Aurelian Claudiu VOLF

Logică şi teoria mulţimilor

Partea a II-a

Universitatea „Al. I Cuza” Iaşi

2016

Cuprins

Către cititor

Parcurgerea unui text matematic este un proces *activ* prin excelenţă. În primul rînd, toate definiţiile nou introduse trebuie să capete rapid un suport intuitiv şi să fie legate de noţiunile deja cunoscute prin căutarea de exemple (şi contraexemple) de obiecte care să satisfacă definiţiile. În plus, cititorul trebuie să *verifice* pe cazuri concrete şi să *demonstreze* afirmaţiile din text. În particular, toate apariţiile unor fraze de tipul „se verifică uşor că …”, „evident, …”, … sînt o invitaţie la demonstrarea efectivă a afirmaţiilor respective. Aceste exerciţii intelectuale sînt un pas indispensabil spre asimilarea conceptelor şi tehnicilor introduse şi, totodată, o verificare a înţelegerii de către cititor a textului.

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

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

Peste tot, în text:

- $|A|$ desemnează cardinalul mulţimii A (numărul elementelor lui A, dacă A este finită).
- $x := y$ înseamnă „x este egal prin definiţie cu y” (unde y este deja definit) sau „notăm pe y cu x”.
- □ marchează sfîrşitul sau absenţa unei demonstraţii. Adesea, aceasta înseamnă că cititorul este invitat să facă el însuşi demonstraţia.

I. Logică, mulţimi, axiome

Studiul logicii matematice şi al teoriei mulţimilor porneşte 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.

Mulţimile apar ca obiecte matematice foarte devreme în învăţămîntul modern, sub o formă intuitivă (în varianta teoriei naive a mulţimilor). Este exclusă o tratare axiomatică a teoriei mulţimilor la nivel preuniversitar; totuşi, un profesor de matematică trebuie să fie familiarizat cu conceptele de bază şi să înţeleagă utilitatea, necesitatea şi mecanismele teoriei axiomatice a mulţimilor.

De ce este important studiul teoriei mulţimilor? *Orice enunţ matematic se poate reformula în termeni de mulţimi*[1]. Aşadar, dacă teoria mulţimilor este bine fundamentată, se obţine o fundamentare a întregii matematici.

Teoria modernă a mulţimilor începe odată cu lucrarea „Teoria raţională a infinităţii" a lui Georg Cantor[2], în care se manevrează liber *mulţimile infinite* şi se dezvoltă o tehnică de măsurare a lor (teoria cardinalelor). Pînă la Cantor, matematicienii adoptau punctul de vedere al filozofilor Greciei antice: există noţiunea de *infinit actual* (o infinitate de obiecte concepute ca existînd simultan) şi cea de *infinit potenţial* (o mulţime sau o mărime finită, dar care se poate mări oricît de mult). Filozoful Zenon, prin faimoasele sale aporii (paradoxuri) a atras atenţia asupra consecinţelor absurde care par să apară introducînd infinitul actual în raţionamente. Se considera de aceea că infinitul actual nu este accesibil intuiţiei şi doar infinitul potenţial poate fi folosit în gîndirea matematică.

Cantor are meritul de a fi spart această barieră mentală şi de a fi încercat să „numere infinitul". El a avut ideea de a compara mulţimile (finite sau nu) cu ajutorul *funcţiilor bijective*: *două mulţimi sînt „la fel de mari" (în limbaj modern „echipotente") dacă există o bijecţie între ele.* Cantor a obţinut rezultate precum: $\mathbb{N}$ este echipotent cu $\mathbb{Q}$ şi cu mulţimea numerelor algebrice (numerele complexe care sînt rădăcini ale unui polinom nenul cu coeficienţi raţionali). Deja aceste afirmaţii nu sînt în acord cu percepţia obişnuită şi arată că în

[1] Dacă cititorul nu este deja convins de aceasta, sperăm că va fi după parcurgerea acestui material!
[2] Georg Ferdinand Ludwig Philipp Cantor (1845-1918), matematician german.

cazul mulţimilor infinite uneori „partea este la fel de mare ca şi întregul”. A mai arătat că $\mathbb{N}$ nu este echipotent cu $\mathbb{R}$; în general, o mulţime A nu este echipotentă cu mulţimea părţilor sale $\mathcal{P}(A)$. Există, deci, mai multe tipuri de infinitate. Alte rezultate contrazic şi mai mult simţul comun: există tot atîtea puncte pe un segment cîte sînt pe o dreaptă sau în întregul plan sau în întregul spaţiu!

În cadrul teoriei lui Cantor a mulţimilor (astăzi numită „naivă”), prin *mulţime* se înţelege o colecţie (un ansamblu, un set) de obiecte distincte (*elementele* mulţimii) bine determinată şi 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 *mulţime* înţelegem orice grupare într-un tot M a unor obiecte distincte şi bine determinate ***m*** ale gîndirii noastre”. Apare aici (deşi nu e enunţată explicit) ideea că *o „proprietate” determină o mulţime: mulţimea obiectelor care satisfac proprietatea respectivă.*

Teoria mulţimilor în forma descrisă de Cantor conducea însă la *paradoxuri,* care provin din „definiţia” foarte permisivă şi vagă a conceptului de mulţime. Însuşi Cantor în 1895 observă că nu se poate vorbi de „mulţimea tuturor ordinalelor” (paradox publicat de Burali-Forti în 1897); mai tîrziu, s-a constatat că există şi alte „mulţimi contradictorii”: „mulţimea tuturor cardinalilor”, „mulţimea tuturor mulţimilor”, „mulţimea mulţimilor care nu se conţin ca element” (paradoxul lui Russel[3]). Prezentăm acest paradox: presupunem că există mulţimea mulţimilor care nu se conţin ca element şi o notăm cu C (în notaţie 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 definiţia lui C, contradicţie. Dacă $C \notin C$, atunci C nu satisface condiţia de definiţie a lui C, deci $C \in C$, contradicţie.

Aceste paradoxuri au putut fi eliminate de *teoria axiomatică a mulţimilor*, care stabileşte *reguli clare de construcţie de mulţimi*. Printre altele, nu se permite considerarea mulţimilor „foarte mari”, care apar mai sus. O primă axiomatizare a fost dată de Zermelo[4] în 1908. Una din axiomele sale (care evită apariţia paradoxurilor de tipul de mai sus) este *Axioma selecţiei*, care în esenţă spune că, fiind date o „proprietate”[5] *P şi o mulţime A*, există „mulţimea elementelor *din A* care satisfac proprietatea *P*”. Cu alte cuvinte, o proprietate nu determină o mulţime (ca în viziunea lui Cantor), ci, *dată o mulţime A*, se poate vorbi doar de existenţa *submulţimii* formată de elementele lui A care satisfac P.

În 1905 matematicianul francez Jules Richard construieşte un paradox de alt tip (simplificat ulterior de Berry şi publicat de Russel în 1906). Să considerăm următorul

[3] Bertrand Russel (1872-1970), matematician şi filozof britanic.
[4] Ernst Friedrich Ferdinand Zermelo (1871-1953), matematician german.
[5] Mai precis, este vorba de un predicat cu o variabilă.

concept: „cel mai mic număr natural care nu poate fi definit cu mai puţin de 17 cuvinte”. Dacă acest număr ar exista, atunci el *poate fi definit cu 16 cuvinte*, chiar de enunţul anterior (care are 16 cuvinte, număraţi). Contradicţia obţinută arată că nu există un astfel de număr. Pe de altă parte, mulţimea numerelor naturale care pot fi definite cu cel mult 16 cuvinte este finită (căci mulţimea frazelor cu cel mult 16 cuvinte care definesc un număr natural este finită) şi deci *există* numere naturale care nu pot fi definite cu mai puţin 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, şi anume *ambiguitatea limbajului* natural, obişnuit. Ce înseamnă exact *a defini* un număr natural?

Din cele spuse reiese că, pe lîngă o axiomatizare a teoriei mulţimilor, trebuie *restrîns limbajul natural* la cîteva modalităţi bine precizate şi simple de exprimare. În acelaşi timp, posibilităţile trebuie să fie suficient de permisive pentru a putea formula orice enunţ matematic. Aceste scopuri sînt realizate de un *limbaj formalizat.*

Vom prezenta intuitiv un astfel de limbaj (o prezentare riguroasă depăşeşte cu mult cadrul şi scopul acestei cărţi). Cu această ocazie, vom sublinia anumite aspecte de logică matematică. În continuare vom descrie axiomele teoriei mulţimilor, aplicaţii (ordinale şi numere naturale). Vom încerca să reliefăm şi modul în care aceste axiome trebuie conştientizate în procesul didactic.

I.1. Limbaj formal, logică

În teoria axiomatică a mulţimilor[6] *toate obiectele sînt mulţimi*. Altfel spus, *nu se face distincţie între conceptele „element” şi „mulţime”.* Acest punct de vedere este firesc, dacă ne gîndim că o mulţime poate fi element al altei mulţimi; în plus, o teorie axiomatică trebuie să pornească de la un minim de noţiuni primare, iar distincţia între element şi mulţime ar complica lucrurile inutil.

Pentru a putea enunţa axiomele teoriei mulţimilor, avem nevoie de prezentarea (intuitivă) a limbajului formal al acestei teorii. Subliniem că <u>nu</u> 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 mulţimilor, poate fi găsit în REGHIŞ [1981]). Mai întîi descriem *sintaxa limbajului* (regulile după care putem forma expresii corecte ale limbajului formal).

[6] Vom prezenta axiomatizarea Zermelo-Fraenkel-Skolem, acceptată în aproape toată matematica modernă.

1.1 Definiţie. O *expresie* (numită şi *enunţ*) a limbajului formal este un şir finit de *simboluri*, format după anumite reguli descrise mai jos. Intuitiv, o expresie exprimă un fapt bine determinat despre mulţimi.

Descriem acum tipurile de simboluri şi construcţia expresiilor limbajului formal:

i) Există simboluri de tip nume, care denumesc *mulţimi* (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 dispoziţie o colecţie suficient de mare de nume constante şi variabile. Exemple de nume: $x, y, a, b, c, A, B, \ldots$

ii) Simbolurile care notează relaţii:

- relaţia de *egalitate*, notată cu simbolul $=$,
- relaţia de apartenenţă, notată cu simbolul $\in$.

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

$x = y$ (citit „x este egal cu y”);

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

iii) Parantezele rotunde "(" şi ")" au rolul de a elimina ambiguităţile.

iv) Conectorii (operatorii) logici se folosesc pentru a exprima proprietăţi mai complexe, pentru a combina mai multe expresii într-una nouă. Operatorii sînt: $\wedge$ (conjuncţia, „şi”), $\vee$ (disjuncţia, „sau”), $\neg$ (negaţia, „non”). Dacă E, F sînt expresii (deja construite), atunci sînt expresii şi următoarele şiruri de simboluri:

$(E) \wedge (F)$ (citită „E şi F”);

$(E) \vee (F)$ (citită „E sau F”);

$\neg(E)$ (citită „non E”).

v) Cuantificatorii logici sînt: $\forall$ (cuantificatorul universal, „oricare”), $\exists$ (cuantificatorul existenţial, „există”). Cu ajutorul cuantificatorilor (numiţi uneori şi *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 şi x este o variabilă (astfel încît E nu conţine $\forall x$ şi nici $\exists x$), 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 şi parantezele pătrate [ ] sau acoladele { }, după regulile uzuale.

Singurele expresii (*enunţuri*) *admise ale limbajului formal sînt cele construite respectînd regulile de mai sus.* În unele cazuri, se poate renunţa 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 conţine nici o cuantificare a lui x (adică nici $\forall x$, nici $\exists x$ nu apar ca subşiruri în E).

Spunem că *variabila x este legată în E* dacă *x nu este liberă în E*, adică E conţine un subşir de simboluri de forma $(\forall x)F$ sau $(\exists x)F$ (unde F este o expresie).

O expresie care nu conţine variabile libere se numeşte *propoziţie.*

Dacă expresia E conţine variabilele *libere* $x_1, \ldots, x_n$, vom sublinia uneori acest lucru scriind $E(x_1, \ldots, x_n)$. Fiind date constantele $c_1, \ldots, c_n$, 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 obţine o nouă expresie (demonstraţi!), notată cu $E(c_1, \ldots, c_n)$. Dacă $x_1, \ldots, x_n$ sînt *toate* variabilele libere din E, atunci $E(c_1, \ldots, c_n)$ este o *propoziţie* (adică o expresie care nu are variabile libere). O expresie care are variabile libere se mai numeşte *predicat.*

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

1.2 Exemple. Presupunem că x, y, z sînt variabile şi a, b sînt constante. Arătaţi că următoarele şiruri 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? Şirurile 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 conţine variabile libere se numeşte *propoziţie*. Oricărei *propoziţii* îi asociem o unică *valoare de adevăr*. Valorile de adevăr sînt: 0 (sau *fals*), şi 1 (sau *adevărat*). O propoziţie cu valoarea de adevăr 0 se numeşte *propoziţie falsă*; o propoziţie cu valoarea de adevăr 1 se numeşte *propoziţie adevărată*. O propoziţie nu poate fi simultan falsă şi adevărată.

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

Fie a, b constante şi x, y variabile.

i) Propoziţiile de forma $a = b$ sînt adevărate exact atunci cînd a şi b denumesc acelaşi obiect (aceeaşi mulţime).

ii) Valoarea de adevăr a propoziţiilor 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 şi numai dacă mulţimea numită a este un element al mulţimii numită de b.

iii) O propoziţie de forma $(E) \wedge (F)$ (unde E şi F sînt propoziţii) este adevărată dacă şi numai dacă E şi F sînt *ambele* adevărate.

iv) O propoziţie de forma $(E) \vee (F)$ este adevărată dacă şi numai dacă *măcar una* din propoziţiile E şi F este adevărată (adică sau E, sau F, sau atît E cît şi F sînt adevărate).

v) O propoziţie de forma $\neg(E)$ este adevărată dacă şi numai dacă propoziţia E este *falsă*.

vi) O propoziţie de forma $(\forall x)(E(x))$ (unde variabila x este liberă în E) este adevărată dacă şi numai dacă pentru *orice* obiect c propoziţia $E(c)$ este adevărată.

vii) O propoziţie de forma $(\exists x)(E(x))$ (unde variabila x este liberă în E) este adevărată dacă şi numai dacă *există măcar un obiect* c astfel încît propoziţia $E(c)$ să fie adevărată.

1.3 Observaţie. Valoarea de adevăr a propoziţiilor 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 combinaţiile posibile de valori de adevăr pentru E şi F. Tabelul se citeşte 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 Definiţie. a) Două propoziţii E şi F se numesc *echivalente* dacă au aceeaşi valoare de adevăr. Scriem aceasta sub forma $E \equiv F$.

b) Definiţia se poate extinde la expresii oarecare. Două expresii E şi F ce conţin aceleaşi constante şi aceleaşi variabile (fie $x_1, \ldots, x_n$ variabilele din E şi F) sînt numite *echivalente* dacă: orice variabilă care este liberă în E este liberă în F (şi reciproc) şi *propoziţiile* $(\forall x_1)(\forall x_2)\ldots(\forall x_n)E(x_1, \ldots, x_n)$ şi $(\forall x_1)(\forall x_2)\ldots(\forall x_n)F(x_1, \ldots, x_n)$ au aceeaşi valoare de adevăr. Scriem atunci $E \equiv F$, sau $E(x_1, \ldots, x_n) \equiv F(x_1, \ldots, x_n)$ dacă vrem să evidenţiem variabilele libere.

1.5 Exerciţiu. Dacă E, F şi G sînt expresii, avem echivalenţele :

$\neg(E \wedge F) \equiv (\neg E) \vee (\neg F)$; $\neg(E \vee F) \equiv (\neg E) \wedge (\neg F)$; (legile lui DeMorgan)

$(E \wedge F) \vee G \equiv (E \vee G) \wedge (F \vee G)$; (distributivitatea lui $\vee$ faţă de $\wedge$)

$(E \vee F) \wedge G \equiv (E \wedge G) \vee (F \wedge G)$; (distributivitatea lui $\wedge$ faţă de $\vee$)

$\neg((\forall x)E) \equiv (\exists x)(\neg E)$; $\neg((\exists x)E) \equiv (\forall x)(\neg E)$ (legile de negare a cuantificatorilor).

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 $\neg(E \wedge F)$ şi $(\neg E) \vee (\neg F)$ demonstrează echivalenţa cerută.

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

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

$E \to F$ în loc de $(\neg E) \vee F$ şi citim „E implică F" sau „dacă E, atunci F"; $\to$ se numeşte operatorul *implicaţie.*

$E \leftrightarrow F$ în loc de $(E \to F) \wedge (F \to E)$ şi citim „E este echivalent cu F".

1.6 Exerciţiu. Scrieţi tabelele de adevăr pentru operatorii $\to$ şi $\leftrightarrow$. Demonstraţi că, dacă E şi F sînt propoziţii, $E \leftrightarrow F$ este adevărată dacă şi numai dacă E şi F au aceeaşi valoare de adevăr.

Insistăm asupra *implicaţiei*, $\to$. Se justifică intuitiv că $E \to F$ este acelaşi lucru cu $(\neg E) \vee F$, astfel: "$E \to F$" înseamnă "dacă E este adevărată, atunci F este adevărată". Altfel spus, sau E este falsă (adică are loc $\neg E$), sau E este adevărată şi atunci automat F este adevărată (adică are loc F); pe scurt, $(\neg E) \vee F$. Este important de conştientizat această echivalenţă logică, utilă mai ales cînd trebuie negată o implicaţie (lucru care intervine frecvent, de exemplu în cazul demonstraţiilor prin reducere la absurd). Astfel, faptul că $E \to F$ este falsă înseamnă că are loc $\neg(E \to F) \equiv \neg((\neg E) \vee F) \equiv E \wedge (\neg F)$ (ipoteza este adevărată şi totuşi concluzia este falsă). Această interpretare este conformă cu intuiţia („bunul-simţ"). De altfel, concluziile bazate pe un calcul logic formal trebuie totdeauna interpretate intuitiv, proces absolut necesar în înţelegerea unor demonstraţii (sau în găsirea unor soluţii la o problemă dată).

Vom mai folosi şi 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 propoziţia $E \to F$ este adevărată, scriem atunci $E \Rightarrow F$. Analog, scrierea $E \Leftrightarrow F$ înseamnă că propoziţia $E \leftrightarrow F$ este adevărată.

1.7 Observaţie. Orice teoremă matematică (propoziţie, lemă etc.) poate fi scrisă în limbaj formal. Expresia obţinută trebuie să fie din punct de vedere logic o *propoziţie* (*nu trebuie să aibă variabile libere*). De exemplu, teorema împărţirii 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 Observaţie. Se foloseşte foarte des în matematică simbolul $\exists!$ (citit *există şi este unic*). Fie $P(x)$ predicat cu o variabilă. Expresia $(\exists!x)P(x)$ înseamnă că *există şi este unic un x cu proprietatea* $P(x)$. Din punct de vedere formal, definiţia 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 încît $P(x)$ să fie adevărată”.

În definiţia formală de mai sus, s-a exprimat faptul că x este unic punînd condiţia ca, de îndată ce y *şi* z satisfac P, să rezulte că $y = z$. Aceasta este şi o metodă de demonstrare a unicităţii în diverse situaţii.

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 definiţia lui $\sqrt{2}$.

I.2. Axiomele teoriei mulţimilor

Prezentăm cîteva elemente din teoria axiomatică Zermelo-Fraenkel-Skolem (ZFS) a mulţimilor. Pentru o tratare mai detaliată, incluzînd 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 rîndul lor definite… Se vede că acest proces nu poate continua la infinit.

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

În axiomatizarea teoriei mulţimilor, noţiunile de *mulţime* şi de *relaţie de apartenenţă* se consideră *noţiuni primare* (nu se definesc) şi *toate obiectele teoriei sînt mulţimi* (în particular, **toate elementele unei mulţimi sînt tot mulţimi**!). Aceste noţiuni satisfac un set de *axiome* (care, într-un anumit sens, *definesc* obiectele respective). Altfel spus, nu ne interesază *ce sînt* mulţimile, ci *cum se comportă* unele faţă de altele şi faţă de relaţia de apartenenţă. Axiomele stabilesc regulile care se aplică obiectelor numite mulţimi şi relaţiei de apartenenţă.

Axiomele sînt *propoziţii* (din limbajul formal construit anterior) care sînt *declarate şi acceptate ca adevărate.* Orice altă afirmaţie despre mulţimi trebuie *demonstrată* pornind de la axiome. În acest mod se deduc toate proprietăţile „uzuale” ale teoriei mulţimilor.

Deşi, după cum am spus, în teoria axiomatică *elementele unei mulţimi sînt tot mulţimi*, vom adopta (pe cît posibil), pentru a nu crea confuzii cititorului, distincţia tradiţională în notaţie: în general, se notează *mulţimile cu majuscule* (*A, B*, …), iar *elementele mulţimilor cu minuscule*

(a, b, …). Dacă A este o mulţime şi a este un element al lui A, atunci scriem $a \in A$ (citit *„a aparţine lui A”* sau *„A conţine pe a”*. Se mai poate scrie $A \ni a$). Dacă a nu este element al mulţimii A, scriem $a \notin A$.

2.1 Axioma extensionalităţii: *Pentru orice două mulţimi A şi B, avem :*

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

Mai riguros spus, propoziţia următoare este adevărată:

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

Această axiomă nu spune decît că *o mulţime este determinată de elementele sale.*[7] O exprimare mai simplă, dar nu foarte precisă, este: *dacă două mulţimi au aceleaşi elemente, atunci mulţimile coincid*.

Observăm că are loc şi implicaţia inversă: dacă $A = B$, atunci orice element care aparţine lui A aparţine şi lui B. Acest fapt este evident: A şi B denumesc acelaşi obiect, deci orice enunţ referitor la A este adevărat şi pentru B (şi reciproc).

Dacă A şi B sînt două mulţimi, vom scrie $A \subseteq B$ (şi citim *A inclus în B* sau *A este submulţime a lui B*) dacă orice element al lui A aparţine şi lui B: $(\forall a)\ [(a \in A) \rightarrow (a \in B)]$. În caz contrar, notăm $A \not\subset B$.

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

Pe această proprietate se bazează majoritatea demonstraţiilor de egalitate de mulţimi: pentru a demonstra că $A = B$, arătăm că orice element al lui A aparţine şi lui B (adică $A \subseteq B$) şi reciproc ($B \subseteq A$).

Axiomele care urmează sînt toate de următorul tip: *fiind date una sau mai multe mulţimi, se garantează existenţa unei noi mulţimi cu anumite proprietăţi* (construită cu ajutorul mulţimilor iniţiale). Cu alte cuvinte, *axiomele descriu construcţii permise în cadrul teoriei*. Se regăseşte astfel motivul pentru care a fost construită teoria: evitarea paradoxurilor generate de construcţii de mulţimi „prea mari”.

2.2 Axioma mulţimii părţilor unei mulţimi. $(\forall M)\ (\exists P)\ ((\forall a)(a \in P \leftrightarrow a \subseteq M))$.

În cuvinte: fiind dată o mulţime M, există o mulţime P astfel încît elementele lui P sînt exact submulţimile lui M.

Mulţimea P a cărei existenţă este garantată mai sus este unic determinată de mulţimea M. Într-adevăr, dacă şi Q satisface condiţia $(\forall A\ (A \in Q \leftrightarrow A \subseteq M))$, atunci avem, pentru orice mulţime A: $A \in Q \leftrightarrow A \subseteq M \leftrightarrow A \in P$. Din axioma extensionalităţii obţinem că $P = Q$.

Notaţia tradiţională pentru P este $\mathcal{P}(M)$ (mulţimea părţilor lui M).

---

[7] De aici provine şi denumirea de "axioma extensionalităţii": două mulţimi sînt egale dacă au aceeaşi "întindere", "extensiune".

2.3 Axioma reuniunii. *Pentru orice mulţime A* (*subînţeles: avînd ca elemente tot mulţimi*), *există o mulţime ale cărei elemente sînt elementele mulţimilor din A*, *adică*:

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

Pentru înţelegerea acestei axiome, este util să privim A ca pe o *familie de mulţimi*. Axioma de mai sus nu face decît să postuleze existenţa *reuniunii* acestei familii de mulţimi.

Mulţimea U – a cărei existenţă este garantată de axiomă – este unic determinată de A (demonstraţi!) şi se notează $\bigcup A$ sau $\bigcup_{x \in A} x$ sau $\bigcup\{x \mid x \in A\}$. A se remarca în acest context futilitatea distincţiei dintre element şi mulţime.

2.4 Schema de axiome de substituţie

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 obţine o axiomă. Aşadar, avem de a face cu *o infinitate* de axiome.

Pentru enunţ, avem nevoie de o **definiţie**. O expresie $E(x, y)$ cu exact două variabile libere x şi y se numeşte *relaţie funcţională* 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 relaţie funcţională ca pe o „funcţie parţial definită": pentru anumiţi x există un unic y astfel încît $E(x, y)$ să aibă loc; se notează uneori chiar „funcţional", $y = \widetilde{E}(x)$ în loc de $E(x, y)$. Observăm că nu este neapărat adevărat că $(\forall x)(\exists y)E(x, y)$.

În termeni mai puţin formali, axioma-schemă a substituţiei afirmă că: *Pentru orice relaţie funcţională* $E(x, y)$ *şi pentru orice mulţime a, există „imaginea prin E a mulţimii a"*.

Evident, trebuie să definim formal conceptul de „imagine a unei mulţimi printr-o relaţie funcţională". Spunem că mulţimea b este *imaginea mulţimii a prin relaţia funcţională* $E(x, y)$ dacă „elementele lui b sînt de forma $\widetilde{E}(x)$, cu $x \in a$", adică:

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

Axioma-schemă a substituţiei este: *pentru orice relaţie funcţională* $E(x, y)$, *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 obţine cîte o axiomă pentru fiecare alegere a unei relaţii funcţionale E*. Nu se pot condensa toate aceste enunţuri într-unul singur, de tipul

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

deoarece acesta *nu* este o expresie a limbajului formal: E nu denumeşte un *obiect* legitim (o mulţime), ci o *expresie*.

Folosind axioma extensionalităţii, se demonstrează imediat că *imaginea unei mulţimi printr-o relaţie funcţională este unic determinată* (mulţimea b a cărei existenţă este postulată de axioma schemă a substituţiei este unic determinată de E şi b).

2.5 Consecinţă (*Schema de comprehensiune, Axioma selecţiei*). *Pentru orice mulţime A şi pentru orice expresie cu o variabilă liberă P*(x)*, există submulţimea elementelor din A pentru care P este adevărată. Formal,* $(\forall A)(\exists B)(\forall x)[x \in B \leftrightarrow (x \in A \wedge P(x))]$.[8]

Demonstraţie. Fie expresia $E(x,y)$: "$(x = y) \wedge P(y)$". Afirmăm că E este o relaţie funcţională. Într-adevăr, fie x, y, z cu $E(x,y)$ şi $E(x,z)$ adevărate. Atunci $x = y$ şi $x = z$, deci $y = z$.

Conform axiomei substituţiei, pentru mulţimea A există o mulţime B astfel încît:

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

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. □

Iarăşi, axioma extensionalităţii asigură că A şi $P(x)$ determină *unic* mulţimea B din enunţ. Această mulţime se notează tradiţional:

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

2.6 Observaţie. *S-a eliminat paradoxul lui Russel*: nu mai este permisă construirea mulţimii (şi nu sînt permise scrieri de tipul)

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

Există însă, <u>pentru orice A mulţime dată</u>, $\{x \in A \mid P(x)\}$.

2.7 Observaţie. Dacă se presupune că există măcar o mulţime[9] A, rezultatul de mai sus asigură existenţa unei (unice) mulţimi ce nu conţine nici un element, numită *mulţimea vidă* şi notată cu $\varnothing$.[10] Într-adevăr, fie $P(x)$: "$x \neq x$". Din schema de comprehensiune, există $\varnothing := \{x \in A \mid x \neq x\}$. Pentru orice x, avem $x \notin \varnothing$ (dacă $x \in \varnothing$, atunci $x \neq x$, absurd). Unicitatea lui $\varnothing$ este o consecinţă a axiomei extensionalităţii. Notăm deci:

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

Pentru orice mulţime M are loc $\varnothing \subseteq M$. Este instructiv să prezentăm în detaliu acest argument. Conform definiţiei, avem $\varnothing \subseteq M$ dacă şi numai dacă $\forall x\ (x \in \varnothing \to x \in M)$. Dar expresia $x \in \varnothing \to x \in M$ este, conform definiţiei, o prescurtare pentru $\neg(x \in \varnothing) \vee (x \in M)$, care este adevărată, căci $\neg(x \in \varnothing)$ este adevărată.

Termenul de *comprehensiune* descrie modalitatea de a *preciza o mulţime prin enunţarea unei proprietăţi pe care o au doar elementele mulţimii şi numai ele*. S-a văzut că acest concept, care a stat la baza teoriei naive a mulţimilor, duce la paradoxuri; schema de

---

[8] În axiomatizarea lui Zermelo din 1908, acest rezultat era enunţat ca axiomă şi era numit *Axioma selecţiei*.
[9] Axioma infinităţii, enunţată mai jos, asigură faptul că există o mulţime.
[10] Nu este litera grecească majusculă *phi*, Φ, ci un simbol matematic derivat dintr-o literă norvegiană, Ø.

comprehensiune restrînge această modalitate doar la posibilitatea următoare: pentru orice *mulţime dată* M şi orice „proprietate” P, există *submulţimea* elementelor lui M care satisfac P.

2.8 Observaţie. Putem acum defini şi alte „operaţii cu mulţimi”. Astfel, pentru orice două mulţimi A şi B, arătaţi că există mulţimile:

$\{x \in A \mid x \in B\}$ (notată $A \cap B$ şi numită *intersecţia* lui A şi B)

$\{x \in A \mid x \notin B\}$ (notată $A \setminus B$ şi numită *diferenţa* lui A şi B).

Demonstraţi că $A \cap B = B \cap A$.

Exerciţii

1. Ce este o mulţime? Ce sînt axiomele? De ce sînt necesare axiomele şi limbajul formal?

2. Scrieţi măcar 5 expresii în limbaj formal folosind doar variabilele x şi y.

3. Demonstraţi că mulţimile a căror existenţă este garantată de axiome sînt unic determinate.

4. Folosind axiomele şi existenţa mulţimii vide, construiţi 4 mulţimi distincte.

5. Daţi exemplu de mulţime $A \neq \varnothing$ astfel încît $\bigcup A = \varnothing$. Cîte astfel de mulţimi există?

6. Are loc întotdeauna $\bigcup A \subseteq A$? Dar $A \subseteq \bigcup A$?

7. Fie A, B mulţimi. Scrieţi o expresie a limbajului formal care să semnifice că:

a) Mulţimea A nu este inclusă în mulţimea B.

b) $A \neq B$ (folosiţi doar relaţia de apartenenţă).

c) A conţine măcar un element.

d) A conţine cel mult un element.

e) A este submulţime a oricărei mulţimi.

f) A este element al oricărei mulţimi.

g) $B \subseteq \bigcup A$.

Pentru fiecare enunţ de mai sus, scrieţi negaţia sa în limbaj natural şi formal.

8. Fie expresia din limbajul teoriei mulţimilor: $(\exists V)(\forall t)(t \notin V)$.

a) Cîte variabile libere are?

b) Formulaţi expresia de mai sus în limbaj natural.

9. Aceeaşi problemă ca mai sus, pentru expresia:

$$(\forall x)(\forall y)(\exists z)((\forall t)(t \in z) \leftrightarrow ((t = x) \vee (t = y)))$$

I.3. Clase, relaţii, funcţii

Nu există o „mulţime a tuturor mulţimilor", căci acest concept conduce la paradoxuri. Dacă ar exista mulţimea tuturor mulţimilor, fie aceasta $\boldsymbol{A}$, atunci, conform schemei de comprehensiune, ar exista şi mulţimea $C = \{B \in \boldsymbol{A} \mid B \notin B\}$. Se vede că regăsim paradoxul lui Russel. Astfel de colecţii „foarte mari" de obiecte apar însă frecvent în matematică (dorim de exemplu să vorbim de o proprietate pe care o au „toate" grupurile) şi este necesară precizarea unui cadru riguros pentru aceste situaţii. O rezolvare rezonabilă este dată de conceptul de *clasă*.

În cadrul teoriei Gödel-Bernays (GB), *clasa* este o noţiune primară (nu se defineşte clasa, ci este dat un set de axiome referitoare la clase; mulţimile vor fi un tip particular de clase – cele care sînt elemente ale altor clase). Teoria astfel dezvoltată este însă considerabil mai complicată decît ZFS [11].

În teoria ZFS, prin *clasă* se înţelege o expresie cu o variabilă liberă (un predicat cu o variabilă)[12]. Cu alte cuvinte, o proprietate nu mai defineşte o *mulţime* de obiecte, ci este privită ea însăşi ca o entitate şi 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 substituţiei). De exemplu, predicatul $P(x)$: „$x = x$" este evident satisfăcut de orice mulţime x; acest predicat defineşte „clasa tuturor mulţimilor". Abuzînd de limbajul de la mulţimi, 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 aparţine clasei P" sau „x este un element al clasei P".

Observăm că orice mulţime a defineşte o clasă, anume „$x \in a$". Reciproc, spunem că o clasă $P(x)$ *corespunde* unei mulţimi 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 mulţime.

În acest sens, *clasa tuturor mulţimilor nu corespunde unei mulţimi*. Demonstraţia a fost dată chiar la începutul acestui paragraf!

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

În această terminologie, schema de comprehensiune nu spune altceva decît că *intersecţia dintre o clasă şi o mulţime este o mulţime.*

[11] În plus, s-a arătat că orice enunţ despre mulţimi demonstrabil în GB este demonstrabil în ZFS.
[12] Această interpretare pentru clase a fost prezentată de W. Quine în 1963.

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

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

3.1 Propoziţie ***(Teorema perechii)****. Fie a şi b două mulţimi. Atunci există o mulţime c care are ca elemente pe a şi pe b şi numai pe ele. Formal:*

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

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

Demonstraţie. Ideea este de a construi o mulţime cu două elemente D şi de a obţine $\{a, b\}$ ca imaginea lui D printr-o relaţie funcţională bine aleasă (se aplică deci axioma substituţiei).

Ştim că există mulţimea vidă $\varnothing$. Construim (cu axioma mulţimii părţilor) mulţimea $\mathcal{P}(\varnothing)$, care are un element (avem $\varnothing \subseteq \varnothing$, deci $\varnothing \in \mathcal{P}(\varnothing)$; $\varnothing$ este chiar unicul element al lui $\mathcal{P}(\varnothing)$) deci $\mathcal{P}(\varnothing) = \{\varnothing\}$). Cum $\varnothing$ nu are nici un element, deducem că $\mathcal{P}(\varnothing) \neq \varnothing$. Construim acum $\mathcal{P}(\mathcal{P}(\varnothing)) = \mathcal{P}(\{\varnothing\})$. Unicele mulţimi incluse în $\{\varnothing\}$ sînt $\varnothing$ şi $\{\varnothing\}$, deci $\mathcal{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$ are două elemente (cum am dorit).

Fie $E(x, y)$: "$(x = \varnothing \wedge y = a) \vee (x = \{\varnothing\} \wedge y = b)$" (verificaţi că este o relaţie funcţională). Imaginea prin E a lui $\mathcal{P}(\{\varnothing\})$ este chiar mulţimea căutată c.

Unicitatea lui c rezultă din axioma extensionalităţii. □

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

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

3.2 Exerciţiu. Fie a şi b mulţimi. Demonstraţi că există reuniunea lor $a \bigcup b$ (adică unica mulţime cu proprietatea $\forall x[(x \in a \bigcup b) \leftrightarrow (x \in a \vee x \in b)]$).

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

3.3 Definiţie. Fie a şi b mulţimi. Aplicînd teorema perechii mulţimilor a şi a, există mulţimea $\{a\}$; există şi $\{a, b\}$. Aplicînd din nou teorema perechii, există mulţimea $\{\{a\}, \{a, b\}\}$, care se notează cu (a, b) şi se numeşte *perechea ordonată* (*cuplul*) format de a şi b. Observaţi că, dacă $a = b$, atunci $(a, b) = \{\{a\}\}$.

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

3.4 Propoziţie. *Fie a, b, a', b' mulţimi. Atunci are loc:* $(a, b) = (a', b') \Leftrightarrow$ *(a = a' şi b = b').* □

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

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

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

şi, prin recurenţă, *n-uplu*, $\forall n \geq 3$ (pentru o tratare riguroasă a inducţiei şi recurenţei, vezi **I.4.21**)

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

Are loc: $(a_1, \ldots, a_n) = (b_1, \ldots, b_n) \leftrightarrow a_1 = b_1 \wedge \ldots \wedge a_n = b_n$.

În manualele de liceu (şi în multe alte cărţi de matematică), o *funcţie* definită pe o mulţime A cu valori într-o mulţime 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 foloseşte noţiunea nedefinită de *procedeu* (*lege*)); în plus, se subînţelege că pentru orice funcţie se poate descrie un *procedeu* (*algoritm*) de obţinere a imaginii oricărui element prin funcţia dată. Acest lucru nu este necesar şi în matematică se întîlnesc exemple de funcţii pentru care acest fapt nu are loc.

Se observă însă că o funcţie $f : A \to B$ este perfect determinată de *graficul* său, adică de mulţimea cuplurilor $\{(a, f(a)) \mid a \in A\}$. Aceasta este şi ideea definiţiei conceptului de funcţie în cadrul unei tratări riguroase. Începem cu alte două noţiuni, şi ele fundamentale:

3.5 Definiţie. Fie A şi B mulţimi. Numim *produsul cartezian*[13] al mulţimilor A şi B mulţimea $A \times B := \{(a, b) \mid a \in A \wedge b \in B\}$.

Avem dreptul de a defini o astfel de mulţime? Ar trebui să arătăm că ne încadrăm în schema de comprehensiune, adică să indicăm o mulţime a cărei existenţă este certă, care să conţină toate perechile de forma (a, b) cu $a \in A$ şi $b \in B$. Dar $(a, b) = \{\{a\}, \{a, b\}\}$. Observăm că avem $\{a\} \in \mathcal{P}(A \cup B)$ şi $\{a, b\} \in \mathcal{P}(A \cup B)$, deci $\{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$. Astfel, putem defini, respectînd 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 noţiunile de *relaţie* şi de *funcţie*:

---

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

3.6 Definiţie. Fie A şi B două mulţimi.

a) Numim *relaţie binară între A şi 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 relaţie între A şi B”. Dacă $A = B$, scriem (A, ρ) şi spunem că ρ este *o relaţie pe A*. Adeseori, în loc de $(x, y) \in \rho$ se scrie $x\rho y$. Dacă sînt subînţelese mulţimile A şi B, se spune, simplu, "relaţia ρ" în loc de (A, B, ρ).

b) O relaţie binară f de la A la B se numeşte *funcţie* (sau *aplicaţie*) *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 funcţie de la A la B dacă:

$$\begin{aligned}&(f \subseteq A\times B) \wedge (\forall a)\{(a \in A) \rightarrow (\exists b)[(b \in B) \wedge (a, b) \in f]\} \wedge \\ &(\forall a)(\forall b)(\forall b')\{(a \in A) \wedge (b \in B) \wedge (b' \in B) \wedge (a, b) \in f \wedge (a, b') \in f \rightarrow (b = b')\}\end{aligned} \qquad (*)$$

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

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

Se mai spune „*f este o funcţie* (*aplicaţie*) *de la A la B*” şi se notează aceasta prin $f : A \rightarrow B$ sau $A \xrightarrow{f} B$. *Notaţia* $f : A \rightarrow B$ *nu este decît o prescurtare a faptului că expresia* (*) este propoziţie adevărată.

Mulţimea A se numeşte *domeniul* funcţiei f şi B se numeşte *codomeniul* lui f. Orice element a din domeniul lui f se numeşte *argument* al funcţiei f. Dacă $a \in A$ şi $b \in B$ astfel încît $f(a) = b$, b se numeşte *valoarea funcţiei f în a*.

Pentru orice mulţime A, notăm cu $\mathbf{1}_A$ sau cu id_A *funcţia identitate* a mulţimii A, anume: $id_A(a) = a$, $\forall a \in A$. Cum se defineşte $\mathbf{1}_A$ ca relaţie de la A la A?

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

3.7 Observaţie. Condiţia (*) se scrie, mai puţin formalizat:

$(f \subseteq A\times B)$ şi $\forall a \in A, \exists\, b \in B$ astfel încît $(a, b) \in f$ şi

$\forall a \in A, \forall b, b' \in B, (a, b) \in f$ şi $(a, b') \in f$ implică $b = b'$.

Observăm că, în expresii, şirurile de forma "$(\forall a)(a \in A)$" se scriu adesea prescurtat "$\forall a \in A$". Această convenţie, larg răspîndită, ascunde o capcană: o implicaţie, de genul $(\forall a)[(a \in A) \rightarrow P(a)]$, se scrie adesea "$\forall a \in A$, $P(a)$", în care implicaţia $\rightarrow$ nu apare explicit. Trebuie conştientizat acest fapt, mai ales cînd apare necesitatea negării unei astfel de expresii: negaţia 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 Observaţie. O expresie cu exact două variabile libere se numeşte *relaţie*. Pentru orice relaţie $R(x, y)$ putem defini "*domeniul*" D_R şi "*imaginea*" I_R ca fiind *clasele*:

$D_R(x)$: "$(\exists y)R(x, y)$"

$$I_R(y): \text{"}(\exists x)R(x, y)\text{"}$$

Demonstraţi că, dacă clasele D_R şi I_R sînt mulţimi, atunci relaţiei $R(x, y)$ i se asociază o relaţie ρ între D_R şi I_R (în sensul definiţiei **3.6.**a), $\rho := \{(x, y) \in D_R \times I_R \mid R(x, y) \text{ adevărată}\}$. Mai mult, această relaţie este *funcţie* (în sensul definiţiei **3.6.**b) dacă şi numai dacă R este *relaţie funcţională*. Invers, unei funcţii $f : A \to B$ i se asociază o relaţie funcţională $F(x, y)$: "$x \in A \wedge y = f(x)$".

Demonstraţi că, dacă R este relaţie funcţională şi D_R este mulţime, atunci I_R este mulţime. Reciproca este adevărată?

3.9 Exerciţiu. Fie A o mulţime. Cîte funcţii $\varphi : \varnothing \to A$ (respectiv $\varphi : A \to \varnothing$) există?

3.10 Definiţie. Fie $f : A \to B$ o funcţie. Dacă $A' \subseteq A$, se defineşte *imaginea lui A' prin f* ca fiind imaginea mulţimii A' prin relaţia funcţională asociată lui f. Cu alte cuvinte, definim

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

Notaţia tradiţională pentru imaginea lui A' prin f este $f(A')$; nu se poate folosi o astfel de notaţie în teoria axiomatică a mulţimilor, pentru că A' poate fi simultan submulţime a lui A şi element al lui A (puteţi da exemplu de un astfel de caz?) şi este foarte posibil ca $f(A')$ (valoarea în A' a lui f) să difere de $f[A']$ (imaginea submulţimii A' prin f).

3.11 Definiţie. Fie I o mulţime (interpretată ca mulţime de „indici”). O funcţie $b : I \to M$, unde M este o mulţime, se numeşte *familie de mulţimi indexată după I*. Notaţii tradiţionale pentru această noţiune: $(B_i)_{i \in I}$ (unde $B_i := b(i)$), sau $\{B_i \mid i \in I\}$.

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

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

Intersecţia familiei $\{B_i\}_{i\in I}$ este, prin definiţie

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

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

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

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

3.12 Propoziţie. *Pentru orice mulţimi A, B, C, şi orce familie de mulţimi $(B_i)_{i \in I}$ au loc egalităţile:*

i) $\varnothing \cap A = \varnothing$, $\varnothing \cup A = A$, $A \setminus \varnothing = A$, $A \setminus A = \varnothing$;

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) $A\bigcap(\bigcup_{i\in I} B_i) = \bigcup_{i\in I}(A\bigcap B_i)$; $A\bigcup(\bigcap_{i\in I} B_i) = \bigcap_{i\in I}(A\cup B_i)$.

vii) $A\bigcup A = A = A\bigcap A$. □

3.13 Definiţie. Se numeşte *inversă a unei relaţii* (A, B, ρ) relaţia (B, A, ρ^{-1}) unde $\rho^{-1} = \{(b, a) \mid (a, b) \in \rho\} \subseteq B \times A$.

Fie relaţiile (A, B, ρ) şi (B, C, τ). Relaţia $(A, C, \tau\circ\rho)$, 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*) *relaţiilor* τ şi ρ.

3.14 Propoziţie. *a) Fiind date funcţiile* $u : A \to B$, $v : B \to C$, *compusa* $v\circ u$ *este tot o funcţie,* $v\circ u : A \to C$, *şi,* $\forall a \in A$, *are loc:*

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

b) Pentru orice relaţii (A, B, ρ), (B, C, τ), (C, D, η), *avem* $(\eta\circ\tau)\circ\rho = \eta\circ(\tau\circ\rho)$ (*compunerea relaţiilor este asociativă*). *În particular, compunerea funcţiilor este asociativă.* □

Se disting următoarele tipuri remarcabile de funcţii:

3.15 Definiţie. Fie $f : A \to B$ o funcţie. Spunem că f este:

i) *funcţie injectivă* dacă $\forall x, y \in A, f(x) = f(y) \Rightarrow x = y$;

ii) *funcţie surjectivă* dacă $\forall y \in B, \exists\, x \in A$ astfel încît $f(x) = y$;

iii) *funcţie bijectivă* dacă este injectivă şi surjectivă;

iv) *funcţie inversabilă* dacă $\exists\; g : B \to A$ (numită inversa lui f) astfel încît $(g\circ f)(x) = x$, $\forall x \in A$ şi $(f\circ g)(y) = y$, $\forall y \in B$.

Notînd, pentru o mulţime M, prin $\mathbf{1}_M : M \to M$ funcţia $\mathbf{1}_M(x) = x$, $\forall x \in M$ (numită şi *funcţia identitate* a lui M, notată şi cu id_M sau id), condiţiile ce definesc funcţia 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 Propoziţie. *Fie* $f : A \to B$ *şi* $g : B \to C$ *funcţii. Atunci:*

a) f *este inversabilă* $\Leftrightarrow$ f *este bijectivă;*

b) $g\circ f$ *este bijectivă* $\Rightarrow$ g *este surjectivă şi* f *este injectivă;*

c) Compunerea a două funcţii injective (*surjective*) *este funcţie injectivă* (*surjectivă*). □

Definiţia produsului cartezian poate fi extinsă prin recurenţă la o familie de trei sau mai multe mulţimi, sau, mai general, la o familie oarecare de mulţimi:

3.17 Definiţie. a) Fiind date mulţimile A_1, A_2, A_3 [14], 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 $n \geq 3$ şi orice familie de n mulţimi $A_1, A_2, \ldots, A_n$, definim (prin recurenţă[15]):

[14] În această ordine! De fapt, se dă o *familie de mulţimi* indexată după $\{1, 2, 3\}$.

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

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

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

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

c) Este necesară şi o definiţie în cazul general al unei familii de mulţimi $(A_i)_{i \in I}$ indexată după o mulţime de indici I. Se defineşte produsul cartezian $\prod_{i \in I} A_i$:

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

3.18 Observaţie. Produsul cartezian definit ca la c), în cazul unei familii finite de mulţimi, nu este acelaşi cu cel definit la a) şi b) şi la **3.5**. Există însă o bijecţie naturală între mulţimile obţinute prin cele două definiţii. De exemplu, dacă $I = \{1, 2\}$, avem funcţia bijectivă β, definită pe $\{\varphi : \{1, 2\} \to A_1 \cup A_2 \mid \varphi(i) \in A_i, \forall i \in I\}$ cu valori în $A_1 \times A_2$, dată de $\beta(\varphi) = (\varphi(1), \varphi(2))$. Se pot astfel identifica noţiunile de produs cartezian definite mai sus.

Definim următoarele *tipuri remarcabile de relaţii pe o mulţime*:

3.19 Definiţie. Fie o mulţime nevidă A şi ρ o relaţie pe A. Spunem că ρ este:

- *reflexivă* dacă $a\rho a$, $\forall a \in A$. Formal: $(\forall a)(a \in A \to a\rho a)$;
- *ireflexivă* dacă $\forall a \in A$, *nu* are loc $a\rho a$;
- *simetrică* dacă $\forall a, b \in A$, $a\rho b \to b\rho a$;
- *asimetrică* dacă $\forall a, b \in A$, $a\rho b \to \neg b\rho a$;
- *antisimetrică* dacă $\forall a, b \in A$, $a\rho b$ şi $b\rho a \to a = b$;
- *tranzitivă* dacă $\forall a, b, c \in A$, $a\rho b$ şi $b\rho c \to a\rho c$;
- *relaţie de echivalenţă* dacă este reflexivă, simetrică şi tranzitivă. Pentru relaţii de echivalenţă se folosesc notaţii de tipul $a \equiv b$, $a \sim b$ în loc de $a\rho b$.
- *relaţie de preordine* dacă este reflexivă şi tranzitivă;
- *relaţie de ordine* dacă este reflexivă, tranzitivă şi antisimetrică. Pentru relaţii de (pre)ordine se folosesc în general notaţii de tipul $a \le b$ în loc de $a\rho b$.
- *relaţie de ordine strictă* dacă este ireflexivă şi tranzitivă. Pentru relaţii de ordine strictă se folosesc în general notaţii de tipul $a < b$ în loc de $a\rho b$.

Relaţiile de *ordine* şi de *echivalenţă* sînt deosebit de importante în toată matematica şi este esenţială o bună cunoaştere a proprietăţilor lor.

3.20 Exerciţiu. a) Scrieţi formal condiţiile de mai sus referitoare la o relaţie ρ.

[15] Folosim deocamdată o accepţie intuitivă a noţiunii de definiţie prin recurenţă. Pentru o tratare riguroasă, vezi **4.21** şi următoarele.

b) Cum se generalizează definiţiile anterioare la *relaţii* (în sensul de expresii cu două variabile libere)? De exemplu, o relaţie $R(x, y)$ se numeşte reflexivă dacă $(\forall x)R(x, x)$.

c) Exprimaţi definiţiile de mai sus în termeni de incluziuni şi compuneri de relaţii (şi eventual de inverse). De exemplu, ρ este reflexivă însemnă că $id_A \subseteq \rho$; ρ este simetrică înseamnă că $\rho^{-1} \subseteq \rho$.

Dacă $\leq$ este o relaţie de ordine pe A, scriem $(A, \leq)$ şi spunem că $(A, \leq)$ este *mulţime ordonată*. Dacă pentru orice $a, b \in A$ avem $a \leq b$ sau $b \leq a$, atunci $(A, \leq)$ se numeşte mulţime *total ordonată* (sau *lanţ*) şi relaţia $\leq$ se numeşte relaţie de *ordine totală*. Uneori, pentru a sublinia că o anumită relaţie de ordine nu este totală, se spune *relaţie de ordine parţială*. În loc de $a \leq b$ se scrie şi $b \geq a$. Se observă că, dacă $\leq$ este o relaţie de ordine pe A, atunci $\geq$ este tot o relaţie de ordine.

3.21 Observaţie. Dacă $\leq$ este o relaţie de ordine pe A, atunci relaţia $<$ pe A, definită prin: $x < y \leftrightarrow (x \leq y \wedge x \neq y)$ este o relaţie 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 obţine o relaţie de ordine pe A. Verificaţi! Aşadar, există o bijecţie între relaţiile de ordine pe A şi relaţiile de ordine strictă pe A. De aceea, orice definiţie sau rezultat aplicabil unei relaţii de ordine se aplică şi relaţiei de ordine strictă asociate (şi reciproc). Cum trebuie adaptate aceste consideraţii la *relaţiile* văzute în sensul de la **3.8**?

3.22 Definiţie. Fie $(A, \leq)$ o mulţime ordonată şi B o submulţime a lui A. Un element $m \in A$ se numeşte *minorant* al lui B dacă $m \leq b$, $\forall b \in B$. Un element $M \in A$ se numeşte *majorant* al lui B dacă $b \leq M$, $\forall b \in B$. Submulţimea B se numeşte *minorată* (resp. *majorată*) dacă are un minorant (resp. majorant). Dacă B conţine un minorant m pentru B, spunem că m este *cel mai mic element* (sau *primul element*) *al lui B*. Notaţie: $m = \min(B)$.

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

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) şi $m' \leq m$ (m' este prim element), deci $m = m'$ din antisimetrie. La fel, *ultimul element al lui B este unic* (*dacă există*).

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

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

este o relaţie de ordine, care *nu este totală* (nu are loc nici $2|3$, nici $3|2$); 0 *este ultimul element* al lui $(\mathbb{N}, |)$ şi 1 *este primul element* al lui $(\mathbb{N}, |)$. Relaţia 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 mulţime $(A, \leq)$ cu proprietatea că orice submulţime nevidă B a lui A are un prim element se numeşte mulţime *bine ordonată* (caz în care relaţia $\leq$ pe A se numeşte *relaţie de bună* *ordine*). Mulţimile bine ordonate sînt foarte importante: pe o mulţime bine ordonată se poate aplica un raţionament prin *inducţie*.

Orice mulţime bine ordonată este total ordonată (demonstraţi!).

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

3.25 Definiţie. Fie $(A, \leq)$ o mulţime ordonată şi B o submulţime a sa. Fie $Maj(B)$ mulţimea majoranţilor lui B. Dacă există cel mai mic element al lui $Maj(B)$, acest element se numeşte *supremumul* (sau *marginea superioară a*) lui B şi se notează $\sup B$. Dacă există $\sup B = c$, atunci c este „*cel mai mic majorant al lui B*”, adică satisface condiţiile:

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

„Dual” (considerînd relaţia de ordine $\geq$) se obţine noţiunea de *infimum* (sau *margine inferioară*) al submulţimii B a lui $(A, \leq)$, notat (dacă există!) cu $\inf B$.

O mulţime ordonată $(A, \leq)$ cu proprietatea că orice submulţime cu două elemente a sa are supremum şi infimum se numeşte *latice*. Dacă orice submulţime a lui A are sup şi inf, A se numeşte *latice completă*.

De exemplu, pentru o mulţime nevidă oarecare M, mulţimea $\mathcal{P}(M)$ a părţilor lui M este ordonată de relaţia 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 submulţime nevidă majorată are supremum (aceasta este o proprietate fundamentală a lui $\mathbb{R}$, esenţială în Analiză). În $\mathbb{Q}$, nu orice submulţime nevidă are supremum (justificaţi!).

Exerciţii

1. Dacă $f : A \to B$ este o funcţie, iar $C, D \subseteq A$, scrieţi formal că $f[C] = f[D]$.

2. Fie $f : A \to B$ o funcţie şi $E \subseteq B$. Definim $f^{-1}(E) = \{a \in A \mid f(a) \in E\}$ (numită *contraimaginea* lui E prin f). Definim $f^* : \mathcal{P}(B) \to \mathcal{P}(A), f^*(E) = f^{-1}(E)$, $\forall E \in \mathcal{P}(B)$. Definim $f_* : \mathcal{P}(A) \to \mathcal{P}(B), f_*(D) = f[D]$, $\forall D \in \mathcal{P}(A)$.

a) Demonstraţi că următoarele afirmaţii 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) Demonstraţi că următoarele afirmaţii sînt echivalente:

(i) f este surjectivă;

(ii) f_* este surjectivă;

(iii) f^* este injectivă;

3. Fie $f : A \to B$ o funcţie.

a) Demonstraţi că f este injectivă dacă şi numai dacă are loc: oricare ar fi o mulţime C şi oricare ar fi $u, v : C \to A$ astfel încît $f \circ u = f \circ v$, rezultă $u = v$. ("f este monomorfism în categoria *Set*").

b) Demonstraţi că f este surjectivă dacă şi numai dacă are loc: oricare ar fi o mulţime C şi oricare ar fi $u, v : A \to C$ astfel încît $u \circ f = v \circ f$, rezultă $u = v$. ("f este epimorfism în categoria *Set*").

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

a) Definiţia de mai sus nu respectă Observaţia **2.6.** Cum trebuie modificată încît să o respecte?

b) Demonstraţi că există o bijecţie între $\{0, 1\}^A$ şi $\mathcal{P}(A)$. (aici 0 şi 1 notează două mulţimi distincte oarecare, de exemplu $0 = \emptyset$, $1 = \{\emptyset\}$.

c) Demonstraţi că există o bijecţie între $(A \times B)^C$ şi $A^C \times B^C$.

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

(a) Cîte elemente are $A \times B$?

(b) Cîte relaţii binare de la A la B există?

(c) Cîte funcţii definite pe A cu valori în B există?

(d) Cîte funcţii injective definite pe A cu valori în B există?

I.4. Ordinale, axioma infinităţii şi mulţimea numerelor naturale

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

O modalitate de abordare a introducerii lui $\mathbb{N}$ este dată de *axiomatica Dedekind-Peano*. *Noţiunile primare* sînt cele de *număr natural* şi *funcţie succesor*[16]. Limbajul acestei teorii axiomatice este format din:

- 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 mulţimilor), 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* şi notat $s(n)$ sau n^+: $(\forall n)(\exists n^+)$.

3. Orice două numere naturale cu acelaşi succesor sînt egale: $(\forall m)(\forall n)(m^+ = n^+ \to m = n)$.

4. 0 nu este succesorul nici unui număr natural: $(\forall n)(n^+ \neq 0)$.

5. (**Axioma inducţiei**) Pentru orice predicat cu o variabilă $A(n)$ are loc:

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

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

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

Începem cu o abordare intuitivă. Instrumentele oferite pînă acum de axiomele teoriei mulţimilor permit considerarea următorului „şir de mulţimi”:

$$\varnothing; \{\varnothing\}; \{\varnothing, \{\varnothing\}\}; \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}; \ldots \tag{1}$$

Se observă că, pentru fiecare termen x al şirului, următorul termen este $x \bigcup \{x\}$. Primul termen are 0 elemente, al doilea are 1 element ş.a.m.d. Ar fi tentant să considerăm drept mulţime a numerelor naturale „mulţimea tuturor termenilor acestui şir”, $\varnothing$ să joace rolul lui 0, iar funcţia succesor să fie $s(x) = x \bigcup \{x\}$. Apar două probleme: *definirea riguroasă* a „mulţimii

[16] Întrucît este vorba de o teorie axiomatică, funcţia succesor nu este a priori o *funcţie* în sensul teoriei mulţimilor (ci este o noţiune primară); este adevărat însă că în *modelul* pe care îl construim, rolul funcţiei succesor va fi jucat de o funcţie în sens uzual.

tuturor termenilor şirului (1)" şi garantarea *existenţei* unei astfel de mulţimi. Faptul că există o mulţime care *include* toţi termenii şirului (1) este asigurat de o nouă axiomă:

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

Intuitiv, este clar că axioma de mai sus garantează existenţa unei mulţimi M care să conţină toate mulţimile şirului (1); aceasta nu înseamnă că M conţine *doar* aceste mulţimi. Vom adopta următoarea strategie: definim riguros *clasa* mulţimilor din şirul (1) (aceasta va fi clasa *ordinalelor finite*, noţiune pe care o vom defini în cele ce urmează); atunci mulţimea $\mathbb{N}$ a numerelor naturale va fi obţinută prin comprehensiune, ca fiind mulţimea acelor elemente din M (dată de axioma infinităţii) 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 Definiţie. O mulţime α se numeşte *ordinal* dacă are următoarele proprietăţi:

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

ii) relaţia de apartenenţă defineşte o relaţie de *ordine strictă* pe α, care este o *bună ordine* pe α. Detaliind, această condiţie este echivalentă cu:

- $\forall x, y, z \in \alpha$, din $x \in y$ şi $y \in z$ rezultă că $x \in z$ (*tranzitivitatea* relaţiei $\in$);
- $\forall x, y \in \alpha$, din $x \in y$ rezultă că $y \notin x$ (*ireflexivitatea* relaţiei $\in$);
- orice submulţime nevidă a lui α are un prim element (faţă de relaţia $\in$):

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

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

Clasa ordinalelor se notează cu *On*. Astfel, scrierea $On(\alpha)$ înseamnă „mulţimea α este un ordinal".[17]

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

4.4 Definiţie. Fie $(A, \leq)$ o mulţime ordonată. O submulţime S a lui A se numeşte *segment iniţial* al lui A dacă are proprietatea că, odată cu un element x, conţine 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 $a \in A$, mulţimea $S_a(A) := \{x \in A \mid x < a\}$ este un segment iniţial în A. Este remarcabil că în mulţimi *bine ordonate*, toate segmentele iniţiale sînt de acest tip:

4.5 Propoziţie. *Fie $(A, \leq)$ o mulţime <u>bine</u> ordonată şi S un segment iniţial al lui A. Atunci: sau $S = A$, sau există $a \in A$ astfel încît $S = S_a(A) := \{x \in A \mid x < a\}$.*

---

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

Demonstraţie. Presupunem că $S \neq A$. Atunci $A \setminus S$ este nevidă şi (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 definiţia segmentului iniţial. Cum A este total ordonată, rezultă că $x < a$, adică $x \in S_a(A)$. Incluziunea cealaltă o lăsăm cititorului. □

4.6 Propoziţie. *Fie α un ordinal şi s un segment iniţial în α. Atunci $s = \alpha$ sau există $\beta \in \alpha$ astfel încît $s = \beta = S_\beta(\alpha)$.*

Demonstraţie. Reamintim că relaţia de ordine strictă pe α este $\in$, faţă de care α este bine ordonată. Din propoziţia precedentă rezultă că $s = \alpha$ sau există $\beta \in \alpha$ astfel încît $s = S_\beta(\alpha)$. Dar $S_\beta(\alpha) = \{x \in \alpha \mid x \in \beta\} = \alpha \cap \beta$. Cum α este ordinal, din $\beta \in a$ rezultă $\beta \subseteq \alpha$, deci $\alpha \cap \beta = \beta$. □

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

Demonstraţie. Fie α un ordinal şi $\beta \in \alpha$. Atunci $\beta = S_\beta(\alpha)$, care este un segment iniţial în α. În general, orice submulţime nevidă a unei mulţimi bine ordonate A este bine ordonată de relaţia de ordine de pe A (demonstraţi!), deci $\beta = S_\beta(\alpha)$ este bine ordonat de $\in$. Avem şi că β este tranzitivă: dacă $x \in \beta$, iar $y \in x$, atunci $x \in \alpha$ (căci $\beta \in \alpha$ şi α este tranzitivă). Acum, din $x \in \alpha$ şi $y \in x$ deducem că $y \in \alpha$. Am obţinut că $y, x, \beta \in \alpha$, $y \in x$ şi $x \in \beta$. Relaţia $\in$ este tranzitivă pe α, deci $y \in \beta$. □

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

Demonstraţie. Relaţia de apartenenţă $\in$ este de ordine strictă pe α, deci este ireflexivă: $\forall x \in \alpha$, avem $x \notin x$. Dacă presupunem că $\alpha \in \alpha$, obţinem astfel că $\alpha \notin \alpha$, absurd. □

4.9 Propoziţie. *Pentru orice ordinale α şi β, are loc una şi numai una din afirmaţiile: $\alpha \in \beta$, $\alpha = \beta$ sau $\beta \in \alpha$.*

Demonstraţie. Fie $\gamma = \alpha \cap \beta = \{x \in \alpha \mid x \in \beta\}$. Se verifică imediat că γ este un segment iniţial în mulţimea ordonată $(\alpha, \in)$ (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 posibilităţile: 1) $\gamma = \alpha$ şi $\gamma = \beta$. Atunci $\alpha = \beta$. 2) $\gamma = \alpha$ şi $\gamma \in \beta$. Atunci $\alpha \in \beta$. 3) $\gamma \in \alpha$ şi $\gamma = \beta$. Atunci $\beta \in \alpha$. 4) $\gamma \in \alpha$ şi $\gamma \in \beta$. Atunci $\gamma \in \alpha \cap \beta = \gamma$, imposibil: γ este ordinal şi s-ar contrazice **4.8**.

Cele trei situaţii din enunţ sînt mutual incompatibile: dacă $\alpha \in \beta$, atunci $\alpha = \beta$ ar contrazice **4.8**, iar $\beta \in \alpha$ implică (pentru că α este tranzitivă) $\alpha \in \alpha$, aceeaşi contradicţie. □

Putem enunţa proprietatea de mai sus sub forma: *Clasa ordinalelor este total ordonată de relaţia de ordine strictă $\in$.*

Mai mult, *clasa ordinalelor este bine ordonată de relaţia de apartenenţă.* Acest enunţ necesită precizări: nu am definit încă noţiunea de *clasă* bine ordonată. O analogie directă cu *mulţimile* bine ordonate ar conduce la următoarea „definiţie”: o clasă $C(x)$ ordonată de o relaţie (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 definiţie conduce de fapt la a da o *schemă* de definiţii, căci clasele nu sînt obiecte ale teoriei, ci expresii ale limbajului formal (cf. comentariul de la Axioma-schemă a substituţiei). Se adoptă următoarea definiţie, mai restrictivă, dar care nu are dezavantajul descris anterior:

4.10 Definiţie. O clasă $C(x)$ se numeşte *bine ordonată* de o relaţie de ordine strictă $R(x, y)$ dacă este total ordonată de R şi orice segment iniţial al lui C în raport cu relaţia R este o <u>mulţime</u> bine ordonată de R. Mai precis, au loc afirmaţiile:

- R este o relaţie ireflexivă pe C: $\forall x(C(x) \to \neg R(x, x))$.
- R este o relaţie tranzitivă pe C: $\forall x\ \forall y\ \forall z(C(x)\wedge C(y)\wedge C(z)\wedge R(x,y)\wedge R(y,z) \to R(x, z))$.
- R este o relaţie totală pe C: $\forall x\ \forall y\ (C(x)\wedge C(y) \to (R(x, y) \vee R(y, x) \vee x = y))$.
- Pentru orice mulţime t, segmentul iniţial al clasei C determinat de t în raport cu relaţia R, adică clasa $S_t(C)(\mathrm{mod}\ R) := C(x) \wedge R(x, t)$, este o *mulţime* bine ordonată de R:

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

Dacă C este bine ordonată de R în sensul definiţiei anterioare, atunci *orice clasă nevidă inclusă în C are prim element*. Într-adevăr, fie D o clasă nevidă inclusă în C şi 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 decît t: $D(q) \wedge R(q, t)$. Dar segmentul iniţial $S_t(C)(\mathrm{mod}\ R)$ este o mulţime; deci intersecţia clasei D cu $S_t(C)(\mathrm{mod}\ R)$ (adică clasa $D(x) \wedge (x \in S_t(C)(\mathrm{mod}\ R))$ este o submulţime S a lui $S_t(C)(\mathrm{mod}\ R)$ (nevidă, căci conţine q). Din buna ordonare a lui $S_t(C)(\mathrm{mod}\ R)$ deducem că există primul element m al mulţimii S. Acesta este primul element al clasei D: dacă ar exista n în D, mai mic decît m, atunci n este mai mic decît t şi deci $n \in S_t(C)(\mathrm{mod}\ R)$. Astfel, $n \in S$ şi obţinem o contradicţie cu faptul că m este primul element al lui S.

Să demonstrăm acum:

4.11 Propoziţie. *Clasa ordinalelor On este bine ordonată de relaţia de apartenenţă.*

Demonstraţie. Am văzut (**4.9**) că relaţia de apartenenţă este totală pe clasa ordinalelor. Fie α un ordinal şi segmentul iniţial $S_\alpha(On)(\mathrm{mod} \in) = On(t)\wedge(t \in \alpha)$. Evident, această clasă este o mulţime, anume α (orice element t al lui α este ordinal). Din definiţia ordinalelor, α este bine ordonat de apartenenţă. □

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

4.12 Propoziţie. *Pentru orice ordinal α, $\alpha \bigcup \{\alpha\}$ este tot ordinal* (*numit* succesorul *lui α*) *şi este cel mai mic ordinal, mai mare decît α.*

Demonstraţie. Propunem spre demonstraţie afirmaţia: α ordinal implică $\alpha \bigcup \{\alpha\}$ ordinal. Fie acum β un ordinal mai mare decît α. Atunci $\alpha \in \beta$ (adică $\{\alpha\} \subseteq \beta$). Deci $\alpha \subseteq \beta$ (căci β ordinal), şi astfel $\alpha \bigcup \{\alpha\} \subseteq \beta$. Aceasta demonstrează că orice ordinal mai mare decît α este mai mare sau egal cu $\alpha \bigcup \{\alpha\}$. Pe de altă parte, este evident că $\alpha \in \alpha \bigcup \{\alpha\}$. □

4.13 Definiţie. Dacă pentru ordinalul β există α astfel încît $\beta = \alpha \bigcup \{\alpha\}$ (β este succesorul lui α), atunci α este ordinal, unic determinat de β (de ce?) şi se numeşte *predecesorul* lui β. Un ordinal α se numeşte *ordinal finit* dacă: sau $\alpha = \emptyset$, sau orice element al lui α şi α însuşi au un predecesor. Un ordinal care nu este finit se numeşte *ordinal infinit*.

Se observă că toate mulţimile din şirul (1) sînt ordinale finite. De altfel, şirul a fost construit plecînd de la $\emptyset$ şi 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, $\alpha \bigcup \{\alpha\}$, este ordinal finit.

4.14 Propoziţie. *Axioma infinităţii este echivalentă cu afirmaţia:*

<u>*Ordinalele finite formează o mulţime*</u> (*notată cu* ω).

Demonstraţie. Presupunem axioma infinităţii adevărată şi considerăm *mulţimea* $\omega := \{\alpha \in M \mid \alpha \text{ ordinal finit}\}$, unde M este dată de **4.1**. Să arătăm că ω conţine orice ordinal finit. Dacă nu ar fi aşa, ar exista un ordinal finit β, cu $\beta \notin M$. Cum clasa ordinalelor 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) aparţine lui M, contradicţie.

Invers, dacă ordinalelele finite formează o mulţime ω, atunci ω satisface proprietăţile din axioma **4.1**: $\emptyset \in \omega$ şi $\forall \alpha \in \omega$, avem $\alpha \bigcup \{\alpha\} \in \omega$. □

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

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

Clar, axiomele **1-4** sînt verificate. Să verificăm şi axioma inducţiei:

4.15 Propoziţie. *(Teorema inducţiei pe mulţimea ordinalelor finite) Fie P o clasă de ordinale finite astfel încît* $P(\emptyset)$ *este adevărată şi,* $\forall \alpha$ *ordinal finit cu* $P(\alpha)$ *adevărată, rezultă că* $P(\alpha \bigcup \{\alpha\})$ *adevărată. Atunci* $P(\alpha)$ *adevărată pentru orice ordinal finit* α.

Demonstraţie. Clasa P corespunde unei submulţimi (notată tot P) a lui ω. Dacă $P \neq \omega$, atunci $\omega \setminus P \neq \emptyset$ şi 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 $\beta \in P$, contradicţie cu $\beta \in \omega \setminus P$. □

4.16 Observaţie. Mulţimea ω a ordinalelor finite este un ordinal (demonstraţi!), care nu este finit.

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

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

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

Este deosebit de important următorul enunţ, care stă la baza raţionamentelor prin inducţie:

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

Considerăm utile cîteva remarci şi rezultate privind tehnica de *demonstraţie prin inducţie*, respectiv de *definire prin recurenţă*. Mai întîi dăm un rezultat care este cunoscut uneori ca o „variantă a principiului de inducţie”:

4.18 Propoziţie. *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 (subînţelegem că toate variabilele sînt în* $\mathbb{N}$*):*

$$\{\forall n\,[(\forall k\,(k < n \to P(k)) \to P(n)]\} \to (\forall n)(P(n)).$$

Demonstraţie. Mai întîi observăm că, în condiţiile din enunţ, $P(0)$ este adevărată. Într-adevăr, pentru $n = 0$ are loc implicaţia: $[\forall k(k < 0 \to P(k)] \to P(0)$. Dar $\forall k(k < 0 \to P(k))$ este adevărată, deoarece $k < 0$ este falsă pentru orice $k \in \mathbb{N}$ (o expresie de forma $p \to q$ este adevărată dacă p este falsă!). Deci $P(0)$ adevărată. [18]

Presupunem prin absurd că există $n \in \mathbb{N}$ astfel încît $P(n)$ să fie falsă. Atunci mulţimea 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 implicaţia $(\forall k(k < a \to P(k)) \to P(a)$, rezultă că $P(a)$ este adevărată, absurd. □

[18] Aşadar, nu are rost să se arate că $P(0)$ este adevărată cînd se foloseşte acest raţionament prin inducţie!

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

4.19 Propoziţie. *Fie* $(A, \leq)$ *o mulţime bine ordonată şi 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* $P(n)$ *adevărată. Atunci* $P(n)$ *adevărată pentru orice* $n \in A$*. Mai precis, are loc* (*subînţelegem că toate variabilele sînt în* A):

$$\{\forall n\, [(\forall k\, (k < n \to P(k)) \to P(n)]\} \to (\forall n)(P(n)). \qquad \square$$

Un exemplu de aplicare a acestei propoziţii este demonstraţia teoremei polinoamelor simetrice (unde mulţimea bine ordonată este $\mathbb{N}^n$, cu ordinea lexicografică).

Mai mult, se poate face inducţie pe *clase bine ordonate*. Dacă $R(x, y)$ este o relaţie de ordine, vom scrie, mai sugestiv, $x < y\ (\text{mod } R)$ în loc de $R(x, y) \wedge (x \neq y)$. Demonstraţia rezultatului ce urmează este similară cu cea de la mulţimi bine ordonate.

4.20 Propoziţie. *Fie* $A(x)$ *o clasă bine ordonată de o relaţie* $R(x, y)$ *şi 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* $k < n\ (\text{mod } R)$*, rezultă că* $P(n)$ *adevărată. Atunci* $P(n)$ *adevărată pentru orice n din A. Mai precis, dacă are loc*:

$$\forall n\{[A(n) \wedge (\forall k\, (A(k) \wedge k < n(\text{mod } R)) \to P(k)] \to P(n)\},$$

atunci are loc $(\forall n)(A(n) \to P(n))$. $\square$

În general, astfel de raţionamente se fac pe *clasa ordinalelor On* şi se numesc raţionamente prin *inducţie transfinită*.

Strîns legat de principiul demonstraţiei prin inducţie este *definirea şirurilor prin recurenţă* (numită uneori *definire prin inducţie*, denumire improprie, căci inducţia este o metodă de demonstraţie). De exemplu, este clar că relaţiile $x_0 = 1$, $x_{n+1} = 2x_n + 1$, $\forall n \in \mathbb{N}$, definesc unic şirul de numere naturale: $x_0 = 1$, $x_1 = 3$, $x_2 = 7$, $x_3 = 15$, … .

4.21 Definiţie. Fie A o mulţime nevidă. Se numeşte *şir* (indexat după ω)[19], cu valori în A, orice funcţie $s : \omega \to A$ (ω este ordinalul tuturor ordinalelor finite). Mai general, dacă α este un ordinal oarecare, vom numi *şir* (indexat după α) cu valori în A orice funcţie definită pe α cu valori în A.

Pentru un şir $s : \alpha \to A$ se folosesc notaţii 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 $s|_\beta$ restricţia lui s la β ($s|_\beta$ este atunci şir indexat după β). De exemplu, dacă $(s_n)_{n\in\omega}$ este un şir indexat după ω, atunci:

$s|_0 = s|_\varnothing = \varnothing$; $\quad s|_1 = s|_{\{0\}} = \{(0, s(0))\}$; $\quad s|_2 = s|_{\{0,1\}} = \{(0, s(0)), (1, s(1))\}$, …,

$s|_n = s|_{\{0,1,\,\dots,\,n-1\}} = \{(0, s(0)), (1, s(1)), \dots, (n-1, s(n-1))\}$.

[19] Reamintim că am identificat $\mathbb{N}$ cu ordinalul ω.

Ce înseamnă a *defini prin recurenţă* un şir $(s_n)_{n\in\omega}$? Intuitiv, pentru orice $n \in \omega$, termenul s_n „depinde de termenii precedenţi $s_0, \ldots, s_{n-1}$”, adică este dată o „relaţie de recurenţă” de forma $s_n = f(s_0, \ldots, s_{n-1})$. Observăm că putem rescrie aceasta sub forma $s_n = f(s|_n)$, folosind notaţiile de mai sus. Deci f este o funcţie cu domeniul format de mulţimea şirurilor (cu valori în A), indexate după un $n = \{0,1, \ldots, n-1\}$. Mai general, putem da următoarea:

4.22 Definiţie. Fie A o mulţime nevidă şi α un ordinal. Pentru fiecare $\beta \in \alpha$ notăm cu

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

mulţimea şirurilor cu valori în A, indexate după β. Fie

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

mulţimea şirurilor cu valori în A, indexate după ordinale din α. Dacă $s : \alpha \to A$ şi $\beta \in \alpha$, atunci $s|_\beta \in S_\beta(A) \subseteq S(A, \alpha)$, deci există $f(s|_\beta) \in A$.

O *relaţie de recurenţă* este o funcţie $f : S(A, \alpha) \to A$. Spunem că şirul $s : \alpha \to A$ este *definit recurent de relaţia de recurenţă* f dacă, $\forall\beta \in \alpha$, avem :

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

4.23 Teoremă. *Fie α un ordinal şi A o mulţime. Pentru orice relaţie de recurenţă $f : S(A, \alpha) \to A$ există un unic şir $s : \alpha \to A$ care este definit recurent de f.*

Demonstraţie. Unicitatea: presupunem că există două şiruri $s : \alpha \to A$ *şi* $t : \alpha \to A$, definite recurent de f, astfel încît $s \neq t$. Deci mulţimea $\{\beta \in \alpha \mid s(\beta) \neq t(\beta)\}$ este nevidă şi are un prim element π. Atunci $s(\gamma) = t(\gamma)$, $\forall\gamma \in \pi$, adică $s|_\pi = t|_\pi$. Dar $s(\pi) = f(s|_\pi) = f(t|_\pi) = t(\pi)$, contradicţie.

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

Afirmăm că *δ este un ordinal*. E suficient să demonstrăm că δ este segment iniţial (vezi **4.6**). Observăm că $\varnothing \in \delta$ (funcţia $\varnothing : \varnothing \to A$ 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 $s : \beta \to A$ 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 şi este definit recurent de f. Astfel, $\gamma \in \delta$.

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

Observăm că, $\forall\beta \in \delta$, şirul s_β definit recurent de f este unic determinat, din prima parte a demonstraţiei. Mai mult, $\forall\beta \in \delta$ şi $\forall\gamma \in \beta$, restricţia lui s_β la γ coincide cu s_γ (tot din unicitate). Definim atunci $s : \delta \to A$ prin : $\forall\beta \in \delta$, $s(\beta) = f(s_\beta)$. Definiţia are sens: s_β este un şir indexat după β (unicul şir definit recurent pe β de f) şi există $f(s_\beta) \in A$.

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

Fie $\beta \in \delta$ şi 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 $\delta \in \alpha$ şi există $s : \delta \to A$ definit recurent de f. Din definiţia lui δ, avem $\delta \in \delta$; absurd. □

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

Prezentăm o proprietate foarte importantă a lui $\mathbb{N}$, a cărei demonstraţie ilustrează principiul de demonstraţie prin inducţie. Se presupun cunoscute operaţiile de adunare şi înmulţire în $\mathbb{N}$ şi proprietăţile lor.

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

Demonstraţie. Fie $b \neq 0$ fixat. Demonstrăm prin inducţie 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 $a \geq b$ şi $P(k)$ este adevărată, $\forall k \in \mathbb{N}$, $k < a$. Să demonstrăm $P(a)$. Cum $a \geq b$ avem $a - b \in \mathbb{N}$ şi $a - b < a$. Deci are loc $P(a - b)$: $\exists q, r$ astfel încît $a - b = bq + r$ şi $r < b$, adică $a = b(q + 1) + r$, cu $r < b$.

Unicitatea: presupunem că $a = bq + r = bt + s$, cu $r < b$ şi $s < b$. 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 obţinem $q - t = 0$ şi $s - r = 0$. □

Teorema împărţirii cu rest este de o importanţă covîrşitoare în matematică. O primă aplicaţie a ei este *reprezentarea numerelor naturale într-o bază dată* (vezi Exerciţii).

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

4.25 Definiţie. Fie $(A, \leq)$ şi $(B, \leq)$ mulţimi ordonate. O aplicaţie $\varphi : A \to B$ se numeşte *morfism de ordine* (sau *aplicaţie crescătoare*) dacă $\forall x, y \in A$, din $x \leq y$ rezultă $\varphi(x) \leq \varphi(y)$. Morfismul φ se numeşte *izomorfism de ordine* dacă φ este bijectivă şi inversa sa φ^{-1} este tot morfism. Mulţimile ordonate $(A, \leq)$ şi $(B, \leq)$ se numesc *izomorfe* dacă există măcar un izomorfism de ordine $\varphi : A \to B$, caz în care scriem $A \cong B$.

4.26 Observaţie. Dacă $(A, \leq)$ şi $(B, \leq)$ sînt *total* ordonate, atunci orice morfism bijectiv $\varphi : A \to B$ este şi izomorfism. Demonstraţi! Pentru mulţimi ordonate în general, nu orice morfism bijectiv este izomorfism, după cum arată exemplul aplicaţiei identitate $\mathrm{id} : (\mathbb{N}^*, |) \to (\mathbb{N}^*, \leq)$, unde $(\mathbb{N}^*, |)$ este mulţimea numerelor naturale nenule înzestrată cu relaţia de ordine divizibilitatea, iar $\leq$ este relaţia de ordine uzuală.

Comparaţi rezultatul următor cu **4.9**:

4.27 Propoziţie. *Fie A şi B mulţimi* <u>*bine ordonate*</u>. *Atunci are loc exact una din situaţiile: $A \cong B$; A izomorf cu un segment iniţial al lui B; B izomorf cu un segment iniţial al lui A.* □

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

4.28 Propoziţie. *Fie $(A, \leq)$ o mulţime bine ordonată. Atunci există un unic ordinal $(\alpha, \in)$ izomorf cu $(A, \leq)$.* □

Astfel, pentru orice tip de *bună* ordine, există un unic ordinal în acel tip (şi, evident, orice ordinal se află într-un unic tip de bună ordine). Din acest motiv, uneori prin *ordinal* se înţelege *un tip de ordine de mulţimi bine ordonate*. Rezultatele enunţate arată echivalenţa celor două abordări.

I.5. Comentarii şi completări privind axiomatica mulţimilor

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

Sistemul ZF propriu-zis conţine 4 axiome şi o schemă de axiome: *axioma extensionalităţii, axioma reuniunii, axioma mulţimii părţilor, schema de axiome a substituţiei* şi *axioma infinităţii.*

Este de dorit ca orice teorie axiomatică (deci şi ZF) să satisfacă următoarele proprietăţi:

Consistenţa (sau *necontradictorietatea*) teoriei: din axiomele teoriei nu se poate deduce simultan o propoziţie şi negaţia ei (adică nu se poate obţine o *contradicţie*). O teorie care nu este consistentă nu are nici o valoare ştiinţifică: *dacă există o propoziţie p astfel încît p şi $\neg p$ sînt adevărate, atunci orice propoziţie q este adevărată* (ceea ce elimină orice interes în stabilirea adevărului unei propoziţii). Într-adevăr, este clar că, dacă p şi $p \to q$ sînt adevărate, atunci q este adevărată. Însă p e adevărată din ipoteză, iar $p \to q$ este $\neg p \vee q$, adevărată căci $\neg p$ este adevărată.

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

Problemele stabilirii consistenţei şi independenţei unui sistem axiomatic sînt dificile şi profunde.

Strîns legată de problema consistenţei este *modelarea* unui sistem axiomatic. Se numeşte *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 şi numai dacă are un model*.

Se observă că, în exemplele de mai sus, modelele teoriilor sînt obiecte construite în cadrul teoriei (axiomatice) a mulţimilor (care este mai largă decît teoriile respective). O teoremă a lui Gödel afirmă, într-o exprimare neriguroasă, că un model pentru o teorie axiomatică poate fi construit doar într-o teorie mai largă. Aşadar, un eventual model pentru ZF (care i-ar demonstra consistenţa) 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 consistenţei unei ipotetice teorii mai largi revine la construcţia unei teorii şi mai largi ş.a.m.d. Se vede că această cale nu conduce la o demonstraţie a consistenţei teoriei ZF. Se poate doar presupune că teoria ZF nu conduce la apariţia de contradicţii (de fapt, am văzut că a fost creată tocmai pentru a elimina contradicţiile apărute în teoria naivă a mulţimilor). În acest sens, este grăitor următorul citat din MANIN [1977], p. 102:

> Problema consistenţei formale a axiomelor Zermelo-Fraenkel trebuie să rămînă o chestiune de credinţă, cu excepţia cazului cînd o eventuală inconsistenţă formală este demonstrată. Pînă acum toate demonstraţiile bazate pe aceste axiome nu au dus niciodată la o contradicţie; dimpotrivă, au deschis în faţa noastră bogata lume a matematicilor clasice şi moderne. Această lume are o anumită realitate şi o viaţă proprii, care depind în mică măsură de formalismele alese pentru a le descrie. O descoperire a unei contradicţii în oricare din diversele formalisme, chiar dacă ar apărea, ar servi doar la clarificarea, rafinarea şi poate reconstrucţia unor anumite idei, dar nu ar conduce la falimentul lor, cum s-a întîmplat de mai multe ori în trecut.

Independenţa axiomelor are şi ea legătură cu consistenţa. Să exemplificăm aceasta pe cazul unei noi axiome, *axioma fundării*.

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

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

Acest enunţ implică: *Nici o mulţime nu este element al ei însăşi*. Într-adevăr, dacă avem o mulţime x astfel încît $x \in x$, atunci $\{x\}$ contrazice axioma fundării: singurul element al lui $\{x\}$ este x şi avem $x\cap x$ nevidă, căci conţine pe x. Mai mult, nu există „lanţuri de mulţimi” de forma $x_0 \in x_1 \in x_2 \in \ldots \in x_n \in x_0$. Dacă ar exista un asemenea lanţ, atunci mulţimea $\{x_0, x_1, \ldots, x_n\}$ contrazice AF (de ce?). La fel, nu poate exista un şir $(x_n)_{n\in\omega}$ astfel încît $x_{n+1} \in x_n$, $\forall n \in \omega$. AF îşi datorează numele faptului că, pentru orice mulţime x, orice lanţ de forma $x \ni x_0 \ni x_1 \ni \ldots \ni x_n \ni \ldots$ este finit şi se termină cu $\varnothing$: $\exists n$ astfel încît $x \ni x_0 \ni x_1 \ni \ldots \ni x_n \ni \varnothing$: orice şir descrescător (faţă de relaţia $\in$) este finit şi *„fundat”* pe $\varnothing$.[20]

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

S-a demonstrat că, dacă acceptăm că ZF este consistentă, atunci ZF + AF (sistemul ZF la care se adaugă AF) nu conduce la contradicţii. Această probare a *consistenţei relative* a AF s-a realizat prin construirea unui model (în cadrul ZF) care satisface ZF + AF. În plus, s-a construit un alt model (tot în cadrul ZF) care satisface ZF şi *negaţia 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 direcţie este demonstrarea *independenţei axiomei infinităţii faţă de restul axiomelor ZF*, printr-un procedeu principial asemănător cu cel de mai sus.

Axioma alegerii (AC)[21] este o nouă axiomă care joacă un rol deosebit în matematică, datorită faptului că, pe de o parte, are un enunţ aparent „evident”; pe de altă parte, are un caracter neconstructiv care i-a atras multe critici. Există multe enunţuri echivalente cu această axiomă. În formularea lui Zermelo, AC se enunţă:

Pentru orice mulţime A în care elementele sînt disjuncte două cîte două[22]*, există o mulţime care conţine exact un element din fiecare mulţime nevidă din A* :

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

Altfel spus, putem „alege” cîte un element din fiecare mulţime nevidă din A şi forma cu ele o nouă mulţime. Controversele privind această axiomă provin şi din faptul că se postulează existenţa unei astfel de mulţimi şi implicit a unui „procedeu de alegere” a unui element dintr-o mulţime 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 enunţuri echivalente cu Axioma Alegerii. Iată cîteva:

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

Produsul cartezian al unei familii de mulţimi nevide este nevid.

Pentru orice mulţime a, există o funcţie de alegere $f : a \rightarrow \bigcup a$ (adică f are proprietatea că, $\forall x \in a, x \neq \varnothing \rightarrow f(x) \in x$).[23]

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

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

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

---

[21] Acronimul expresiei Axiom of Choice.
[22] Reamintim că elementele lui A sînt tot mulţimi.
[23] Altfel spus, funcţia f "alege" cîte un element $f(x)$ din fiecare mulţime nevidă $x \in a$.

I.6. Cardinali

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

6.29 Definiţie. Fie A şi B două mulţimi. Spunem că A şi B sînt *echipotente* (sau că sînt *cardinal echivalente*, sau că *au acelaşi cardinal*) dacă există o bijecţie $f: A \to B$. Scriem atunci $A \sim B$ sau $|A| = |B|$.

Pentru orice mulţimi A, B, C, au loc:

a) $A \sim A$ (reflexivitate);

b) Dacă $A \sim B$, atunci $B \sim A$ (simetrie);

c) Dacă $A \sim B$ şi $B \sim C$, atunci $A \sim C$ (tranzitivitate).

Astfel, putem spune că relaţia de echipotenţă " $\sim$ " este o relaţie de echivalenţă pe clasa mulţimilor. Clasa[24] tuturor mulţimilor echipotente cu o mulţime dată A se numeşte *cardinalul mulţimii A* şi se notează card A sau $|A|$. Spunem că A este o mulţime *finită* cu n elemente ($n \in \mathbb{N}$) dacă $A \sim \{1, \dots, n\}$ şi atunci notăm $|A| = |\{1, \dots, n\}| =: n$. O mulţime care nu este finită se numeşte *infinită*.

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

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

Se introduce o *relaţie de ordine* între cardinali: spunem că $|A| \le |B|$ dacă există o funcţie injectivă $\varphi: A \to B$. Definiţia este corectă: dacă $A \sim A'$, $B \sim B'$ şi există o funcţie injectivă $\varphi: A \to B$, atunci există o există o funcţie injectivă $\varphi': A' \to B'$ (demonstraţi!).

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

a) $|A| \le |A|$ (*reflexivitate*);

b) $|A| \le |B|$ şi $|B| \le |C|$ implică $|A| \le |C|$ (*tranzitivitate*);

Are loc următoarea teoremă importantă, care arată că $\le$ este şi *antisimetrică* (deci are într-adevăr aceleaşi proprietăţi ca o relaţie de ordine).

6.30 Teoremă. (Cantor-Schröder-Bernstein) *Fie A şi B două mulţimi. Dacă $|A| \le |B|$ şi $|B| \le |A|$, atunci $|A| = |B|$.*

Demonstraţie. Idee: să găsim $D \subseteq A$ astfel încît $A \setminus D \subseteq$ Img şi $\alpha: A \to B$, 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 bijecţie (faceţi un desen!). Trebuie să avem atunci $A \setminus D = g(B \setminus f(D))$, adică $D = A \setminus g(B \setminus f(D))$.

[24] Nu putem vorbi de "*mulţimea* tuturor mulţimilor echipotente cu A".

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

Se arată uşor 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, $\varnothing \in M$.

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 $D \subseteq \varphi(D)$. Aplicînd φ acestei incluziuni, obţinem $\varphi(D) \subseteq \varphi(\varphi(D))$ 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 bijecţie. □

Relaţia de ordine ≤ este şi *totală* (demonstraţia face apel la Axioma Alegerii):

6.31 Teoremă. *Oricare ar fi două mulţimi A, B, are loc* $|A| \le |B|$ *sau* $|B| \le |A|$. □

Această ultimă proprietate este echivalentă cu Axioma Alegerii.

Exerciţii

1. Demonstraţi că axioma infinităţii este echivalentă cu enunţul: *Există un ordinal infinit.*

2. Demonstraţi că clasa ordinalelor On nu este mulţime („paradoxul Burali-Forti”).

3. Demonstraţi că reuniunea unei mulţimi A de ordinale este un ordinal şi este marginea superioară a lui A în On.

4. Un ordinal se numeşte *ordinal limită* dacă nu are un predecesor. Arătaţi că ω este cel mai mic ordinal limită şi că axioma infinităţii este echivalentă cu afirmaţia: *Există un ordinal limită.* Care este succesorul lui ω?

5. Arătaţi că ordinalul α este ordinal limită dacă şi numai dacă $\alpha = \sup\{\beta \mid \beta \in \alpha\}$ (margine superioară în On).

6. Inducţia transfinită (pe clasa ordinalelor On) se face adesea distingînd cazul ordinalelor limită. Mai precis, demonstraţi că dacă o expresie $P(x)$ are proprietăţile:

a) $P(\varnothing)$ adevărată;

b) $\forall \alpha\, [(On(\alpha) \wedge P(\alpha)) \to P(\alpha + 1)]$;

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 infinităţii face referire la mulţimea vidă $\varnothing$, a cărei existenţă rezultă din existenţa măcar a unei mulţimi. Dar acest lucru este asigurat de axioma infinităţii. Cum se poate ieşi din acest (aparent) cerc vicios?

8. Arătaţi că, pentru orice mulţime A, are loc $|\mathcal{P}(A)| > |A|$.

9. Demonstraţi că, pentru orice mulţime *A, A* este strict inclusă în $A\bigcup\{A\}$. (*Folosiţi axioma fundării).*

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

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

În cazul în care are loc egalitatea (*R*) de mai sus, se mai scrie $a = \overline{c_{n-1}\ldots c_1c_0}$, scriere numită *reprezentarea lui a în baza b*. Numerele naturale 0, 1, …, $b-1$ se numesc *cifre*[25] *în baza b* (pentru scrierea concretă se dau *b* simboluri care reprezintă aceste cifre şi nu se foloseşte bara superioară, scrisă aici pentru a evita confuzia cu produsul $c_{n-1}\ldots c_1c_0$). Uneori, în notaţie, se mai specifică baza *b*, ca indice. De exemplu, $105_7 = 54_{10}$. (Ind. Din teorema împărţirii cu rest aplicată lui *a* şi *b*, $\exists!\ q, r \in \mathbb{N}$ astfel încît $a = bq + r$. Se pune $c_0 = r$ şi se repetă procedeul pentru *q* – sau, mai riguros, se aplică o inducţie după *a*. Pentru unicitate, se observă că c_0 este restul împărţirii lui *a* la *b* şi se aplică o inducţie după cel mai mic număr de cifre din ipoteticele reprezentări ale lui *a* în baza *b*).

11. Reprezentaţi în baza 10 numerele 1011_2, 1212_3. Scrieţi în bazele 2, 7, 16, numerele 129_{10}, 1152_{10}.

[25] A se remarca distincţia între *număr* şi *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. Mulţimi factor şi construcţii de structuri numerice fundamentale

Presupunînd cunoscută mulţimea $\mathbb{N}$ a numerelor naturale, înzestrat cu operaţiile de adunare şi înmulţire (cu proprietăţile cunoscute) şi cu structura sa de ordine uzuală ($\mathbb{N}$ este o mulţime *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 noţiunea de „număr”. În multe cărţi se pun întrebări (probleme) de genul „ce este *numărul* (eventual raţional sau real sau complex)”, urmînd ca autorul să dea un răspuns de natură filozofică sau matematică. Noţiunea de *număr* (privit ca element individual, izolat) nu are o semnificaţie deosebită în matematică, mult mai importantă fiind cea de *structură pe o mulţime numerică*. Astfel, de pildă mulţimea $\mathbb{R}$ a numerelor reale este importantă prin *structurile* cu care este înzestrată: structura *algebrică* de corp comutativ, cea de *ordine* (este total ordonată şi orice submulţime majorată are supremum), cea *topologică* derivată din acestea (este spaţiu metric complet); un număr real, luat ca element individual al lui $\mathbb{R}$, nu poate fi pus nicidecum în legătură cu astfel de proprietăţi. Insistăm asupra acestei distincţii pentru că o conştientizare a ei îşi poate pune amprenta şi asupra stilului de predare a acestor concepte fundamentale.

II.1. Relaţii de echivalenţă şi mulţimi factor

Relaţiile de echivalenţă sînt un instrument esenţial în matematică, mai ales în problemele de *construcţii* de obiecte (structuri) noi. Vom descrie un procedeu general, *construcţia mulţimii factor (cît) în raport cu o relaţie de echivalenţă*, care, aplicat în diverse cazuri particulare, duce la construcţii importante. Trebuie subliniat că mulţimea factor obţinută se înzestrează cu o structură care este de obicei legată de structura mulţimii iniţiale (ceea ce presupune o *compatibilitate între relaţia de echivalenţă şi structura iniţială*). Această metodă permite construcţia unor structuri matematice importante: $\mathbb{Z}$ (construit ca mulţime factor a lui $\mathbb{N} \times \mathbb{N}$), $\mathbb{Q}$ (mulţime factor a lui $\mathbb{Z} \times \mathbb{Z}^*$; acelaşi procedeu dă în general inele şi corpuri de fracţii), $\mathbb{R}$ (mulţime factor a mulţimii şirurilor Cauchy de numere raţionale), $\mathbb{C}$ (mulţime factor a inelului de polinoame $\mathbb{R}[X]$). Remarcăm că majoritatea construcţiilor în matematică sînt mulţimi factor în raport cu o anumită relaţie de echivalenţă: produsul tensorial a două module, grupul liber pe o mulţime, spaţiile proiective din geometrie, spaţiile L^p din analiză, … şi lista este departe de a fi completă.

Fie A o mulţime şi ρ o relaţie de echivalenţă pe A. Mulţimea

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

poartă numele de *clasa de echivalenţă* a elementului a relativ la relaţia ρ şi se notează cu $\widehat{a}$. Se folosesc adesea multe alte notaţii, depinzînd de cazul particular ales şi de dorinţa de a include sau nu relaţia ρ în notaţie. De exemplu, clasa lui a se mai notează C_a, $\overline{a}$, $\widehat{a}_\rho$, $[a]_\rho$ etc.

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

1.1 Definiţie. Mulţimea claselor de echivalenţă în raport cu relaţia ρ se numeşte *mulţimea cît* (sau *factor*) a lui A în raport cu ρ şi se notează cu A/ρ. Deci $A/\rho := \{\widehat{a} \mid a \in A\}$.

1.2 Propoziţie. *Fie ρ o relaţie de echivalenţă pe A. Atunci:*

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

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

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

d) $\bigcup_{a\in A} \hat{a} = A$. □

O mulţime P de submulţimi nevide ale lui A, disjuncte două cîte două, a căror reuniune este A, este numită *partiţie* a lui A. Mai precis, P este *partiţie a lui A* dacă:

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

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

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

Propoziţia anterioară nu spune altceva decît că *mulţimea factor a lui A în raport cu o relaţie de echivalenţă este o partiţie a lui A.* Reciproc, orice partiţie poate fi obţinută dintr-o relaţie de echivalenţă:

1.3 Propoziţie. *Fie P o partiţie a mulţimii A. Atunci relaţia ρ definită prin:*

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

este o relaţie de echivalenţă pe A şi P este chiar mulţimea cît A/ρ. □

În aplicaţii, mulţimea iniţială are de obicei o *structură* (algebrică, topologică, de ordine,…), iar relaţia de echivalenţă este *compatibilă* cu structura dată (sensul precis al acestei compatibilităţi fiind definit în fiecare caz în parte; în general, definiţia este „naturală”). Atunci mulţimea factor obţinută va moşteni o structură de acelaşi tip ca mulţimea iniţială. Vom prezenta exemple de aplicare în algebră a acestei construcţii fundamentale (trecerea de la o mulţime la mulţimea factor în raport cu o relaţie de echivalenţă) în paragrafele următoare.

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

1.4 Definiţie. Fie ρ o relaţie de echivalenţă pe mulţimea A. Spunem că submulţimea $S \subseteq A$ este un *sistem de reprezentanţi*[26] *pentru clasele de echivalenţă* (*modulo* ρ) dacă orice element din A este echivalent modulo ρ cu exact un element din S. Intuitiv, un sistem de reprezentanţi se obţine „alegînd" din fiecare clasă de echivalenţă cîte un element („reprezentantul" clasei respective). Astfel S este sistem de reprezentanţi dacă şi 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 Exerciţii. a) Fie relaţia de echivalenţă 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 echivalenţă sînt dreptele paralele cu Oy. Un sistem de reprezentanţi este (de exemplu) $\{(x,0) \mid x \in \mathbb{R}\}$. Mulţimea factor $\mathbb{R}^2/\sim$ este în bijecţie cu $\mathbb{R}$. Cum se poate defini o relaţie de echivalenţă pe $\mathbb{R}^2$ astfel încît clasele de echivalenţă să fie dreptele paralele cu o dreaptă fixată ce trece prin origine, de ecuaţie $y = \alpha x$?

b) Puteţi defini o relaţie de echivalenţă pe $\mathbb{R}^2$ astfel încît clasele de echivalenţă 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 relaţia de „congruenţă 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 reprezentanţi 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 relaţii.* Fie ρ o relaţie pe mulţimea A. Definim o nouă relaţie τ_ρ pe A, astfel: $\forall a, b \in A$, $a\tau_\rho b \Leftrightarrow \exists n \in \mathbb{N}$ şi $x_1, \dots, x_n \in A$ astfel încît $a = x_1$, $b = x_n$ şi $x_i\, \rho\, x_{i+1}$, $i = 1,\dots, n-1$. Atunci τ_ρ este o relaţie *tranzitivă* pe A. Mai mult, τ_ρ este cea mai mică (în sensul incluziunii) relaţie tranzitivă pe A care include relaţia ρ.

II.2. Inelul numerelor întregi

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

De aici apare şi ideea de a concepe un „număr întreg negativ" ca o *diferenţă* de numere naturale. Bineînţeles, pentru o „diferenţă" dată există mai multe (chiar o infinitate de) perechi de numere naturale care au aceeaşi diferenţă: de exemplu perechile (0, 1), (1, 2), (2, 3), … au

[26] O denumire mai corectă, dar mai greu de manipulat, este *sistem complet şi independent de reprezentanţi.*

aceeaşi diferenţă (numărul întreg -1). Ar trebui deci să vedem un număr întreg ca pe o pereche de numere naturale (de forma (a, b)), cu convenţia că „se consideră egale" două perechi (a, b) şi (c, d) dacă $a - b = c - d$. Cum scăderea nu este definită pentru orice pereche de numere naturale, rescriem această condiţie sub forma $a + d = b + c$. Exprimăm riguros aceste consideraţii euristice:

Pe mulţimea $\mathbb{N} \times \mathbb{N}$ se consideră relaţia $\sim$, 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 (verificaţi!) că aceasta este o relaţie de echivalenţă. O clasă de echivalenţă în raport cu această relaţie o numim *număr întreg*, iar mulţimea factor $\mathbb{N} \times \mathbb{N}/\sim$ se numeşte *mulţimea numerelor întregi* şi se notează cu $\mathbb{Z}$.

Notaţia $\mathbb{Z}$ provine de la cuvîntul german *zahl* (pronunţat *ţal*, cu un *a* lung), care înseamnă *număr*. A se observa grafia ($\mathbb{Z}$ şi nu Z), litera $\mathbb{Z}$ scrisă astfel fiind rezervată exclusiv notării mulţimii numerelor întregi (după cum $\mathbb{N}$ este folosită exclusiv pentru mulţimea numerelor naturale).

Nu ne putem opri aici cu construcţia. Trebuie arătat că obiectul pe care l-am construit (riguros) satisface toate proprietăţile pe care ne-am aştepta să le aibă mulţimea numerelor întregi: „include" mulţimea $\mathbb{N}$, orice număr întreg este sau număr natural, sau opusul unui număr natural, este definită o adunare şi o înmulţire în raport cu care este inel, este o mulţime total ordonată, iar ordinea este compatibilă cu adunarea şi înmulţirea.

Mai întîi să determinăm un sistem de reprezentanţi. Mulţimea

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

este sistem de reprezentanţi: 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 echivalenţă a lui $(a, 0)$ (lucru permis de faptul că aplicaţia care duce a în $(a, 0)$ este injectivă de la $\mathbb{N}$ la $\mathbb{N} \times \mathbb{N}/\sim$, demonstraţi!) şi vom nota cu $-a$ clasa de echivalenţă a lui $(0, a)$. Ce mai trebuie verificat pentru a demonstra că Z, definit mai sus, este sistem de reprezentanţi?

Cu aceste identificări, putem scrie:

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

Să definim *operaţiile de adunare şi înmulţire* pe $\mathbb{Z}$ (pornind de la cele de pe $\mathbb{N}$). Pentru aceasta, se definesc operaţii pe clasele de echivalenţă din $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$, folosind reprezentanţi oarecare, urmînd să se demonstreze că nu depind de reprezentanţi şi 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

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

Bineînţeles, $a + c$ semnifică suma în $\mathbb{N}$ a numerelor naturale a şi c. Operaţia este *corect definită*.[27] Aceasta înseamnă că, $\forall (a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$ cu $(a, b) \sim (a', b')$ şi $(c, d) \sim (c', d')$, atunci $(a + c,\ \ b + d) \sim (a' + c',\ \ b' + d')$. Verificarea este uşoară şi constă în aplicarea definiţiilor relaţiei de echivalenţă şi a operaţiei $+$.

Invităm cititorul să definească înmulţirea, să demonstreze corectitudinea definiţiei şi proprietăţile uzuale ale operaţiilor, care conferă lui $\mathbb{Z}$ structură de *inel comutativ şi unitar, fără divizori ai lui* 0 (se mai spune că $\mathbb{Z}$ este *inel integru* sau *domeniu de integritate*).

Relaţia de ordine pe $\mathbb{Z}$: fie $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$. Spunem că $\overline{(a, b)} \le \overline{(c, d)}$ dacă şi numai dacă $a + d \ge b + c$ în $\mathbb{N}$ (de ce am definit astfel?). Demonstraţi corectitudinea definiţiei şi faptul că se obţine o *relaţie de ordine totală* pe $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$.

Se mai pot defini operaţiile pe $\mathbb{Z}$ (respectiv relaţia de ordine pe $\mathbb{Z}$) folosind sistemul de reprezentanţi Z de mai sus şi operaţiile din $\mathbb{N}$ (cum?). Ce avantaje şi dezavantaje au cele două abordări?

O funcţie deosebit de importantă este funcţia *valoare absolută* (sau *modul*) $|\ | : \mathbb{Z} \to \mathbb{Z}$,

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

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

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

II.3. Corpul numerelor raţionale

În gimnaziu, se introduc mai întîi doar numerele raţionale *pozitive*, din motive didactice. Această distincţie oarecum artificială nu îşi are locul aici. Din punct de vedere algebric, construcţia lui $\mathbb{Q}$ pornind de la $\mathbb{Z}$ este principial aceeaşi cu construcţia *corpului de fracţii al unui inel integru oarecare R*.

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

[27] Subliniem că necesitatea demonstrării corectitudinii definiţiei apare tot timpul cînd se dau definiţii pe o mulţime factor, folosind reprezentanţi oarecare ai claselor.

soluţii în $\mathbb{Z}$. Apare ideea (similară cu aceea de la construcţia precedentă a lui $\mathbb{Z}$) de a introduce o nouă mulţime de numere (numerele *raţionale*) ca fiind „toate cîturile posibile de numere întregi". De exemplu, cîtul împărţirii lui 3 la 2 va fi „numărul raţional" („fracţia") 3/2. Deoarece acelaşi cît este dat şi de împărţirea lui 6 la 4 (sau a lui 9 la 6 etc.), este necesar să precizăm *cînd două fracţii a/b şi c/d sînt egale*. Aceasta revine la *a defini o relaţie de echivalenţă* pe mulţimea perechilor de forma (a, b), cu $a, b \in \mathbb{Z}$, $b \neq 0$ (o fracţie va fi o clasă de echivalenţă de perechi). Relaţia de echivalenţă este definită de

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

Cititorul poate demonstra uşor că este vorba într-adevăr de o relaţie de echivalenţă.

O clasă de echivalenţă (un element al mulţimii $\mathbb{Z}\times\mathbb{Z}^*/\sim$) este notată cu a/b sau $\dfrac{a}{b}$ şi este numit(ă) *fracţie*; a este *numărătorul*, iar b este *numitorul* fracţiei a/b. Mulţimea fracţiilor (mulţimea cît $\mathbb{Z}\times\mathbb{Z}^*/\sim$) se notează prin tradiţie cu $\mathbb{Q}$ (de la iniţiala cuvîntului *quotient*, care înseamnă *cît* în engleză şi în franceză). Mulţimea $\mathbb{Z}$ se poate identifica cu o parte a lui $\mathbb{Q}$: numărul întreg a se identifică cu fracţia $\dfrac{a}{1}$. Pe $\mathbb{Q}$ se introduc operaţiile de adunare şi înmulţire, inspirate de regulile cunoscute din gimnaziu (aducerea la acelaşi numitor etc.):

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

Ca şi la construcţia lui $\mathbb{Z}$, trebuie arătat că *definiţiile sînt corecte* (nu depind de alegerea reprezentanţilor fracţiilor) şi că $\mathbb{Q}$, înzestrat cu aceste operaţii, este *inel comutativ unitar* (elementul nul este fracţia 0/1, iar elementul unitate este fracţia 1/1). Mai mult, $\mathbb{Q}$ este *corp*: orice element nenul $\dfrac{a}{b}$ are invers faţă de înmulţire: $\left(\dfrac{a}{b}\right)^{-1} = \dfrac{b}{a}$.

Importanţa construcţiei de mai sus depăşeşte cadrul elementar al construcţiei lui $\mathbb{Q}$; aceeaşi idee, cu modificări minore, se aplică la *construcţia inelului de fracţii al unui inel comutativ relativ la un sistem multiplicativ închis* al său, construcţie fundamentală în toată matematica.

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

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

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

Corectitudinea definiţiei este propusă ca exerciţiu.

3.3 Definiţie. Un corp comutativ $(K, +, \cdot)$ se numeşte *corp ordonat* dacă este înzestrat cu o relaţie 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) $a \leq b$ şi $c \geq 0 \Rightarrow ac \leq bc$.

$\mathbb{Q}$ este un corp ordonat faţă de relaţia de ordine uzuală; mai mult, orice relaţie de ordine pe $\mathbb{Q}$ în raport cu care acesta devine un corp ordonat coincide cu ordinea uzuală (vezi Exerciţii).

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

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

Exerciţii

1. Demonstraţi că orice element din $\mathbb{Q}$ se poate scrie ca o fracţie a/b, cu $a, b \in \mathbb{Z}$ şi $b > 0$.

2. Demonstraţi că relaţia de ordine uzuală pe $\mathbb{Q}$ (vezi def. II.3.2) este corect definită şi $\mathbb{Q}$ devine corp ordonat.

3. Fie $(K, +, \cdot, \leq)$ un corp ordonat, cu element nul 0 şi 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) $0 < a$ şi $0 < b \Rightarrow 0 < ab$ şi $0 < a^{-1}$; e) $0 < a < b \Rightarrow 0 < b^{-1} < a^{-1}$.

În particular, $\operatorname{car} K = 0$ (adică $n\cdot 1 \neq 0$, $\forall n \in \mathbb{N}^*$) şi există un unic morfism de corpuri $\varphi : \mathbb{Q} \to K$. Morfismul φ este cu necesitate injectiv; arătaţi că este şi morfism de ordine.

4. Demonstraţi că relaţia de ordine uzuală este singura relaţie de ordine pe $\mathbb{Q}$ în raport cu care acesta devine corp ordonat.

5. Fie K un corp ordonat. Demonstraţi că funcţia valoare absolută $|\ |: K \to K$ are proprietăţile 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. Arătaţi că nu orice submulţime nevidă majorată a lui $\mathbb{Q}$ are margine superioară.

II.4. Corpul numerelor reale

Necesitatea introducerii numerelor întregi şi a celor raţionale este aproape evidentă din experienţa imediată. Nu acesta este cazul numerelor reale, care au apărut din raţiuni 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 ştiinţei şi 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 gîndirii), unde s-a fixat un punct O (*originea*, corespunzînd lui 0) şi un alt punct U, diferit de primul (corespunzător lui 1 şi 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 *distanţa* de la O la P (dacă P este de aceeaşi parte ca şi U faţă de O), respectiv distanţa de la O la P luată cu semnul minus dacă O este între U şi P. Se conturează astfel ideea intuitivă că numerele reale „pot măsura orice distanţă”. Este semnificativ acest punct de vedere dacă se observă rolul esenţial pe care îl are $\mathbb{R}$ în definiţia generală a *spaţiilor metrice* (spaţii în care este definită o noţiune de *distanţă*).

În multe cărţi (între care şi manualele de Analiză de liceu) structura numerelor reale este dată „axiomatic”: se numeşte *corp al numerelor reale* un *corp comutativ* $(\mathbb{R}, +, \cdot)$ înzestrat cu o relaţie de *ordine totală* " $\leq$ ", satisfăcînd proprietăţile:

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

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

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

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

Evident, această definiţie ridică două probleme: *existenţa* unei structuri cu proprietăţile de mai sus şi *unicitatea* sa. Unicitatea este tranşată de următorul rezultat:

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

Problema existenţei se rezolvă printr-o *construcţie efectivă* a lui $\mathbb{R}$, presupunînd dat $\mathbb{Q}$. Cele mai cunoscute procedee sînt *construcţia zecimală*, *construcţia prin tăieturi în* $\mathbb{Q}$ şi *construcţia cu ajutorul şirurilor Cauchy* (şiruri *fundamentale*). Construcţia folosind şirurile Cauchy prezintă avantajele eleganţei şi rapidităţii şi se foloseşte şi la alte construcţii importante: *completatul unui corp normat oarecare, completatul unui spaţiu metric, completatul unui spaţiu vectorial normat*.

Pentru edificarea cititorului, vom schiţa construcţia zecimală şi apoi prezentăm construcţia cu şirurile Cauchy. Construcţia prin tăieturi, aparţinînd lui Dedekind, este descrisă la exerciţii.

Construcţia zecimală a lui $\mathbb{R}$ (datorată lui Weierstrass[28]) identifică un număr real cu o „fracţie 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 spaţiu…;). Formal, se consideră mulţimea :

$$\mathfrak{R} = \{b_0{,}b_1b_2\ldots b_n\ldots \mid b_0 \in \mathbb{Z}, b_i \in \{0, 1, \ldots, 9\}, \forall i \in \mathbb{N}^*\}$$

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

Interpretarea intuitivă este: „$b_0,b_1b_2\ldots b_n\ldots$ este suma seriei $b_0 + \sum_{n\geq 1} b_i \cdot 10^{-i}$" (dar, evident, nu putem *defini* astfel un număr real. De ce?).

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

Apar însă probleme : 0,9999… , scris şi ca 0,(9) („cu perioada 9") este de fapt 1 (formal 1,000…), după cum se vede făcînd suma seriei corespunzătoare; cum nu dorim ca un acelaşi număr real să aibă două reprezentări zecimale distincte, trebuie făcută următoarea „identificare": orice şir de forma $b = b_0,b_1b_2\ldots b_n\ldots$, cu proprietatea că $\exists k \geq 0$ astfel încît $b_i = 9$, $\forall i > k$ şi $b_k < 9$, este identificat cu şirul $b_0,b_1b_2\ldots(b_k + 1)000\ldots$ (dacă $k \geq 1$), respectiv cu $(b_0 + 1),000\ldots$ (dacă $k = 0$). Pentru rigurozitate, se defineşte o relaţie de echivalenţă $\sim$ pe $\mathfrak{R}$, ca mai sus, iar mulţimea factor $\mathfrak{R}/\sim$ va fi prin definiţie $\mathbb{R}$. Alte dificultăţi apar la definirea adunării şi înmulţirii a două fracţii zecimale infinite (de fapt a unor clase de echivalenţă din $\mathfrak{R}/\sim$), fiind necesară apelarea la operaţiile pe „trunchierile raţionale" ale şirurilor respective şi la definirea unei noţiuni de limită în $\mathfrak{R}/\sim$. Invităm cititorul să încerce să dea singur aceste definiţii şi să demonstreze pe baza lor proprietăţile uzuale ale operaţiilor cu numere reale, pentru a măsura dificultăţile construcţiei. Avantajele acestei abordări (în măsura detalierii efective de către cititor!) constau în apropierea de imaginea intuitivă a conceptului de număr real şi la definirea *relaţiei de ordine*, care coincide cu cea *lexicografică*[29]: se defineşte $b_0,b_1b_2\ldots b_n\ldots < c_0,c_1c_2\ldots c_n\ldots \Leftrightarrow \exists k \in \mathbb{N}$ astfel încît $b_k < c_k$ şi, $\forall i < k$, are loc $b_i = c_i$.

Construcţia lui $\mathbb{R}$ cu ajutorul şirurilor Cauchy (G. Cantor)

$\mathbb{Q}$ este un *corp normat*. Mai precis, aplicaţia *valoare absolută* (sau *modùl*) $|\cdot| : \mathbb{Q} \to \mathbb{Q}$,

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

are proprietăţile (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*[30]. Cu ajutorul normei definim o *distanţă* (o *metrică*)[31], adică o aplicaţie $d : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, $d(x, y) := |x - y|$, $\forall (x, y) \in \mathbb{Q}$, cu proprietăţile:

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 $d(x, y) = 0 \Leftrightarrow x = 0$.

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

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

---

[29] Lexicon = dicţionar. Puteţi spune de ce se numeşte aşa ordinea definită?

[30] În general, o *normă* ia valori în $\mathbb{R}$, pe care nu l-am construit încă… , deci titulatura este puţin forţată.

[31] Aceeaşi observaţie ca mai sus: o *distanţă* ia în general valori reale.

Metrica determină o *topologie*[32] pe $\mathbb{Q}$. Proprietăţile metrice şi topologice ale lui $\mathbb{Q}$ nu sînt prea bune, tocmai din cauzele amintite la început: nu orice şir de numere raţionale „care ar trebui să fie convergent la ceva” este convergent la un număr raţional (de exemplu, şirul aproximărilor zecimale ale lui $\sqrt{2}$).

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

Bineînţeles, nu orice şir de numere raţionale „are o limită” în sens intuitiv (de exemplu şirul $((-1)^n)_{n \geq 1}$). Pe de altă parte, nu putem defini „existenţa limitei” şirului (x_n) direct ($\exists l$ astfel încît $x_n \to l$), căci l este în general un număr real, concept pe care tocmai îl construim! Din fericire, ştim de la Analiză că *şirurile care au limită în $\mathbb{R}$ sînt exact şirurile Cauchy* (noţiune în care *nu apare explicit* limita şirului).

4.1 Definiţie. Şirul de numere raţionale $(x_n)_{n \geq 1}$ se numeşte *şir Cauchy* (sau *şir fundamental*) dacă satisface condiţia:

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

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

Putem aplica acum ideea intuitivă expusă la început şi să definim două şiruri $(x_n), (y_n) \in \mathcal{C}$ ca fiind *echivalente*[33] dacă „au aceeaşi limită”. Şi 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 sfîrşit, definim un *număr real* ca o *clasă de echivalenţă de şiruri din* $\mathcal{C}$; mai precis, mulţimea factor $\mathcal{C}/\sim$ o notăm cu $\mathbb{R}$ şi o numim *mulţimea numerelor reale*. Se observă că orice număr raţional a poate fi identificat cu clasa în $\mathcal{C}/\sim$ a *şirului constant* $(a, a, \ldots) \in \mathcal{C}$ (adică am obţinut într-adevăr o *extindere* a lui $\mathbb{Q}$).

Rămîn sarcinile: de a *defini operaţiile*, de a demonstra *corectitudinea definiţiilor* şi de a *verifica axiomele de corp comutativ* pentru $\mathbb{R}$. Apoi trebuie definită *relaţia de ordine* şi arătat că: $\mathbb{R}$ este *total ordonat*, *relaţia de ordine este compatibilă cu structura de corp şi orice submulţime nevidă majorată are margine superioară*.

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

---

[32] Nu mai definim topologia, vezi orice manual de Analiză elementară.
[33] Adică "definesc" acelaşi număr real.

$(x_n - y_n) \to 0$ (unde scriem $(z_n) \to 0$ 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

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

se demonstrează că $\mathfrak{Z}$ este *ideal maximal* în $\mathfrak{C}$ (şi relaţia "~" coincide cu relaţia de congruenţă modulo $\mathfrak{Z}$). Rezultă imediat atunci că $\mathbb{R} = \mathfrak{C}/\mathfrak{Z}$ este corp comutativ şi cu aceasta se încheie partea „algebrică” a construcţiei lui $\mathbb{R}$. Notăm cu $[(x_n)]$ imaginea în $\mathfrak{C}/\mathfrak{Z}$ a şirului $(x_n) \in \mathfrak{C}$. Sumarizăm construcţia în următoarea:

4.2 Teoremă. *a) Mulţimea $\mathfrak{C}$ a şirurilor Cauchy de numere raţionale este un inel comutativ unitar*[34] *în raport cu operaţiile de adunare şi înmulţire definite „punctual”:*

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

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

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

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

d) Definim pe $\mathfrak{C}/\mathfrak{Z}$ relaţia binară " $<$ " :

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

Atunci " $<$ " este bine definită (nu depinde de reprezentanţi) şi este o relaţie de ordine strictă pe $\mathfrak{C}/\mathfrak{Z}$ (ireflexivă şi tranzitivă). Relaţia de ordine nestrictă asociată, notată " $\leq$ ", este o relaţie 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 $|\cdot| : \mathbb{R} \to \mathbb{R}, |[(x_n)]| = [(|x_n|)]$, $\forall (x_n) \in \mathfrak{C}$. Definiţia este corectă şi au loc proprietăţile normei N1-N4 *de mai sus (bineînţeles, $\mathbb{Q}$ este înlocuit cu $\mathbb{R}$).*

f) Orice şir Cauchy $(r_n)_{n \geq 1}$ de numere reale este convergent la un număr real.[35]

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

h) $\mathbb{Q}$ este dens în $\mathbb{R}$ (orice număr real este limita unui şir de numere raţionale).

Demonstraţie. *a)* Demonstrarea faptului că suma şi produsul a două şiruri Cauchy este tot şir Cauchy este un exerciţiu elementar de Analiză (cf. demonstraţia la „suma, resp. produsul, a două şiruri convergente este un şir convergent”). Este utilă demonstrarea în prealabil a faptului că orice şir 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 $\mathfrak{C}$?

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

---

[34] Este şi integru?

[35] Lăsăm cititorului sarcina de a defini noţiunile de şir Cauchy şi de limită în $\mathbb{R}$.

$\mathfrak{Z}$ este maximal: dacă $(x_n) \in \mathfrak{C} \setminus \mathfrak{Z}$, atunci există $N \in \mathbb{N}$ şi $\delta > 0$ 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, $\forall n \geq N$,

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

Raţionamentul, ca şi multe altele de acelaşi gen, se vede mai bine (şi 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 şirul (y_n) prin: $y_n = 0$ dacă $n < N$ şi $y_n = 1/x_n$ dacă $n \geq N$. Şirul (y_n) este Cauchy (demonstraţi!) şi $x_n y_n = 1 + z_n$, unde z_n este 0 pentru $n \geq N$, deci $(z_n) \in \mathfrak{Z}$.

e) Trebuie arătat mai întîi că $(|x_n|)$ este şir Cauchy şi că definiţia nu depinde de reprezentanţi. Demonstraţia proprietăţilor normei se face apelînd la proprietăţile 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 şir Cauchy de numere reale. Fie $r_n = [(r_{nk})_{k \geq 1}]$, unde $(r_{nk})_{k \geq 1}$ este un şir Cauchy de numere raţionale (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 nişte şiruri strict crescătoare de numere naturale pe care le definim inductiv, astfel:

Cum $(r_n)_{n \geq 1}$ este şir 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 şir 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 $n \in \mathbb{N}$, $n \geq 2$ şi presupunem că am definit $i_1 < i_2 < \ldots < i_{n-1}$ şi $j_1 < j_2 < \ldots < j_{n-1}$, numere naturale astfel încît, $\forall k \in \{1, \ldots, n-1\}$:

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

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

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

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

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

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

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

Cum $(r(i_n, k))_{k \geq 1}$ e şir 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 $k = n - 1$ şi $s = i_n$, $t = i_{n-1}$, avem $|r_{i_n} - r_{i_{n-1}}| < 1/2^n$ (inegalitate în $\mathbb{R}$), deci (din definiţia relaţiei 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) şi (3) sînt satisfăcute, cu $k = n$ şi că $j_n > j_{n-1}$. Am construit inductiv şirurile 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 şir 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 $j_m > j_m$ şi 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 şir Cauchy.

Să arătăm că r_n are limita $x := [(r(i_n, j_n))_{n \geq 1}]$. Fie $\varepsilon > 0$ şi $k \in \mathbb{N}$ 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 demonstraţia). Aceasta revine la a proba existenţa 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 inegalităţii (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 convergenţei în $\mathbb{R}$ se vor fi întrebat de ce am dat o demonstraţie separată pentru *f)*, deşi rezultă din *g)* (vezi Exerciţii). Pentru răspuns, vezi construcţia de mai jos a *completatului unui corp normat*.

h) Exerciţiu. □

Metoda completării prin şiruri Cauchy este folosită şi la ***completatul unui spaţiu metric*** oarecare, construcţie fundamentală în Analiză şi topologie:

4.3 Definiţie. Fie X o mulţime nevidă. O funcţie $d : X \times X \to \mathbb{R}$ se numeşte *distanţă* (*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: $d(x, y) = 0 \Leftrightarrow x = 0$; 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 distanţă pe X, se numeşte *spaţiu metric*; elementele lui X se mai numesc şi *puncte* ale lui X.

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

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

Distanţa d defineşte o *topologie* pe X, în care un sistem fundamental de vecinătăţi al unui punct $x \in X$ este $\{S(x, r) \mid r \in \mathbb{R}, r > 0\}$ (mulţimea sferelor deschise centrate în x). Altfel spus, o submulţime D a lui X este declarată *deschisă* dacă $\forall x \in D$, $\exists r > 0$ astfel încît $S(x, r) \subseteq D$. Un şir $(x_n)_{n \geq 1}$ este *convergent* la $x \in X$ dacă şi numai dacă $\forall \varepsilon > 0$, $\exists N \in \mathbb{N}$ astfel încît $\forall n > N$ are loc $d(x_n, x) < \varepsilon$. Spaţiul metric (X, d) se numeşte *complet* dacă orice şir Cauchy de elemente din X este convergent la un element din X.

Am văzut că $\mathbb{Q}$ este spaţiu metric, cu distanţa $d(x, y) = |x - y|$, dar nu este complet. Din punct de vedere topologic, construcţia lui $\mathbb{R}$ prezentată mai sus este un caz particular al *completării unui spaţiu metric*, care, plecînd de la un spaţiu metric (X, d), construieşte un spaţiu metric *complet* $(\widehat{X}, \widehat{d})$ şi o aplicaţie injectivă $\varphi : X \to \widehat{X}$, astfel încît $\varphi(X)$ este densă în $\widehat{X}$ şi φ păstrează distanţele. Construcţia 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 foloseşte direct o relaţie de echivalenţă "~" definită pe mulţimea $\mathcal{C}$ a şirurilor Cauchy de elemente din X; mulţimea $\mathcal{C}/\sim$ se înzestrează cu o metrică (cum?) şi este spaţiul metric complet căutat.

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

4.4 Definiţie. Fie K un corp comutativ. O funcţie $N : K \to \mathbb{R}$ se numeşte *normă* dacă satisface condiţiile:

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 şi N o normă pe K se numeşte *corp normat*. Exemple uzuale sînt $(\mathbb{Q}, |\ |)$, $(\mathbb{R}, |\ |)$.

Norma pe K defineşte o metrică $d : K \times K \to \mathbb{R}$ prin relaţia $d(x, y) := N(x - y)$ (verificaţi!). Dacă spaţiul metric (K, d) *nu* este complet, se poate construi ca mai sus *completatul său* $\widehat{K}$, care e spaţiu metric; în plus, se pot defini operaţii pe $\widehat{K}$ faţă de care acesta devine corp normat. O abordare mai rapidă reia ideea de a folosi idealul $\mathcal{Z}$ al şirurilor cu limita 0 în inelul $\mathcal{C}$ al şirurilor Cauchy de elemente din K şi construieşte $\widehat{K} := \mathcal{C}/\mathcal{Z}$.

4.5 Exemplu. (Corpul numerelor p-adice) Fie $p \in \mathbb{Z}$ un număr prim. Dacă $n \in \mathbb{Z}$ şi $\alpha \in \mathbb{N}$, scriem $p^{\alpha} \| n$ dacă $p^{\alpha} | n$ şi $p^{\alpha+1} \nmid n$. Pentru orice $n \in \mathbb{Z}$, $\exists! \alpha \in \mathbb{N}$ astfel încît $p^{\alpha} \| n$. Definim $v_p(n)$, *valuarea p-adică* a lui n, ca fiind unicul numărul natural α astfel încît $p^{\alpha} \| n$. Dacă $r = m/n \in \mathbb{Q}$, cu $m, n \in \mathbb{Z}$, definim[36] $v_p(m/n) := v_p(m) - v_p(n)$. Norma *p-adică* a lui r este

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

[36] Verificaţi corectitudinea definiţiei!

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

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

Un corp normat $(K, |\ |)$ care satisface proprietatea NA se numeşte *non-arhimedian* (*sau ultrametric*), deoarece nu satisface *proprietatea lui Arhimede*[37]: $\forall x, y \in K$ cu $x \ne 0$, $\exists n \in \mathbb{N}^*$ astfel încît $|nx| \ge |y|$.

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

Aceeaşi idee, a şirurilor Cauchy, apare şi la construcţia *completatului unui spaţiu liniar normat*. Nu mai intrăm în detalii (vezi de ex. MARINESCU [1983]).

Exerciţii

1. Demonstraţi că în $\mathbb{R}$ (construit cu şiruri Cauchy) orice submulţime nevidă majorată are margine superioară.

2. Fie K un corp comutativ total ordonat în care orice submulţime nevidă majorată are margine superioară. Demonstraţi că orice şir Cauchy în K este convergent.

3. (Construcţia lui Dedekind a lui $\mathbb{R}$ prin tăieturi în $\mathbb{Q}$) Se numeşte *tăietură* în $\mathbb{Q}$ o pereche (A, B) de submulţimi ale lui $\mathbb{Q}$ cu proprietăţile: i) $A \ne \varnothing$, $B \ne \varnothing$; ii) $A \bigcup B = \mathbb{Q}$; iii) $\forall a \in A$, $\forall b \in B$ are loc $a < b$; iv) B nu are minim.

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

a) Dacă (A, B) este tăietură în $\mathbb{Q}$, atunci $A \bigcap B = \varnothing$ şi $B = \mathbb{Q} \setminus A$.

b) $\forall (A, B) \in T(\mathbb{Q})$ are proprietatea: iii') $\forall a \in A$, $\forall c \in \mathbb{Q}$ cu $c < a$ are loc $c \in A$. Reciproc, dacă perechea (A, B) satisface i), ii), iii') şi $A \bigcap B = \varnothing$, atunci (A, B) satisface i)-iii).

b) Pentru o pereche (A, B) care satisface proprietăţile i)-iii), definim

$$n(A, B) = \begin{cases} (A, B) & \text{dacă } B \text{ nu are minim} \\ \big(A \cup \min(B), B \setminus \min(B)\big) & \text{dacă } B \text{ are minim} \end{cases}$$

Atunci $n(A, B)$ este tăietură în $\mathbb{Q}$.

b) Definind relaţia " $\le$ " pe $T(\mathbb{Q})$ prin $(A, B) \le (C, D) \Leftrightarrow A \subseteq C$ ($\Leftrightarrow D \subseteq B$), se obţine o relaţie de ordine totală pe $T(\mathbb{Q})$.

[37] $\mathbb{Q}$ şi $\mathbb{R}$ sînt *corpuri arhimediene*, căci satisfac această proprietate.

c) Aplicaţia $\varphi : \mathbb{Q} \to T(\mathbb{Q})$, $\varphi(x) = (L_x, R_x)$, cu $L_x = \{y \in \mathbb{Q} \mid y \le x\}$ şi $R_x = \{y \in \mathbb{Q} \mid y > x\}$, este injectivă şi crescătoare (deci x poate fi identificat cu $\varphi(x) \in T(\mathbb{Q})$, iar $\mathbb{Q}$ cu $\varphi(\mathbb{Q})$). Notăm prin abuz tot cu a tăietura $\varphi(a)$, $\forall a \in \mathbb{Q}$.

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

e) Definind: $(A, B) + (C, D) := n(A + C, \mathbb{Q} \setminus (A + C))$, $\forall (A, B), (C, D) \in T(\mathbb{Q})$, (unde $A + C = \{a + c \mid a \in A, c \in C\}$), se obţine o lege de compoziţie pe $T(\mathbb{Q})$; $(T(\mathbb{Q}), +)$ este grup abelian, iar $\varphi : \mathbb{Q} \to T(\mathbb{Q})$ definit mai sus este morfism de grupuri. (Obs. Opusul lui $\alpha = (A, B)$ este $n(-B, -A)$, notat cu $-\alpha$. Am notat $-A = \{-a \mid a \in A\}$. Demonstraţi că $\forall \alpha \in T(\mathbb{Q})$, are loc[38]: $\alpha > 0 \Leftrightarrow -\alpha < 0$.)

f) Fie $\alpha = (A, B)$, $\gamma = (C, D) \in T(\mathbb{Q})$. Definim produsul $\alpha\gamma$ astfel:

Dacă $\alpha \ge 0$, $\gamma \ge 0$, fie $L := \{x \in \mathbb{Q} \mid \exists a \in A, \exists c \in C, a \ge 0, c \ge 0$ astfel încît $x \le ac\}$. Definim în acest caz $\alpha\gamma := n(P, \mathbb{Q} \setminus P)$.

Dacă $\alpha \ge 0$, $\gamma < 0$, atunci $-\gamma > 0$ şi definim $\alpha\gamma := -(\alpha(-\gamma))$.

Dacă $\alpha < 0$, $\gamma < 0$, definim $\alpha\gamma := (-\alpha)(-\gamma)$.

Atunci "·" definită ca mai sus defineşte o operaţie pe $T(\mathbb{Q})$, $(T(\mathbb{Q}), +, \cdot, \le)$ este corp ordonat şi $\varphi : \mathbb{Q} \to T(\mathbb{Q})$ este morfism de corpuri.

4. Verificaţi afirmaţiile nedemonstrate de la exemplul II.4.5.

[38] Relaţia de ordine este, desigur, cea definită la b).

Index

R

S

Ş

T

U

V

Z

Bibliografie

1. BECHEANU, M. et al. [1983], *Algebră pentru perfecţionarea profesorilor,* Ed. didactică şi pedagogică, Bucureşti.
2. FREUDENTHAL, H. [1973], *Limbajul logicii matematice,* Ed. Tehnică, Bucureşti.
3. ION, I.D., NĂSTĂSESCU, C., NIȚĂ, C. [1984] *Complemente de algebră*, Ed. Ştiinţifică şi enciclopedică, Bucureşti.
4. ION, I.D., RADU, N. [1981a] *Algebra*, Ed. Didactică şi pedagogică, Bucureşti.
5. ION, I.D., RADU, N., NIȚĂ, C., POPESCU, D. [1981b] *Probleme de algebră*, Ed. Didactică şi pedagogică, Bucureşti.
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., Bucureşti.
8. NĂSTĂSESCU, C. [1974] *Introducere în teoria mulţimilor*, Ed. Didactică şi pedagogică, Bucureşti.
9. NĂSTĂSESCU, C. [1976] *Inele. Module. Categorii*, Ed. Academiei R.S.R., Bucureşti.
10. NĂSTĂSESCU, C., NIȚĂ, C., VRACIU, C. [1986] *Bazele Algebrei, vol. I*, Ed. Academiei R.S.R., Bucureşti.
11. NĂSTĂSESCU, C. [1983] *Teoria dimensiunii în algebra necomutativă,* Ed. Academiei R.S.R., Bucureşti.
12. NIȚĂ, C., SPIRCU, T. [1974] *Probleme de structuri algebrice*, Ed. Tehnică, Bucureşti.
13. PURDEA, I. [1982] *Tratat de algebră modernă,* vol II, Ed. Academiei R.S.R., Bucureşti.
14. REGHIŞ, M. [1981] *Elemente de teoria mulţimilor şi logică matematică*, Ed. Facla, Timişoara.
15. SCORPAN, A. [1996] *Introducere în teoria axiomatică a mulţimilor*, Ed. Universităţii Bucureşti, Bucureşti.
16. SIREȚCHI, GH. [1978] *Analiză matematică, vol. I*, ed IV., Tipografia Univ. Bucureşti.
17. VAN DERWAERDEN, B.L. [1985], *A History of Algebra,* Springer-Verlag, Berlin.