CZU 512.55 (075.8)
C28

Lucrarea prezintă un ciclu de lecţii despre sistemele numerice principale: numere naturale, întregi, raţionale, reale, complexe şi cuaternioni. Se aplică metoda axiomatică şi pentru fiecare sistem numeric se demonstrează unicitatea, existenţa şi proprietăţile de bază.

Se adresează studenţilor de la specialitatea Matematică, profesorilor de matematică, poate fi utilă tuturor celor care se interesează de fundamentele matematicii.

Recenzent: **Vasile Marin**, doctor în ştiinţe fizico-matematice, conferenţiar universitar

DESCRIEREA CIP A CAMEREI NAŢIONALE A CĂRŢII
Caşu, Alexei
Sisteme numerice: **[**pentru uzul studenţilor**]** / Alexei Caşu, Ion Goian, Parascovia Sârbu; Univ. de Stat din Moldova, Centrul de Educaţie şi Cercetare în Matematică şi Informatică (CECMI). –Ch.: CEP USM, 2008, 165 p.
Bibliogr.: P.162 - 150 ex.
ISBN 978-9975-70-742-8
511.11(075.8)
C 28

ISBN

Cuprins

Introducere

Eroul principal al acestei cărți este numărul, „el, care a declanşat atâtea secole de matematică şi este încă un mister pentru matematician” ([7]). Scopul prezentei lucrări este de a diminua în măsura posibilităților partea misterioasă a numerelor, de a elucida unele aspecte esențiale ale acestui concept de bază al matematicii. Esența lucrării constă în abordarea problemei din punct de vedere axiomatic, ceea ce permite obținerea tuturor sistemelor numerice principale, consecutiv, în ordinea lor firească: numere naturale $\mathbb{N}$, întregi $\mathbb{Z}$, raționale $\mathbb{Q}$, reale $\mathbb{R}$, complexe $\mathbb{C}$, hipercomplexe $\mathbb{H}$. Începând cu sistemul de numere naturale, fiecare sistem următor de numere îl generalizează pe cel precedent şi îl conține, posedând proprietăți noi. Se termină construirea acestui „edificiu” cu fixarea „acoperişului” – teorema lui Frobenius, care arată că alte generalizări de acest tip nu există.

R.Dedekind, unul dintre fondatorii acestui domeniu al matematicii, afirma că „numerele sunt creații libere ale intelectului uman, ele servesc ca mijloc de a înțelege mai uşor şi mai clar diversitatea lucrurilor”. Fără a exagera se poate spune că sistemele numerice tradiționale formează cel mai important fundament al întregii matematici, de aceea cunoaşterea acestui domeniu este absolut obligatorie pentru orice om ce se interesează de matematică, atât pentru profesionişti, cât şi pentru amatori. O bună parte a istoriei matematicii este, de fapt, istoria dezvoltării noțiunii de număr. Este uşor de observat că ordinea expunerii noastre a sistemelor numerice nu corespunde în totalitate cu ordinea apariției istorice a acestor tipuri de numere (de exemplu, numerele negative au apărut mai târziu decât cele raționale pozitive).

Remarcăm că materia expusă în această carte a servit drept bază pentru un curs care în diferite timpuri s-a numit „Bazele aritmeticii”, „Bazele cursului şcolar de matematică”, „Sisteme numerice”, „Aritmetica teoretică”.

În mod tradițional, expunerea începe cu cel mai „simplu” sistem numeric – cel al numerelor naturale $\mathbb{N}$. El se defineşte cu

ajutorul sistemului de axiome Peano, printre care cea mai lucrativă este axioma inducţiei, ea servind drept bază pentru cunoscuta metodă de demonstrare – metoda inducţiei matematice. Reieşind din axiome, se obţine existenţa operaţiilor de adunare şi înmulţire şi proprietăţile lor, cât şi relaţia de ordine (totală) în $\mathbb{N}$. Astfel întreaga teorie a numerelor naturale poate fi dedusă din sistemul de axiome Peano.

Cercetarea numerelor, efectuată în această lucrare, are la baza noţiunea de mulţime si aplicarea consecventă a metodei axiomatice. Noi vom utiliza in conţinutul de bază al lucrării numai unele rezultate din teoria mulţimilor (fără a specifica axiomatica acestei teorii) şi unele aspecte din logica matematică. Totuşi, in Anexa I prezentăm un sistem de axiome al teoriei mulţimilor, suficient pentru expunerea materialului acestei lucrări. Se ştie că condiţiile principale referitoare la un sistem de axiome sunt următoarele: compatibilitatea (lipsa contradicţiilor), completitudinea şi independenţa axiomelor. Prima condiţie poate fi verificată prin construirea unor interpretări (modele) şi se reduce în cazul nostru la existenţa sistemului numeric, definit prin axiomele formulate. A doua condiţie constă în existenţa unui singur obiect (făcând abstracţie de izomorfism) care satisface aceste axiome şi, în cazul nostru, se reduce la unicitatea sistemului numeric construit în baza axiomelor date. A treia condiţie pentru un sistem din n axiome se verifică cu ajutorul unor interpretări (modele) construite pentru $n-1$ axiome. Din aceste considerente principiale rezultă schema expunerii materialului pentru fiecare dintre sistemele numerice cercetate: mai întâi se introduce definiţia sistemului numeric (ea conţine axiomele sistemului numeric analizat), se demonstrează unicitatea sistemului numeric, iar apoi se arată existenţa lui printr-o metodă specială de construcţie a sistemului. Independenţa axiomelor se arată numai pentru numerele naturale, iar în celelalte cazuri se consideră că această cerinţă nu joacă un rol esenţial.

La trecerea de la un sistem numeric la altul se arată necesitatea extinderii sistemului precedent, de regulă se invocă necesitatea închiderii acestui sistem în raport cu noi operaţii,

precum scăderea, împărțirea, trecerea la limită, extragerea rădăcinii. Lărgirea sistemului precedent se înțelege în sensul că sistemul nou conține o parte „izomorfă” cu sistemul care este extins. Astfel sistemul numeric nou îl conține şi îl „perfecționează” pe cel vechi, având în acelaşi timp şi proprietăți noi.

Cel mai important pas în acest proces de extindere a sistemelor numerice constă în demonstrarea existenței noului sistem, arătând în mod concret metoda de construire a lui cu ajutorul sistemului numeric precedent. Astfel existența sistemului nou rezultă din existența predecesorului său. Cât priveşte baza acestui proces – sistemul numerelor naturale, existența lui este echivalentă cu existența unei mulțimi infinite. Aceasta are loc dacă acceptăm axioma infinitului, care este o parte componentă a axiomaticii teoriei mulțimilor.

Ca şi alte domenii ale matematicii, cel cercetat în această lucrare este rodul muncii asidue a multor generații de matematicieni. Vom numi doar câțiva dintre cei mai celebri savanți care şi-au adus aportul în dezvoltarea teoriei sistemelor numerice pe parcursul istoriei: Euclid (356-300 î.e.n.), Arhimedes (287-212 î.e.n.), Rene Descartes (1596-1650), Leonard Euler (1707-1783), Carl Fridrich Gauss (1777-1855), Augustin-Louis Cauchy (1789-1857), William Hamilton (1805-1865), Richard Dedekind (1831-1916), Georg Cantor (1845-1918), Ferdinand Frobenius (1849-1917), Giusseppe Peano (1858-1932).

Capitolul I

Numere naturale

§1. Axiomele lui Peano. Unicitatea şi existența sistemului de numere naturale

În cadrul tendințelor de axiomatizare a matematicii s-a încercat şi axiomatizarea aritmeticii. În cele ce urmează vom prezenta una din variantele posibile de axiomatizare a aritmeticii (în special a numerelor naturale) – cea propusă de matematicianul italian Giusseppe Peano (1858–1932).

Definiția 1. *Vom numi* ***sistem Peano*** *(sau* ***sistem de numere naturale****) un triplet* $(N, 0, s)$, *format dintr-o mulțime nevidă* N, *un element evidențiat al ei* $0 \in N$ *şi o aplicație* $s: N \to N$ *(funcția-succesor), care satisfac condițiile:*

P_1*)* $s(x) \neq 0$, *pentru orice* $x \in N$ *(adică* 0 *nu este succesor pentru nici un element din* N, *de aceea el se va numi* ***element inițial****);*

P_2*)* s *este o funcție injectivă:* $s(x_1) = s(x_2) \Rightarrow x_1 = x_2$ *(adică elemente diferite au succesori diferiți);*

P_3*)* *dacă submulțimea* $P \subseteq N$ *posedă proprietățile:*

(i) $0 \in P$,

(ii) $x \in P$ *implică* $s(x) \in P$,

atunci P *coincide cu* N $(P = N)$.

Afirmațiile $P_1)$, $P_2)$, $P_3)$ se numesc *axiomele lui Peano*. Un rol deosebit îl joacă axioma $P_3)$ numită *axioma inducției,* care servește bază pentru demonstrații prin *metoda inducției matematice* (condiția (i) este baza inducției, iar condiția (ii) reprezintă pasul

inducției, adică trecerea de la elementul $x \in P$ la succesorul său $s(x) \in P$). Elementul x se va numi *predecesorul* lui $s(x)$.

Unul dintre rezultatele principale despre sistemele Peano constă în următoarele.

Teorema 1.1. *Fie* $(N, 0, s)$ *un sistem Peano arbitrar. Atunci:*

1) *pentru orice element* $y \in N$, $y \neq 0$, *există* $x \in N$ *astfel încât* $y = s(x)$ *(adică orice element nenul din* N *posedă predecesor în* N*);*
2) *pentru orice triplet* (A, θ, λ), *unde* A *este o mulțime nevidă,* θ *este un element evidențiat din* A *şi* λ *este o aplicație din* A *în* A, *există o unică funcție* $f : N \to A$, *astfel încât* $f(0) = \theta$ *şi* $f \circ s = \lambda \circ f$, *adică* $f(s(x)) = \lambda(f(x))$, *pentru orice* $x \in N$ *(*f *păstrează elementul inițial şi este compatibilă cu aplicațiile* s *şi* λ *ale sistemelor date):*

$$\begin{array}{ccc} N & \xrightarrow{\ f\ } & A \\ {\scriptstyle s}\downarrow & & \downarrow{\scriptstyle \lambda} \\ N & \xrightarrow{\ f\ } & A \end{array}$$

3) *dacă* (A, θ, λ) *este de asemenea un sistem Peano, atunci* f *este o funcție bijectivă.*

*Demonstrație***.** 1) Notăm prin $s(N) = \{s(x) \mid x \in N\}$ imaginea aplicației $s : N \to N$. Separăm în N submulțimea $M = \{0\} \bigcup s(N)$. Deoarece sunt verificate condițiile:

(i) $0 \in M$,

(ii) din $M \subseteq N$ rezultă $s(M) \subseteq s(N) \subseteq M$

(adică $x \in M$ implică $s(x) \in M$), putem aplica axioma P_3) pentru mulțimea M și obținem $M = N$. Prin urmare, orice element nenul $y \in N$ aparține lui $s(N)$, adică există $x \in N$, astfel încât $y = s(x)$.

2) Considerăm produsul cartezian $N \times A = \{(n,a) \mid n \in N, a \in A\}$. Vom cerceta submulțimi $E \subseteq N \times A$ cu proprietățile:

α) $(0,\theta) \in E$;

β) dacă $(x,y) \in E$, atunci $(s(x), \lambda(y)) \in E$.

Notăm prin $\boldsymbol{S}$ familia tuturor submulțimilor $E \subseteq N \times A$ ce verifică α) și β). Este evident că $N \times A \in \boldsymbol{S}$, de aceea $\boldsymbol{S} \neq \emptyset$. Fie $F = \bigcap_{E \in S} E$. Atunci $F \in \boldsymbol{S}$ și F este cea mai mică submulțime în $N \times A$ care satisface α) și β). Să arătăm că F posedă proprietățile:

I. Pentru orice $x \in N$ *există* $y \in A$ *astfel încât* $(x,y) \in F$;

II. Dacă $(x,y_1), (x,y_2) \in F$, *atunci* $y_1 = y_2$

(*adică orice* $x \in N$ *are un „însoțitor” și acesta este unic*).

Verificăm proprietatea I. Considerăm submulțimea

$$P = \{x \in N \mid \exists\, y \in A, (x,y) \in F\}.$$

Deoarece $F \in \boldsymbol{S}$, din condiția α) avem $(0,\theta) \in F$, adică $0 \in P$. Mai mult, dacă $x \in P$ atunci prin definiție $(x,y) \in F$ pentru un element $y \in A$, și din condiția β) avem $(s(x), \lambda(y)) \in F$, prin urmare $s(x) \in P$. Acum putem aplica axioma P_3) mulțimii P, obținând $P = N$, adică are loc proprietatea I.

Verificăm proprietatea II. Separăm în N submulțimea:

$$P = \{x \in N \mid \textit{există un singur } y \in A \textit{ astfel încât } (x,y) \in F\}.$$

Avem $(0,\theta) \in F$ și, dacă $(0,y) \in F$ pentru un element $y \neq 0$, atunci notând $F' = F \setminus \{(0,y)\}$, obținem mulțimea $F' \in \boldsymbol{S}$ (adică

F' satisface $\alpha)$ şi $\beta))$ şi $F' \subsetneqq F$, ceea ce contrazice minimalitatea lui F. Prin urmare, $y = \theta$ şi $0 \in P$.

Să arătăm că din condiţia $x \in P$ urmează $s(x) \in P$. Fie $x \in P$, adică există un singur $y \in A$ cu $(x, y) \in F$. Atunci din condiţia $\beta)$ rezultă că $(s(x), \lambda(y)) \in F$. Dacă $s(x) \notin P$, atunci există $z \in A$, $z \neq \lambda(y)$ încât $(s(x), z) \in F$; notăm $F'' = F \setminus \{(s(x), z)\}$. Se observă că $F'' \in \boldsymbol{S}$ şi $F'' \subsetneqq F$, în contradicţie cu minimalitatea lui F. Aceasta arată că $s(x) \in P$. Acum din axioma $P_3)$ rezultă $P = N$, adică F posedă proprietatea II.

Cele două proprietăţi I şi II ale mulţimii F ne permit să definim o funcţie $f : N \to A$ prin regula:

$$f(x) = y \Leftrightarrow (x, y) \in F.$$

Din condiţia $\alpha)$ avem $f(0) = \theta$, iar din condiţia $\beta)$ rezultă că pentru orice $x \in N$ din $(x, f(x)) \in F$ urmează $(s(x), \lambda f(x)) \in F$, iar din definiţia funcţiei f avem:

$$f(s(x)) = \lambda(f(x)), \qquad (1)$$

pentru orice $x \in N$, adică $f \circ s = \lambda \circ f$. Rămâne de verificat *unicitatea* acestei funcţii. Fie că mai există o funcţie $g : N \to A$ cu $g(0) = \theta$ şi $g \circ s = \lambda \circ g$. Considerăm mulţimea

$$P = \{x \in N \mid g(x) = f(x)\}.$$

Deoarece $f(0) = \theta$ şi $g(0) = \theta$ avem $0 \in P$. Mai mult, dacă $x \in P$ atunci $g(x) = f(x)$, de aceea:

$$g(s(x)) = \lambda(g(x)) = \lambda(f(x)) \overset{(1)}{=} f(s(x)),$$

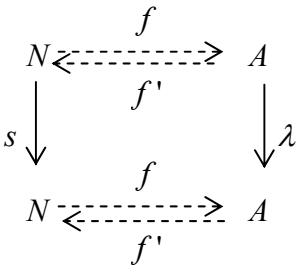
prin urmare $s(x) \in P$. Acum putem aplica axioma $P_3)$ din care rezultă $P = N$, ceea ce denotă că $g = f$.

3) Presupunem că şi tripletul (A, θ, λ) este un sistem Peano, ca şi cel iniţial $(N, 0, s)$. Din cele arătate mai sus (p.2) rezultă că există o singură funcţie $f : N \to A$ cu proprietăţile

$$f(0)=\theta,\quad f\circ s=\lambda\circ f. \tag{2}$$

Dar afirmația din p.2) se poate aplica şi la sistemul Peano (A,θ,λ), obținând o unică funcție $f':A\to N$ cu condiții similare:

$$f'(\theta)=0,\ f'\circ\lambda=s\circ f'. \tag{3}$$



Atunci pentru produsul $f'\circ f:N\to N$ avem:

$$(f'\circ f)(0)=f'(f(0))=f'(\theta)=0,$$
$$(f'\circ f)\circ s=f'\circ(f\circ s)\overset{(2)}{=}f'\circ(\lambda\circ f)=$$
$$=(f'\circ\lambda)\circ f\overset{(3)}{=}(s\circ f')\circ f=s\circ(f'\circ f).$$

Afirmația de *unicitate* din p.2), aplicată la morfismul $f'\circ f:N\to N,$ ne arată că $f'\circ f=1_N.$ În mod similar se arată că $f\circ f'=1_A,$ prin urmare aplicațiile f şi f' sunt reciproc inverse, adică f este o bijecție. □

Din ultima afirmație a acestei teoreme rezultă

Corolarul 1.2. (***unicitatea sistemului Peano***). *Orice două sisteme Peano* $(N_1,0_1,s_1)$ *şi* $(N_2,0_2,s_2)$ *coincid în limitele unei bijecții* $f:N_1\to N_2$ *cu proprietățile* $f(0_1)=0_2$ *şi* $f\circ s_1=s_2\circ f$

(conservarea elementului iniţial şi compatibilitatea cu funcţiile-succesor). □

În acest sens se poate vorbi despre *unicitatea sistemului Peano* (până la un izomorfism).

Fixăm un sistem arbitrar Peano $(\mathbb{N}, 0, s)$. Elementele lui le vom numi *numere naturale*. Dacă $n \in \mathbb{N}$ atunci numărul $n' = s(n)$ se numeşte *succesorul* lui n, iar n se numeşte *predecesorul* lui n'. Numerele naturale sunt notate astfel:

$$0, \quad 1 \overset{def}{=} s(o), \quad 2 \overset{def}{=} s(1), \quad ...$$

şi se numesc, respectiv: *zero*, *unu*, *doi* ş.a.m.d.

Să trecem la cercetarea problemei despre *existenţa* sistemului de numere naturale (sau a sistemului Peano). În cadrul axiomaticii propuse aici ea nu poate fi rezolvată, deoarece depinde de sistemul de axiome al teoriei mulţimilor pe care ne bazăm. Pentru a formula una dintre aceste axiome să amintim definiţia noţiunii de mulţime infinită (ce nu depinde de mulţimea numerelor naturale).

Mulţimea M se numeşte *infinită* dacă există o aplicaţie injectivă $f : M \to M$, astfel încât $f(M) \neq M$. (Această definiţie provine de la Dedekind şi exprimă ideea că în mulţimile finite orice aplicaţie injectivă $f : M \to M$ este o bijecţie şi numai pentru mulţimile infinite poate exista o aplicaţie injectivă $f : M \to M$ care nu este o bijecţie).

Acum putem formula:

Axioma infinitului. *Există mulţimi infinite.*

Propoziţia 1.3. *Existenţa sistemului de numere naturale* $(\mathbb{N}, 0, s)$ *(sau a unui sistem Peano) este echivalentă cu existenţa unei mulţimi infinite (adică cu axioma infinitului).*

Demonstraţie. ($\Rightarrow$) Fie $(\mathbb{N}, 0, s)$ un sistem Peano. Atunci funcţia $s : \mathbb{N} \to \mathbb{N}$ este o aplicaţie injectivă (axioma P_2)) şi $s(\mathbb{N}) \neq \mathbb{N}$,

deoarece $0 \notin s(\mathbb{N})$ conform axiomei P_1). Prin urmare, $\mathbb{N}$ este o mulțime infinită.

($\Leftarrow$) Fie A o mulțime infinită. Atunci, prin definiție, există o aplicație injectivă $f : A \to A$ cu proprietatea $f(A) \neq A$. De aceea putem alege un element $0 \in A$ astfel încât $0 \notin f(A)$.

Fie $\boldsymbol{J}$ totalitatea acelor submulțimi $M \subseteq A$, care posedă proprietățile: $0 \in M$ şi $f(M) \subseteq M$. Deoarece $A \in \boldsymbol{J}$, avem $\boldsymbol{J} \neq \varnothing$ şi putem defini submulțimea $N = \bigcap_{M \in J} M$. Atunci tripletul $(N, 0, f|_N)$ este un sistem Peano:

P_1): $0 \notin f(N)$ (deoarece $0 \notin f(A)$ şi $f(N) \subseteq f(A)$);

P_2): aplicația $f|_N$ (restricția lui f pe N) este injectivă, deoarece f este injectivă;

P_3): fie că $P \subseteq N$ şi P posedă proprietățile:

(i) $0 \in P$,

(ii) $x \in P$ implică $f(x) \in P$.

Astfel avem $0 \in P$ şi $f(P) \subseteq P$, deci $P \in \boldsymbol{J}$ şi din definiția lui N, rezultă $N \subseteq P$, prin urmare $N = P$. □

Observație. La sfârşitul acestei lucrări, în Anexa I, este expus un sistem de axiome ale teoriei mulțimilor. Scopul teoriei axiomatice a mulțimilor este de a indica un sistem de axiome, în baza căruia ar putea fi construită teoria mulțimilor, fără a conduce la apariția paradoxurilor.

În încheierea acestui compartiment remarcăm faptul că există diverse forme de expunere a axiomelor lui Peano. Pentru cele ce urmează (demonstrarea independenței axiomelor) este comod de utilizat următoarea formă a axiomelor Peano.

Definiția 2. ***Numere naturale*** *se numesc elementele unei mulțimi* $\mathbb{N}$ *în care pentru unele elemente* a *şi* b *există relația „*b *este succesorul elementului* a*”* *(numărul ce succede lui* a *se notează cu* a'*) şi care satisface următoarele axiome:*

I. Există numărul 0 *care nu succede nici unui număr natural, adică* $a' \neq 0$ *pentru orice* $a \in \mathbb{N}$;

II. Pentru orice număr $a \in \mathbb{N}$ *există succesorul său* a' *care este unic (adică din* $a = b$ *rezultă* $a' = b'$);

III. Orice număr succede nu mai mult decât unui număr, adică din $a' = b'$ *rezultă* $a = b$*;*

*IV. (****Axioma inducției****) Orice submulțime* $M \subseteq \mathbb{N}$ *ce posedă proprietățile:*

(i) $0 \in M$,

(ii) $a \in M$ *implică* $a' \in M$,

conține toate numerele naturale $(M = \mathbb{N})$.

Observăm că sistemul de axiome $P_1) - P_3)$ este echivalent cu sistemul de axiome I-IV. Relația binară „b este succesorul elementului a” pe mulțimea $\mathbb{N}$, ce verifică axioma II, defineşte o funcție-succesor s pe $\mathbb{N}$, iar axioma III cere ca funcția s să fie injectivă.

Altă variantă a axiomei IV este următoarea:

IV. Dacă* $M \subseteq \mathbb{N}$, $M \neq \varnothing$ *şi* M *posedă proprietățile:*

*(i)** *dacă există un astfel de număr* $0 \in \mathbb{N}$, *ce nu succede nici unui număr natural, atunci* $0 \in M$;

(ii) $a \in M$ *implică* $a' \in M$,

atunci M *coincide cu* $\mathbb{N}$.

Exerciţii

1. Demonstraţi că mulţimea punctelor oricărui segment al unei drepte este infinită.
2. Indicaţi un mod de a stabili o corespondenţă bijectivă între mulţimea punctelor unei drepte şi mulţimea punctelor interioare ale unui segment al dreptei date.
3. Demonstraţi că sistemul de axiome $P_1), P_2), P_3)$ este echivalent cu sistemul de axiome I, II, III, IV.

§2. Adunarea şi înmulţirea numerelor naturale

Să amintim mai întâi că *operaţie algebrică* (sau *lege de compoziţie*) pe mulţimea A se numeşte orice aplicaţie de forma:

$$\varphi : A \times A \to A, (x, y) \to \varphi(x, y) \in A.$$

În acest compartiment vom defini şi vom cerceta două operaţii pe mulţimea $\mathbb{N}$ a numerelor naturale, cu elementul iniţial $0 \in \mathbb{N}$ şi funcţia-succesor $s : \mathbb{N} \to \mathbb{N}$. Pentru comoditate vom nota $s(n) = n'$.

Teorema 2.1. *Există o unică lege de compoziţie*

$$\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \ \varphi(m, n) = m + n$$

*(notată aditiv şi numită **adunare**) pe mulţimea numerelor naturale* $\mathbb{N}$ *astfel încât sunt satisfăcute condiţiile:*

$A_1)$ $m + 0 = m$ *pentru orice* $m \in \mathbb{N}$;

$A_2)$ $m + n' = (m + n)'$ *pentru orice* $m, n \in \mathbb{N}$.

*Demonstraţie***.** Fixăm un număr natural $m \in \mathbb{N}$ şi construim cu ajutorul lui tripletul $(\mathbb{N}, m, s = (\ )')$. Conform teoremei 1.1, p.2), există o unică funcţie $f_m : \mathbb{N} \to \mathbb{N}$ astfel încât $f_m(0) = m$ şi $f_m(n') = (f_m(n))'$. Acum pentru orice pereche $(m, n) \in \mathbb{N} \times \mathbb{N}$ definim legea de compoziţie φ (sau „+") astfel:

$$\varphi(m, n) = m + n \overset{def}{=} f_m(n). \qquad (1)$$

Din această definiție obținem:

$$m+0=f_m(0)=m \text{ (condiția } A_1\text{)};$$

$$m+n'=f_m(n')=(f_m(n))'=(m+n)' \text{ (condiția } A_2\text{)},$$

deci operația $(+)$ satisface condițiile $A_1)$ și $A_2)$. Rămâne de verificat unicitatea acestei operații. Fie că mai avem o lege de compoziție $\psi : \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ cu condițiile $A_1)$ și $A_2)$:

$A_1)$: $\psi(m,0)=m$ pentru orice $m\in\mathbb{N}$;

$A_2)$: $\psi\left(m,n'\right)=\left(\psi\left(m,n\right)\right)'$ pentru orice $m,n\in\mathbb{N}$.

Fixăm un element $m\in\mathbb{N}$ și definim aplicația $g_m:\mathbb{N}\to\mathbb{N}$ astfel:

$$g_m(n)=\psi(m,n), \quad \forall n\in\mathbb{N}.$$

Din condiția $A_1)$ avem $g_m(0)=\psi(m,0)=m,$ iar din $A_2)$ obținem:

$$g_m(n')=\psi(m,n')=(\psi(m,n))'=(g_m(n))'.$$

Prin urmare, g_m satisface condițiile din Teorema 1.1, p.2), de unde rezultă că $g_m=f_m$. Acum pentru orice $m,n\in\mathbb{N}$ avem:

$$\psi(m,n)=g_m(n)=f_m(n)=\varphi(m,n),$$

adică $\varphi=\psi$. □

Astfel condițiile $A_1)$ și $A_2)$ definesc în mod unic operația adunării în $\mathbb{N}$. Aceste condiții se numesc *axiomele adunării* în $\mathbb{N}$.

În continuare vom demonstra unele proprietăți ale operației adunării în $\mathbb{N}$. Pentru aceasta avem nevoie de următoarea afirmație preliminară.

Lema 2.2. *Operația adunării în* $\mathbb{N}$ *satisface condițiile:*

$A_1^{\,0})$ $0+n=n$, *pentru orice* $n\in\mathbb{N}$;

$A_2^{\,0})$ $m'+n=(m+n)'$, *pentru orice* $m,n\in\mathbb{N}$.

Demonstrație. A_1^0) Fie $P = \{n \in \mathbb{N} \mid 0 + n = n\}$. Aplicând A_1) pentru $m = 0$, avem $0 + 0 = 0$, adică $0 \in P$. Dacă $n \in P$ atunci $0 + n = n$ şi, aplicând A_2), obținem

$$0 + n' = (0 + n)' = n',$$

deci $n' \in P$. Acum putem aplica axioma P_3) din care rezultă $P = \mathbb{N}$, adică are loc A_1^0).

A_2^0) Fie

$$P = \{n \in \mathbb{N} \mid m' + n = (m + n)', \text{ pentru orice } m \in \mathbb{N}\}.$$

Din A_1) rezultă $m' + 0 = m' = (m + 0)'$, deci $0 \in P$. Dacă $n \in P$, atunci $m' + n = (m + n)'$ pentru orice $m \in \mathbb{N}$, de aceea din A_2) obținem:

$$m' + n' = (m' + n)' = ((m + n)')' = (m + n')',$$

adică $n' \in P$. Axioma P_3) implică $P = \mathbb{N}$, adică are loc condiția A_2^0). □

Următoarea teoremă conține proprietățile de bază ale operației de adunare în $\mathbb{N}$: asociativitatea şi comutativitatea ei.

Teorema 2.3. *Adunarea numerelor naturale este asociativă şi comutativă, iar elementul inițial* $0 \in \mathbb{N}$ *este element neutru în raport cu această operație, adică:*

1) $(m + n) + p = m + (n + p)$,

2) $m + n = n + m$,

3) $0 + n = n + 0 = n$,

pentru orice $m, n, p \in \mathbb{N}$.

Demonstrație. 1) Fixăm numerele $m, n \in \mathbb{N}$ şi considerăm mulțimea:

$$P = \{p \in \mathbb{N} \mid (m + n) + p = m + (n + p)\}.$$

Din A_1) avem $(m+n)+0=m+n$ şi $m+(n+0)=m+n$, prin urmare, $0\in P$. Pentru orice $p\in P$ din condiţia A_2) obţinem:

$$(m+n)+p'=((m+n)+p)'=(m+(n+p))'=$$
$$=m+(n+p)'=m+(n+p'),$$

prin urmare, $p'\in P$. Din axioma P_3) avem $P=\mathbb{N}$, adică adunarea este asociativă.

2) Fixăm un element $m\in\mathbb{N}$ şi considerăm submulţimea:

$$P=\{n\in\mathbb{N}\mid m+n=n+m\}.$$

Din A_1) şi $A_1{}^0$) avem $m+0=m=0+m$, prin urmare $0\in P$. Dacă $n\in P$, atunci $m+n=n+m$ şi, utilizând condiţiile A_2) şi $A_2{}^0$), obţinem:

$$m+n'=(m+n)'=(n+m)'=n'+m,$$

adică $n'\in P$. Axioma P_3) acum implică $P=\mathbb{N}$, adică adunarea este comutativă.

3) Din $A_1{}^0$) şi A_1) avem $0+n=n=n+0$ pentru orice $n\in\mathbb{N}$. □

Acum vom utiliza operaţia de adunare pentru a defini în $\mathbb{N}$ o altă lege de compoziţie – *înmulţirea numerelor naturale*.

Teorema 2.4. *Pe mulţimea numerelor naturale* $(\mathbb{N},0,(\,)')$ *se poate defini o unică lege de compoziţie*

$$\varphi:\mathbb{N}\times\mathbb{N}\to\mathbb{N}\ ,\ \varphi(m,n)=m\cdot n,$$

(notată multiplicativ şi numită ***înmulţire****) care satisface condiţiile:*

I_1) $m\cdot 0=0$ *pentru orice* $m\in\mathbb{N}$;

I_2) $m\cdot n'=mn+m$ *pentru orice* $m,n\in\mathbb{N}$.

*Demonstraţie***.** Fixăm elementul $m\in\mathbb{N}$ şi definim cu ajutorul lui aplicaţia $\lambda_m:\mathbb{N}\to\mathbb{N}$ prin regula

$$\lambda_m(n)\overset{def}{=}n+m$$

pentru orice $n \in \mathbb{N}$. Obținem tripletul $(\mathbb{N}, 0, \lambda_m)$. Din Teorema 1.1, p.2), rezultă că există o unică funcție $f_m : \mathbb{N} \to \mathbb{N}$ ce verifică condițiile

$$f_m(0) = 0, \quad f_m(n') = \lambda_m(f_m(m)) = f_m(n) + m$$

pentru orice $n \in \mathbb{N}$. Definim pentru orice $m, n \in \mathbb{N}$ operația înmulțirii prin regula:

$$m \cdot n \overset{def}{=} f_m(n). \tag{2}$$

Din definiție rezultă imediat:

$$m \cdot 0 = f_m(0) = 0,$$

$$m \cdot n' = f_m(n') = f_m(n) + m = m \cdot n + m,$$

adică sunt satisfăcute condițiile $I_1)$ şi $I_2)$.

Să arătăm unicitatea operației $\varphi = (\cdot)$, definite prin $\varphi(m, n) = f_m(n) = m \cdot n$. Presupunem că mai există o operație ψ ce verifică condițiile $I_1)$ şi $I_2)$. Atunci pentru orice $m \in \mathbb{N}$ avem funcția $g_m : \mathbb{N} \to \mathbb{N}$, unde $g_m(n) = \psi(m, n)$. Condițiile $I_1)$ şi $I_2)$ arată că g_m este o aplicație ca în Teorema 1.1, p.2), de aceea din unicitatea ei rezultă că $f_m = g_m$, de unde obținem $\varphi = \psi$. □

Condițiile $I_1)$ şi $I_2)$ se numesc *axiomele înmulțirii* în $\mathbb{N}$.

Trecând la cercetarea proprietăților acestei operații, mai întâi demonstrăm

Lema 2.5. *Înmulțirea numerelor naturale satisface condițiile:*

$I_1^0)$ $0 \cdot n = 0$ *pentru orice* $n \in \mathbb{N}$;

$I_2^0)$ $m' \cdot n = m \cdot n + n$ *pentru orice* $m, n \in \mathbb{N}$.

Demonstrație. $I_1^0)$ Notăm $P = \{n \in \mathbb{N} \mid 0 \cdot n = 0\}$. Din $I_1)$ pentru $m = 0$ avem $0 \cdot 0 = 0$, adică $0 \in P$. Dacă $n \in P$ atunci $0 \cdot n = 0$ şi

utilizând I_2) şi A_1), obţinem: $0 \cdot n' = 0 \cdot n + 0 = 0 + 0 = 0$, prin urmare, $n' \in P$. Axioma P_3) implică $P = \mathbb{N}$, deci are loc $I_1{}^0$).

$I_2{}^0$) Fixăm un număr natural $m \in \mathbb{N}$ şi notăm:

$$P = \{n \in \mathbb{N} \mid m' \cdot n = mn + n\}.$$

Din I_1) avem $m' \cdot 0 = 0$ şi $m \cdot 0 + 0 = 0 + 0 = 0$, de aceea $0 \in P$. Dacă $n \in P$, atunci $m'n = mn + n$ şi, cu ajutorul condiţiilor I_2) şi A_2), precum şi luând în considerare asociativitatea şi comutativitatea adunării, obţinem:

$$\begin{aligned} m'n' &= m'n + m' = (mn + n) + m' = \\ &= mn + (n + m') = mn + (n + m)' = \\ &= mn + (m + n)' = mn + (m + n') = \\ &= (mn + m) + n' = mn' + n', \end{aligned}$$

ceea ce arată că $n' \in P$. Din axioma P_3) rezultă $P = \mathbb{N}$, adică are loc $I_2{}^0$). □

Cu ajutorul acestei leme acum putem demonstra proprietăţile de bază ale operaţiei de înmulţire a numerelor naturale.

Teorema 2.6. *Înmulţirea numerelor naturale este distributivă în raport cu adunarea, este asociativă şi comutativă, iar numărul* $1 = 0'$ *este element neutru în raport cu această operaţie, adică:*

1) $m(n + p) = mn + mp$,

2) $(mn)p = m(np)$,

3) $mn = nm$,

4) $1 \cdot n = n \cdot 1 = n$,

pentru orice $m, n, p \in \mathbb{N}$.

*Demonstraţie***.** 1) Fixăm numerele $m, n \in \mathbb{N}$ şi considerăm mulţimea:

$$P = \{p \in \mathbb{N} \mid m(n + p) = mn + mp\}.$$

Din A_1) şi I_1) avem:

$$m(n+0)=mn, \quad mn+m\cdot 0=mn+0=mn,$$

de unde rezultă $0\in P$.

Dacă $p\in P$, atunci utilizând A_2), I_2) şi asociativitatea operației de adunare, obținem:

$$m(n+p')=m(n+p)'=m(n+p)+m=(mn+mp)+m=$$
$$=mn+(mp+m)=mn+mp',$$

de aceea $p'\in P$. Din axioma P_3) avem $P=\mathbb{N}$, deci are loc 1).

2) Fixăm numerele $m,n\in\mathbb{N}$ şi definim mulțimea

$$P=\{p\in\mathbb{N}\mid (mn)p=m(np)\}.$$

Din I_1) avem $(mn)0=0$ şi $m(n\cdot 0)=m\cdot 0=0$, de aceea $0\in P$.

Dacă $p\in P$, atunci $(mn)p=m(np)$ şi, utilizând I_2) şi distributivitatea înmulțirii în raport cu adunarea, obținem:

$$(mn)p'=(mn)p+mn=m(np)+mn=m(np+n)=m(np'),$$

deci $p'\in P$. Acum axioma P_3) arată că $P=\mathbb{N}$, adică are loc 2).

3) Fixăm $m\in\mathbb{N}$ şi notăm:

$$P=\{n\in\mathbb{N}\mid mn=nm\}.$$

Din I_1) şi $I_1^{\,0}$) avem $m\cdot 0=0=0\cdot m$, deci $0\in P$. Dacă $n\in P$, atunci $mn=nm$ şi din I_2) şi $I_2^{\,0}$) obținem:

$$mn'=mn+m=nm+m=n'm,$$

deci $n'\in P$. Din axioma P_3) rezultă $P=\mathbb{N}$, deci are loc 3).

4) Utilizând 3), I_2), I_1) şi $A_1^{\,0}$), avem:

$$1\cdot n=n\cdot 1=n\cdot 0'=n\cdot 0+n=0+n=n. \ \square$$

Finalizăm acest paragraf cu încă o serie de proprietăți utile ale operațiilor de adunare şi înmulțire ale numerelor naturale.

Propoziția 2.7. *Pentru orice numere naturale* $m,n,p\in\mathbb{N}$ *au loc afirmațiile:*

1) dacă $m+n=0$, *atunci* $m=0$ *şi* $n=0$;

2) *dacă* $m+n=m+p$, *atunci* $n=p$;

3) *dacă* $mn=0$, *atunci* $m=0$ *sau* $n=0$;

4) *dacă* $mn=mp$ *şi* $m\neq 0$, *atunci* $n=p$;

5) *dacă* $mn=1$, *atunci* $m=1$ *şi* $n=1$.

*Demonstraţie***.** 1) Fie $m+n=0$ şi $m\neq 0$. Atunci conform Teoremei 1.1, p.1), elementul m are predecesor, adică $m=u'$ pentru un element $u\in\mathbb{N}$. Prin urmare, din $A_2{}^0$) şi axioma P_1) avem:

$$m+n=u'+n=(u+n)'\neq 0,$$

contradicţie. Deci $m=0$ şi $n=0+n=m+n=0$.

2) Fie

$$P=\{m\in N \mid m+n=m+p \textit{ implică } n=p\}.$$

Evident, $0\in P$. Luăm un element arbitrar $m\in P$. Atunci relaţia $m+n=m+p$ implică $n=p$ şi dacă presupunem $m'+n=m'+p$, din $A_2{}^0$) obţinem $(m+n)'=(m+p)'$ şi axioma P_2) arată că în acest caz $m+n=m+p$. Conform ipotezei, aceasta implică $n=p$, prin urmare, $m'\in P$. Astfel putem aplica axioma P_3), din care avem $P=\mathbb{N}$, adică are loc 2).

3) Fie $mn=0$ şi $m\neq 0$. Atunci m are predecesor (Teorema 1.1, p.1)), adică $m=u'$ pentru un element $u\in\mathbb{N}$. Astfel avem:

$$0=mn=u'n=un+n$$

(folosind I_2)**),** iar din afirmaţia 1) a acestei propoziţii rezultă $n=0$.

4) Fie $0\neq m\in\mathbb{N}$ şi considerăm mulţimea:

$$P=\{n\in\mathbb{N} \mid mn=mp \textit{ implică } n=p\}.$$

Dacă $m\cdot 0=mp$, atunci $0=mp$ $(m\neq 0)$ şi din afirmaţia 3) rezultă $p=0$. Aceasta arată că $0\in P$.

Fie acum $n\in P$ şi să arătăm că $n'\in P$ (adică din $mn'=mq$ rezultă $n'=q$). Admitem că $mn'=mq$. Deoarece $m\neq 0$ şi $n'\neq 0$ (axioma P_1)), avem $mn'\neq 0$ conform afirmaţiei 3). Prin urmare,

$mq \neq 0$, deci $q \neq 0$. Atunci q are predecesor: $q = p'$, $p \in \mathbb{N}$. Din $mn' = mp'$, utilizând I_2), obținem

$$mn + m = mp + m,$$

deci $mn = mp$ (afirmația 2)). Deoarece $n \in P$, din ultima relație și din definiția lui P rezultă că $n = p$, prin urmare $n' = p' = q$. Astfel am arătat că relația $mn' = mq$ implică $n' = q$, ceea ce înseamnă că $n' \in P$ (dacă $n \in P$). Aceasta permite aplicarea axiomei P_3), obținând $P = \mathbb{N}$, adică are loc 4).

5) Fie $mn = 1$. Atunci din axioma P_1) avem $mn = 1 = 0' \neq 0$, de aceea $m \neq 0$ și $n \neq 0$. Prin urmare, m și n posedă predecesori: $m = u'$, $n = v'$, $u, v \in \mathbb{N}$. Atunci, utilizând I_2^0) și A_2), obținem:

$$0' = 1 = mn = u'n = un + n = un + v' = (un + v)'.$$

Acum din axioma P_2) avem $0 = un + v$ și, aplicând afirmațiile 1) și 3), obținem: $un = 0$ și $v = 0$. Deoarece $n \neq 0$, rezultă $u = 0$, prin urmare, $m = u' = 0' = 1$, $n = v' = 0' = 1$. □

§3. Relația de ordine pe mulțimea numerelor naturale. Operații parțiale pe $\mathbb{N}$: scăderea și împărțirea

Vom defini pe mulțimea numerelor naturale $\mathbb{N}$ o relație binară **„<”** (prin operația adunării) în felul următor:

Definiția 1. *Fie* $m, n \in \mathbb{N}$. *Spunem că* m *este* ***mai mic decât*** n *(și scriem* $m < n$*) dacă există un element* $u \in \mathbb{N}$, $u \neq 0$ *astfel încât* $m + u = n$.

Observații. a) Pentru orice $n \in \mathbb{N}$ avem (din A_1) și A_2)):

$$n' = (n + 0)' = n + 0' = n + 1,$$

unde $1 = 0' \neq 0$ (axioma P_1)), de aceea conform definiției avem $n < n'$.

b) Relaţia **„<”** este *tranzitivă*, deoarece $m<n,\ n<p$ implică existenţa numerelor naturale nenule u şi v, astfel încât $m+u=n$, $n+v=p$, deci $p=m+(u+v),\ u+v\neq 0$ şi $m<p$.

c) Pentru orice m natural nenul avem $1=m$ sau $1<m$. În adevăr, $m=u'=u+1$; dacă $u=0$, avem $m=1$, iar dacă $u\neq 0$, atunci $1<m$.

d) 0 este cel mai mic număr natural, deoarece $0<0'=1,\ 1<m$ pentru $m\neq 1$, deci $0<m$, pentru orice număr nenul $m\in\mathbb{N}$.

e) Pentru orice număr natural n, între n şi n' nu există numere naturale. Într-adevăr, dacă ar exista m cu $n<m<n'$, atunci am avea: $n+u=m,\ u\neq 0$ şi $m+v=n',\ v\neq 0$. În acest caz

$$n+u+v=n'=n+1,$$

adică $u+v=1$ (Propoziţia 2.7, p.2)). Din $v\neq 0$ rezultă că v are predecesor (Teorema 1.1, p.1)), adică $v=w'$ pentru un element $w\in\mathbb{N}$. Atunci

$$0'=1=u+v=u+w'=(u+w)',$$

de unde $0=u+w$ (axioma P_2)). Prin urmare, $u=0$ (Propoziţia 2.7, p.1)), contradicţie.

Proprietatea e) se exprimă spunând că $\mathbb{N}$ este o mulţime *discretă*.

Teorema 3.1 ***(legea trihotomiei)***. *Pentru orice două numere naturale $m,n\in\mathbb{N}$ este justă una din relaţiile următoare:*

$$m<n,\quad m=n,\quad n<m \tag{1}$$

şi numai una.

Demonstraţie. Să verificăm mai întâi că nu pot avea loc două dintre relaţiile indicate în (1).

a) Fie $m<n$ şi $m=n$. Din prima relaţie avem $m+u=n$ pentru un element $u\in\mathbb{N},\ u\neq 0$. Din egalităţile $m=n$ şi $m+u=n$ avem

$$m+u=m=m+0,$$

de aceea $u=0$ (Prop.2.7, p.2)), contradicţie.

b) În mod similar se arată că nu pot avea loc concomitent relațiile $m = n$ şi $n < m$.

c) Fie $m < n$ şi $n < m$. Din tranzitivitatea relației „<” rezultă $m < m$, contradicție.

Aşadar, numai una dintre relațiile (1) poate avea loc. Să arătăm că una din aceste relații întotdeauna are loc.

Fixăm un număr $m \in \mathbb{N}$ şi considerăm mulțimea P ce constă din acele numere $n \in \mathbb{N}$, pentru care între m şi n are loc una din relațiile indicate. Pentru $n = 0$ avem:

$n = m$ dacă $m = 0$;

$n < m$, dacă $m \neq 0$, deoarece 0 e cel mai mic număr natural.

Aceasta arată că $0 \in P$.

Fie $n \in P$. Atunci sunt posibile trei cazuri:

1) $m = n$; deci $m = n < n'$;

2) $m < n$; atunci $m + u = n$, $u \neq 0$, de aceea

$$m + u' = (m + u)' = n',$$

prin urmare, $m < n'$, deoarece $u' \neq 0$.

3) $n < m$; atunci $n + v = m$, $v \neq 0$, şi numărul v are predecesor: $v = w'$, $w \in \mathbb{N}$. Dacă $w = 0$, atunci

$$m = n + v = n + w' = n + 0' = n + 1 = n',$$

iar dacă $w \neq 0$, atunci

$$n' + w = n + w' = n + v = m,$$

prin urmare, $n' < m$.

Aşadar, în toate cazurile posibile între m şi n' are loc una dintre cele trei relații, de aceea $n' \in P$.

Acum putem aplica axioma P_3), din care rezultă că $P = \mathbb{N}$, ceea ce demonstrează teorema. □

Modificăm relația „<” prin următoarea definiție.

Definiția 2. *Vom spune că* m *este* ***mai mic sau egal cu*** n *(şi vom scrie* $m \leq n$*), dacă* $m < n$ *sau* $m = n$.

Din demonstrația legii trihotomiei rezultă că $n < m$ implică $n' \leq m$. Se verifică uşor faptul că relația binară „$\leq$" este o relație de ordine, adică este *reflexivă* $(n \leq n)$, *antisimetrică* $(m \leq n,\ n \leq m, \Rightarrow m = n)$ şi *tranzitivă* $(m \leq n, n \leq p \Rightarrow m \leq p)$. Astfel $(\mathbb{N},\ \leq)$ este o *mulțime parțial ordonată* şi „$\leq$" se numeşte **relație de ordine naturală** pe $\mathbb{N}$. Din teorema 3.1 rezultă că pentru orice două numere $m, n \in \mathbb{N}$ are loc $m \leq n$ sau $n \leq m$. Aceasta înseamnă că $(\mathbb{N},\ \leq)$ este o mulțime *total ordonată*.

Acum vom demonstra o proprietate importantă a relației de ordine pe $\mathbb{N}$ şi anume că orice submulțime nevidă A din $\mathbb{N}$ posedă margine inferioară exactă (adică există cel mai mic număr din A).

Teorema 3.2 ***(Principiul celui mai mic număr)***. *Dacă A este o mulțime nevidă de numere naturale, atunci există un singur număr $a \in A$, astfel încât $a \leq x$, pentru orice $x \in A$.*

Demonstrație. Având submulțimea $A \subseteq \mathbb{N}, A \neq \varnothing,$ definim

$$P = \{n \in \mathbb{N} \mid n \leq x \text{ pentru orice } x \in A\}.$$

Evident, $0 \in P$. Dacă am avea $n' \in P$ pentru orice $n \in P$, atunci din axioma P_3) ar rezulta $P = \mathbb{N}$, contradicție, deoarece dacă $b \in A \neq \varnothing$ atunci din $b' \in \mathbb{N} = P$ avem $b' \leq x$ pentru orice $x \in A$, în particular $b' \leq b$, ceea ce este imposibil.

Prin urmare, există un număr $c \in P$ astfel încât $c' \notin P$ .Să arătăm că $c' \in A$. Fie că $c' \notin A$, atunci din $c \in P$ avem $c \leq x$, pentru orice $x \in A$, prin urmare $c + u = x$, $u \neq 0$; dacă $u = v'$, atunci

$$x = c + u = c + v' = c' + v,$$

adică $c' \leq x$ pentru orice $x \in A$, deci $c' \in P$, contradicție.

Astfel rămâne că $c' \in A$ şi $c' \leq x$ pentru orice $x \in A$. Unicitatea celui mai mic element se demonstrează astfel: dacă avem două elemente $d, e \in A$ cu $d \leq x$ şi $e \leq x$, pentru orice $x \in A$, atunci în particular, $d \leq e$ şi $e \leq d$, deci din antisimetria relației „$\leq$" rezultă $e = d$. □

Propoziția 3.3. *Orice submulțime nevidă din* $\mathbb{N}$ *care este mărginită superior conține cel mai mare număr.*

Demonstrație. Fie $\varnothing \neq A \subseteq \mathbb{N}$ şi submulțimea A mărginită superior (adică există $k \in \mathbb{N}$ încât $a \leq k$ pentru orice $a \in A$). Considerăm submulțimea

$$B = \{b \in \mathbb{N} \mid b \geq a, \forall a \in A\}.$$

Deoarece A este mărginită superior, mulțimea B nu este vidă. Conform teoremei 3.2, mulțimea B posedă cel mai mic număr, fie acesta $c \in B$. Prin definiție, $c \geq x$ pentru orice $x \in A$. Să arătăm că $c \in A$ şi, prin urmare, c este cel mai mare element din A.

Fie $c \notin A$. Atunci $c > a$ pentru orice $a \in A$. Notăm cu d predecesorul lui c (el există, deoarece $A \neq \varnothing$). Atunci $d \geq a$ (vezi observația a)), pentru orice $a \in A$, deci $d \in B$, contradicție cu alegerea lui c. □

Să clarificăm acum comportamentul relației de ordine naturală în $\mathbb{N}$ față de operațiile de adunare şi înmulțire.

Propoziția 3.4. *Relația de ordine naturală pe* $\mathbb{N}$ *este compatibilă cu adunarea şi înmulțirea numerelor naturale, adică:*

1) dacă $m < n$ *atunci* $m + p < n + p$ *pentru orice* $p \in \mathbb{N}$;

2) dacă $m < n$ *atunci* $mp < np$ *pentru orice* $p \in \mathbb{N}$, $p \neq 0$.

Demonstrație. 1) Dacă $m < n$ atunci $m + u = n$, $u \neq 0$, deci $(m + p) + u = n + p$ prin urmare, $m + p < n + p$.

2) Dacă $m < n$ atunci $m + u = n$, $u \neq 0$, deci $mp + up = np$ şi din $p \neq 0$ avem $up \neq 0$ (Propoziția 2.7, p.3)), prin urmare, $mp < np$. □

Din afirmația 2), în particular, rezultă că $m \leq mn$ pentru $n \neq 0$.

Să formulăm şi să demonstrăm un rezultat important care va avea loc şi în alte sisteme numerice, ce vor fi cercetate în cele ce urmează. Convenim, în prealabil, să notăm $m \geq n$ dacă şi numai

dacă $n \le m$. Se observă că $n > m$, $n = u' \Rightarrow u \ge m$. Într-adevăr, dacă am avea $u < m$, atunci $u' \le m$ şi $n \le m$. Contradicție cu legea trihotomiei.

Lema 3.5 (***lema lui Arhimede***). *Fie* $n \in \mathbb{N}$, $n \neq 0$. *Atunci pentru orice* $m \in \mathbb{N}$ *există un număr* $t \in \mathbb{N}$ *astfel încât* $tn > m$.

Demonstrație. Fixăm un număr $n \in \mathbb{N}$, $n \neq 0$ şi fie $m \in \mathbb{N}$. Deoarece $mn \ge m$ (vezi p.27), luând $t = m'$, avem

$$tn = m'n \overset{I_2^0}{=} mn + n > mn \ge m,$$

de aceea $tn > m$. □

Teorema 3.6 ***(teorema împărțirii cu rest în*** $\mathbb{N}$*)*. *Fie* $0 \neq n \in \mathbb{N}$. *Atunci pentru orice număr* $m \in \mathbb{N}$ *există şi sunt unice numerele* $q, r \in \mathbb{N}$ *astfel încât* $m = nq + r, r < n$.

Demonstrație. Fixăm numărul $n \in \mathbb{N}^*$ şi considerăm submulțimea:

$$P = \{m \in \mathbb{N} \mid \text{există } q, r \in \mathbb{N} \text{ astfel încât } m = nq + r,\ r < n\}.$$

Pentru $m = 0$ avem $0 = n \cdot 0 + 0$, $0 < n$, de aceea $0 \in P$.

Fie $m \in P$ şi verificăm faptul că $m' \in P$. Avem:

$$m' = m + 1 = (nq + r) + 1,\ r < n, \Rightarrow m' = nq + (r + 1),\ r + 1 \le n.$$

Dacă $r + 1 = n$, atunci punem $r^* = 0, q^* = q + 1$; dacă $r + 1 < n$, atunci notăm $q^* = q, r^* = r + 1$. În ambele cazuri avem

$$m' = nq^* + r^*,\quad r^* < n.$$

Astfel din $m \in P$ rezultă $m' \in P$ şi avem dreptul să aplicăm axioma P_3), din care rezultă că $P = \mathbb{N}$, ceea ce demonstrează existența descompunerii din teoremă.

Să arătăm acum unicitatea ei. Fie:

$$m = nq_1 + r_1,\quad r_1 < n;$$
$$m = nq_2 + r_2,\quad r_2 < n.$$

Dacă $q_1 < q_2$, atunci $q_1 + u = q_2, u \neq 0$, deci

$$nq_1 + r_1 = m = nq_2 + r_2 = n(q_1 + u) + r_2 = nq_1 + nu + r_2,$$

prin urmare,

$$r_1 = nu + r_2 \geq nu \geq n \quad (u \neq 0),$$

contradicție cu $r_1 < n$. În mod simetric se arată că nu poate avea loc relația $q_2 < q_1$. Din legea trihotomiei (Teorema 3.1) rezultă $q_1 = q_2$. Atunci din relațiile de descompunere imediat avem $r_1 = r_2$. □

Acum vom cerceta operațiile inverse adunării şi înmulțirii în mulțimea numerelor naturale $\mathbb{N}$.

Definiția 3. *Fie* $m, n \in \mathbb{N}$. *Vom numi* ***diferență*** *a numărului* m *prin* n *un număr* $x \in \mathbb{N}$ *astfel încât* $m = n + x$. *Se notează:* $x = m - n$.

Propoziția 3.7. *Diferența* $m - n$ *există dacă şi numai dacă* $n \leq m$. *În acest caz numărul* $x = m - n$ *este unic determinat*.

Demonstrație. Dacă există numărul $x = m - n$ atunci prin definiție $m = n + x$, prin urmare $n \leq m$ (definiția 2). Reciproc, dacă $n \leq m$, atunci conform definiției 2, există $x \in \mathbb{N}$ încât $n + x = m$, adică $x = m - n$ (definiția 3).

Dacă $m = n + x_1$ şi $m = n + x_2$, atunci $n + x_1 = n + x_2$ şi din Propoziția 2.7, p.2), avem $x_1 = x_2$, ceea ce arată unicitatea diferenței $m - n$. □

Astfel obținem pe $\mathbb{N}$ o operație parțială – *scăderea* numerelor naturale. În continuare, când scriem $m - n$, presupunem că $n \leq m$.

Propoziția 3.8. *Operația de scădere a numerelor naturale posedă proprietățile:*

1) $(m - n)p = mp - np$;

2) $m - n = p - q$ *dacă şi numai dacă* $m + q = n + p$;

3) $(m-n)+(p-q)=(m+p)-(n+q)$;

4) $(m-n)-(p-q)=(m+q)-(n+p)$;

5) $(m-n)(p-q)=(mp+nq)-(np+mq)$.

Demonstrație. 1) Prin definiție $m=(m-n)+n$ şi, înmulțind cu p, obținem

$$mp=(m-n)p+np$$

de unde, aplicând definiția scăderii, avem

$$(m-n)p=mp-np.$$

La fel de simplu se verifică celelalte afirmații, demonstrațiile cărora se propun ca exercițiu. □

Definiția 4. *Fie* $m,n\in\mathbb{N},\ n\neq 0$. *Vom numi* ***cât*** *al numărului* m *prin* n *un număr* $x\in\mathbb{N}$ *astfel încât* $nx=m$. *Se notează:* $x=\frac{m}{n}$. *În acest caz vom mai spune că* a ***se împarte la*** b, a ***se divide cu*** b *sau* a ***este divizibil cu*** b.

Propoziția 3.9. *Pentru existența câtului* $\frac{m}{n}$ $(n\neq 0)$ *este necesar (dar nu şi suficient) ca* $n\le m$. *Dacă câtul* $\frac{m}{n}$ *există, atunci el este unic.*

Demonstrație. Dacă câtul $\frac{m}{n}$ există, atunci $n\le m$, deoarece în caz contrar $m<n$ şi $\frac{m}{n}\cdot m<\frac{m}{n}\cdot n=m$, contradicție. Dacă $m=nx_1$ şi $m=nx_2$, atunci $nx_1=nx_2$ $(n\neq 0)$, deci $x_1=x_2$ (Propoziția 2.7, p.4)), prin urmare câtul este unic. □

Am obținut o operație parțială în $\mathbb{N}$, inversă înmulțirii, care se numeşte *împărțirea numerelor naturale*.

Propoziția 3.10. *Operația împărțirii numerelor naturale posedă următoarele proprietăți:*

1) $\frac{m}{n} \le m$;

2) $\frac{m}{n} = 1 \Leftrightarrow m = n$;

3) $\frac{m}{n} = m \Leftrightarrow n = 1$;

4) $\frac{m}{n} < \frac{m}{p} \Leftrightarrow p < n$;

5) $\frac{m}{n} = \frac{m}{p} \Leftrightarrow n = p$;

6) $\frac{m}{n} = \frac{p}{q} \Leftrightarrow mq = np$.

7) Pentru orice număr natural $m > 1$*, nu există câtul succesorului său* m' *cu* m.

Demonstrația se reduce la verificare directă şi o lăsăm ca exercițiu. □

Exerciții

1. Demonstrați că mulțimea numerelor naturale nu conține cel mai mare număr.
2. Demonstrați că pentru orice număr natural n sunt adevărate egalitățile: a) $n' - 1 = n$; b) $n' - n = 1$.
3. Demonstrați următoarele proprietăți ale operației de scădere a numerelor naturale:

a) dacă $a = b$ şi $b > c$, atunci $a - c = b - c$;

b) dacă $a > b$ şi $b > c$, atunci $a - c > b - c$;

c) dacă $a > b$, atunci $a - b = (a + c) - (b + c)$, $\forall c \in \mathbb{N}$;

d) dacă $a > b > c$, atunci $a - b = a - c - (b - c)$;

e) dacă $n > m'$, atunci $a - m' = (a - m) - 1$, $\forall a \in \mathbb{N}$;

f) dacă $a > b + c + d$, atunci $a - (b + c + d) = [(a - b) - c] - d$;

g) dacă $a > c$ şi $b > d$, atunci $(a + b) - (c + d) = (a - c) + (b - d)$.

4. Demonstrați următoarele proprietăți ale împărțirii numerelor naturale:

a) dacă $a = b$ şi b este divizibil cu c, atunci câtul de la împărțirea lui a la c coincide cu câtul de la împărțirea lui b la c;

b) dacă numerele a şi b sunt divizibile cu c şi $a > b$, atunci $\frac{a}{c} > \frac{b}{c}$;

$\frac{a-b}{c} = \frac{a}{c} - \frac{b}{c}$;

c) dacă $a > b$, $c > d$, a este divizibil cu d şi b este divizibil cu c, atunci $\frac{a}{d} > \frac{b}{c}$;

5. Demonstrați că orice număr natural nenul divizibil cu 4 este sumă a două numere naturale impare consecutive.
6. Fie a un număr natural nenul. Ce numere naturale, fiind împărțite cu a, dau câtul egal cu restul?
7. Demonstrați proprietățile scăderii numerelor naturale, date în Propoziția 3.8, p.2-5;
8. Demonstrați proprietățile împărțirii numerelor naturale, date în Propoziția 3.10.
9. Fie ca la împărțirea numerelor naturale $a_1, a_2, \ldots, a_k$ la 9 obțin resturile $r_1, r_2, \ldots, r_k$, respectiv. Demonstrați că

a) la împărțirea sumei $a_1 + a_2 + \ldots + a_k$ la 9 se va obține acelaşi rest ca şi la împărțirea sumei $r_1 + r_2 + \ldots + r_k$;

b) la împărțirea produsului $a_1 a_2 \ldots a_k$ la 9 se va obține acelaşi rest ca şi la împărțirea produsului $r_1 r_2 \ldots r_k$.

Demonstrați că această afirmație este adevărată nu numai pentru numărul 9, dar şi pentru orice număr natural $n > 1$.

10. Dacă r este restul de la împărțirea numărului a la b, atunci la împărțirea puterii a^n la b se obține acelaşi rest ca şi la împărțirea puterii r^n la b. Demonstrați.

§4. Asupra proprietăților sistemului de axiome Peano

În paragrafele precedente a fost efectuată o încercare de a construi axiomatic numerele naturale, luând drept bază axiomele lui Peano. Acum vom arăta unele proprietăți ale acestui sistem de axiome.

În orice teorie abstractă construită în mod formal pe baza unui sistem de axiome apar în mod firesc trei întrebări fundamentale, referitoare la sistemul dat de axiome:

1) *compatibilitatea*,
2) *completitudinea*,
3) *independența*

axiomelor sistemului.

În continuare vom explica sensul fiecărei din aceste cerințe asupra unui sistem de axiome, verificând condițiile respective pentru cazul concret al sistemului de axiome Peano. Pentru comoditate în cazul independenței vom utiliza axiomele Peano, formulate în definiția 2 din §1, mai exact vom considera sistemul de axiome I, II, III şi IV* din §1.

1. *Compatibilitatea* unui sistem de axiome înseamnă că sistemul dat este necontradictoriu, adică pe baza lui nu se poate demonstra atât o afirmație A cât şi negația ei $\overline{A}$. Una din metodele de verificare a compatibilității unui sistem de axiome constă în construirea aşa numitelor *interpretări* (sau *modele*) ale sistemului dat. Se numeşte interpretare a unui sistem de axiome o mulțime concretă pentru elementele căreia sunt definite relațiile de bază şi sunt satisfăcute axiomele teoriei axiomatice date. Sistemul dat de axiome se spune că este compatibil (sau necontradictoriu) dacă pentru el există cel puțin o interpretare.

Pentru sistemul de axiome Peano existența interpretării rezultă din propoziția 1.3. Dacă acceptăm axioma infinitului, atunci din orice mulțime infinită A se poate obține un sistem Peano $(N, 0, f|_N)$. În toate sistemele de axiome ale teoriei mulțimilor

există sau axioma infinitului în mod direct, sau o afirmație din care aceasta rezultă.

Concluzia 1. *Vom lua în calitate de afirmație fundamentală axioma infinitului care ne asigură existența sistemului de numere naturale. Deci sistemul de axiome Peano în acest caz este compatibil.*

Pentru toate celelalte sisteme numerice, care vor fi cercetate în viitor, vom demonstra existența lor prin construirea unei interpretări a sistemului respectiv. De fiecare dată demonstrația se bazează pe *existența* sistemului numeric precedent şi se arată metoda de construire a noului sistem numeric.

2. *Completitudinea* unui sistem de axiome se înțelege în sensul că oricare două interpretări ale lui sunt izomorfe. Aceasta înseamnă că dacă M şi M' sunt două interpretări ale aceluiaşi sistem de axiome, atunci există o bijecție $M \cong M'$, care păstrează toate relațiile din sistemul de axiome analizat. Astfel completitudinea în acest sens se reduce la *unicitatea* interpretării (abstracție făcând de izomorfism).

Pentru cazul sistemului de axiome Peano în calitate de interpretare se poate lua orice sistem Peano $(N, 0, s)$ (vezi §1, definiția 1). În §1 (Corolarul 1.2) s-a arătat că orice două sisteme Peano sunt izomorfe, deci putem formula

Concluzia 2. *Sistemul de axiome Peano este complet.*

Este evident faptul că nu orice sistem de axiome are această proprietate excelentă. De exemplu, sistemele de axiome ce definesc grupurile, inelele, spațiile vectoriale şi alte sisteme algebrice, nu sunt complete (spre norocul nostru), deoarece există sisteme algebrice neizomorfe.

Pentru sistemele numerice, care vor fi cercetate în continuare, completitudinea se înțelege ca unicitate a sistemului nou (până la un

izomorfism) şi se demonstrează utilizând unicitatea sistemului numeric precedent.

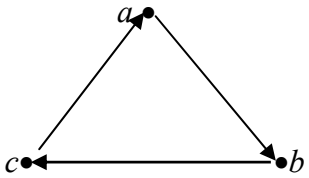
3. *Independența* sistemului de axiome înseamnă minimalitatea lui în sensul că *nici una din axiomele acestui sistem nu poate fi dedusă din celelalte* (altfel ea ar putea fi eliminată fără daune pentru teoria construită pe baza sistemului dat de axiome). Aşadar, independența este o cerință de economie şi minimalitate şi se referă mai mult la aspectul estetic.

Demonstrarea independenței unui sistem de axiome se efectuează astfel: pentru fiecare axiomă se construieşte o interpretare astfel încât sunt satisfăcute toate celelalte axiome ale sistemului dat, cu excepția celei cercetate. Dacă axioma dată ar fi o consecință a celorlalte, atunci o astfel de interpretare ar fi imposibilă.

Să realizăm această metodă de demonstrare a independenței axiomelor pentru sistemul de axiome Peano (utilizând sistemul de axiome I, II, III, IV* din definiția 2, §1).

a) *Independența axiomei I*:

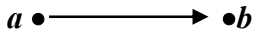
Fie $N = \{a, b, c\}$, $a' = b$, $b' = c$, $c' = a$.



Observăm că mulțimea N cu relația $(\,)'$ nu are element inițial (axioma I): orice element este succesorul altui element din N. Pe de altă parte, axiomele II, III şi IV* sunt în mod evident satisfăcute.

b) *Independența axiomei II*:

Fie $N = \{a, b\}$, $a' = b$.



Elementul b nu are succesor, deci axioma II nu are loc. În mod evident, axiomele I, III şi IV* sunt satisfăcute.

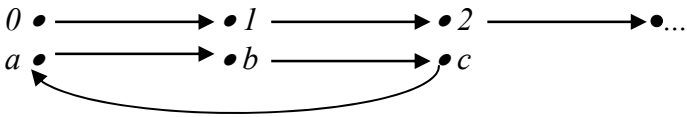
c) *Independența axiomei III*:

Fie $N = \{a, b, c, d\}$, $a' = b$, $b' = c$, $c' = d$, $d' = b$.

Elementul b succede atât lui a cât şi lui d, de aceea axioma III nu are loc. Pe de altă parte, N are element inițial, orice element are succesor unic şi are loc axioma inducției, deci axiomele I, II, IV* sunt satisfăcute.

d) *Independența axiomei IV*:*

Fie $M = \{0, 1, 2, ..., n, n+1, ...\} \cup \{a, b, c\} = \mathbb{N} \cup \{a, b, c\}$,



cu relația obişnuită de ordine naturală pe $\mathbb{N}$. Aici există un element inițial (ce nu succede nici unui element), numărul 0; orice element are succesor (unic) şi dacă are predecesor, atunci el este unic. Astfel sunt satisfăcute axiomele I, II şi III. Dar axioma IV* nu este satisfăcută deoarece $\mathbb{N} \subseteq M$ şi verifică condițiile

A) $0 \in M$;

B) $m \in \mathbb{N}$ implică $m' \in \mathbb{N}$, însă $M \neq \mathbb{N}$.

Astfel, din cele arătate mai sus se poate deduce

Concluzia 3. *Sistemul de axiome Peano I, II, III, IV* (§1, definiția 2) este independent.*

Pentru fiecare dintre celelalte sisteme numerice care vor fi cercetate vom demonstra *existența* (compatibilitatea) și *unicitatea* (completitudinea). Cât privește independența sistemului de axiome, aceasta nu este o problemă principială (și deseori nici nu se cere din considerente de comoditate), de aceea nu va fi cercetată.

Exerciții

1. Să se arate echivalența definițiilor 1 și 2.
2. Să se formuleze și să se demonstreze principiul inducției matematice (în diverse forme).
3. Să se demonstreze propoziția 3.10 și afirmațiile 2)–5) din propoziția 3.8.
4. Utilizând inducția matematică,

a) demonstrați egalitățile:

1) $1+3+5+\ldots+2n-1=n^2$;

2) $1^2+2^2+3^2+\ldots+n^2=\dfrac{n(n+1)(2n+1)}{6}$;

3) $1^2+3^2+5^2+\ldots+(2n-1)^2=\dfrac{n(2n-1)(2n+1)}{3}$;

4) $1^3+2^3+3^3+\ldots+n^3=(1+2+3+\ldots+n)^2$;

5) $1\cdot 2+2\cdot 3+3\cdot 4+\ldots+n\cdot(n+1)=\dfrac{n(n+1)(n+2)}{3}$;

6) $1\cdot 2\cdot 3+2\cdot 3\cdot 4+\ldots+n(n+1)(n+2)=\dfrac{n(n+1)(n+2)(n+3)}{4}$;

7) $1\cdot 2\cdot\ldots\cdot k+2\cdot 3\cdot\ldots(k+1)+\ldots+n(n+1)\ldots(n+k-1)=$
$=\dfrac{n(n+1)\ldots(n+k)}{k+1}$, pentru orice $k\in\mathbb{N}$, $k\geq 2$;

8) $1\cdot 1!+2\cdot 2!+3\cdot 3!+\ldots+n\cdot n!=(n+1)!-1$,

b) demonstrați inegalitățile:

1) $2^n > 2n+1, \quad n \geq 3$;

2) $2^n > n^2, \quad n \geq 5$;

3) $2^n > n^3, \quad n \geq 10$;

4) $(n!)^2 \geq n^n, \quad n \geq 1$;

5) $n! > 2^n, \quad n \geq 2$.

c) demonstrați afirmațiile:

1) $7^{n+2} + 8^{2n+1}$ se divide cu 57;

2) $2^{n+2} \cdot 3^n + 5n - 4$ se divide cu 25;

3) $n^{n+2} + 12^{2n+1}$ se divide cu 133, pentru orice $n \geq 1$;

4) $6^{2n} + 3^{n+2} + 3^n$ se divide cu 11;

5) $3^{2n+2} \cdot 5^{2n} - 3^{3n+2} \cdot 2^{2n}$ se divide cu 1053;

6) $20^n + 16^n - 3^n - 1$ se divide cu 323, pentru orice $n \in \mathbb{N} \setminus \{1\}$.

5. Să se arate că:

a) pentru orice $p > 3$ prim și n natural, numărul $n^p - n$ se divide cu $6p$;

b) toți coeficienții descompunerii $(a+b)^n$ sunt impari dacă și numai dacă $n = 2^m - 1$;

c) numerele $sn+1$ și $(s+1)n+1$ sunt prime între ele;

d) dacă $(a,b) = 1$, atunci $(a+b, ab) = 1$, $(a+b, a^2 + ab + b^2) = 1$, $(a+b, a-b) = 1$ sau 2;

e) dacă $2^n + 1$ este un număr prim atunci n este o putere a numărului 2;

f) pentru orice număr natural m există m numere naturale consecutive compuse;

g) pentru orice număr natural m există m numere naturale impare consecutive compuse;

h) suma pătratelor oricăror trei numere prime mai mari decât 3 este un număr compus.

Capitolul II

Numere întregi

§5. Inelul numerelor întregi (unicitatea şi existența)

Cercetând mulțimea numerelor naturale $\mathbb{N}$ (§1–4) am observat pe lângă multe proprietăți excelente şi unele „defecte" ale acestui sistem numeric, în particular, faptul că operațiile scăderii şi împărțirii nu întotdeauna au loc, de exemplu, diferența $m-n$ există numai atunci când $m \geq n$ (Propoziția 3.7).

Numerele naturale nu sunt suficiente pentru a măsura mărimi care variază în două sensuri opuse. Iată câteva din ele.

a) Inginerii, fizicienii, astronomii, medicii măsoară temperaturi care variază în două sensuri opuse.

b) Geologii şi geografii măsoară înălțimile neregularităților terenurilor, dar şi adâncurile apelor, luând drept origine nivelul mediu al mărilor.

c) Geografii, marinarii şi cartografii caracterizează latitudinea şi longitudinea localităților.

d) Arheologii şi istoricii caracterizează scara vremii, începând de la un eveniment cunoscut.

e) Fizicienii şi chimiştii au observat două tipuri de încărcături electrice.

Acestea şi alte probleme au creat necesitatea extinderii sistemului numerelor naturale. Pentru rezolvarea ei să amintim mai întâi una din noțiunile de bază ale algebrei – cea de inel.

Definiția 1. *Mulțimea nevidă R pe care sunt definite două operații algebrice „$+$" şi „$\bullet$" se numeşte* ***inel*** *dacă:*

1) $R(+)$ este un grup abelian, adică operația „$+$" este asociativă şi comutativă, posedă element neutru $0 \in R$ $(0+r=r, \forall r \in R)$ şi orice $r \in R$ posedă element opus $(-r)$: $r+(-r)=0$.

2) Operația $(\cdot)$ *este distributivă la dreapta şi la stânga în raport cu „+”.*

Vom nota inelul definit mai sus cu $R(+,\cdot)$ sau, simplu, cu R. Un inel $R(+,\cdot)$ se numeşte *comutativ* (respectiv, *asociativ*) dacă înmulțirea $(\cdot)$ este comutativă (asociativă). Dacă in inelul $R(+,\cdot)$ înmulțirea $(\cdot)$ posedă elementul neutru e, atunci spunem ca $R(+,\cdot)$ este un inel cu elementul unitate e.

In continuare, în lucrarea data vom considera doar inele asociative, omițând cuvântul „asociativ”.

Este evident că în orice inel $R(+,\cdot)$ este definită operația inversă adunării – scăderea:

$$r_1 - r_2 = r_1 + (-r_2).$$

Observăm că $(\mathbb{N},+,\cdot)$ nu este un inel: din cerințele definiției lipseşte doar una singură – nu orice element din $\mathbb{N}$ posedă element opus (aceasta este echivalent cu faptul că nu întotdeauna există diferența a două numere). De aceea uneori $\mathbb{N}(+,\cdot)$ se numeşte *semiinel*.

Acum introducem noțiunea de bază a acestui paragraf – cea de sistem de numere întregi, care este şi una dintre noțiunile importante în întreaga matematică. În acest context L.Kronecker (1823–1891) spunea: „Dumnezeu a creat numerele întregi, toate celelalte în matematică sunt făcute de oameni”.

Definiția 2. ***Sistem de numere întregi*** $\mathbb{Z}$ *se numeşte un inel minimal (în raport cu incluziunea) ce conține semiinelul numerelor naturale* $\mathbb{N}$, *adică:*

1) $\mathbb{Z}$ *este un inel ce conține* $\mathbb{N}$;

2) operațiile din $\mathbb{Z}$ *coincid cu cele din* $\mathbb{N}$ *pentru numerele naturale;*

3) $\mathbb{Z}$ *este minimal (în raport cu incluziunea) printre inelele cu condițiile* 1) *şi* 2).

Cerinţele formulate în definiţiile 1 şi 2 constituie sistemul de axiome ce definesc numerele întregi.

Pentru cele ce urmează este comod de exprimat condiţia minimalităţii din definiţia 2 în altă formă, cum arată

Lema 5.1. *Fie R un inel arbitrar ce conţine $\mathbb{N}$. Inelul R este minimal printre inelele ce conţin $\mathbb{N}$ dacă şi numai dacă orice element din R are forma $m-n$, unde $m,n\in\mathbb{N}$ şi „–” este scăderea din inelul R.*

Demonstraţie. ($\Rightarrow$) Fie R un inel minimal ce conţine $\mathbb{N}$. Considerăm în R submulţimea:

$$R'=\{x\in R \mid x=m-n;\, m,n\in\mathbb{N}\}.$$

Se observă imediat că mulţimea R' este închisă în raport cu operaţiile „$+$” şi „$\cdot$” din R, adică R' formează un subinel în R. Mai mult, $R'\supseteq\mathbb{N}$ (orice $n\in\mathbb{N}$ are forma $n-0\in R'$). Din faptul că R este minimal rezultă $R=R'$, adică orice element din R are forma $m-n$, unde $m,\ n\in\mathbb{N}$.

($\Leftarrow$) Fie $R\supseteq\mathbb{N}$ şi orice element din R are forma $m-n$, unde $m,n\in\mathbb{N}$. Dacă R' este un subinel în R, ce conţine $\mathbb{N}$, atunci conform definiţiei inelului, R' este obligat să conţină şi toate elementele de forma $m-n$, pentru $m,n\in\mathbb{N}$, deci $R'=R$. Aceasta arată că inelul R este minimal. □

Uşor se observă că reprezentarea $x=m-n$ nu este unică şi $m-n=m_1-n_1$ dacă şi numai dacă $m+n_1=m_1+n$.

Lema 5.1 are misiunea de a ne ajuta să demonstrăm *unicitatea* sistemului de numere întregi $\mathbb{Z}$. Ca de obicei, unicitatea se înţelege până la un izomorfism (în cazul dat, a unui izomorfism de inele). Să amintim că aplicaţia $f:R\to S$ dintre două inele se numeşte *izomorfism de inele* dacă:

a) f este o bijecţie (corespondenţă bijectivă);

b) f păstrează cele două operaţii ale inelului în următorul sens:

$$f(x+y)=f(x)+f(y),\quad f(xy)=f(x)f(y),$$

pentru orice $x,y\in R$. Se notează: $R\cong S$.

Teorema 5.2 (***unicitatea inelului numerelor întregi*** $\mathbb{Z}$). *Dacă* $\mathbb{Z}_1$ *şi* $\mathbb{Z}_2$ *sunt două sisteme de numere întregi, atunci aceste inele sunt izomorfe:* $\mathbb{Z}_1\cong\mathbb{Z}_2$.

Demonstraţie. Fie $\mathbb{N}_1\subseteq\mathbb{Z}_1$ şi $\mathbb{N}_2\subseteq\mathbb{Z}_2$ unde $\mathbb{N}_1$ şi $\mathbb{N}_2$ sunt sisteme de numere naturale. Din unicitatea sistemului de numere naturale (vezi Teorema 1.1, p.3)) rezultă existenţa unei bijecţii $\varphi:\mathbb{N}_1\to\mathbb{N}_2$ ce păstrează relaţiile respective, de unde rezultă că φ păstrează şi operaţiile de adunare şi înmulţire. Să arătăm că bijecţia φ poate fi prelungită până la un izomorfism de inele $\overline{\varphi}:\mathbb{Z}_1\to\mathbb{Z}_2$. Orice element $x\in\mathbb{Z}_1$, conform Lemei 5.1, poate fi reprezentat în forma $x=m-n,$ unde $m,n\in\mathbb{N}_1$. Definim aplicaţia $\overline{\varphi}:\mathbb{Z}_1\to\mathbb{Z}_2$ astfel:

$$\overline{\varphi}(x)=\overline{\varphi}(m-n)\overset{def}{=}\varphi(m)-\varphi(n),\qquad(1)$$

unde scăderea a doua se efectuează în inelul $\mathbb{Z}_2$. Definiţia este corectă, adică rezultatul nu depinde de reprezentarea elementului în forma $m-n$ (această reprezentare nu este unică). Într-adevăr, dacă avem altă reprezentare $x=m_1-n_1$ a aceluiaşi element $x\in\mathbb{Z}_1$, atunci:

$$\begin{aligned}
m-n=m_1-n_1 \quad&\Rightarrow\\
m+n_1=m_1+n \quad&\Rightarrow\\
\varphi(m+n_1)=\varphi(m_1+n) \quad&\Rightarrow\\
\varphi(m)+\varphi(n_1)=\varphi(m_1)+\varphi(n) \quad&\Rightarrow\\
\varphi(m)-\varphi(n)=\varphi(m_1)-\varphi(n_1).&
\end{aligned}$$

Se vede imediat că aplicaţia $\overline{\varphi}$ este o prelungire a aplicaţiei φ: dacă $n\in\mathbb{N}_1,$ atunci $n=n-0$ şi conform definiţiei (1) avem:

$$\overline{\varphi}(n) = \overline{\varphi}(n-0) = \varphi(n) - \varphi(0) = \varphi(n) - 0 = \varphi(n).$$

Să verificăm dacă aplicația $\overline{\varphi}$ este bijectivă.

a) Dacă $x, y \in \mathbb{Z}_1$ şi $\overline{\varphi}(x) = \overline{\varphi}(y)$ atunci, luând reprezentările $x = m - n$ şi $y = k - l,$ obținem

$$\begin{aligned} &\overline{\varphi}(m-n) = \overline{\varphi}(k-l) \quad \Rightarrow \\ &\varphi(m) - \varphi(n) = \varphi(k) - \varphi(l) \quad \Rightarrow \\ &\varphi(m) + \varphi(l) = \varphi(k) + \varphi(n) \quad \Rightarrow \\ &\varphi(m+l) = \varphi(k+n). \end{aligned}$$

Deoarece φ este aplicație injectivă, avem $m + l = k + n,$ prin urmare $m - n = k - l$, adică $x = y$. Astfel am arătat că $\overline{\varphi}$ este o *aplicație injectivă*.

b) Fie z un element arbitrar din $\mathbb{Z}_2$ şi $z = s - t$, unde $s, t \in \mathbb{N}_2$ (Lema 5.1). Notăm $m = \varphi^{-1}(s), n = \varphi^{-1}(t) \in \mathbb{N}_1$ (amintim că φ este o bijecție). Considerăm elementul $x = m - n \in \mathbb{Z}_1$, pentru care avem:

$$\overline{\varphi}(x) = \overline{\varphi}(m-n) \overset{(1)}{=} \varphi(m) - \varphi(n) = s - t = z.$$

Astfel orice element din $\mathbb{Z}_2$ are imagine inversă în $\mathbb{Z}_1$, adică $\overline{\varphi}$ este o *aplicație surjectivă*. Din a) şi b) rezultă că $\overline{\varphi}$ este o bijecție. Rămâne de arătat că $\overline{\varphi}$ păstrează operațiile adunării şi înmulțirii. Fie $x, y \in \mathbb{Z}_1$ şi $x = m - n,\ y = k - l,$ unde $m, n, k, l \in \mathbb{N}_1$. Atunci:

$$\begin{aligned} &\overline{\varphi}(x+y) = \overline{\varphi}((m-n)+(k-l)) = \overline{\varphi}((m+k)-(n+l)) \overset{(1)}{=} \\ &= \varphi(m+k) - \varphi(n+l) = \varphi(m) + \varphi(k) - \varphi(n) - \varphi(l); \\ &\overline{\varphi}(x) + \overline{\varphi}(y) = \overline{\varphi}(m-n) + \overline{\varphi}(k-l) \overset{(1)}{=} \\ &= \varphi(m) - \varphi(n) + \varphi(k) - \varphi(l). \end{aligned}$$

Comparând rezultatele, vedem că $\overline{\varphi}$ păstrează adunarea. În mod similar se arată că $\overline{\varphi}$ păstrează şi operația înmulțirii. Din cele demonstrate mai sus rezultă că $\overline{\varphi}$ este un izomorfism de inele, ceea

ce arată unicitatea inelului numerelor întregi (abstracție făcând de izomorfism). □

Conform celor expuse în §4, unicitatea inelului $\mathbb{Z}$ arată că sistemul de axiome ce defineşte acest inel (vezi definiția 2) este *complet*.

Următoarea întrebare principială este *compatibilitatea* sistemului de axiome care se reduce la existența interpretării lui (vezi § 4). În continuare demonstrăm *existența* sistemului de numere întregi $\mathbb{Z}$, arătând cum poate fi el construit pe baza sistemului de numere naturale $\mathbb{N}$. Pentru aceasta sunt necesare următoarele două observații.

Observația 1. Incluziunea $\mathbb{N} \subseteq \mathbb{Z}$ (sau, mai general, incluziunea unui inel în alt inel) se va trata ca o aplicație injectivă de la primul inel la al doilea

$$f : \mathbb{N} \to \mathbb{Z} \qquad (n_1 \neq n_2 \Rightarrow f(n_1) \neq f(n_2))$$

ce păstrează operațiile $(+)$ şi $(\cdot)$. Dacă $f(\mathbb{N}) = \{f(n) \mid n \in \mathbb{N}\}$ este imaginea acestei aplicații, atunci avem izomorfismul $\mathbb{N} \cong \operatorname{Im} f$, deci în acest caz elementele $n \in \mathbb{N}$ pot fi identificate cu imaginile lor $f(n) \in \mathbb{Z}$. Cu alte cuvinte, $\mathbb{Z}$ conține o imagine izomorfică a sistemului $\mathbb{N}$.

Observația 2. Construcția următoare, ca şi un şir de construcții ce vor fi efectuate în viitor, se bazează pe noțiunea cunoscută de mulțime-factor, care se defineşte printr-o relație de echivalență „$\sim$”, adică o relație binară pe M, cu proprietățile: *reflecxivitate* $(a \sim a, \forall a \in M)$, *simetrie* $(a \sim b \Rightarrow b \sim a;\ a, b \in M)$ şi *tranzitivitate* $(a \sim b, b \sim c \Rightarrow a \sim c;\ a, b, c \in M)$. Orice relație de echivalență „$\sim$” pe mulțimea M defineşte o partiție a mulțimii M în clase de echivalență: orice $a \in M$ defineşte clasa

$$\overline{a} = \{b \in M \mid a \sim b\}.$$

Mulțimea claselor de echivalență

$$M/\sim\ = \{\overline{a} \mid a \in M\}$$

se numeşte *mulţime-factor a mulţimii* M în raport cu relaţia de echivalenţă „$\sim$”. Are loc şi afirmaţia reciprocă: orice partiţie a mulţimii M defineşte pe M o relaţie de echivalenţă.

Să trecem la *construirea inelului* $\mathbb{Z}$ cu ajutorul sistemului de numere naturale $\mathbb{N}$. Considerăm pătratul cartezian $\mathbb{N}\times\mathbb{N}$ şi definim pe el următoarea relaţie binară:

$$(m,n)\sim(p,q) \quad \overset{def}{\Leftrightarrow} \quad m+q=n+p \tag{2}$$

Lema 5.3. *Relaţia binară „$\sim$”, definită pe $\mathbb{N}\times\mathbb{N}$ prin (2), este o relaţie de echivalenţă (adică este reflexivă, simetrică şi tranzitivă).*

Demonstraţia se reduce la verificare directă şi se propune ca exerciţiu. □

Prin urmare, relaţia „$\sim$” determină o partiţie a mulţimii $\mathbb{N}\times\mathbb{N}$ în clase disjuncte de echivalenţă (vezi observaţia 2). Pentru orice element $(m,n)\in\mathbb{N}\times\mathbb{N}$ notăm clasa de echivalenţă definită de el în mod obişnuit:

$$\overline{(m,n)} = \{(p,q)\in\mathbb{N}\times\mathbb{N} \mid (m,n)\sim(p,q)\}.$$

Obţinem mulţimea-factor:

$$\mathbb{Z} = (\mathbb{N}\times\mathbb{N})/\sim\ = \{\overline{(m,n)} \mid m,n\in\mathbb{N}\}.$$

Conform definiţiei avem:

$$\overline{(m,\ \ n)} = \overline{(p,\ \ q)} \Leftrightarrow (m,\ \ n)\sim(p,\ \ q) \Leftrightarrow m+q=n+p.$$

Imediat se observă relaţia dintre $\mathbb{Z}$ şi $\mathbb{N}$: există o *aplicaţie injectivă* (adică o incluziune):

$$\varphi:\mathbb{N}\to\mathbb{Z}=(\mathbb{N}\times\mathbb{N})/\sim,$$

definită prin regula $\varphi(n)=\overline{(n,0)}$ (este clar că dacă $m\neq n$, atunci $\overline{(m,0)}\neq\overline{(n,0)}$, în caz contrar $(m,0)\sim(n,0),\ \ m+0=0+n,\ \ m=n$).

Pentru a transforma mulțimea $\mathbb{Z}$ în inel, mai întâi definim următoarele două operații pe $\mathbb{N}\times\mathbb{N}$:

$$(m,n)+(p,q)=(m+p,n+q), \tag{3}$$
$$(m,n)\cdot(p,q)=(mp+nq,mq+np). \tag{4}$$

Lema 5.4. *Adunarea şi înmulțirea pe* $\mathbb{N}\times\mathbb{N}$*, definite prin regulile (3) şi (4), sunt operații algebrice comutative şi asociative; mai mult, ele sunt legate prin legea distributivă,* $(0,0)$ *şi* $(1,0)$ *sunt elemente neutre pentru adunare şi înmulțire, respectiv.*

Demonstrația este directă şi poate fi efectuată în mod independent. □

Însă în $\mathbb{N}\times\mathbb{N}$ nu există elementul opus $-(m,n)$ pentru fiecare $m,n\in\mathbb{N}$. Dacă

$$(m,n)+(p,q)=(0,0),$$

atunci $m+p=0, n+q=0,$ ceea ce nu are loc pentru $m>0, n>0.$ Deci $\mathbb{N}\times\mathbb{N}$ nu formează inel în raport cu aceste operații.

Următorul pas al construcției: transferăm operațiile (3) şi (4) din $\mathbb{N}\times\mathbb{N}$ pe mulțimea-factor $\mathbb{Z}=(\mathbb{N}\times\mathbb{N})/\sim$ prin regulile:

$$\overline{(m,n)}+\overline{(p,q)} \overset{def}{=} \overline{(m,n)+(p,q)} \overset{(3)}{=} \overline{(m+p,n+q)}; \tag{5}$$
$$\overline{(m,n)}\cdot\overline{(p,q)} \overset{def}{=} \overline{(m,n)\cdot(p,q)} \overset{(4)}{=} \overline{(mp+nq,mq+np)}. \tag{6}$$

Lema 5.5. *Operațiile definite pe* $\mathbb{Z}$ *prin regulile (5) şi (6) sunt corect definite, adică rezultatele nu depind de alegerea reprezentanților claselor de echivalență.*

*Demonstrație***.** Având doi reprezentanți ai aceleaşi clase

$$(m_1,n_1)\sim(m_2,n_2),$$

se cere de arătat că

$$(m_1, n_1) + (p, q) \sim (m_2, n_2) + (p, q), \tag{7}$$
$$(m_1, n_1) \cdot (p, q) \sim (m_2, n_2) \cdot (p, q). \tag{8}$$

Verificăm relația (7). Conform ipotezei, avem $m_1 + n_2 = n_1 + m_2$ şi adăugând $p + q$ la ambele părți obținem:

$$(m_1 + n_2) + (p + q) = (n_1 + m_2) + (p + q) \quad \Rightarrow$$
$$(m_1 + p) + (n_2 + q) = (n_1 + q) + (m_2 + p) \quad \Rightarrow$$
$$(m_1 + p, \quad n_1 + q) \sim (m_2 + p, \quad n_2 + q),$$

de unde rezultă (7). În mod similar se verifică (8). □

Lema 5.6. *Mulțimea* $\mathbb{Z} = (\mathbb{N} \times \mathbb{N}) / \sim$ *formează un inel comutativ în raport cu operațiile (5) şi (6). Prin incluziunea* $\varphi : \mathbb{N} \to \mathbb{Z}, \quad n \to \overline{(n, 0)}$, *operațiile în* $\mathbb{Z}$ *sunt prelungiri ale operațiilor respective din* $\mathbb{N}$.

Demonstrație. Proprietățile operațiilor $(+)$ şi $(\cdot)$ pe $\mathbb{N} \times \mathbb{N}$ sunt arătate în Lema 5.4. Dar operațiile (5) şi (6) pe $\mathbb{Z}$ sunt definite pe baza operațiilor respective din $\mathbb{N} \times \mathbb{N}$, de aceea este uşor de văzut că toate proprietățile amintite se transferă la operațiile din $\mathbb{Z}$. Prin urmare, operațiile $(+)$ şi $(\cdot)$ din $\mathbb{Z}$ sunt comutative şi asociative, iar $(\cdot)$ este distributivă în raport cu $(+)$.

Element neutru pentru adunarea din $\mathbb{Z}$ este clasa $\overline{(0,0)}$ $(= \overline{(n, n)})$, deoarece pentru orice $\overline{(m, n)} \in \mathbb{Z}$ avem:

$$\overline{(m, n)} + \overline{(0, 0)} \overset{(5)}{=} \overline{(m + 0, n + 0)} = \overline{(m, n)}.$$

Urmează momentul cel mai delicat: existența elementului opus (care lipseşte în $\mathbb{N}$ şi de dragul căruia am început construcția). Fie $\overline{(m, n)} \in \mathbb{Z}$. Considerăm clasa $\overline{(n, m)} \in \mathbb{Z}$ şi observăm că:

$$\overline{(m, n)} + \overline{(n, m)} = \overline{(m + n, n + m)} = \overline{(0, 0)},$$

adică $\overline{(n,m)} = -\overline{(m,n)}$. Astfel, *orice element* $\overline{(m,n)} \in \mathbb{Z}$ *are element opus, egal cu* $\overline{(n,m)}$.

Din cele arătate mai sus rezultă că $\mathbb{Z}(+,\cdot)$ este un inel comutativ. Mai mult, el este un inel cu element unitate, unde $1_{\mathbb{Z}} = \overline{(1,0)} = \overline{(n+1,n)}$. Într-adevăr,

$$\overline{(m,n)} \cdot \overline{(1,0)} \overset{(6)}{=} \overline{(m \cdot 1 + n \cdot 0, m \cdot 0 + n \cdot 1)} = \overline{(m,n)}.$$

Mai rămâne de observat că incluziunea menționată mai sus $\varphi : \mathbb{N} \to \mathbb{Z}$ $(n \to \overline{(n,0)})$ păstrează operațiile $(+)$ şi $(\cdot)$:

$$\varphi(m+n) = \varphi(m) + \varphi(n), \quad \varphi(mn) = \varphi(m) \cdot \varphi(n).$$

Deci, identificând $\mathbb{N}$ cu $\varphi(\mathbb{N}) \subseteq \mathbb{Z}$, putem spune că operațiile din $\mathbb{Z}$ coincid cu cele din $\mathbb{N}$ pe elementele din $\mathbb{N}$. □

Finalizăm construcția noastră prin următoarea concluzie.

Teorema 5.7. *Inelul* $\mathbb{Z} = (\mathbb{N} \times \mathbb{N}) / \sim (+,\cdot)$ *este un sistem de numere întregi, adică un inel minimal ce conține sistemul de numere naturale* $\mathbb{N}$.

*Demonstrație***.** Conform Lemei 5.6, $\mathbb{Z}$ este un inel ce conține $\mathbb{N}$ şi operațiile lui le prelungesc pe cele din $\mathbb{N}$. Rămâne de arătat că $\mathbb{Z}$ este minimal (în raport cu incluziunea) printre inelele de acest tip. Aplicăm Lema 5.1, din care rezultă că este suficient de arătat următoarele: orice element din $\mathbb{Z}$ are forma $m-n$, unde $m,n \in \mathbb{N}$. Având în vedere că noi identificăm elementele din $\mathbb{N}$ cu imaginile lor în $\mathbb{Z}$ $(n \leftrightarrow \overline{(n,0)})$, pentru orice $\overline{(m,n)} \in \mathbb{Z}$ avem:

$$\overline{(m,n)} = \overline{(m,0)} + \overline{(0,n)} = \overline{(m,0)} - \overline{(n,0)},$$

unde $\overline{(m,0)}$ este $m \in \mathbb{N}$ şi $\overline{(n,0)}$ este $n \in \mathbb{N}$. Deci, condiția din Lema 5.1 are loc şi astfel $\mathbb{Z}$ este minimal cu condiția impusă. □

În felul acesta am construit interpretarea (modelul)

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N}) / \sim$$

sistemului de numere întregi şi aceasta demonstrează faptul că *sistemul de axiome care defineşte* $\mathbb{Z}$ *este compatibil*.

Exerciţii

1. Demonstraţi Lema 5.3 şi Lema 5.4.

§6. Relaţia de ordine în inelul numerelor întregi

În §3 s-a arătat că pe sistemul de numere naturale $\mathbb{N}$ se poate defini o relaţie de ordine $(\leq)$, ce posedă multe proprietăţi excelente, în particular, ea este compatibilă cu operaţiile din $\mathbb{N}$ (Propoziţia 3.3). În acest compartiment vom arăta că această relaţie din $\mathbb{N}$ poate fi extinsă pe întreg inelul $\mathbb{Z}$, păstrând toate proprietăţile ce le avea în $\mathbb{N}$ (ordine *totală*, lema lui Arhimede, teorema împărţirii cu rest, etc.)

Conform legii trihotomiei (Teorema 3.1), pentru orice elemente $m, n \in \mathbb{N}$ are loc una şi numai una dintre următoarele relaţii:

$$n < m, \quad n = m, \quad m < n.$$

Având în vedere acest fapt, vom diviza $\mathbb{Z}$ în trei părţi prin următoarea definiţie.

Definiţia 1. *Vom spune că clasa de echivalenţă* $\overline{(m,n)} \in \mathbb{Z}$ *este:*

- ***pozitivă****, dacă* $m > n$;
- ***nulă****, dacă* $m = n$;
- ***negativă****, dacă* $m < n$,

unde „<” este relaţia de ordine definită în $\mathbb{N}$ *(§3).*

Se observă că definiţia este corectă, adică tipul clasei de echivalenţă nu depinde de alegerea reprezentantului ei. Într-adevăr, fie $m > n$ şi $(p,q) \in \overline{(m,n)}$. Atunci $(m,n) \sim (p,q)$, adică $m + q = n + p$. Prin definiţie din $m > n$ rezultă $n + u = m$, $u \neq 0$, de aceea

$n+u+q=n+p$, prin urmare, $u+q=p$ (propoziția 2.7), $u\neq 0$, ceea ce înseamnă că $p>q$. Astfel, dacă $\overline{(m,n)}$ este o clasă pozitivă, atunci pentru orice reprezentant al ei (p,q) are loc relația $p>q$. La fel se verifică corectitudinea în celelalte două cazuri ($m=n$, $m<n$). Notăm :

$\mathbb{Z}^{(+)}$ - mulțimea claselor pozitive din $\mathbb{Z}$;

$\{0\}$ - clasa nulă din $\mathbb{Z}$ ($\overline{(0,0)}=\overline{(n,n)}$);

$\mathbb{Z}^{(-)}$ - mulțimea claselor negative din $\mathbb{Z}$.

Din legea trihotomiei, menționată mai sus (Teorema 3.1), rezultă că inelul $\mathbb{Z}$ are următoarea descompunere în trei părți care nu se intersectează:

$$\mathbb{Z}=\mathbb{Z}^{(-)}\cup\{0\}\cup\mathbb{Z}^{(+)}.$$

Aplicația $\psi:\{0\}\cup\mathbb{Z}^{(+)}\to\mathbb{N}$, definită prin regula $\psi(\overline{(m,n)})=m-n$ (are sens, deoarece $m\geq n$), determină o bijecție ce păstrează operațiile, de aceea putem scrie

$$\{0\}\cup\mathbb{Z}^{(+)}\cong\mathbb{N}$$

şi identifica clasa $\overline{(m,n)}$ cu $m-n\in\mathbb{N}$ în cazul $m\geq n$. Notăm:

$$1=\overline{(1,0)},\quad -1=\overline{(0,1)},\quad n=\overline{(n,0)},\quad -n=\overline{(0,n)},\quad \forall n\in\mathbb{N}.$$

Fie $P=\mathbb{Z}^{(+)}\cup\{0\}$ şi $-P=Z^{(-)}$. Să arătăm că P este con pozitiv (vezi Anexa II) al inelului $(\mathbb{Z},+,\cdot)$. Pentru aceasta trebuie să demonstrăm că suma şi produsul a două clase din P este din P, iar dacă o clasă este şi din P şi din $-P$, atunci ea este clasa nulă.

Într-adevăr, fie $x=\overline{(m,n)}, y=\overline{(p,q)}\in\mathbb{Z}^{(+)}$, adică $m>n$ şi $p>q$. Atunci $m=n+u, p=q+v, u\neq 0, v\neq 0$ şi

$$x+y=\overline{(m,n)}+\overline{(p,q)}=\overline{(m+p,n+q)}=$$
$$=\overline{(n+u+q+v,n+q)}=\overline{\big((n+q)+(u+v),n+q\big)}.$$

Din $u+v\neq 0$, rezultă $(n+q)+(u+v)>n+q$, deci $x+y\in\mathbb{Z}^{(+)}$. La fel obținem:

$$x\cdot y=\overline{(m,n)}\cdot\overline{(p,q)}=\overline{(mp+nq,mq+np)}=$$

$$=\left(\overline{(n+u)(q+v)+nq,(n+u)q+n(q+v)}\right)=$$

$$=\overline{(nq+uq+nv+uv+nq,nq+uq+nq+nv)}\in\mathbb{Z}^{(+)},$$

deoarece $uv\neq 0$.

Dacă x (sau y) este clasa nulă $\overline{(0,0)}$, atunci $x+y=y$ (sau $x+y=x$), $xy=\overline{(0,0)}$, deci $x+y\in P$ şi $xy\in P$.

În sfârşit, fie $z=\overline{(r,s)}\in P\bigcap(-P)$. Atunci $\overline{(r,s)}\in P$, $\overline{(s,r)}\in P$, deci $r\geq s, s\geq r$ de unde rezultă $r=s$ si $z=\overline{(0,0)}$. Aşadar, P este conul pozitiv al inelului $(\mathbb{Z},+,\cdot)$.

Relația de ordine $(\leq)$ pe $\mathbb{Z}$ se determină acum astfel:

$$x\leq y\Leftrightarrow y-x\in P.$$

Deoarece $P\bigcup(-P)=\mathbb{Z}$, rezultă că $(\mathbb{Z},+,\cdot,\leq)$ este un inel total ordonat. Prin urmare, e adevărată

Propoziția 6.1. *Relația binară „$\leq$” definită pe $\mathbb{Z}$ este o relație de ordine (adică este reflexivă, tranzitivă şi antisimetrică). Mai mult, $\mathbb{Z}(\leq)$ este o mulțime total (sau liniar) ordonată, adică oricare două numere întregi $x,y\in\mathbb{Z}$ sunt comparabile: $x\leq y$ sau $y\leq x$. Relația „$\leq$” din $\mathbb{Z}$ este o prelungire a relației de ordine „$\leq$” din $\mathbb{N}$.*

Relația binară „$\leq$” se numeşte *relație de ordine naturală* pe $\mathbb{Z}$. În continuare vom arăta câteva proprietăți ale acestei relații de ordine, proprietăți care rezultă din teoria generală a inelelor total ordonate (a se vedea, de exemplu, [26]).

Propoziția 6.2. *Relația de ordine naturală pe $\mathbb{Z}$ posedă următoarele proprietăți:*

1) dacă $x < y$ *atunci* $x + z < y + z$ *pentru orice* $z \in \mathbb{Z}$;

2) dacă $x < y$ *şi* $z > 0$, *atunci* $xz < yz$;

3) dacă $x < y$, *atunci* $-y < -x$;

4) dacă $0 < x < y$, *atunci* $x^2 < y^2$. □

În continuare vom transfera în inelul $\mathbb{Z}$ unele rezultate demonstrate anterior pentru mulțimea numerelor naturale, în particular lema lui Arhimede şi teorema împărțirii cu rest (Lema 3.4, Teorema 3.5).

Lema 6.3 ***(lema lui Arhimede pentru inelul*** $\mathbb{Z}$***).*** *Pentru orice două numere întregi* $x, y \in \mathbb{Z}$, $x > 0$, *există un număr natural* n, *încât* $nx > y$.

Demonstrație. Dacă $y \le 0$, atunci $1 \cdot x = x > y$. Dacă $y > 0$, atunci $x, y \in \mathbb{N}$ şi putem aplica lema lui Arhimede pentru $\mathbb{N}$ (Lema 3.4): există $n \in \mathbb{N}$, astfel încât $nx > y$. □

În §3 am observat că $\mathbb{N}$ este o mulțime discretă. Să arătăm că această proprietate se păstrează şi în $\mathbb{Z}$.

Propoziția 6.4. *Inelul numerelor întregi* $\mathbb{Z}$ *este discret, adică între oricare două numere întregi succesive* (x *şi* $x+1$) *nu există alte numere întregi.*

Demonstrație. Situația $x < y < x + 1$ este imposibilă deoarece adăugând $(-x)$ la cele trei părți, obținem $0 < y - x < 1$, contradicție (vezi §3, observația 6). □

Pentru formularea teoremei împărțirii cu rest în $\mathbb{Z}$ (analogul teoremei 3.5) avem nevoie de următoarea noțiune.

Definiția 2. ***Modul*** *(sau* ***valoare absolută****) al numărului* $x \in \mathbb{Z}$ *se numeşte numărul natural* $|x| = x \cdot \operatorname{sgn}(x)$, *adică:*

$$|x| = \begin{cases} x, & \text{dacă } x > 0; \\ 0, & \text{dacă } x = 0; \\ -x, & \text{dacă } x < 0. \end{cases}$$

Proprietăți ale modulului unui număr la aplicarea operațiilor din $\mathbb{Z}$ sunt date în următoarea afirmație.

Lema 6.5. *Pentru orice numere* $x, y \in \mathbb{Z}$ *au loc relațiile:*

1) $|xy| = |x| \cdot |y|$;

2) $|x + y| \le |x| + |y|$.

Demonstrația se propune în calitate de exercițiu. □

Acum avem toate cele necesare pentru a formula şi a demonstra

Teorema 6.6 ***(teorema împărțirii cu rest în*** $\mathbb{Z}$***).*** *Pentru orice două numere întregi* $x, y \in \mathbb{Z}$, $y \neq 0$, *există două numere întregi* $q, r \in \mathbb{Z}$ *astfel încât*

$$x = yq + r, \quad 0 \le r \le |y|.$$

Numerele q şi r cu această proprietate sunt determinate în mod unic.

Demonstrație. Cazul $x = 0$ este trivial: $0 = y \cdot 0 + 0$. Se consideră toate celelalte cazuri posibile:

$$a)\ x > 0, \quad y > 0; \qquad b)\ x > 0, \quad y < 0;$$

$$c)\ x < 0, \quad y > 0; \qquad d)\ x < 0, \quad y < 0.$$

$a)$. Dacă $x > 0$ şi $y > 0$, atunci $x, y \in \mathbb{N}$ şi, aplicând teorema împărțirii cu rest pentru $\mathbb{N}$ (vezi Teorema 3.5), obținem $x = yq + r$, unde $q, r \in \mathbb{N}, r < y = |y|$.

b). Dacă $x>0$ şi $y<0$, atunci $x,-y\in\mathbb{N}$ şi, aplicând teorema 3.5, obţinem $x=(-y)q_1+r_1$, unde $r_1\in\mathbb{N}$ şi $r_1<(-y)$. Notăm: $q=-q_1$ şi $r=r_1$. Atunci $x=y(-q_1)+r_1=yq+r$, unde $0\le r<(-y)=|y|$.

c). Fie $x<0$ şi $y>0$. Atunci $-x,y\in\mathbb{N}$ şi din teorema 3.5 avem

$$-x=yq_1+r_1,\ 0\le r_1<y.$$

Dacă $r_1=0$, atunci $-x=yq_1$, de aceea $x=y(-q_1)$ şi putem lua $q=-q_1$ şi $r=0$. Dacă $0<r_1$, atunci

$$x=-yq_1-r_1=y(-q_1-1)+y-r_1.$$

Notând $q=-q_1-1$ şi $r=y-r_1$, obţinem $x=yq+r$. Din relaţia $0<r_1<y$ avem $-y<-r_1<0$, prin urmare,

$$0<y-r_1<y=|y|,\ 0<r<|y|.$$

d). Fie $x<0, y<0$. Atunci $-x,-y\in\mathbb{N}$ şi din teorema 3.5 obţinem:

$$-x=(-y)q_1+r_1,\ \ 0\le r_1<(-y).$$

Dacă $r_1=0$ atunci $-x=(-y)q_1$, deci $x=yq_1$ şi putem lua $q=q_1$ şi $r=0$. Dacă $r_1>0$, atunci:

$$x=yq_1-r_1=y(q_1+1)+(-y-r_1)$$

şi, notând

$$q=q_1+1, r=-y-r_1,$$

obţinem $x=yq+r$. Din relaţia $0<r_1<(-y)$ avem (înmulţind cu -1) $y<-r_1<0$, de unde (adăugând $-y$) rezultă $0<-y-r_1<-y$, adică $0<r<|y|$.

Astfel, în toate cazurile posibile am obţinut relaţia din teoremă. Rămâne de verificat unicitatea câtului şi a restului. Presupunem că $x\in\mathbb{Z}$ posedă două descompuneri:

$$x=yq+r,\quad 0\le r<|y|;$$

$$x = yq_1 + r_1, \qquad 0 \le r_1 < |y|.$$

Atunci

$$yq + r = yq_1 + r_1,$$

de unde

$$y(q - q_1) = r_1 - r.$$

Notând $u = q - q_1$, obținem $yu = r_1 - r$ şi, din lema 6.5, p.1), avem:

$$|y||u| = |r_1 - r|. \tag{1}$$

Deoarece $r, r_1 \in \mathbb{N}$, în cazul $r_1 \le r$ avem $0 \le r - r_1 \le r < |y|$, iar în cazul $r \le r_1$ avem $0 \le r_1 - r \le r_1 < |y|$. Aşadar, în ambele cazuri posibile obținem $|r - r_1| < |y|$.

Se vede că presupunerea $u = q - q' \ne 0$ aduce la contradicție: în acest caz $|u| \ge 1$, deci $|y||u| \ge |y|$ şi relația (1) implică

$$|y| \le |y||u| = |r_1 - r| < |y|.$$

Astfel rămâne doar posibilitatea $u = 0$, adică $q = q_1$. Acum din descompunerile inițiale rezultă $r = r_1$. □

Exerciții

1. Pentru care numere întregi a şi b sunt adevărate relațiile:

a) $a - b < a < a + b$;

b) $a + b < a < a - b$;

c) $|a + b| = |a| + |b|$;

d) $|a - b| = |a| - |b|$;

e) $|a - b| = |a| + |b|$;

f) $|a| + |b| \le 1$.

2. Utilizând algoritmul împărțirii cu rest să se arate că, oricare ar fi numărul $c > 1$, orice număr întreg a poate fi scris în forma $a = \pm(a_0 c^n + a_1 c^{n-1} + ... + a_{n-2} c^2 + a_{n-1}\, c + a_n)$, unde $a_i \in \mathbb{N}, a_i < c, i = \overline{0,n}.$
3. Demonstrați Lema 6.5.
4. La împărțirea numerelor naturale a şi b la 7 s-au obținut, respectiv, resturile 4 si 3. Care este restul de la împărțirea la 7 a următoarelor numere: $a+b$, $a-b$, ab, $2a+3b$, a^2, b^2, a^3, b^3, a^2+b^2?

Capitolul III

Numere raționale

§7. Câmpul numerelor raționale $\mathbb{Q}$ (unicitatea şi existența)

În §5 a fost efectuată trecerea de la sistemul numerelor naturale $\mathbb{N}$ la sistemul numerelor întregi $\mathbb{Z}$, reieşind din necesitatea ca să fie posibilă operația inversă adunării - scăderea. Pentru noul sistem numeric $\mathbb{Z}$ avem operația scăderii, dar nu întotdeauna este posibilă operația inversă înmulțirii - împărțirea (fără rest, vezi teorema 6.6). Aceasta motivează necesitatea construirii unui nou sistem numeric, care ar trebui să conțină $\mathbb{Z}$, să păstreze toate proprietățile acestui inel, dar în afară de aceasta să posede şi operația de împărțire.

Necesitatea extinderii numerelor întregi a apărut din timpuri străvechi. Cerințele vieții înconjurătoare de a măsura diferite mărimi (segmente, greutăți, arii, volume, vârste ş.a.) i-au impus pe oameni să introducă şi alte numere, diferite de cele întregi: jumătăți, sferturi, optimi ş.a. Istoriceşte numerele raționale pozitive au apărut înaintea numerelor întregi negative.

Problema este următoarea. Dacă se alege o unitate de măsură (cm, g, cm^2, cm^3, an, oră ş.a.), atunci nu toate mărimile de tipul dat pot fi măsurate cu această unitate. Apare necesitatea de a împărți unitatea dată în câteva părți egale, deci de a extinde numerele întregi.

În acest caz este comod de utilizat noțiunea de câmp care este o specificare a celei de inel.

Definiția 1. *Inelul comutativ* $K(+,\cdot)$*, care conține cel puțin două elemente, se numeşte* ***câmp*** *dacă pentru orice două elemente* $a,b \in K$*,* $b \neq 0$*, există un element* $x \in K$ *astfel încât* $bx = a$

(elementul x se notează $\frac{a}{b}$ şi se numeşte ***câtul*** *elementului a prin elementul $b \neq 0$).*

Orice câmp K posedă element unitar 1_K, pentru care $1_K \cdot a = a$, $\forall a \in K$. Mai mult, orice element $a \in K$, $a \neq 0$, posedă element invers a^{-1}, pentru care $aa^{-1} = a^{-1}a = 1_K$ şi acest element este determinat în mod unic, prin urmare şi câtul a două elemente $\frac{a}{b}$, $b \neq 0$, este determinat în mod unic.

Reieşind din sarcina pusă mai sus, formulăm

Definiția 2. ***Sistem de numere raționale*** *se numeşte un câmp minimal (în raport cu incluziunea) $\mathbb{Q}$ care conține inelul numerelor întregi $\mathbb{Z}$, adică:*

1) $\mathbb{Z} \subseteq \mathbb{Q}$, unde $\mathbb{Q}$ este un câmp;

2) operațiile de adunare şi înmulțire în $\mathbb{Q}$ coincid cu operațiile respective din $\mathbb{Z}$ pentru elementele din $\mathbb{Z}$;

3) $\mathbb{Q}$ este un câmp minimal (în raport cu incluziunea) ce satisface condițiile 1) şi 2).

În definițiile 1 şi 2 se conțin axiomele sistemului de numere raționale. În continuare verificăm cele mai importante cerințe asupra unui sistem de axiome: completitudinea, care se reduce la unicitatea sistemului numeric şi compatibilitatea, ce este echivalentă cu existența unei interpretări (vezi §4).

Începem cu problema unicității sistemului de numere raționale şi pentru rezolvarea ei, ca şi în cazul precedent (lema 5.1), exprimăm minimalitatea câmpului într-o formă mai comodă.

Lema 7.1. *Fie K un câmp arbitrar ce conține $\mathbb{Z}$. Câmpul K este minimal printre câmpurile ce conțin $\mathbb{Z}$ dacă şi numai dacă*

orice element din K *are forma* $\frac{a}{b}$, *unde* $a,b\in\mathbb{Z}$, $b\neq 0$ şi *împărţirea se efectuează în câmpul* K.

Demonstraţie. ($\Rightarrow$) Fie $\mathbb{Z}\subseteq K$ şi K un câmp minimal cu această condiţie. Considerăm următoarea submulţime în K:

$$K'=\left\{\frac{a}{b}\,|\,b\neq 0;\ a,b\in\mathbb{Z}\right\}.$$

Se verifică uşor că K' este închisă în raport cu operaţia adunării şi înmulţirii în K $(+,\cdot)$, unde :

$$\frac{a}{b}\pm\frac{c}{d}=\frac{ad\pm bc}{bd},\qquad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

Mai mult, K' este închisă şi în raport cu operaţia împărţirii din K $(+,\cdot)$, ce se efectuează prin regula:

$$\frac{a}{b}:\frac{c}{d}=\frac{ad}{bc}.$$

Prin urmare, K' este un subcâmp în K. Observăm că $\mathbb{Z}\subseteq K'$, deoarece orice număr întreg $a\in\mathbb{Z}$ poate fi reprezentat în forma $\frac{a}{1}$ (sau: $\frac{ab}{b}$, $b\neq 0$). Acum din minimalitatea lui K rezultă $K=K'$, adică orice element din K are forma $\frac{a}{b}$, unde $a,b\in\mathbb{Z}$, $b\neq 0$.

($\Leftarrow$) Presupunem că $\mathbb{Z}\subseteq K$ şi orice element din K are forma $\frac{a}{b}$, unde $a,b\in K$ şi $b\neq 0$. Atunci orice subcâmp $K'\subseteq K$, ce conţine $\mathbb{Z}$, este obligat, prin definiţie, să conţină şi toate elementele de forma $\frac{a}{b}$; $a,b\in\mathbb{Z}$, $b\neq 0$, deaceea $K'=K$. Aceasta arată minimalitatea câmpului K. □

Acum putem demonstra *unicitatea sistemului de numere raționale* până la un izomorfism (de comparat cu teorema 5.2).

Teorema 7.2. *Dacă* $\mathbb{Q}_1$ *şi* $\mathbb{Q}_2$ *sunt două sisteme de numere raționale, atunci câmpurile* $\mathbb{Q}_1$ *şi* $\mathbb{Q}_2$ *sunt izomorfe:* $\mathbb{Q}_1 \cong \mathbb{Q}_2$.

Demonstrație. Fie $\mathbb{Z}_1 \subseteq \mathbb{Q}_1$ şi $\mathbb{Z}_2 \subseteq \mathbb{Q}_2$, unde $\mathbb{Z}_1$ şi $\mathbb{Z}_2$ sunt sisteme de numere întregi. Din unicitatea sitemului de numere întregi (teorema 5.2) rezultă existența unui izomorfism de inele $\varphi : \mathbb{Z}_1 \to \mathbb{Z}_2$. Vom arăta că φ poate fi extins pînă la un izomorfism $\overline{\varphi} : \mathbb{Q}_1 \to \mathbb{Q}_2$. Conform Lemei 7.1, orice element din $\mathbb{Q}_1$ are forma $\frac{a}{b}$, unde $a, b \in \mathbb{Z}_1$ şi $b \neq 0$. Definim aplicația $\overline{\varphi} : \mathbb{Q}_1 \to \mathbb{Q}_2$ prin regula:

$$\overline{\varphi}\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)}, \qquad (1)$$

unde din $b \neq 0$ avem $\varphi(b) \neq 0$.

Deoarece exprimarea în forma $\frac{a}{b}$ nu este unică, trebuie de verificat *corectitudinea* acestei definiții. Fie $\frac{a}{b} = \frac{a'}{b'}$. Atunci $ab' = ba'$ (în $\mathbb{Z}_1$) şi deaceea $\varphi(ab') = \varphi(ba')$, prin urmare, $\varphi(a)\varphi(b') = \varphi(b)\varphi(a')$, adică

$$\frac{\varphi(a)}{\varphi(b)} = \frac{\varphi(a')}{\varphi(b')}.$$

Aceasta arată că imaginea $\varphi(x)$ nu depinde de exprimarea elementului $x \in \mathbb{Q}_1$ în forma $\frac{a}{b}$. Se observă uşor că $\overline{\varphi}$ este o continuare a lui φ: pentru orice $a \in \mathbb{Z}_1$,

$$\overline{\varphi}(a)=\overline{\varphi}(\frac{a}{1_{\mathbb{Z}_1}})=\frac{\varphi(a)}{\varphi(1_{\mathbb{Z}_1})}=\frac{\varphi(a)}{1_{\mathbb{Z}_2}}=\varphi(a).$$

Să arătăm că $\overline{\varphi}$ este o aplicație bijectivă.

a) $\overline{\varphi}$ este *injectivă*: dacă $\overline{\varphi}(\frac{a}{b})=\overline{\varphi}(\frac{c}{d})$, unde $\frac{a}{b},\frac{c}{d}\in\mathbb{Q}_1$, $a,b\neq 0,c,d\neq 0\in\mathbb{Z}_1$, atunci

$$\frac{\varphi(a)}{\varphi(b)}=\frac{\varphi(c)}{\varphi(d)},$$

deaceea $\varphi(a)\varphi(d)=\varphi(b)\varphi(c)$ şi $\varphi(ad)=\varphi(bc)$. Deoarece φ este un izomorfism, de aici rezultă $ad=bc$, prin urmare, $\frac{a}{b}=\frac{c}{d}$.

b) $\overline{\varphi}$ este *surjectivă:* pentru orice $\frac{k}{l}\in\mathbb{Q}_2$ $(k,l\in\mathbb{Z}_2,l\neq 0)$, notînd $a=\varphi^{-1}(k),b=\varphi^{-1}(l)\in\mathbb{Z}_1$, obținem

$$\overline{\varphi}\left(\frac{a}{b}\right)=\frac{\varphi(a)}{\varphi(b)}=\frac{\varphi\varphi^{-1}(k)}{\varphi\varphi^{-1}(l)}=\frac{k}{l},$$

adică orice element din $\mathbb{Q}_2$ are imagine inversă în $\mathbb{Q}_1$.

Din a) şi b) acum rezultă că $\overline{\varphi}$ este o bijecție. Rămâne să verificăm că $\overline{\varphi}$ păstrează operațiile adunării şi înmulțirii. De exemplu, pentru operația adunării avem:

$$\overline{\varphi}\left(\frac{a}{b}+\frac{c}{d}\right)=\overline{\varphi}\left(\frac{ad+bc}{bd}\right)\overset{(1)}{=}\frac{\varphi(ad+bc)}{\varphi(bd)}=\frac{\varphi(ad)+\varphi(bc)}{\varphi(b)\varphi(d)},$$

$$\overline{\varphi}(\frac{a}{b})+\overline{\varphi}(\frac{c}{d})\overset{(1)}{=}\frac{\varphi(a)}{\varphi(b)}+\frac{\varphi(c)}{\varphi(d)}=$$

$$=\frac{\varphi(a)\varphi(d)+\varphi(b)\varphi(c)}{\varphi(b)\varphi(d)}=\frac{\varphi(ad)+\varphi(bc)}{\varphi(b)\varphi(d)}.$$

La fel se verifică păstrarea operației înmulțirii.

Din cele demonstrate mai sus putem deduce că câmpurile $\mathbb{Q}_1$ şi $\mathbb{Q}_2$ sunt izomorfe. □

Trecem la analiza problemei despre *existența* sistemului de numere raționale. Pentru a soluționa această problemă vom arăta o metodă de construcție a sistemului $\mathbb{Q}$, utilizând atât sistemul de numere întregi $\mathbb{Z}$, cât şi procedeul de trecere la mulțimea-factor (vezi §5).

Notăm $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ şi definim pe produsul cartezian $\mathbb{Z} \times \mathbb{Z}^*$ următoarea relație binară:

$$(a,b) \sim (c,d) \overset{def}{\Leftrightarrow} ad = bc, \tag{2}$$

unde $a, c \in \mathbb{Z}$, iar $b, d \in \mathbb{Z}^*$.

Lema 7.3. *Relația binară „$\sim$” definită pe produsul cartezian $\mathbb{Z} \times \mathbb{Z}^*$ prin regula (2) este o relație de echivalență (adică este reflexivă, simetrică şi tranzitivă).*

Demonstrația se reduce la verificare directă. □

Prin urmare, relația „$\sim$” determină o partiție a mulțimii $\mathbb{Z} \times \mathbb{Z}^*$ în clase de echivalență: orice $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ determină o clasă

$$\overline{(a,b)} = \{(c,d) \in \mathbb{Z} \times \mathbb{Z}^* \mid (a,b) \sim (c,d)\}.$$

Vom nota această clasă de echivalență prin $\frac{a}{b}$. Două clase de echivalență sunt egale dacă şi numai dacă:

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow (a,b) \sim (c,d) \Leftrightarrow ad = bc.$$

În particular,

$$\frac{a}{b} = \frac{am}{bm}, \quad m \neq 0.$$

Astfel obținem mulțimea-factor:

$$\mathbb{Q} = \left(\mathbb{Z} \times \mathbb{Z}^*\right) / \sim$$

ce constă din toate clasele de echivalență ale mulțimii $\mathbb{Z}\times\mathbb{Z}^*$ în raport cu relația „$\sim$”. Orice element din clasa de echivalență $\overline{(a,b)}\in\mathbb{Q}$ poate fi luat în calitate de reprezentant al ei.

Observăm că câmpul $\mathbb{Q}$ poate fi considerat ca o extindere a inelului $\mathbb{Z}$, deoarece există o aplicație injectivă

$$\varphi:\mathbb{Z}\to\mathbb{Q}=\left(\mathbb{Z}\times\mathbb{Z}^*\right)/\sim,\ \ \varphi\left(a\right)=\frac{a}{1}=\overline{(a,1)}$$

(dacă $a\neq b$, atunci $\frac{a}{1}\neq\frac{b}{1}$). În particular, numărului $1\in\mathbb{Z}$ îi corespunde clasa de echivalență

$$\overline{(1,1)}=\frac{1}{1}=\frac{a}{a}\quad\left(0\neq a\in\mathbb{Z}\right).$$

Scopul nostru este transformarea mulțimii $\mathbb{Q}$ în câmp şi pentru aceasta introducem pe mulțimea $\mathbb{Q}$ următoarele două operații:

$$\frac{a}{b}+\frac{c}{d}\overset{def}{=}\frac{ad+bc}{bd},\tag{3}$$

$$\frac{a}{b}\cdot\frac{c}{d}\overset{def}{=}\frac{ac}{bd}.\tag{4}$$

Lema 7.4. *Operațiile de adunare şi înmulțire, date in (3) şi (4), pe mulțimea* $\mathbb{Q}=\left(\mathbb{Z}\times\mathbb{Z}^*\right)/\sim$ *sunt definite corect, adică rezultatele efectuării lor nu depind de alegerea reprezentanților claselor de echivalență.*

Demonstrație. Verificăm afirmația pentru operația adunării. Dacă

$$\frac{a}{b}=\frac{a_1}{b_1}\ \text{şi}\ \frac{c}{d}=\frac{c_1}{d_1},$$

atunci $ab_1=ba_1$ şi $cd_1=dc_1$, de aceea:

$$(ad+bc)b_1d_1=(ab_1)(dd_1)+(bb_1)(cd_1)=$$
$$=(ba_1)(dd_1)+(bb_1)(dc_1)=$$
$$=(bd)(a_1d_1)+(bd)(b_1c_1)=(bd)(a_1d_1+b_1c_1),$$

dar aceasta arată că

$$\frac{ad+bc}{bd}=\frac{a_1d_1+b_1c_1}{b_1d_1},$$

adică

$$\frac{a}{b}+\frac{c}{d}=\frac{a_1}{b_1}+\frac{c_1}{d_1}.$$

Prin urmare, operația adunării este corect definită. La fel se verifică corectitudinea operației înmulțirii. □

Lema 7.5. *Mulțimea* $\mathbb{Q}=\left(\mathbb{Z}\times\mathbb{Z}^*\right)/\sim$ *în raport cu operația* $(+)$ *este un grup abelian.*

Demonstrație. Operația $(+)$ în $\mathbb{Q}$ este comutativă şi asociativă, ceea ce rezultă din regula (3) şi din faptul că în $\mathbb{Z}$ operațiile sunt asociative şi comutative. Mai mult, $\mathbb{Q}(+)$ posedă element neutru - clasa de echivalență $\frac{0}{1}$ (sau $\frac{0}{a}$, $a\neq 0$), deoarece

$$\frac{a}{b}+\frac{0}{1}=\frac{a\cdot 1+b\cdot 0}{b\cdot 1}=\frac{a}{b},\quad \forall\frac{a}{b}\in\mathbb{Q}.$$

În sfârşit, orice $\frac{a}{b}\in\mathbb{Q}$ posedă element opus $\frac{-a}{b}$, deoarece

$$\frac{a}{b}+\frac{-a}{b}=\frac{ab-ba}{b\cdot b}=\frac{0}{b\cdot b}=\frac{0}{1}.\quad \square$$

Lema 7.6. *Operația înmulțirii în* $\mathbb{Q}$ *(regula (4)) este asociativă şi comutativă, are element neutru* $1_{\mathbb{Q}}$ *şi este distributivă*

în raport cu adunarea. Mai mult, orice element $0 \neq r \in \mathbb{Q}$ *posedă element invers în* $\mathbb{Q}$ *(adică există* $r^{-1} \in \mathbb{Q}$, *astfel încât* $r \cdot r^{-1} = 1_{\mathbb{Q}}$*).*

Demonstrație. Din regula (4) şi din faptul că în $\mathbb{Z}$ operația înmulțirii este asociativă şi comutativă, rezultă că înmulțirea în $\mathbb{Q}$ posedă aceleaşi proprietăți.

Elementul $\frac{1}{1} = \frac{a}{a}$ $(a \neq 0)$ este element neutru în $\mathbb{Q}(\cdot)$, deoarece

$$\frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b},$$

pentru orice $\frac{a}{b} \in \mathbb{Q}$ (vom nota acest element prin $1_{\mathbb{Q}}$). Mai observăm că orice element $0 \neq r = \frac{a}{b} \in \mathbb{Q}$ are element invers $r^{-1} = \frac{b}{a}$ $(a \neq 0)$ deoarece

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = 1_{\mathbb{Q}}. \quad \square$$

Este evident că existența elementului invers dă posibilitatea de a defini în $\mathbb{Q}$ *operația împărțirii*: pentru orice elemente $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, $\frac{c}{d} \neq 0$, punem prin definiție

$$\frac{a}{b} : \frac{c}{d} \overset{def}{=} \frac{a}{b} \cdot \left(\frac{c}{d}\right)^{-1} = \frac{a}{b} \cdot \frac{d}{c} = \frac{ad}{bc}. \tag{5}$$

Lema 7.7. *Mulțimea* $\mathbb{Q} = \left(\mathbb{Z} \times \mathbb{Z}^*\right) / \sim$ *formează un câmp în raport cu operațiile adunării şi înmulțirii. Prin incluziunea*

$$\varphi : \mathbb{Z} \to \mathbb{Q},\ \varphi(a) = \overline{(a,1)} = \frac{a}{1},$$

operațiile în $\mathbb{Q}$ sunt prelungiri ale operațiilor respective din $\mathbb{Z}$.

Demonstrație. Din lemele 7.5 şi 7.6 avem că $\mathbb{Q}(+)$ este un grup abelian şi $\mathbb{Q}(+,\cdot)$ este un inel comutativ cu unitatea $1_{\mathbb{Q}}$, în care orice element $0 \neq r \in \mathbb{Q}$ are invers, deci $\mathbb{Q}(+,\cdot)$ este un câmp. Pentru orice $a,b \in \mathbb{Z}$ avem

$$\frac{a}{1}+\frac{b}{1}=\frac{a+b}{1} \text{ şi } \frac{a}{1}\cdot\frac{b}{1}=\frac{ab}{1}$$

şi, utilizând $\varphi:\mathbb{Z}\to\mathbb{Q}$ (adică identificând $a\in\mathbb{Z}$ cu $\frac{a}{1}\in\mathbb{Q}$), este clar că operațiile din $\mathbb{Q}$ coincid cu cele din $\mathbb{Z}$ pentru elementele din $\varphi(\mathbb{Z})$. □

Totalizând cele expuse mai sus (lemele 7.3-7.7), putem formula rezultatul principal.

Teorema 7.8. *Câmpul $\mathbb{Q}=\left(\mathbb{Z}\times\mathbb{Z}^*\right)/\sim$, cu operațiile date în (3) şi (4), este un sistem de numere raționale, adică un câmp minimal care conține inelul numerelor întregi $\mathbb{Z}$.*

Demonstrație. Având în vedere lema 7.7, rămâne de arătat minimalitatea lui $\mathbb{Q}$ printre câmpurile ce conțin $\mathbb{Z}$. Pentru aceasta, conform lemei 7.1, este suficient de verificat că orice element din $\mathbb{Q}$ este egal cu câtul a două numere întregi. Într-adevăr, orice element $\frac{a}{b}\in\mathbb{Q}$ este câtul numerelor $\frac{a}{1}$ şi $\frac{b}{1}$ din $\mathbb{Z}$, deoarece

$$\left(\frac{a}{1}\right):\left(\frac{b}{1}\right)\overset{(5)}{=}\frac{a\cdot 1}{1\cdot b}=\frac{a}{b}. \quad \square$$

Din toate cele expuse în acest compartiment putem face următoarea concluzie: *sistemul de numere raționale* $\mathbb{Q}$ *există şi este unic, abstracție făcând de izomorfism*.

Exerciții

1. Demonstrați Lema 7.3.

§8. **Relația de ordine naturală în câmpul numerelor raționale**

Sistemul numerelor naturale $\mathbb{N}$ şi sistemul numerelor întregi $\mathbb{Z}$ sunt total ordonate (vezi §3,6) prin relația de ordine naturală. În acest paragraf vom arăta că relația de ordine menționată poate fi extinsă peste câmpul numerelor raționale $\mathbb{Q}$. Metoda de extindere este similară cu cea utilizată la trecerea de la $\mathbb{N}$ la $\mathbb{Z}$ (vezi §6).

Câmpul numerelor raționale $\mathbb{Q}$ a fost construit (§7) în forma

$$\mathbb{Q} = \left(\mathbb{Z} \times \mathbb{Z}^*\right) / \sim = \left\{ \overline{(a,b)} = \frac{a}{b} \mid a,b \in \mathbb{Z}, b \neq 0 \right\},$$

unde $(a,b) \sim (c,d) \overset{def}{\Leftrightarrow} ad = bc.$

Definiția 1. *Vom spune că clasa de echivalență* $\overline{(a,b)} = \frac{a}{b}$ *din* $\mathbb{Q}$ *este*

- ***pozitivă****, dacă* $ab > 0$ *;*
- ***nulă****, dacă* $ab = 0$ *;*
- ***negativă****, dacă* $ab < 0$.

Notăm: $\mathbb{Q}^{(+)}$ – mulțimea elementelor *pozitive* din $\mathbb{Q}$; $\mathbb{Q}^{(-)}$ – mulțimea elementelor *negative* din $\mathbb{Q}$.

Observăm că definiția este corectă, adică tipul clasei de echivalență nu depinde de alegerea reprezentantului ei. De exemplu, dacă

$$\frac{a}{b} \in \mathbb{Q}, \frac{a}{b} = \frac{c}{d}$$

şi $ab > 0$, atunci $ad = bc, c \neq 0$, altfel $a = 0$ şi $ab = 0$. Deci $(ab)(cd) = (bc)^2 > 0$ şi condiția $ab > 0$ implică $cd > 0$.

Deoarece $\mathbb{Z} = \mathbb{Z}^{(-)} \cup \{0\} \cup \mathbb{Z}^{(+)}$ (§6), este clar că pentru orice clasă de echivalență $\overline{(a,b)} = \frac{a}{b} \in \mathbb{Q}$ are loc una şi numai una dintre următoarele trei posibilități:

1) clasa $\frac{a}{b}$ este pozitivă;

2) clasa $\frac{a}{b}$ este nulă;

3) clasa $\frac{a}{b}$ este negativă,

adică

$$\mathbb{Q} = \mathbb{Q}^{(-)} \cup \{0\} \cup \mathbb{Q}^{(+)}. \qquad (1)$$

Ca şi în cazul inelului $\mathbb{Z}$, notăm $P = \mathbb{Q}^{(+)} \cup \{0\}$ şi arătăm că $P + P \subseteq P$, $P \cdot P \subseteq P$, $P \cap -P = \{0\}$ şi $P \cup -P = \mathbb{Q}$. Mai întâi să observăm că orice clasă $\frac{a}{b} \in \mathbb{Q}$ poate fi scrisă şi în forma $\frac{-a}{-b}$. Prin urmare, întotdeauna se pot alege reprezentanți ai clasei $\overline{(a,b)} = \frac{a}{b} \in \mathbb{Q}$, astfel încât b să fie pozitiv.

Fie x, y elemente arbitrare din P. Dacă $x = 0$ sau $y = 0$, atunci $x + y = y$ sau, respectiv, $x + y = x$ şi $xy = 0$, deci $x + y \in P$ şi $xy \in P$. Fie acum $x \neq 0 \neq y$, $x = \frac{a}{b}$, $y = \frac{c}{d}$, unde a, b, c, d sunt numere întregi pozitive. Atunci

$$x+y=\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},\ xy=\frac{ac}{bd}.$$

Deoarece ad, bc, ac şi bd sunt pozitive, rezultă $x+y\in\mathbb{Q}^+, xy\in\mathbb{Q}^+$. Definitiv obţinem că $x+y\in P$ şi $xy\in P$. Celelalte două proprietăţi rezultă din (1). Deci P este conul pozitiv al câmpului numerelor raţionale.

Este comodă şi următoarea regulă de comparare a numerelor raţionale cu numitori pozitivi:

$$\frac{a}{b}<\frac{c}{d}\Leftrightarrow ad<bc.$$

Demonstraţia este directă.

Acum definim relaţia de ordine naturală în câmpul $\mathbb{Q}$.

Definiţia 2. *Fie* $r,s\in\mathbb{Q}$. *Punem prin definiţie:*

$$r<s \overset{def}{\Leftrightarrow} s-r\in\mathbb{Q}^{(+)};$$

$$r\le s \overset{def}{\Leftrightarrow} r<s \ \ sau \ \ r=s \ (\Leftrightarrow s-r\in P).$$

Propoziţia 8.1. *Relaţia binară "*$\le$*" este o relaţie de ordine totală pe mulţimea* $\mathbb{Q}$ *a numerelor raţionale.* □

Relaţia binară "$\le$" (Definiţia 2) se numeşte *relaţia de ordine naturală* în câmpul $\mathbb{Q}$ şi este evident că ea reprezintă o extindere a relaţiei similare din $\mathbb{Z}$.

Din teoria generală a inelelor ordonate rezultă

Propoziţia 8.2. *Relaţia de ordine naturală în câmpul* $\mathbb{Q}$ *posedă următoarele proprietăţi:*

1) dacă $r<s$, *atunci* $r+u<s+u$, *pentru orice* $u\in\mathbb{Q}$;

2) dacă $r<s$ *şi* $u>0$, *atunci* $ru<su$;

3) dacă $r<s$, *atunci* $-s<-r$;

4) dacă $0<r<s$, *atunci* $r^2<s^2$. □

În mod obişnuit (vezi §6) se defineşte şi în $\mathbb{Q}$ *modulul* sau *valoarea absolută* a unui număr:

$$|r| = \begin{cases} r, \ dacă & r > 0; \\ 0, \ dacă & r = 0; \\ -r, \ dacă & r < 0. \end{cases}$$

$$|r| \geq 0, \quad |r| = 0 \Leftrightarrow r = 0.$$

Prin reducere la cazul numerelor întregi (Propoziția 6.5) uşor se demonstrează proprietățile:

$$|rs| = |r| \cdot |s|,$$

$$|r + s| \leq |r| + |s|.$$

În §§ 3,6 a fost menționat faptul că sistemele numerice $\mathbb{N}$ şi $\mathbb{Z}$ sunt discrete, adică între două numere succesive de aceste tipuri nu există alt număr din acelaşi sistem. Cu totul altă situație este în câmpul $\mathbb{Q}$, precum se vede din următoarea afirmație.

Propoziția 8.3. *Câmpul numerelor raționale* $\mathbb{Q}$ *posedă* ***proprietatea densității****, adică între oricare două numere raționale există cel puțin un număr rațional.*

Demonstrație. Fie $\frac{a}{b} > \frac{c}{d}$, unde $b > 0$ şi $d > 0$. Atunci numărul $\frac{ad + bc}{2bd}$ este aranjat între cele două numere date:

$$\frac{a}{b} > \frac{ad + bc}{2bd} > \frac{c}{d}.$$

Într-adevăr, din relația $\frac{a}{b} > \frac{c}{d}$ avem $\frac{ad}{bd} > \frac{bc}{bd}$ şi $ad > bc$, adică $ad - bc > 0$. De aceea:

$$\frac{a}{b}-\frac{ad+bc}{2bd}=\frac{2ad-ad-bc}{2bd}=\frac{ad-bc}{2bd}>0 \quad \Rightarrow \quad \frac{a}{b}>\frac{ad+bc}{2bd};$$
$$\frac{ad+bc}{2bd}-\frac{c}{d}=\frac{ad+bc-2bc}{2bd}=\frac{ad-bc}{2bd}>0 \quad \Rightarrow \quad \frac{ad+bc}{2bd}>\frac{c}{d}. \ \square$$

Printre proprietățile sistemelor $\mathbb{N}$ şi $\mathbb{Z}$ care se păstrează în $\mathbb{Q}$ se poate menționa lema lui Arhimede (vezi lemele 3.4 şi 6.3) .

Lema 8.4 ***(lema lui Arhimede pentru câmpul*** $\mathbb{Q}$***).*** *Câmpul numerelor raționale* $\mathbb{Q}$ *este un câmp total ordonat* ***arhimedean****, adică pentru orice numere* $r,s\in\mathbb{Q},s>0,$ *există un număr natural* n*, astfel încât* $ns>r$*.*

*Demonstrație***.** Conform Propoziției 8.1 câmpul $\mathbb{Q}$ este total ordonat. Să arătăm că el este arhimedean. Fie $r=\frac{a}{b}$, $s=\frac{c}{d}$, unde $c>0$, $b>0$ şi $d>0$. Sunt posibile două cazuri:

1) $\frac{a}{b}<\frac{c}{d}$; atunci luăm $n=1$ şi obținem $n\cdot s=n\cdot\frac{c}{d}>\frac{a}{b}=r$;

2) $\frac{a}{b}\geq\frac{c}{d}$; atunci $ad\geq bc>0$ şi, aplicând lema lui Arhimede pentru $\mathbb{Z}$ (vezi Lema 6.3) numerelor ad şi $bc>0$, găsim un număr natural $n\in\mathbb{N}$, astfel încât $nbc>ad,$ de unde obținem (înmulțind cu $\frac{1}{bd}$):

$$n\cdot\frac{c}{d}>\frac{a}{b},$$

adică $ns>r$. $\square$

Acum vom arăta o proprietate specifică a câmpului $\mathbb{Q}$ care îl deosebeşte printre alte câmpuri şi semnalează în anumit sens „omnipotenţa" lui. Mai întâi amintim următoarea noţiune.

Definiţia 3. ***Caracteristică*** *a câmpului* K *(**char** K) se numeşte:*

- *numărul zero, dacă* $na \neq 0$ *pentru orice* $a \in K, a \neq 0$ *şi* $n \in \mathbb{N}$, $n \neq 0$;
- *numărul prim* p *dacă* $pa = 0$ *pentru orice* $a \in K$.

Câmpul K se numeşte *prim* dacă el nu are subcâmpuri proprii (adică diferite de K).

Propoziţia 8.5. *Câmpul numerelor raţionale este un câmp prim. Orice câmp* P *de caracteristică zero conţine un singur subcâmp* P' *care este izomorf cu câmpul numerelor raţionale* $\mathbb{Q}$.

Demonstraţie. Orice subcâmp netrivial $\mathbb{Q}'$ al câmpului $\mathbb{Q}$ este, prin definiţie, o submulţime în $\mathbb{Q}$, închisă în raport cu cele 4 operaţii din $\mathbb{Q}$, de aceea conţine atât unitatea $1_{\mathbb{Q}}$, cât şi toţi multiplii ei $n \cdot 1_{\mathbb{Q}}, n \in \mathbb{Z}$, adică conţine $\mathbb{Z}$. Prin urmare, $\mathbb{Q}'$ conţine şi toate câturile $\frac{a}{b}$ pentru $a, b \in \mathbb{Z}$, $b \neq 0$, de aceea $\mathbb{Q}' = \mathbb{Q}$.

Fie P un câmp arbitrar cu $\operatorname{char} P = 0$. Notăm prin e elementul unitate al acestui câmp şi separăm în P submulţimea:

$$\mathbb{Z}' = \{ne \mid n \in \mathbb{Z}\}.$$

Din condiţia $\operatorname{char} P = 0$ avem: $ne \neq 0$, pentru orice număr nenul $n \in \mathbb{Z}$ şi $n_1 e \neq n_2 e$, dacă $n_1 \neq n_2$. Prin urmare, aplicaţia

$$f : \mathbb{Z} \to \mathbb{Z}', \ f(n) = ne,$$

determină un izomorfism de inele: $\mathbb{Z} \cong \mathbb{Z}' \subseteq P$. Definim înmulţirea numerelor raţionale cu elementele din P astfel:

$$\frac{a}{b}\cdot e \overset{def}{=} \frac{ae}{be},\ \frac{a}{b}\cdot x \overset{def}{=} (\frac{a}{b}\cdot e)\cdot x,$$

unde $x \in P,$ iar înmulțirea şi împărțirea se efectuează în P. Considerăm în P submulțimea:

$$\mathbb{Q}' = \left\{ \frac{a}{b}\cdot e \,|\, \frac{a}{b} \in \mathbb{Q} \right\}.$$

Utilizând din nou condiția $\operatorname{char} P = 0$, obținem izomorfismul $\mathbb{Q}' \cong \mathbb{Q}$ definit de aplicația

$$f\left(\frac{a}{b}\right) = \frac{a}{b}\cdot e$$

Astfel, P conține un subcâmp $\mathbb{Q}'$ izomorf cu $\mathbb{Q}$. Mai mult, acest $\mathbb{Q}'$ este *unicul subcâmp* în P cu această proprietate: dacă mai avem un subcâmp $\mathbb{Q}'' \subseteq P$ cu $\mathbb{Q}'' \cong \mathbb{Q},$ atunci $\mathbb{Q}''$ este obligat să conțină şi $e \in P,$ deci şi toți multiplii ei ne (adică $\mathbb{Z}'$), prin urmare şi toate elementele $\frac{ne}{me}$ (adică $\mathbb{Q}'$). Din ipoteza $\mathbb{Q}'' \cong \mathbb{Q},$ rezultă că $\mathbb{Q}''$ este prim, prin urmare, $\mathbb{Q}' = \mathbb{Q}''$. □

Teoria divizibilității pentru câmpul numerelor raționale $\mathbb{Q}$, ca şi pentru orice câmp, este trivială şi se reduce la faptul evident că orice număr se împarte (fără rest) la orice număr nenul (aceasta explică faptul că pentru $\mathbb{Q}$ nu se demonstrează rezultatul similar teoremei împărțirii cu rest).

Finisăm acest paragraf cu o observație referitoare la aranjamentul pe axa numerică a numerelor din $\mathbb{Q}$ în raport cu cele din $\mathbb{Z}$.

Propoziția 8.6. *Pentru orice număr rațional* $\frac{a}{b} \in \mathbb{Q}$, *există un număr întreg* $q \in \mathbb{Z}$ *astfel încât*

$$q \le \frac{a}{b} < q+1$$

(adică orice număr raţional se află între două numere întregi consecutive).

Demonstraţie. Fie $\frac{a}{b} \in \mathbb{Q}$ şi $b > 0$. Aplicăm teorema împărţirii cu rest în $\mathbb{Z}$ (teorema 6.6) numerelor a şi b: există $q, r \in \mathbb{Z}$, astfel încât $a = qb + r$, $0 \le r < |b| = b$. Atunci $\frac{a}{b} = q + \frac{r}{b}$ şi din relaţia $r < |b| = b$ avem $\frac{r}{b} < 1$, deci $q \le \frac{a}{b} < q + 1$. □

Exerciţii

1. Demonstraţi că pentru orice două numere raţionale r şi s avem:
   a) $|r + s| \le |r| + |s|$,
   b) $|rs| = |r| \cdot |s|$.
2. Demonstraţi Propoziţia 8.1 si Propoziţia 8.2.
3. Demonstraţi că mulţimea numerelor raţionale $\mathbb{Q}$ este echivalentă cu:
   a) mulţimea numerelor naturale pare;
   b) mulţimea numerelor naturale divizibile cu un număr natural dat.
4. Fie date numerele raţionale $\frac{7}{15}$ si $\frac{8}{15}$. Înscrieţi între ele trei numere raţionale cu ajutorul semnului „<”. Câte numere raţionale pot fi înscrise în acest mod între două numere raţionale diferite?
5. Demonstraţi că nu există un număr raţional, pătratul căruia să fie egal cu 3.
6. Fie $\frac{a}{b}$ un număr raţional pozitiv. Demonstraţi că $\frac{a}{b} + \frac{b}{a} \ge 2$.
7. Demonstraţi că suma fracţiilor $\frac{1}{n+1}, \frac{1}{n+2}, \ldots, \frac{1}{2n}$ este mai mare ca $\frac{1}{2}$, pentru orice număr natural $n \ge 1$.

8. Demonstrați că:

a) pentru orice număr natural nenul n, numărul $\frac{10^n+2}{3}$ este întreg;

b) pentru orice număr natural nenul n, numerele $\frac{n-4}{21}$ si $\frac{n-3}{12}$ nu pot fi simultan întregi;

c) $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\ldots+\frac{1}{n(n-1)}=\frac{n}{n+1}$.

9. Poate oare suma a două fracții să fie egală cu produsul lor? Dacă da, atunci care este forma acestor fracții?

10. Poate oare diferența a două fracții să fie egală cu produsul lor? Dacă da, atunci care este forma acestor fracții?

11. Să se demonstreze că ecuația $x^3-kx+1=0$ nu are rădăcini raționale, pentru orice $k\in\mathbb{N}$, $k>2$.

Capitolul IV

Numere reale

§9. Necesitatea extinderii câmpului numerelor raționale. Şiruri fundamentale

Până în prezent am efectuat două extinderi ale sistemelor numerice : $\mathbb{N} \to \mathbb{Z} \to \mathbb{Q}$, motivându-le prin necesitatea existenței operațiilor inverse adunării şi înmulțirii. Astfel, în $\mathbb{Q}$ ca şi în orice câmp, avem patru operații. Mai mult, se poate spune că câmpul $\mathbb{Q}$ este satisfăcător şi din punct de vedere practic: orice măsurare poate fi efectuată prin numere raționale cu orice grad de exactitate (cu orice precizie).

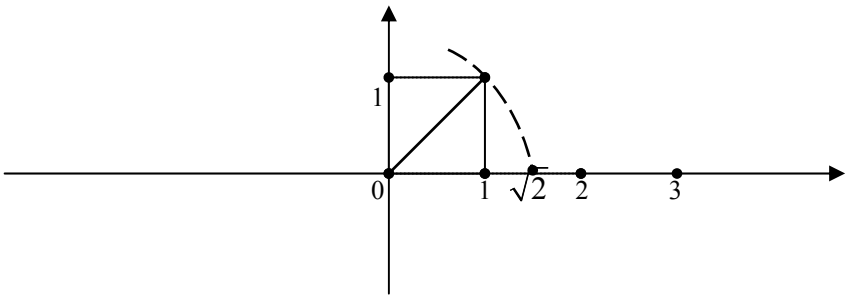
Dar dezvoltarea matematicii a arătat că câmpul $\mathbb{Q}$ are un şir de „defecte", pentru înlăturarea cărora este necesar de lărgit acest câmp. În continuare vom expune câteva argumente în folosul unei astfel de extinderi. Mai concret, vom arăta că numerele raționale nu sunt suficiente pentru rezolvarea unor probleme din algebră şi geometrie.

a) În câmpul $\mathbb{Q}$ este imposibilă extragerea rădăcinii din unele numere. De exemplu, dacă p este un număr natural prim şi $n \in \mathbb{N}, n > 1,$ atunci numărul $\sqrt[n]{p}$ (adică numărul x astfel încât $x^n = p$) nu poate fi un număr rațional $\frac{a}{b}$, unde $a, b \in \mathbb{Z}, b \neq 0$.

b) Numerele raționale sunt insuficiente pentru măsurarea segmentelor. Să amintim că *măsură comună* a două segmente se numeşte segmentul care se cuprinde de un număr natural de ori în ambele segmente. Dacă două segmente au măsură comună, atunci ele se numesc *comensurabile*, iar în caz contrar - *incomensurabile*. Este uşor de verificat că lungimea unui segment a în etalonul de lungime e este un număr rațional dacă şi numai dacă segmentele a şi e sunt comensurabile. Dar încă din antichitate este cunoscut

faptul că există segmente incomensurabile, de exemplu, latura unui pătrat este incomensurabilă cu diagonala lui. Aceasta arată că pentru măsurarea segmentelor este necesară lărgirea câmpului $\mathbb{Q}$.

c) Numerele raționale nu completează toată dreapta numerică, adică există „goluri" pe aceasta dreaptă. Într-adevăr, reprezentând numerele raționale pe dreapta numerică, găsim puncte cărora nu le corespunde nici un număr rațional, de exemplu, capătul din dreapta al segmentului egal cu diagonala pătratului din desenul de mai jos:



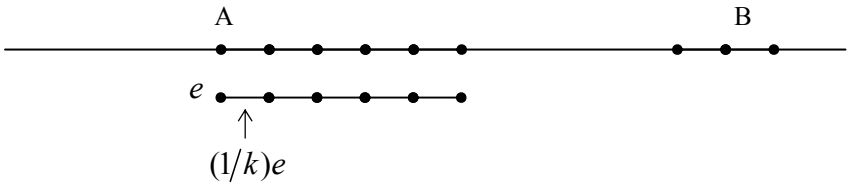
d) Există fracții zecimale care nu reprezintă nici un număr rațional. Într-adevăr, trecând de la fracții ordinare $\frac{m}{n}$ la cele zecimale (adică efectuând împărțirea lui m prin n în sistemul zecimal), sunt posibile 2 cazuri: sau fracția obținută este finită, sau ea este infinită, dar în acest caz ea este neapărat periodică (deoarece resturi pot fi doar numerele $0,1,...,n-1$, deci cel mult peste n paşi un rest se va repeta, dar atunci şi la cât numărul se va repeta). Pe de altă parte, uşor se poate arăta o fracție zecimală infinită, care nu este periodică, de exemplu, 0,1001000100001 ... Este clar că această fracție nu poate fi obținută nici dintr-un număr rațional $\frac{m}{n}$.

Din cele expuse mai sus putem face concluzia că pentru rezolvarea unor probleme din algebră şi geometrie este necesară extinderea sistemului de numere raționale $\mathbb{Q}$.

Pentru a preciza sarcina ce ne revine şi a găsi căile de îndeplinire a ei, să analizăm mai amănunţit următoarele două probleme.

Problema 1: m*ăsurarea segmentelor*.

Fie că pe o dreaptă avem un segment AB şi un etalon de lungime e:



Fixăm un număr natural $k > 0$ (baza sistemului de numeraţie, de exemplu $k = 10$) şi împărţim etalonul în k părţi egale. Depunem segmentul $\frac{1}{k}e$ pe segmentul AB din punctul A spre B. Atunci există un număr natural p_1 încât

$$\frac{p_1}{k}e \le AB < \frac{p_1+1}{k}e,$$

adică pentru lungimile acestor segmente are loc relaţia

$$a_1 = \frac{p_1}{k} \le l(AB) < \frac{p_1+1}{k} = b_1, \quad b_1 - a_1 = \frac{1}{k}$$

(aici este aplicată lema lui Arhimede pentru $l(AB)$ şi $\frac{1}{k}e$). Numărul $a_1 = \frac{p_1}{k}$ se numeşte *lungimea aproximativă* a segmentului AB *prin lipsă* cu exactitatea $\frac{1}{k}$; în mod similar, numărul $b_1 = \frac{p_1+1}{k}$ se numeşte *lungimea aproximativă* a segmentului AB *prin adaos* cu exactitatea $\frac{1}{k}$.

Continuăm măsurarea, luând la următorul pas în locul numărului k numărul k^2. În mod similar obținem lungimi aproximative cu exactitatea de $\frac{1}{k^2}$:

$$a_2 = \frac{p_2}{k^2} \le l(AB) < \frac{p_2+1}{k^2} = b_2, \quad b_2 - a_2 = \frac{1}{k^2}.$$

Procedăm în mod analog pentru numerele $k^3, k^4, \ldots, k^n, \ldots$ şi obținem două şiruri de numere raționale:

$$a_1 \le a_2 \le \ldots \le a_n \le \ldots , \tag{1}$$

$$b_1 \ge b_2 \ge \ldots \ge b_n \ge \ldots , \tag{2}$$

unde primul este un şir ascendent ce tinde de jos spre $l(AB)$, iar al doilea este un şir descendent care tinde de sus spre $l(AB)$. Este evident că

$$b_n - a_n = \frac{p_n+1}{k^n} - \frac{p_n}{k^n} = \frac{1}{k^n}$$

şi această diferență tinde spre zero, când n tinde spre infinit, adică: $\forall \varepsilon > 0\ (\varepsilon \in \mathbb{Q}), \exists n_0 \in \mathbb{N}$, astfel încât

$$\forall n, m > n_0, \quad |a_n - a_m| < \varepsilon. \tag{3}$$

Din cele expuse rezultă următoarea *concluzie*: dacă segmentul AB este incomensurabil cu segmentul unitar e, atunci şirurile (1) şi (2) sunt infinite şi ambele au în calitate de limită numărul $l(AB)$ care nu aparține câmpului numerelor raționale $\mathbb{Q}$. Şirurile cu proprietatea de condensare (3) se vor numi *fundamentale* şi astfel, în acest caz, avem şirurile fundamentale (1) şi (2) de numere raționale, limita cărora nu este un număr rațional.

Problema 2: *extragerea rădăcinilor*.

Fie $a \in \mathbb{Q}\ (a > 0)$ şi se cere de aflat numărul $\sqrt[k]{a}$ $(k > 1, k \in \mathbb{N})$ adică un număr x încât $x^k = a$. Pentru simlpicitate vom

folosi sistemul zecimal şi vom căuta numai valoarea pozitivă a rădăcinii.

Primul pas: aplicăm lema lui Arhimede pentru numerele $a+1$ şi $\frac{1}{10}>0,$ găsind un număr $m\in\mathbb{N}$ astfel încât $m\cdot\frac{1}{10}>a+1.$ Atunci:

$$\left(m\cdot\frac{1}{10}\right)^k>m\cdot\frac{1}{10}>a+1>a\,,$$

deci mulțimea numerelor naturale

$$A=\left\{l\in\mathbb{N}\,|\left(l\cdot\frac{1}{10}\right)^k\le a\right\}$$

este mărginită de sus (de exemplu, de numărul m), de aceea posedă cel mai mare număr, fie acesta a_1' :

$$\left(a_1'\cdot\frac{1}{10}\right)^k\le a<\left(\left(a_1'+1\right)\cdot\frac{1}{10}\right)^k.$$

Notând $a_1=a_1'\cdot\frac{1}{10}$ şi $b_1=\left(a_1'+1\right)\cdot\frac{1}{10},$ avem

$$a_1^{\,k}\le a<b_1^{\,k},b_1-a_1=\frac{1}{10}.$$

Acum este clar că numărul căutat se află între a_1 şi b_1:

$$a_1\le\sqrt[k]{a}<b_1.$$

Vom numi:

a_1 valoarea aproximativă a lui $\sqrt[k]{a}$ *prin lipsă* cu exactitate de $\frac{1}{10}$;

b_1 valoarea aproximativă a lui $\sqrt[k]{a}$ *prin adaos* cu exactitate de $\frac{1}{10}$.

Pasul al doilea: în mod similar pentru $\frac{1}{10^2}$ obținem situația

$$a_2\le\sqrt[k]{a}<b_2,\quad b_2-a_2=\frac{1}{10^2},$$

având valorile aproximative ale lui $\sqrt[k]{a}$ cu exactitatea de $\frac{1}{10^2}$. La pasul n vom obține numerele a_n, b_n cu condiția

$$a_n \le \sqrt[k]{a} < b_n, \quad b_n - a_n = \frac{1}{10^n}.$$

Continuând procesul, vom avea două şiruri de numere raționale :

$$a_1 \le a_2 \le ... \le a_n \le ... \tag{4}$$

$$b_1 \ge b_2 \ge ... \ge b_n \ge ..., \tag{5}$$

unde primul este un şir ascendent ce tinde spre $\sqrt[k]{a}$ (aproximarea prin lipsă), iar al doilea este un şir descendent ce tinde spre $\sqrt[k]{a}$ (aproximarea prin adaos). Din construcție este clar că $b_n - a_n$ tinde spre zero când n tinde spre infinit. La fel de evident este faptul că ambele aceste şiruri satisfac condiția de condensare (3).

Astfel din analiza precedentă putem face concluzia:
dacă numărul $\sqrt[k]{a}$ nu este rațional (vezi punctul a)), atunci ambele şiruri (4) şi (5) sunt şiruri infinite şi fundamentale de numere raționale, ce au drept limită numărul $\sqrt[k]{a}$ care nu aparține câmpului $\mathbb{Q}$.

Finisând scurta cercetare a problemelor 1 şi 2 , putem spune că pentru rezolvarea lor ce cere completarea câmpului $\mathbb{Q}$ astfel încât să fie posibilă o nouă operație - *trecerea la limită* în noul câmp, asigurând proprietatea: orice şir de numere cu proprietatea de condensare (3) să aibă limită în acest câmp.

Există diverse metode de efectuare a unei astfel de extinderi, de exemplu, Dedekind a propus aşa numita *metodă a secțiunilor*. Noi vom expune o altă metodă (construcția lui Georg Cantor), bazată pe şirurile fundamentale de numere raționale.

Pentru cele ce urmează avem nevoie de unele rezultate preliminare, pe care le vom expune într-un cadru mai general - pentru un câmp total ordonat P ce conține $\mathbb{Q}$.

Fie P un câmp cu relația de ordine „$\leq$”, compatibilă cu operațiile (+) şi $(\cdot)$ din P. Atunci în mod obişnuit se poate defini *modulul* sau *valoarea absolută* a elementului $a \in P$.

Câmpul P se numeşte *arhimedean ordonat* dacă este satisfăcută *lema lui Arhimede*: *pentru orice* $a \in P$ *şi orice* $b \in P$, $b > 0$, *există un număr natural* $n > 0$ *astfel încât* $nb > a$.

Şir de elemente din P se numeşte orice funcție f cu $f(n) = a_n \in P$, definită pe numerele naturale $\{1, 2, ..., n, ...\}$ cu valori în P şi scrise în forma: $a_1, a_2, ..., a_n, ...$; $\{a_n\}_{n=1}^{\infty}$ sau, simplu, $\{a_n\}$. Şirul de forma $a, a, ..., a, ...$ se numeşte şir *staționar* şi se mai notează $\{a\}$. Elementul $a \in P$ se numeşte *limită* a şirului $\{a_n\}$ de elemente din P dacă pentru orice $\varepsilon > 0$ $(\varepsilon \in P)$ există un număr natural n_0 (ce depinde de ε), astfel încât pentru orice $n > n_0$, are loc relația:

$$|a - a_n| = |a_n - a| < \varepsilon .$$

Se notează: $\lim\{a_n\} = a$. Dacă şirul $\{a_n\}$ posedă limită atunci el se numeşte *şir convergent*. Se verifică imediat unicitatea limitei.

Propoziția 9.1. *Orice şir convergent din câmpul* P *are o singură limită.*

Demonstrație. Dacă $a = \lim\{a_n\}$, $b = \lim\{a_n\}$ şi $b \neq a$ atunci, luând $\varepsilon = \dfrac{|a-b|}{2} > 0$, din definiția limitei avem existența a două numere n_1 şi n_2, astfel încât:

$$|a_n - a| < \frac{|a-b|}{2}, \quad \forall n > n_1,$$

$$|a_n - b| < \frac{|a-b|}{2}, \quad \forall n > n_2.$$

Atunci pentru $n_0 = \max(n_1, n_2)$ avem :

$$|a-b| = |(a-a_n)+(a_n-b)| \le |a-a_n| +$$

$$+(a_n-b) < \frac{|a-b|}{2} + \frac{|a-b|}{2} = |a-b|,$$

pentru orice $n > n_0$, ceea ce este o contradicție. □

Următoarea noțiune joacă un rol central în construcțiile ce urmează.

Definiția 1. *Şirul* $\{a_n\}$ *de elemente din* P *se numeşte* ***fundamental*** *(sau şir Cauchy) dacă pentru orice* $\varepsilon > 0 \quad (\varepsilon \in P)$ *există un număr natural* n_0 *astfel încât pentru orice* $n > n_0$ *şi orice număr natural* p *are loc relația*

$$|a_{n+p} - a_n| < \varepsilon.$$

(Altă formă a acestei condiții: pentru orice $\varepsilon > 0 \quad (\varepsilon \in P)$ *există un număr* n_0 *astfel încât pentru orice* $m, n > n_0$ *avem* $|a_m - a_n| < \varepsilon$ *).*

Propoziția 9.2. *Orice şir convergent de elemente din câmpul* P *este fundamental.*

Demonstrație. Fie $\{a_n\}$ un şir convergent şi $\lim\limits_{n\to\infty}\{a_n\} = a$. Atunci, conform definiției, pentru orice $\varepsilon > 0 \quad (\varepsilon \in P)$ există un număr natural n_0 astfel încât $|a_n - a| < \frac{\varepsilon}{2}$ pentru orice $n > n_0$. De aceea pentru $n > n_0$ şi orice număr natural p avem:

$$|a_{n+p} - a_n| = |a_{n+p} - a + a - a_n| \le |a_{n+p} - a| + |a - a_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

deci şirul $\{a_n\}$ este fundamental. □

Astfel condiția de a fi şir fundamental este necesară pentru convergența lui în P, dar nu este şi suficientă. De exemplu, şirurile (1), (2), (4) şi (5), sunt în mod evident fundamentale în $\mathbb{Q}$, dar în cazurile specificate anterior nu au limită în câmpul $\mathbb{Q}$.

Pentru cele ce vor urma este util de menționat unele proprietăți ale operației de trecere la limită .

Propoziția 9.3. 1*) Fie* $\{a_n\}$ *şi* $\{b_n\}$ *două şiruri din câmpul* P. *Dacă şirul* $\{a_n\}$ *este convergent şi* $\lim\{a_n - b_n\} = 0$, *atunci şi şirul* $\{b_n\}$ *este convergent cu aceeaşi limită:* $\lim\{a_n\} = \lim\{b_n\}$.

2) Dacă şirurile $\{a_n\}$ *şi* $\{b_n\}$ *sunt convergente atunci:*

a) $\lim\{a_n \pm b_n\} = \lim\{a_n\} \pm \lim\{b_n\}$;

b) $\lim\{a_n b_n\} = \lim\{a_n\} \cdot \lim\{b_n\}$;

c) $\lim\left\{\dfrac{a_n}{b_n}\right\} = \dfrac{\lim\{a_n\}}{\lim\{b_n\}}$ *dacă* $\lim\{b_n\} \neq 0$ *şi* $\{b_n\} \neq 0$, $\forall n \in \mathbb{N}$.

Demonstrația se reduce la verificare directă. □

Exerciții

1. Demonstrați propoziția 9.3.

§10. Proprietăți ale şirurilor fundamentale de numere raționale

În acest paragraf vom cerceta şirurile fundamentale de numere raționale şi vom arăta unele proprietăți ale lor, necesare pentru construcțiile ulterioare.

Propoziția 10.1. *Orice şir fundamental de numere raționale* $\{a_n\}$ *este mărginit, adică există un număr rațional* $M > 0$ *încât* $|a_n| < M$ *pentru orice* n.

Demonstrație. Deoarece $\{a_n\}$ este un şir fundamental, pentru $\varepsilon = 1$ există un număr natural n_0 astfel încât $|a_m - a_{n_0+1}| < 1$ pentru orice $m > n_0$. Atunci avem:

$$|a_m| = |a_{n_0+1} + a_m - a_{n_0+1}| \le |a_{n_0+1}| + |a_m - a_{n_0+1}| < |a_{n_0+1}| + 1,$$

pentru orice $m > n_0$.

Luând un număr rațional pozitiv M cu proprietatea:

$$M > \max\left\{|a_1|, |a_2|..., |a_{n_0}|, |a_{n_0+1}| + 1\right\}.$$

avem $|a_m| < M$, pentru orice m. □

Notăm prin $\mathcal{F}$ *mulțimea tuturor şirurilor fundamentale* de numere raționale. Vom cerceta această mulțime, introducând pe ea diferite operații algebrice.

Definiția 1. ***Sumă***, ***diferență*** *şi* ***produs*** *a două şiruri fundamentale de numere raționale* $\{a_n\}$ *şi* $\{b_n\}$ *se numesc, respectiv, şirurile:*

$$\{a_n + b_n\}, \quad \{a_n - b_n\}, \quad \{a_n b_n\}.$$

Propoziția 10.2. *Suma, diferența şi produsul a două şiruri fundamentale sunt şiruri fundamentale.*

Demonstrație. Fie $\{a_n\}, \{b_n\} \in \mathcal{F}$ şi $\varepsilon > 0 \left(\varepsilon \in \mathbb{Q}\right)$. Alegem un număr n_0 astfel încât:

$$|a_{n+p} - a_n| < \frac{\varepsilon}{2}, \quad |b_{n+p} - b_n| < \frac{\varepsilon}{2},$$

pentru orice $n \geq n_0$ şi orice $p \in \mathbb{N}$. Atunci avem:

$$\left|\left(a_{n+p} \pm b_{n+p}\right) - \left(a_n \pm b_n\right)\right| = \left|\left(a_{n+p} - a_n\right) \pm \left(b_{n+p} - b_n\right)\right| \leq$$

$$\leq \left|a_{n+p} - a_n\right| + \left|b_{n+p} - b_n\right| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

deci $\left\{a_n \pm b_n\right\}$ este un şir fundamental.

Verificăm afirmaţia pentru produsul a două şiruri. Fie $\{a_n\}, \{b_n\} \in \mathcal{F}$. Atunci aceste şiruri sunt mărginite (Propoziţia 10.1), de aceea există un număr raţional pozitiv M încât $\left|a_n\right| < M$ şi $\left|b_n\right| < M$, pentru orice n natural. Deoarece şirurile date sunt fundamentale, pentru orice $\varepsilon > 0$ există un număr n_0 astfel încât:

$$\left|a_{n+p} - a_n\right| < \frac{\varepsilon}{2M}, \quad \left|b_{n+p} - b_n\right| < \frac{\varepsilon}{2M},$$

pentru orice $n > n_0$ şi orice $p \in \mathbb{N}$. Prin urmare, pentru produsul şirurilor obţinem:

$$\left|a_{n+p}b_{n+p} - a_n b_n\right| = \left|a_{n+p}b_{n+p} - a_{n+p}b_n + a_{n+p}b_n - a_n b_n\right| \leq$$

$$\leq \left|a_{n+p}\right|\left|b_{n+p} - b_n\right| + \left|b_n\right|\left|a_{n+p} - a_n\right| <$$

$$< M \cdot \frac{\varepsilon}{2M} + M \cdot \frac{\varepsilon}{2M} = \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

pentru $\forall\ n > n_0$, ceea ce arată că şirul $\left\{a_n b_n\right\}$ este fundamental. □

Din definiţia 1 se vede că proprietăţile operaţiilor din $\mathbb{Q}$ pot fi transferate la operaţiile din $\mathcal{F}$.

Corolarul 10.3. *Operaţiile de* a*dunare şi înmulţire a şirurilor fundamentale sunt comutative şi asociative. Mai mult, înmulţirea este distributivă în raport cu adunarea.* □

Acum avem nevoie de analogul numărului 0 din $\mathbb{Q}$ - elementul neutru în raport cu adunarea din $\mathcal{F}$.

Definiția 2. *Şirul de numere raționale* $\{a_n\}$ *se numeşte* ***şir nul*** *dacă el converge către zero:* $\lim\{a_n\} = 0$.

Evident, orice şir nul este fundamental, deci şi mărginit.

Propoziția 10.4. *Suma şi diferența a două şiruri nule sunt şiruri nule. Produsul oricărui şir fundamental cu un şir nul este un şir nul.*

Demonstrație. Prima afirmație rezultă din Propopoziția 9.3, p.2a).

Fie $\{a_n\}$ un şir nul şi $\{b_n\} \in \mathcal{F}$. Atunci $\{b_n\}$ este mărginit (Propopoziția 10.1), adică $|b_n| < M$, pentru un număr rațional $M > 0$ şi orice n . Deoarece şirul $\{a_n\}$ este nul, pentru orice $\varepsilon > 0$ există un număr n_0 astfel încât $|a_n| < \dfrac{\varepsilon}{M}$ pentru orice $n > n_0$. Prin urmare:

$$|a_n b_n| = |a_n| \cdot |b_n| < \frac{\varepsilon}{M} \cdot M = \varepsilon ,$$

pentru orice $n > n_0$, ceea ce înseamnă că $\lim\{a_n b_n\} = 0$. □

Ca şi în sistemele numerice cercetate până acum, în mulțimea $\mathcal{F}$ a şirurilor fundamentale de numere raționale se pot defini elemente pozitive şi negative.

Definiția 3. *Şirul fundamental de numere raționale* $\{a_n\}$ *se numeşte* ***pozitiv*** *dacă există un număr rațional* $\varepsilon > 0$ *şi un număr natural* n_0 *încât* $a_n > \varepsilon$ *pentru orice* $n > n_0$. *Dacă* $\{a_n\}$ *este un şir*

pozitiv, atunci şirul $\{b_n\} = \{-a_n\}$ *se numeşte* ***negativ*** *(adică toate elementele lui, începând cu un anumit* b_{n_0}*, sunt numere negative, mai mici decât un număr fixat negativ).*

Notăm :

$\mathcal{F}^{(+)}$ – mulțimea tuturor şirurilor fundamentale *pozitive*;

$\mathcal{F}^{(-)}$ – mulțimea tuturor şirurilor fundamentale *negative*.

Să studiem comportamentul acestor tipuri de şiruri în raport cu operațiile din definiția 1.

Propoziția 10.5. *1) Suma şi produsul a două şiruri fundamentale pozitive sunt şiruri fundamentale pozitive.*

2) Suma a două şiruri fundamentale negative este un şir fundamental negativ.

3) Produsul a două şiruri fundamentale negative este un şir fundamental pozitiv.

4) Produsul unui şir fundamental pozitiv cu un şir fundamental negativ este un şir fundamental negativ.

Demonstrație. 1) Fie $\{a_n\}, \{b_n\} \in \mathcal{F}^{(+)}$. Atunci prin definiție:

$$\exists n_1, \exists \varepsilon_1 > 0 \quad (\varepsilon_1 \in \mathbb{Q}): \quad a_n > \varepsilon_1, \quad \forall n > n_1;$$

$$\exists n_2, \exists \varepsilon_2 > 0 \quad (\varepsilon_2 \in \mathbb{Q}): \quad b_n > \varepsilon_2, \quad \forall n > n_2.$$

Luând $n_0 = \max\{n_1, n_2\}$, obținem că pentru orice $n > n_0$:

$$a_n + b_n > \varepsilon_1 + \varepsilon_2 > 0, \quad a_n b_n > \varepsilon_1 \varepsilon_2 > 0.$$

Afirmațiile 2), 3) şi 4) se verifică în mod similar. □

Propoziția 10.6 (***legea trihotomiei în*** $\mathcal{F}$*). Pentru orice şir fundamental* $\{a_n\} \in \mathcal{F}$ *are loc una şi numai una dintre următoarele trei posibilități:*

a) $\{a_n\} \in \mathcal{F}^{(+)}$

b) $\{a_n\}$ *este un şir nul;*

c) $\{a_n\} \in \mathcal{F}^{(-)}$

Prin urmare , $\mathcal{F} = \mathcal{F}^{(+)} \cup \{0\} \cup \mathcal{F}^{(-)}$.

Demonstraţie. Este clar că a) şi c) se exclud reciproc. Rămâne de arătat că dacă $\{a_n\}$ nu este nici pozitiv şi nici negativ, atunci el este un şir nul.

Fie $\{a_n\} \in F$ şi fie că nici acest şir, nici opusul lui $\{-a_n\}$, nu este pozitiv. Atunci pentru orice $\varepsilon > 0$ $(\varepsilon \in \mathbb{Q})$ şi orice număr natural n_0 există numerele naturale $n_1 > n_0$ şi $n_2 > n_0$ încât

$$a_{n_1} \le \frac{\varepsilon}{2} \quad \text{şi} \quad -a_{n_2} \le \frac{\varepsilon}{2}. \tag{1}$$

Acum utilizăm faptul că şirurile $\{a_n\}$ şi $\{-a_n\}$ sunt fundamentale: pentru acest $\varepsilon > 0$ putem alege n_0 încât pentru numerele $n_1 > n_0$, $n_2 > n_0$ şi pentru orice $n > n_0$ să aibă loc inegalităţile:

$$\left|a_n - a_{n_1}\right| < \frac{\varepsilon}{2}, \quad \left|a_n - a_{n_2}\right| < \frac{\varepsilon}{2}. \tag{2}$$

Din relaţiile (1) şi (2), pentru orice $n > n_0$, avem :

$$a_n = a_n - a_{n_1} + a_{n_1} \le \left|a_n - a_{n_1}\right| + a_{n_1} < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon;$$

$$-a_n = a_{n_2} - a_n - a_{n_2} \le \left|a_{n_2} - a_n\right| - a_{n_2} < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Prin urmare, $\left|a_n\right| < \varepsilon$ pentru orice $n > n_0$. Deoarece $\varepsilon > 0$ este un număr arbitrar, din această relaţie rezultă că $\{a_n\}$ este un şir nul. □

În încheierea acestui compartiment considerăm încă o operaţie în mulţimea $\mathcal{F}$: *împărţirea* şirurilor fundamentale de numere raţionale.

Propoziția 10.7. *Fie* $\{a_n\},\{b_n\}\in\mathcal{F}$, *unde* $\{b_n\}$ *nu este un şir nul şi* $b_n\neq 0$ *pentru orice* n. *Atunci şi şirul cât* $\left\{\frac{a_n}{b_n}\right\}\in\mathcal{F}$.

Demonstrație. Şirul $\{a_n\}$ este mărginit (Propoziția 10.1), de aceea există un număr $M\in\mathbb{Q},\quad M>0$, încât $|a_n|<M$ pentru orice n. Şirul $\{b_n\}$ nu este nul, de aceea există $\varepsilon>0$ ($\varepsilon\in\mathbb{Q}$) şi un număr n_1 astfel încât $|b_n|>\varepsilon$ pentru orice $n>n_1$. Deoarece şirurile date sunt fundamentale, avem: pentru orice $\varepsilon_1>0$ există n_2 încât:

$$|a_{n+p}-a_n|<\frac{\varepsilon_1\varepsilon}{2}$$

pentru orice $n>n_2$ şi orice p, şi există n_3, încât:

$$|b_{n+p}-b_n|<\frac{\varepsilon_1\varepsilon^2}{2M}$$

pentru orice $n>n_3$ şi orice p.

Luând $n_0=\max\{n_1,n_2,n_3\}$, pentru orice $n>n_0$ avem:

$$\left|\frac{a_{n+p}}{b_{n+p}}-\frac{a_n}{b_n}\right|=\left|\frac{a_{n+p}}{b_{n+p}}-\frac{a_{n+p}}{b_n}+\frac{a_{n+p}}{b_n}-\frac{a_n}{b_n}\right|=$$

$$=\left|\frac{a_{n+p}(b_n-b_{n+p})}{b_{n+p}b_n}+\frac{a_{n+p}-a_n}{b_n}\right|\leq$$

$$\leq|a_{n+p}|\frac{|b_n-b_{n+p}|}{|b_{n+p}||b_n|}+\frac{|a_{n+p}-a_n|}{|b_n|}<$$

$$<M\cdot\frac{\varepsilon_1\varepsilon^2}{2M\varepsilon^2}+\frac{\varepsilon_1\varepsilon}{2\varepsilon}=\frac{\varepsilon_1}{2}+\frac{\varepsilon_1}{2}=\varepsilon_1.$$

Aceasta arată că şirul $\left\{\frac{a_n}{b_n}\right\}$ este fundamental. □

Exerciții

1. Demonstrați afirmațiile 2), 3) si 4) din propoziția 10.5.
2. Demonstrați Corolarul 10.3.

§ 11. Câmpul numerelor reale $\mathbb{R}$ (unicitatea)

Scopul următoarelor investigații este trecerea la un nou sistem numeric (sistemul numerelor reale $\mathbb{R}$), utilizând şiruri fundamentale de numere raționale, cu intenția de a lichida „defectele" câmpului $\mathbb{Q}$, indicate în § 9. Acolo s-a stabilit că cel mai mare „păcat" al lui $\mathbb{Q}$ constă în aceea că nu orice şir fundamental cu elemente din $\mathbb{Q}$ are limită în acest câmp.

Definiția 1. *Câmpul liniar ordonat P se numeşte **complet** dacă orice şir fundamental de elemente din P are limită în acest câmp.*

Câmpul numerelor raționale $\mathbb{Q}$ nu este complet: şirurile (1), (2), (4), (5) din § 9 sunt fundamentale, dar în anumite cazuri (la măsurarea segmentelor incomensurabile cu unitatea, la extragerea rădăcinilor din numere prime) ele nu au limită în $\mathbb{Q}$.

Definiția 2. *Câmpul liniar ordonat P se numeşte **continuu** dacă el este complet şi arhimedean ordonat (§ 9), adică satisface lema lui Arhimede: pentru orice $a,b\in P, b>0$ există un număr natural $n>0$ astfel încât $nb>a$.*

Observație. În definiția 2 este suficient de luat $b=e$ (e este elementul unitate a câmpului P), deoarece pentru orice $a,b\in P$,

$b>0$, aplicând afirmația pentru perechea $\left(\frac{a}{b}, e\right)$ avem $n \cdot e > \frac{a}{b}$, de unde $nb > a$.

Sarcina noastră constă în extinderea câmpului $\mathbb{Q}$ astfel încât noul câmp $\mathbb{R}$ să fie continuu şi atunci în acest câmp dispar toate defectele lui $\mathbb{Q}$, în particular, vor avea soluție problemele de măsurare a segmentelor şi de extragere a rădăcinilor (§ 9).

Definiția 3. ***Sistem de numere reale*** *se numeşte un câmp* $\mathbb{R}$ *care este continuu (adică complet şi arhimedean) şi conține ca subcâmp sistemul numerelor raționale* $\mathbb{Q}$.

Observăm că, spre deosebire de cazurile precedente, în definiție nu se cere *minimalitatea* lui $\mathbb{R}$, dar după cum vom vedea imediat, acest fapt rezultă din lema lui Arhimede, cu ajutorul următoarei afirmații.

Lema 11.1. *Câmpul liniar ordonat* P *care conține câmpul numerelor raționale* $\mathbb{Q}$, *este arhimedean ordonat dacă şi numai dacă orice element din* P *este limita unui şir de numere raționale.*

Demonstrație. ($\Rightarrow$) Fie P un câmp arhimedean ordonat şi $P \supseteq \mathbb{Q}$. Vom arăta că lema lui Arhimede permite aproximarea oricărui element $a \in P$ printr-un şir de numere raționale (vezi procedeul utilizat în §9).

Fie $a \in P$ şi $n > 0$ un număr natural arbitrar. Aplicăm lema lui Arhimede pentru perechile

$$\left(a, \frac{1}{n}\right) \text{ şi } \left(-a, \frac{1}{n}\right):$$

există numerele naturale m_1 şi m_2 încât

$$m_1 \cdot \frac{1}{n} > a, \quad m_2 \cdot \frac{1}{n} > -a.$$

Prin urmare, $\left(-m_2\right)\cdot\frac{1}{n} < a,$ deci mulțimea de numere naturale

$$A = \left\{ l \in \mathbb{N} \mid l \cdot \frac{1}{n} \le a \right\}$$

este mărginită superior de numărul m_1 şi este nevidă, deoarece conține numărul $-m_2$. Prin urmare, A conține cel mai mare număr, fie acesta m:

$$m \cdot \frac{1}{n} \le a, \ \left(m+1\right)\cdot\frac{1}{n} > a.$$

Atunci avem:

$$\frac{m}{n} \le a < \frac{m+1}{n}.$$

Adăugând la aceste relații $\left(\frac{-m}{n}\right)$ şi notând $a_n = \frac{m}{n}$, obținem:

$$0 \le a - a_n < \frac{1}{n}. \qquad (1)$$

Astfel vom avea un şir de numere raționale $\{a_n\}$, definit de elementul $a \in P$. Din relația (1) se vede că $a - a_n$ tinde spre zero, când n tinde spre ∞, prin urmare $\lim\{a_n\} = a.$

($\Leftarrow$) Fie $P \supseteq \mathbb{Q}$ şi admitem că orice element din P este limita unui şir de numere raționale. Este suficient de arătat că pentru orice $a \in P$ există un număr natural n încât $n \cdot 1 > a$ (vezi observația de mai sus).

Fie $a \in P$ şi $a = \lim\{a_n\}$, $a_n \in \mathbb{Q}$. Pentru $\varepsilon = 1$ există numărul natural k, încât $|a_k - a| < 1,$ prin urmare

$$a \le |a| = |(a - a_k) + a_k| \le |a - a_k| + |a_k| < 1 + |a_k|.$$

Aplicăm lema lui Arhimede pentru numerele raționale $\left(1, \frac{1}{1+|a_k|}\right)$: există numărul natural n, încât

$$n \cdot \frac{1}{1+|a_k|} > 1.$$

Înmulțind cu $1+|a_k|$, obținem $n > 1+|a_k|$. Deoarece am văzut că $1+|a_k| > a$, avem $n > a$, ceea ce trebuia de demonstrat. □

Acum putem demonstra *unicitatea* sistemului de numere reale.

Teorema 11.2. *Orice două sisteme de numere reale* $\mathbb{R}_1$ *şi* $\mathbb{R}_2$ *sunt câmpuri izomorfe, adică sistemul de numere reale este unic până la un izomorfism de câmpuri*.

Demonstrație. Fie $\mathbb{R}_1 \supseteq \mathbb{Q}_1$ şi $\mathbb{R}_2 \supseteq \mathbb{Q}_2$ sisteme de numere reale care, conform definiției, conțin sisteme de numere raționale $\mathbb{Q}_1$ şi $\mathbb{Q}_2$. Din unicitatea câmpului de numere raționale rezultă că există un izomorfism de câmpuri $\varphi : \mathbb{Q}_1 \to \mathbb{Q}_2$ care păstrează şi ordinea elementelor. Să arătăm că φ poate fi extins până la un izomorfism $\overline{\varphi} : \mathbb{R}_1 \to \mathbb{R}_2$.

Luăm un element arbitrar $d_1 \in \mathbb{R}_1$. Conform definiției, $\mathbb{R}_1$ este arhimedean şi din lema 11.1 rezultă că orice element din $\mathbb{R}_1$ este limita unui şir de elemente din $\mathbb{Q}_1$, de aceea $d_1 = \lim\{a_n\}$, $a_n \in \mathbb{Q}_1$. Şirul convergent $\{a_n\}$ este fundamental în $\mathbb{R}_1$ (Propoziția 9.2), deci şi în $\mathbb{Q}_1$. Izomorfismul φ defineşte şirul $\{\varphi(a_n)\}$ de elemente din $\mathbb{Q}_2$ care este fundamental în $\mathbb{Q}_2$, deci şi în $\mathbb{R}_2$. Dar $\mathbb{R}_2$ este un câmp complet, prin urmare acest şir are limită în $\mathbb{R}_2$, fie $\lim\{\varphi(a_n)\} = d_2 \in \mathbb{R}_2$.

Definim aplicația $\overline{\varphi} : \mathbb{R}_1 \to \mathbb{R}_2$ prin regula:

$$\overline{\varphi}(d_1) = d_2.$$

Următoarele verificări au scopul să ne convingă că $\overline{\varphi}$ este un izomorfism de câmpuri, ce păstrează ordinea.

1) Definiția aplicației $\overline{\varphi}$ este *corectă*, adică d_2 nu depinde de alegerea şirului $\{a_n\}$ cu proprietatea $\lim\{a_n\} = d_1$.

Într-adevăr, dacă mai avem un şir $\{b_n\}$ cu aceeaşi proprietate $\left(\lim\{b_n\} = d_1\right)$, atunci $\lim\{a_n - b_n\} = 0$ în $\mathbb{R}_1$, deci şi în $\mathbb{Q}_1$. Aplicând φ, obținem în $\mathbb{R}_2$:

$$\lim\{\varphi(a_n) - \varphi(b_n)\} = 0,\ \lim\{\varphi(a_n)\} = \lim\{\varphi(b_n)\} = d_2.$$

2) $\overline{\varphi}$ este o *continuare* a izomorfismului φ:
dacă $d_1 \in \mathbb{Q}_1$, atunci putem lua şirul staționar $\{a_n = d_1\}$ care trece în şirul staționar $\{\varphi(a_n) = \varphi(d_1)\}$ cu limita $\varphi(a_n) = \varphi(d_1)$.

3) $\overline{\varphi}$ este o *bijecție*.
Într-adevăr, dacă $c_1 \neq d_1$ $(c_1, d_1 \in \mathbb{R}_1)$, $c_1 = \lim\{a_n\}$, $d_1 = \lim\{b_n\}$, atunci $\lim\{a_n - b_n\} \neq 0$, de aceea $\lim\{\varphi(a_n - b_n)\} \neq 0$, de unde $\overline{\varphi}(c_1) \neq \overline{\varphi}(d_1)$. Deci $\overline{\varphi}$ este injectivă.

Orice element $d_2 \in \mathbb{R}_2$ este limita unui şir $\{x_n\}, x_n \in \mathbb{Q}_2$; atunci şirul $\{a_n = \varphi^{-1}(x_n)\}$ este fundamental în $\mathbb{R}_1$. Luând $d_1 = \lim\{a_n\}$ avem, prin definiție, $d_2 = \overline{\varphi}(d_1)$, deci $\overline{\varphi}$ este surjectivă, adică o bijecție.

4) $\overline{\varphi}$ *păstrează operațiile* $(+)$ şi $(\cdot)$:
$\overline{\varphi}(c_1 + d_1) = \overline{\varphi}(c_1) + \overline{\varphi}(d_1)$, $\overline{\varphi}(c_1 d_1) = \overline{\varphi}(c_1) \cdot \overline{\varphi}(d_1)$, ceea ce este evident din definiții.

5) $\overline{\varphi}$ *păstrează relaţia de ordine*:

fie $c_1 < d_1$ în $\mathbb{Q}_1$ şi $c_1 = \lim\{a_n\}$, $d_1 = \lim\{b_n\}$; atunci există n_0 încât $a_n < b_n$ pentru orice $n > n_0$, prin urmare, $\varphi(a_n) < \varphi(b_n)$ în $\mathbb{R}_2$ pentru $n > n_0$. De aceea $\lim\{\varphi(a_n)\} < \lim\{\varphi(b_n)\}$ în $\mathbb{R}_2$, adică $\overline{\varphi}(c_1) < \overline{\varphi}(d_1)$. □

§12. Existenţa sistemului de numere reale. Teorema despre completitudinea câmpului $\mathbb{R}$

În acest compartiment vom analiza problema *existenţei* sistemului de numere reale $\mathbb{R}$, care este echivalentă cu problema compatibilităţii sistemului de axiome, ce defineşte câmpul $\mathbb{R}$ (vezi §4). Ca şi în toate cazurile precedente, problema se rezolvă prin construirea unei interpretări, adică a unei mulţimi ce satisface cerinţele definiţiei 3 din §11: $\mathbb{R}$ este un câmp continuu, ce conţine $\mathbb{Q}$. Pregătirea preliminară din § 10,11 ne permite să efectuăm o astfel de construcţie cu ajutorul şirurilor fundamentale de numere raţionale (metoda lui Georg Cantor).

Ca şi în §10, notăm prin $\mathcal{F}$ mulţimea tuturor şirurilor fundamentale de numere raţionale. Definim pe această mulţime următoarea relaţie binară:

$\{a_n\} \sim \{b_n\} \overset{def}{\Leftrightarrow} \{a_n - b_n\}$ este un şir nul, adică $\lim\{a_n - b_n\} = 0$. (vezi §10, definiţia 2),

Lema 12.1. *Relaţia binară „~” este o relaţie de echivalenţă, adică este reflexivă, simetrică şi tranzitivă.*

Demonstraţie. Reflexivitatea şi simetria rezultă direct din definiţie. Să verificăm ultima proprietate. Fie $\{a_n\} \sim \{b_n\}$ şi

$\{b_n\} \sim \{c_n\}$. Pentru orice $\varepsilon > 0$, dacă n este suficient de mare, avem:

$$|a_n - c_n| = |a_n - b_n + b_n - c_n| \le |a_n - b_n| + |b_n - c_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

deci $\{a_n\} \sim \{c_n\}$. □

Să ne amintim că pe mulțimea $\mathcal{F}$ au fost introduse patru operații (§10) şi au fost definite şirurile nule, pozitive şi negative, demonstrând legea trihotomiei:

$$\mathcal{F} = \mathcal{F}^{(+)} \cup \{0\} \cup \mathcal{F}^{(-)}$$

(Propoziția10.6). De aceea relația de ordine în F poate fi definită în mod obişnuit astfel:

$$\{a_n\} \le \{b_n\} \overset{def}{\Leftrightarrow} \{b_n - a_n\} \text{ este pozitiv sau nul.}$$

În continuare vom arăta câteva proprietăți ale relației de echivalență „$\sim$” pe $\mathcal{F}$, legate de compatibilitatea ei cu operațiile din F şi relația de ordine în $\mathcal{F}$.

Lema 12.2. *Orice două şiruri fundamentale nule sunt echivalente. Dacă* $\{a_n\} \sim \{b_n\}$ *şi* $\{a_n\}$ *este un şir pozitiv (negativ), atunci şi* $\{b_n\}$ *este un şir pozitiv (negativ).*

Demonstrație. Dacă $\lim\{a_n\} = \lim\{b_n\} = 0$ atunci

$$\lim\{a_n - b_n\} = \lim\{a_n\} - \lim\{b_n\} = 0,$$

deci $\{a_n\} \sim \{b_n\}$.

Fie $\{a_n\}$ un şir pozitiv şi $\{a_n\} \sim \{b_n\}$. Atunci există $\varepsilon > 0$ şi un număr natural n_1 încât $a_n > \varepsilon$ pentru orice $n > n_1$. Din condiția $\lim\{a_n - b_n\} = 0$ rezultă existența unui număr n_2 astfel încât

$$|a_n - b_n| < \frac{\varepsilon}{2}$$

pentru orice $n > n_2$. De aceea pentru $n_0 = \max\{n_1, n_2\}$ şi pentru orice $n > n_0$ avem:

$$b_n = a_n - (a_n - b_n) > \varepsilon - \frac{\varepsilon}{2} = \frac{\varepsilon}{2} > 0,$$

adică şi $\{b_n\}$ este un şir pozitiv. □

Lema 12.3. *Dacă din şirul* $\{a_n\} \in \mathcal{F}$ *se elimină primii* p *termeni,* $p \in \mathbb{N}$, *atunci şirul rămas este echivalent cu cel iniţial*.

Demonstraţie. Eliminăm din şirul $\{a_n\} \in \mathcal{F}$ primii p termeni şi obţinem şirul $\{b_n\} = \{a_{n+p}\}$. Şirul $\{a_n\}$ este fundamental, deci pentru orice $\varepsilon > 0$, există n_0 încât

$$|b_n - a_n| = |a_{n+p} - a_n| < \varepsilon$$

pentru orice $n > n_0$, de unde rezultă că $\lim\{a_n - b_n\} = 0$, adică $\{a_n\} \sim \{b_n\}$. □

Lema 12.4. *Dacă* $\{a_n\} \sim \{b_n\}$ *şi* $\{a_n\}$ *este convergent, atunci* $\{b_n\}$ *este convergent şi are aceeaşi limită (adică echivalenţa şirurilor convergente înseamnă coincidenţa limitelor lor).*

Demonstraţie. Fie $\{a_n\} \sim \{b_n\}$, unde $\{a_n\}$ este un şir convergent cu limita r. Atunci $\lim\{a_n - b_n\} = 0$, adică pentru orice $\varepsilon > 0$ există n_1 încât

$$|a_n - b_n| < \frac{\varepsilon}{2}$$

pentru orice $n > n_1$. Din relaţia $\lim\{a_n\} = r$ pentru acelaşi $\varepsilon > 0$ rezultă că există n_2 încât

$$|a_n - r| < \frac{\varepsilon}{2}$$

pentru orice $n > n_2$. Luând $n_0 = \max\{n_1, n_2\}$, pentru orice $n > n_0$ obținem:

$$|b_n - r| = |b_n - a_n + a_n - r| \le |b_n - a_n| + |a_n - r| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

prin urmare $\lim\{b_n\} = r$. □

Acum vom arăta că relația de echivalență „~ ’’ din $\mathcal{F}$ este compatibilă cu operațiile din $\mathcal{F}$ (vezi §10).

Lema 12.5. *Dacă la efectuarea celor patru operații aritmetice în $\mathcal{F}$ componentele se înlocuiesc cu şiruri echivalente, atunci rezultatele operațiilor sunt echivalente cu cele inițiale*.

Demonstrație. Fie $\{a_n\} \sim \{a'_n\}$ şi $\{b_n\} \sim \{b'_n\}$. Atunci

$$\lim\{a_n - a'_n\} = 0 \text{ şi } \lim\{b_n - b'_n\} = 0,$$

deci pentru orice $\varepsilon > 0$ există n_0 încât

$$|a_n - a'_n| < \frac{\varepsilon}{2}, \qquad |b_n - b'_n| < \frac{\varepsilon}{2}$$

pentru orice $n > n_0$. Prin urmare,

$$\left|(a_n \pm b_n) - (a'_n \pm b'_n)\right| \le |a_n - a'_n| + |b_n - b'_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

pentru orice $n > n_0$. Aceasta arată că şirurile $\{a_n \pm b_n\}$ şi $\{a'_n \pm b'_n\}$ sunt echivalente. În mod similar se verifică afirmația pentru celelalte operații. □

Acum trecem nemijlocit la *construirea interpretării (modelului) sistemului de numere reale*, utilizând rezultatele precedente.

Fie $\mathbb{R} = \mathcal{F} / \sim$ mulţimea claselor de echivalenţă a şirurilor fundamentale de numere raţionale în raport cu relaţia „$\sim$”. Notăm prin $\overline{\{a_n\}}$ clasa de echivalenţă definită de $\{a_n\}$:

$$\overline{\{a_n\}} = \{\{b_n \in \mathcal{F} \mid \{a_n\} \sim \{b_n\}\}\}.$$

Prin urmare, $\overline{\{a_n\}} = \overline{\{b_n\}} \Leftrightarrow \{a_n\} \sim \{b_n\}$. Definim pe mulţimea $\mathbb{R}$ următoarele operaţii:

$$\overline{\{a_n\}} \pm \overline{\{b_n\}} = \overline{\{a_n \pm b_n\}},$$

$$\overline{\{a_n\}} \cdot \overline{\{b_n\}} = \overline{\{a_n b_n\}},\ \frac{\overline{\{a_n\}}}{\overline{\{b_n\}}} = \overline{\left\{\frac{a_n}{b_n}\right\}} \left(b_n \neq 0\right) \qquad (1)$$

Din lema 12.5 rezultă *corectitudinea* acestei definiţii.

Clasa $\overline{\{a_n\}}$ se numeşte *pozitivă* (*nulă*, *negativă*) dacă $\{a_n\}$ este un şir pozitiv (nul, negativ). Din lema 12.2 rezultă că această definiţie este corectă. Mai mult, din legea trihotomiei pentru $\mathbb{Q}$ (vezi Propoziţia 10.6) rezultă imediat aceeaşi lege pentru $\mathbb{R}$:

$$\mathbb{R} = \mathbb{R}^{(+)} \cup \overline{\{0\}} \cup \mathbb{R}^{(-)}.$$

Prin urmare, putem introduce în mod obişnuit pe $\mathbb{R}$ *relaţia de ordine* naturală şi *modulul* sau *valoarea absolută* a numărului.

Definiţia 1. *Fie* $\alpha, \beta \in \mathbb{R}$. *Atunci considerăm:*

$$\alpha \leq \beta \overset{def}{\Leftrightarrow} \beta - \alpha \text{ este o clasă pozitivă sau nulă;}$$

$$|\alpha| \overset{def}{=} \begin{cases} \alpha, & dacă \quad \alpha \in \mathbb{R}^{(+)} \\ \overline{\{0\}}, & dacă \quad \alpha = \overline{\{0\}} \\ -\alpha, & dacă \quad \alpha \in \mathbb{R}^{(-)} \end{cases} \qquad (2)$$

Observaţie. Dacă $\alpha = \overline{\{a_n\}}$ şi $\beta = \overline{\{b_n\}}$, atunci din aceea că există n_0 încât $a_n \geq b_n$, pentru orice $n > n_0$, rezultă relaţia $\alpha \geq \beta$.

Scopul următoarelor afirmații este de a verifica faptul că $\mathbb{R} = \mathcal{F} / \sim$ este un sistem de numere reale.

Teorema 12.6. *Mulțimea $\mathbb{R} = \mathcal{F} / \sim$, în raport cu operațiile (1), formează un câmp liniar ordonat care conține câmpul numerelor raționale $\mathbb{Q}$.*

Demonstrație. Din corolarul 10.3 avem că operațiile $(+)$ şi $(\cdot)$ în $\mathcal{F}$ satisfac legile: comutativă, asociativă şi distributivă. Din (1) se vede că aceste legi au loc şi în $\mathbb{R} = \mathcal{F} / \sim$. Element neutru pentru adunare în $\mathbb{R}$ este clasa $\overline{\{0\}}$ care constă din şiruri nule (lema12.2).

Existența operațiilor inverse „$-$” şi „ :” în $\mathbb{R}$ rezultă din existența lor în $\mathcal{F}$, deci $\mathbb{R}$ este un câmp, elementul unitate al căruia $1 = \overline{\{a_n\}}$ constă din toate şirurile $\{a_n\}$ cu proprietatea $\lim\{a_n\} = 1$ (pentru simplitate ca reprezentant poate fi luat şirul staționar $\{1\}$) .

Faptul că $\mathbb{R}$ este liniar ordonat rezultă din definiția 1 şi din aceea că câmpul $\mathbb{Q}$ este liniar ordonat.

Să arătăm că există o aplicație injectivă $i : \mathbb{Q} \to \mathbb{R}$ (în acest sens se spune că $\mathbb{R}$ conține $\mathbb{Q}$). Oricărui număr rațional $r \in \mathbb{Q}$ îi punem în corespondență şirul staționar $\{a_n = r\}$ şi clasa lui de echivalență $\overline{\{r\}} \in \mathbb{R}$ (care pentru simplitate se notează prin (r)). Dacă $r \neq s$, unde $r, s \in \mathbb{Q}$, atunci este evident că $(r) \neq (s)$, adică i este o aplicație injectivă. Este uşor de văzut că ea păstrează operațiile, deci $\mathbb{R}$ conține subcâmpul $\mathbb{Q}' = \{(r) \mid r \in \mathbb{Q}\}$ izomorf cu $\mathbb{Q}$. □

Teorema 12.7. *Câmpul liniar ordonat* $\mathbb{R} = \mathcal{F} / \sim$ *este arhimedean, adică pentru orice* $\alpha, \beta \in \mathbb{R}$, *unde* $\beta > 0$, *există un număr natural* n *încât* $n\beta > \alpha$.

Demonstrație. Fie $\alpha = \overline{\{a_n\}}, \beta \in \overline{\{b_n\}} \in \mathbb{R}$ şi $\beta > 0$. Şirul fundamental $\{a_n\}$ este mărginit (Propoziția 10.1), deci există un număr raţional pozitiv M încât $|a_n| < M$ pentru orice n. Atunci şirul $\{M\} - \{a_n\}$ este pozitiv sau nul, deci $M \geq \alpha$. Deoarece $\beta > 0$, şirul $\{b_n\}$ este pozitiv, adică există $\varepsilon > 0$ ($\varepsilon \in \mathbb{Q}$) încât $b_n > \varepsilon$ pentru n suficient de mare, dar în acest caz $\beta \geq (\varepsilon)$ (vezi observația de mai sus). Aplicând lema lui Arhimede pentru numerele raționale M şi $\varepsilon > 0$, găsim un număr natural n astfel încât $n\varepsilon > M$. Atunci $n\beta \geq n\varepsilon > M \geq \alpha$, adică $n\beta > \alpha$. Prin urmare, lema lui Arhimede are loc şi în câmpul $\mathbb{R}$. □

Ultimul şi cel mai important pas în construcția noastră constă în verificarea *completitudinii* câmpului $\mathbb{R}$.

Teorema 12.8 ***(teorema despre completitudinea câmpului*** $\mathbb{R}$ ***sau teorema lui Cauchy)***. $\mathbb{R} = \mathcal{F} / \sim$ *este un câmp complet, adică orice şir fundamental de numere reale posedă limită în câmpul numerelor reale.*

Demonstrație. Vom demonstra afirmația teoremei în două etape.

I. Să arătăm mai întâi că orice şir fundamental de numere *raționale* posedă limită în $\mathbb{R}$.

Fie $\{a_n\} \in F$ şi notăm $\alpha = \overline{\{a_n\}}$ (clasa de echivalență respectivă). Considerăm numerele raționale $a_n \in \mathbb{Q}$ ca elemente din $\mathbb{R}$, înlocuind fiecare număr a_n cu clasa de echivalență (a_n), definită de şirul staționar, determinat de acest număr. Atunci avem şirul

$(a_1),(a_2),...,(a_n),...$ de elemente din $\mathbb{R}$. Deoarece $\{a_n\}$ este fundamental în $\mathbb{Q}$, el este fundamental şi în $\mathbb{R}$. Acum vom arăta că $\lim\{(a_n)\} = \alpha$.

Fie $\varepsilon > \overline{\{0\}}$ un element din $\mathbb{R}$ cu reprezentantul $\{e_n\}$ (adică $\varepsilon = \overline{\{e_n\}}$). Prin definiţie, din $\{e_n\} > 0$ rezultă că există un număr raţional $e > 0$ şi un număr natural n_0 încât $e_n > e > 0$ pentru orice $n > n_0$. Deci $\varepsilon \geq (e)$ – clasa determinată de şirul staţionar $\{e\}$. Alegem un număr raţional e' cu proprietatea $e > e' > 0$ (de exemplu, $e' = \frac{e}{2}$). Atunci avem: $(e') < (e) \leq \varepsilon$. Deoarece $\{a_n\}$ este un şir fundamental în $\mathbb{Q}$ există un număr n_0 astfel încât $|a_p - a_q| < e'$ pentru orice $p > n_0$ şi $q > n_0$. Prin urmare, pentru numărul dat $n > n_0$ avem:

$$a_p - a_n < e', \quad a_n - a_q < e'$$

penru orice $p > n_0$ şi $q > n_0$. Pentru acest număr n trecem de la şiruri la clasele de echivalenţe definite de ele (avînd a_n fixat, $\{a_p\}_{p>n_0}$ şir echivalent cu $\{a_n\}$ şi $\{a_q\}_{q>n_0}$ şir echivalent cu $\{a_n\}$):

$$\alpha - (a_n) \leq (e'), \quad (a_n) - \alpha \leq e'.$$

Prin urmare,

$$|(a_n) - \alpha| \leq (e') < \varepsilon$$

pentru orice $n > n_0$, ceea ce înseamnă că $\lim\{(a_n)\} = \alpha$.

II. Vom considera acum cazul general şi vom arăta că orice şir fundamental $\{\alpha_n\}$ de elemente din $\mathbb{R}$ posedă limită în $\mathbb{R}$.

Fie $\{\alpha_n\}$ un şir fundamental arbitrar de elemente din $\mathbb{R}$. Deoarece $\mathbb{R}$ este arhimedean (Teorema 12.7), din Lema 11.1 rezultă că fiecare element $\alpha_n \in \mathbb{R}$ este limita unui şir fundamental

format din clase cu reprezentanți staționari din $\mathbb{Q}$. Pentru fiecare $n = 1, 2, \ldots$ în şirul fundamental, care are drept limită elementul α_n, alegem o clasă (a_n) care satisface condiția :

$$|\alpha_n - (a_n)| < \left(\frac{1}{n}\right) \qquad (3)$$

(alegerea este posibilă, deoarece α_n este limita şirului respectiv). Să arătăm că şirul de elemente astfel alese din $\mathbb{Q}$:

$$(a_1), (a_2), \ldots, (a_n), \ldots$$

este fundamental în $\mathbb{R}$, deci şi în $\mathbb{Q}$.

Fie $\varepsilon > \overline{\{0\}}$ un element arbitrar din $\mathbb{R}$. Procedând ca şi în demonstrația etapei I, găsim un număr rațional $e > 0$ încât $(e) < \varepsilon$. Alegem un număr natural $n_1 > \frac{3}{e}$ (sau $\frac{1}{n_1} < \frac{e}{3}$). Deoarece $\{\alpha_n\}$ este un şir fundamental, există un număr natural n_2 încât:

$$|\alpha_p - \alpha_q| < \left|\frac{e}{3}\right| \qquad (4)$$

pentru orice $p > n_2$ şi $q > n_2$. Luând $n_0 = \max\{n_1, n_2\}$, pentru orice $p > n_0$ şi $q > n_0$, obținem cu ajutorul relațiilor (3) şi (4):

$$|(a_p) - (a_q)| \le |(a_p) - \alpha_p| + |\alpha_p - \alpha_q| + |\alpha_q - (a_q)| <$$

$$< \left(\frac{1}{p}\right) + \left(\frac{e}{3}\right) + \left(\frac{1}{q}\right) < \left(\frac{e}{3}\right) + \left(\frac{e}{3}\right) + \left(\frac{e}{3}\right) = (e) < \varepsilon.$$

Aceasta arată că şirul $\{(a_n)\}$ este fundamental. Identificând clasa (a_n) cu numărul $a_n \in \mathbb{Q}$ se poate spune că şirul $\{a_n\}$ de numere raționale este fundamental în $\mathbb{Q}$. Acum aplicăm prima parte a acestei demonstrații şi facem concluzia că acest şir are limită în $\mathbb{R}$, fie $\lim\{a_n\} = \alpha$, unde $\alpha = \overline{\{a_n\}}$.

Să verificăm faptul că $\lim\{(a_n)-\alpha_n\}=0$. Într-adevăr, pentru orice $\varepsilon>(\bar{0})$ din $\mathbb{R}$ luăm un număr raţional $e>0$ astfel încât $(e)<\varepsilon$ şi alegem un număr natural n_0 cu condiţia $\frac{1}{n_0}<e$. Atunci, pentru orice $n>n_0$, din relaţia (3) avem:

$$|(a_n)-\alpha_n|<\left(\frac{1}{n}\right)<\left(\frac{1}{n_0}\right)<(e)<\varepsilon.$$

Aceasta arată că $\lim\{(a_n)-\alpha_n\}=0$. Prin urmare,

$$\lim\{\alpha_n\}=\lim\{(a_n)\}=\alpha.$$

Astfel am arătat că orice şir fundamental $\{\alpha_n\}$ din $\mathbb{R}$ are limită în $\mathbb{R}$, adică $\mathbb{R}$ este un câmp complet . □

Din teoremele 12.6, 12.7, 12.8 obţinem următorul rezultat final care arată *existenţa* sistemului de numere reale.

Teorema 12.9. *Mulţimea* $\mathbb{R}=\mathcal{F}/\sim$ *cu operaţiile* (1) *şi relaţia de ordine* (2) *formează un câmp arhimedean complet, adică un câmp continuu ce conţine câmpul numerelor raţionale* $\mathbb{Q}$. *Prin urmare,* $\mathbb{R}$ *este un sistem de numere reale, ceea ce soluţionează problema existenţei acestui sistem, deci şi compatibilitatea axiomelor ce definesc acest sistem.* □

Exerciţii

1. Fie a si b două numere reale, pentru care suma şi diferenţa $a+b$ şi $a-b$ sunt numere raţionale. Sunt oare a, b şi $a\cdot b$ numere raţionale?
2. Fie a un număr real. Este oare posibil ca primele zece puteri $a, a^2, \ldots, a^{10}$ ale lui a să fie numere iraţionale, iar următoarele zece puteri $a^{11}, \ldots, a^{20}$ să fie raţionale?

§13. Reprezentarea numerelor reale prin fracţii zecimale (Descompunerea zecimală a numerelor reale)

În paragraful precedent am reprezentat numerele reale ca clase de echivalenţă a şirurilor fundamentale de numere raţionale. Lucrul cu astfel de clase nu este comod, de aceea în practică se preferă reprezentarea numerelor reale cu ajutorul fracţiilor în sistemul numeric zecimal. În continuare arătăm posibilitatea descompunerii zecimale a oricărui număr real.

Să amintim că incluziunea $i:\mathbb{Q}\to\mathbb{R}$ a fost definită astfel (vezi Teorema 12.6): oricărui număr raţional $r\in\mathbb{Q}$ îi punem în corespondenţă şirul staţionar $\{a_n = r\}$ şi clasa lui de echivalenţă $\overline{\{r\}}\in\mathbb{R}$. În caz general, numărul real $\alpha\in\mathbb{R}$ poate să nu aibă un reprezentant $\{a_n\}$ de formă suficient de simplă, deaceea se foloseşte metoda aşa numitelor aproximaţii ale numărului $\alpha\in\mathbb{R}$ prin fracţii zecimale. Această metodă se bazează pe următoarele afirmaţii.

Teorema 13.1. *Pentru orice număr real $\alpha\in\mathbb{R}$ există un număr întreg M astfel încât au loc relaţiile:*

$$M\le\alpha<M+1$$

şi acest număr M este determinat univoc.

Demonstraţie. Fie $\alpha=\overline{\{a_n\}}$. Şirul fundamental $\{a_n\}$ este mărginit (Propoziţia 10.1), de aceea există un număr natural N astfel încât

$$-N<a_n<N$$

pentru orice n. Atunci pentru numărul real $\alpha=\overline{\{a_n\}}$ are loc relaţia:

$$-N\le\alpha\le N,$$

de unde rezultă că

$$-N-1<\alpha<N+1.$$

Printre numerele întregi:

$$-N-1,\ -N,\ -N+1,\dots,\ -1,\ 0,\ 1,\dots,\ N,\ N+1$$

se poate găsi primul număr M cu condiția $\alpha < M+1$. Atunci avem: $M \le \alpha < M+1$. Mai mult, acest număr M este unic: dacă există un număr întreg M_1 cu proprietatea $M_1 \le \alpha < M_1+1$, atunci relația $M_1 < M$ este imposibilă (deoarece în acest caz $M_1+1 \le M$ şi am avea $M_1+1 \le \alpha$, în contradicție cu relația $M_1+1 > \alpha$). Analog se arată că nu este posibilă relația $M_1 > M$. Prin urmare, avem $M_1 = M$. □

Corolarul 13.2. *Pentru orice număr real* $\alpha \in \mathbb{R}$ *şi orice număr natural* $N \neq 0$ *există un singur număr întreg* M *astfel încât*

$$\frac{M}{N} \le \alpha < \frac{M+1}{N}.$$

Demonstrație. Conform teoremei 13.1, pentru numărul real $N\alpha$ există un singur număr întreg M, astfel încât

$$M \le N\alpha < M+1,$$

de unde rezultă relația cerută. □

Definiția 1. *Numerele raționale* $\frac{M}{N}$ *şi* $\frac{M+1}{N}$ *se numesc* ***valori aproximative*** *ale numărului real* α *prin lipsă şi prin adaos, respectiv, cu exactitate de* $\frac{1}{N}$.

Acum vom fixa un număr natural arbitrar $k > 1$. Dacă în corolarul precedent numărul N ia succesiv valorile $1, k, k^2, ..., k^n, ...$ atunci pentru numărul real α obținem două şiruri de numere raționale

$$\left\{\frac{M_n}{k^n}\right\} \text{ şi } \left\{\frac{M_n+1}{k^n}\right\},$$

univoc determinate, ce verifică inegalitățile

$$\frac{M_n}{k^n} \le \alpha < \frac{M_n + 1}{k^n}$$

pentru orice n natural nenul.

Teorema 13.3. *Şirurile* $\left\{\frac{M_n}{k^n}\right\}$ *şi* $\left\{\frac{M_n + 1}{k^n}\right\}$, *obţinute mai sus pentru numărul real* α, *au aceeaşi limită, care este egală cu* α *(adică aceste şiruri aparţin clasei* α *şi o definesc în mod unic).*

Demonstraţie. Mai întâi observăm că $k^n > n$, pentru orice $n \in \mathbb{N}$ $(n \neq 0)$. Într-adevăr, dacă $n = 1$ atunci $k^1 > 1$ conform alegerii numărului k. Presupunem că $k^n > n$, pentru $n \in \mathbb{N}, n > 1$. Atunci pentru $n+1$ obţinem: $k^{n+1} > nk$ şi, notând $l = k - 1$, avem:

$$nk = n(1 + l) = n + nl \ge n + 1,$$

adică $k^{n+1} > n + 1$. Prin inducţie facem concluzia că $k^n > n$, pentru orice n.

Utilizând relaţia obţinută, pentru orice $\varepsilon > 0$, avem $k^n \varepsilon > n\varepsilon$. Aplicăm lema lui Arhimede pentru numerele ε şi 1: există un număr n încât $k^n \varepsilon > n\varepsilon > 1$. Prin urmare, pentru orice n suficient de mare are loc relaţia $\frac{1}{k^n} < \varepsilon$.

Acum demonstrăm nemijlocit afirmaţia teoremei. Pentru orice $\varepsilon > 0$ există un număr natural n_0 astfel încât au loc relaţiile:

$$\left|\alpha - \frac{M_n}{k^n}\right| < \frac{M_n + 1}{k^n} - \frac{M_n}{k^n} = \frac{1}{k^n} < \varepsilon,$$

$$\left|\alpha - \frac{M_n + 1}{k^n}\right| = \frac{M_n + 1}{k^n} - \alpha \le \frac{M_n + 1}{k^n} - \frac{M_n}{k^n} = \frac{1}{k^n} < \varepsilon,$$

pentru orice $n > n_0$. □

În continuare vom preciza cum se obţin aproximaţiile $M_n, M_{n+1}, \ldots$ una din alta. Pentru simplitate vom considera *numere*

pozitive $\alpha > 0$. Mai mult, alegem $k = 10$ şi numerele M_n vor fi scrise în *sistemul zecimal* de numeraţie.

Teorema 13.4. *Considerăm două aproximaţii consecutive ale numărului real* $\alpha > 0$:

$$\frac{M_n}{10^n} \le \alpha < \frac{M_n + 1}{10^n}, \quad \frac{M_{n+1}}{10^{n+1}} \le \alpha < \frac{M_{n+1} + 1}{10^{n+1}}.$$

Atunci numărul întreg M_{n+1} *se obţine din numărul* M_n *prin scrierea la dreapta lui* M_n *a unei cifre (unic determinate) dintre* $0, 1, 2, \ldots., 8, 9$.

Demonstraţie. Din relaţiile:

$$\frac{M_n}{10^n} = \frac{10M_n}{10^{n+1}} \le \alpha < \frac{M_n + 1}{10^n} = \frac{10M_n + 10}{10^{n+1}},$$
$$\frac{M_{n+1}}{10^{n+1}} \le \alpha < \frac{M_{n+1} + 1}{10^{n+1}}$$

rezultă (conform construcţiei numerelor M_n)

$$\frac{10M_n}{10^{n+1}} \le \frac{M_{n+1}}{10^{n+1}} \le \alpha < \frac{10M_n + 10}{10^{n+1}},$$
$$10M_n \le M_{n+1} < 10M_n + 10.$$

Prin urmare, $M_{n+1} = 10M_n + q_{n+1}$, unde $0 \le q_{n+1} < 10$. Numărul q_{n+1} este definit în mod unic, deoarece M_n şi M_{n+1} sunt definite în mod unic de numărul $\alpha \in \mathbb{R}$. □

Dacă scriem numerele pozitive în formă de fracţii zecimale, atunci şirul $\left\{\frac{M_n}{10^n}\right\}$ în formă desfăşurată se prezintă astfel:

$$M_0 = p; \quad p, q_1; \quad p, q_1 q_2; \quad ...; \quad p, q_1 q_2 ... q_n; \quad ...$$

Se scrie mai scurt acest şir astfel: $p, q_1 q_2 \ldots q_n \ldots$ Numim această expresie *descompunere zecimală* a numărului real α.

Teorema 13.5. *Descompunerea zecimală a oricărui număr real α nu poate fi o fracţie periodică cu cifra 9 în perioadă.*

Demonstraţie. Presupunem contrarul: există un număr n, încât pentru orice $m > n$, avem $q_m = 9$, adică descompunerea zecimală are forma:

$$p, q_1 q_2 ... q_n 99...9...$$

Atunci pentru $m = n+1$ avem:

$$M_{n+1} = 10M_n + 9, \quad M_{n+1} + 1 = 10M_n + 10,$$

$$\frac{M_{n+1}+1}{10^{n+1}} = \frac{10M_n + 10}{10^{n+1}} = \frac{M_n + 1}{10^n}.$$

Astfel aproximarea prin adaos a numărului α la pasul n coincide cu aproximarea similară la pasul $n+1$. Dar atunci uşor se vede că ea coincide şi cu toate aproximările de sus ce urmează: dacă pentru un număr m avem

$$\frac{M_m + 1}{10^m} = \frac{M_n + 1}{10^n},$$

atunci pentru $m+1$ obţinem

$$M_{m+1} = 10M_n + 9, \qquad M_{m+1} + 1 = 10M_m + 10,$$

Deci

$$\frac{M_{m+1}+1}{10^{m+1}} = \frac{10M_m + 10}{10^{m+1}} = \frac{M_m + 1}{10^m} = \frac{M_n + 1}{10^n}.$$

Astfel şirul $\left\{\frac{M_n+1}{10^n}\right\}$ staționează, începând cu un număr n, de aceea toți membrii acestui şir, începând cu n, vor fi egali cu numărul rațional $r=\frac{M_n+1}{10^n}$. Deoarece acest şir determină numărul α, avem $\alpha=r$, ceea ce contrazice faptul că prin construcție $\alpha<\frac{M_n+1}{10^n}$. □

Aşadar, orice număr real α determină în mod unic descompunerea sa zecimală $p,q_1q_2...q_n...$, care nu poate fi o fracție periodică cu cifra 9 în perioadă. La rândul ei, această descompunere zecimală determină univoc numărul real α, deoarece este un şir fundamental de numere raționale, care aparține clasei α şi numai ei. Este clar că dacă numerele reale $\alpha>0$ şi $\beta>0$ nu coincid, atunci şi descompunerile zecimale respective nu coincid.

Să cercetăm acum trecerea inversă – de la descompuneri de formă $p,q_1q_2...q_n...$, unde p este un număr întreg şi $0\le q_n<10$, la numere reale.

Teorema 13.6. *Orice expresie de forma* $p,q_1q_2...q_n...$, *unde* $p\in\mathbb{N}$, $0\le q_n<10$, *şi nu are perioadă 9, reprezintă descompunerea zecimală a unui număr real* $\alpha>0$ *unic determinat*.

Demonstrație. Şirul $\{a_n\}=\{p,q_1,q_2...q_n\}$ este fundamental, deoarece pentru orice $\varepsilon>0$ există un astfel de număr n_0 încât pentru orice m cu condiția $m>n>n_0$ are loc relația:

$$|a_m-a_n|=0,\underbrace{00...0}_{n\ ori}\underbrace{q_{n+1}q_{n+z}...q_m}_{m-n\ ori}\le 0,\underbrace{0...0}_{n}\underbrace{9....9}_{m-n}<\frac{1}{10^n}<\varepsilon.$$

Deci şirul $\{a_n\}$ determină un număr real α, adică $\alpha = \overline{\{a_n\}}$. Fixând un număr n, pentru orice $m > n$ avem:

$$p, q_1 q_2 ... q_m \geq p, q_1 q_2 ... q_n,$$

adică $a_m \geq a_n$. Din definiția relației de ordine în $\mathbb{R}$ (vezi §12, observație) acum rezultă că $\alpha \geq a_n$, pentru orice număr ales n.

Deoarece din condiția teoremei expresia dată nu are cifra 9 în perioadă, pentru orice număr ales n există un număr $s > n$ încât $q_s \neq 9$. Atunci, pentru orice $m > s$, au loc relațiile:

$$a_m = p, q_1 q_2 ... q_n ... q_s ... q_m \leq p, q_1 q_2 ... q_n \underbrace{9...9}_{s-n\ ori} < a_n + \frac{1}{10^n},$$

deci

$$\alpha \leq p, q_1 q_2 ... q_n \underbrace{9...9}_{s-n\ ori}$$

pentru orice număr ales n. Astfel avem

$$a_n \leq \alpha < a_n + \frac{1}{10^n},$$

ceea ce înseamnă că numerele $p, q_1 q_2 ... q_n$ şi $p, q_1 q_2 ... q_n + \frac{1}{10^n}$ reprezintă valori aproximative (prin lipsă şi, respectiv, prin adaos) ale numărului α cu exactitatea de $\frac{1}{10^n}$. Prin urmare, şirul $p, q_1 q_2 ... q_n ...$ este o descompunere zecimală a numărului real α. □

Rămâne de observat că presupunerea $\alpha > 0$ nu este esențială: dacă $\alpha < 0$ atunci putem lua descompunerea zecimală a numărului pozitiv $-\alpha$, iar la rezultat punem înainte semnul „$-$”; pentru numărul 0 avem descompunerea $0,00...0...$.

Notăm cu $\mathbb{R}'$ mulțimea tuturor descompunerilor zecimale fără 9 în perioadă. Din cele demonstrate mai sus rezultă următoarea concluzie.

Corolarul 13.7. *Orice număr real $\alpha \in \mathbb{R}$ (ca clasă de echivalență) conține în sine o singură descompunere zecimală fără 9 în perioadă. Reciproc, orice descompunere zecimală, fără 9 în perioadă, se conține într-o singură clasă de echivalență $\alpha \in \mathbb{R}$. Astfel se defineşte o corespondență bijectivă între $\mathbb{R}$ şi $\mathbb{R}'$, prin urmare $\mathbb{R}'$ este o altă interpretare a sistemului de numere reale.* □

Exerciții

1. Pentru fracțiile zecimale periodice următoare să se găsească numărul rațional pe care îl reprezintă:
   a) 1,22(7); b) -0,(14); c) 2.013(23); e) -0,01(023); f) -2,001(7).

2. Să se arate că nu există numere raționale $\frac{m}{n}$ astfel încât:

a) $\left(\frac{m}{n}\right)^3 = 2$, b) $\left(\frac{m}{n}\right)^3 = 3$, c) $\left(\frac{m}{n}\right)^3 = 6$.

3. Să se arate că numerele $\sqrt{2}+\sqrt{3}$ şi $\sqrt{2}-\sqrt{3}$ sunt iraționale.

4. Să se găsească primele patru cifre după virgulă ale sumelor:

a) $\frac{1}{3}+\sqrt{3}$; b) $\sqrt{2}+\sqrt{3}$; c) $-\sqrt{3}+\sqrt{7}$.

5. Să se găsească aproximările zecimale cu o eroare mai mică decât 0,1 prin lipsă şi adaos, pentru numerele

   a) $\sqrt{5}$; b) $-\sqrt{5}$; c) $\frac{11}{7}$; d) $-\frac{11}{7}$; e) $\frac{178}{13}$; f) $\sqrt{11}$.

Capitolul V

Numere complexe şi hipercomplexe

§14. Câmpul numerelor complexe

După cum am văzut în capitolul precedent numerele reale sunt suficiente pentru fundamentarea teoriei limitelor, pentru măsurarea mărimilor scalare ş.a., dar aceste numere sunt insuficiente pentru rezolvarea ecuațiilor algebrice. Este bine cunoscut faptul că nu orice ecuație pătrată cu coeficienți reali are soluție în câmpul numerelor reale $\mathbb{R}$. Cea mai simplă ecuație de acest fel este $x^2+1=0$ (ea nu poate fi rezolvată în $\mathbb{R}$, deoarece pentru orice $a\in\mathbb{R}$ avem $a^2\geq 0$).

Următorul pas în procesul de extindere a sistemelor numerice constă în lărgirea câmpului $\mathbb{R}$ până la un câmp $\mathbb{C}$, în care este posibilă operația extragerii rădăcinii din orice număr. Începem cu o cerință mai modestă şi anume: să existe soluția ecuației $x^2+1=0$ în noul câmp, adică să existe un element $i\in\mathbb{C}$ încât $i^2=-1$. În concordanță cu acest scop, este firească

Definiția 1. *Vom numi* ***sistem de numere complexe*** *un câmp* $\mathbb{C}$ *care conține câmpul numerelor reale* $\mathbb{R}$ *ca subcâmp, posedă un element* $i\in\mathbb{C}$ *astfel încât* $i^2=-1$ *şi* $\mathbb{C}$ *este minimal cu aceste două condiții.*

Elementul i din Definiția 1 se numeşte *unitate imaginară* a câmpului $\mathbb{C}$.

Vom proceda ca şi în cazurile precedente, demonstrând mai întâi *unicitatea* sistemului de numere complexe şi cu acest scop exprimăm minimalitatea, cerută în definiție, într-o formă mai comodă.

Lema 14.1. *Fie* P *un câmp ce conține* $\mathbb{R}$ *ca subcâmp şi posedă unitate imaginară* $i\in P$ *(adică* $i^2=-1$*). Câmpul* P *este minimal*

cu aceste proprietăţi (adică va fi un sistem de numere complexe) dacă şi numai dacă orice element $x \in P$ *are o reprezentare unică în forma*

$$x = a + bi, \tag{1}$$

unde $a, b \in \mathbb{R}$.

Demonstraţie. Presupunem că P este un câmp minimal în sensul indicat. Separăm în P submulţimea:

$$P' = \{a + bi \mid a, b \in \mathbb{R}\}.$$

Observăm că dacă un element din P are reprezentare în forma (1), atunci ea este unică:

$$a + bi = c + di \quad \Leftrightarrow \quad a = c, \quad b = d.$$

Într-adevăr, dacă $b \neq d$, atunci $i = \dfrac{a-c}{d-b} \in \mathbb{R}$, contradicţie. De aceea $b = d$, de unde imediat rezultă $a = c$.

Mai mult, din proprietăţile operaţiilor câmpului rezultă:

$$(a + bi) \pm (c + di) = (a \pm c) + (b \pm d)i \tag{2}$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i. \tag{3}$$

Din unicitatea reprezentării (1), demonstrată mai sus, avem:

$$a + bi = 0 \quad \Leftrightarrow \quad a = 0 \quad \text{şi} \quad b = 0.$$

De aceea dacă $c + di \neq 0$ atunci $c \neq 0$ sau $d \neq 0$, dar aceasta este echivalent cu faptul că $c^2 + d^2 > 0$, prin urmare:

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd}{c^2+d^2} + \left(\frac{bc-ad}{c^2+d^2}\right)i. \tag{4}$$

Relaţiile (2), (3) şi (4) arată că submulţimea P' este închisă în raport cu cele 4 operaţii din câmpul P, de aceea P' este un subcâmp în P. Acest subcâmp posedă proprietăţile:

a) $P' \supseteq \mathbb{R}$, deoarece $a = a + 0 \cdot i$, pentru orice $a \in R$;

b) $i \in P'$, deoarece $i = 0 + 1 \cdot i$.

Din minimalitatea lui P rezultă că $P' = P$, adică orice element din P are o reprezentare unică în forma (1).

Reciproc, fie că orice element din P poate fi exprimat în mod unic în forma (1). Presupunem că P posedă un subcâmp P' ce conține $\mathbb{R}$ şi are un element $j \in P'$ astfel încât $j^2 = -1$. Atunci $i^2 = j^2 = -1$, de aceea

$$(i + j)(i - j) = i^2 - ij + ji - j^2 = -1 + 1 = 0.$$

Deoarece P nu are divizori ai lui zero, avem $i + j = 0$ sau $i - j = 0$, de unde $j = \pm i$. Atunci pentru orice $x \in P$, conform ipotezei,

$$x = a + bi = a \pm bj,$$

adică $x \in P'$, prin urmare $P = P'$. Aceasta arată minimalitatea câmpului P. □

Acum putem demonstra *unicitatea* sistemului de numere complexe.

Teorema 14.2. *Orice două sisteme de numere complexe* $\mathbb{C}_1$ *şi* $\mathbb{C}_2$ *sunt câmpuri izomorfe:* $\mathbb{C}_1 \cong \mathbb{C}_2$ *adică sistemul de numere complexe este unic, abstracţie făcând de izomorfismul câmpurilor*.

Demonstraţie. Fie $\mathbb{C}_1$ şi $\mathbb{C}_2$ două sisteme de numere complexe, cu unităţile imaginare i_1 şi i_2, respectiv, adică $i_1^2 = -1$ şi $i_2^2 = -1$. Conform lemei 14.1, orice element din $\mathbb{C}_1$ are forma $a + bi_1$ şi, la fel, orice element din $\mathbb{C}_2$ are forma $a + bi_2$, unde $a, b \in \mathbb{R}$. Prin urmare, aplicaţia $f : \mathbb{C}_1 \to \mathbb{C}_2$ definită prin regula $f(a + bi_1) = a + bi_2$, este o bijecţie. Mai mult, din relaţiile (2), (3) şi (4) se vede că operaţiile definite în $\mathbb{C}_1$ şi $\mathbb{C}_2$ se reduc la operaţiile din $\mathbb{R}$, de aceea aplicaţia f păstrează operaţiile, adică este un izomorfism de câmpuri. □

Să trecem la cercetarea problemei despre *existența* sistemului de numere complexe. Ca de obicei, pentru a soluționa această problemă, vom construi o interpretare a sistemului indicat. Ideea construcției este sugerată de Lema 14.1, conform căreia orice element din sistemul căutat este determinat în mod univoc de o pereche ordonată (a,b) de numere reale.

Fie $\mathbb{C}$ mulțimea tuturor perechilor ordonate (a,b) de numere reale. Vom considera că $(a,b)=(c,d)$ dacă şi numai dacă $a=c$ şi $b=d$ (deci, spre deosebire de cazurile precedente, aici nu avem nevoie de trecerea la o mulțime-factor prin relație de echivalență). Având în vedere relațiile (2) şi (3), definim în $\mathbb{C}$ următoarele operații:

$$(a,b)+(c,d)=(a+c,b+d), \tag{5}$$

$$(a,b)(c,d)=(ac-bd,ad+bc), \tag{6}$$

Propoziția 14.3. *Mulțimea* $\mathbb{C}$ *formează un câmp în raport cu operațiile, definite prin relațiile (5) şi (6).*

Demonstrație. Operațiile în $\mathbb{C}$ sunt definite cu ajutorul operațiilor din $\mathbb{R}$, unde au loc legile comutativă, asociativă şi distributivă. Se verifică direct că aceste legi au loc şi în $\mathbb{C}$. Elementul neutru pentru adunare în $\mathbb{C}$ este perechea $(0,0)$. Perechea opusă perechii $(a,b)\in\mathbb{C}$ este $(-a,-b)$. Rolul unității în $\mathbb{C}$ îl joacă perechea $(1,0)=1_{\mathbb{C}}$ (se verifică uşor utilizând relația (6)). Astfel $\mathbb{C}(+,\cdot)$ este un inel comutativ cu element unitate.

Rămâne de arătat că în $\mathbb{C}$ este posibilă împărțirea (operația inversă înmulțirii). Pentru aceasta considerăm ecuația:

$$(a,b)(x,y)=(c,d),$$

unde $(a,b)\neq(0,0)$ (adică $a\neq 0$ sau $b\neq 0$, ceea ce înseamnă că $a^2+b^2\neq 0$). Conform regulii (6), ecuația dată are forma

$$(ax-by,ay+bx)=(c,d),$$

de unde avem:

$$\begin{cases} ax - by = c, \\ bx + ay = d. \end{cases}$$

Din condiția $a^2 + b^2 \neq 0$ rezultă că acest sistem are o singură soluție, şi anume:

$$(x, y) = \left(\frac{ac + bd}{a^2 + b^2}, \frac{ad - bc}{a^2 + b^2} \right),$$

unde $(x, y) = \dfrac{(c, d)}{(a, b)}$ este *câtul* celor două perechi date. Astfel în $\mathbb{C}$ este definită operația împărțirii (la elemente nenule), de aceea $\mathbb{C}$ este un câmp. □

Teorema 14.4 (***existența sistemului de numere complexe***). *Câmpul* $\mathbb{C}$ *conține câmpul numerelor reale* $\mathbb{R}$ *ca subcâmp şi posedă un element* $i \in \mathbb{C}$, *astfel încât* $i^2 = -\mathbf{1}_{\mathbb{C}}$. *Mai mult,* $\mathbb{C}$ *este minimal cu aceste proprietăți, de aceea* $\mathbb{C}$ *este un sistem de numere complexe.*

Demonstrație. Aplicația injectivă $f : \mathbb{R} \to \mathbb{C}$ se defineşte prin regula $f(a) = (a, 0)$ şi în continuare identificăm numărul real $a \in \mathbb{R}$ cu perechea $(a, 0) \in \mathbb{C}$.

Deoarece unitatea câmpului $\mathbb{C}$ are forma $\mathbf{1}_{\mathbb{C}} = (1, 0)$, obținem: $-\mathbf{1}_{\mathbb{C}} = (-1, 0)$. Acum notăm $i = (0, 1)$. Avem:

$$i^2 = (0,1)(0,1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0) = -\mathbf{1}_{\mathbb{C}},$$

adică i este *unitate imaginară* în $\mathbb{C}$.

Având în vedere identificarea lui $a \in \mathbb{C}$ cu $(a, 0)$, din $(b, 0) = b$ şi $(0, 1) = i$ obținem:

$$bi = (b, 0)(0, 1) = (b \cdot 0 - 0 \cdot 1, b \cdot 1 + 0 \cdot 0) = (0, b).$$

De aceea orice element din $\mathbb{C}$ poate fi exprimat în forma:

$$(a, b) = (a, 0) + (0, b) = a + bi,$$

şi această reprezentare este unică. Din Lema 14.1 rezultă că câmpul $\mathbb{C}$ este minimal printre câmpurile ce conțin $\mathbb{R}$ şi au unitate

imaginară. Conform definiției aceasta înseamnă că $\mathbb{C}$ este un sistem de numere complexe. □

Interpretarea $\mathbb{C}$ a sistemului de numere complexe demonstrează *existența* acestei sistem, deci şi *compatibilitatea* sistemului de axiome din Definiția 1.

Expresia $a+bi$, unde $a,b\in\mathbb{R}$ şi $i^2=-1$, se numeşte *forma algebrică* a numărului complex, în care a este *partea reală*, iar bi este *partea imaginară*. Numărul real nenegativ $|a+bi|=\sqrt{a^2+b^2}$ se numeşte *modulul* numărului complex $\alpha=a+bi\in\mathbb{C}$. Numărul $\overline{\alpha}=a-bi$ se numeşte *numărul conjugat* lui α. Aplicația $\alpha\to\overline{\alpha}$ este singurul automorfism netrivial al lui $\mathbb{C}$ care lasă elementele din $\mathbb{R}$ neschimbate. (Demonstrați!)

Sunt posibile şi alte interpretări ale sistemului de numere reale. În continuare vom arăta încă o interpretare de acest tip, bazată pe matrice de formă specială cu elemente din câmpul $\mathbb{R}$.

Teorema 14.5. *Mulțimea de matrice*

$$\mathbb{C}_1=\left\{\begin{pmatrix} a & b\\ -b & a\end{pmatrix}\;\middle|\;\; a,b\in\mathbb{R}\right\}$$

cu operațiile obişnuite de adunare şi înmulțire a matricelor formează un câmp care este izomorf cu câmpul $\mathbb{C}$, *de aceea şi* $\mathbb{C}_1$ *este un sistem de numere complexe.*

Demonstrație. Se verifică uşor faptul că mulțimea de matrice $\mathbb{C}_1$ este închisă în raport cu operațiile adunării şi înmulțirii, formând un câmp în raport cu aceste operații.

Aplicația

$$(a,b)=a+bi\xrightarrow{\varphi}\begin{pmatrix} a & b\\ -b & a\end{pmatrix}$$

din $\mathbb{C}$ în $\mathbb{C}_1$ este bijectivă şi păstrează operaţiile, ceea ce se verifică direct, utilizând regulile (2), (3) şi regulile obişnuite de adunare şi înmulţire a matricelor.

De exemplu, pentru operaţia înmulţirii avem:

$$\varphi((a+bi)(c+di)) = \varphi((ac-bd)+(ad+bc)i) = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix},$$

$$\varphi(a+bi)\cdot\varphi(c+di) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}.$$

Comparând rezultatele, vedem că φ păstrează operaţia înmulţirii. La fel, chiar mai simplu, se verifică acest fapt pentru adunare.

Din cele expuse mai sus rezultă că $\mathbb{C} \cong \mathbb{C}_1$. □

Următoarea afirmaţie arată o proprietate specifică a câmpului de numere complexe (spre deosebire de toate sistemele numerice precedente).

Propoziţia 14.6. *Câmpul numerelor complexe nu poate fi liniar ordonat.*

*Demonstraţie***.** În orice câmp ordonat $P(\leq)$ are loc legea semnelor şi legea trihotomiei (vezi Anexa II), de aceea pentru orice element $0 \neq a \in P$ sunt posibile două cazuri:

1) $a > 0$, atunci $a^2 = a \cdot a > 0$

2) $a < 0$, atunci $a^2 = (-a)^2 = (-a)(-a) > 0.$

Dar în câmpul numerelor complexe avem elementul $i \neq 0$ (unitatea imaginară), pentru care $i^2 = -1 < 0$. □

Acum vom aminti câteva rezultate cunoscute din cursul general de algebră care se referă la numerele complexe.

Importanța deosebită şi puterea extraordinară a teoriei numerelor complexe rezultă din faptul că în câmpul $\mathbb{C}$ are soluție nu numai ecuația $x^2+1=0$, care a servit drept punct de plecare la definirea lui $\mathbb{C}$, dar şi orice ecuație de forma

$$a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n=0 \qquad (7)$$

unde $n\geq 1$ şi $a_0\neq 0$. Dacă $a_0\neq 0$, ecuația (7) are în $\mathbb{C}$ exact n rădăcini (considerând şi ordinul de multiplicitate al lor).

Câmpul P se numeşte *algebric închis* dacă orice polinom cu coeficienții din P, de grad $n\geq 1$, are cel puțin o rădăcină în câmpul P. Unul dintre rezultatele remarcabile în domeniul algebrei este

Teorema 14.7 (***teorema fundamentală a algebrei***). *Câmpul numerelor complexe este algebric închis.* □

Demonstrația acestei teoreme poate fi găsită, de exemplu, în [26]. În particular, din teorema fundamentală a algebrei rezultă că *orice polinom de grad* $n\geq 1$, *cu coeficienți complecşi, se descompune peste câmpul* $\mathbb{C}$ *în produs de binoame de gradul 1.*

Să amintim că un polinom $f(X)$ cu coeficienții din câmpul P se numeşte *ireductibil* peste P dacă el nu poate fi descompus în produs de polinoame (netriviale) de grad mai mic peste P. Astfel, din teorema fundamentală a algebrei rezultă că peste câmpul $\mathbb{C}$ sunt ireductibile numai polinoamele de gradul 1. Cu totul alta este situația în câmpul numerelor reale $\mathbb{R}$ care nu este algebric închis şi în care are loc

Teorema 14.8. *Orice polinom de gradul* $n\geq 1$, *cu coeficienții în câmpul numerelor reale* $\mathbb{R}$, *se descompune într-un produs de polinoame ireductibile peste* $\mathbb{R}$ *care au gradul 1 sau gradul 2 (polinoamele ireductibile de gradul 2 corespund perechilor de rădăcini complexe conjugate).* □

Exerciţii

1. Fie dat polinomul $f(X)=X^3-X^2+X+4$. Posedă oare $f(X)$ rădăcini complexe z cu proprietatea $|z|\le 1$?

2. Fie n un număr natural nenul şi $w=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$. Spunem că numărul complex z este o rădăcină primitivă de ordinul n din 1 dacă pentru $k=0,1,2,\ldots,n-1$ numerele z^k sunt toate soluţiile ecuaţiei $x^n=1$. Demonstraţi că z este o rădăcină primitivă de ordinul n din 1 dacă şi numai dacă există un număr întreg pozitiv $1\le m<n$, $(m,n)=1$, astfel încât $z=w^m$.

3. Funcţia exponenţială $f:\mathbb{R}\to\mathbb{R}, f(x)=e^x$, se prelungeşte pe mulţimea numerelor complexe în felul următor $f:\mathbb{C}\to\mathbb{C}$, $f(z)=e^x(\cos y+i\sin y)$, unde $z=x+iy$, $x,y\in\mathbb{C}$. Notăm $f(z)=e^z$. Demonstraţi egalităţile:

a) $e^{z_1+z_2}=e^{z_1}e^{z_2}$, $\forall z_1,z_2\in\mathbb{C}$; b) $e^{kz}=(e^z)^k$, $\forall z\in\mathbb{C}$, $\forall k\in\mathbb{Z}$;

c) $e^{2n\pi i}=1$, $\forall n\in\mathbb{Z}$.

§15. Corpul cuaternionilor

În afară de câmpul numerelor complexe $\mathbb{C}$ mai există şi alte extensiuni ale câmpului numerelor reale $\mathbb{R}$. Am văzut că pentru a obţine câmpul $\mathbb{C}$ este suficient de adăugat câmpului $\mathbb{R}$ un element i cu condiţia $i^2=-1$. Acum vom generaliza această construcţie adăugând câmpului $\mathbb{R}$ nu numai o singură unitate imaginară, dar trei unităţi de acest tip: i,j şi k, cu condiţii speciale, care se exprimă printr-un tabel al înmulţirii elementelor unitare i,j,k. Important este faptul că în acest caz noi (pentru prima oară) renunţăm la comutativitatea înmulţirii, adică vom construi un corp necomutativ, ce conţine câmpul $\mathbb{R}$.

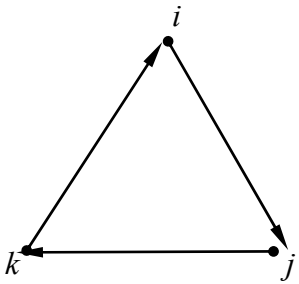
Definiţia 1. *Sistem de cuaternioni* se numeşte corpul minimal $\mathbb{H}$ care conţine $\mathbb{R}$ ca subcâmp şi posedă astfel de

elemente i, j, k, ce comută cu toate numerele reale şi satisfac condiţiile:

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j \qquad (1)$$

Aceste condiţii se pot exprima prin tabelul:

·	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1



Din definiţie este evident că sistemul de cuaternioni nu este comutativ. Pentru a demonstra *unicitatea* sistemului de cuaternioni, noi procedăm în mod obişnuit, indicând mai întâi o condiţie echivalentă cerinţei de minimalitate din Definiţia 1.

Lema 15.1. *Fie K un corp ce conţine $\mathbb{R}$ şi posedă elementele i, j şi k cu proprietăţile din Definiţia 1. Corpul K este minimal cu aceste proprietăţi (adică este un sistem de cuaternioni) dacă şi numai dacă orice element x din K posedă o reprezentare (unică) în forma*

$$x = a + bi + cj + dk, \qquad (2)$$

unde $a, b, c, d \in \mathbb{R}$.

Demonstraţie. ($\Rightarrow$) Fie K un sistem de cuaternioni (Definiţia 1). Separăm în K următoarea submulţime:

$$K' = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}.$$

Utilizând proprietăţile operaţiilor din K (asociativitatea şi distributivitatea), se verifică uşor faptul că operaţiile în K' se efectuează conform următoarelor reguli:

$$\begin{aligned}&\left(a_1+b_1i+c_1j+d_1k\right)\pm\left(a_2+b_2i+c_2j+d_2k\right)=\\&=\left(a_1\pm a_2\right)+\left(b_1\pm b_2\right)i+\left(c_1\pm c_2\right)j+\left(d_1\pm d_2\right)k,\end{aligned}\tag{3}$$

şi

$$\begin{aligned}&\left(a_1+b_1i+c_1j+d_1k\right)\cdot\left(a_2+b_2i+c_2j+d_2k\right)=\\&=\left(a_1a_2-b_1b_2-c_1c_2-d_1d_2\right)+\left(a_1b_2+b_1a_2+c_1d_2-d_1c_2\right)i+\\&+\left(a_1c_2+c_1a_2+d_1b_2-b_1d_2\right)j+\left(a_1d_2+d_1a_2+b_1c_2-c_1b_2\right)k.\end{aligned}\tag{4}$$

Din aceste relaţii se vede că mulţimea K' este închisă în raport cu adunarea şi înmulţirea, definite în K. Mai mult, $K'\supseteq\mathbb{R}$ (această incluziune o obţinem luând $b=c=d=0$) şi K' conţine elementele i,j,k (de exemplu, $i=0+1\cdot i+0\cdot j+0\cdot k$). Deoarece

$$a_1+b_1i+c_1j+d_1k=a_2+b_2i+c_2j+d_2k\quad\Leftrightarrow$$

$$\Leftrightarrow\quad a_1=a_2,\quad b_1=b_2,\quad c_1=c_2,\quad d_1=d_2,$$

orice element din K' se exprimă în forma (2) în mod unic.

Pentru a vedea că K' este un subcorp în K să arătăm că K' este închis în raport cu operaţia împărţirii. Considerăm ecuaţia:

$$(a+bi+cj+dk)(x+yi+uj+vk)=1=1+0\cdot i+0\cdot j+0\cdot k,$$

Unde $a+bi+cj+dk\neq 0$, adică $a^2+b^2+c^2+d^2\neq 0$. Efectuând înmulţirea conform regulii (4), obţinem:

$$\begin{aligned}&(ax-by-cu-dv)+(ay+bx+cv-du)i+\\&+(au+cx+dy-bv)j+(av+dx+bu-cy)k=1.\end{aligned}$$

Egalând coeficienţii respectivi, avem următorul sistem de ecuaţii şi matricea lui:

$$\begin{cases}ax-by-cu-dv=1,\\bx+ay-du+cv=0,\\cx+dy+au-bv=0,\\dx-cy+bu+av=0.\end{cases}\qquad\left(\begin{array}{cccc|c}a&-b&-c&-d&1\\b&a&-d&c&0\\c&d&a&-b&0\\d&-c&b&a&0\end{array}\right)\tag{5}$$

Determinantul sistemului (5) este $(a^2+b^2+c^2+d^2)^2\neq 0$,

deci acest sistem are o singură soluție și anume:

$$x=\frac{a}{\Delta}, y=\frac{-b}{\Delta}, u=\frac{-c}{\Delta}, v=\frac{-d}{\Delta}, \tag{6}$$

unde $\Delta=a^2+b^2+c^2+d^2$.

Din cele demonstrate mai sus rezultă că orice element nenul din K' posedă element invers, adică în K' are loc operația împărțirii (la elemente nenule), prin urmare K' este un corp. Acum din minimalitatea lui K rezultă că $K'=K$, adică orice element din K posedă reprezentare (unică) în formă (2).

($\Leftarrow$) Fie $K\supseteq\mathbb{R}$ şi K conține elementele i,j,k, care se înmulțesc conform egalităților (1). Mai mult, presupunem că orice element din K are reprezentare în forma (2). Atunci orice subcorp $K_1\subseteq K$, ce conține $\mathbb{R}$ şi elementele i,j,k, este obligat să conțină şi toate elementele de forma $a+bi+cj+dk$, unde $a,b,c,d\in\mathbb{R}$, prin urmare $K_1=K$. Deci corpul K este minimal cu proprietățile arătate. □

Lema demonstrată ne permite să arătăm unicitatea sistemului de cuaternioni, abstracție făcând de izomorfism.

Teorema15.2. *Orice două sisteme de cuaternioni* $\mathbb{H}'$ *şi* $\mathbb{H}''$ *sunt corpuri izomorfe.*

Demonstrație. Lema 15.1 arată că orice element din $\mathbb{H}'$ şi orice element din $\mathbb{H}''$ se exprimă în mod unic în forma (2) prin unitățile respective, de aceea este clar că corespondența:

$$a+bi'+cj'+dk'\to a+bi''+cj''+dk''$$

din $\mathbb{H}'$ în $\mathbb{H}''$ defineşte un izomorfism de corpuri. □

Trecem la demonstrarea *existenței* sistemului de cuaternioni, arătând două interpretări ale lui.

Fie $\mathbb{H} = \{(a,b,c,d) \mid a,b,c,d \in \mathbb{R}\}$ mulțimea tuturor cuadruplelor (cuartetelor) ordonate de numere reale. Adunarea şi înmulțirea lor se definesc în mod similar cu regulile (3) şi (4). Atunci are loc:

Teorema 15.3. $\mathbb{H}(+,\cdot)$ *este un sistem de cuaternioni*.

Demonstrație. Proprietățile operațiilor în $\mathbb{H}$ se verifică în mod direct, utilizând (3), (4) şi faptul că aceste proprietăți au loc în $\mathbb{R}$. Elementul neutru pentru adunare este $(0,0,0,0)$, iar elementul opus lui (a,b,c,d) este $(-a,-b,-c,-d)$. Unitatea în $\mathbb{H}$ are forma $(1,0,0,0)$, iar elementul invers lui $(a,b,c,d) \neq 0$ este

$$\left(\frac{a}{\Delta}, \frac{-b}{\Delta}, \frac{-c}{\Delta}, \frac{-d}{\Delta}\right),$$

unde $\Delta = a^2 + b^2 + c^2 + d^2 \neq 0$ (vezi demonstrația lemei 15.1). Prin urmare, $\mathbb{H}$ este un corp. Incluziunea $\mathbb{R} \to \mathbb{H}$ se obține prin aplicația: $a \to (a,0,0,0)$. Rolul unităților imaginare îl joacă elementele din $\mathbb{H}$**:**

$$i = (0,1,0,0), \quad j = (0,0,1,0), \quad k = (0,0,0,1).$$

Din regula înmulțirii elementelor din $\mathbb{H}$ (vezi (4)), se deduce faptul că elementele $1, i, j, k$ din $\mathbb{H}$ se înmulțesc conform tabelului (1) şi comută cu numerele reale. Mai mult, identificând elementul $a \in R$ cu $(a,0,0,0) \in H$, avem

$$(a,0,0,0)\cdot(0,1,0,0) = ai,$$

şi orice element din $\mathbb{H}$ are o descompunere unică în forma:

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

$$= (a,0,0,0) + (0,b,0,0) + (0,0,c,0) + (0,0,0,d) =$$

$$= a + bi + cj + dk.$$

Din existența acestei reprezentări, conform Lemei 15.1, rezultă minimalitatea lui $\mathbb{H}$ cu proprietățile din Definiția 1, prin urmare $\mathbb{H}$ este un sistem de cuaternioni. □

Această formă de reprezentare a cuaternionilor (şi însăşi sistemul de cuaternioni) a fost creată de celebrul matematician irlandez W.Hamilton în anul 1843.

Ca şi în cazul numerelor complexe, pentru cuaternioni mai avem o interpretare interesantă, bazată pe matrice cu elemente din câmpul $\mathbb{C}$. Notăm:

$$\mathbb{H}_1 = \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} | \, \alpha, \beta \in \mathbb{C} \right\},$$

unde α şi β sunt numere complexe şi dacă $\alpha = a + bi$ atunci $\overline{\alpha} = a - bi$ este numărul complex conjugat . Operaţiile de adunare şi înmulţire în $\mathbb{H}_1$ se efectuează conform regulilor obişnuite de adunare şi înmulţire a matricelor. Mai întâi se verifică faptul că mulţimea de matrice $\mathbb{H}_1$ este închisă în raport cu operaţiile (+) şi $(\cdot)$. Mai mult, pentru orice matrice din $\mathbb{H}_1$ există matricea opusă

$$\begin{pmatrix} -\alpha & -\beta \\ \overline{\beta} & -\overline{\alpha} \end{pmatrix},$$

care la fel este din $\mathbb{H}_1$, deci $\mathbb{H}_1 (+,\cdot)$ este un inel. Mai mult, acest inel este necomutativ, deoarece, de exemplu,

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

Orice matrice nenulă din $\mathbb{H}$ are determinantul nenul: dacă $\alpha = a + bi$ şi $\beta = c + di$, atunci numărul

$$\begin{vmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{vmatrix} = \alpha\overline{\alpha} + \beta\overline{\beta} = a^2 + b^2 + c^2 + d^2$$

este egal cu zero, dacă şi numai dacă $a = b = c = d = 0$. Prin urmare, orice matrice nenulă din $\mathbb{H}_1$, posedă matrice inversă

$$\frac{1}{a^2 - b^2 - c^2 - d^2} \begin{bmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{bmatrix},$$

dar aceasta înseamnă că $\mathbb{H}_1$ *este un corp*.

Este evident din definiție că $\mathbb{C}_1 \subseteq \mathbb{H}_1$, unde $\mathbb{C}_1$ constă din matricele de forma

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

$a, b \in \mathbb{R}$ (vezi Teorema 13.5). Astfel avem situația:

$$\mathbb{R} \subseteq \mathbb{C} \cong \mathbb{C}_1 \subseteq \mathbb{H}_1,$$

adică $\mathbb{H}_1$ poate fi considerat o lărgire (= extindere) a câmpului $\mathbb{C}$, deci şi a câmpului $\mathbb{R}$. În corpul $\mathbb{H}_1$ unitatea are forma

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

deci

$$-1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Mai mult, rolul unităților imaginare îl vor avea următoarele elemente din $\mathbb{H}_1$:

$$\mathrm{I} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

unde i este unitatea imaginară a câmpului $\mathbb{C}$.

Orice matrice din $\mathbb{H}_1$ se poate reprezenta univoc în forma:

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} =$$

$$= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} +$$

$$+ \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} =$$

$$= a \cdot 1 + b \cdot I + c \cdot J + d \cdot K.$$

Din cele menționate mai sus rezultă:

Teorema 15.4. *Corpul* $\mathbb{H}_1$ *este un sistem de cuaternioni (prin urmare,* $\mathbb{H} \cong \mathbb{H}_1$*).* □

În continuare vom nota prin $\mathbb{H}$ un sistem arbitrar de cuaternioni cu unitatea reală 1 şi unităţile imaginare i, j şi k. Astfel, elementele bazei $\{1, i, j, k\}$ se înmulţesc conform tabelului (1) şi orice element $\alpha \in \mathbb{H}$ se exprimă univoc în forma

$$\alpha = a + bi + cj + dk,$$

unde $a, b, c, d \in \mathbb{R}$. Este clar, că înmulțirea elementelor din $\mathbb{H}$ este complet definită de tabelul înmulţirii elementelor bazei. Pentru elementul $\alpha = a + bi + cj + dk \in \mathbb{H}$ notăm prin $\overline{\alpha} = a - bi - cj - dk$ *cuaternionul conjugat* lui α. Numărul real

$$N(\alpha) = \alpha\overline{\alpha} = \overline{\alpha}\alpha = a^2 + b^2 + c^2 + d^2$$

se numeşte *norma* cuaternilonului α. Următoarele afirmaţii se verifică în mod direct: a) $\alpha = 0 \Leftrightarrow N(\alpha) = 0$; b) $\overline{\alpha\beta} = \overline{\alpha} \cdot \overline{\beta}$; c) $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$; d) $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$.

Orice cuaternion $\alpha \neq 0$ este inversabil şi

$$\alpha^{-1} = \frac{\overline{\alpha}}{N(\alpha)},$$

deoarece

$$\alpha \cdot \frac{\overline{\alpha}}{N(\alpha)} = \frac{\alpha\overline{\alpha}}{N(\alpha)} = 1.$$

Ecuaţia $\alpha x = \beta$ $(\alpha \neq 0)$ se rezolvă, înmulţind ambele părţi ale ei *din stânga* cu α^{-1}, adică:

$$x = \alpha^{-1}\beta = \frac{\overline{\alpha}\beta}{N(\alpha)};$$

Ecuația $x\alpha = \beta \quad (\alpha \neq 0)$ se rezolvă în mod similar, înmulțind ecuația *la dreapta* cu α^{-1} şi obținând:

$$x = \beta\alpha^{-1} = \frac{\beta\overline{\alpha}}{N(\alpha)}.$$

Uşor se verifică relația:

$$N(\alpha^{-1}) = \frac{1}{N(\alpha)}.$$

Este interesant de observat că câmpul numerelor complexe $\mathbb{C}$ poate fi inclus în $\mathbb{H}$ în trei moduri (spre deosebire de cazurile precedente, când incluziunile respective se definesc univoc):

$$\mathbb{C} \cong \{a + bi \mid a, b \in R\},$$
$$\mathbb{C} \cong \{a + cj \mid a, c \in R\},$$
$$\mathbb{C} \cong \{a + dk \mid a, d \in R\}.$$

Teoria cuaternionilor este bine dezvoltată şi ea are o serie de aplicări interesante în multe domenii ale matematicii (teoria numerelor, calculul vectorial, etc.).

Exerciții

1. Demonstrați afirmațiile:
   a) $\alpha = 0 \Leftrightarrow N(\alpha) = 0$;
   b) $\overline{\alpha\beta} = \overline{\alpha} \cdot \overline{\beta}$;
   c) $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$;
   d) $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$.

§16. Algebre cu diviziune peste câmpul $\mathbb{R}$. Teorema lui Frobenius

Încercările de a extinde în continuare sistemele numerice au adus la apariția unor noi domenii ale matematicii: teoria spațiilor vectoriale, teoria algebrelor (sau a sistemelor hipercomplexe). Să analizăm ultimele trei sisteme numerice $\mathbb{R}$, $\mathbb{C}$ şi $\mathbb{H}$ studiate în compartimentele precedente, comparându-le între ele:

1) în $\mathbb{R}$ există un element $1 \in \mathbb{R}$, prin care toate celelalte se exprimă ca o combinație liniară trivială: $r = r \cdot 1$;
2) în $\mathbb{C}$ există două elemente $\{1, i\}$ astfel încât orice element $a + bi$ din $\mathbb{C}$ se exprimă ca o combinație liniară $a \cdot 1 + b \cdot i$ cu coeficienți $a, b \in \mathbb{R}$;
3) în $\mathbb{H}$ există un sistem din patru elemente $\{1, i, j, k\}$, prin care orice element din $\mathbb{H}$ se exprimă în forma de combinație liniară $a \cdot 1 + b \cdot i + c \cdot j + b \cdot k$ cu coeficienți reali.

De aceea apare în mod firesc întrebarea: există oare alte extensiuni ale câmpului $\mathbb{R}$ cu alt număr n de elemente ale bazei (diferite de cele arătate mai sus, unde $n = 1, 2, 4$)? Scopul acestui paragraf constă în formularea şi argumentarea răspunsului complet la întrebarea dată. Pentru aceasta avem nevoie de câteva noțiuni şi rezultate preliminare, pe care le reamintim în cele ce urmează.

Definiția 1. ***Spațiu vectorial*** *V peste câmpul $\mathbb{R}$ se numeşte grupul abelian $V(+)$ cu aplicația*

$$\mathbb{R} \times V \to V, \quad (a, v) \to av \in V,$$

care satisface condițiile:

$$a(u + v) = au + av, \quad (a + b)u = au + bu,$$

$$(ab)u = a(bu), \quad 1 \cdot v = v,$$

pentru $\forall\, a, b \in \mathbb{R}$ şi $\forall\, u, v \in V$. Spațiul vectorial V peste $\mathbb{R}$ se numeşte ***n-dimensional*** *dacă posedă o bază ce constă din n*

elemente, adică există un sistem liniar independent $u_1, u_2, \ldots, u_n$ în V *încât orice* $x \in V$ *se exprimă în mod univoc în forma:*

$$x = a_1u_1 + a_2u_2 + \ldots + a_nu_n$$

unde $a_1, a_2, \ldots, a_n \in \mathbb{R}$.

Elementele $u_1, u_2, \ldots, u_n \in V$ *se numesc* ***liniar independente*** *dacă din relația*

$$a_1u_1 + a_2u_2 + \ldots + a_nu_n = 0$$

rezultă $a_i = 0$, *pentru orice* $i = 1, 2, \ldots, n$.

Spațiul vectorial V peste $\mathbb{R}$ de dimensiunea n se determină în mod unic (în limitele unui izomorfism) de dimensiunea sa, deoarece în acest caz avem:

$${}_RV \cong \underbrace{\mathbb{R} \times \mathbb{R} \times \ldots \times \mathbb{R}}_{n-ori} = \left\{ (a_1, a_2 \ldots a_n) \mid a_i \in \mathbb{R} \right\},$$

unde operațiile pe produsul cartezian a n exemplare ale câmpului $\mathbb{R}$ se definesc „pe componente". În calitate de bază se poate lua mulțimea vectorilor unitari:

$$e_1 = (1, 0, \ldots, 0), \quad e_2 = (0, 1, 0, \ldots, 0), \quad \ldots, \quad e_n = (0, 0, \ldots, 0, 1).$$

Acum introducem noțiunea principală utilizată în acest compartiment.

Definiția 2. ***Algebră*** *asociativă de rangul* n *peste câmpul* $\mathbb{R}$ *(sau* $\mathbb{R}$***-algebră*** *asociativă de rangul* n*) se numeşte un spațiu vectorial* A *peste* $\mathbb{R}$ *de dimensiunea* n *dacă în* A *este definită şi operația înmulțirii* $(\cdot)$ *care este asociativă, este distributivă în raport cu operația adunării (la stânga şi la dreapta) şi are loc condiția:*

$$(au)v = u(av) = a(uv), \qquad (1)$$

pentru orice $a \in \mathbb{R}$ *şi orice* $u, v \in A$ *(prin urmare,* $A(+, \cdot)$ *este un inel asociativ). Dacă* $A(+, \cdot)$ *este un* ***corp*** *(adică orice element* $u \in A$, $u \neq 0$, *posedă invers), atunci* A *se numeşte* ***algebră cu***

diviziune *peste* $\mathbb{R}$. ***Rang*** *al algebrei* A *se numeşte dimensiunea spaţiului vectorial* ${}_{\mathbb{R}}A$.

Astfel, conform definiţiei, pe algebra ${}_{\mathbb{R}}A$ sunt definite trei operaţii:

1) operaţia internă de adunare $(+)$, în raport cu care $A(+)$ este un *grup abelian*;
2) operaţia externă de înmulţire a vectorilor din A cu scalarii din $\mathbb{R}$; împreună cu adunarea această operaţie defineşte pe A structura de *spaţiu vectorial* peste $\mathbb{R}$;
3) operaţia internă de înmulţire în A, care împreună cu operaţia de adunare $(+)$ defineşte pe A structura de *inel* (sau de *corp* în cazul algebrelor cu diviziune).

Observaţii.

1. Fie A o algebră asociativă cu diviziune peste $\mathbb{R}$. Atunci A este un corp, deci are unitate, fie $e \in A$. Mai mult, în A se poate efectua împărţirea la elemente nenule. Aplicaţia:

$$\mathbb{R} \to A, \quad a \to ae,$$

este injectivă şi, identificând numerele reale $a \in \mathbb{R}$ cu vectorii $ae \in A$, putem considera că A conţine câmpul $\mathbb{R}$. Din relaţiile (1) se vede că $au = ua$ pentru orice $a \in \mathbb{R}$ şi $u \in A$, prin urmare, $\mathbb{R}$ se conţine în centrul algebrei A. De aceea în continuare considerăm că $\mathbb{R} \subseteq A$ şi drept unitate în A serveşte numărul $1 \in \mathbb{R}$.

2. Dacă A este o algebră asociativă cu diviziune peste $\mathbb{R}$ de rangul n şi ea are baza $\{e_1, e_2, ..., e_n\}$, atunci orice element din A se exprimă în mod unic în forma

$$\sum_{i=1}^{n} a_i e_i$$

şi înmulţirea în A se efectuează prin regula:

$$\left(\sum_{i=1}^{n} a_i e_i\right)\cdot\left(\sum_{j=1}^{n} b_j e_j\right)=\sum_{i=1}^{n}\sum_{j=1}^{n}\left(a_i b_j\right)\left(e_i e_j\right).$$

Prin urmare, operaţia înmulţirii în A este complet determinată de tabela înmulţirii elementelor bazei.

În expunerea de mai departe vom considera numai $\mathbb{R}$-*algebre asociative de rang finit.*

Pentru ilustrarea Definiţiei 1, acum putem arăta câteva *exemple* de algebre asociative cu diviziune peste $\mathbb{R}$.

1. Însăşi *câmpul* $\mathbb{R}$ poate fi considerat (în mod trivial) ca algebră (asociativă şi comutativă) cu diviziune peste $\mathbb{R}$ (în acest caz înmulţirea externă coincide cu cea internă). Algebra ${}_{\mathbb{R}}\mathbb{R}$ are baza $\{1\}$, deci are rangul $n=1$. Este evident, că orice algebră asociativă cu diviziune peste $\mathbb{R}$ de rangul 1 este izomorfă cu algebra ${}_{\mathbb{R}}\mathbb{R}$.

2. *Câmpul* $\mathbb{C}$ al numerelor complexe este o algebră asociativă, comutativă, cu diviziune peste $\mathbb{R}$, o bază a ei fiind $\{1,i\}$, deci ${}_{\mathbb{R}}\mathbb{C}$ are rangul doi.

3. *Corpul cuaternionilor* $\mathbb{H}$ este o algebră peste $\mathbb{R}$ (asociativă, cu diviziune, dar necomutativă), una din bazele ei fiind $\{1,i,j,k\}$, prin urmare, ${}_{\mathbb{R}}H$ este o $\mathbb{R}$-algebră de rangul 4.

Întrebarea formulată anterior acum poate fi interpretată astfel: *mai există oare alte* $\mathbb{R}$*-algebre asociative cu diviziune de rang finit peste* $\mathbb{R}$ *sau exemplele indicate epuizează toată rezerva de* $\mathbb{R}$*- algebre de acest tip?*

Surprinzător este faptul că alte $\mathbb{R}$-algebre de tipul dat, în afară de $\mathbb{R},\mathbb{C}$ şi $\mathbb{H}$**,** ***nu există***. Acesta este sensul celebrei teoreme a lui Frobenius, pe care o vom demonstra în continuare în câteva etape cu ajutorul unor afirmaţi auxiliare.

Lema 16.1. *Dacă A este o $\mathbb{R}$-algebră asociativă de rangul n, atunci pentru $k > n$ orice k elemente din A sunt liniar dependente peste $\mathbb{R}$.*

Demonstrația rezultă din definiția bazei (baza conține un număr maximal de elemente liniar independente). □

Lema 16.2. *Fie A o $\mathbb{R}$-algebră asociativă de rangul n. Atunci orice element $\alpha \in A$ este rădăcină a unui polinom de gradul $k \le n$ cu coeficienții în câmpul $\mathbb{R}$.*

Demonstrație. Considerăm $n+1$ elemente: $1, \alpha, \alpha^2, ..., \alpha^n$, unde α este un element nenul din A. Deoarece A are rangul n, ele sunt liniar dependente (conform Lemei 16.1). Prin urmare, există elementele $a_1, a_1 .... , a_n \in \mathbb{R}$ (nu toate egale cu zero) încât

$$a_0 \cdot 1 + a_1 \cdot \alpha + \ldots + a_n \alpha^n = 0,$$

adică α este rădăcină a polinomului

$$f(X) = a_0 + a_1 X + ... + a_n X^n$$

cu coeficienții din $\mathbb{R}$. □

Se poate întâmpla că α este rădăcină şi pentru un polinom de grad $k < n$ (principiul celui mai mic număr).

Propoziția 16.3. *Fie A o algebră asociativă cu diviziune peste $\mathbb{R}$ de rangul n. Atunci:*

1) *orice element $\alpha \in A$ este rădăcină a unui polinom de gradul 1 sau de gradul 2, ireductibil peste $\mathbb{R}$; în acest caz: $\alpha \notin \mathbb{R}$ dacă si numai dacă α este rădăcină a unui polinom de gradul 2, ireductibil peste $\mathbb{R}$, ceea ce la rândul său, este echivalent cu faptul că există numerele reale $a \neq 0$ şi a', încât*

$$(a\alpha + a')^2 = -1;$$

2) *dacă* $n=2$, *atunci algebra* ${}_{\mathbb{R}}A$ *este izomorfă cu algebra numerelor complexe* ${}_{\mathbb{R}}\mathbb{C}$.

Demonstrație. 1) Orice polinom cu coeficienții din $\mathbb{R}$, de gradul $n>0$, se descompune în produs de polinoame ireductibile peste $\mathbb{R}$ de gradul 1 sau de gradul 2 (Teorema 14.7). Conform Lemei 16.2, orice element $\alpha \in A$ este rădăcină a unui polinom

$$f(X)=a_0+a_1X+....+a_nX^n$$

cu coeficienții reali. Luăm descompunerea acestui polinom în produs de polinoame ireductibile peste $\mathbb{R}$, de gradul 1 sau 2:

$$f(X)=\varphi_1(X)\cdot\varphi_2(X)....\varphi_s(X),\ 1\le s\le n.$$

Aici polinoamele de gradul 1 corespund rădăcinilor reale, iar cele de gradul 2 corespund perechilor $(a,\overline{\alpha})$ de rădăcini complexe. Pentru $\alpha \in A$, avem

$$f(\alpha)=\varphi_1(\alpha)\cdot\varphi_2(\alpha)....\varphi_s(\alpha)=0$$

deoarece în A (ca şi în orice corp) nu sunt divizori ai lui 0, există $i\in\{1,....,s\}$, încât $\varphi_i(\alpha)=0$. Aceasta demonstrează prima parte a afirmației 1).

Elementul $\alpha \in A$ aparține lui $\mathbb{R}$ dacă şi numai dacă polinomul $\varphi_i(X)$ cu proprietatea $\varphi_i(\alpha)=0$ are gradul 1. Prin urmare, $\alpha \notin \mathbb{R}$ dacă şi numai dacă $\varphi_i(X)$ este un polinom de gradul 2, ireductibil peste $\mathbb{R}$. Presupunem că acest polinom este X^2+pX+q, adică

$$\alpha^2+p\alpha+q=0, \qquad (2)$$

unde $p,q\in\mathbb{R}$. Din condiția $\alpha\notin\mathbb{R}$ rezultă că $p^2-4q<0$ (în caz contrar rădăcinile acestui polinom ar fi numere reale). Deoarece avem $4q-p^2>0$ şi în $\mathbb{R}$ se poate extrage rădăcina din numere pozitive, există $b\in\mathbb{R}, b\neq 0$, încât

$$b^2 = \frac{1}{4q - p^2}.$$

Înmulțind egalitatea (2) cu $4b^2$, obținem:

$$4b^2\alpha^2 + 4b^2 p\alpha + 4b^2 q = 0,$$

şi, deoarece $b^2p^2 + 1 = 4b^2q$, avem $4b^2\alpha^2 + 4b^2 p\alpha + b^2p^2 + 1 = 0$, de unde $(2b\alpha + bp)^2 + 1 = 0$, adică $(2b\alpha + bp)^2 = -1, b \neq 0$. Aceasta demonstrează afirmația 1).

2) Fie A o $\mathbb{R}$-algebră asociativă cu diviziune de rangul 2. Atunci $\mathbb{R} \subset A$ şi există un element $\alpha \in A$ încât $\alpha \notin \mathbb{R}$. În acest caz elementele $\{1, \alpha\}$ sunt liniar independente peste $\mathbb{R}$. Atunci pentru orice $a, a' \in \mathbb{R}$ $(a \neq 0)$ şi elementele $\{1, \tau = a\alpha + a'\}$ sunt liniar independente peste $\mathbb{R}$ (dacă avem $b \cdot 1 + c \cdot \tau = 0$ pentru $c \neq 0$, atunci $b + ca\alpha + ca' = 0$ şi $\alpha \in \mathbb{R}$, contradicție). Alegem numerele $0 \neq a$, $a' \in \mathbb{R}$, astfel încât $\tau^2 = (a\alpha + a')^2 = -1$ (posibilitatea unei astfel de alegeri a fost arătată în afirmația 1)). Deoarece algebra A are rangul 2 şi elementele $\{1, \tau\}$ sunt liniar independente, putem face concluzia că perechea $\{1, \tau\}$ formează o bază în A, adică orice element din A se exprimă în mod unic în forma $a + b\tau$, unde $a, b \in \mathbb{R}$. Atunci uşor se vede că aplicația $a + b\tau \to a + bi$ defineşte un izomorfism: ${}_{\mathbb{R}}A \cong {}_{\mathbb{R}}\mathbb{C}$. □

Din propoziția demonstrată rezultă următoarea **concluzie**: *abstracție făcând de izomorfism, singura $\mathbb{R}$-algebră asociativă cu diviziune de rangul 2 este ${}_{\mathbb{R}}\mathbb{C}$.*

Acum este firesc să trecem la cercetarea cazului $\mathbb{R}$-agebrelor asociative cu diviziune, de rangul $n = 3$. Răspunsul este dezamăgitor.

Lema 16.4. *Peste câmpul $\mathbb{R}$ algebre asociative cu diviziune, de rangul 3, nu există.*

Demonstrație. Fie A o $\mathbb{R}$-algebră asociativă cu diviziune de rangul $n \geq 3$. Aplicând afirmația 1) din Propoziția 16.3, putem selecta $\alpha \in A$, $\alpha \notin \mathbb{R}$, încât elementele $\{1, \alpha\}$ să fie liniar independente și $\alpha^2 = -1$. Deoarece rangul algebrei A este $n \geq 3$, putem aplica încă o dată acelaşi procedeu, separând un element $\beta \notin \mathbb{R}$, astfel încât $\beta^2 = -1$ şi elementele $\{1, \alpha, \beta\}$ să fie liniar independente. Vom arăta că în acest caz elementele $\{1, \alpha, \beta, \alpha\beta\}$ sunt *liniar independente* peste $\mathbb{R}$ şi astfel vom obține $n \geq 4$, ceea ce demonstrează lema.

Reducere la absurd: presupunem că elementele $\{1, \alpha, \beta, \alpha\beta\}$ sunt liniar dependente peste $\mathbb{R}$. Atunci există numerele reale $a, b, c \in \mathbb{R}$ încât

$$\alpha\beta = a + b\alpha + c\beta.$$

Înmulțind din stânga la α, obținem

$$\alpha^2\beta = a\alpha + b\alpha^2 + c\alpha\beta,$$

adică

$$-\beta = a\alpha - b + c(a + b\alpha + c\beta).$$

Transformări simple aduc la egalitatea:

$$(ca - b) + (a + bc)\alpha + (1 + c^2)\beta = 0.$$

Însă elementele $(1, \alpha, \beta)$ sunt liniar independente, deci $ca - b = 0$, $a + bc = 0$ şi $1 + c^2 = 0$. Ultima relație în $\mathbb{R}$ este imposibilă, prin urmare presupunerea de mai sus implică o contradicție, ceea ce demonstrează lema. □

Pentru a cerceta cazul $n = 4$ avem nevoie de următorul rezultat auxiliar.

Lema 16.5. *Fie A o $\mathbb{R}$-algebră asociativă cu diviziune, de rangul $n \geq 4$, cu elementele $\{1, \alpha, \beta\}$, care sunt liniar independente peste $\mathbb{R}$ şi $\alpha^2 = \beta^2 = -1$ (vezi Propoziția 16.3, p.1)). Atunci $\alpha\beta + \beta\alpha \in \mathbb{R}$.*

Demonstrație. Posibilitatea alegerii elementelor $\{1,\alpha,\beta\}$ cu proprietățile indicate este asigurată de Propoziția 16.3, p.1) şi faptul că $n \geq 4$. Întrucât elementele $\{1,\alpha,\beta\}$ sunt liniar independente, obținem că $\alpha+\beta \notin \mathbb{R}$ şi $\alpha-\beta \notin \mathbb{R}$. Prin urmare, fiecare dintre aceste numere este rădăcină a unui polinom de gradul 2, ireductibil peste $\mathbb{R}$ (Propoziția 15.3, p.1)). Astfel, există numerele p,q, $p',q' \in \mathbb{R}$ încât:

$$\begin{cases} (\alpha+\beta)^2 = p(\alpha+\beta)+q, \\ (\alpha-\beta)^2 = p'(\alpha-\beta)+q'. \end{cases} \qquad (3)$$

Pe de altă parte, avem:

$$(\alpha+\beta)^2 = \alpha^2+\beta\alpha+\alpha\beta+\beta^2 = -2+\beta\alpha+\alpha\beta,$$

$$(\alpha-\beta)^2 = \alpha^2-\beta\alpha-\alpha\beta+\beta^2 = -2-\beta\alpha-\alpha\beta.$$

Astfel, adunând termen cu termen egalitățile (3), obținem:

$$-4 = (p+p')\alpha+(p-p')\beta+q+q'.$$

Din nou utilizăm independența liniară a elementelor $\{1,\alpha,\beta\}$ şi din ultima relație avem:

$$p+p'=0, \quad p-p'=0, \quad q+q'+4=0.$$

Din primele două egalități deducem că $p=0$ şi $p'=0$. Revenim la sistemul de ecuații (3) şi, scăzând din prima ecuație a doua, obținem:

$$q-q' = (\alpha+\beta)^2-(\alpha-\beta)^2 = (-2+\beta\alpha+\alpha\beta)-$$
$$-(-2-\beta\alpha-\alpha\beta) = 2(\beta\alpha+\alpha\beta).$$

Prin urmare,

$$\alpha\beta+\beta\alpha = \frac{q-q'}{2} \in \mathbb{R}. \quad \square$$

Teorema 16.6. *Orice algebră asociativă cu diviziune, de rangul 4, peste câmpul* $\mathbb{R}$ *este izomorfă cu algebra cuaternionilor* ${}_{\mathbb{R}}\mathbb{H}$.

Demonstrație. Fie A o $\mathbb{R}$-algebră asociativă cu diviziune, de rangul 4. Este suficient de arătat că A posedă o bază ce constă din 4 elemente $\{1, i, j, k\}$ astfel încât $i^2 = j^2 = -1$ şi $ij = -ji = k$ (atunci uşor se verifică faptul că $k^2 = -1$ şi au loc celelalte relații din tabla înmulțirii elementelor din $\mathbb{H}$ (§14)). În aceste condiții este clar că ${}_{\mathbb{R}}A \cong {}_{\mathbb{R}}\mathbb{H}$.

Argumentele din demonstrația Propoziției 16.3 arată că în A există elementele $\{1, \alpha, \beta\}$, liniar independente peste $\mathbb{R}$ încât $\alpha^2 = \beta^2 = -1$. Pentru a găsi baza $\{1, i, j, k\}$ notăm:

$$i = \alpha, \quad j = x\alpha + y\beta,$$

unde $x, y \in \mathbb{R}$. Vom alege numerele reale x şi y, astfel încât să fie satisfăcute condițiile:

1) elementele $1, i, j$ sunt liniar independente peste $\mathbb{R}$;
2) $ij + ji = 0$;
3) $i^2 = j^2 = -1$.

Condiția 1) este satisfăcută pentru orice număr real $y \neq 0$. Într-adevăr, dacă elementele $1, i = \alpha, x\alpha + y\beta$ ar fi liniar dependente, atunci am avea

$$a + bi + c(x\alpha + y\beta) = 0,$$

($a, b, c \in \mathbb{R}$, nu toate fiind egale cu zero). Atunci $c \neq 0$ şi din $y \neq 0$ rezultă că β se poate exprima liniar prin 1 şi α. Însă $\{1, \alpha, \beta\}$ sunt liniar independente, contradicție.

Acum aplicăm Lema 16.5, din care rezultă că $\alpha\beta + \beta\alpha \in \mathbb{R}$. Notăm:

$$a = \frac{\alpha\beta + \beta\alpha}{2} \in \mathbb{R}.$$

Atunci avem:

$$ij + ji = \alpha(x\alpha + y\beta) + (x\alpha + y\beta)\alpha =$$
$$= 2x\alpha^2 + y(\alpha\beta + \beta\alpha) =$$
$$= -2x + 2ay = 2(ay - x).$$

Prin urmare, condiția 2) $(ij + ji = 0)$ este satisfăcută dacă $x = ay$. Rămâne să asigurăm respectarea condiției 3) $(i^2 = j^2 = -1)$ prin alegerea potrivită a numărului $y \in \mathbb{R}, y \neq 0$. Considerăm elementul $a\alpha + \beta$ pentru care:

$$\left(a\alpha + \beta\right)^2 = a^2\alpha^2 + a\left(\alpha\beta + \beta\alpha\right) + \beta^2 =$$
$$= -a^2 + 2a^2 - 1 = a^2 - 1 \in \mathbb{R}.$$

Deoarece sistemul $\{1, \alpha, \beta\}$ este liniar independent peste $\mathbb{R}$, avem $a\alpha + \beta \notin \mathbb{R}$, de aceea $a^2 - 1 < 0$ (în caz contrar avem: $a^2 - 1 \geq 0 \Rightarrow \left(a\alpha + \beta\right)^2 \geq 0 \Rightarrow$ există $\sqrt{\left(a\alpha + \beta\right)^2} \Rightarrow a\alpha + \beta \in \mathbb{R}$, contradicție). Prin urmare,

$$\frac{-1}{a^2 - 1} > 0,$$

şi în $\mathbb{R}$ există un astfel de număr y încât

$$y^2 = \frac{-1}{a^2 - 1},$$

adică $y^2(a^2 - 1) = -1.$ Această alegere a numărului y este motivată de faptul că:

$$j^2 = (x\alpha + y\beta)^2 = ((ay)\alpha + y\beta)^2 = a^2y^2\alpha^2 + y^2\beta^2 + ay^2\alpha\beta + ay^2\beta\alpha =$$
$$= -a^2y^2 - y^2 + ay^2(\alpha\beta + \beta\alpha) = -a^2y^2 - y^2 + 2a^2y^2 =$$
$$= a^2y^2 - y^2 = y^2(a^2 - 1) = -1.$$

Aşadar, alegând numerele $x, y \in \mathbb{R}$ astfel încât

$$x = ay, y^2 = \frac{-1}{a^2 - 1},$$

condițiile 1), 2) şi 3) vor fi satisfăcute şi din ele rezultă că sistemul liniar independent

$$\{1, i, j, k = ij\}$$

(vezi Lema 15.4) formează o bază a algebrei A. Mai mult, elementele acestei baze se înmulțesc ca şi elementele bazei algebrei cuaternionilor ${}_{\mathbb{R}}\mathbb{H}$. Din unicitatea sistemului de cuaternioni rezultă că ${}_{\mathbb{R}}A \cong {}_{\mathbb{R}}\mathbb{H}$. □

Pentru a finisa cercetarea noastră rămâne de efectuat ultimul pas: de analizat cazul când rangul $\mathbb{R}$-algebrei este mai mare decât 4 ($n \geq 5$).

Teorema 15.7. *Peste câmpul numerelor reale* $\mathbb{R}$ *nu există algebre asociative cu diviziune de rangul* $n \geq 5$.

Demonstrație. Reducere la absurd: fie că există o $\mathbb{R}$-algebră A cu diviziune, de rangul $n \geq 5$. Procedând la fel ca în demonstrația Teoremei 16.6, găsim elementele $1, i, j, k \in A$ astfel încât:

1) sistemul $\{1, i, j, k\}$ este liniar independent peste $\mathbb{R}$;
2) $i^2 = j^2 = -1,\ ij = -ji = k.$

Deoarece rangul n al algebrei A este mai mare decât 4, în A există un element $l \in A$ încât sistemul $\{1, i, j, k, l\}$ este liniar independent peste $\mathbb{R}$. Mai mult, din Propoziția 16.3, p.1) se vede că putem considera $l^2 = -1$. Acum aplicăm Lema 16.5 pentru fiecare dintre tripletele $\{1, i, l\}$, $\{1, j, l\}$ şi $\{1, k, l\}$, obținând că există elementele $a, b, c \in \mathbb{R}$ încât:

$$il + li = a, \tag{4}$$

$$jl + lj = b, \tag{5}$$
$$kl + lk = c. \tag{6}$$

Aplicând succesiv aceste relații, avem:

$$lk = (li)j = (a - il)j = aj - i(lj) = aj - i(b - jl) =$$
$$= aj - bi + ijl = aj - bi + kl = aj - bi + c - lk,$$

de unde

$$2lk = aj - bi + c. \tag{7}$$

Înmulțind egalitatea (7) din dreapta la k, obținem:

$$2lk^2 = ajk - bik + ck,$$

adică

$$-2l = ai + bj + ck.$$

Aceasta contrazice faptul că sistemul $\{1, i, j, k, l\}$ este liniar independent. Prin urmare, presupunerea că există o $\mathbb{R}$-algebră A de rangul $n \geq 5$ este greşită. □

Totalizând cele demonstrate mai sus, acum putem formula rezultatul final al acestui studiu, care descrie toate $\mathbb{R}$-algebrele acociative cu diviziune, de rang finit. Acest rezultat poartă numele unuia dintre creatorii algebrei numerelor hipercomplexe – matematicianul german F.G.Frobenius (1849-1917).

Teorema 15.8 ***(teorema lui Frobenius)****. Peste câmpul numerelor reale $\mathbb{R}$ orice algebră asociativă A cu diviziune, de rang finit, are rangul 1, 2 sau 4. Mai exact:*

1) dacă $n = 1$, atunci ${}_{\mathbb{R}}A \cong {}_{\mathbb{R}}\mathbb{R}$;

2) dacă $n = 2$, atunci ${}_{\mathbb{R}}A \cong {}_{\mathbb{R}}\mathbb{C}$;

3) dacă $n = 4$, atunci ${}_{\mathbb{R}}A \cong {}_{\mathbb{R}}\mathbb{H}$;

4) dacă $n = 3$ sau $n \geq 5$, atunci $\mathbb{R}$-algebre asociative cu diviziune, de rangul n, nu există.

Demonstraţie. Cazul $n=1$ este trivial (vezi exemplul 1). Cazul $n=2$ este demonstrat în Propoziţia 15.3(2). Cazul $n=4$ este arătat în teorema 15.6. Afirmaţia 4) rezultă din Lema 15.4 şi Teorema 15.7. □

Încheiem expunerea cu câteva *observaţii finale*. Pe parcursul acestui ciclu de lecţii au fost cercetate următoarele sisteme numerice:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H},$$

adică numerele naturale, întregi, raţionale, reale, complexe şi cuaternionii. Cu excepţia sistemului $\mathbb{N}$, fiecare din ele este o extindere a sistemului precedent, obţinând astfel noi proprietăţi în concordanţă cu cerinţele formulate (existenţa operaţiilor scăderii, împărţirii, trecerii la limită, extragerea rădăcinii din numere negative).

Pentru fundamentarea acestei teorii a sistemelor numerice am aplicat metoda axiomatică, verificând de fiecare dată compatibilitatea şi completitudinea sistemului de axiome (adică *existenţa* şi *unicitatea* sistemelor numerice respective). Demonstraţia acestor rezultate se bazează pe proprietăţile similare ale sistemului precedent (cu excepţia lui $\mathbb{N}$, unde existenţa se bazează pe axioma infinitului).

Extinderea sistemelor numerice conduce la „perfecţionarea" lor, însă putem observa că pe parcurs am avut şi unele „pierderi", de exemplu, la trecerea $\mathbb{R} \to \mathbb{C}$ am renunţat la relaţia de ordine totală, existentă în toate sistemele precedente. La fel, la trecerea $\mathbb{C} \to \mathbb{H}$ am „sacrificat" proprietatea de comutativitate a înmulţirii (pe când toate sistemele precedente sunt comutative).

Procedura de extindere a sistemelor numerice a fost finalizată cu teorema lui Frobenius, sensul căreia constă în aceea că extinderea de mai departe în modul practicat nu este posibilă, deoarece algebre de tipul cercetat peste $\mathbb{R}$ nu există pentru rangul $n \geq 5$. In realitate, mai este posibilă o cedare, renunţând şi la ultimul bastion - condiţia asociativităţii.

Insă, considerând algebre neasociative, noi nu obţinem prea mult: pe lângă algebrele din teorema lui Frobenius mai există doar o

singură $\mathbb{R}$-algebră cu diviziune, de rang finit, neasociativă (şi necomutativă), care are rangul 8 şi se numeşte *algebra Cayley-Dixon* (sau *algebra octavelor*). Aceasta este aşa numita *teoremă generalizată a lui Frobenius*. Cei interesaţi pot găsi aceste rezultate, de exemplu, în [19].

O continuare firească a materialului acestui ciclu de lecţii îl constituie *teoria algebrelor* (inele, câmpuri, module, algebre etc.) care generalizează sistemele numerice. Tot materialul expus mai sus formează doar un preludiu în simfonia măreaţă a algebrei moderne. Trebuie menţionat faptul că cercetările mai recente nu anulează valoarea sau importanţa sistemelor numerice care formează fundamentul trainic al întregii matematici. Aceste sisteme numerice servesc drept model şi sursă de exemple, drept bază pentru diverse generalizări. Cunoaşterea sistemelor numerice şi a metodei axiomatice este absolut obligatorie pentru orice matematician, ca element necesar al culturii matematice generale.

Anexa I

Câteva axiome ale teoriei mulțimilor

Expunerea materiei cursului dat începe prin admiterea existenței unei mulțimi infinite. Pentru rigurozitate ar fi nevoie de utilizat teoria axiomatică a mulțimilor. Spre regret, expunerea detaliată a axiomelor teoriei mulțimilor ne-ar fi îndepărtat de subiectul acestei lucrări. Cu toate că din punct de vedere logic o astfel de discuție ar trebui să anticipeze expunerea materialului, studiul teoriei axiomatice a mulțimilor este, în general, lăsat în seama cititorului. În bibliografie sunt incluse mai multe cursuri introductive la teoria axiomatică a mulțimilor. Totuşi, în anexa de față vom expune în linii generale un sistem de axiome care este suficient pentru necesitățile materialului inclus în cursul dat.

G.Cantor este autorul aşa-numitei „teorii naive" a mulțimilor, apărută în anii 70-80 ai secolului XIX. După G.Cantor mulțimea este o colecție de obiecte bine determinate, distincte ale intuiției sau gândirii noastre, considerate ca un tot. Pentru dezvoltarea teoriei „naive" a mulțimilor şi aplicațiile ei putea fi utilizată o astfel de definiție, deoarece în matematică sunt esențiale relațiile între obiectele mulțimii (sau între diferite mulțimi) şi nu natura obiectelor. Ulterior, prin însăşi dezvoltarea ei, teoria mulțimilor creată de G.Cantor a demonstrat însă insuficiența definiției „naive" a mulțimii, manifestată prin apariția unor paradoxuri (antinomii) inevitabile.

Dat fiind sensul noțiunii de mulțime după Cantor, s-ar putea crede că putem forma inclusiv mulțimi de tipul $C = \{X \mid X \ e \ mulțime \ infinită\}$ sau $C = \{X \mid X \ e \ mulțime\}$. În aceste cazuri avem $C \in C$. S-a observat că dacă nu impunem nişte restricții, atunci libertatea de a forma mulțimi poate conduce la paradoxuri. Unul din ele este cunoscut astăzi ca paradoxul lui Russell şi constă în următoarele.

Fie $C = \{X \mid X \ e \ mulțime \ şi \ X \notin X\}$. Conform definiției relației de apartenență, poate fi adevărată doar una din condițiile: $C \in C$ sau $C \notin C$. Observăm însă că dacă $C \in C$ atunci, conform

definiției lui C, trebuie să aibă loc $C \notin C$, deci obținem o contradicție. Dacă însă $C \notin C$ atunci, la fel din definiția lui C, rezultă că $C \in C$ şi obținem din nou contradicție. Aceste contradicții pot fi înlăturate recunoscând că obiectul C nu există sau că el nu este o mulțime.

Unele paradoxuri ale teoriei mulțimilor nu reprezintă decât variante ale dificultăților logice evidențiate încă din antichitate de şcoala filozofică a sofiştilor (sec.V î.e.n.). Un astfel de exemplu prezintă aşa-numita antinomie a mincinosului, cunoscută de la Epimenide din Creta, sec. VI î.e.n., care constă în următoarele: când mincinosul spune „mint" afirmația sa nu poate fi nici adevărată, nici falsă (se admite prin definiție că mincinosul spune întotdeauna numai neadevăruri). Într-adevăr, dacă afirmația sa ar fi adevărată ar însemna că mincinosul spune adevărul, ceea ce ar contrazice definiția mincinosului. Dacă însă afirmația „mint" ar fi falsă atunci contrariul ei ar fi adevărat, adică mincinosul spune iar adevărul, ceea ce este imposibil.

Contradicțiile care apar arată că intuiția noastră nu este un ghid foarte sigur în caz infinit. Adaptarea intuiției omului la cazul infinit poate fi făcută prin stabilirea unor condiții stricte în care operațiile, acțiunile, construcțiile matematice respective ar rămâne valabile. Pentru înlăturarea paradoxurilor teoriei „naive" a mulțimilor s-a recurs la organizarea noii teorii pe baza unui sistem de axiome. Primul sistem de axiome a teoriei mulțimilor a fost propus în 1908 de Ernest Zermelo (1871-1953). Axiomele lui Zermelo au fost preluate mai târziu (1921-1922) de A.Fraenkel şi de A.Schoenfliess care au contribuit esențial la axiomatizarea inițială a teoriei mulțimilor. Ulterior au fost elaborate sau perfecționate şi alte sisteme de axiome prin aportul mai multor matematicieni şi logicieni cunoscuți, printre care B.Russell, D.Hilbert, A.Tarski, J.Lukasiewicz, J.v.Neumann, C.Kuratowski, P.Finsler, K.Gödel, H.Herbrand, C.S.Kleene, P.Bernays, A.Mostowski, F.Gonseth, A.Church ş.a.

Scopul teoriei axiomatice a mulțimilor este de a indica un sistem de axiome care ar permite obținerea afirmațiilor referitoare la

mulțimi, ce nu ar conduce la paradoxuri. Aceste afirmații trebuie să fie suficient de profunde pentru a putea permite fundamentarea tuturor noțiunilor şi construcțiilor matematice.

În continuare vom utiliza noțiunile de *clasă* şi de *mulțime*. Noțiunea de clasă va coincide cu cea de mulțime în sensul „naiv" al lui G.Cantor, dată mai sus. Obiectele din care este formată o clasă le vom numi elementele ei. Termenul *mulțime* va desemna o clasă ce aparține ca element unei clase prealabil definite. Mai spunem în acest caz că clasa dată este *insertibilă*. În caz contrar clasa se numeşte *neinsertibilă*. De exemplu, clasa C a mulțimilor care nu se au pe ele însele ca element, nu poate fi o mulțime după cum am văzut mai sus.

Pentru prezentarea unui sistem de axiome s-ar părea că avem nevoie de obiecte de două tipuri: elemente şi mulțimi, unde obiectele numite mulțimi se construiesc în careva mod din elemente, de exemplu, ca mulțimi de elemente, mulțimi de mulțimi de elemente ş.a.m.d. Însă, după cum vom vedea, având noțiunea de mulțime vidă şi principiile de bază ale existenței mulțimilor, vom putea demonstra existența unei mulțimi P, a unui element notat cu 1 şi a unei operații notate cu Sc pe mulțimea P astfel încât $(P, Sc, 1)$ să fie un sistem Peano. De aceea admiterea existenței unor „elemente", deosebite de mulțimi, poate fi evitată. Astfel vom considera că toate obiectele de bază sunt mulțimi. Vom admite de asemenea că domeniul de definiție al variabilelor pe care le considerăm: x, y, z, A, B, C, M, S ş.a.m.d. este clasa tuturor mulțimilor.

Noțiuni de bază ale teoriei date vor fi două relații între mulțimi: relația de egalitate „=" şi relația de apartenență „$\in$". După cum suntem obişnuiți, relația de inegalitate se va nota cu „$\neq$", iar relația de neapartenență cu „$\notin$". Axiomele principale referitoare la relațiile „=" şi „$\in$" sunt următoarele:

Axioma 1. *Pentru orice* x *are loc* $x = x$.

Axioma 2. *Pentru orice* x *şi* y, *dacă* $x = y$, *atunci* $y = x$.

Axioma 3. *Pentru orice* x, y *şi* z *dacă* $x = y$ *şi* $y = z$, *atunci* $x = z$.

Axioma 4. *Pentru orice* X *şi* Y, *dacă* $X = Y$ *atunci pentru orice* Z, $X \in Z$ *dacă şi numai dacă* $Y \in Z$ *şi pentru orice* W, $W \in X$ *dacă şi numai dacă* $W \in Y$.

Primele patru axiome exprimă aspecte logice ale relației de egalitate şi aceste afirmații sunt considerate adevărate în orice context matematic (pentru relația de egalitate).

Axioma 5. (*Axioma extensiei*) *Pentru orice* A *şi* B, *dacă pentru fiecare* x *relația* $x \in A$ *este echivalentă cu* $x \in B$, *atunci* $A = B$.

Axioma 5 se numeşte *axioma extensiei* şi arată că orice mulțime este complet definită de elementele sale. În conformitate cu această axiomă definiția mulțimii poartă un caracter extensiv, adică a defini o mulțime înseamnă a descrie sau a enumera elementele ce aparțin mulțimii. De exemplu, o mulțime finită poate fi dată prin simpla enumerare a elementelor ei. O mulțime infinită C poate fi cuprinsă într-o descriere sau poate fi dată cu ajutorul unei proprietăți caracteristice $P(x)$, punând $C = \{x \mid P(x)\}$, unde $P(x)$ este o propoziție (funcție propozițională) ce exprimă o condiție satisfăcută de variabila x dacă şi numai dacă $x \in C$.

Vom formula acum câteva axiome referitoare la *existența* mulțimilor.

Axioma 6. *Există o mulțime* A *astfel încât* $x \notin A$ *pentru fiecare* x.

Axioma 6 garantează existența cel puțin a unei mulțimi. Conform axiomei extensiei, orice două mulțimi ce posedă proprietatea din axioma 6 coincid. Astfel putem introduce următorul obiect: $\varnothing$ este unica mulțime A astfel încât $x \notin A$ pentru fiecare x. Ea se numeşte *mulțimea vidă*.

Observăm că expresia „există un singur x astfel încât $A(x)$" va însemna că condiția $A(x)$ satisface următoarele cerințe:

(i) există x astfel încât $A(x)$;

(ii) pentru orice x şi y dacă $A(x)$ şi $A(y)$, atunci $x = y$.

Următoarea axiomă face posibilă construirea unor perechi neordonate.

Axioma 7. *Pentru orice a şi b, există A astfel încât pentru fiecare x, $x \in A$ dacă şi numai dacă $x = a$ sau $x = b$.*

Conform axiomei extensiei mulțimea A ce verifică condițiile axiomei 7 este unică. Pentru orice a şi b cu simbolul $\{a,b\}$ vom nota unica mulțime A ce verifică condițiile axiomei 7 şi o vom numi *pereche neordonată*. Punem prin definiție $\{a\} = \{a,a\}$, pentru orice a.

Pereche ordonată vom numi mulțimea $\{\{a\},\{a,b\}\}$, pentru orice a şi b, pe care o vom nota cu (a,b).

Axioma 8. *Pentru orice A, există S astfel încât pentru orice x, $x \in S$ dacă şi numai dacă pentru un $X \in A$ are loc $x \in X$.*

Axioma 8 defineşte operația de reuniune a mulțimilor. Axioma extensiei garantează unicitatea mulțimii S. Pentru orice A notăm cu $\bigcup_{X \in A} X$ unica mulțime S ce verifică condițiile axiomei 8. În particular, punem

$$A \cup B = \bigcup_{X \in \{A,B\}} X .$$

Axioma 8 permite construirea mulțimilor:

$$\{a,b,c\} = \{a,b\} \cup \{c\}, \quad \{a,b,c,d\} = \{a,b,c\} \cup \{d\} \quad \text{ş.a.m.d.}$$

După cum vom vedea în cele ce urmează, nu este necesar de cerut axiomatic existența intersecției mulțimilor, aceasta rezultând din alte axiome. Pentru orice A şi B, notăm $A \subseteq B$ dacă pentru

orice x, din $x \in A$ rezultă $x \in B$. Dacă $A \subseteq B$ atunci mulţimea A se numeşte *submulţime* a mulţimii B.

Axioma 9. *Pentru orice A există S astfel încât pentru fiecare X, $X \in S$ dacă şi numai dacă $X \subseteq A$.*

Axioma 9 garantează existenţa mulţimii tuturor submulţimilor lui A, numită *booleanul* mulţimii A. Pentru orice A notăm cu $\mathcal{P}(A)$ unica mulţime S ce verifică condiţiile axiomei 9 (adică booleanul mulţimii A).

În următoarea axiomă $\mathcal{A}(x)$ este o proprietate arbitrară care poate fi formulată integral în termenii „=” şi „$\in$”, utilizând doar legăturile logice: negaţie, conjuncţie, disjuncţie, implicaţie, cuantificatorii universal şi existenţial şi unde toate variabilele se referă la mulţimi, însă care nu conţine mulţimea A în calitate de variabilă liberă, deşi poate conţine alte variabile libere.

Axioma 10. *Pentru orice mulţime S există o mulţime A astfel încât pentru orice x, $x \in A$ dacă şi numai dacă $x \in S$ şi $\mathcal{A}(x)$.*

Pentru orice mulţime S vom nota cu $\{x \mid x \in S \text{ şi } \mathcal{A}(x)\}$ unica mulţime A ce verifică condiţiile axiomei 10. Axioma extensiei garantează unicitatea mulţimii A.

Cu ajutorul axiomelor definite mai sus poate fi demonstrată existenţa intersecţiei, diferenţei şi produsului cartezian al mulţimilor.

Fie $M \neq \varnothing$ şi $S \in M$. Notăm cu $\bigcap_{X \in M} X$ mulţimea

$$\{x \mid x \in S \text{ şi } x \in X \text{ pentru orice } X \in M\}$$

şi o numim *intersecţia* mulţimilor din M. Dacă $M = \varnothing$ atunci punem prin definiţie $\bigcap_{X \in M} X = \varnothing$. Observăm că $\bigcap_{X \in M} X$ nu depinde de alegerea lui $S \in M$ dacă $M \neq \varnothing$, însă pentru a putea aplica axioma

10 în definiția intersecției mulțimilor este necesară prezența unei astfel de mulțimi S. În particular, punem prin definiție

$$A \cap B = \bigcap_{X \in \{A,B\}} X$$

şi numim intersecția mulțimilor A şi B. Din definiția intersecției rezultă că dacă $M \neq \varnothing$, atunci

$$\bigcap_{X \in M} X \subseteq S$$

pentru orice $S \in M$.

Pentru orice două mulțimi S şi A definim mulțimea

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

şi o numim *diferența* mulțimilor S şi A.

Pentru a demonstra existența *produsului cartezian* al mulțimilor A şi B, notat cu $A \times B$, utilizăm definiția perechii ordonate. Astfel, pentru orice $a \in A$ şi $b \in B$ avem $\{a\} \in \mathcal{P}(A \cup B)$ şi $\{a,b\} \in \mathcal{P}(A \cup B)$, de unde rezultă $\{\{a\},\{a,b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$, deci putem defini produsul cartezian $A \times B$ al mulțimilor A şi B în felul următor:

$$A \times B = \{x \mid x \in \mathcal{P}(\mathcal{P}(A \cup B)) \text{ şi există } a \in A \text{ şi } b \in B \text{ astfel încât } x = (a,b)\}.$$

În definiția produsului cartezian sunt utilizate axiomele 7-9 şi axioma 10 pentru $S = \mathcal{P}(\mathcal{P}(A \cup B))$.

Dacă am stabili existența cel puțin a unei mulțimi S, atunci din Axioma 10 ar rezulta existența mulțimii vide (adică axioma 6), aceasta fiind $\{x \mid x \in S \text{ si } x \neq x\}$. Observăm că dacă din formularea axiomei 10 am elimina restricția referitoare la mulțimea S, atunci din această axiomă ar rezulta axiomele 7-9. Însă paradoxul lui Russell arată că axioma 10, formulată fără S, conduce la apariția unor contradicții şi deci în acest caz din ea ar putea fi dedusă orice

afirmație. Pe de altă parte, nu există până astăzi o demonstrație a faptului că axioma 10 nu implică axiomele 7-9.

De asemenea, reieşind din axiomele expuse mai sus, nu se poate demonstra existența mulțimilor infinite, deşi putem formula un şir de afirmații care garantează existența unei clase infinite de mulțimi distincte două câte două. De exemplu, afirmația că oricare două dintre mulțimile $\varnothing$, $\{\varnothing\}$, $\{\{\varnothing\}\}$, $\{\{\{\varnothing\}\}\}$, ... sunt distincte între ele. Într-adevăr, observăm la început că $\{x\} \neq \varnothing$ pentru orice x, deoarece $x \in \{x\}$. Observăm de asemenea că din egalitatea $\{x\} = \{y\}$ rezultă $x = y$ deoarece $x \in \{x\}$ şi atunci, conform axiomei 4, obținem că $\{x\} = \{y\}$ implică $x \in \{y\}$, de unde rezultă $x = y$. Astfel obținem $\{\{\varnothing\}\} \neq \{\varnothing\}$ deoarece în caz contrar am avea $\{\varnothing\} = \varnothing$. Analog se demonstrează că $\{\{\{\varnothing\}\}\} \neq \{\varnothing\}$, $\{\{\{\varnothing\}\}\} \neq \{\{\varnothing\}\}$ ş.a.m.d. Existența unei mulțimi care ar conține în calitate de elemente toate mulțimile $\varnothing$, $\{\varnothing\}$, $\{\{\varnothing\}\}$, $\{\{\{\varnothing\}\}\}$, ... nu poate fi dedusă din axiomele 1-10 şi o vom cere printr-o axiomă nouă, numită *Axioma infinitului*.

Axioma 11. (***Axioma infinitului***) *Există o mulțime* S *astfel încât* $\varnothing \in S$ *şi pentru orice* x, $x \in S$ *implică* $\{x\} \in S$.

Fie S o mulțime ce verifică condițiile axiomei 11 şi fie

$$M = \{X \mid X \in \mathcal{P}(S),\ \varnothing \in X \ \text{şi pentru orice}\ x,\ x \in X \ \text{implică}\ \{x\} \in X\}.$$

Considerăm mulțimea $P = \bigcap_{X \in M} X$ şi observăm că P poate fi percepută ca cea mai mică (în raport cu incluziunea) mulțime ce verifică condițiile axiomei 11.

Teoremă. *Punând prin definiție* $Sc(x) = \{x\}$, *pentru fiecare* $x \in P$, *avem:*

(i) $\varnothing \in P$ *;*
(ii) dacă $x \in P$ *, atunci* $Sc(x) \in P$ *;*
(iii) $Sc(x) \neq \varnothing$ *pentru orice* $x \in P$ *;*
(iv) pentru orice $x, y \in P$ *din* $Sc(x) = Sc(y)$ *rezultă* $x = y$ *;*
(v) dacă X *este o submulţime a lui* P *astfel încât* $\varnothing \in X$ *şi pentru orice* $x, x \in X$ *implică* $Sc(x) \in X$ *, atunci* $X = P$ *.*

Din teorema de mai sus rezultă că mulţimea P (şi atunci şi mulţimea S) este infinită, iar $(P, Sc, \varnothing)$ este un *sistem Peano*. Reciproc, dacă există o mulţime infinită, atunci conform Propoziţiei 1.3, există un sistem Peano $(\mathbb{N}, 0, s)$, deci există o mulţime $\mathbb{N}$ ce verifică condiţiile axiomei 11. Astfel, axioma 11 este echivalentă cu existenţa unei mulţimi infinite.

Un alt mod de introducere a sistemului Peano, utilizat în teoria mulţimilor, constă în următoarele: în loc de $Sc(x) = \{x\}$ se ia $Sc(x) = x \bigcup \{x\}$ şi se admite existenţa unei mulţimi ce conţine $\varnothing$ şi care, împreună cu orice element al său x, conţine şi $Sc(x)$. Mulţimea minimală de acest fel este formată din elementele $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$, $\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$, ş.a.m.d., deci notând aceste mulţimi cu 0,1,2,3, …, respectiv, obţinem 0, 1={0}, 2={0,1}, 3={0,1,2} ş.a.m.d.

Un alt principiu de bază în teoria mulţimilor îl reprezintă *Axioma alegerii* pe care o formulăm în continuare.

Axioma 12. (***Axioma alegerii***) *Fie* M *o mulţime astfel încât pentru orice* $X \in M$ *are loc* $X \neq \varnothing$ *şi pentru orice* $X, Y \in M$ *, din* $X \neq Y$ *rezultă* $X \bigcap Y = \{\varnothing\}$ *. Atunci există o mulţime* A *astfel încât pentru fiecare* $X \in M$ *există* y *ce verifică condiţia* $A \bigcap X = \{y\}$ *.*

Axioma alegerii poate fi reformulată în felul următor: pentru orice mulţime M, formată din mulţimi nevide, disjuncte două câte

două, există o mulțime A ce conține exact câte un element comun cu fiecare mulțime din M.

Afirmații mai simple, echivalente cu axioma alegerii, pot fi formulate cu ajutorul noțiunii de funcție. Amintim că o funcție, conform definiției, este o mulțime F de perechi ordonate (x, y) astfel încât pentru orice x din domeniul de definiție al funcției, există un singur y ce satisface condiția $(x, y) \in F$. Acest unic y se notează cu $F(x)$.

Axioma 12'. *Fie M o mulțime astfel încât pentru orice $X \in M$ are loc $X \neq \emptyset$ şi pentru orice $X, Y \in M$, din $X \neq Y$ rezultă $X \cap Y = \{\emptyset\}$. Atunci există o funcție F cu domeniul de definiție $D(F) = M$ şi pentru orice $X \in M$ are loc $F(X) \in X$.*

Axioma 12". *Pentru orice mulțime M există o funcție G cu domeniul de definiție $D(G) = \{X \mid X \in M \text{ si } X \neq \emptyset\}$ şi pentru orice $X \in D(G)$ are loc $G(X) \in X$.*

Arătăm că axiomele 12, 12' şi 12" sunt echivalente în condițiile axiomelor 1-10.

Mai întâi arătăm că axioma 12 implică axioma 12'. Mulțimea M ce verifică condițiile axiomei 12' verifică şi condițiile axiomei 12. Prin urmare, există o mulțime A astfel încât pentru fiecare $X \in M$ există y ce verifică condiția $A \cap X = \{y\}$. Fie $F = \{(X, y) \mid X \in M \text{ şi } y \in A \cap X\}$. Existența mulțimii F rezultă din axioma 10, fiind o submulțime în $M \times A$. Este clar că F este funcția, existența căreia este dată de axioma 12'. Prin urmare, axioma 12 implică axioma 12'.

Presupunem acum adevărată axioma 12'. Considerăm mulțimea M ce verifică condițiile axiomei 12". Elementele mulțimii M nu sunt neapărat disjuncte două câte două şi nevide. Fie $M_1 = \{X \mid X \in M \text{ si } X \neq \emptyset\}$ şi $M_2 = \{X \times \{X\} \mid X \in M_1\}$. Mulțimea M_1 există în virtutea axiomei 10. Existența mulțimii M_2 rezultă din

faptul că $M_2 \subseteq M_1 \times P(M_1)$. Mulţimea M_2 verifică condiţiile axiomei 12', deci există o funcţie F cu domeniul de definiţie $D(F) = M_2$ şi pentru orice $X \in M_2$ are loc $F(X) \in X$. Prin urmare, pentru orice $X \in M$ şi $X \neq \varnothing$ rezultă $F(X \times \{X\}) = (y, X)$ pentru un $y \in X$. Fie

$$G = \{(X, y) \mid X \in M_1 \text{ şi } F(X \times \{X\}) = (y, X)\},$$

atunci G verifică condiţiile axiomei 12". În mod analog se demonstrează că axioma 12" implică axioma 12.

Observăm că în matematică este cunoscut un număr mare de afirmaţii echivalente cu axioma alegerii. În Anexa II, referitoare la structuri algebrice parţial ordonate, sunt formulate două afirmaţii bine cunoscute de acest fel: Teorema lui Zermelo şi Lema lui Zorn. Faptul că axioma alegerii era necesară la demonstrarea multor afirmaţii din analiza matematică a fost pentru prima dată menţionat de Zermelo. Axioma alegerii are un rol discutat în matematica contemporană. Spre deosebire de celelalte axiome de existenţă ale teoriei mulţimilor, axioma alegerii nu descrie explicit (cu ajutorul unor condiţii pe care trebuie să le verifice obiectele mulţimilor) mulţimea, existenţa căreia este afirmată. Astfel, axioma alegerii se bazează pe un alt tip de raţionament intuitiv decât celelalte axiome.

Rolul metodei axiomatice în matematică este de necontestat. O latură mai puţin „plăcută" a acestei metode constă însă în faptul că ea impune implicit restricţii serioase posibilităţilor de expansiune a teoriilor matematice în baza axiomelor de plecare. Astfel, teoria axiomatică a mulţimilor va cuprinde întotdeauna mai puţine rezultate decât teoria „naivă" a lui Cantor. Pe de altă parte, diferite sisteme de axiome, referitoare la aceeaşi teorie, conduc la crearea unor sisteme de cunoştinţe diferite, fapt ce menţine actuală problema confruntării rezultatelor teoriilor matematice cu experienţa.

Menţionăm că există sisteme de axiome ale teoriei mulţimilor mai riguroase decât cel expus mai sus. Aceste sisteme sunt utilizate în prezent drept fundament pentru toate elaborările matematice. Însă este firesc de evidenţiat un număr minimal de

axiome care ar fi suficiente pentru expunerea teoriei unui compartiment concret al matematicii. Cercetarea diferitor sisteme de axiome utilizează aparatul metamatematicii – compartimentul logicii matematice care studiază teoriile matematice formalizate. Astfel de cercetări ale fundamentelor matematicii constituie o parte a eforturilor continue de studiere a noţiunilor de bază ale matematicii, a metodelor matematicii şi a interconexiunilor dintre ele.

Anexa II

Structuri algebrice parțial ordonate

În această anexă vom expune fără demonstrații câteva afirmații ce țin de mulțimi parțial ordonate şi strudturi algebrice parțial ordonate.

Fie M o mulțime nevidă pe care este definită o relație binară „$\leq$”. Vom spune că M este *parțial ordonată* dacă această relație este reflexivă ($a \leq a, \forall a \in M$), antisimetrică ($a \leq b$ şi $b \leq a$ implică $a = b$) şi tranzitivă ($a \leq b$ şi $b \leq c$ implică $a \leq c$). Relația „$\leq$” se numeşte *ordine* (*parțială*) pe A. Ca de obicei, vom scrie $a < b$ dacă $a \leq b$ şi $a \neq b$; $b \geq a$ dacă $a \leq b$; $b > a$ dacă $a < b$.

Fie X o submulțime arbitrară a mulțimii M. Un element $a \in M$ se numeşte *majorant* (*minorant*) pentru X dacă $x \leq a$ $(x \geq a)$, pentru orice $x \in X$. Dacă X posedă un majorant (minorant), se spune că X este *mărginită superior* (*inferior*). Un element $a \in M$ se numeşte *margine superioară* (*inferioară*) pentru X dacă a este un majorant (minorant) şi din faptul că b este un majorant (minorant) pentru X, rezultă $a \leq b$ $(a \geq b)$. Dacă există marginea superioară (inferioară) pentru X, atunci ea este unică şi se notează cu $\sup X$ $(\inf X)$. Dacă pentru orice $x, y \in M$ există $\sup\{x, y\}$ şi $\inf\{x, y\}$, atunci M se numeşte *latice*. De regulă, notăm în acest caz $\sup\{x, y\} = x \vee y$ şi $\inf\{x, y\} = x \wedge y$. O latice se numeşte *completă* dacă orice familie de elemente din M are atât margine superioară cât şi margine inferioară.

Un element m al mulțimii ordonate M se numeşte *maximal* (*minimal*) dacă din $x \geq m$ $(x \leq m)$, unde $x \in M$, rezultă $x = m$. Un element $a \in M$ se numeşte *supremum* (*infimum*) dacă $a = \sup M$ $(a = \inf M)$. Mulțimea M se numeşte *bine ordonată* dacă orice submulțime nevidă a sa posedă infimum.

O mulțime ordonată M se numeşte *total* (sau *liniar*) *ordonată* dacă oricare ar fi elementele $a, b \in M$ avem $a < b$ sau $a = b$ sau $a > b$ (legea trihotomiei).

Teorema 1. *Următoarele afirmaţii sunt echivalente:*

(i) (Axioma alegerii) Pentru orice mulţime M există o funcţie φ care asociază oricărei submulţimi nevide X a lui M un element $\varphi(x)$ care aparţine lui X.

(ii) (Teorema lui Zermelo) Orice mulţime nevidă poate fi bine ordonată.

(iii) (Lema lui Zorn) Dacă M este o mulţime ordonată şi orice submulţime nevidă total ordonată a sa are margine superioară, atunci pentru orice element $a \in M$ există un element maximal $m \in M$ astfel încât $a \le m$.

Structură algebrică se numeşte orice mulţime nevidă, înzestrată cu una sau mai multe operaţii algebrice.

O structură algebrică $(G,*)$ se numeşte *grup* dacă sunt verificate condiţiile: 1) operaţia „$*$” este asociativă ($(a*b)*c = a*(b*c)$, $\forall a,b,c \in G$); 2) operaţia „$*$” posedă element neutru ($\exists e \in G: a*e = e*a = a$, $\forall a \in G$); 3) orice element din G este simetrizabil în raport cu „$*$” ($\forall a \in G, \exists a' \in G: a*a' = a'*a = e$).

Un grup $(G,*)$ se numeşte *comutativ* sau *abelian* dacă $a*b = b*a$, $\forall a,b \in G$.

Structura algebrică $(G,*)$ ce verifică 1) şi 2) se numeşte *monoid*.

O structură algebrică $(S,+,\cdot)$ se numeşte *semiinel* dacă $(S,+)$ este un monoid şi operaţia „$\cdot$” este distributivă în raport cu „$+$” ($a\cdot(b+c) = a\cdot b + a\cdot c$ şi $(b+c)\cdot a = b\cdot a + c\cdot a$, $\forall a,b,c \in S$).

Structura algebrică $(R,+,\cdot)$ se numeşte *inel* dacă $(R,+)$ este grup abelian şi operaţia „$\cdot$” este distributivă în raport cu „$+$”. Inelul $(R,+,\cdot)$ se numeşte *asociativ* (*comutativ*, *cu element unitate*) dacă operaţia „$\cdot$” este asociativă (respectiv, comutativă, posedă element neutru).

Un grup $(G,\cdot)$ se numeşte *ordonat* dacă $(G,\le)$ este mulţime ordonată şi se verifică una din următoarele condiţii echivalente:

(1) dacă $a \le b$, atunci $ac \le bc$ şi $ca \le cb$ pentru orice $c \in G$;

(2) dacă $a \le b$, atunci $cad \le cbd$ pentru orice $c,d \in G$;
(3) dacă $a < b$, atunci $cad < cbd$ pentru orice $c,d \in G$;
(4) dacă $a < b$ şi $c \le d$, atunci $ac < bd$ şi $ca < db$;
(5) dacă $a \le b$ şi $c < d$, atunci $ac < bd$ şi $ca < db$.

Notăm $P = \{a \mid a \in G, a > e\} \cup \{e\}$ şi numim această mulţime *con pozitiv* al grupului G. Relaţia de ordine „$\le$” se determină complet de conul pozitiv deoarece

$$a \le b \Leftrightarrow a^{-1}b \in P \text{ (sau } ba^{-1} \in P\text{).}$$

Teorema 2. *Submulţimea P a grupului G este con pozitiv pentru o ordine (parţială) „$\le$” dacă şi numai dacă:*

(i) $P \cap P^{-1} = \{e\}$;

(ii) $PP \subseteq P$;

(iii) $xPx^{-1} \subseteq P$ *pentru orice* $x \in G$.

Un grup ordonat G este total ordonat dacă şi numai dacă $P \cup P^{-1} = G$. Dacă G este un grup total ordonat, atunci *valoarea absolută* (*modulul*) elementului a se defineşte prin egalitatea $|a| = \max\{a, a^{-1}\}$.

Un grup ordonat $(G,\cdot)$ se numeşte *arhimedean* dacă pentru orice $a,b \in G$, $a > e$, $b > e$, există un număr natural $n \ge 1$ astfel încât $a^n > b$.

Inelul $(R,+,\cdot)$ se numeşte *inel ordonat* dacă $(R,+)$ este un grup ordonat şi relaţiile $a \le b$, $c > 0$ implică $ca \le cb$ şi $ac \le bc$.

Ca şi mai sus, notăm

$$P = \{a \mid a \in R, a > 0\} \cup \{0\}.$$

Elementele nenule (diferite de 0) din P se numesc *elemente pozitive*. Submulţimea P se numeşte *con pozitiv* al inelului $(R,+,\cdot)$.

Submulţimea P determină complet relaţia de ordine pe R prin echivalenţa:

$$a \le b \Leftrightarrow b - a \in P.$$

Teorema 3. *Submulțimea P a inelului R este con pozitiv pentru o relație de ordine dacă şi numai dacă sunt verificate următoarele trei condiții:*

(i) $P \cap -P = \{0\}$;

(ii) $P + P \subseteq P$;

(iii) $PP \subseteq P$.

Un inel R este total ordonat dacă şi numai dacă $P \cup -P = R$. Se demonstrează că produsul a două elemente negative este pozitiv; produsul a două elemente, dintre care unul este negativ iar celălalt pozitiv, este negativ; ş.a.m.d.

Bibliografie

1. Becheanu M., Dincă A., Ion I.D. şi a. (8 autori), Algebră pentru perfecţionarea profesorilor. EDP, Bucureşti, 1983.
2. Creangă I., Enescu I., Algebra. Ed.Tehnică, Bucureşti, 1973.
3. Dammit D. , Foote R. Abstract algebra. Second Edition. John Wiley and sons, Inc.,1999 (3 ed., Wiley, 2004).
4. Ebinghaus H,-D., Hermes H., Hirzenbruch F., etc. (8 authors), Numbers. Springer-Verlag, 1991.
5. Miron R., Brânzei D., Backgrounds of Arithmetic and Geometry. World Scientific, Singapore, New Jersey, London, Hong Kong, 1995.
6. Năstăsescu C., Introducere în teoria mulţimilor, EDP, Bucureşti, 1974.
7. Năstăsescu C., Niţă C., Vraciu C., Aritmetică şi algebră. EDP, Bucureşti, 1993.
8. Popescu N., Categorii abeliene. Ed. Acad. RSR, Bucureşti, 1971.
9. Popovici C.P., Aritmetica şi teoria numerelor. EDP, Bucureşti, 1970.
10. Purdea I., Tratat de algebră modernă.Vol.II. Ed. Acad. RSR, Bucureşti, 1982.
11. Rusu E., Aritmetica şi teoria numerelor. EDP, Bucureşti, 1963.
12. Александров П.С. Введение в теорию и общую топологию. Наука, М., 1977.
13. Андронов И.К., Математика действительных и комплексных чисел. Просвещение, М., 1975.
14. Андронов И.К., Окунев А.К., Арифметика рациональных чисел. Просвещение, М., 1971.
15. Гонин Е.Г., Теоретическая арифметика. Учпедгиз, М., 1959.
16. Демидов И.Т., Основания арифметики. Учпедгиз, М., 1963.
17. Дэвенпорт Г., Высшая арифметика. Наука, М.,1965.
18. Кантор И.Л., Солодовников А.С., Гиперкомплексные числа. Наука, М.,1973.
19. Куратовский К., Мостовский А., Теория множеств. Мир. М., 1969.
20. Курош А.Г. Лекции по общей алгебре. Наука, М.,1973.
21. Молин Ф.Э. Числовые системы. Новосибирск, Наука, 1985.
22. НечаевВ.И., Числовые системы. Просвещение, М., 1975.
23. Понтрягин Л.С., Обобщения чисел. Наука, М.,1986.
24. Проскуряков И.В., Числа и многочлены. Просвещение, М., 1965.
25. Столл Р.Р., Множества. Логика. Аксиоматические теории. Просвещение, М., 1968. (Robert R.Stoll, Sets, Logic, and Axiomatic Theories. W.H.Freeman and Comp. San Francisco-N.Y.)
26. Фаддеев Д.К. Лекции по алгебре. Наука, М.,1984.

27. Феферман С., Числовые системы. Основания алгебры и анализа. Наука, М.,1971. (Feferman S., The number theory. Foundations of algebra and analysis. Palo Alto – London, 1963)
28. Фукс Л., Частично упорядоченные алгебраические системы. Мир. М., 1965. (Fuchs L., Partially ordered algebraic systems. Oxford-London-N.Y.-Paris, 1963)

Indice