Dumitru Buşneag

Florentina Chirteş **Dana Piciu**

COMPLEMENTE DE ALGEBRĂ

Editura GIL

CUPRINS

Capitolul 1

MULȚIMEA NUMERELOR NATURALE $\mathbb{N}$

Dumnezeu a creat numerele naturale – restul este munca omului.

(L. Kronecker)

1.1. Triplete Peano

Definiția 1.1.1. Numim *triplet Peano* un triplet (N, 0, s) unde N este o mulțime nevidă, $0 \in N$ iar $s: N \to N$ este o funcție astfel încât sunt verificate axiomele :

P_1 : $0 \notin s(N)$;

P_2 : s este o funcție injectivă ;

P_3 : dacă $P \subseteq N$ este o submulțime astfel încât $0 \in P$ și $(n \in P \Rightarrow s(n) \in P)$, atunci $P = N$.

În cele ce urmează, acceptăm ca axiomă existența unui triplet Peano (cititorului dornic de aprofundarea acestei chestiuni îi recomandăm lucrările [17] și [38]) .

Lema 1.1.2. Dacă (N, 0, s) este un triplet Peano, atunci $N = \{0\} \cup s(N)$.

Demonstrație. Dacă notăm $P = \{0\} \cup s(N)$, atunci $P \subseteq N$ și cum P verifică P_3, deducem că $P = N$. ■

Teorema 1.1.3. Fie (N, 0, s) un triplet Peano iar (N′, 0′, s ′) un alt triplet format dintr-o mulțime nevidă N′, un element $0' \in N'$ și o funcție $s': N' \to N'$. Atunci :

(i) Există o unică funcție $f: N \to N'$ astfel încât $f(0) = 0'$, iar diagrama

$$\begin{array}{ccc} N & \xrightarrow{f} & N' \\ {\scriptstyle s}\downarrow & & \downarrow{\scriptstyle s'} \\ N & \xrightarrow[f]{} & N' \end{array}$$

este comutativă (adică $f \circ s = s' \circ f$);

(ii) Dacă (N′, 0′, s′) este un triplet Peano, atunci f este bijecție.

Demonstrație. (i). Pentru a proba existența lui f, vom considera toate relațiile $R \subseteq N \times N'$ astfel încât :

r_1 : $(0, 0') \in R$

r_2 : Dacă $(n, n') \in R$, atunci $(s(n), s'(n')) \in R$ iar prin R_0 vom nota intersecția acestor relații .

Vom demonstra că R_0 este o relație funcțională și astfel f va fi funcția ce va avea drept grafic pe R_0 (astfel, din $(0, 0') \in R_0$ vom deduce că $f(0) = 0'$ iar dacă $n \in N$ și $f(n) = n' \in N'$, $(n , n') \in R_0$, deci $(s(n), s'(n')) \in R_0$, adică, $f(s(n)) = s'(n') = s'(f(n))$. Pentru a demonstra că R_0 este o relație funcțională, vom demonstra că pentru orice $n \in N$, există

$n' \in N'$ astfel încât $(n, n') \in R_0$ iar dacă pentru $n \in N$ şi $n', n'' \in N'$ avem $(n, n') \in R_0$ şi $(n, n'') \in R_0$, atunci $n' = n''$.

Pentru prima parte, fie $P=\{n \in N$: există $n' \in N'$ astfel încât $(n, n') \in R_0\} \subseteq N$. Cum $(0, 0') \in R_0$ deducem că $0 \in P$. Fie acum $n \in P$ şi $n' \in N'$ astfel încât $(n, n') \in R_0$. Din definiţia lui R_0 deducem că $(s(n), s'(n')) \in R_0$; obţinem că $s(n) \in P$ şi cum $(N, 0, s)$ este triplet Peano, deducem că $P=N$.

Pentru a doua parte, fie

$$Q=\{n \in N : \text{dacă } n', n'' \in N' \text{ şi } (n, n'), (n, n'') \in R_0 \Rightarrow n' = n''\} \subseteq N$$

şi să demonstrăm la început că $0 \in Q$.

În acest sens, vom demonstra că dacă $(0, n') \in R_0$ atunci $n' = 0'$. Dacă prin absurd, $n' \neq 0'$, atunci vom considera relaţia $R_1 = R_0 \setminus \{(0, n')\} \subseteq N \times N'$. Din $n' \neq 0'$ deducem că $(0, 0') \in R_1$ iar dacă pentru $m \in N'$ avem $(n, m) \in R_1$, atunci $(n, m) \in R_0$ şi $(n, m) \neq (0, n')$. Astfel $(s(n), s'(m)) \in R_0$ şi cum $(s(n), s'(m)) \neq (0, n')$ (căci $s(n) \neq 0$ conform cu P_1), deducem că $(s(n), s'(m)) \in R_1$. Cum R_1 verifică r_1 şi r_2 ar trebui ca $R_0 \subseteq R_1$ – absurd (căci R_1 este inclusă strict în R_0).

Pentru a proba că $0 \in Q$, fie $n', n'' \in N'$ astfel încât $(0, n'), (0, n'') \in R_0$. Atunci, ţinând cont de cele stabilite mai sus, deducem că $n' = n'' = 0'$, deci $0 \in Q$.

Fie acum $n \in Q$ şi $n' \in N'$ astfel încât $(n, n') \in R_0$; vom demonstra că dacă $(s(n), n'') \in R_0$, atunci $n'' = s(n')$. Să presupunem prin absurd că $n'' \neq s(n')$ şi să considerăm relaţia $R_2 = R_0 \setminus \{(s(n), n'')\}$. Vom demonstra că R_2 verifică r_1 şi r_2 . Într–adevăr, $(0,0') \in R_2$ (căci $0 \neq s(n)$) iar dacă $(p, p') \in R_2$, atunci $(p, p') \in R_0$ şi $(p, p') \neq (s(n), n'')$.

Deducem că $(s(p), s'(p')) \in R_0$ şi dacă presupunem $(s(p), s'(p')) = (s(n), n'')$, atunci $s(p) = s(n)$, deci $p=n$. De asemenea, $s'(p') = n''$. Atunci $(n, n') \in R_0$ şi $(n, p') \in R_0$ iar cum $n \in Q \Rightarrow n' = p'$, deci $n'' = s'(p') = s'(n')$, ceea ce contrazice faptul că $n'' \neq s(n')$. Prin urmare, $(s(p), s'(p')) \neq (s(n), n'')$, ceea ce ne arată că $(s(p), s'(p')) \in R_2$, adică R_2 satisface r_1 şi r_2 . Din nou ar trebui ca $R_0 \subset R_2$ – absurd !. Deci $(s(n), n'') \in R_0 \Rightarrow n'' = s'(n')$ astfel că dacă $r, s \in N'$ şi $(s(n), r), (s(n), s) \in R_0$, atunci $r = s = s'(n')$, adică $s(n) \in Q$, deci $Q=N$.

Pentru a proba unicitatea lui f, să presupunem că mai există $f' : N \to N'$ astfel încât $f'(0) = 0'$ şi $s'(f'(n)) = f'(s(n))$ pentru orice $n \in N$.

Considerând $P=\{n \in N : f(n) = f'(n)\} \subseteq N$, atunci $0 \in P$ iar dacă $n \in P$ (adică $f(n) = f'(n)$), atunci $s'(f(n)) = s'(f'(n)) \Rightarrow f(s(n)) = f'(s(n)) \Rightarrow s(n) \in P$ şi atunci $P=N$, adică $f=f'$.

(ii). Să arătăm la început că f este injectivă. Pentru aceasta vom considera $P=\{n \in N$: dacă $m \in N$ şi $f(m)=f(n) \Rightarrow m=n\} \subseteq N$ şi să demonstrăm la început că $0 \in P$. Pentru aceasta fie $m \in N$ astfel încât $f(0)=f(m)$ şi să demonstrăm că $m=0$. Dacă prin absurd $m \neq 0$, atunci $m=s(n)$ cu $n \in N$ iar egalitatea $f(m)=f(0)$ devine $f(s(n))=f(0)=0'$, de unde $s'(f(n))=0'$, ceea ce este absurd deoarece prin ipoteză $(N', 0', s')$ este un triplet Peano.

Fie acum $n \in P$; pentru a demonstra că $s(n) \in P$, fie $m \in N$ astfel încât $f(m)=f(s(n))$.

Atunci $m \neq 0$ (căci în caz contrar ar rezulta că $0' = f(0) = f(s(n)) = s'(f(n))$, absurd !), deci conform Lemei 1.1.2, $m=s(p)$ cu $p \in N$ iar egalitatea $f(m)=f(s(n))$ devine

$f(s(p))=f(s(n)) \Leftrightarrow s'(f(p))=s'(f(n))$, adică $f(p)=f(n)$ şi cum $n\in P$, atunci $n=p$ şi astfel $m=s(p)=s(n)$.

Pentru a demonstra surjectivitatea lui f să considerăm

$$P'=\{n'\in N': \text{există } n\in N \text{ astfel încât } n'=f(n)\}\subseteq N' .$$

Cum $f(0)=0'$ deducem că $0'\in P'$. Fie acum $n'\in P'$; atunci există $n\in N$ astfel încât $n'=f(n)$. Deoarece $s'(n')=s'(f(n))=f(s(n))$, deducem că $s'(n')\in P'$ şi cum tripletul $(N', 0', s')$ este un triplet Peano, deducem că $P'=N'$, adică f este şi surjectivă, deci bijectivă . ■

Observaţie. Conform Teoremei 1.1.3 (cunoscută şi sub numele de *teorema de recurenţă*) un triplet Peano este unic până la o bijecţie.

În cele ce urmează vom alege un triplet Peano oarecare $(\mathbb{N}, 0, s)$ şi pe care îl vom fixa ; elementele lui $\mathbb{N}$ le vom numi *numere naturale* .

Elementul 0 va purta numele de *zero* . Notăm $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.

Vom nota $1=s(0)$, $2=s(1)$, $3=s(2)$, e.t.c., astfel că $\mathbb{N}=\{0, 1, 2, \ldots\}$. Funcţia s poartă numele de *funcţia succesor* . Axiomele $P_1 - P_3$ sunt cunoscute sub numele de *axiomele lui Peano* .

Axioma P_3 poartă numele de *axioma inducţiei matematice*.

1.2. Adunarea numerelor naturale

Teorema 1.2.1. Există o unică operaţie algebrică pe $\mathbb{N}$ pe care o vom nota prin „+" şi o vom numi *adunarea numerelor naturale* astfel încât pentru orice m, n∈ℕ să avem :

A_1 : $0+m=m$;

A_2 : $s(n)+m=s(n+m)$.

Demonstraţie. Să probăm la început unicitatea şi pentru aceasta să presupunem că mai există o operaţie algebrică $\oplus$ pe $\mathbb{N}$ astfel încât sunt verificate A_1 şi A_2.

Fie $P=\{n\in\mathbb{N} : n+m=n\oplus m, \text{ pentru orice } m\in\mathbb{N}\}\subseteq\mathbb{N}$.

Din A_1 deducem că $0\in P$ iar din A_2 deducem că dacă $n\in P$, atunci $s(n)+m=s(n)\oplus m \Leftrightarrow s(n+m)=s(n\oplus m)$, ceea ce este adevărat deoarece s este injectivă şi am presupus că $n\in P$. Deci $P=\mathbb{N}$, adică cele două operaţii coincid.

Considerăm un element $m\in\mathbb{N}$ (pe care îl fixăm) şi tripletul $(\mathbb{N}, m, s)$; conform Teoremei 1.1.3 există o unică funcţie $f_m:\mathbb{N}\to\mathbb{N}$ astfel încât $f_m(0)=m$ şi $s(f_m(n))=f_m(s(n))$ pentru orice $n\in\mathbb{N}$. Pentru $n\in\mathbb{N}$ definim $n+m=f_m(n)$. Atunci $0+m=f_m(0)=m$ iar $s(n)+m= =f_m(s(n)) = s(f_m(n)) = s(n+m)$. ■

Observaţie. Axiomele A_1–A_2 poartă numele de *axiomele adunării numerelor naturale*.

Propoziţia 1.2.2. Pentru orice m, n∈ℕ avem

A_1^0 : $n+0=n$;

A_2^0 : $n+s(m)= s(n+m)$.

Demonstraţie. Fie $P=\{m\in\mathbb{N}: m+0=m\}\subseteq\mathbb{N}$. Dacă în A_1 facem pe $m=0$, deducem că $0+0=0$, adică $0\in P$. Dacă $m\in P$, (adică $m+0=m$), atunci $s(m)+0=s(m+0)=s(m)$, adică $s(m)\in P$, deci $P=\mathbb{N}$. Analog se probează şi a doua relaţie.■

Propoziția 1.2.3. Dubletul $(\mathbb{N}, +)$ este monoid comutativ cu proprietatea de simplificare.

Demonstrație. Din cele stabilite anterior, deducem că 0 este element neutru pentru adunarea numerelor naturale.

Pentru a proba comutativitatea adunării să considerăm

$$P=\{n\in\mathbb{N} : n+m=m+n \text{ pentru orice } m\in\mathbb{N}\} \subseteq \mathbb{N}.$$

Evident $0\in P$. Dacă $n\in P$, adică $n+m=m+n$ pentru orice $m\in\mathbb{N}$, atunci $s(n)+m=m+s(n) \Leftrightarrow s(n+m)=s(m+n) \Leftrightarrow n+m=m+n$, ceea ce este adevărat. Deducem că $P=\mathbb{N}$, adică adunarea numerelor naturale este comutativă.

Pentru a demonstra asociativitatea adunării numerelor naturale, să considerăm

$$P=\{n\in\mathbb{N}: (n+m)+p=n+(m+p) \text{ pentru orice } m, p\in\mathbb{N}\}\subseteq\mathbb{N}.$$

Evident $0\in P$. Fie acum $n\in P$. Atunci $(s(n)+m)+p=s(n+m)+p=s((n+m)+p)$ iar $s(n)+(m+p)=s(n+(m+p))$ și cum $(n+m)+p=n+(m+p)$ deducem că $s(n)\in P$, adică $P=\mathbb{N}$.

Pentru partea finală fie $P=\{p\in\mathbb{N} : \text{dacă } m+p=n+p \Rightarrow m=n\}\subseteq\mathbb{N}$.

Evident $0\in P$ și să presupunem că $p\in P$. Atunci $m+s(p)=n+s(p) \Leftrightarrow s(m+p)=s(n+p) \Leftrightarrow m+p=n+p \Leftrightarrow m=n$ (căci $p\in P$), adică $s(p)\in P$ și astfel din nou $P=\mathbb{N}$. ■

Observație. Dacă $n\in\mathbb{N}$, atunci $s(n)=s(n+0)=n+s(0)=n+1$.

Propoziția 1.2.4. Dacă $m, n\in\mathbb{N}$ și $m+n=0$, atunci $m=n=0$.

Demonstrație. Dacă $m\neq 0$ sau $n\neq 0$, atunci există $p, q\in\mathbb{N}$ astfel încât $m=s(p)$ sau $n=s(q)$. În primul caz, obținem că $m+n=s(p)+n=s(p+n)\neq 0$ – absurd ! și analog în al doilea caz. Deci $m=n=0$. ■

1.3. Înmulțirea numerelor naturale

Propoziția 1.3.1. Există o unică operație algebrică pe $\mathbb{N}$ notată „$\cdot$” și numită *înmulțirea numerelor naturale* astfel încât pentru orice $m, n\in\mathbb{N}$ să avem :

I_1 : $m\cdot 0=0$;

I_2 : $m\cdot s(n)=mn+m$.

Demonstrație. Fie $m\in\mathbb{N}$ fixat ; considerând tripletul $(\mathbb{N}, 0, f_m)$, unde $f_m:\mathbb{N}\to\mathbb{N}$ este definită prin $f_m(n)=n+m$ pentru orice $n\in\mathbb{N}$, atunci conform Teoremei 1.1.3. există o unică funcție $g_m:\mathbb{N}\to\mathbb{N}$ astfel încât $g_m(0)=0$ și $f_m\circ g_m=g_m\circ s$.

Definim $m\cdot n=g_m(n)$ și astfel $m\cdot 0=g_m(0)=0$ iar $m\cdot s(n)=g_m(s(n))=f_m(g_m(n))=f_m(m\cdot n)=$ $=m\cdot n+m$. Unicitatea operației de înmulțire cu proprietățile I_1 și I_2 se probează ca în cazul adunării. ■

Observație. I_1 și I_2 poartă numele de *axiomele înmulțirii numerelor naturale.*

În cele ce urmează, dacă nu este pericol de confuzie, vom scrie $m\cdot n=mn$ pentru $m, n\in\mathbb{N}$.

Analog ca în cazul adunării numerelor naturale, se demonstrează că pentru oricare numere naturale m, n avem :

I_1^0 : $0\cdot m=0$;

I_2^0 : $s(n)\cdot m=nm+m$.

Lema 1.3.2. Înmulţirea numerelor naturale este distributivă la stânga faţă de adunarea numerelor naturale.

Demonstraţie. Fie $P=\{p\in\mathbb{N} : m(n+p) = mn+mp$ pentru oricare $m, n\in\mathbb{N}\}\subseteq\mathbb{N}$.

Ţinând cont de A_1 şi I_1 deducem că $0\in P$.

Să presupunem acum că $p\in P$ şi fie $m, n\in\mathbb{N}$.

Avem $m(n+s(p))=m(s(n+p))=m(n+p)+m=mn+mp+m=mn+ms(p)$, adică $s(p)\in P$ şi astfel $P=\mathbb{N}$. ■

Propoziţia 1.3.3. Dubletul $(\mathbb{N}, \cdot)$ este monoid comutativ.

Demonstraţie. Pentru a proba asociativitatea înmulţirii fie

$$P=\{p\in\mathbb{N} : (mn)p = m(np) \text{ pentru oricare } m, n\in\mathbb{N}\}\subseteq\mathbb{N}.$$

În mod evident, $0\in P$. Să presupunem acum că $p\in P$ şi să demonstrăm că $s(p)\in P$. Avem $(mn)s(p)=(mn)p+mn$ iar $m(ns(p))=m(np+n)=m(np)+mn$ (conform Lemei 1.3.2), de unde egalitatea $(mn)s(p)=m(ns(p))$, adică $s(p)\in P$, deci $P=\mathbb{N}$.

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

Pentru a proba comutativitatea înmulţirii numerelor naturale fie

$$P=\{n\in\mathbb{N} : nm=mn \text{ pentru orice } m\in\mathbb{N}\}\subseteq\mathbb{N}.$$

În mod evident $0\in P$ şi să presupunem că $n\in\mathbb{N}$.

Atunci pentru orice $m\in\mathbb{N}$, $s(n)\cdot m=n\cdot m+m$ iar $m\cdot s(n)=mn+m$, de unde $s(n)\cdot m=m\cdot s(n)$, adică $s(n)\in P$, deci $P=\mathbb{N}$. ■

1.4. Relaţia naturală de ordine de pe $\mathbb{N}$

Definiţia 1.4.1. Pentru $m, n\in\mathbb{N}$ vom scrie $m\leq n$ (şi vom spune că m este *mai mic sau egal* decât n sau că n este *mai mare sau egal* decât m) dacă există $p\in\mathbb{N}$ astfel încât $m+p=n$; convenim în acest caz să notăm $p=n-m$.

Dacă $p\in\mathbb{N}^*$, atunci $m\leq n$ şi $m\neq n$; în acest caz vom scrie $m<n$ şi vom spune că m este *strict mai mic* decât n.

Lema 1.4.2. Dacă $m, n\in\mathbb{N}$ şi $m<n$, atunci $s(m)\leq n$.

Demonstraţie. Deoarece $m<n$, există $p\in\mathbb{N}^*$ astfel încât $m+p=n$. Cum $p\in\mathbb{N}^*$, există $k\in\mathbb{N}$ astfel încât $p=s(k)$ (conform Lemei 1.1.2). Atunci din $m+p=n$ deducem că $m+s(k)=n \Rightarrow s(m+k)=n \Rightarrow s(m)+k=n \Rightarrow s(m)\leq n$. ■

Corolar 1.4.3. Pentru orice $n\in\mathbb{N}$, $n<s(n)$.

Propoziţia1.4.4. Dubletul $(\mathbb{N},\leq)$ este o mulţime total ordonată.

Demonstraţie. Deoarece pentru orice $n\in\mathbb{N}$, $n+0=n$ deducem că $n\leq n$, adică relaţia $\leq$ este reflexivă. Fie acum $m, n\in\mathbb{N}$ astfel încât $m\leq n$ şi $n\leq m$. Atunci există $p, q\in\mathbb{N}$ astfel încât $m+p=n$ şi $n+q=m$. Deducem că $n+(p+q)=n$, de unde $p+q=0$ (conform Propoziţiei 1.2.3), iar de aici $p=q=0$ (conform Propoziţiei 1.2.4), adică $m=n$, deci relaţia $\leq$ este antisimetrică .

Fie acum m, n, p∈ℕ astfel încât m≤ n şi n≤ p. Atunci există r, s∈ℕ astfel încât m+r=n şi n+s=p. Deducem imediat că m+(r+s)=p, adică m≤p, deci relaţia ≤ este şi tranzitivă, adică ≤ este o relaţie de ordine pe ℕ.

Pentru a proba că ordinea ≤ de pe ℕ este totală, fie m∈ℕ fixat iar

$$P_m=\{n\in\mathbb{N}: n\le m \text{ sau } m\le n\}\subseteq\mathbb{N}.$$

În mod evident $0\in P_m$ şi fie $n\in P_m$. Dacă n=m, atunci cum n<s(n) avem m<s(n), adică $s(n)\in P_m$. Dacă n<m, atunci conform Lemei 1.4.2 avem s(n)≤m şi din nou $s(n)\in P_m$. Dacă m<n, cum n<s(n) avem că m<s(n) şi din nou $s(n)\in P_m$. Rezultă că $P_m=\mathbb{N}$ şi cum m este oarecare deducem că ordinea ≤ de pe ℕ este totală. ■

Observaţie. Relaţia de ordine ≤ definită anterior pe ℕ poartă numele de *ordinea naturală* de pe ℕ.

Teorema 1.4.5. Dubletul (ℕ, ≤) este o mulţime bine ordonată.

Demonstraţie. Trebuie să demonstrăm că orice submulţime nevidă A⊆ℕ are un cel mai mic element. Pentru aceasta fie:

$$P=\{n\in\mathbb{N}: n\le x \text{ pentru orice } x\in A\}\subseteq\mathbb{N}.$$

Evident 0∈P. Dacă pentru orice n∈P ar rezulta s(n)∈P, atunci am deduce că P=ℕ. Astfel că alegând un $x_0\in A$ atunci $x_0\in P$, deci $s(x_0)\in P$. În particular ar rezulta că $s(x_0)\le x_0$, absurd!.

Deducem că P≠ℕ, adică există a∈P astfel încât s(a)∉P.

Vom demonstra că a∈A şi că a este cel mai mic element al lui A.

Dacă a∉A, atunci pentru orice x∈A avem a<x, de unde s(a)≤x (conform Lemei 1.4.2), adică s(a)∈P – absurd !, deci a∈A şi cum a∈P deducem că a ≤x pentru orice x∈A, adică a este cel mai mic element al lui A . ■

Corolar 1.4.6. Orice şir descrescător de numere naturale este staţionar.

Demonstraţie. Fie $(a_n)_{n\in\mathbb{N}}$ un şir descrescător de numere naturale iar $A=\{a_n : n\in\mathbb{N}\}\subseteq\mathbb{N}$. Conform Teoremei 1.4.5 mulţimea A are un cel mai mic element a_k; atunci pentru orice m≥k avem $a_m\ge a_k$ şi cum $a_k\le a_m$ deducem că $a_m=a_k$, adică şirul $(a_n)_{n\in\mathbb{N}}$ este staţionar. ■

Corolar 1.4.7. În ℕ nu putem găsi un şir strict descrescător şi infinit de numere naturale.

Corolar 1.4.8. Fie P⊆ℕ astfel încât pentru orice n∈ℕ (x<n ⇒ x∈P) ⇒ n∈P. Atunci P=ℕ.

Demonstraţie. Fie $A=\mathbb{N}\setminus P\subseteq\mathbb{N}$ şi să presupunem prin absurd că $A\neq\emptyset$.

Conform Teoremei 1.4.5 mulţimea A va avea un cel mai mic element a∈A. Cum pentru x∈ℕ, x<a ⇒ x∉A ⇒ x∈P, conform ipotezei P=ℕ, adică a∈P şi astfel a∉A – absurd !. Deci A=∅, de unde P=ℕ . ■

Corolar 1.4.9. (*Teorema împărţirii cu rest în* $\mathbb{N}$). **Pentru oricare două numere naturale m, n cu** $n\neq 0$, **există şi sunt unice două numere naturale c şi r astfel încât** $m=n\cdot c+r$ **şi** $r<n$.

Demonstraţie. Fie $A=\{s\in\mathbb{N}$: există $p\in\mathbb{N}$ astfel încât $m=np+s\}\subseteq\mathbb{N}$. Deoarece $m=0\cdot m+m$ deducem că $m\in A$, adică $A\neq\emptyset$. Conform Teoremei 1.4.5 mulţimea A posedă un element minimal $r\in A$. Atunci există $c\in\mathbb{N}$ astfel încât $m=c\cdot n+r$ şi să demonstrăm că $r<n$.

Dacă prin absurd $r\not<n$, atunci conform Propoziţiei 1.4.4, $r\geq n$, adică există $u\in\mathbb{N}$ astfel încât $r=n+u$. Deducem că $m=nc+r=nc+n+u=n(c+1)+u$, adică $u\in A$, deci $r\leq u$ şi cum $u\leq r$ deducem că $u=r$, adică $n=0$ – absurd !.

Pentru a demonstra unicitatea lui c şi r să presupunem că $m=cn+r=c'n+r'$, cu r, $r'<n$ şi să arătăm că $c=c'$ şi $r=r'$.

Să presupunem de exemplu că $c<c'$, adică $c+u=c'$ cu $u\in\mathbb{N}^*$.

Atunci $m=nc'+r'=n(c+u)+r'=nc+nu+r'$, deci $r=nu+r'>n$ – absurd !.

Deci $c=c'$ şi deducem imediat că şi $r=r'$. ■

Observaţie. Numărul c poartă numele de *câtul împărţirii lui m la n* iar r se zice *restul* acestei împărţiri.

Teorema 1.4.10. Fie $m, n, m', n', p\in\mathbb{N}$ **astfel încât** $m\leq n$ **şi** $m'\leq n'$. **Atunci:**

(i) $m+m'\leq n+n'$ **şi** $mm'\leq nn'$

(ii) $mp\leq np$ **şi** $m^p\leq n^p$.

Demonstraţie (i). Putem scrie $m+r=n$ şi $m'+r'=n'$, cu $r, r'\in\mathbb{N}$.

Din $(m+m')+(r+r')=n+n'$ deducem că $m+m'\leq n+n'$.

De asemenea $nn'=(m+r)(m'+r')=mm'+mr'+rm'+rr'$ şi cum $mr'+rm'+rr'\in\mathbb{N}$ deducem că $mm'\leq nn'$.

(ii). Se deduce ca şi (i) ţinând cont de (i) precum şi de regulile de calcul din $\mathbb{N}$ stabilite mai înainte. ■

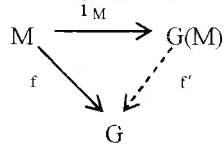
INELUL NUMERELOR ÎNTREGI $(\mathbb{Z}, +, \cdot)$

2.1. Construcţia grupului $(\mathbb{Z}, +)$

În vederea construirii mulţimii numerelor întregi $\mathbb{Z}$, vom prezenta la început Teorema lui Malţev de scufundare a unui monoid comutativ cu proprietatea de simplificare într-un grup comutativ urmând ca prin particularizare la cazul monoidului $(\mathbb{N}, +)$ să obţinem grupul aditiv $(\mathbb{Z}, +)$.

Teorema 2.1.1. (*Malţev*) **Fie $(M, \cdot)$ un monoid comutativ cu proprietatea de simplificare. Atunci există un grup comutativ G(M) şi un morfism injectiv de monoizi $i_M: M \to G(M)$ ce verifică următoarea proprietate de universalitate :**

Pentru orice grup comutativ G şi orice morfism de monoizi $f: M \to G$ există un unic morfism de grupuri $f': G(M) \to G$ astfel încât diagrama



este comutativă (adică $f' \circ i_M = f$).

Demonstraţie. Pe mulţimea $M' = M \times M$ definim relaţia $(x, y) \sim (x', y') \overset{def}{\Leftrightarrow} xy' = yx'$ şi să probăm că $\sim$ este o echivalenţă pe M' compatibilă cu structura de monoid a lui M' (adică $\sim$ este o congruenţă pe monoidul produs $M' = M \times M$).

În mod evident, relaţia $\sim$ este reflexivă şi simetrică. Dacă $(x, y) \sim (x', y')$ şi $(x', y') \sim (x'', y'')$ atunci $xy' = yx'$ şi $x'y'' = x''y'$, de unde $xx'y'y'' = x'x''yy'$, deci $xy'' = yx''$ (am simplificat prin $x'y'$), adică $(x, y) \sim (x'', y'')$, deci relaţia $\sim$ este şi tranzitivă, de unde concluzia că $\sim$ este o echivalenţă pe M' .

Fie acum $(x, y), (x', y'), (a, b), (a', b') \in M'$ astfel încât $(x, y) \sim (a, b)$ şi $(x', y') \sim (a', b')$ şi să probăm că şi $(xx', yy') \sim (aa', bb')$.

Avem deci $xb = ya$ şi $x'b' = y'a'$, de unde $xx'bb' = yy'aa'$, adică $(xx', yy') \sim (aa', bb')$, adică relaţia $\sim$ este o congruenţă pe monoidul produs M' în care reamintim că operaţia de compunere se defineşte prin $(x, y) \cdot (x', y') = (xx', yy')$. Vom considera monoidul cât $G(M) = M'/\sim$ iar pentru $(x, y) \in M'$ vom nota prin $[x, y]$ clasa sa de echivalenţă în $G(M)$. Datorită faptului că relaţia $\sim$ este o congruenţă pe M' deducem imediat că $G(M)$ devine în mod canonic monoid comutativ, definind pentru $[x, y], [x', y'] \in G(M)$, $[x, y] \cdot [x', y'] = [xx', yy']$ (elementul neutru al lui $G(M)$ va fi $e_{G(M)} = [e, e]$, e fiind elementul neutru al lui M).

Deoarece pentru $[x, y] \in G(M)$, $[x, y] \cdot [y, x] = [xy, xy] = [e, e]$ deducem că $[y, x] = [x, y]^{-1}$, adică $G(M)$ este grup (comutativ). Definim $i_M : M \to G(M)$ prin $i_M(x) = [x, e]$ pentru orice $x \in M$. Pentru $x, y \in M$ avem $i_M(x) \cdot i_M(y) = [x, e] \cdot [y, e] = [xy, e] = i_M(xy)$ adică i_M

este morfism de monoizi. Dacă $i_M(x)=i_M(y)$, atunci $[x, e]=[y, e] \Leftrightarrow xe=ye \Leftrightarrow x=y$, adică i_M este chiar morfism injectiv de monoizi.

Să arătăm acum că dubletul $(G(M), i_M)$ verifică proprietatea de universalitate din enunț. Pentru aceasta fie $(G,\circ)$ un grup comutativ oarecare şi $f:M\to G$ un morfism de monoizi. Pentru $[x, y]\in G(M)$, definim $f'([x, y])=f(x)\circ(f(y))^{-1}$. Observăm că dacă $[x, y]=[x', y']$, atunci $xy'=x'y$, deci $f(x)\circ f(y')=f(x')\circ f(y) \Leftrightarrow f(x)\circ(f(y))^{-1}=f(x')\circ(f(y'))^{-1}$, adică f' este corect definită. Să probăm acum că f' este morfism de grupuri.

Avem $f'([x, y]\cdot[x', y'])=f'([xx', yy'])=f(xx')\circ[f(yy')]^{-1}=f(x)\circ f(x')\circ[f(y)\circ f(y')]^{-1}=$
$=(f(x)\circ[f(y)]^{-1})\circ(f(x')\circ[f(y')]^{-1})=f'([x, y])\circ f'([x', y'])$.

Pentru $x\in M$ avem $(f'\circ i_M)(x) = f'(i_M(x)) = f'([x, e]) = f(x)[f(e)]^{-1} = f(x)$, de unde concluzia că $f'\circ i_M=f$.

Pentru a proba unicitatea lui f' (cu proprietatea din enunț) să presupunem că mai există un morfism de grupuri $f'':G(M)\to G$ astfel încât $f''\circ i_M=f$.

Atunci, pentru $[x, y]\in G(M)$ avem $[x, y]=[x, e]\cdot[e, y]=[x, e]\cdot[y, e]^{-1}$, de unde $f''([x, y])=f''([x, e]\cdot[y, e]^{-1})=f''(i_M(x)\cdot(i_M(y)^{-1}))=f''(i_M(x))\circ(f''(i_M(y)))^{-1}=f(x)\circ(f(y))^{-1}=$
$=f'([x, y])$, adică $f''=f'$. ■

Observaţii 1. Dacă f este un morfism injectiv de grupuri, atunci şi f' este morfism injectiv de grupuri.

Într-adevăr, dacă $[x, y]\in G(M)$ şi $f'([x, y])=e_G$, atunci $f(x)\circ(f(y))^{-1}=e_G$, deci $f(x)=f(y)$, de unde $x=y$, adică $[x, y]=[x, x]=[e, e]=e_{G(M)}$.

2. Dacă pe mulţimea dubletelor (G, f) cu G grup abelian şi $f:M\to G$ morfism injectiv de monoizi definim relaţia $(G, f)\le(G', f') \Leftrightarrow$ există $h:G\to G'$ astfel încât h este morfism injectiv de grupuri şi $h\circ f=f'$, atunci se verifică imediat că relaţia de mai sus este o relaţie de ordine iar dubletul $(G(M), i_M)$ din Teorema lui Malţev este cel mai mic element faţă de această relaţie de ordine.

Definiţia 2.1.2. Considerăm monoidul $(\mathbb{N}, +)$ (ce are proprietatea de simplificare conform Propoziţiei 1.2.3) şi urmând tehnica dată de Teorema lui Malţev, mulţimea subiacentă grupului aditiv $(G(\mathbb{N}), +)$ se notează prin $\mathbb{Z}$ şi poartă numele de *mulţimea numerelor întregi*.

Ţinând cont de faptul că $i_{\mathbb{N}}:\mathbb{N}\to\mathbb{Z}$, $i_{\mathbb{N}}(n)=[n, 0]$ pentru orice $n\in\mathbb{N}$ este morfism injectiv de monoizi, vom identifica fiecare număr natural $n\in\mathbb{N}$ prin elementul întreg $[n, 0]$ astfel că $\mathbb{N}$ va fi privită în continuare ca submulţime a lui $\mathbb{Z}$.

Fie acum $z=[m, n]\in\mathbb{Z}$. Dacă $m=n$, atunci $z=0$. Dacă $m<n$, atunci există $p\in\mathbb{N}^*$ astfel încât $m+p=n$ (în acest caz convenim să notăm $p=n-m$ şi astfel $m+(n-m)=n$) iar $z=[0, p]=-[p, 0]$ se identifică cu numărul întreg $-p$ iar dacă $n<m$, atunci există $q\in\mathbb{N}^*$ astfel încât $n+q=m$ şi astfel $z=[q, 0]$ identificându-se cu numărul natural q.

Ţinând cont de acestea putem scrie pe $\mathbb{Z}$ sub forma $\mathbb{Z}=(-\mathbb{N}^*)\cup\mathbb{N}$ unde $-\mathbb{N}^*=\{-n : n\in\mathbb{N}^*\}$ sau $\mathbb{Z}=\{0, \pm1, \pm2, \ldots\}$. Vom nota $\mathbb{Z}^* = \mathbb{Z}\setminus\{0\}$.

2.2. Înmulţirea numerelor întregi

Lema 2.2.1. Fie $x, y, z, t, x', y', z', t'\in\mathbb{N}$ astfel încât $[x, y]=[x', y']$ şi

[z, t]=[z′, t′]. Atunci [xz+yt, xt+yz]=[x′z′+y′t′, x′t′+y′z′].

Demonstrație. Din ipoteză avem x+y′=y+x′ şi z+t′=z′+t astfel că

[xz+yt, xt+yz]=[x′z′+y′t′, x′t′+y′z′] ⇔ (xz+yt)+(x′t′+y′z′)=(xt+yz)+(x′z′+y′t′) ⇔ x(z-t)+y(t-z)=x′(z′-t′)+y′(t′-z′) ⇔ (x-y)(z-t)=(x′-y′)(z′-t′) ceea ce este adevărat deoarece x-y=x′-y′ şi z-t=z′-t′. ■

Fie acum α=[x, y] şi β=[z, t] două numere întregi.

Definind α·β=[xz+yt, xt+yz], conform Lemei 2.2.1 deducem că această definiție este corectă .

Propoziția 2.2.2. (ℤ, +, ·) este domeniu de integritate.

Demonstrație. Conform celor de mai înainte (ℤ, +) este grup comutativ. Să demonstrăm acum că (ℤ, ·) este monoid comutativ iar pentru aceasta fie α=[x, y], α′=[x′, y′], α″=[x″, y″] trei elemente oarecare din ℤ.

Atunci :

α(α′α″)=[x,y][x′x″+y′y″,x′y″+y′x″]

=[x(x′x″+y′y″)+y(x′y″+y′x″), x(x′y″+y′x″)+y(x′x″+y′y″)]

=[xx′x″+xy′y″+x′yy″+x″yy′, xx′y″+xx″y′+x′x″y+yy′y″] iar

(αα′)α″=[xx′+yy′, xy′+x′y][x″, y″]

=[(xx′+yy′)x″+(xy′+x′y)y″, (xx′+yy′)y″+(xy′+x′y)x″]

=[xx′x″+xy′y″+x′yy″+x″yy′, xx′y″+xx″y′+x′x″y+yy′y″] ,

de unde deducem că α(α′α″)=(αα′)α″ adică înmulțirea numerelor întregi este asociativă.

În mod evident, αα′=α′α (deoarece înmulțirea numerelor naturale este comutativă), adică înmulțirea numerelor întregi este comutativă.

Deoarece α[1, 0]=[x, y][1, 0]=[x, y]=α, deducem că elementul neutru pentru înmulțirea numerelor întregi este [1, 0].

Să arătăm acum că înmulțirea numerelor întregi este distributivă față de adunarea numerelor întregi . Într – adevăr,

α(α′+α″) = [x, y][x′+x″ , y′+y″] = [x (x′+x″)+y(y′+y″), x(y′+y″)+y (x′+x″)]

= [xx′+xx″+yy′+yy″, xy′+xy″+yx′+yx″] iar

αα′+αα″ = [x, y][x′,y′]+[x, y] [x″, y″] = [xx′+yy′, xy′+yx′]+[xx″+yy″, xy″+yx″]

= [xx′+yy′+xx″+yy″, xy′+yx′+xy″+yx″] de unde se observă că

α(α′+α″) = αα′+αα″ .

Am probat până acum că (ℤ, +, ·) este un inel comutativ unitar. Pentru a arăta că inelul ℤ nu are divizori ai lui zero, fie αα′=0=[0, 0] cu α≠0. Atunci xx′+yy′=xy′+x′y, de unde (x-y)(x′-y′)=0. Cum α≠0 (adică x-y≠0) rezută că x′-y′=0 ⇔x′=y′⇔ α′=0. ■

2.3. Relația de ordine naturală de pe ℤ

Definiția 2.3.1. Pentru x, y∈ℤ definim relația ≤ prin x≤y ⇔ y-x∈ℕ.

Teorema 2.3.2. Dubletul (ℤ, ≤) este mulțime total ordonată.

Demonstrație. Fie $x, y, z \in \mathbb{Z}$; deoarece $x-x=0 \in \mathbb{N}$ deducem că $x \leq x$.

Dacă $x \leq y$ şi $y \leq x$ atunci există $m, n \in \mathbb{N}$ astfel încât $y-x=m$ şi $x-y=n$, de unde $m+n=0$ şi deci $m=n=0$, adică $x=y$.

Dacă $x \leq y$ şi $y \leq z$, atunci există $m, n \in \mathbb{N}$ astfel încât $x+m=y$ şi $y+n=z$.

Cum $x+(m+n)=z$ deducem că $x \leq z$, adică $(\mathbb{Z}, \leq)$ este o mulțime ordonată. Faptul că ordonarea de pe $\mathbb{Z}$ este totală rezultă din aceea că $\mathbb{Z}=(-\mathbb{N}^*) \cup \mathbb{N}$ iar $(-\mathbb{N}^*) \cap \mathbb{N}=\emptyset$. ■

Observație. Din felul în care am definit relația de ordine $\leq$ pe $\mathbb{Z}$ deducem că $\mathbb{N}=\{x \in \mathbb{Z} : x \geq 0\}$ iar $-\mathbb{N}=\{x \in \mathbb{Z} : x \leq 0\}$.

Propoziția 2.3.3. Fie $x, y, z \in \mathbb{Z}$ astfel încât $x \leq y$.
Atunci (i) $-y \leq -x$
(ii) dacă $z \geq 0$ atunci $xz \leq yz$
(iii) dacă $z \leq 0$ atunci $xz \geq yz$.

Demonstrație. (i). Din $x \leq y$ deducem că $y-x \in \mathbb{N}$ şi cum $(-x)-(-y)=y-x \in \mathbb{N}$ rezultă că $-y \leq -x$.

(ii). Cum $y-x \in \mathbb{N}$ şi $z \in \mathbb{N}$ avem $(y-x)z \in \mathbb{N}$ adică $yz-xz \in \mathbb{N}$, deci $xz \leq yz$.

(iii). Cum $-z \in \mathbb{N}$ şi $y-x \in \mathbb{N}$ deducem că şi $(y-x)(-z) \in \mathbb{N}$ iar cum $(y-x)(-z)=xz-yz \in \mathbb{N}$ rezultă că $xz \geq yz$. ■