Cursul 2

Structuri algebrice de bază.
Mulţimi fundamentale de numere: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ şi $\overline{\mathbb{R}}$.
Operaţii cu ordinali şi cardinali.
Inegalităţi numerice importante.

Inevitabil, o prezentare riguroasă a mulţimilor numerice $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ şi $\mathbb{R}$ invocă expunerea prealabilă a unor noţiuni de bază (precum cele de operaţie algebrică, monoid, grup, inel, corp şi morfism) din cadrul teoriei structurilor algebrice, cu măcar enumerarea unor elemente de fundament. De aceea, pentru început, ne referim la asemenea elemente, după care, pe rând şi axiomatic, ne vom ocupa de mulţimile numerice vizate. Cum unele dintre acestea pot fi, prin înzestrarea cu operaţii algebrice specifice, structurate ca o latice sau o algebră Boole, vom introduce aici şi astfel de noţiuni.În final, menţionăm câteva inegalităţi numerice (Hölder, Cauchy, Minkowski, Carleman), în $\mathbb{R}$, cu vădită importanţă în contextul prezentelor note de curs.

Operaţii algebrice. Proprietăţi. Monoizi. Morfisme.

Fie M o mulţime nevidă.

Definiţia 2.1 *Numim **operaţie algebrică** (internă) sau **lege de compoziţie** (internă) **pe** M o funcţie $\varphi : M \times M \to M$. Pentru $x, y \in M$, elementul $\varphi(x, y) \in M$ se numeşte **compusul lui** x **cu** y **prin operaţia** φ.*

Pentru simplificarea scrierii, de regulă, $\varphi(x, y)$ se redă prin $x \circ y$, unde, după caz, "$\circ$" semnifică "$+$", când operaţia φ este aditivă, sau "$\cdot$", când φ este multiplicativă.

Definiţia 2.2 *O operaţie algebrică pe M (notată, generic, cu "$\circ$") se numeşte*

i) ***asociativă**, dacă $(x \circ y) \circ z = x \circ (y \circ z)$, $\forall\, x, y, z \in M$;*

ii) ***comutativă**, dacă $x \circ y = y \circ x$, $\forall\, x, y \in M$;*

iii) ***cu element neutru**, dacă există $e \in M$, astfel încât*

$$x \circ e = e \circ x = x, \forall\, x \in M.$$

În acest caz, e este unic şi constituie respectivul element neutru al operaţiei "$\circ$".

Definiţia 2.3 *Un dublet $(M, \circ)$, unde M este o mulţime nevidă, iar "$\circ$" este o operaţie algebrică pe M, se numeşte **semigrup** dacă operaţia "$\circ$" este asociativă. În plus, dacă operaţia "$\circ$" are şi element neutru, atunci $(M, \circ)$ se numeşte **monoid**. Dacă "$\circ$" este şi comutativă, **monoidul** $(M, \circ)$ se numeşte **comutativ**.*

Exemple:

1) Dacă $M \neq \varnothing$, atunci $(\mathcal{P}(M), \cap)$, $(\mathcal{P}(M), \cup)$ şi $(\mathcal{P}(M), \Delta)$ sunt monoizi comutativi.

2) Dacă $A \neq \varnothing$, atunci $(Hom(A), \circ)$, unde $Hom(A) = \{f : A \to A\}$, iar "$\circ$" semnifică operaţia uzuală de compunere a funcţiilor, este un monoid necomutativ.

Definiţia 2.4 *Fie* $(M, \circ)$ *şi* $(M', \perp)$ *doi monoizi. O funcţie* $f : M \to M'$ *se numeşte* ***morfism de monoizi*** *dacă* $f(e) = e'$ *(unde* e *şi* e' *sunt elementele neutre, din* M *şi respectiv* M'*, ale operaţiilor “*$\circ$*“ şi, corespunzător, “*$\perp$*“) şi*

$$f(x \circ y) = f(x) \perp f(y), \forall\, x, y \in M.$$

Se notează cu $Hom(M, M')$ mulţimea $\{f : M \to M' \mid \ f$ morfism de la monoizi$\}$. Se numeşte ***monomorfism de monoizi*** orice element din $Hom(M, M')$ care este funcţie injectivă. O funcţie surjectivă din $Hom(M, M')$ se numeşte ***epimorfism de monoizi***. Un morfism bijectiv de monoizi se numeşte ***izomorfism de monoizi***. Când $M' = M$, monomorfismul se numeşte ***endomorfism***, iar izomorfismul, ***automorfism***.

Definiţia 2.5 *Fie* $(M, \circ)$ *un monoid. Un element* $x \in M$ *se numeşte* ***inversabil (simetrizabil)*** *în raport cu “*$\circ$*“, dacă există* $\tilde{x} \in M$ *(numit* ***inversul*** *sau* ***simetricul*** *lui* x*), astfel încât* $x \circ \tilde{x} = \tilde{x} \circ x = e$ *(unde* e *este elementul neutru, din* M*, faţă de “*$\circ$*“).*

Se poate vedea că, dacă există simetricul $\tilde{x}$, atunci el este unic.

Când operaţia “$\circ$“ este aditivă, $\tilde{x}$ se numeşte ***opusul*** lui x şi, de regulă, se notează cu $(-x)$, iar dacă operaţia este multiplicativă, ***inversul*** $\tilde{x}$ se notează cu x^{-1}.

Mulţimea tuturor elementelor simetrizabile ale unui monoid $(M, \circ)$ constituie ansamblul unităţilor lui M şi se notează cu $U(M)$. În cazul în care A este o mulţime nevidă, avem: $U((\mathcal{P}(A), \cap)) = \{A\}$, $U((\mathcal{P}(A), \cup)) = \{\varnothing\}$, $U((\mathcal{P}(A), \Delta)) = \mathcal{P}(A)$, $U((Izo(A), \circ)) = Izo(A)$, unde $Izo(A)$ este mulţimea bijecţiilor de la A la A.

Grupuri. Inele. Corpuri.

Definiţia 2.6 *Numim* ***grup*** *un monoid* $(G, \circ)$ *pentru care* $U(G) = G$*. Un grup* $(G, \circ)$ *se numeşte* ***abelian (comutativ)*** *dacă operaţia “*$\circ$*“ este comutativă.*

Exemple:

1) $A \neq \varnothing \Rightarrow (\mathcal{P}(A), \Delta)$ este grup comutativ;

2) Dacă $(M, \circ)$ este monoid, atunci $(U(M), \circ)$ este grup.

Definiţia 2.7 *O funcţie* $f : G \to G'$ *se numeşte* ***morfism de grupuri*** *(de la grupul* $(G, \circ)$ *la grupul* $(G', \star)$*) dacă satisface relaţia:*

$$f(x \circ y) = f(x) \star f(y), \forall\, x, y \in G.$$

Se spune că $f : G \to G'$ este ***izomorfism de grupuri*** când f este un morfism bijectiv de grupuri. Un morfism de la un grup G la el însuşi se numeşte ***endomorfism*** al lui G şi dacă, în plus, endomorfismul este bijectiv, el se numeşte ***automorfism*** al lui G.

Teorema 2.1 ***(Malţev)*** *Fie* $(M, \cdot)$ *un monoid comutativ, cu proprietatea de simplificare (*$\forall\, x, y \in M$*, aşa încât* $x \cdot z = y \cdot z$*,* $\forall\, z \in M$*, avem* $x = y$*). Există atunci un grup comutativ* $G(M)$ *şi un monomorfism de monoizi* $i_M : M \to G(M)$*, astfel că, pentru orice grup* G *şi orice morfism de monoizi* $f : M \to G$*, se poate defini un unic morfism de grupuri* $f' : G(M) \to G$ *care satisface relaţia* $f' \circ i_M = f$ *(adică diagrama*

$$\begin{tikzcd} M \arrow[r, "i_M"] \arrow[d, "f"'] & G(M) \arrow[dl, "f'"'] \\ G & \end{tikzcd}$$

este comutativă).

Demonstraţie: Pe mulţimea $M \times M$ se consideră relaţia "$\sim$", definită prin: $(x, y) \sim (x', y') \Leftrightarrow x \cdot y' = y \cdot x'$. Se constată că "$\sim$" este o relaţie de echivalenţă pe $M \times M$, fiind reflexivă, simetrică şi tranzitivă. Considerăm $G(M) = M \times M/_\sim$ (mulţimea claselor de echivalenţă din $M \times M$, în raport cu "$\sim$"). Definim operaţia "$\circ$": $G(M) \to G(M)$ prin

$$[(x,y)]_\sim \circ [(x',y')]_\sim = [(x \cdot x', y \cdot y')]_\sim, \ \forall\, [(x,y)]_\sim, [(x',y')]_\sim \in G(M),$$

unde $[(x, y)]_\sim$ este notaţia pentru clasa de echivalenţă cu reprezentantul $(x, y) \in M \times M$. Se vede că operaţia "$\circ$" este bine definită pe $G(M)$, nedepinzând de reprezentanţii claselor de echivalenţă implicate. De asemenea, se constată că $(G(M), \circ)$ este monoid, cu elementul neutru $[(e, e)]_\sim$ (unde e este elementul neutru din M). Cum, pentru orice $[(x, y)]_\sim \in M$, avem

$$[(x,y)]_\sim \circ [(y,x)]_\sim = [(xy, xy)]_\sim = [(e,e)]_\sim,$$

deducem că $[(y, x)]_\sim = [(x, y)]_\sim^{-1}$. Deci $U(G(M)) = G(M)$, adică $(G(M), \circ)$ este grup. În plus, $G(M)$ este şi comutativ.

Definim acum $i_M : M \to G(M)$, prin: $i_M(x) = [(x, e)]_\sim$, $\forall\, x \in M$. Avem $i_M(e) = [(e, e)]_\sim \equiv e' \in G(M)$ şi

$$i_M(x) \circ i_M(y) = [(x,e)]_\sim \circ [(y,e)]_\sim = [(x \cdot y, e)]_\sim = i_M(x \cdot y).$$

Deci i_M este morfism de monoizi. Cum, în plus, dacă $i_M(x) = i_M(y)$, adică $[(x, e)]_\sim = [(y, e)]_\sim$, rezultă $x = y$, se poate spune că i_M este şi injectiv. Aşadar i_M este un monomorfism de monoizi. Astfel, perechea $(G(M), i_M)$ verifică proprietatea din enunţul teoremei.

În continuare, dacă $(G, \star)$ este un grup abelian oarecare şi $f : M \to G$ este un morfism de monoizi, atunci, pentru $[(x, y)]_\sim \in G(M)$, definim $f' : G(M) \to G$ prin $f'([(x, y)]_\sim) = f(x) \star (f(y))^{-1}$. Observăm că, dacă $[(x, y)]_\sim = [(x', y')]_\sim$, atunci $x \cdot y' = x' \cdot y$ şi deci $f(x) \star f(y') = f(x') \star f(y)$, adică $f(x) \star (f(y))^{-1} = f(x') \star (f(y'))^{-1}$, ceea ce înseamnă că f' este corect definită. În plus, f' este morfism de grupuri deoarece:

$$\begin{aligned} f'([(x,y)]_\sim \circ [(x',y')]_\sim) &= f'([(x \cdot x', y \cdot y')]_\sim) = \\ = f(x \cdot x') \star \big(f(y \cdot y')\big)^{-1} &= f(x) \star f(x') \star \big(f(y')\big)^{-1} \star (f(y))^{-1} = \\ &= \Big(f(x) \star (f(y))^{-1}\Big) \star \Big(f(x') \star \big(f(y')\big)^{-1}\Big) = \\ &= f'([(x,y)]_\sim) \star f'([(x',y')]_\sim), \ \forall\, [(x,y)]_\sim, [(x',y')]_\sim \in G(M). \end{aligned}$$

De asemenea, avem: $(f' \circ i_M)(x) = f'(i_M(x)) = f'([(x, e)]_\sim) = f(x) \cdot (f(e))^{-1} = f(x)$, $\forall\, x \in M$. Deci $f' \circ i_M = f$.

În privinţa unicităţii lui f', presupunând că ar mai exista un morfism $f'' : G(M) \to G$ aşa încât $f'' \circ i_M = f$, atunci am avea $f' \circ i_M = f = f'' \circ i_M$. Adică $(f'' \circ i_M)(x) = f''([(x, e)]_\sim) = f'([(x, e)]_\sim) = (f' \circ i_M)(x)$. În consecinţă am obţine:

$$\begin{aligned} f''([(x,y)]_\sim) = f''([(x,e)]_\sim \circ [(e,y)]_\sim) &= f(x) \star (f(y))^{-1} = \\ &= f'([(x,y)]_\sim), \ \forall\, [(x,y)]_\sim \in G(M). \end{aligned}$$

Deci $f'' \equiv f'$. ◀

Definiţia 2.8 *Un triplet $(A, +, \cdot)$, unde A este o mulţime nevidă, iar "$+$" şi "$\cdot$" sunt operaţii algebrice pe A, se numeşte* ***inel*** *dacă:*

i) $(A, +)$ este grup comutativ;

ii) $(A, \cdot)$ *este semigrup;*

iii) Operaţia "$\cdot$" este distributivă faţă de "+", adică

$$x \cdot (y + z) = x \cdot y + x \cdot z \text{ şi}$$

$$(x + y) \cdot z = x \cdot z + y \cdot z, \ \forall\, x, y, z \in A.$$

Dacă "$\cdot$" este o operaţie comutativă, atunci inelul A se numeşte ***comutativ***. Dacă "$\cdot$" are element neutru, atunci inelul A se numeşte ***unitar***. Dacă elementul neutru în raport cu "+" coincide cu cel în raport cu "$\cdot$", atunci ***inelul*** se numeşte ***nul***. În caz contrar, el se numeşte ***inel nenul***.

Prin convenţie, se notează: $A^* = A \setminus \{0\}$ (0 fiind elementul neutru în raport cu "+"). ***Mulţimea unităţilor unui inel unitar*** A, notată cu $U(A)$, este următoarea $\{a \in A \mid \ \exists\, b \in A$ aşa încât $a \cdot b = b \cdot a = 1\}$ (1 fiind notaţia pentru elementul neutru în raport cu "$\cdot$").

Definiţia 2.9 *Fie $(A, +, \cdot)$ un inel. Un element $a \in A$ se numeşte* ***divizor al lui zero*** *(0)* ***la stânga*** *(respectiv* ***la dreapta****) dacă există $b \in A^*$, aşa încât $a \cdot b = 0$ (respectiv $b \cdot a = 0$).*

Definiţia 2.10 *Numim* ***domeniu de integritate (inel integru)*** *un inel comutativ, nenul şi fără divizori ai lui zero, diferiţi de zero.*

Definiţia 2.11 *Fiind date două inele $(A, +, \cdot)$ şi $(B, \circ, \star)$, o funcţie $f : A \to B$ se numeşte* ***morfism (/monomorfism/epimorfism/izomorfism) de inele****, dacă:*

j) $f(a + b) = f(a) \circ f(b), \ \forall\, a, b \in A$ *şi*

jj) $f(a \cdot b) = f(a) \star f(b), \ \forall\, a, b \in A$

(/iar f este injectivă/surjectivă/bijectivă respectiv).

Definiţia 2.12 *Fie $(A, +, \cdot)$ un inel comutativ şi unitar. O submulţime nevidă $S \subseteq A$ se numeşte* ***sistem multiplicativ*** *dacă $1 \in S$ şi, $\forall\, a, b \in S$, $a \cdot b \in S$ (adică $(S, \cdot)$ este monoid).*

Dacă un sistem multiplicativ S nu are divizori ai lui zero, atunci se poate vorbi despre inelul "fracţiilor" relative la S, notat cu A_S şi introdus după cum urmează. Pe $A \times S$ se consideră relaţia binară "$\sim$", definită prin $(a, s) \sim (a', s') \leftrightarrow a \cdot s' = a' \cdot s$. Se vede lesne că "$\sim$" este o relaţie de echivalenţă pe $A \times S$. Clasa de echivalenţă corespunzătoare lui $(a, s) \in A \times S$, se notează, simbolic, cu $\dfrac{a}{s}$ şi se numeşte "fracţie". Mulţimea factor $A \times S/_{\sim}$ se notează cu A_S. Deci: $A_S = \{\dfrac{a}{s} \mid a \in A, 0 \neq s \in S\}$ (S nu are divizori ai lui 0). Cum $\dfrac{a}{s} = [(a, s)]_{\sim}, \ \forall\, a \in A$ şi $\forall\, s \in S \setminus \{0\}$, se pot defini operaţiile de adunare şi de înmulţire a fracţiilor prin:

$$\frac{a_1}{s_1} \oplus \frac{a_2}{s_2} = [(a_1 \cdot s_2 + a_2 \cdot s_1, s_1 \cdot s_2)]_{\sim} \text{ şi } \frac{a_1}{s_1} \odot \frac{a_2}{s_2} = [(a_1 \cdot a_2, s_1 \cdot s_2)]_{\sim},$$

$\forall\, a_1, a_2 \in A$ şi $s_1, s_2 \in S \setminus \{0\}$. Atunci $(A_S, \oplus, \odot)$ este un inel comutativ unitar şi se poate defini morfismul injectiv (monomorfismul) de inele unitare, $i_S : A \to A_S$, prin: $i_S(a) = \dfrac{a}{1} = [(a, 1)]_{\sim} \in A_S$. În plus, $i_S(s) \in U(A_S), \forall\, s \in S \setminus \{0\}$.

Definiţia 2.13 *Un inel unitar $(K, +, \cdot)$ se numeşte* ***corp*** *dacă $U(K) = K^* \equiv K \setminus \{0\}$.*

Dacă $(A, +, \cdot)$ este un inel integru, atunci se poate vedea că A_S, unde S este mulţimea tuturor non-divizorilor lui zero (adică A^*), este un corp numit ***corpul de fracţii*** (câturi) al lui A.

Mulţimea $\mathbb{N}$ a numerelor naturale.

Axiomatic, bazându-ne pe consideraţiile lui G. Peano, s-ar putea introduce mulţimea numerelor naturale atâta timp cât admitem existenţa a cel puţin unui aşa-numit triplet Peano.

Definiţia 2.14 *Entitatea matematică $(N, 0, s)$, în care N este o mulţime nevidă, $0 \in N$ şi $s : N \to N$ este o funcţie astfel încât au loc axiomele*

(P_1) $0 \notin s(N)$,

(P_2) *s este injectivă,*

(P_3) *dacă $M \subseteq N$, $0 \in M$ şi $\forall n \in M \Rightarrow s(n) \in M$, atunci $M = N$,*

*se numeşte **triplet Peano**.*

*Firesc, $(P_1) \sim (P_3)$ se numesc **axiome Peano**.*

Propoziţia 2.1 *Dacă $(N, 0, s)$ este un triplet Peano, atunci $N = \{0\} \cup s(N)$.*

Demonstraţie: Fie $M = \{0\} \cup s(N)$. Aşadar, $M \subseteq N$ şi, cu evidenţă, M verifică (P_3) (numită axioma inducţiei matematice). Astfel $0 \in M$ şi $\forall n \in M, s(n) \in M$. În consecinţă $M = N$. ◀

Teorema 2.2 *Orice triplet Peano este unic până la o bijecţie. Mai exact, dacă $(N, 0, s)$ este un triplet Peano, iar $(N', 0', s')$ este un alt triplet, nu numaidecât Peano, format dintr-o mulţime nevidă N', un element $0' \in N'$ şi o funcţie $s' : N' \to N'$, atunci există o funcţie unică $f : N \to N'$ aşa încât $f(0) = 0'$ şi $f \circ s = s' \circ f$, adică diagrama următoare*

$$\begin{array}{ccc} N & \xrightarrow{f} & N' \\ \downarrow_s & & \downarrow_{s'} \\ N & \xrightarrow{f} & N' \end{array}$$

este comutativă. Dacă $(N', 0', s')$ este chiar triplet Peano, atunci f este o bijecţie.

Demonstraţie: În prima situaţie, pentru existenţa lui f, considerăm toate relaţiile binare $R \subseteq N \times N'$ pentru care avem satisfăcute următoarele condiţii:

(I_1) $(0, 0') \in R$ şi

(I_2) dacă $(n, n') \in R$, atunci $(s(n), s'(n')) \in R$.

Mulţimea acestor relaţii nu este vidă, deoarece cel puţin $N \times N'$ este o astfel de relaţie (care verifică ambele impuneri (I_1) şi (I_2)). Fie $R_0 = \bigcap R$ (intersecţia tuturor relaţiilor ce satisfac (I_1) şi (I_2)). Se arată că R_0 este o relaţie funcţională ce defineşte pe f (funcţia cu graficul R_0). Pentru o asemenea funcţie, ţinând seama de (I_1), avem $(0, 0') \in R_0$, adică $f(0) = 0'$. Pe de altă parte, în virtutea condiţiei (I_2), dacă n este arbitrar din N şi $n' = f(n) \in N'$, adică $(n, n') \in R_0$, atunci $(s(n), s'(n')) \in R_0$, deci $f(s(n)) = s'(f(n)) = s'(n')$. Altfel spus, avem $f \circ s = s' \circ f$.

Pentru a vedea că R_0 este într-adevăr o relaţie funcţională, considerăm $M = \{n \in N \mid \exists n' \in N'$ aşa încât $(n, n') \in R_0\} \subseteq N$ şi arătăm că M satisface (P_3) (din Definiţia 2.14). În acest sens, pe baza ipotezei (I_1), avem $(0, 0') \in R_0$ şi deci $0 \in M$. Folosind (I_2), $\forall n \in M$, cu $n' \in N'$ aşa încât $(n, n') \in R_0$, avem $(s(n), s'(n')) \in R_0$. Deci $s(n) \in M$. Astfel, în virtutea axiomei (P_3), deoarece $(N, 0, s)$ este un triplet Peano, rezultă că $M = N$. Aşadar, deocamdată, R_0 este o relaţie binară între întreaga mulţime N şi mulţimea N'. În continuare, considerând mulţimea $\tilde{M} = \{n \in N \mid n', n'' \in N \text{ şi } (n, n'), (n, n'') \in R_0 \Rightarrow n' = n''\} \subseteq N$, arătăm că $\tilde{M} = N$, ceea ce ar însemna că R_0 este o relaţie funcţională de la N la N'. În acest scop, vedem mai ıntâi că, dacă $(0, n') \in R_0$ (cum, deja, $(0, 0') \in R_0$), atunci $n' = 0'$. Dacă însă, prin absurd, $n' \neq 0'$, atunci luăm în considerare relaţia $R_1 = R_0 \setminus \{(0, n')\} \subset N \times N'$. Cum $n' \neq 0'$, folosind (I_1), deducem că $(0, 0') \in R_1$. Dacă, pentru $m \in N'$, avem $(n, m) \in R_1$, atunci $(n, m) \in R_0$ şi $(n, m) \neq (0, n')$. Prin (I_2), deducem că $(s(n), s'(m)) \in R_0$ şi, cum $(s(n), s'(m)) \neq (0, n')$ (căci $s(n) \neq 0$, în conformitate cu (P_1)), avem: $(s(n), s'(m)) \in R_1$. Prin urmare, R_1 verifică (I_1) şi (I_2), ceea ce înseamnă că ar trebui să avem $R_0 \subseteq R_1$, contrar faptului că, în realitate, $R_1 \subset R_0$. În consecinţă, contradicţia ne asigură că $n' = 0'$.

Putem afirma acum că $0 \in \tilde{M}$, întrucât, dacă n' şi n'', din N', sunt aşa încât $(0, n')$ şi $(0, n'') \in R_0$, atunci, în mod necesar, avem $n' = n'' = 0'$.

În continuare, fie $n \in \tilde{M}$ şi $n' \in N'$ aşa încât $(n, n') \in R_0$. Arătăm că, dacă avem $(s(n), n'') \in R_0$ (cu $n'' \in N''$), atunci $n'' = s'(n')$. Să admitem, prin absurd, că $n'' \neq s'(n')$. Considerând atunci relaţia $R_2 = R_0 \setminus \{(s(n), n'')\}$, vedem că R_2 satisface (I_1) şi (I_2). Într-adevăr, $(0, 0') \in R_2$ (căci $0 \neq s(n)$) (adică are loc (I_1)), iar dacă $(p, p') \in R_2$, atunci $(p, p') \in R_0$ şi $(p, p') \neq (s(n), n'')$. Prin (I_2), deducem că $(s(p), s'(p')) \in R_0$. Dacă presupunem că $(s(p), s'(p')) = (s(n), n'')$, am avea $s(p) = s(n)$, adică $p = n$, şi $s'(p') = n''$. Atunci, cum $(n, n') \in R_0$ şi $(n, p') = (p, p') \in R_0$, iar $n \in \tilde{M}$, găsim $n' = p'$. Astfel, am găsi că $n'' = s'(p') = s'(n')$, ceea ce contrazice presupunerea $n'' \neq s'(n')$. Prin urmare, avem $(s(p), s'(p')) \neq (s(n), n'')$, adică $(s(p), s'(p')) \in R_2$. Cu alte cuvinte, R_2 satisface (I_1) şi (I_2) şi ar trebui ca $R_0 \subseteq R_2$, contrazicând realitatea considerată ($R_2 \subsetneq R_0$). În consecinţă, $(s(n), n'') \in R_0$ implică $n'' = s'(n')$, aşa că, dacă $r, t \in N'$ şi $(s(r), r), (s(t), t) \in R_0$, atunci $r = t = s'(n')$. Aşadar $\tilde{M} = N$, adică R_0 este de tip funcţional.

Pentru a arăta că f este unică, admitem prin absurd că mai există o funcţie $f' : N \to N'$ aşa încât $f'(0) = 0'$ şi $s'(f'(n)) = f'(s(n)), \forall n \in N$. Considerăm mulţimea $\hat{M} = \{n \in N \mid f(n) = f'(n)\} \subseteq N$. Observăm că $0 \in \hat{M}$ (întrucât $f(0) = f'(0) = 0'$). În plus, dacă $n \in \hat{M}$, adică $f(n) = f'(n)$, atunci $s'(f(n)) = s'(f'(n))$, de unde: $f(s(n)) = f'(s(n))$. Deci $s(n) \in \hat{M}$. Aşadar, prin (P_3), avem $\hat{M} = N$. Altfel spus, $f = f'$ (peste tot pe N).

Finalmente, arătăm că dacă $(N', 0', s')$ este un triplet Peano, atunci f este o bijecţie. Mai întâi, fie $P = \{n \in N \mid \text{dacă } m \in N \text{ şi } f(m) = f(n), \text{ atunci } m = n\} \subseteq N$. Sesizăm că $0 \in P$, întrucât, dacă $m \in N$ este aşa încât $f(m) = f(0)$, atunci $m = 0$. Altfel, dacă $m \neq 0$, atunci, în conformitate cu Propoziţia 2.1, există $n \in N$ aşa încât $m = s(n)$ şi $f(s(n)) = f(0) = 0'$, adică $s'(f(n)) = 0'$, ceea ce nu se poate, deoarece, prin ipoteză, $(N', 0', s')$ este un triplet Peano şi deci, prin (P_1), $0'$ nu este "succesorul" niciunui element din N'.

Fie acum $n \in P$, arbitrar. Să arătăm că $s(n) \in P$. Luăm atunci $m \in N$, aşa încât $f(m) = f(s(n))$. Este clar că $m \neq 0$. Altfel, ar rezulta că $0' = f(0) = f(s(n)) = s'(f(n))$, ceea ce ar fi contrar axiomei (P_1), verificată de tripletul Peano $(N', s', 0')$. Deci $m \neq 0$ şi atunci, aplicând Propoziţia 2.1, există $u \in N$ aşa încât $m = s(u)$. Astfel, avem $f(m) = f(s(u)) = f(s(n))$, adică $s'(f(u)) = s'(f(n))$, ceea ce implică $f(u) = f(n)$. Cum $n \in P$, reiese că $u = n$, de unde $m = s(u) = s(n)$. În concluzie, $P = N$ şi f este injectivă.

Pentru a arăta surjectivitatea lui f, considerăm mulţimea $Q = \{n' \in N' \mid \exists\, n \in N \text{ aşa încât } n' = f(n)\}$. Cum $f(0) = 0'$, deducem că $0' \in Q$. În plus, dacă $n' \in Q$, atunci $\exists\, n \in N$, aşa încât $n' = f(n)$. Astfel, $s'(n') = s'(f(n)) = f(s(n'))$, adică $s'(n') \in Q$. Concluzia este că avem $Q = N'$, întrucât $(N', s', 0')$ este triplet Peano. Aşadar, f este şi surjectivă. ◀

Pe baza Teoremei 2.2, putem considera că, în definitiv, esenţial este un reprezentant al tuturor tripletelor Peano existente. Mulţimea dintr-un asemenea triplet se numeşte, prin convenţie, ***mulţime a numerelor naturale*** şi se notează cu $\mathbb{N}$. Elementul 0 se va numi ***prim element*** al lui $\mathbb{N}$, iar funcţia s - ***funcţie de succesiune***. Drept urmare, elementul $s(n)$ se va numi ***succesorul*** lui $n \in \mathbb{N}$.

Tot axiomatic, se pot introduce operaţiile algebrice de ***adunare*** şi de ***înmulţire a numerelor naturale***, în raport cu care, atât $(\mathbb{N}, +)$ cât şi $(\mathbb{N}, \cdot)$ sunt monoizi comutativi.

Teorema 2.3 ***(Axiomele adunării numerelor naturale)*** *Există o unică operaţie algebrică pe* $\mathbb{N}$, *notată cu "+" şi denumită adunare a numerelor naturale, astfel încât să avem:*

(A_1) $0 + n = n$, $\forall\, n, m \in \mathbb{N}$ *şi*

(A_2) $s(n) + m = s(n + m)$, $\forall\, n, m \in \mathbb{N}$.

Demonstraţie: Fie $m \in \mathbb{N}$, arbitrar fixat. Considerăm tripletul Peano $(\mathbb{N}, m, s)$. Potrivit Teoremei 2.2, există o funcţie bijectivă unică $f_m : \mathbb{N} \to \mathbb{N}$, astfel ca $f_m(0) = m$ şi $s(f_m(n)) = f_m(s(n))$, $\forall\, n \in \mathbb{N}$. Pentru $n \in \mathbb{N}$, arbitrar fixat, definim operaţia "+" : $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ prin $n + m = f_m(n)$. Atunci, $0 + m = f_m(0) = m$ şi $s(n) + m = f_m(s(n)) = s(f_m(n)) = s(n + m)$. Deci au loc (A_1) şi (A_2). ◀

Propoziţia 2.2 *Au loc relaţiile:*

a) $m + 0 = m$, $\forall\, m \in \mathbb{N}$,

b) $n + s(m) = s(n + m)$, $\forall\, n, m \in \mathbb{N}$

Demonstraţie: Pentru m fixat arbitar în $\mathbb{N}$, considerăm mulţimile $L = \{m \in \mathbb{N} \mid m + 0 = m\} \subseteq \mathbb{N}$ şi $S = \{n \in \mathbb{N} \mid n + s(m) = s(n + m)\} \subseteq \mathbb{N}$. Arătăm că L şi S se supun axiomei (P_3) din definiţia unui triplet Peano. În acest fel, obţinem faptul că $L = \mathbb{N}$ şi $S = \mathbb{N}$, ceea ce asigură valabilitatea relaţiilor a) şi b) din enunţul acestei propoziţii.

Într-adevăr, cum, în $\mathbb{N}$, are loc (A_1) din Teorema 2.3, luând acolo $m = 0$, avem: $0 + 0 = 0$. Deci $0 \in L$. Apoi, dacă $m \in L$, atunci $m + 0 = m$ şi $s(m) + 0 = s(m + 0) = s(m)$, adică: $s(m) \in L$. Aşadar, $L = \mathbb{N}$ (prin (P_3)), adică a).

Pentru b), observăm că $0 \in S$, deoarece: $0 + s(m) = s(0 + m) = s(m)$. De asemenea, dacă $n \in S$, atunci $n + s(m) = s(n + m)$ şi, mai departe, $s(n) + s(m) = s(n + s(m))$. Deci $s(n) \in S$, adică $S = \mathbb{N}$. Astfel, are loc b). ◀

Propoziţia 2.3 $(\mathbb{N}, +)$ *este un monoid (aditiv) comutativ, cu proprietatea de simplificare (dacă* $m, n \in \mathbb{N}$ *sunt aşa încât* $m + p = n + p$, *cu* $p \in \mathbb{N}$, *atunci* $m = n$*).*

Demonstraţie: În conformitate cu (A_1) din Teorema 2.3 şi cu a) din Propoziţia 2.2, reiese că 0 este element neutru pentru adunarea numerelor naturale.

Pentru a demonstra asociativitatea adunării numerelor naturale, considerăm mulţimea $B = \{n \in \mathbb{N} \mid (n + m) + p = n + (m + p), \forall\, m, p \in \mathbb{N}\}$. Evident $0 \in B$. Totodată, dacă $n \in B$, avem $s(n) \in B$, deoarece: $(s(n) + m) + p = s((n + m) + p) = s(n + (m + p)) = s(n) + m + p$, $\forall\, m, p \in \mathbb{N}$. Aşadar, B satisface (P_3) din Definiţia 2.14 şi deci $B = \mathbb{N}$.

Comutativitatea adunării numerelor naturale se dovedeşte în mod asemănător, arătând că mulţimea $D = \{n \in \mathbb{N} \mid n + m = m + n, \forall\, m \in \mathbb{N}\} \subseteq \mathbb{N}$ satisface (P_3). În acest sens, constatăm că $0 \in D$ (deoarece $0 + m = m = m + 0$, $\forall\, m \in \mathbb{N}$) şi că, dacă $n \in D$, atunci şi $s(n) \in D$, întrucât avem:

$$s(n) + m = s(n + m) = s(m + n) = m + s(n), \forall\, m \in \mathbb{N}.$$

În consecinţă, $D = \mathbb{N}$, ceea ce înseamnă că operaţia de adunare este într-adevăr comutativă pe $\mathbb{N}$.

Pentru final, privitor la "simplificare", fie $m, n \in \mathbb{N}$ (fixate arbitrar) şi $H = \{p \in \mathbb{N} \mid n + p = m + p \Rightarrow m = n\} \subseteq \mathbb{N}$. Vedem că $0 \in H$, întrucât $n + 0 = m + 0 \Rightarrow n = m$. De asemenea, deducem că dacă $p \in H$, atunci şi $s(p) \in H$, deoarece avem:

$$n + s(p) = m + s(p) \Leftrightarrow s(n + p) = s(m + p) \Rightarrow n + p = m + p \Rightarrow n = m.$$

Deci $H = \mathbb{N}$. ◀

Convenind să notăm cu 1 succesorul lui 0 ($1 = s(0)$), avem: $s(n) = s(n+0) = n + s(0) = n + 1$, $\forall\, n \in \mathbb{N}$. În felul acesta, reiese că $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, unde, tot convenţional, am adoptat notaţiile $2 = s(1), 3 = s(2)$ etc.

Se poate arăta că, dacă m şi n sunt din $\mathbb{N}$, aşa încât $m + n = 0$, atunci, în mod necesar, avem: $m = n = 0$.

Teorema 2.4 ***(Axiomele înmulţirii numerelor naturale)*** *Există o unică operaţie algebrică pe* $\mathbb{N}$, *notată cu "·" şi denumită* ***înmulţire a numerelor naturale***, *astfel încât au loc relaţiile:*

I_1) $m \cdot 0 = 0$, $\forall\, m \in \mathbb{N}$;

I_2) $m \cdot s(n) = m \cdot n + m$, $\forall\, m, n \in \mathbb{N}$.

Demonstraţie: Fie $m \in \mathbb{N}$, fixat arbitrar, şi tripletul Peano $(\mathbb{N}, 0, f_m)$, unde $f_m : \mathbb{N} \to \mathbb{N}$ este definită prin $f_m(n) = n + m$, $\forall\, n \in \mathbb{N}$. Atunci, potrivit Teoremei 2.2, există o funcţie unică, $g_m : \mathbb{N} \to \mathbb{N}$, aşa încât $g_m(0) = 0$ şi $f_m \circ g_m = g_m \circ s$. Definim atunci operaţia de înmulţire "·" : $\mathbb{N} \times \mathbb{N} \to N$, prin: $m \cdot n = g_m(n)$, $\forall\, n \in \mathbb{N}$. Astfel, avem: $m \cdot 0 = g_m(0) = 0$ (adică I_1)) şi $m \cdot s(n) = g_m(s(n)) = (g_m \circ s)(n) = (f_m \circ g_m)(n) = f_m(g_m(n)) = f_m(m \cdot n) = m \cdot n + m$ (adică I_2)) ◀

Ca şi în cazul adunării numerelor naturale, se poate demonstra, în mod cu totul analog, că au loc relaţiile:

c) $0 \cdot m = 0$, $\forall\, m \in \mathbb{N}$;

d) $s(n) \cdot m = n \cdot m + m$, $\forall\, m, n \in \mathbb{N}$.

Propoziţia 2.4 *Înmulţirea numerelor naturale este distributivă, la stânga, faţă de adunarea numerelor naturale.*

Demonstraţie: Fie $M = \{p \in \mathbb{N} \mid m \cdot (n + p) = m \cdot n + m \cdot p, \forall\, m, n \in \mathbb{N}\}$. Avem $0 \in M$, deoarece $m \cdot (n + 0) = m \cdot n = m \cdot n + 0 = m \cdot n + m \cdot 0$. De asemenea, dacă $p \in M$ şi $m, n \in \mathbb{N}$, avem:

$$m \cdot (n + s(p)) = m \cdot s(n + p) = m \cdot (n + p) + m = m \cdot n + m \cdot p + m = m \cdot n + m \cdot s(p).$$

Deci $s(p) \in M$. Astfel, în conformitate cu (P_3) din Definiţia 2.14, deducem că $M = N$. Altfel spus, distributivitatea la stânga a înmulţirii faţă de adunare, are loc peste tot pe $\mathbb{N}$. ◀

Teorema 2.5 *Dubletul* $(\mathbb{N}, \cdot)$ *este monoid (multiplicativ) comutativ, în care, dacă* $m, n \in \mathbb{N}$ *şi* $m \cdot n = 0$, *atunci* $m = 0$ *sau* $n = 0$.

Demonstraţie: Asociativitatea înmulţirii pe $\mathbb{N}$ se arată considerând mulţimea $P = \{p \in \mathbb{N} \mid (m \cdot n) \cdot p = m \cdot (n \cdot p), \forall\, m, n \in \mathbb{N}\} \subseteq \mathbb{N}$. Cu evidenţă, $0 \in P$, deoarece: $(m \cdot n) \cdot 0 = 0 = m \cdot 0 = m \cdot (n \cdot 0)$, $\forall\, m, n \in \mathbb{N}$. În plus, dacă $p \in P$, avem şi $s(p) \in P$, întrucât:

$$(m \cdot n) \cdot s(p) = (m \cdot n) \cdot p + m \cdot n = m \cdot (n \cdot p) + m \cdot n = m \cdot (n \cdot p + n) = m \cdot (n \cdot s(p)), \forall\, m, n \in \mathbb{N}.$$

Deci P satisface (P_3) din Definiţia 2.14 şi, în consecinţă, $P = N$.

Cum, $\forall\, n \in \mathbb{N}$, avem $n \cdot 1 = n \cdot s(0) = n \cdot 0 + n = 0 + n = n$, iar $1 \cdot n = s(0) \cdot n = 0 + n = n$, deducem că 1 (adică $s(0)$) este elementul neutru al înmulţirii numerelor naturale.

Pentru a vedea că înmulţirea este comutativă, luăm în considerare mulţimea $Q = \{n \in \mathbb{N} \mid n \cdot m = m \cdot n, \forall\, m \in \mathbb{N}\}$. Vedem că $0 \in Q$, deoarece $0 \cdot m = 0 = m \cdot 0$, $\forall\, m \in \mathbb{N}$. De asemenea, dacă $n \in Q$, avem:

$$s(n) \cdot m = n \cdot m + m = m \cdot n + m = m \cdot s(n), \forall\, m \in \mathbb{N}.$$

Deci $s(n) \in Q$ şi, prin (P_3), $Q = \mathbb{N}$.

În fine, dacă $m, n \in \mathbb{N}$ sunt aşa încât $m \cdot n = 0$ şi $m \neq 0$, atunci există $k \in \mathbb{N}$ încât $m = s(k)$ şi avem:

$$0 = m \cdot n = s(k) \cdot n = k \cdot n + n.$$

De aici, rezultă că $n = 0$ şi $k \cdot n = 0$, cu necesitate. ◀

Definiţia 2.15 *Pentru $m, n \in \mathbb{N}$, scriem $m \leq n$ şi spunem că m este* ***mai mic sau egal decât*** *n (sau, echivalent, că n este* ***mai mare sau egal decât*** *m), dacă există $p \in \mathbb{N}$ astfel încât $m + p = n$.*

Dacă $m, n \in \mathbb{N}$ sunt aşa încât $m \leq n$ şi $m \neq n$, atunci scriem $m < n$ şi spunem că m este ***strict mai mic decât*** *n. În acest caz, există $p \in \mathbb{N}^* = s(\mathbb{N})$, aşa încât $m + p = n$.*

Propoziţia 2.5 *Dacă $m, n \in \mathbb{N}$ şi $m < n$, atunci $s(m) \leqslant n$.*

Demonstraţie: Fie $m, n \in \mathbb{N}$, încât $m < n$. Atunci $\exists\, p \in \mathbb{N}^*$ astfel încât $m + p = n$. Cum $p \in \mathbb{N}^*$, există $k \in \mathbb{N}$ încât $p = s(k)$. Prin urmare, avem: $m + p = n \Leftrightarrow m + s(k) = n \Leftrightarrow s(m + k) = n \Leftrightarrow s(m) + k = n \Rightarrow s(m) \leq n$. ◀

Se poate, relativ uşor, vedea că $n < s(n)$, $\forall\, n \in \mathbb{N}$.

Teorema 2.6 *Dubletul $(\mathbb{N}, \leqslant)$ este o mulţime total şi bine ordonată, adică relaţia "$\leqslant$" este una de totală ordine pe $\mathbb{N}$ şi orice submulţime nevidă $A \subseteq \mathbb{N}$ are un cel mai mic element.*

Demonstraţie: Pentru început, deoarece $n + 0 = n$, $\forall\, n \in \mathbb{N}$, vedem că $n \leq n$, $\forall\, n \in \mathbb{N}$. Deci relaţia "$\leq$" este reflexivă pe $\mathbb{N}$. Luând apoi $m, n \in \mathbb{N}$ aşa încât $m \leq n$ şi $n \leq m$, vor exista p şi q din $\mathbb{N}$ aşa încât $m + p = n$ şi $n + q = m$. Deducem de aici că $m + (p + q) = m$, de unde reiese că $p + q = 0$. Deci $p = q = 0$. Astfel, rezultă că $m = n$. Altfel spus, relaţia "$\leq$" este antisimetrică. În fine, dacă $m, n, p \in \mathbb{N}$ sunt aşa încât $m \leq n$ şi $n \leq p$, atunci există r şi $s \in \mathbb{N}$ ca să avem $m + r = n$ şi $n + s = p$. Deducem că $m + (r + s) = p$, adică $m \leq p$. Aşadar, relaţia "$\leq$" este şi tranzitivă, fiind de fapt o relaţie de ordine pe $\mathbb{N}$.

În scopul demonstrării faptului ca "$\leq$" este o relaţie de ordine totală (numită ***ordinea naturală***) pe $\mathbb{N}$, considerăm $m \in \mathbb{N}$, arbitrar fixat şi faţă de care mulţimea $P_m = \{n \in \mathbb{N} \mid n \leq m \text{ sau } m \leq n\} \subseteq \mathbb{N}$. Observăm că $0 \in P_m$, deoarece $0 \leq m$, cu evidenţă. Luând acum un n oarecare din P_m, deducem că, dacă $n = m$, atunci, întrucât $n < s(n)$, avem $m < s(n)$, adică $s(n) \in P_m$. Dacă $n < m$, atunci, în conformitate cu Propoziţia 2.5, avem $s(n) \leq m$ şi deci, iarăşi, $s(n) \in P_m$. Dacă $m < n$, cum $n < s(n)$ şi "$\leq$" este o relaţie tranzitivă, avem $m < s(n)$ şi deci $s(n) \in P_m$. Prin (P_3), rezultă aşadar că $P_m = \mathbb{N}$. Cum m este oarecare în $\mathbb{N}$, reiese că ordinea "$\leq$" este totală pe $\mathbb{N}$.

Arătăm acum că $(\mathbb{N}, \leq)$ este bine ordonată. Fie, în acest scop, o mulţime nevidă $A \subseteq \mathbb{N}$ şi $Q = \{n \in \mathbb{N} \mid n \leq a, \forall\, a \in A\}$. Evident, $0 \in Q$. Dacă, pe lângă asta, $\forall\, n \in Q$, ar rezulta că $s(n) \in Q$, atunci am avea, prin (P_3), $Q = \mathbb{N}$. În consecinţă, alegând un $a \in A \subseteq \mathbb{N} = Q$, am putea spune că $s(a) \in Q$. Or, acest lucru ar însemna că $s(a) \leq a$, ceea ce ar fi absurd. Deducem astfel că, de fapt, avem $Q \subsetneq \mathbb{N}$. Există deci $r \in Q$ aşa încât $s(r) \notin Q$. Arătăm că $r \in A$ şi că r este cel mai mic element al lui A. Dacă r nu ar aparţine lui A, atunci, fiind din Q, am avea $r < a$, $\forall\, a \in A$. De aici ar reieşi că $s(r) \leq a$, $\forall\, a \in A$. Deci $s(r) \in Q$ (absurd). Aşadar, $r \in A$ şi, cum $r \in Q$, avem $r \leq a$, $\forall\, a \in A$. Deci r este cel mai mic element al lui A. ◀

Observaţii

1) În virtutea Definiţiei 1.20-b, se poate vedea că $\mathbb{N}$ este un ordinal infinit şi anume chiar cel mai mic, adică ω.

2) $\forall\, n \in \mathbb{N}$, mulţimea $\{0, 1, \ldots, n\}$ este, de asemenea, un ordinal finit.

3) Un ordinal defineşte un număr natural, dacă şi numai dacă orice submulţime nevidă a sa are cel mai mare element.

4) Intuitiv, un ordinal desemnează poziţii într-un şir bine ordonat de entităţi şi, de aceea, prin analogie cu elementele lui $\mathbb{N}$ i se mai spune ***număr ordinal***.

Principiul inducţiei transfinite

Varianta I: Fie $P(x)$ o proprietate astfel încât, pentru orice ordinal α, avem:

$$\forall\, \beta\ (\beta < \alpha \Longrightarrow P(\beta)) \Longrightarrow P(\alpha)$$

Atunci P este satisfăcută de orice ordinal.

Varianta II: Fie $P(x)$ o proprietate astfel încât:

j) $P(0)$ are loc;

jj) pentru orice ordinal α, $P(\alpha)$ implică $P(S(\alpha))$;

jjj) pentru orice ordinal limită $\alpha \neq 0$, dacă $P(\beta)$ are loc pentru orice $\beta < \alpha$, atunci şi $P(\alpha)$ are loc.

Atunci P este satisfăcută de toţi ordinalii.

Principiul recursiei transfinite

Fie γ un ordinal, adică un element al mulţimii Ord, A o mulţime oarecare şi $\mathcal{F}$ mulţimea tuturor funcţiilor (inclusiv cea vidă) cu valori în A şi definite pe $\{\beta \in Ord \mid \beta < \gamma\}$. De asemenea, fie $H : \mathcal{F} \to A$. Atunci există o funcţie unică G, cu domeniul $\{\alpha \in Ord \mid \alpha < \gamma\}$, astfel încât, pentru orice $\alpha < \gamma$, are loc relaţia:

$$G(\alpha) = H\left(G|_{\{\beta \in Ord\ \mid\ \beta < \alpha\}}\right).$$

Aritmetica ordinalilor

Pe baza principiului recursiei transfinite, se pot defini operaţiile de adunare, înmulţire şi exponenţiere a numerelor ordinale. Prin folosirea unor notaţii similare celor de la aritmetica numerelor naturale, succesorul unui ordinal α (adică $S(\alpha)$) va fi redat prin $\alpha + 1$ şi operaţiile cu ordinale specificate mai sus se pot exprima mai lesne, fiind introduse, împreună cu proprietăţile lor definitorii, după cum urmează.

Propoziţia 2.6 *1° Există "+": $Ord \times Ord \to Ord$, astfel încât:*

(a) $\alpha + 0 = \alpha$, $\forall\, \alpha \in Ord$,

(b) $\alpha + (\beta + 1) = (\alpha + \beta) + 1$, $\forall\, \alpha, \beta \in Ord$,

(c) $\alpha + \beta = \sup\{\alpha + \gamma \mid \gamma < \beta\}$, $\forall\, \alpha, \beta \in Ord$, $\beta =$ *ordinal limită,* $\beta \neq 0$.

2° Există "·": $Ord \times Ord \to Ord$, astfel încât:

(a) $\alpha \cdot 0 = 0, \forall \alpha \in Ord$,

(b) $\alpha \cdot (\beta + 1) = \alpha \cdot \beta + \alpha, \forall \alpha, \beta \in Ord$,

(c) $\alpha \cdot \beta = \sup \{\alpha \cdot \gamma \mid \gamma < \beta\}, \forall \alpha, \beta \in Ord$, $\beta =$ *ordinal limită*, $\beta \neq 0$.

3° Există "^": $Ord \times Ord \to Ord$, astfel încât:

(a) $\alpha\hat{}0 = 1, \forall \alpha \in Ord$,

(b) $\alpha\hat{}(\beta + 1) = (\alpha\hat{}\beta) \cdot \alpha, \forall \alpha, \beta \in Ord$,

(c) $\alpha\hat{}\beta = \sup \{\alpha\hat{}\gamma \mid \gamma < \beta\}, \forall \alpha, \beta \in Ord$, $\beta =$ *ordinal limită*, $\beta \neq 0$.

Se poate vedea că adunarea ordinalilor şi înmulţirea ordinalilor sunt asociative, dar nu şi comutative. De asemenea, înmulţirea ordinalilor se dovedeşte a fi distributivă faţă de adunare.

Observaţii

1) O mulţime A care este echipotentă cu o mulţime de numere naturale de forma $\{1, 2, \ldots, n\}$ ($n \in \mathbb{N}^*$) se numeşte ***mulţime finită*** şi are cardinalul egal cu n.

2) O mulţime care nu este finită se numeşte ***mulţime infinită***.

3) Cardinalul unei mulţimi finite se numeşte ***cardinal finit***, iar cardinalul unei mulţimi infinite se numeşte ***cardinal transfinit***.

4) O mulţime echipotentă cu $\mathbb{N}$ se numeşte ***mulţime numărabilă***, cardinalul său fiind notat cu $\aleph_0$ (alef zero).

5) O mulţime care este finită sau numărabilă se numeşte ***cel mult numărabilă***.

1. Se poate arăta că orice mulţime infinită A conţine o submulţime numărabilă, ceea ce, formulat altfel, înseamnă că, pentru A, are loc relaţia:

$$\aleph_0 \leqslant card(A).$$

Operaţii aritmetice cu numere cardinale

Pentru $\alpha = card(A)$ şi $\beta = card(B)$, se pot defini următoarele operaţii (cu numere cardinale):

$$\alpha + \beta = card(A \cup B), \text{ dacă } A \cap B = \varnothing,$$

$$\alpha \cdot \beta = card(A \times B)$$

$$\alpha^\beta = card(\{f : B \to A\})$$

Observaţii

1) Adunarea, înmulţirea şi exponenţierea numerelor cardinale, restricţionate la cardinali finiţi, coincid cu operaţiile corespunzătoare pe $\mathbb{N}$.

2) Pentru orice cardinal α, avem $\alpha + 1 = \alpha$ dacă şi numai dacă α este un cardinal infinit.

Mulţimile $\mathbb{Z}$ şi $\mathbb{Q}$

Definiţia 2.16 *Fie monoidul* $(\mathbb{N}, +)$. *Prin tehnica din Teorema 2.1 (Malţev), mulţimea ce corespunde grupului aditiv* $(G(\mathbb{N}), +)$ *se notează cu* $\mathbb{Z}$ *şi poartă denumirea de* ***mulţime a numerelor întregi****. Corespunzător,* $(\mathbb{Z}, +)$ *este grupul aditiv al numerelor întregi.*

Potrivit respectivei Teoreme 2.1, există monomorfismul de monoizi $i_{\mathbb{N}} : \mathbb{N} \to \mathbb{Z}$, definit prin $i_{\mathbb{N}}(n) = [(n, 0)]$, $\forall n \in \mathbb{N}$. În virtutea acestuia, "identificăm" fiecare număr natural n cu "întregul" $[(n, 0)]$. Astfel, putem spune că avem: $\mathbb{N} \subset \mathbb{Z}$.

Totodată, clasa $[(n, n)]$ se notează cu 0 $(\in \mathbb{Z})$, pe când elementul $[(0, p)] = -[(p, 0)]$ se identifică cu numărul întreg $-p$ $(p \in \mathbb{N})$. Ţinând cont de acestea, putem scrie: $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N}^*)$, cu $(-\mathbb{N}^*) = \{-n \mid n \in \mathbb{N}^*\}$. Deci: $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Pe $\mathbb{Z} \cong G(\mathbb{N})$, se mai poate defini şi înmulţirea (numerelor întregi), prin:

$$(*) \quad \alpha \cdot \beta = [(x, y)] \cdot [(z, t)] = [(xz + yt, xt + yz)], \ \forall \alpha = [(x, y)], \beta = [(z, t)] \in \mathbb{Z}$$

Propoziţia 2.7 *Dubletul* $(\mathbb{Z}, \cdot)$ *este un monoid (multiplicativ) comutativ, în care operaţia "$\cdot$" este distributivă faţă de "$+$" şi, dacă* $\alpha, \beta \in \mathbb{Z}$ *sunt aşa încât* $\alpha \cdot \beta = 0$*, atunci* $\alpha = 0$ *sau* $\beta = 0$.

Demonstraţie: Se arată simplu că înmulţirea numerelor întregi, în sensul relaţiei de definiţie $(*)$, este asociativă, are elementul neutru $1 = [(1, 0)]$, este comutativă şi distributivă faţă de adunarea numerelor întregi. Se vede apoi că, dacă $\alpha = [(x, y)], \beta = [(x', y')] \in \mathbb{Z}$ sunt astfel încât $\alpha \cdot \beta = 0$ şi $\alpha \neq 0$, adică $[(x, y)] \cdot [(x', y')] = [(0, 0)]$ şi $x \neq y$, atunci $x' = y'$, adică $\beta = 0$. La fel, dacă $\beta \neq 0$, rezultă $\alpha = 0$. ◀

Se poate afirma acum că $(\mathbb{Z}, +, \cdot)$ este un inel integru, în care $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ este un sistem multiplicativ maximal.

Definiţia 2.17 *Pentru* $x, y \in \mathbb{Z}$*, spunem că* $x \leqslant y$*, dacă şi numai dacă* $y - x \in \mathbb{N}$.

Propoziţia 2.8 *Dubletul* $(\mathbb{Z}, \leq)$ *este o mulţime total ordonată.*

Demonstraţie: Se arată lesne că "$\leqslant$" este o relaţie binară reflexivă, antisimetrică şi tranzitivă pe $\mathbb{Z}$. Faptul că avem $\mathbb{Z} = (-\mathbb{N}^*) \cup \mathbb{N}$ ne spune că relaţia de ordine "$\leqslant$" este şi totală pe $\mathbb{Z}$. ◀

În sensul definirii corpului total de fracţii al unui inel integru, putem spune acum că, relativ la $(\mathbb{Z}, +, \cdot)$, corpul corespunzător este tocmai mulţimea $\mathbb{Q}$ a ***numerelor raţionale***. În plus, prin existenţa monomorfismului $i_{\mathbb{Z}^*} : \mathbb{Z} \to \mathbb{Q}$, putem conta pe relaţia $\mathbb{Z} \subset \mathbb{Q}$. De asemenea, prin extensie, se poate vorbi de o relaţie totală de ordine pe $\mathbb{Q}$, definită prin:

$$u, v \in \mathbb{Q}, u \leq v \Longleftrightarrow \exists\, w \in \mathbb{Q}_+ = i_{\mathbb{Z}_+^*}(\mathbb{Z}_+) = i_{\mathbb{N}_+^*}(\mathbb{N}_+) \text{ cu } u + w = v.$$

Deci $(\mathbb{Q}, +, \cdot, \leq)$ este un corp total ordonat, cu ordinea compatibilă cu "$+$" şi, pentru elemente din $\mathbb{Q}_+$, chiar cu "$\cdot$".

Analizând mulţimea $A = \{x \in \mathbb{Q} \mid 0 < x^2 < 2\}$, observăm că ea este majorată în $\mathbb{Q}$, dar $\sup A \notin \mathbb{Q}$. Prin urmare există submulţimi ale lui $\mathbb{Q}$ care, majorate fiind, nu-şi au marginea superioară în $\mathbb{Q}$. Dintr-un astfel de punct de vedere, spunem că mulţimea $\mathbb{Q}$ nu-i completă, în sens Cantor-Dedekind. Mulţimea care satisface, pe lângă axiomele îndeplinite de $\mathbb{Q}$, şi ***axioma de completitudine a lui Cantor-Dedekind***, potrivit căreia, orice submulţime nevidă şi majorată a ei are cel puţin o margine superioară (în mulţimea de referinţă) este ***mulţimea numerelor reale***, notată cu $\mathbb{R}$.

Mulţimile $\mathbb{R}$ şi $\overline{\mathbb{R}}$

Faptul că mulţimea $\mathbb{R}$, cu caracteristicile deja menţionate, există într-adevăr se poate arăta în câteva moduri, între care specificăm aici, metoda lui Dedekind, bazată pe aşa-numita noţiune de tăietură, metoda lui Weierstrass, sprijinită pe noţiunea de fracţie zecimală şi metoda lui Cantor, axată pe noţiunea de şir fundamental (Cauchy) de numere raţionale. Aceasta din urmă, neeludând principiul teoremei lui Malţev, va fi prezentată, preferenţial, în secţiunea ce urmează celei de faţă şi se referă la şiruri de elemente din inele şi corpuri ordonate, precum $\mathbb{Q}$.

Deocamdată, din cele spuse până aici, se impune atenţiei următoarea definiţie axiomatică a ***mulţimii*** $\mathbb{R}$ ***a numerelor reale***.

Definiţia 2.18 $\mathbb{R}$ *este o mulţime cu cel puţin două elemente, înzestrată cu două operaţii algebrice – una numită adunare, notată cu "$+$" şi cealaltă numită înmulţire, notată cu "$\cdot$" – precum şi cu o relaţie de ordine, notată cu "$\leq$", în raport cu care sunt îndeplinite următoarele axiome:*

AR1. $x+(y+z)=(x+y)+z$, $\forall\, x,y,z\in\mathbb{R}$;

AR2. $\exists\, 0\in\mathbb{R}$, *astfel încât* $x+0=0+x=x$, $\forall\, x\in\mathbb{R}$;

AR3. $\forall\, x\in\mathbb{R}$, $\exists\,(-x)\in\mathbb{R}$ *aşa încât* $x+(-x)=(-x)+x=0$;

AR4. $x+y=y+x$, $\forall\, x,y\in\mathbb{R}$;

AR5. $(x\cdot y)\cdot z=x\cdot(y\cdot z)$, $\forall\, x,y,z\in\mathbb{R}$;

AR6. $\exists\, 1\in R$, *astfel încât* $x\cdot 1=1\cdot x=x$, $\forall\, x\in\mathbb{R}$;

AR7. $\forall\, x\in\mathbb{R}\setminus\{0\}$, $\exists\, x^{-1}\in\mathbb{R}$ *aşa încât* $x\cdot x^{-1}=x^{-1}\cdot x=1$;

AR8. $x\cdot y=y\cdot x$, $\forall\, x,y\in\mathbb{R}$;

AR9. $x\cdot(y+z)=x\cdot y+x\cdot z$, $\forall\, x,y,z\in\mathbb{R}$;

AR10. $\forall\, x,y\in\mathbb{R}$ *avem* $x\leq y$ *sau* $y\leq x$;

AR11. $\forall\, x,y\in\mathbb{R}$, *dacă* $x\leq y$ *şi* $y\leq x$, *atunci* $x=y$;

AR12. $\forall\, x,y,z\in\mathbb{R}$ *cu* $x\leq y$ *şi* $y\leq z\Longrightarrow x\leq z$;

AR13. $\forall\, x,y\in\mathbb{R}$ *cu* $x\leq y\Longrightarrow x+z\leq y+z$, $\forall\, z\in\mathbb{R}$;

AR14. $\forall\, x,y,z\in\mathbb{R}$ *cu* $x\leq y$ *şi* $0\leq z\Longrightarrow x\cdot z\leq y\cdot z$;

AR15. Orice submulţime nevidă şi majorată a lui $\mathbb{R}$ *are o margine superioară în* $\mathbb{R}$.

Altfel spus, $(\mathbb{R},+,\cdot,\leqslant)$ este un corp comutativ şi total ordonat, care satisface axioma lui Cantor-Dedekind (de completitudine) AR15.

După cum ne vom convinge în secţiunea următoare, mulţimea $\mathbb{R}$, introdusă axiomatic prin Definiţia 2.18, este unică până la un izomorfism de corpuri comutative, total ordonate. În $\mathbb{R}$, apar submulţimile remarcabile $\mathbb{N},\mathbb{Z}$ şi $\mathbb{Q}$, unice şi ele până la un izomorfism (de monoizi/inele/corpuri), aflate în relaţia:

$$\mathbb{N}\subsetneq\mathbb{Z}\subsetneq\mathbb{Q}\subsetneq\mathbb{R}.$$

Printre proprietăţile lui $\mathbb{R}$ figurează şi acelea cuprinse în următorul enunţ, lipsit aici de demonstraţie.

Propoziţia 2.9 *a) Mulţimea numerelor reale din intervalul* $[0,1]$ *este nenumărabilă. Cardinalul ei se numeşte* ***puterea continuului*** *şi notat, prin tradiţie, cu c, este egal cu* $2^{\aleph_0}$.

b) Următoarele mulţimi sunt de ***puterea continuului:***

(1) mulţimea $\mathbb{R}$*;*

(2) orice interval din $\mathbb{R}$*, de forma* $[a, b]$*,* $[a, b)$*,* (a, b)*,* $(a, b]$*, unde* $a < b$*;*

(3) mulţimea $\mathbb{R} \setminus \mathbb{Q}$ *a numerelor iraţionale;*

(4) orice submulţime a lui $\mathbb{R}$ *care conţine un interval deschis;*

(5) mulţimea lui Cantor, adică mulţimea C *a tuturor numerelor din intervalul* $[0, 1]$ *care au reprezentarea, în baza* 3*, numai cu cifrele* 0 *şi* 2*.*

Ipoteza continuului.

Pe baza Propoziţiei 1.7, putem vorbi despre suita de numere cardinale:

$$\aleph_0 \leqslant h(\aleph_0) \stackrel{def}{=} \aleph_1 \leqslant h(\aleph_1) \stackrel{def}{=} \aleph_2 \leqslant \ldots$$

Întrebarea firească este aceea asupra poziţiei pe care o are, în această suită, cardinalul $c = 2^{\aleph_0} > \aleph_0$. În acest sens, există ***ipoteza continuului***, potrivit căreia, am avea: $\aleph_1 = 2^{\aleph_0}$. Cu alte cuvinte, Cantor, cel care a emis o asemenea ipoteză, a presupus că nu există nici o mulţime al cărei cardinal este cuprins strict între cardinalul lui $\mathbb{N}$ şi cardinalul lui $\mathbb{R}$. Un asemenea postulat este, în teoria mulţimilor, analog axiomei paralelelor din geometria plană euclidiană.

Deoarece între mulţimea $\mathbb{R}$ şi mulţimea punctelor de pe o dreaptă (pe care s-a stabilit un punct numit origine, un sens – o orientare – şi o unitate de măsură) se poate pune în evidenţă o corespondenţă biunivocă (bijecţie), se ajunge de cele mai multe ori la identificarea mulţimii numerelor reale cu punctele dreptei respective, numită (pe bună dreptate) ***dreapta reală***. Astfel, adoptând un limbaj geometric, vom folosi termenul de "punct" (pe acea dreaptă) în locul celui de număr real, după cum şi termenul de "dreaptă reală" în loc de $\mathbb{R}$.

Cum, pentru o mulţime $\varnothing \neq A \subset \mathbb{R}$, nemajorată, nu mai avem asigurat faptul că $\sup A$ (în sensul ordinei totale pe $\mathbb{R}$) aparţine lui $\mathbb{R}$, iar pentru o mulţime nevidă şi neminorată $B \subset \mathbb{R}$ nu putem spune că $\inf B \in \mathbb{R}$, se iau în consideraţie două simboluri (elemente), numite ***plus infinit*** – notat cu $+\infty$ (sau, pe scurt, ∞) şi respectiv ***minus infinit*** – notat cu $-\infty$, astfel încât, pe mulţimea $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$ – numită ***dreapta reală extinsă*** (sau ***încheiată***), în virtutea convenţiei prin care $-\infty < +\infty$ şi $\forall x \in \mathbb{R}$, $-\infty < x < +\infty$, se pot extinde operaţiile "$+$" şi "$\cdot$" de pe $\mathbb{R}$, precum şi relaţia de ordine naturală, luând, prin definiţie: $x + (+\infty) = (+\infty) + x = +\infty$, $\forall x \in \overline{\mathbb{R}} \setminus \{-\infty\}$; $x + (-\infty) = (-\infty) + x = -\infty$, $\forall x \in \overline{\mathbb{R}} \setminus \{+\infty\}$; $x \cdot (+\infty) = (+\infty) \cdot x = +\infty$, dacă $0 < x$ şi $x \cdot (+\infty) = (+\infty) \cdot x = -\infty$, dacă $x < 0$; $x \cdot (-\infty) = (-\infty) \cdot x = -\infty$, dacă $0 < x$ şi $x \cdot (-\infty) = (-\infty) \cdot x = +\infty$, dacă $x < 0$; $\dfrac{x}{+\infty} = \dfrac{x}{-\infty} = 0$, $\forall x \in \mathbb{R}$.

Se consideră lipsite de sens, fiind nedeterminate, operaţiile următoare: $(+\infty) + (-\infty)$, $(+\infty) - (+\infty)$, $(-\infty) + (+\infty)$, $(-\infty) - (-\infty)$ (pe scurt $(\infty) - (\infty)$); $0 \cdot (+\infty)$, $0 \cdot (-\infty)$, $(+\infty) \cdot 0$, $(-\infty) \cdot 0$ (pe scurt $0 \cdot \infty$) şi $\dfrac{+\infty}{+\infty}$, $\dfrac{+\infty}{-\infty}$, $\dfrac{-\infty}{+\infty}$, $\dfrac{-\infty}{-\infty}$ (pe scurt $\dfrac{\infty}{\infty}$). Elucidarea sensului acestor operaţii are loc, de regulă, pe seama expresiilor din care provin.

Prin extensia menţionată, mulţimea $\overline{\mathbb{R}}$ este total ordonată, iar elementele $+\infty$ şi $-\infty$ – numite (acum) ***numere reale infinite*** (punctele de la infinit ale dreptei reale) sunt ***cel mai mare*** şi respectiv ***cel mai mic*** dintre elementele sale. Într-un asemenea context, elementele mulţimii $\mathbb{R} \subset \overline{\mathbb{R}}$ se numesc ***numere reale finite***.

Cum, cu privire la aspectele de ordin algebric ale mulţimilor numerice $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ şi $\mathbb{R}$, ar putea fi făcute şi consideraţii din domeniul laticelor sau al algebrelor Boole, iată aici câteva elemente de referinţă.

Latici şi algebre Boole

Definiţia 2.19 *O mulţime nevidă L, împreună cu două operaţii interne "$\vee$" $: L \times L \to L$ şi "$\wedge$" $: L \times L \to L$, este numită* ***latice*** *dacă ambele legi, "$\vee$" şi "$\wedge$", sunt asociative, comutative, idempotente şi absorbante, adică:*

(L_1) (a) $x \vee (y \vee z) = (x \vee y) \vee z$, $\forall\, x, y, z \in L$,
(b) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$, $\forall\, x, y, z \in L$,

(L_2) (a) $x \vee y = y \vee x$, $\forall\, x, y \in L$,
(b) $x \wedge y = y \wedge x$, $\forall\, x, y \in L$,

(L_3) (a) $x \vee x = x$, $\forall\, x \in L$,
(b) $x \wedge x = x$, $\forall\, x \in L$,

(L_4) (a) $x \vee (x \wedge y) = x$, $\forall\, x, y \in L$,
(b) $x \wedge (x \vee y) = x$, $\forall\, x, y \in L$.

Caracterul algebric al Definiţiei 2.19 este evident. Pe baza acestei definiţii, se poate introduce o relaţie de ordine parţială pe laticea L (prin "$x \leq y$", dacă şi numai dacă "$x = x \wedge y$"), în raport cu care $(L, \leq)$ reprezintă o structură parţial ordonată.

Reciproc, dacă $(A, \leq)$ este o mulţime (nevidă) parţial ordonată, atunci se pot defini operaţiile $\vee$ şi $\wedge$ (pe A), prin:

$$x \vee y = \sup\{x, y\} \text{ (în sensul dat în cursul 1) şi respectiv}$$

$$x \wedge y = \inf\{x, y\} \text{ (vezi cursul 1)}, \forall\, x, y \in A,$$

observându-se faptul că, în felul acesta, $(A, \vee, \wedge)$ constituie o latice, în sensul Definiţiei 2.19. În virtutea unei astfel de observaţii, noţiunea de latice se poate baza şi pe următoarea definiţie, echivalentă cu cea de mai sus:

Definiţia 2.20 *O mulţime parţial ordonată $(L, \leqslant)$ este numită latice dacă şi numai dacă, pentru orice x şi y din L, atât $\sup\{x, y\}$, cât şi $\inf\{x, y\}$, există şi sunt (ambele) din L.*

Un exemplu elementar de latice îl constituie mulţimea numerelor naturale, înzestrată cu relaţia de ordine uzuală, prin intermediul căreia se pot defini operaţiile: $n_1 \wedge n_2 = \min\{n_1, n_2\}$, $n_1 \vee n_2 = \max\{n_1, n_2\}$, $\forall\, n_1, n_2 \in \mathbb{N}$. Este satisfăcută, cu evidenţă, Definiţia 2.19.

Definiţia 2.21 *În general, o* ***latice*** *$(L, \vee, \wedge)$ este* ***denumită****:*

i) ***distributivă***, când oricare dintre operaţiile "$\vee$" şi "$\wedge$" este distributivă faţă de cealaltă, adică

(a) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ sau
(b) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$, $\forall\, x, y, z \in L$;

ii) ***modulară***, când

(a) $(x \wedge y) \vee (y \wedge z) = y \wedge ((x \wedge y) \vee z)$, $\forall\, x, y, z \in L$;

ii) ***completă***, când, prin prisma Definiţiei 2.20, pentru orice submulţime $\tilde{L} \subseteq L$, există atât $\sup \tilde{L}$, cât şi $\inf \tilde{L}$, în L.

Definiţia 2.22 *Două* ***latici*** L_1 *şi* L_2 *se numesc* ***izomorfe*** *dacă există o bijecţie* $\phi : L_1 \to L_2$ *astfel încât:*

$$\phi(x \vee_{L_1} y) = \phi(x) \vee_{L_2} \phi(y), \forall\, x, y \in L_1 \text{ şi}$$

$$\phi(x \wedge_{L_1} y) = \phi(x) \wedge_{L_2} \phi(y), \forall\, x, y \in L_1.$$

Definiţia 2.23 *O submulţime* $L' \neq \varnothing$ *a unei latice* $(L, \vee, \wedge)$ *se numeşte* ***sublatice*** *(a lui* L*) dacă* $(L', \vee, \wedge)$ *este o latice în sine.*

Alături de noţiunea de latice, un alt concept de importanţă certă pe tărâmul informaticii, ca disciplină teoretică, este acela de ***algebră Boole***, definit după cum urmează.

Definiţia 2.24 *O mulţime nevidă* B*, înzestrată cu două operaţii binare, "*$\vee$*" şi "*$\wedge$*", o operaţie unară (de complementariere), notată cu "* $'$ *" şi două elemente "neutre", "0" şi "1", se numeşte* ***algebră Boole*** *dacă:*

(B_1*)* $(B, \vee, \wedge)$ *este o latice distributivă,*

(B_2*)* $x \wedge 0 = 0$ *şi* $x \vee 1 = 1$*,* $\forall\, x \in B$*,*

(B_3*)* $x \wedge x' = 0$ *şi* $x \vee x' = 1$*,* $\forall\, x \in B$*.*

Un exemplu clar de algebră Boole îl constituie mulţimea $\mathcal{P}(X)$, a tuturor submulţimilor unei mulţimi X, în raport cu operaţiile de reuniune şi de intersecţie, alături de care şi cea de complementariere uzuală (la mulţimi), având mulţimea vidă în rolul lui "0" şi mulţimea X în rolul lui "1".

Alte aspecte de ordin algebric (sau de altă natură) privitoare la $\mathbb{R}$ şi $\overline{\mathbb{R}}$ vor fi relevate în următoarele capitole. Deocamdată, de trebuinţă ulterioară, sunt de semnalat câteva inegalităţi numerice mai importante, între care aceea a lui Hölder şi aceea a lui Minkowski.

Inegalităţi cu elemente din $\mathbb{R}$

Propoziţia 2.10 ***(Inegalitatea lui Hölder, cu ponderi)*** *Fie* $n \in \mathbb{N}$*,* $\lambda_0, \lambda_1, \ldots \lambda_n$*,* $a_0, a_1, \ldots, a_n$*,* $b_0, b_1, \ldots, b_n \in \mathbb{R}_+ = \{x \in \mathbb{R} \mid x \geq 0\}$ *şi* $p, q \in \mathbb{R}_+^* = \mathbb{R}_+ \setminus \{0\}$*, astfel încât* $\dfrac{1}{p} + \dfrac{1}{q} = 1$*. Atunci:*

$$(*) \quad \sum_{i=0}^{n} \lambda_i a_i b_i \leq \left(\sum_{i=0}^{n} \lambda_i a_i^p\right)^{\frac{1}{p}} \cdot \left(\sum_{i=0}^{n} \lambda_i b_i^q\right)^{\frac{1}{q}}.$$

Demonstraţie: Se consideră mulţimea $M = \{n \in \mathbb{N}$, astfel încât are loc (*)$\} \subseteq \mathbb{N}$ şi se arată că M satisface condiţia (axioma) (P_3) (Peano) din Definiţia 2.14. Rezultă atunci că $M = N$, ceea ce înseamnă că $(*)$ are loc într-adevăr, pentru orice număr natural real n, cu datele din enunţ.

Satisfacerea axiomei (P_3) de către M reiese din faptul că $0 \in M$, în mod evident, iar dacă $n \in M$, atunci, pentru $s(n)$ (adică pentru $n+1$), avem:

$$\sum_{i=0}^{n+1} \lambda_i a_i b_i = \sum_{i=0}^{n} \lambda_i a_i b_i + \lambda_{n+1} a_{n+1} b_{n+1} \leq$$

$$\leq \left(\sum_{i=0}^{n} \lambda_i a_i^p\right)^{\frac{1}{p}} \cdot \left(\sum_{i=0}^{n} \lambda_i b_i^q\right)^{\frac{1}{q}} + \lambda_{n+1} a_{n+1} b_{n+1}$$

$$\leq \left(\sum_{i=0}^{n} \lambda_i a_i^p + \lambda_{n+1} a_{n+1}^p \right)^{\frac{1}{p}} \cdot \left(\sum_{i=0}^{n} \lambda_i b_i^q + \lambda_{n+1} b_{n+1}^p \right)^{\frac{1}{q}}.$$

Prima inegalitate are loc deoarece $n \in M$ (şi, ca atare, $(*)$ are loc pentru n), iar cea de-a doua este de fapt inegalitatea $(*)$ din cazul $n = 2$, cu ponderile 1 şi λ_{n+1} în rolurile lui λ_1 şi λ_2, cu $\left(\sum_{i=0}^{n} \lambda_i a_i^p \right)^{\frac{1}{p}}$ şi a_{n+1} în rolurile lui a_1 şi respectiv a_2, precum şi cu $\left(\sum_{i=0}^{n} \lambda_i b_i^q \right)^{\frac{1}{q}}$ şi b_{n+1} în rolurile lui b_1 şi respectiv b_2. Aşa încât, este suficient să ne convingem de faptul că este adevărată inegalitatea:

$$(\bullet) \quad \lambda_1 a_1 b_1 + \lambda_2 a_2 b_2 \leq (\lambda_1 a_1^p + \lambda_2 a_2^p)^{\frac{1}{p}} \cdot (\lambda_1 b_1^q + \lambda_2 b_2^q)^{\frac{1}{q}}.$$

Acest lucru decurge din faptul că, pentru funcţia $f : \mathbb{R}_+ \to \mathbb{R}$, definită prin $f(x) = (\lambda_1 a_1^p + \lambda_2 a_2^p)^{\frac{1}{p}} \cdot (\lambda_1 b_1^q + \lambda_2 x^q)^{\frac{1}{q}} - \lambda_1 a_1 b_1 - \lambda_2 a_2 x$, există punctul de minim global $x_0 = b_1 (a_2/a_1)^{\frac{p}{q}}$ (când $a_1 \neq 0$) şi, studiind variaţia lui f, găsim: $f(b_2) \geq f(x_0) = 0$. Când $a_1 = 0$, inegalitatea (de fapt, egalitatea) $(\bullet)$ este evidentă.

În fine, este de menţionat că, în $(*)$, egalitatea are loc dacă şi numai dacă n-uplele $(a_0^p, a_1^p, \ldots, a_n^p)$ şi $(b_0^p, b_1^p, \ldots, b_n^p)$ sunt proporţionale. ◀

Folosind un raţionament asemănător, se poate demonstra şi că este adevărată propoziţia ce urmează. În prealabil, precizăm că, atunci când $\lambda_1 = \lambda_2 = \ldots = \lambda_n \in \mathbb{R}_+^*$, relaţia $(*)$ reprezintă *inegalitatea lui Hölder fără ponderi.* De asemenea, specificăm că, pentru $p = q = 2$ şi $\lambda_1 = \lambda_2 = \ldots = \lambda_n \in \mathbb{R}_+^*$, inegalitatea $(*)$ capătă forma

$$(**) \quad \sum_{i=0}^{n} a_i b_i \leq \left(\sum_{i=0}^{n} a_i^2 \right)^{\frac{1}{2}} \cdot \left(\sum_{i=0}^{n} b_i^2 \right)^{\frac{1}{2}},$$

fiind cunoscută atunci sub denumirea de ***inegalitatea lui Cauchy-Buniakowski-Schwarz***. În $(**)$, egalitatea are loc, în concordanţă cu ce am precizat în legătura cu $(*)$, dacă şi numai dacă există $u, v \in \mathbb{R}$, cu $u^2 + v^2 \neq 0$, aşa încât $ua_i + vb_i = 0$, $\forall\, i \in \{0, 1, 2, ...n\}$.

Propoziţia 2.11 ***(Inegalitatea lui Minkowski, cu ponderi)*** *Pentru $p \in \mathbb{R}$, $p \geq 1$, $n \in \mathbb{N}$ şi $\lambda_0, \lambda_1, \ldots \lambda_n$, $a_0, a_1, \ldots, a_n$, $b_0, b_1, \ldots, b_n$ din $\mathbb{R}_+^*$, are loc inegalitatea*

$$(***) \quad \left(\sum_{i=0}^{n} \lambda_i (a_i + b_i)^p \right)^{\frac{1}{p}} \leq \left(\sum_{i=0}^{n} \lambda_i a_i^p \right)^{\frac{1}{p}} + \left(\sum_{i=0}^{n} \lambda_i b_i^p \right)^{\frac{1}{p}}$$

În cazul $0 < p < 1$, inegalitatea $(***)$ are loc cu sensul schimbat. În $(***)$, are loc egalitatea dacă şi numai dacă n-uplele $(a_0, a_1, \ldots, a_n)$ şi $(b_0, b_1, \ldots, b_n)$ sunt proporţionale.

Demonstraţie: Ca şi în situaţia inegalităţii lui Hölder, considerând mulţimea L a tuturor acelor $n \in \mathbb{N}$ pentru care, fie în cazul $p \geq 1$, fie în cazul $0 < p < 1$,are loc inegalitatea $(***)$, se vede că $0 \in L$ şi că dacă $n \in L$, atunci $n + 1 = s(n) \in L$. Acest din urmă lucru revine, ca şi în demonstrarea inegalităţii $(*)$, la a arăta că $(***)$ este adevărată, de fapt, pentru $n = 2$, ceea ce se poate dovedi pe seama studiului variaţiei unei funcţii potrivit alese în context. Astfel, prin (P_3), rezultă că $L = \mathbb{N}$, ceea ce înseamnă că $(***)$ are loc pentru orice $n \in \mathbb{N}$, cu datele şi în situaţiile din enunţ. ◀

Propoziţia 2.12 ***(Inegalitatea lui Carleman)*** *Pentru orice $n \in \mathbb{N}^*$ şi $a_1, a_2, \ldots, a_n \in \mathbb{R}_+$ are loc inegalitatea*

$$(!) \quad \sum_{k=1}^{n} (a_1 a_2 \ldots a_k)^{\frac{1}{k}} \leq e \sum_{k=1}^{n} a_k,$$

egalitatea având loc doar când $a_1 = a_2 = \ldots = a_n = 0$.

Demonstraţie: Considerând n arbitrar din $\mathbb{N}^*$, $a_1, a_2, \ldots, a_n$ din $\mathbb{R}_+$ şi $b_1, b_2, \ldots, b_n \in \mathbb{R}_+^*$, pe baza inegalităţii mediilor, adică a inegalităţii

$$(x_1 x_2 \ldots x_n)^{\frac{1}{n}} \leq \frac{x_1 + x_2 + \ldots + x_n}{n}$$

(adevărată pentru orice $n \in \mathbb{N}^*$ şi $x_1, x_2, \ldots, x_n \in \mathbb{R}_+$), avem

$$(b_1 a_1 b_2 a_2 \ldots b_k a_k)^{\frac{1}{k}} \leq \frac{b_1 a_1 + b_2 a_2 + \ldots + b_k a_k}{k}, \ \forall\, k \in \mathbb{N}^*$$

şi, prin aceasta, putem scrie:

$$(!!) \sum_{k=1}^{n} (a_1 a_2 \ldots a_k)^{\frac{1}{k}} = \sum_{k=1}^{n} \left(\frac{b_1 a_1 b_2 a_2 \ldots b_k a_k}{b_1 b_2 \ldots b_k} \right)^{\frac{1}{k}} = \sum_{k=1}^{n} (b_1 b_2 \ldots b_k)^{-\frac{1}{k}} (b_1 a_1 b_2 a_2 \ldots b_k a_k)^{\frac{1}{k}} \leq$$

$$\leq \sum_{k=1}^{n} \left((b_1 b_2 \ldots b_k)^{-\frac{1}{k}} \cdot \frac{1}{k} \sum_{l=1}^{k} b_l a_l \right) = \sum_{l=1}^{n} b_l a_l \cdot \sum_{k=l}^{n} \frac{(b_1 b_2 \ldots b_k)^{-\frac{1}{k}}}{k}.$$

Luând $b_n = \dfrac{(n+1)^n}{n^{n-1}}$, $\forall\, n \in \mathbb{N}^*$, atunci $b_1 b_2 \ldots b_k = (k+1)^k$, $\forall\, k \in \mathbb{N}^*$ şi

$$\sum_{k=l}^{n} \frac{(b_1 b_2 \ldots b_k)^{-\frac{1}{k}}}{k} = \sum_{k=l}^{n} \frac{1}{k(k+1)} = \sum_{k=l}^{n} \left(\frac{1}{k} - \frac{1}{k+1} \right) = \frac{1}{l} - \frac{1}{n+1} < \frac{1}{l}, \ \forall\, n \in \mathbb{N}^*.$$

Astfel, din (!!) obţinem

$$\sum_{k=1}^{n} (a_1 a_2 \ldots a_k)^{\frac{1}{k}} \leq \sum_{l=1}^{n} \frac{b_l}{l} a_l = \sum_{l=1}^{n} \left(1 + \frac{1}{l}\right)^l a_l \leq e \sum_{k=1}^{n} a_k,$$

adică tocmai (!).

Întrucât $\left(1 + \dfrac{1}{l}\right)^l < e, \forall\, l \in \mathbb{N}^*$, relaţia (!) devine egalitate doar când $a_1 = a_2 = \ldots = a_n = 0$. ◀

Bibliografie selectivă

1. D. Buşneag, D. Piciu - *Lecţii de algebră*, Ed. Universitaria, Craiova, 2002.
2. Rodica Luca-Tudorache - *Analiză matematică*, Editura Tehnopress, Iaşi, 2005.
3. Mihai Onucu Drâmbe - *Inegalităţi. Idei şi metode.*, Ed. GIL, Zalău, 2003.
4. I. D. Ion, R. Nicolae - *Algebră*, E. D. P., Bucureşti, 1982.
5. S. Burris, H. P. Sankappanavar - *A Course in Universal Algebra*, The Millenium Edition, 2000.
6. F. L. Ţiplea - *Introducere în teoria mulţimilor*, Ed. Univ. "Al. I. Cuza", Iaşi, 1998.