

Cursul 2

Structuri algebrice de bază.

Mulțimi fundamentale de numere: \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} și $\overline{\mathbb{R}}$.

Operații cu ordinali și cardinali.

Inegalități numerice importante.

Inevitabil, o prezentare riguroasă a mulțimilor numerice \mathbb{N} , \mathbb{Z} , \mathbb{Q} și \mathbb{R} invocă expunerea prealabilă a unor noțiuni de bază (precum cele de operație algebrică, monoid, grup, inel, corp și 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 și axiomatic, ne vom ocupa de mulțimile numerice vizate. Cum unele dintre acestea pot fi, prin înzestrarea cu operații algebrice specifice, structurate ca o latice sau o algebră Boole, vom introduce aici și astfel de noțiuni. În final, menționăm câteva inegalități numerice (Hölder, Cauchy, Minkowski, Carleman), în \mathbb{R} , cu vădită importanță în contextul prezentelor note de curs.

Operații algebrice. Proprietăți. Monoizi. Morfisme.

Fie M o mulțime nevidă.

Definiția 2.1 Numim **operație algebrică (internă)** sau **lege de compoziție (internă)** pe M o funcție $\varphi : M \times M \rightarrow M$. Pentru $x, y \in M$, elementul $\varphi(x, y) \in M$ se numește **compusul lui x cu y prin operația φ** .

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

Definiția 2.2 O operație algebrică pe M (notată, generic, cu “ \circ ”) se numește

- 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 și constituie respectivul element neutru al operației “ \circ ”.

Definiția 2.3 Un dublet (M, \circ) , unde M este o mulțime nevidă, iar “ \circ ” este o operație algebrică pe M , se numește **semigrup** dacă operația “ \circ ” este asociativă. În plus, dacă operația “ \circ ” are și element neutru, atunci (M, \circ) se numește **monoid**. Dacă “ \circ ” este și comutativă, **monoidul** (M, \circ) se numește **comutativ**.

Exemple:

- 1) Dacă $M \neq \emptyset$, atunci $(\mathcal{P}(M), \cap)$, $(\mathcal{P}(M), \cup)$ și $(\mathcal{P}(M), \Delta)$ sunt monoizi comutativi.
- 2) Dacă $A \neq \emptyset$, atunci $(Hom(A), \circ)$, unde $Hom(A) = \{f : A \rightarrow A\}$, iar “ \circ ” semnifică operația uzuală de compunere a funcțiilor, este un monoid necomutativ.

Definiția 2.4 Fie (M, \circ) și (M', \perp) doi monoizi. O funcție $f : M \rightarrow M'$ se numește **morfism de monoizi** dacă $f(e) = e'$ (unde e și e' sunt elementele neutre, din M și respectiv M' , ale operațiilor “ \circ ” și, corespunzător, “ \perp ”) și

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

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

Definiția 2.5 Fie (M, \circ) un monoid. Un element $x \in M$ se numește **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 , față de “ \circ ”).

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

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

Mulțimea tuturor elementelor simetrizabile ale unui monoid (M, \circ) constituie ansamblul unităților lui M și se notează cu $U(M)$. În cazul în care A este o mulțime nevidă, avem: $U((\mathcal{P}(A), \cap)) = \{A\}$, $U((\mathcal{P}(A), \cup)) = \{\emptyset\}$, $U((\mathcal{P}(A), \Delta)) = \mathcal{P}(A)$, $U((\text{Izo}(A), \circ)) = \text{Izo}(A)$, unde $\text{Izo}(A)$ este mulțimea bijecțiilor de la A la A .

Grupuri. Inele. Corpuri.

Definiția 2.6 Numim **grup** un monoid (G, \circ) pentru care $U(G) = G$. Un grup (G, \circ) se numește **abelian (comutativ)** dacă operația “ \circ ” este comutativă.

Exemple:

- 1) $A \neq \emptyset \Rightarrow (\mathcal{P}(A), \Delta)$ este grup comutativ;
- 2) Dacă (M, \circ) este monoid, atunci $(U(M), \circ)$ este grup.

Definiția 2.7 O funcție $f : G \rightarrow G'$ se numește **morfism de grupuri** (de la grupul (G, \circ) la grupul (G', \star)) dacă satisface relația:

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

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

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

$$\begin{array}{ccc} M & \xrightarrow{i_M} & G(M) \\ f \downarrow & f' \swarrow & \\ G & & \end{array}$$

este comutativă).

Demonstrație: Pe mulțimea $M \times M$ se consideră relația “ \sim ”, definită prin: $(x, y) \sim (x', y') \Leftrightarrow x \cdot y' = y \cdot x'$. Se constată că “ \sim ” este o relație de echivalență pe $M \times M$, fiind reflexivă, simetrică și tranzitivă. Considerăm $G(M) = M \times M / \sim$ (mulțimea claselor de echivalență din $M \times M$, în raport cu “ \sim ”). Definim operația “ \circ ”: $G(M) \rightarrow G(M)$ prin

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

unde $[(x, y)]_{\sim}$ este notația pentru clasa de echivalență cu reprezentantul $(x, y) \in M \times M$. Se vede că operația “ \circ ” este bine definită pe $G(M)$, nedepinzând de reprezentanții claselor de echivalență 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 și comutativ.

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

$$i_M(x) \circ i_M(y) = [(x, e)]_{\sim} \circ [(y, e)]_{\sim} = [(x \cdot y, e)]_{\sim} = i_M(x \cdot y), \quad \forall x, y \in M.$$

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 și injectiv. Așadar i_M este un monomorfism de monoizi. Astfel, perechea $(G(M), i_M)$ verifică proprietatea din enunțul teoremei.

În continuare, dacă (G, \star) este un grup abelian oarecare și $f : M \rightarrow G$ este un morfism de monoizi, atunci, pentru $[(x, y)]_{\sim} \in G(M)$, definim $f' : G(M) \rightarrow G$ prin $f'([(x, y)]_{\sim}) = f(x) \star (f(y))^{-1}$. Observăm că, dacă $[(x, y)]_{\sim} = [(x', y')]_{\sim}$, atunci $x \cdot y' = x' \cdot y$ și 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:

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

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 privința unicității lui f' , presupunând că ar mai exista un morfism $f'' : G(M) \rightarrow G$ așa 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 consecință am obține:

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

Deci $f'' \equiv f'$. ◀

Definiția 2.8 Un triplet $(A, +, \cdot)$, unde A este o mulțime nevidă, iar “ $+$ ” și “ \cdot ” sunt operații algebrice pe A , se numește **inel** dacă:

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

ii) (A, \cdot) este semigrup;

iii) Operația “ \cdot ” este distributivă față de “ $+$ ”, adică

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

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

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

Prin convenție, se notează: $A^* = A \setminus \{0\}$ (0 fiind elementul neutru în raport cu “ $+$ ”). **Mulțimea unităților unui inel unitar** A , notată cu $U(A)$, este următoarea $\{a \in A \mid \exists b \in A \text{ așa încât } a \cdot b = b \cdot a = 1\}$ (1 fiind notația pentru elementul neutru în raport cu “ \cdot ”).

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

Definiția 2.10 Numim **domeniu de integritate (inel integru)** un inel comutativ, nenul și fără divizori ai lui zero, diferiți de zero.

Definiția 2.11 Fiind date două inele $(A, +, \cdot)$ și (B, \circ, \star) , o funcție $f : A \rightarrow B$ se numește **morfism (/monomorfism/epimorfism/izomorfism) de inele**, dacă:

$$i) f(a + b) = f(a) \circ f(b), \forall a, b \in A \text{ și}$$

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

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

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

Dacă un sistem multiplicativ S nu are divizori ai lui zero, atunci se poate vorbi despre inelul “fracțiilor” relative la S , notat cu A_S și introdus după cum urmează. Pe $A \times S$ se consideră relația binară “ \sim ”, definită prin $(a, s) \sim (a', s') \leftrightarrow a \cdot s' = a' \cdot s$. Se vede lesne că “ \sim ” este o relație de echivalență pe $A \times S$. Clasa de echivalență corespunzătoare lui $(a, s) \in A \times S$, se notează, simbolic, cu $\frac{a}{s}$ și se numește “fracție”. Mulțimea factor $A \times S / \sim$ se notează cu A_S . Deci: $A_S = \{\frac{a}{s} \mid a \in A, 0 \neq s \in S\}$ (S nu are divizori ai lui 0). Cum $\frac{a}{s} = [(a, s)]_{\sim}$, $\forall a \in A$ și $\forall s \in S \setminus \{0\}$, se pot defini operațiile de adunare și de înmulțire a fracțiilor prin:

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

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

În plus, $i_S(s) \in U(A_S), \forall s \in S \setminus \{0\}$.

Definiția 2.13 Un inel unitar $(K, +, \cdot)$ se numește **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 mulțimea tuturor non-divizorilor lui zero (adică A^*), este un corp numit **corpul de fracții** (cături) al lui A .

Mulțimea \mathbb{N} a numerelor naturale.

Axiomatic, bazându-ne pe considerațiile lui G. Peano, s-ar putea introduce mulțimea numerelor naturale atâta timp cât admitem existența a cel puțin unui așa-numit triplet Peano.

Definiția 2.14 *Entitatea matematică $(N, 0, s)$, în care N este o mulțime nevidă, $0 \in N$ și $s : N \rightarrow N$ este o funcție astfel încât au loc axiomele*

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

(P_2) s este injectivă,

(P_3) dacă $M \subseteq N$, $0 \in M$ și $\forall n \in M \Rightarrow s(n) \in M$, atunci $M = N$,
se numește **triplet Peano**.

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

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

Demonstrație: Fie $M = \{0\} \cup s(N)$. Așadar, $M \subseteq N$ și, cu evidență, M verifică (P_3) (numită axioma inducției matematice). Astfel $0 \in M$ și $\forall n \in M, s(n) \in M$. În consecință $M = N$. ◀

Teorema 2.2 *Orice triplet Peano este unic până la o bijecție. Mai exact, dacă $(N, 0, s)$ este un triplet Peano, iar $(N', 0', s')$ este un alt triplet, nu numai că Peano, format dintr-o mulțime nevidă N' , un element $0' \in N'$ și o funcție $s' : N' \rightarrow N'$, atunci există o funcție unică $f : N \rightarrow N'$ așa încât $f(0) = 0'$ și $f \circ s = s' \circ f$, 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 bijecție.

Demonstrație: În prima situație, pentru existența lui f , considerăm toate relațiile binare $R \subseteq N \times N'$ pentru care avem satisfăcute următoarele condiții:

(I_1) $(0, 0') \in R$ și

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

Mulțimea acestor relații nu este vidă, deoarece cel puțin $N \times N'$ este o astfel de relație (care verifică ambele impuneri (I_1) și (I_2)). Fie $R_0 = \bigcap R$ (intersecția tuturor relațiilor ce satisfac (I_1) și (I_2)). Se arată că R_0 este o relație funcțională ce definește pe f (funcția cu graficul R_0). Pentru o asemenea funcție, ținând seama de (I_1) , avem $(0, 0') \in R_0$, adică $f(0) = 0'$. Pe de altă parte, în virtutea condiției (I_2) , dacă n este arbitrar din N și $n' = f(n) \in N'$, 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 relație funcțională, considerăm $M = \{n \in N \mid \exists n' \in N' \text{ așa încât } (n, n') \in R_0\} \subseteq N$ și arătăm că M satisface (P_3) (din Definiția 2.14). În acest sens, pe baza ipotezei (I_1) , avem $(0, 0') \in R_0$ și deci $0 \in M$. Folosind (I_2) , $\forall n \in M$, cu $n' \in N'$ așa

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 $M = N$. Așadar, deocamdată, R_0 este o relație binară între întreaga mulțime N și mulțimea N' . În continuare, considerând mulțimea $\tilde{M} = \{n \in N \mid n', n'' \in N \text{ și } (n, n'), (n, n'') \in R_0 \Rightarrow n' = n''\} \subseteq N$, arătăm că $\tilde{M} = N$, ceea ce ar însemna că R_0 este o relație funcțională de la N la N' . În acest scop, vedem mai întâi 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 relația $R_1 = R_0 \setminus \{(0, n')\} \subset N \times N'$. 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 $(n, m) \in R_0$ și $(n, m) \neq (0, n')$. Prin (I_2) , deducem că $(s(n), s'(m)) \in R_0$ și, 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) și (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 consecință, contradicția ne asigură că $n' = 0'$.

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

Mai departe, fie $n \in \tilde{M}$ și $n' \in N'$ așa 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 relația $R_2 = R_0 \setminus \{(s(n), n'')\}$, vedem că R_2 satisface (I_1) și (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 $(p, p') \in R_0$ și $(p, p') \neq (s(n), n'')$. 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 $p = n$, și $s'(p') = n''$. Atunci, cum $(n, n') \in R_0$ și $(n, p') = (p, p') \in R_0$, 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) și (I_2) și ar trebui ca $R_0 \subseteq R_2$, contrazicând realitatea considerată ($R_2 \subsetneq R_0$). În consecință, $(s(n), n'') \in R_0$ implică $n'' = s'(n')$, așa că, dacă $r, t \in N'$ și $(s(r), r), (s(t), t) \in R_0$, atunci $r = t = s'(n')$. Așadar $\tilde{M} = N$, adică R_0 este de tip funcțional.

Pentru a arăta că f este unică, admitem prin absurd că mai există o funcție $f' : N \rightarrow N'$ așa încât $f'(0) = 0'$ și $s'(f'(n)) = f'(s(n))$, $\forall n \in N$. Considerăm mulțimea $\hat{M} = \{n \in N \mid f(n) = f'(n)\} \subseteq N$. 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 $s(n) \in \hat{M}$. Așadar, 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 bijecție. Mai întâi, fie $P = \{n \in N \mid \text{dacă } m \in N \text{ și } f(m) = f(n), \text{ atunci } m = n\} \subseteq N$. Sesizăm că $0 \in P$, întrucât, dacă $m \in N$ este așa încât $f(m) = f(0)$, atunci $m = 0$. Altfel, dacă $m \neq 0$, atunci, în conformitate cu Propoziția 2.1, există $n \in N$ așa încât $m = s(n)$ și $f(s(n)) = f(0) = 0'$, adică $s'(f(n)) = 0'$, ceea ce nu se poate, deoarece, prin ipoteză, $(N', 0', s')$ este un triplet Peano și 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 $m \in N$, așa 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 $m \neq 0$ și atunci, aplicând Propoziția 2.1, există $u \in N$ așa 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, $P = N$ și f este injectivă.

Pentru a arăta surjectivitatea lui f , considerăm mulțimea $Q = \{n' \in N' \mid \exists n \in N \text{ așa încât } n' = f(n)\}$. Cum $f(0) = 0'$, deducem că $0' \in Q$. În plus, dacă $n' \in Q$, atunci $\exists n \in N$, așa 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. Așadar, f este și surjectivă. ◀

Pe baza Teoremei 2.2, putem considera că, în definitiv, esențial este un reprezentant al tuturor tripletelor Peano existente. Mulțimea dintr-un asemenea triplet se numește, prin convenție, **mulțime a numerelor naturale** și se notează cu \mathbb{N} . Elementul 0 se va numi **prim element** al lui \mathbb{N} , iar funcția s - **funcție de succesiune**. Drept urmare, elementul $s(n)$ se va numi **succesorul** lui $n \in \mathbb{N}$.

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

Teorema 2.3 (Axiomele adunării numerelor naturale) *Există o unică operație algebrică pe \mathbb{N} , notată cu “+” și denumită adunare a numerelor naturale, astfel încât să avem:*

$$(A_1) \quad 0 + m = m, \forall m \in \mathbb{N} \text{ și}$$

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

Demonstrație: Fie $m \in \mathbb{N}$, arbitrar fixat. Considerăm tripletul Peano (\mathbb{N}, m, s) . Potrivit Teoremei 2.2, există o funcție bijectivă unică $f_m : \mathbb{N} \rightarrow \mathbb{N}$, astfel ca $f_m(0) = m$ și $s(f_m(n)) = f_m(s(n))$, $\forall n \in \mathbb{N}$. Pentru $n \in \mathbb{N}$, arbitrar fixat, definim operația “+” : $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ prin $n + m = f_m(n)$. Atunci, $0 + m = f_m(0) = m$ și $s(n) + m = f_m(s(n)) = s(f_m(n)) = s(n + m)$. Deci au loc (A_1) și (A_2) . ◀

Propoziția 2.2 *Au loc relațiile:*

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

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

Demonstrație: Pentru m fixat arbitrar în \mathbb{N} , considerăm mulțimile $L = \{m \in \mathbb{N} \mid m + 0 = m\} \subseteq \mathbb{N}$ și $S = \{n \in \mathbb{N} \mid n + s(m) = s(n + m)\} \subseteq \mathbb{N}$. Arătăm că L și S se supun axiomei (P_3) din definiția unui triplet Peano. În acest fel, obținem faptul că $L = \mathbb{N}$ și $S = \mathbb{N}$, ceea ce asigură valabilitatea relațiilor a) și b) din enunțul acestei propoziții.

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 $m + 0 = m$ și $s(m) + 0 = s(m + 0) = s(m)$, adică: $s(m) \in L$. Așadar, $L = \mathbb{N}$ (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 $n + s(m) = s(n + m)$ și, mai departe, $s(n) + s(m) = s(n + s(m))$. Deci $s(n) \in S$, adică $S = \mathbb{N}$. Astfel, are loc b). ◀

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

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

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

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

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

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

Pentru final, privitor la “simplificare”, fie $m, n \in \mathbb{N}$ (fixate arbitrar) și $H = \{p \in \mathbb{N} \mid n + p = m + p \Rightarrow m = n\} \subseteq \mathbb{N}$. Vedem că $0 \in H$, întrucât $n + 0 = m + 0 \Rightarrow n = m$. De asemenea, deducem că dacă $p \in H$, atunci și $s(p) \in H$, 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 $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, unde, tot convențional, am adoptat notațiile $2 = s(1), 3 = s(2)$ etc.

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

Teorema 2.4 (*Axiomele înmulțirii numerelor naturale*) Există o unică operație algebrică pe \mathbb{N} , notată cu “ \cdot ” și denumită **înmulțire a numerelor naturale**, astfel încât au loc relațiile:

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

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

Demonstrație: Fie $m \in \mathbb{N}$, fixat arbitrar, și tripletul Peano $(\mathbb{N}, 0, f_m)$, unde $f_m : \mathbb{N} \rightarrow \mathbb{N}$ este definită prin $f_m(n) = n + m$, $\forall n \in \mathbb{N}$. Atunci, potrivit Teoremei 2.2, există o funcție unică, $g_m : \mathbb{N} \rightarrow \mathbb{N}$, așa încât $g_m(0) = 0$ și $f_m \circ g_m = g_m \circ s$. Definim atunci operația de înmulțire “ \cdot ” : $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, prin: $m \cdot n = g_m(n)$, $\forall n \in \mathbb{N}$. Astfel, avem: $m \cdot 0 = g_m(0) = 0$ (adică I_1) și $m \cdot s(n) = g_m(s(n)) = (g_m \circ s)(n) = (f_m \circ g_m)(n) = f_m(g_m(n)) = f_m(m \cdot n) = m \cdot n + m$ (adică I_2) ◀

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

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

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

Propoziția 2.4 *Înmulțirea numerelor naturale este distributivă, la stânga, față de adunarea numerelor naturale.*

Demonstrație: 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 $p \in M$ și $m, n \in \mathbb{N}$, 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 Definiția 2.14, deducem că $M = \mathbb{N}$. Altfel spus, distributivitatea la stânga a înmulțirii față de adunare, are loc peste tot pe \mathbb{N} . ◀

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

Demonstrație: Asociativitatea înmulțirii pe \mathbb{N} se arată considerând mulțimea $P = \{p \in \mathbb{N} \mid (m \cdot n) \cdot p = m \cdot (n \cdot p), \forall m, n \in \mathbb{N}\} \subseteq \mathbb{N}$. Cu evidență, $0 \in P$, 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 și $s(p) \in P$, 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 Definiția 2.14 și, în consecință, $P = \mathbb{N}$.

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 înmulțirii numerelor naturale.

Pentru a vedea că înmulțirea este comutativă, luăm în considerare mulțimea $Q = \{n \in \mathbb{N} \mid n \cdot m = m \cdot n, \forall m \in \mathbb{N}\}$. 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 $s(n) \in Q$ și, prin (P_3) , $Q = \mathbb{N}$.

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

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

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

Definiția 2.15 Pentru $m, n \in \mathbb{N}$, scriem $m \leq n$ și 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 așa încât $m \leq n$ și $m \neq n$, atunci scriem $m < n$ și spunem că m este **strict mai mic decât** n . În acest caz, există $p \in \mathbb{N}^* = s(\mathbb{N})$, așa încât $m + p = n$.

Propoziția 2.5 Dacă $m, n \in \mathbb{N}$ și $m < n$, atunci $s(m) \leq n$.

Demonstrație: 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 ușor, vedea că $n < s(n), \forall n \in \mathbb{N}$.

Teorema 2.6 Dubletul (\mathbb{N}, \leq) este o mulțime total și bine ordonată, adică relația “ \leq ” este una de totală ordine pe \mathbb{N} și orice submulțime nevidă $A \subseteq \mathbb{N}$ are un cel mai mic element.

Demonstrație: Pentru început, deoarece $n + 0 = n, \forall n \in \mathbb{N}$, vedem că $n \leq n, \forall n \in \mathbb{N}$. Deci relația “ \leq ” este reflexivă pe \mathbb{N} . Luând apoi $m, n \in \mathbb{N}$ așa încât $m \leq n$ și $n \leq m$, vor exista p și q din \mathbb{N} așa încât $m + p = n$ și $n + q = m$. 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, relația “ \leq ” este antisimetrică. În fine, dacă $m, n, p \in \mathbb{N}$ sunt așa încât $m \leq n$ și $n \leq p$, atunci există r și $s \in \mathbb{N}$ ca să avem $m + r = n$ și $n + s = p$. Deducem că $m + (r + s) = p$, adică $m \leq p$. Așadar, relația “ \leq ” este și tranzitivă, fiind de fapt o relație de parțială ordine pe \mathbb{N} .

În scopul demonstrării faptului ca “ \leq ” este o relație de ordine totală (numită **ordinea naturală**) pe \mathbb{N} , considerăm $m \in \mathbb{N}$, arbitrar fixat și, față de acesta, mulțimea $P_m = \{n \in \mathbb{N} \mid n \leq m \text{ sau } m \leq n\} \subseteq \mathbb{N}$. Observăm că $0 \in P_m$, deoarece $0 \leq m$, cu evidentă. 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 Propoziția 2.5, avem $s(n) \leq m$ și deci, iarăși, $s(n) \in P_m$. Dacă $m < n$, cum $n < s(n)$ și “ \leq ” este o relație tranzitivă, avem $m < s(n)$ și deci $s(n) \in P_m$. Prin (P_3) , rezultă așadar 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 mulțime nevidă $A \subseteq \mathbb{N}$ și $Q = \{n \in \mathbb{N} \mid n \leq a, \forall a \in A\}$. 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 consecință, 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 $r \in Q$ așa încât $s(r) \notin Q$. Arătăm că $r \in A$ și că r este cel mai mic element al lui A . Dacă r nu ar aparține lui A , atunci, fiind din Q , am avea $r < a, \forall a \in A$. De aici ar reieși că $s(r) \leq a, \forall a \in A$. Deci $s(r) \in Q$ (absurd). Așadar, $r \in A$ și, cum $r \in Q$, avem $r \leq a, \forall a \in A$. Deci r este cel mai mic element al lui A . ◀

Observații

- 1) În virtutea Definiției 1.20-b, se poate vedea că \mathbb{N} este un ordinal infinit și anume chiar cel mai mic, adică ω .
- 2) $\forall n \in \mathbb{N}$, mulțimea $\{0, 1, \dots, n\}$ este, de asemenea, un ordinal și anume un ordinal finit.
- 3) Un ordinal definește un număr natural, dacă și numai dacă orice submulțime nevidă a sa are cel mai mare element.
- 4) Intuitiv, un ordinal desemnează poziții într-un șir bine ordonat de entități și, de aceea, prin analogie cu elementele lui \mathbb{N} i se mai spune **număr ordinal**.

Principiul inducției transfinite

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

$$\forall \beta (\beta < \alpha \implies P(\beta)) \implies P(\alpha)$$

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 și $P(\alpha)$ are loc.

Atunci P este satisfăcută de toți ordinalii.

Principiul recursiei transfinite

Fie γ un ordinal, adică un element al mulțimii Ord , A o mulțime oarecare și \mathcal{F} mulțimea tuturor funcțiilor (inclusiv cea vidă) cu valori în A și definite pe $\{\beta \in Ord \mid \beta < \gamma\}$. De asemenea, fie $H : \mathcal{F} \rightarrow A$. Atunci există o funcție unică G , cu domeniul $\{\alpha \in Ord \mid \alpha < \gamma\}$, astfel încât, pentru orice $\alpha < \gamma$, are loc relația:

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

Aritmetica ordinalilor

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

Propoziția 2.6 1° Există "+" : $Ord \times Ord \rightarrow Ord$, astfel încât:

- (a) $\alpha + 0 = \alpha$, $\forall \alpha \in Ord$,
- (b) $\alpha + (\beta + 1) = (\alpha + \beta) + 1$, $\forall \alpha, \beta \in Ord$,
- (c) $\alpha + \beta = \sup \{\alpha + \gamma \mid \gamma < \beta\}$, $\forall \alpha, \beta \in Ord$, $\beta = \text{ordinal limită}$, $\beta \neq 0$.

\mathcal{L} Există " \cdot ": $Ord \times Ord \rightarrow Ord$, 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) $\alpha \cdot \beta = \sup \{\alpha \cdot \gamma \mid \gamma < \beta\}, \forall \alpha, \beta \in Ord, \beta = \text{ordinal limită}, \beta \neq 0$.

\mathcal{L} Există " $\hat{\cdot}$ ": $Ord \times Ord \rightarrow Ord$, 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) $\alpha \hat{\beta} = \sup \{\alpha \hat{\gamma} \mid \gamma < \beta\}, \forall \alpha, \beta \in Ord, \beta = \text{ordinal limită}, \beta \neq 0$.

Se poate vedea că adunarea ordinalilor și înmulțirea ordinalilor sunt asociative, dar nu și comutative. De asemenea, înmulțirea ordinalilor se dovedește a fi distributivă față de adunare.

Observații

- 1) O mulțime A care este echipotentă cu o mulțime de numere naturale de forma $\{1, 2, \dots, n\}$ ($n \in \mathbb{N}^*$) se numește **mulțime finită** și are cardinalul egal cu n .
- 2) O mulțime care nu este finită se numește **mulțime infinită**.
- 3) Cardinalul unei mulțimi finite se numește **cardinal finit**, iar cardinalul unei mulțimi infinite se numește **cardinal transfinit**.
- 4) O mulțime echipotentă cu \mathbb{N} se numește **mulțime numărabilă**, cardinalul său fiind notat cu \aleph_0 (alef zero).
- 5) O mulțime care este finită sau numărabilă se numește **cel mult numărabilă**.
1. Se poate arăta că orice mulțime infinită A conține o submulțime numărabilă, ceea ce, formulat altfel, înseamnă că, pentru A , are loc relația:

$$\aleph_0 \leqslant \text{card}(A).$$

Operații aritmetice cu numere cardinale

Pentru $\alpha = \text{card}(A)$ și $\beta = \text{card}(B)$, se pot defini următoarele operații (cu numere cardinale):

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

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

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

Observații

- 1) Adunarea, înmulțirea și exponențierea numerelor cardinale, restricționate la cardinali finiți, coincid cu operațiile corespunzătoare pe \mathbb{N} .
- 2) Pentru orice cardinal α , avem $\alpha + 1 = \alpha$ dacă și numai dacă α este un cardinal infinit.

Mulțimile \mathbb{Z} și \mathbb{Q}

Definiția 2.16 Fie monoidul $(\mathbb{N}, +)$. Prin tehnica din Teorema 2.1 (Malțev), mulțimea ce corespunde grupului aditiv $(G(\mathbb{N}), +)$ se notează cu \mathbb{Z} și poartă denumirea de **mulțime a numerelor întregi**. Corespunzător, $(\mathbb{Z}, +)$ este grupul aditiv, abelian, al numerelor întregi.

Potrivit respectivei Teoreme 2.1, există monomorfismul de monoizi $i_{\mathbb{N}} : \mathbb{N} \rightarrow \mathbb{Z}$, 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 $-p$ ($p \in \mathbb{N}$). Ținând cont de acestea, putem scrie: $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N}^*)$, cu $(-\mathbb{N}^*) = \{-n \mid n \in \mathbb{N}^*\}$. Deci: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.

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

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

Propoziția 2.7 Dubletul (\mathbb{Z}, \cdot) este un monoid (multiplicativ) comutativ, în care operația “ \cdot ” este distributivă față de “ $+$ ” și, dacă $\alpha, \beta \in \mathbb{Z}$ sunt așa încât $\alpha \cdot \beta = 0$, atunci $\alpha = 0$ sau $\beta = 0$.

Demonstrație: Se arată simplu că înmulțirea numerelor întregi, în sensul relației de definiție (*), este asociativă, are elementul neutru $1 = [(1, 0)]$, este comutativă și distributivă față de adunarea numerelor întregi. Se vede apoi că, dacă $\alpha = [(x, y)], \beta = [(x', y')] \in \mathbb{Z}$ sunt astfel încât $\alpha \cdot \beta = 0$ și $\alpha \neq 0$, adică $[(x, y)] \cdot [(x', y')] = [(0, 0)]$ și $x \neq y$, 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.

Definiția 2.17 Pentru $x, y \in \mathbb{Z}$, spunem că $x \leq y$, dacă și numai dacă $y - x \in \mathbb{N}$.

Propoziția 2.8 Dubletul (\mathbb{Z}, \leq) este o mulțime total ordonată.

Demonstrație: Se arată lesne că “ \leq ” este o relație binară reflexivă, antisimetrică și tranzitivă pe \mathbb{Z} . Faptul că avem $\mathbb{Z} = (-\mathbb{N}^*) \cup \mathbb{N}$ ne spune că relația de ordine “ \leq ” este și totală pe \mathbb{Z} . ◀

În sensul definirii corpului total de fracții al unui inel integru, putem spune acum că, relativ la $(\mathbb{Z}, +, \cdot)$, corpul corespunzător este tocmai mulțimea \mathbb{Q} a **numerelor raționale**. În plus, prin existența monomorfismului $i_{\mathbb{Z}^*} : \mathbb{Z} \rightarrow \mathbb{Q}$, putem conta pe relația $\mathbb{Z} \subset \mathbb{Q}$. De asemenea, prin extensie, se poate vorbi de o relație totală de ordine pe \mathbb{Q} , definită prin:

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

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

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

Mulțimile \mathbb{R} și $\overline{\mathbb{R}}$

Faptul că mulțimea \mathbb{R} , cu caracteristicile deja menționate, există într-adevăr se poate arăta în câteva moduri, între care specificăm aici, metoda lui Dedekind, bazată pe așa-numita noțiune de tăietură, metoda lui Weierstrass, sprijinită pe noțiunea de fracție zecimală și metoda lui Cantor, axată pe noțiunea de șir fundamental (Cauchy) de numere raționale. Aceasta din urmă, neeludând principiul teoremei lui Mașev, va fi prezentată, preferențial, în secțiunea ce urmează celei de față și se referă la șiruri de elemente din inele și corpuri ordonate, precum \mathbb{Q} .

Deocamdată, din cele spuse până aici, se impune atenției următoarea definiție axiomatică a **mulțimii \mathbb{R} a numerelor reale**.

Definiția 2.18 \mathbb{R} este o mulțime cu cel puțin două elemente, înzestrată cu două operații algebrice – una numită adunare, notată cu “+” și cealaltă numită înmulțire, notată cu “ \cdot ” – precum și cu o relație de ordine, notată cu “ \leq ”, în raport cu care sunt îndeplinite următoarele axiome:

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

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

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

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

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

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

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

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

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

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

$$AR11. \quad \forall x, y \in \mathbb{R}, \text{ dacă } x \leq y \text{ și } y \leq x, \text{ atunci } x = y;$$

$$AR12. \quad \forall x, y, z \in \mathbb{R} \text{ cu } x \leq y \text{ și } y \leq z \implies x \leq z;$$

$$AR13. \quad \forall x, y \in \mathbb{R} \text{ cu } x \leq y \implies x + z \leq y + z, \quad \forall z \in \mathbb{R};$$

$$AR14. \quad \forall x, y, z \in \mathbb{R} \text{ cu } x \leq y \text{ și } 0 \leq z \implies x \cdot z \leq y \cdot z;$$

$$AR15. \quad \text{Orice submulțime nevidă și majorată a lui } \mathbb{R} \text{ are o margine superioară în } \mathbb{R}.$$

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

După cum ne vom convinge în secțiunea următoare, mulțimea \mathbb{R} , introdusă axiomatic prin Definiția 2.18, este unică până la un izomorfism de corpuri comutative, total ordonate. În \mathbb{R} , apar submulțimile remarcabile \mathbb{N}, \mathbb{Z} și \mathbb{Q} , unice și ele până la un izomorfism (de monoizi/inele/corpuri), aflate în relația:

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

Printre proprietățile lui \mathbb{R} figurează și acelea cuprinse în următorul enunț, lipsit aici de demonstrație.

Propoziția 2.9 a) *Mulțimea numerelor reale din intervalul $[0, 1]$ este nenumărabilă. Cardinalul ei se numește **puterea continuului** și notat, prin tradiție, cu c , este egal cu 2^{\aleph_0} .*

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

- (1) mulțimea \mathbb{R} ;
- (2) orice interval din \mathbb{R} , de forma $[a, b]$, $[a, b)$, (a, b) , $(a, b]$, unde $a < b$;
- (3) mulțimea $\mathbb{R} \setminus \mathbb{Q}$ a numerelor iraționale;
- (4) orice submulțime a lui \mathbb{R} care conține un interval deschis;
- (5) mulțimea lui Cantor, adică mulțimea C a tuturor numerelor din intervalul $[0, 1]$ care au reprezentarea, în baza 3, numai cu cifrele 0 și 2.

Ipoteza continuului.

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

$$\aleph_0 \leq h(\aleph_0) \stackrel{\text{def}}{=} \aleph_1 \leq h(\aleph_1) \stackrel{\text{def}}{=} \aleph_2 \leq \dots$$

Întrebarea firească este aceea asupra poziției 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 mulțime al cărei cardinal este cuprins strict între cardinalul lui \mathbb{N} și cardinalul lui \mathbb{R} . Un asemenea postulat este, în teoria mulțimilor, analog axiomei paralelelor din geometria plană euclidiană.

Deoarece între mulțimea \mathbb{R} și mulțimea punctelor de pe o dreaptă (pe care s-a stabilit un punct numit origine, un sens – o orientare – și o unitate de măsură) se poate pune în evidență o corespondență biunivocă (bijecție), se ajunge de cele mai multe ori la identificarea mulțimii numerelor reale cu punctele drepte 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 și termenul de “dreaptă reală” în loc de \mathbb{R} .

Cum, pentru o mulțime $\emptyset \neq A \subset \mathbb{R}$, nemajorată, nu mai avem asigurat faptul că $\sup A$ (în sensul ordinii totale pe \mathbb{R}) aparține lui \mathbb{R} , iar pentru o mulțime nevidă și neminorată $B \subset \mathbb{R}$ nu putem spune că $\inf B \in \mathbb{R}$, se iau în considerație două simboluri (elemente), numite **plus infinit** – notat cu $+\infty$ (sau, pe scurt, ∞) și respectiv **minus infinit** – notat cu $-\infty$, astfel încât, pe mulțimea $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$ – numită **dreapta reală extinsă** (sau **încheiată**), în virtutea convenției prin care $-\infty < +\infty$ și $\forall x \in \mathbb{R}$, $-\infty < x < +\infty$, se pot extinde operațiile “+” și “.” de pe \mathbb{R} , precum și relația de ordine naturală, luând, prin definiție: $x + (+\infty) = (+\infty) + x = +\infty$, $\forall x \in \overline{\mathbb{R}} \setminus \{-\infty\}$; $x + (-\infty) = (-\infty) + x = -\infty$, $\forall x \in \overline{\mathbb{R}} \setminus \{+\infty\}$; $x \cdot (+\infty) = (+\infty) \cdot x = +\infty$, dacă $0 < x$ și $x \cdot (+\infty) = (+\infty) \cdot x = -\infty$, dacă $x < 0$; $x \cdot (-\infty) = (-\infty) \cdot x = -\infty$, dacă $0 < x$ și $x \cdot (-\infty) = (-\infty) \cdot x = +\infty$, dacă $x < 0$; $\frac{x}{+\infty} = \frac{x}{-\infty} = 0$, $\forall x \in \mathbb{R}$.

Se consideră lipsite de sens, fiind nedeterminate, operațiile 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 $0 \cdot \infty$) și $\frac{+\infty}{+\infty}$, $\frac{+\infty}{-\infty}$, $\frac{-\infty}{+\infty}$, $\frac{-\infty}{-\infty}$ (pe scurt $\frac{\infty}{\infty}$). Elucidarea sensului acestor operații are loc, de regulă, pe seama expresiilor din care provin.

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

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

Latici și algebre Boole

Definiția 2.19 O mulțime nevidă L , împreună cu două operații interne “ \vee ” : $L \times L \rightarrow L$ și “ \wedge ” : $L \times L \rightarrow L$, este numită **latice** dacă ambele legi, “ \vee ” și “ \wedge ”, sunt asociative, comutative, idempotente și absorbante, adică:

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

$$(b) \quad x \wedge (y \wedge z) = (x \wedge y) \wedge z, \forall x, y, z \in L,$$

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

$$(b) \quad x \wedge y = y \wedge x, \forall x, y \in L,$$

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

$$(b) \quad x \wedge x = x, \forall x \in L,$$

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

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

Caracterul algebric al Definiției 2.19 este evident. Pe baza acestei definiții, se poate introduce o relație de ordine parțială pe laticea L (prin “ $x \leq y$ ”, dacă și numai dacă “ $x = x \wedge y$ ”), în raport cu care (L, \leq) reprezintă o structură parțial ordonată.

Reciproc, dacă (A, \leq) este o mulțime (nevidă) parțial ordonată, atunci se pot defini operațiile \vee și \wedge (pe A), prin:

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

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

observându-se faptul că, în felul acesta, (A, \vee, \wedge) constituie o latice, în sensul Definiției 2.19. În virtutea unei astfel de observații, noțiunea de latice se poate baza și pe următoarea definiție, echivalentă cu cea de mai sus:

Definiția 2.20 O mulțime parțial ordonată (L, \leq) este numită **latice** dacă și numai dacă, pentru orice x și y din L , atât $\sup \{x, y\}$, cât și $\inf \{x, y\}$, există și sunt (ambele) din L .

Un exemplu elementar de latice îl constituie mulțimea numerelor naturale, înzestrată cu relația de ordine uzuală, prin intermediul căreia se pot defini operațiile: $n_1 \wedge n_2 = \min \{n_1, n_2\}$, $n_1 \vee n_2 = \max \{n_1, n_2\}$, $\forall n_1, n_2 \in \mathbb{N}$. Este satisfăcută atunci, cu evidență, Definiția 2.19.

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

i) **distributivă**, când oricare dintre operațiile “ \vee ” și “ \wedge ” este distributivă față de cealaltă, adică

$$(a) \quad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \text{ sau}$$

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

ii) **modulară**, când

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

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

Definiția 2.22 Două **latici** L_1 și L_2 se numesc **izomorfe** dacă există o bijecție $\phi : L_1 \rightarrow L_2$ astfel încât:

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

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

Definiția 2.23 O submulțime $L' \neq \emptyset$ a unei latici (L, \vee, \wedge) se numește **sublatice** (a lui L) dacă (L', \vee, \wedge) este o latice în sine.

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

Definiția 2.24 O mulțime nevidă B , înzestrată cu două operații binare, “ \vee ” și “ \wedge ”, o operație unară (de complementariere), notată cu “ $'$ ” și două elemente “neutre”, “ 0 ” și “ 1 ”, se numește **algebră Boole** dacă:

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

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

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

Un exemplu clar de algebră Boole îl constituie mulțimea $\mathcal{P}(X)$, a tuturor submulțimilor unei mulțimi X , în raport cu operațiile de reuniune și de intersecție, alături de care și cea de complementariere uzuală (la mulțimi), având mulțimea vidă în rolul lui “ 0 ” și mulțimea X în rolul lui “ 1 ”.

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

Inegalități cu elemente din \mathbb{R}

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

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

Demonstrație: Se consideră mulțimea $M = \{n \in \mathbb{N}, \text{ astfel încât are loc } (*)\} \subseteq \mathbb{N}$ și se arată că M satisface condiția (axioma) (P_3) (Peano) din Definiția 2.14. Rezultă atunci că $M = \mathbb{N}$, ceea ce înseamnă că (*) are loc într-adevăr, pentru orice număr natural real n , cu datele din enunț.

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:

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

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

Prima inegalitate are loc deoarece $n \in M$ (și, ca atare, $(*)$ are loc pentru n), iar cea de-a doua este de fapt inegalitatea $(*)$ din cazul $n = 2$, cu ponderile 1 și λ_{n+1} în rolurile lui λ_1 și λ_2 , cu $\left(\sum_{i=0}^n \lambda_i a_i^p \right)^{\frac{1}{p}}$ și a_{n+1} în rolurile lui a_1 și respectiv a_2 , precum și cu $\left(\sum_{i=0}^n \lambda_i b_i^q \right)^{\frac{1}{q}}$ și b_{n+1} în rolurile lui b_1 și respectiv b_2 . Așa 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 funcția $f : \mathbb{R}_+ \rightarrow \mathbb{R}$, 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 $a_1 \neq 0$) și, studiind variația 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 menționat că, în $(*)$, egalitatea are loc dacă și numai dacă n -uplele $(a_0^p, a_1^p, \dots, a_n^p)$ și $(b_0^p, b_1^p, \dots, b_n^p)$ sunt proporționale. ◀

Folosind un raționament asemănător, se poate demonstra și că este adevărată propoziția ce urmează. În prealabil, precizăm că, atunci când $\lambda_1 = \lambda_2 = \dots = \lambda_n \in \mathbb{R}_+^*$, relația $(*)$ reprezintă *inegalitatea lui Hölder fără ponderi*. De asemenea, specificăm că, pentru $p = q = 2$ și $\lambda_1 = \lambda_2 = \dots = \lambda_n \in \mathbb{R}_+^*$, 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 concordanță cu ce am precizat în legătura cu $(*)$, dacă și numai dacă există $u, v \in \mathbb{R}$, cu $u^2 + v^2 \neq 0$, așa încât $ua_i + vb_i = 0$, $\forall i \in \{0, 1, 2, \dots, n\}$.

Propoziția 2.11 (Inegalitatea lui Minkowski, cu ponderi) Pentru $p \in \mathbb{R}$, $p \geq 1$, $n \in \mathbb{N}$ și $\lambda_0, \lambda_1, \dots, \lambda_n, a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_n$ 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 și numai dacă n -uplele (a_0, a_1, \dots, a_n) și (b_0, b_1, \dots, b_n) sunt proporționale.

Demonstrație: Ca și în situația inegalității lui Hölder, considerând mulțimea 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 $0 \in L$ și că dacă $n \in L$, atunci $n+1 = s(n) \in L$. Acest din urmă lucru revine, ca și în demonstrarea inegalității $(*)$, la a arăta că $(***)$ este adevărată, de fapt, pentru $n = 2$, ceea ce se poate dovedi pe seama studiului variației unei funcții 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 și în situațiile din enunț. ◀

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

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

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

Demonstrație: Considerând n arbitrar din \mathbb{N}^* , a_1, a_2, \dots, a_n din \mathbb{R}_+ și $b_1, b_2, \dots, b_n \in \mathbb{R}_+^*$, pe baza inegalității mediilor, adică a inegalității

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

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

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

și, prin aceasta, putem scrie:

$$\begin{aligned} (!!) \quad \sum_{k=1}^n (a_1 a_2 \dots a_k)^{\frac{1}{k}} &= \sum_{k=1}^n \left(\frac{b_1 a_1 b_2 a_2 \dots b_k a_k}{b_1 b_2 \dots b_k} \right)^{\frac{1}{k}} = \sum_{k=1}^n (b_1 b_2 \dots b_k)^{-\frac{1}{k}} (b_1 a_1 b_2 a_2 \dots b_k a_k)^{\frac{1}{k}} \leq \\ &\leq \sum_{k=1}^n \left((b_1 b_2 \dots b_k)^{-\frac{1}{k}} \cdot \frac{1}{k} \sum_{l=1}^k b_l a_l \right) = \sum_{l=1}^n b_l a_l \cdot \sum_{k=l}^n \frac{(b_1 b_2 \dots b_k)^{-\frac{1}{k}}}{k}. \end{aligned}$$

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

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

Astfel, din (!!) obținem

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

adică tocmai (!).

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

Bibliografie selectivă

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