Cu aceste identificări, putem scrie:

$$\mathbb{Z} = \{a \mid a \in \mathbb{N}\} \cup \{-a \mid a \in \mathbb{N}^*\}.$$

Să definim *operațiile de adunare și înmulțire* pe \mathbb{Z} (pornind de la cele de pe \mathbb{N}). Pentru aceasta, se definesc operații pe clasele de echivalență din $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$, folosind reprezentanți oarecare, urmînd să se demonstreze că nu depind de reprezentanți și deci sînt corect definite. De exemplu, notînd cu $\overline{(a, b)} \in \mathbb{N} \times \mathbb{N}/\sim$ clasa lui $(a, b) \in \mathbb{N} \times \mathbb{N}$, definim

$$\overline{(a, b)} + \overline{(c, d)} := \overline{(a + c, b + d)}.$$

Bineînțeles, $a + c$ semnifică suma în \mathbb{N} a numerelor naturale a și c . Operația este *corect definită*.²⁶ Aceasta înseamnă că, $\forall (a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$ cu $(a, b) \sim (a', b')$ și $(c, d) \sim (c', d')$, atunci $(a + c, b + d) \sim (a' + c', b' + d')$. Verificarea este ușoară și constă în aplicarea definițiilor relației de echivalență și a operației $+$.

Invităm cititorul să definească înmulțirea, să demonstreze corectitudinea definiției și proprietățile uzuale ale operațiilor, care conferă lui \mathbb{Z} structură de *inel comutativ și unitar, fără divizori ai lui 0* (se mai spune că \mathbb{Z} este *inel integru* sau *domeniu de integritate*).

Relația de ordine pe \mathbb{Z} : fie $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$. Spunem că $\overline{(a, b)} \leq \overline{(c, d)}$ dacă și numai dacă $a + d \geq b + c$ în \mathbb{N} (de ce am definit astfel?). Demonstrați corectitudinea definiției și faptul că se obține o *relație de ordine totală* pe $\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim$.

Se mai pot defini operațiile pe \mathbb{Z} (respectiv relația de ordine pe \mathbb{Z}) folosind sistemul de reprezentanți Z de mai sus și operațiile din \mathbb{N} (cum?). Ce avantaje și dezavantaje au cele două abordări?

O funcție deosebit de importantă este funcția *valoare absolută* (sau *modul*) $|\cdot| : \mathbb{Z} \rightarrow \mathbb{Z}$,

$$|x| = \begin{cases} x & \text{dacă } x \geq 0 \\ -x & \text{dacă } x < 0 \end{cases}$$

Importanța acestei funcții apare în legătură cu faptul că \mathbb{Z} este *inel euclidian*, adică are loc:

2.1 Teoremă. (Teorema împărțirii cu rest în \mathbb{Z}) *Pentru orice numere întregi a, b , cu $b \neq 0$, există $q, r \in \mathbb{N}$, astfel încât $a = bq + r$, cu $r = 0$ sau $|r| < |b|$ (q se numește cît, iar r rest al împărțirii lui a la b). Dacă se impune și $r > 0$, q și r sînt unic determinate cu aceste proprietăți.* □

II.3. Corpul numerelor raționale

În gimnaziu, se introduc mai întîi doar numerele raționale *pozitive*, din motive didactice. Această distincție oarecum artificială nu își are locul aici. Din punct de vedere algebric, construcția lui \mathbb{Q} pornind de la \mathbb{Z} este principial aceeași cu construcția *corpului de fracții al unui inel integru oarecare* R .

Introducerea lui \mathbb{Q} este motivată, printre altele, de imposibilitatea efectuării unor împărțiri în \mathbb{Z} . De exemplu, nu este definit rezultatul (cîtul) împărțirii lui 3 la 2; altfel spus, ecuația $3x = 2$ nu are soluții în \mathbb{Z} . Mai general, dacă $b, a \in \mathbb{Z}$ și a nu divide b , ecuația $bx = a$ nu are

²⁶ Subliniem că necesitatea demonstrării corectitudinii definiției apare tot timpul cînd se dau definiții pe o mulțime factor, folosind reprezentanți oarecare ai claselor.

soluții în \mathbb{Z} . Apare ideea (similară cu aceea de la construcția precedentă a lui \mathbb{Z}) de a introduce o nouă mulțime de numere (numerele *raționale*) ca fiind „toate cîturile posibile de numere întregi”. De exemplu, cîtul împărțirii lui 3 la 2 va fi „numărul rațional” („fracția”) $3/2$. Deoarece același cît este dat și de împărțirea lui 6 la 4 (sau a lui 9 la 6 etc.), este necesar să precizăm *cînd două fracții a/b și c/d sînt egale*. Aceasta revine la a defini o relație de echivalență pe mulțimea perechilor de forma (a, b) , cu $a, b \in \mathbb{Z}$, $b \neq 0$ (o fracție va fi o clasă de echivalență de perechi). Relația de echivalență este definită de

$$\forall (a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*, (a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Cîtitorul poate demonstra ușor că este vorba într-adevăr de o relație de echivalență.

O clasă de echivalență (un element al mulțimii $\mathbb{Z} \times \mathbb{Z}^* / \sim$) este notată cu a/b sau $\frac{a}{b}$ și este numit(ă) *fracție*; a este *numărătorul*, iar b este *numitorul* fracției a/b . Mulțimea fracțiilor (mulțimea cît $\mathbb{Z} \times \mathbb{Z}^* / \sim$) se notează prin tradiție cu \mathbb{Q} (de la inițiala cuvîntului *quotient*, care înseamnă *cît* în engleză și în franceză). Mulțimea \mathbb{Z} se poate identifica cu o parte a lui \mathbb{Q} : numărul întreg a se identifică cu fracția $\frac{a}{1}$. Pe \mathbb{Q} se introduc operațiile de adunare și înmulțire, inspirate de regulile cunoscute din gimnaziu (aducerea la același numitor etc.):

$$\forall a/b, c/d \in \mathbb{Q}, \frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}; \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

Ca și la construcția lui \mathbb{Z} , trebuie arătat că *definițiile sînt corecte* (nu depind de alegerea reprezentanților fracțiilor) și că \mathbb{Q} , înzestrat cu aceste operații, este *inel comutativ unitar* (elementul nul este fracția $0/1$, iar elementul unitate este fracția $1/1$). Mai mult, \mathbb{Q} este *corp*: orice element nenul $\frac{a}{b}$ are invers față de înmulțire: $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

Importanța construcției de mai sus depășește cadrul elementar al construcției lui \mathbb{Q} ; aceeași idee, cu modificări minore, se aplică la *construcția inelului de fracții al unui inel comutativ relativ la un sistem multiplicativ închis* al său, construcție fundamentală în toată matematica.

Rămîne să definim ordinea uzuală pe \mathbb{Q} .

3.2 Definiție. Fie a/b și $c/d \in \mathbb{Q}$, unde $a, b, c, d \in \mathbb{Z}$, cu $b, d > 0$. Definim:

$$a/b \leq c/d \Leftrightarrow ad \leq bc.$$

Corectitudinea definiției este propusă ca exercițiu.

3.3 Definiție. Un corp comutativ $(K, +, \cdot)$ se numește *corp ordonat* dacă este înzestrat cu o relație de ordine totală " \leq " pe K astfel încît, $\forall a, b, c \in K$, au loc:

- i) $a \leq b \Rightarrow a + c \leq b + c$;
- ii) $a \leq b$ și $c \geq 0 \Rightarrow ac \leq bc$.

\mathbb{Q} este un corp ordonat față de relația de ordine uzuală; mai mult, orice relație de ordine pe \mathbb{Q} în raport cu care acesta devine un corp ordonat coincide cu ordinea uzuală (vezi Exerciții).

O funcție deosebit de importantă pentru un corp ordonat K este *valoarea absolută (modulul)* $|| : K \rightarrow K$, definit la fel ca valoarea absolută pe \mathbb{Z} :

$$|x| = \begin{cases} x & \text{dacă } x \geq 0 \\ -x & \text{dacă } x < 0 \end{cases}$$

Exerciții

1. Demonstrați că orice element din \mathbb{Q} se poate scrie ca o fracție a/b , cu $a, b \in \mathbb{Z}$ și $b > 0$.
2. Demonstrați că relația de ordine uzuală pe \mathbb{Q} (vezi def. II.3.2) este corect definită și \mathbb{Q} devine corp ordonat.
3. Fie $(K, +, \cdot, \leq)$ un corp ordonat, cu element nul 0 și element unitate 1. Atunci, $\forall a, b, c \in K$, au loc: a) $a \leq b \Rightarrow -a \geq -b$; b) $0 < 1$; c) $0 < n \cdot 1, \forall n \in \mathbb{N}$; d) $0 < a$ și $0 < b \Rightarrow 0 < ab$ și $0 < a^{-1}$; e) $0 < a < b \Rightarrow 0 < b^{-1} < a^{-1}$.
În particular, car $K = 0$ (adică $n \cdot 1 \neq 0, \forall n \in \mathbb{N}^*$) și există un unic morfism de corpuri $\varphi : \mathbb{Q} \rightarrow K$. Morfismul φ este cu necesitate injectiv; arătați că este și morfism de ordine.
4. Demonstrați că relația de ordine uzuală este singura relație de ordine pe \mathbb{Q} în raport cu care acesta devine corp ordonat.
5. Fie K un corp ordonat. Demonstrați că funcția valoare absolută $|| : K \rightarrow K$ are proprietățile uzuale ale modulului: a) $\forall x \in K \Rightarrow |x| \geq 0$; b) $\forall x \in K$, are loc: $|x| = 0 \Leftrightarrow x = 0$; c) $\forall x, y \in K \Rightarrow |x + y| \leq |x| + |y|$ (inegalitatea triunghiulară); d) $\forall x, y \in K \Rightarrow |x \cdot y| = |x| \cdot |y|$.
6. Arătați că nu orice submulțime nevidă majorată a lui \mathbb{Q} are margine superioară.

II.4. Corpul numerelor reale

Necesitatea introducerii numerelor întregi și a celor raționale este aproape evidentă din experiența imediată. Nu acesta este cazul numerelor reale, care au apărut din rațiuni mai profunde. Descoperirea de către matematicienii Greciei antice că diagonala pătratului de lungime 1 nu poate fi exprimată ca un raport de numere întregi (în termeni moderni, $\sqrt{2} \notin \mathbb{Q}$) a condus la o adevărată criză a științei și filozofiei în acea vreme.

Imaginea intuitivă cea mai simplă despre \mathbb{R} , care reflectă cel mai bine structura de ordine, este cea a punctelor de pe o *dreaptă* (alt concept abstract, dar mai accesibil gândirii), unde s-a fixat un punct O (*originea*, corespunzând lui 0) și un alt punct U , diferit de primul (corespunzător lui 1 și avînd rolul de a fixa unitatea de măsură pe acea dreaptă). Orice număr

real corespunde în mod unic unui punct de pe dreaptă: numărul real corespunzător punctului P este *distanța* de la O la P (dacă P este de aceeași parte ca și U față de O), respectiv distanța de la O la P luată cu semnul minus dacă O este între U și P . Se conturează astfel ideea intuitivă că numerele reale „pot măsura orice distanță”. Este semnificativ acest punct de vedere dacă se observă rolul esențial pe care îl are \mathbb{R} în definiția generală a *spațiilor metrice* (spații în care este definită o noțiune de *distanță*).

În multe cărți (între care și manualele de Analiză de liceu) structura numerelor reale este dată „axiomatic”: se numește *corp al numerelor reale* un *corp comutativ* $(\mathbb{R}, +, \cdot)$ înzestrat cu o relație de *ordine totală* " \leq ", satisfăcând proprietățile:

R1. \mathbb{R} este *corp ordonat*, adică $\forall a, b, c \in \mathbb{R}$ au loc:

$$a \leq b \Rightarrow a + c \leq b + c;$$

$$a \leq b \text{ și } c \geq 0 \Rightarrow ac \leq bc.$$

R2. Orice submulțime nevidă majorată a lui \mathbb{R} are margine superioară.

Evident, această definiție ridică două probleme: *existența* unei structuri cu proprietățile de mai sus și *unicitatea* sa. Unicitatea este tranșată de următorul rezultat:

4.1 Teoremă. *Pentru orice două corpuri comutative ordonate $(K, +, \cdot, \leq)$ și $(L, +, \cdot, \leq)$ care satisfac proprietatea R2 există un unic izomorfism de corpuri $\varphi: K \rightarrow L$, care este și izomorfism de ordine: $\forall x, y \in K, x \leq y \Rightarrow \varphi(x) \leq \varphi(y)$. \square*

Problema existenței se rezolvă printr-o *construcție efectivă* a lui \mathbb{R} , presupunând dat \mathbb{Q} . Cele mai cunoscute procedee sînt *construcția zecimală*, *construcția prin tăieturi în \mathbb{Q}* și *construcția cu ajutorul șirurilor Cauchy* (șiruri *fundamentale*). Construcția folosind șirurile Cauchy prezintă avantajele eleganței și rapidității și se folosește și la alte construcții importante: *completatul unui corp normat oarecare*, *completatul unui spațiu metric*, *completatul unui spațiu vectorial normat*.

Pentru edificarea cititorului, vom schița construcția zecimală și apoi prezentăm construcția cu șirurile Cauchy. Construcția prin tăieturi, aparținînd lui Dedekind, este descrisă la exerciții.

Construcția zecimală a lui \mathbb{R} (datorată lui Weierstrass²⁷) identifică un număr real cu o „fracție zecimală infinită”. De exemplu,

1,4142135623730950488016887242097..., 3,1415926535897932384626433832795...
sînt numerele reale $\sqrt{2}$, respectiv π (de fapt, e vorba de „trunchieri” ale lor; nu am scris *toate* zecimalele, din motive evidente de spațiu...). Formal, se consideră mulțimea :

$$\mathfrak{R} = \{b_0, b_1 b_2 \dots b_n \dots \mid b_0 \in \mathbb{Z}, b_i \in \{0, 1, \dots, 9\}, \forall i \in \mathbb{N}^*\}$$

²⁷ Karl Theodor Wilhelm Weierstrass (1815-1897), matematician german, considerat "părintele analizei moderne".

Interpretarea intuitivă este: „ $b_0, b_1 b_2 \dots b_n \dots$ este suma seriei $b_0 + \sum_{n \geq 1} b_n \cdot 10^{-n}$ ” (dar, evident, nu putem *defini* astfel un număr real. De ce?).

Alegerea lui 10 ca bază este mai degrabă legată de tradiție, în locul său putînd fi ales orice număr natural $b \geq 2$ (evident, avem atunci $b_i \in \{0, 1, \dots, b-1\}$, adică b_i sînt cifre în baza b).

Apar însă probleme: $0,9999\dots$, scris și ca $0,(9)$ („cu perioada 9”) este de fapt 1 (formal $1,000\dots$), după cum se vede făcînd suma seriei corespunzătoare; cum nu dorim ca un același număr real să aibă două reprezentări zecimale distincte, trebuie făcută următoarea „identificare”: orice șir de forma $b = b_0, b_1 b_2 \dots b_n \dots$, cu proprietatea că $\exists k \geq 0$ astfel încît $b_i = 9, \forall i > k$ și $b_k < 9$, este identificat cu șirul $b_0, b_1 b_2 \dots (b_k + 1)000\dots$ (dacă $k \geq 1$), respectiv cu $(b_0 + 1),000\dots$ (dacă $k = 0$). Pentru rigurozitate, se definește o relație de echivalență \sim pe \mathfrak{R} , ca mai sus, iar mulțimea factor \mathfrak{R}/\sim va fi prin definiție \mathbb{R} . Alte dificultăți apar la definirea adunării și înmulțirii a două fracții zecimale infinite (de fapt a unor clase de echivalență din \mathfrak{R}/\sim), fiind necesară apelarea la operațiile pe „trunchierile raționale” ale șirurilor respective și la definirea unei noțiuni de limită în \mathfrak{R}/\sim . Invităm cititorul să încerce să dea singur aceste definiții și să demonstreze pe baza lor proprietățile uzuale ale operațiilor cu numere reale, pentru a măsura dificultățile construcției. Avantajele acestei abordări (în măsura detalierei efective de către cititor!) constau în apropierea de imaginea intuitivă a conceptului de număr real și la definirea *relației de ordine*, care coincide cu cea *lexicografică*²⁸: se definește $b_0, b_1 b_2 \dots b_n \dots < c_0, c_1 c_2 \dots c_n \dots \Leftrightarrow \exists k \in \mathbb{N}$ astfel încît $b_k < c_k$ și, $\forall i < k$, are loc $b_i = c_i$.

Construcția lui \mathbb{R} cu ajutorul șirurilor Cauchy (G. Cantor)

\mathbb{Q} este un *corp normat*. Mai precis, aplicația *valoare absolută* (sau *modul*) $|\cdot| : \mathbb{Q} \rightarrow \mathbb{Q}$,

$$|x| = \begin{cases} x & \text{dacă } x \geq 0 \\ -x & \text{dacă } x < 0 \end{cases}$$

are proprietățile (binecunoscute) următoare:

N1. $\forall x \in \mathbb{Q}$ are loc $|x| \geq 0$.

N2. $\forall x \in \mathbb{Q}$ are loc $|x| = 0 \Leftrightarrow x = 0$.

N3. $\forall x, y \in \mathbb{Q}$ are loc $|x + y| \leq |x| + |y|$ (inegalitatea triunghiulară).

N4. $\forall x, y \in \mathbb{Q}$ are loc $|x \cdot y| = |x| \cdot |y|$.

Altfel spus, valoarea absolută este o *normă*²⁹. Cu ajutorul normei definim o *distanță* (o *metrică*)³⁰, adică o aplicație $d : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$, $d(x, y) := |x - y|$, $\forall (x, y) \in \mathbb{Q}$, cu proprietățile:

D1. $\forall x, y \in \mathbb{Q}$ are loc $d(x, y) = d(y, x) \geq 0$.

D2. $\forall x, y \in \mathbb{Q}$ are loc $d(x, y) = 0 \Leftrightarrow x = y$.

D3. $\forall x, y, z \in \mathbb{Q}$ are loc $d(x, y) \leq d(x, z) + d(z, y)$ (inegalitatea triunghiulară).

Ca o consecință, se obține $|x - y| \geq ||x| - |y||$, $\forall x, y \in \mathbb{Q}$.

²⁸ Lexicon = dicționar. Puteți spune de ce se numește așa ordinea definită?

²⁹ În general, o *normă* ia valori în \mathbb{R} , pe care nu l-am construit încă... , deci titulatura este puțin forțată.

³⁰ Aceeași observație ca mai sus: o *distanță* ia în general valori reale.

Metrica determină o *topologie*³¹ pe \mathbb{Q} . Proprietățile metrice și topologice ale lui \mathbb{Q} nu sînt prea bune, tocmai din cauzele amintite la început: nu orice șir de numere raționale „care ar trebui să fie convergent la ceva” este convergent la un număr rațional (de exemplu, șirul aproximărilor zecimale ale lui $\sqrt{2}$).

Construcția lui \mathbb{R} cu șiruri Cauchy pornește de la ideea că un număr real este o „limită a unui șir de numere raționale”. În loc să ne îndreptăm atenția asupra unui tip particular de șiruri de numere raționale, ca la construcția zecimală (șirurile cu termen general de forma $b_0 + \sum_{i=1}^n b_i \cdot 10^{-i}$), se consideră *toate* șirurile de numere raționale $(x_n)_{n \geq 1}$ „care au o limită, nu neapărat în \mathbb{Q} ”.

Bineînțeles, nu orice șir de numere raționale „are o limită” în sens intuitiv (de exemplu șirul $((-1)^n)_{n \geq 1}$). Pe de altă parte, nu putem defini „existența limitei” șirului (x_n) direct ($\exists l$ astfel încît $x_n \rightarrow l$), căci l este în general un număr real, concept pe care tocmai îl construim! Din fericire, știm de la Analiză că *șirurile care au limită în \mathbb{R} sînt exact șirurile Cauchy* (noțiune în care *nu apare explicit* limita șirului).

4.1 Definiție. Șirul de numere raționale $(x_n)_{n \geq 1}$ se numește *șir Cauchy* (sau *șir fundamental*) dacă satisface condiția:

$$\forall \varepsilon \in \mathbb{Q}, \varepsilon > 0 \Rightarrow \exists N \in \mathbb{N} \text{ astfel încît } \forall m, n \geq N \text{ să aibă loc } |x_m - x_n| < \varepsilon.$$

Fie $\mathcal{C} := \{(x_n)_{n \geq 1} \mid x_n \in \mathbb{Q}, \forall n \geq 1, (x_n)_{n \geq 1} \text{ șir Cauchy}\}$.

Putem aplica acum ideea intuitivă expusă la început și să definim două șiruri $(x_n), (y_n) \in \mathcal{C}$ ca fiind *echivalente*³² dacă „au aceeași limită”. Și această idee se poate exprima fără a invoca explicit valoarea limitei:

$$(x_n)_n \sim (y_n)_n \Leftrightarrow \forall \varepsilon \in \mathbb{Q}, \varepsilon > 0 \Rightarrow \exists N \in \mathbb{N} \text{ astfel încît } \forall n \geq N \text{ să aibă loc } |x_n - y_n| < \varepsilon. \quad (R)$$

În sfîrșit, definim un *număr real* ca o *clasă de echivalență de șiruri din \mathcal{C}* ; mai precis, mulțimea factor \mathcal{C}/\sim o notăm cu \mathbb{R} și o numim *mulțimea numerelor reale*. Se observă că orice număr rațional a poate fi identificat cu clasa în \mathcal{C}/\sim a *șirului constant* $(a, a, \dots) \in \mathcal{C}$ (adică am obținut într-adevăr o *extindere* a lui \mathbb{Q}).

Rămîn sarcinile: de a *defini operațiile*, de a demonstra *corectitudinea definițiilor* și de a *verifica axiomele de corp comutativ* pentru \mathbb{R} . Apoi trebuie definită *relația de ordine* și arătat că: \mathbb{R} este *total ordonat*, *relația de ordine este compatibilă cu structura de corp* și *orice submulțime nevidă majorată are margine superioară*.

Aceste sarcini se pot ușura considerabil dacă folosim instrumente algebrice elementare: *ideale* și *inele factor*. Observăm că \mathcal{C} este *inel comutativ unitar* și că $(x_n)_n \sim (y_n)_n \Leftrightarrow$

³¹ Nu mai definim topologia, vezi orice manual de Analiză elementară.

³² Adică "definesc" același număr real.

$(x_n - y_n) \rightarrow 0$ (unde scriem $(z_n) \rightarrow 0$ dacă $\forall \varepsilon \in \mathbb{Q}, \varepsilon > 0 \Rightarrow \exists N \in \mathbb{N}$ astfel încît $\forall n \geq N$ să aibă loc $|z_n| < \varepsilon$). Dacă notăm

$$\mathfrak{Z} := \{(z_n)_{n \geq 1} \in \mathcal{C} \mid (z_n) \rightarrow 0\},$$

se demonstrează că \mathfrak{Z} este *ideal maximal* în \mathcal{C} (și relația " \sim " coincide cu relația de congruență modulo \mathfrak{Z}). Rezultă imediat atunci că $\mathbb{R} = \mathcal{C}/\mathfrak{Z}$ este corp comutativ și cu aceasta se încheie partea „algebrică” a construcției lui \mathbb{R} . Notăm cu $[(x_n)]$ imaginea în \mathcal{C}/\mathfrak{Z} a șirului $(x_n) \in \mathcal{C}$. Sumarizăm construcția în următoarea:

4.2 Teoremă. a) *Mulțimea \mathcal{C} a șirurilor Cauchy de numere raționale este un inel comutativ unitar³³ în raport cu operațiile de adunare și înmulțire definite „punctual”:*

$$(x_n)_n + (y_n)_n := (x_n + y_n)_n,$$

$$(x_n)_n \cdot (y_n)_n := (x_n \cdot y_n)_n,$$

$\forall (x_n), (y_n) \in \mathcal{C}$.

b) *Mulțimea $\mathfrak{Z} = \{(z_n)_{n \geq 1} \in \mathcal{C} \mid (z_n) \rightarrow 0\}$ a șirurilor din \mathcal{C} care au limita 0 este un ideal maximal în \mathcal{C} , deci inelul factor $\mathcal{C}/\mathfrak{Z} =: \mathbb{R}$ este corp comutativ.*

c) *Pentru orice $a \in \mathbb{Q}$, considerăm „șirul constant” $(a_n)_n \in \mathcal{C}$, $a_n = a$, $\forall n \in \mathbb{N}^*$. Aplicația care asociază lui $a \in \mathbb{Q}$ clasa în $\mathcal{C}/\mathfrak{Z} = \mathbb{R}$ a șirului constant $(a_n)_n$ este un morfism de corpuri. Clasa $[(a_n)] \in \mathbb{R}$ a șirului constant (a_n) va fi numită prin abuz „numărul rațional a ”.*

d) *Definim pe \mathcal{C}/\mathfrak{Z} relația binară " $<$ ”:*

$$[(x_n)] < [(y_n)] \Leftrightarrow \exists \varepsilon \in \mathbb{Q}, \varepsilon > 0 \text{ și } \exists N \in \mathbb{N} \text{ astfel încît } x_n + \varepsilon \leq y_n, \forall n \geq N.$$

Atunci " $<$ ” este bine definită (nu depinde de reprezentanți) și este o relație de ordine strictă pe \mathcal{C}/\mathfrak{Z} (ireflexivă și tranzitivă). Relația de ordine nestrictă asociată, notată " \leq ”, este o relație de ordine totală pe \mathbb{R} ; mai mult, \mathbb{R} devine corp ordonat în raport cu această ordine.

e) *(Valoarea absolută pe \mathbb{R}) Fie $|\cdot| : \mathbb{R} \rightarrow \mathbb{R}, [(x_n)] = [(|x_n|)]$, $\forall (x_n) \in \mathcal{C}$. Definiția este corectă și au loc proprietățile normei N1-N4 de mai sus (bineînțelese, \mathbb{Q} este înlocuit cu \mathbb{R}).*

f) *Orice șir Cauchy $(r_n)_{n \geq 1}$ de numere reale este convergent la un număr real.³⁴*

g) *Orice submulțime nevidă majorată a lui \mathbb{R} are margine superioară.*

h) *\mathbb{Q} este dens în \mathbb{R} (orice număr real este limita unui șir de numere raționale).*

Demonstrație. a) Demonstrarea faptului că suma și produsul a două șiruri Cauchy este tot șir Cauchy este un exercițiu elementar de Analiză (cf. demonstrația la „suma, resp. produsul, a două șiruri convergente este un șir convergent”). Este utilă demonstrarea în prealabil a faptului că orice șir Cauchy (x_n) este mărginit ($\exists M \in \mathbb{Q}$ astfel încît $|x_n| \leq M$, $\forall n \in \mathbb{N}^*$). Care este elementul nul, respectiv unitate, în \mathcal{C} ?

b) \mathfrak{Z} este ideal: argument standard de Analiză, ca la punctul precedent (se adaptează demonstrația proprietăților $\lim(x_n + y_n) = \lim x_n + \lim y_n$, $\lim(x_n \cdot y_n) = \lim x_n \cdot \lim y_n$).

³³ Este și integru?

³⁴ Lăsăm cititorului sarcina de a defini noțiunile de șir Cauchy și de limită în \mathbb{R} .

\mathcal{Z} este maximal: dacă $(x_n) \in \mathcal{C} \setminus \mathcal{Z}$, atunci există $N \in \mathbb{N}$ și $\delta > 0$ astfel încît $|x_n| > \delta$, $\forall n \geq N$. Într-adevăr, cum (x_n) nu tinde la 0, $\exists \varepsilon > 0$ astfel încît $\forall n \in \mathbb{N}$, $\exists k_n > n$ astfel încît $|x_{k_n}| > \varepsilon$. Însă (x_n) este Cauchy, deci, pentru $\varepsilon/2$, există $N \in \mathbb{N}$ astfel încît $\forall m, n \geq N$, $|x_n - x_m| < \varepsilon/2$. Fie $m = k_N$ dat de proprietatea precedentă. Atunci, $\forall n \geq N$,

$$|x_n| = |x_m + x_n - x_m| \geq |x_m| - |x_n - x_m| > \varepsilon - \varepsilon/2 = \varepsilon/2.$$

Raționamentul, ca și multe altele de același gen, se vede mai bine (și poate fi intuit!) reprezentînd numerele pe axă.

Revenind la (x_n) , rezultă că $\exists N \in \mathbb{N}$ astfel încît $x_n \neq 0$ dacă $n \geq N$. Definim atunci șirul (y_n) prin: $y_n = 0$ dacă $n < N$ și $y_n = 1/x_n$ dacă $n \geq N$. Șirul (y_n) este Cauchy (demonstrați!) și $x_n y_n = 1 + z_n$, unde z_n este 0 pentru $n \geq N$, deci $(z_n) \in \mathcal{Z}$.

e) Trebuie arătat mai întîi că $(|x_n|)$ este șir Cauchy și că definiția nu depinde de reprezentanți. Demonstrația proprietăților normei se face apelînd la proprietățile corespunzătoare pentru norma în \mathbb{Q} .

f) Argumentul este tipic de Analiză, dar îl includem, fiind mai delicat. Fie $(r_n)_{n \geq 1}$ un șir Cauchy de numere reale. Fie $r_n = [(r_{nk})_{k \geq 1}]$, unde $(r_{nk})_{k \geq 1}$ este un șir Cauchy de numere raționale (pentru orice n fixat). Notăm $r_{nk} =: r(n, k)$, $\forall n, k \geq 1$. Vom arăta că $(r_n)_{n \geq 1}$ are limită în \mathbb{R} , anume $[(r(i_n, j_n))_{n \geq 1}]$, unde i_n, j_n sînt niște șiruri strict crescătoare de numere naturale pe care le definim inductiv, astfel:

Cum $(r_n)_{n \geq 1}$ este șir Cauchy în \mathbb{R} , pentru $\varepsilon = 1/4$, $\exists i_1 \in \mathbb{N}$ astfel încît $\forall s, t \geq i_1$ avem $|r_s - r_t| < 1/4$.

Cum $(r_{i_1 k})_{k \geq 1}$ e șir Cauchy în \mathbb{Q} , $\exists j_1 \in \mathbb{N}$ astfel încît $|r(i_1, u) - r(i_1, v)| < 1/4$, $\forall u, v \geq j_1$.

Fie $n \in \mathbb{N}$, $n \geq 2$ și presupunem că am definit $i_1 < i_2 < \dots < i_{n-1}$ și $j_1 < j_2 < \dots < j_{n-1}$, numere naturale astfel încît, $\forall k \in \{1, \dots, n-1\}$:

$$|r_s - r_t| < 1/2^{k+1}, \forall s, t \geq i_k \text{ (inegalitate în } \mathbb{R}) \quad (1)$$

$$|r(i_k, u) - r(i_k, v)| < 1/2^{k+1}, \forall u, v \geq j_k \quad (2)$$

$$|r(i_k, u) - r(i_{k-1}, u)| < 1/2^k, \forall u \geq j_k \quad (3)$$

Condiția (3) este vidă pentru $k = 1$.

Să găsim i_n și j_n încît (1), (2) și (3) să fie satisfăcute pentru $k = n$.

Șirul $(r_n)_{n \geq 1}$ este Cauchy în \mathbb{R} ; luînd $\varepsilon = 1/2^{n+1}$, există $i_n \in \mathbb{N}$ astfel încît $i_n > i_{n-1}$ și

$$|r_s - r_t| < 1/2^{n+1}, \forall s, t \geq i_n \text{ (inegalitate în } \mathbb{R}).$$

Cum $(r(i_n, k))_{k \geq 1}$ e șir Cauchy în \mathbb{Q} , $\exists p_n \in \mathbb{N}$ astfel încît

$$|r(i_n, u) - r(i_n, v)| < 1/2^{n+1}, \forall u, v \geq p_n$$

Pe de altă parte, din (1) aplicat pentru $k = n-1$ și $s = i_n$, $t = i_{n-1}$, avem $|r_{i_n} - r_{i_{n-1}}| < 1/2^n$ (inegalitate în \mathbb{R}), deci (din definiția relației de ordine în \mathbb{R}) $\exists q_n$ astfel încît

$$|r(i_n, u) - r(i_{n-1}, u)| < 1/2^n, \forall u \geq q_n.$$

Luînd $j_n = \max(j_{n-1} + 1, p_n, q_n)$, rezultă că (2) și (3) sînt satisfăcute, cu $k = n$ și că $j_n > j_{n-1}$. Am construit inductiv șirurile strict crescătoare i_n, j_n , satisfăcînd (1), (2), (3), pentru orice $k \geq 1$.

Notăm $x_n := r(i_n, j_n)$, $\forall n \geq 1$. Să arătăm că $(x_n)_{n \geq 1}$ e șir Cauchy în \mathbb{Q} . Pentru orice $n, m \in \mathbb{N}$ cu $n < m$, avem:

$$|x_m - x_n| = |r(i_m, j_m) - r(i_n, j_n)| \leq |r(i_m, j_m) - r(i_n, j_m)| + |r(i_n, j_m) - r(i_n, j_n)| \quad (4)$$

Dar, folosind (3), avem

$$|r(i_m, j_m) - r(i_n, j_m)| = \sum_{k=n+1}^m |r(i_k, j_m) - r(i_{k-1}, j_m)| < \sum_{k=n+1}^m \frac{1}{2^k} < \frac{1}{2^n}. \quad (4')$$

Pe de altă parte, $|r(i_n, j_m) - r(i_n, j_n)| < 1/2^n$ pentru că $j_m > j_n$ și se aplică (2).

Înlocuind în (4), avem:

$$|x_m - x_n| < |r(i_m, j_m) - r(i_n, j_n)| < 1/2^n + 1/2^n = 1/2^{n-1},$$

ceea ce arată că (x_n) este șir Cauchy.

Să arătăm că r_n are limita $x := [(r(i_n, j_n))_{n \geq 1}]$. Fie $\varepsilon > 0$ și $k \in \mathbb{N}$ astfel încît $1/2^k < \varepsilon/3$. Din (1) avem:

$$|r_s - r_t| < 1/2^{k+1}, \forall s, t \geq i_k \quad (5)$$

Dacă $n \geq i_k$, arătăm că $|r_n - x| < \varepsilon$ (ceea ce va termina demonstrația). Aceasta revine la a proba existența unui N (depinzînd posibil de n) astfel încît $\forall t \geq N$ să avem

$$|r_{nt} - x_t| = |r(n, t) - r(i_t, j_t)| < \varepsilon.$$

Fixăm $q \in \mathbb{N}$ cu $i_q \geq n$. Din (5), $|r_n - r_{i_q}| < 1/2^{k+1}$, deci există un N_0 astfel încît, $\forall t \geq N_0$:

$$|r(n, t) - r(i_q, t)| < \varepsilon/3 \quad (6)$$

Cum r_n e Cauchy, există N_1 astfel încît, $\forall s, t \geq N_1$,

$$|r(n, t) - r(n, s)| < \varepsilon/3 \quad (7)$$

Fie $N := \max(N_0, N_1, i_q)$. Dacă $t \geq N$, avem:

$$|r(n, t) - r(i_t, j_t)| \leq |r(n, t) - r(n, j_t)| + |r(n, j_t) - r(i_q, j_t)| + |r(i_q, j_t) - r(i_t, j_t)| \quad (8)$$

Primul termen din dreapta inegalității (8) e mai mic decît $\varepsilon/3$ din (7). Al doilea termen e mai mic decît $\varepsilon/3$ din (6) (clar, $j_t > t \geq N$). Al treilea termen e mai mic decît $1/2^q$ din (4').

g) Cititorii care au parcurs teoria elementară a convergenței în \mathbb{R} se vor fi întrebat de ce am dat o demonstrație separată pentru f), deși rezultă din g) (vezi Exerciții). Pentru răspuns, vezi construcția de mai jos a *completatului unui corp normat*.

h) Exercițiu. □

Metoda completării prin șiruri Cauchy este folosită și la *completatul unui spațiu metric* oarecare, construcție fundamentală în Analiză și topologie:

4.3 Definiție. Fie X o mulțime nevidă. O funcție $d : X \times X \rightarrow \mathbb{R}$ se numește *distanță* (*metrică*) pe X dacă satisface axiomele: i) $\forall x, y \in X$ are loc $d(x, y) = d(y, x) \geq 0$; ii) $\forall x, y \in X$ are loc: $d(x, y) = 0 \Leftrightarrow x = y$; iii) $\forall x, y, z \in X$ are loc $d(x, y) \leq d(x, z) + d(z, y)$ (inegalitatea triunghiulară). Un cuplu (X, d) , unde d este o distanță pe X , se numește *spațiu metric*; elementele lui X se mai numesc și *puncte* ale lui X .

Pentru orice $x \in X$, *sfera (bila) deschisă de rază r cu centrul în x* este mulțimea

$$S(x, r) := \{y \in X \mid d(x, y) < r\}.$$

Distanța d definește o *topologie* pe X , în care un sistem fundamental de vecinătăți al unui punct $x \in X$ este $\{S(x, r) \mid r \in \mathbb{R}, r > 0\}$ (mulțimea sferelor deschise centrate în x). Altfel spus, o submulțime D a lui X este declarată *deschisă* dacă $\forall x \in D, \exists r > 0$ astfel încât $S(x, r) \subseteq D$. Un șir $(x_n)_{n \geq 1}$ este *convergent* la $x \in X$ dacă și numai dacă $\forall \varepsilon > 0, \exists N \in \mathbb{N}$ astfel încât $\forall n > N$ are loc $d(x_n, x) < \varepsilon$. Spațiul metric (X, d) se numește *complet* dacă orice șir Cauchy de elemente din X este convergent la un element din X .

Am văzut că \mathbb{Q} este spațiu metric, cu distanța $d(x, y) = |x - y|$, dar nu este complet. Din punct de vedere topologic, construcția lui \mathbb{R} prezentată mai sus este un caz particular al *completării unui spațiu metric*, care, plecând de la un spațiu metric (X, d) , construiește un spațiu metric *complet* $(\widehat{X}, \widehat{d})$ și o aplicație injectivă $\varphi: X \rightarrow \widehat{X}$, astfel încât $\varphi(X)$ este densă în \widehat{X} și φ păstrează distanțele. Construcția este asemănătoare cu cea de mai sus, cu deosebirea că nu putem face apel la ideale, nefiind definită nici o structură algebrică pe X . Se folosește direct o relație de echivalență " \sim " definită pe mulțimea \mathcal{C} a șirurilor Cauchy de elemente din X ; mulțimea \mathcal{C}/\sim se înzestreaază cu o metrică (cum?) și este spațiul metric complet căutat.

Mai importantă pentru Algebră și Teoria numerelor este *completarea unui corp normat*.

4.4 Definiție. Fie K un corp comutativ. O funcție $N: K \rightarrow \mathbb{R}$ se numește *normă* dacă satisface condițiile:

N1. $\forall x \in K$ are loc $N(x) \geq 0$.

N2. $\forall x \in K$ are loc $N(x) = 0 \Leftrightarrow x = 0$.

N3. $\forall x, y \in K$ are loc $N(x + y) \leq N(x) + N(y)$ (inegalitatea triunghiulară).

N4. $\forall x, y \in K$ are loc $N(x \cdot y) = N(x) \cdot N(y)$.

Un cuplu (K, N) , unde K este corp și N o normă pe K se numește *corp normat*. Exemple uzuale sînt $(\mathbb{Q}, |\cdot|)$, $(\mathbb{R}, |\cdot|)$.

Norma pe K definește o metrică $d: K \times K \rightarrow \mathbb{R}$ prin relația $d(x, y) := N(x - y)$ (verificați!). Dacă spațiul metric (K, d) nu este complet, se poate construi ca mai sus *completatul său* \widehat{K} , care e spațiu metric; în plus, se pot defini operații pe \widehat{K} față de care acesta devine corp normat. O abordare mai rapidă reia ideea de a folosi idealul \mathfrak{Z} al șirurilor cu limita 0 în inelul \mathcal{C} al șirurilor Cauchy de elemente din K și construiește $\widehat{K} := \mathcal{C}/\mathfrak{Z}$.

4.5 Exemplu. (Corpul numerelor p -adice) Fie $p \in \mathbb{Z}$ un număr prim. Dacă $n \in \mathbb{Z}$ și $\alpha \in \mathbb{N}$, scriem $p^\alpha \parallel n$ dacă $p^\alpha \mid n$ și $p^{\alpha+1} \nmid n$. Pentru orice $n \in \mathbb{Z}$, $\exists! \alpha \in \mathbb{N}$ astfel încât $p^\alpha \parallel n$. Definim $v_p(n)$, *valuarea p -adică* a lui n , ca fiind unicul numărul natural α astfel încât $p^\alpha \parallel n$. Dacă $r = m/n \in \mathbb{Q}$, cu $m, n \in \mathbb{Z}$, definim³⁵ $v_p(m/n) := v_p(m) - v_p(n)$. Norma p -adică a lui r este

$$|r|_p := p^{-v_p(r)}.$$

³⁵ Verificați corectitudinea definiției!

Se demonstrează că norma p -adică este o normă pe \mathbb{Q} și îndeplinește o proprietate mai tare decât axioma N3 (inegalitatea triunghiulară), anume:

$$\text{NA: } \quad \forall x, y \in \mathbb{Q} \text{ are loc } |x + y|_p \leq \max(|x|_p, |y|_p).$$

Un corp normat $(K, |\cdot|)$ care satisface proprietatea NA se numește *non-archimedean* (sau *ultrametric*), deoarece nu satisface *proprietatea lui Arhimede*³⁶: $\forall x, y \in K$ cu $x \neq 0$, $\exists n \in \mathbb{N}^*$ astfel încât $|nx| \geq |y|$.

Completatul lui \mathbb{Q} în raport cu norma p -adică se notează cu \mathbb{Q}_p și se numește *corpul numerelor p -adice*. Aceste corpuri joacă un rol important în teoria numerelor.

Aceeași idee, a șirurilor Cauchy, apare și la construcția *completatului unui spațiu liniar normat*. Nu mai intrăm în detalii (vezi de ex. MARINESCU [1983]).

Exerciții

1. Demonstrați că în \mathbb{R} (construit cu șiruri Cauchy) orice submulțime nevidă majorată are margine superioară.

2. Fie K un corp comutativ total ordonat în care orice submulțime nevidă majorată are margine superioară. Demonstrați că orice șir Cauchy în K este convergent.

3. (Construcția lui Dedekind a lui \mathbb{R} prin tăieturi în \mathbb{Q}) Se numește *tăietură* în \mathbb{Q} o pereche (A, B) de submulțimi ale lui \mathbb{Q} cu proprietățile: i) $A \neq \emptyset$, $B \neq \emptyset$; ii) $A \cup B = \mathbb{Q}$; iii) $\forall a \in A$, $\forall b \in B$ are loc $a < b$; iv) A nu are cel mai mare element.

Fie $T(\mathbb{Q}) := \{(A, B) \mid (A, B) \text{ tăietură în } \mathbb{Q}\}$. Demonstrați că:

a) Dacă (A, B) este tăietură în \mathbb{Q} , atunci $A \cap B = \emptyset$ și $B = \mathbb{Q} \setminus A$.

b) Definind relația " \leq " pe $T(\mathbb{Q})$ prin $(A, B) \leq (C, D) \Leftrightarrow A \subseteq C \Leftrightarrow D \subseteq B$, se obține o relație de ordine totală pe $T(\mathbb{Q})$.

c) Aplicația $\varphi: \mathbb{Q} \rightarrow T(\mathbb{Q})$, $\varphi(x) = (L_x, R_x)$, cu $L_x = \{y \in \mathbb{Q} \mid y < x\}$ și $R_x = \{y \in \mathbb{Q} \mid y \geq x\}$, este injectivă și crescătoare (deci x poate fi identificat cu $\varphi(x) \in T(\mathbb{Q})$, iar \mathbb{Q} cu $\varphi(\mathbb{Q})$).

d) Orice submulțime $(A_i, B_i)_{i \in I}$ a lui $T(\mathbb{Q})$ care este majorată în $T(\mathbb{Q})$ are margine superioară, anume $(\bigcup_{i \in I} A_i, \bigcap_{i \in I} B_i) \in T(\mathbb{Q})$.

e) Definind: $(A, B) + (C, D) := (A + C, B + D)$, $\forall (A, B), (C, D) \in T(\mathbb{Q})$, (unde $A + C = \{a + c \mid a \in A, c \in C\}$), se obține o lege de compoziție pe $T(\mathbb{Q})$; $(T(\mathbb{Q}), +)$ este grup abelian, iar $\varphi: \mathbb{Q} \rightarrow T(\mathbb{Q})$ definit mai sus este morfism de grupuri.

f) Fie $\alpha = (A, B)$, $\beta = (C, D) \in T(\mathbb{Q})$. Definim " \cdot ": $T(\mathbb{Q}) \times T(\mathbb{Q}) \rightarrow T(\mathbb{Q})$ prin:

³⁶ \mathbb{Q} și \mathbb{R} sînt *corpuri arhimediene*, căci satisfac această proprietate.

$$\alpha \cdot \beta = \begin{cases} (AC, BD) & \text{dacă } \alpha, \beta \geq 0 \\ |\alpha| \cdot |\beta| & \text{dacă } \alpha, \beta < 0 \\ -|\alpha| \cdot |\beta| & \text{în celelalte cazuri} \end{cases}$$

(unde $A \cdot C = \{a \cdot c \mid a \in A, c \in C\}$ și $||$ este funcția modul pe K). Atunci $(T(\mathbb{Q}), +, \cdot, \leq)$ este corp ordonat și $\varphi: \mathbb{Q} \rightarrow T(\mathbb{Q})$ este morfism de corpuri.

4. Verificați afirmațiile nedemonstrate de la exemplul II.4.5.

Index

A

apartenență, 7
aplicație, 19
 crescătoare, 34
argument, 19
axioma
 alegerii, 37
 extensionalității, 12
 fundării, 36
 inducției, 26
 infinității, 27
 mulțimii părților, 12
 reuniunii, 13
axioma-schemă a substituției, 13
axiome, 11
axiomele Dedekind-Peano, 26

B

bilă, 53

C

cardinal, 38
clasa
 ordinalelor, 27
clasă, 16
 bine ordonată, 29
clasă de echivalență, 42
codomeniul unei funcții, 19
compunerea a două relații, 21
conectori, 7

conjuncția, 7
constantă, 7
contraimagea unei submulțimi printr-o funcție, 24
cuantificatori, 7
cuantori, 7
cuplu, 17

D

definiții prin recurență, 32
diferență, 15
disjuncția, 7
distanță, 53
domeniul unei funcții, 19

E

egalitate, 7
enunț, 7
expresie, 7
expresii echivalente, 9
extensiune, 17

F

familie de mulțimi, 20
funcția identică, 19
funcție, 19
 bijectivă, 21
 identitate, 21
 injectivă, 21
 inversabilă, 21
 surjectivă, 21

G

graficul
unei funcții, 19

I

image, 20
image printr-o relație funcțională, 13
inducție
transfinită, 32
infimum, 24
intersecție, 15
a unei familii, 20
inversa
unei relații, 20
inversa unei funcții, 21
izomorfism
de ordine, 34

L

lanț, 23
latice, 24
completă, 24
Lema lui Zorn, 37

M

majorant, 23
majorată (submulțime), 23
maximal (element), 24
metrică, 53
minorant, 23
minorată (submulțime), 23
model, 35
modul (funcția), 47
morfism
de ordine, 34
mulțime, 5
bine ordonată, 23
finită, 38

inductiv ordonată, 37
infinită, 38
numărabilă, 38
ordonată, 23
total ordonată, 23

mulțime cât, 42
mulțime factor, 42
mulțimea vidă, 14
mulțimi
cardinal echivalente, 38
echipotente, 38

N

negația, 7
normă, 54
noțiuni primare, 11
nume constant, 7
nume variabil, 7

O

ordinal, 27, 35
finit, 30
infinit, 30
limită, 39
predecesor, 30
succesor, 29
ordine
lexicografică, 49

P

partiție
a unei mulțimi, 42
pereche ordonată, 17
predicat, 8
primul element, 23
Principiul bunei ordonări, 37
produs cartezian, 18
propoziție, 8

- R**
- relație
- antisimetrică, 22
 - de bună ordine, 23
 - de echivalență, 22
 - de ordine, 22
 - de ordine strictă, 22
 - de ordine totală, 23
 - de preordine, 22
 - ireflexivă, 22
 - reflexivă, 22
 - simetrică, 22
 - tranzitivă, 22
- relație (clasă), 19
- relație binară, 18
- relație funcțională, 13
- reprezentarea unui număr într-o bază, 40
- reuniune
- a unei familii, 20
 - disjunctă, 20
- S**
- schema de comprehensiune, 14
- segment inițial, 27
- sferă, 53
- simbol, 7
- sistem de reprezentanți, 42
- spațiu metric, 53
- complet, 54
- submulțime, 12
- supremum, 24
- Ș**
- șir, 32
- șir Cauchy, 50
- șir fundamental, 50
- T**
- tăietură, 55
- teorema perechii, 17
- tip de ordine, 35
- U**
- ultimul element, 23
- V**
- valoare de adevăr, 8
- valoarea absolută, 47
- valuarea p -adică, 54
- variabilă, 7
- variabilă legată, 8
- variabilă liberă, 8
- Z**
- Zermelo, 5
- ZFS, 11

Bibliografie

1. BECHEANU, M. et al. [1983], *Algebră pentru perfecționarea profesorilor*, Ed. didactică și pedagogică, București.
2. FREUDENTHAL, H. [1973], *Limbajul logicii matematice*, Ed. Tehnică, București.
3. ION, I.D., NĂSTĂSESCU, C., NIȚĂ, C. [1984] *Complemente de algebră*, Ed. Științifică și enciclopedică, București.
4. ION, I.D., RADU, N. [1981a] *Algebra*, Ed. Didactică și pedagogică, București.
5. ION, I.D., RADU, N., NIȚĂ, C., POPESCU, D. [1981b] *Probleme de algebră*, Ed. Didactică și pedagogică, București.
6. MANIN, YU. I. [1977], *A Course in Mathematical Logic*, Springer Verlag, New York.
7. MARINESCU, GH. [1983], *Analiză matematică, vol. I*, Ed. Academiei R.S.R., București.
8. NĂSTĂSESCU, C. [1974] *Introducere în teoria mulțimilor*, Ed. Didactică și pedagogică, București.
9. NĂSTĂSESCU, C. [1976] *Inele. Module. Categorii*, Ed. Academiei R.S.R., București.
10. NĂSTĂSESCU, C., NIȚĂ, C., VRACIU, C. [1986] *Bazele Algebrei, vol. I*, Ed. Academiei R.S.R., București.
11. NĂSTĂSESCU, C. [1983] *Teoria dimensiunii în algebra necomutativă*, Ed. Academiei R.S.R., București.
12. NIȚĂ, C., SPIRCU, T. [1974] *Probleme de structuri algebrice*, Ed. Tehnică, București.
13. PURDEA, I. [1982] *Tratat de algebră modernă, vol II*, Ed. Academiei R.S.R., București.
14. REGHIȘ, M. [1981] *Elemente de teoria mulțimilor și logică matematică*, Ed. Facla, Timișoara.
15. SCORPAN, A. [1996] *Introducere în teoria axiomatică a mulțimilor*, Ed. Universității București, București.
16. SIREȚCHI, GH. [1978] *Analiză matematică, vol. I, ed IV.*, Tipografia Univ. București.
17. SPINDLER, K. [1994] *Abstract Algebra with Applications, vol. I, II*, M. Dekker, New York.
18. VAN DERWAERDEN, B.L. [1985], *A History of Algebra*, Springer-Verlag, Berlin.