DUMITRU BUŞNEAG **DANA PICIU**

LECȚII
de
ALGEBRĂ

Editura UNIVERSITARIA
CRAIOVA
2002

Referenți ştiințifici:
Prof.univ.dr.Constantin Năstăsescu,Universitatea Bucuresti
Membru corespondent al Academiei Române
Prof.univ.dr. Constantin Niță,Universitatea Bucureşti

Tehnoredactare computerizată : Dana Piciu, Livia Popescu
Copertă: Cătălin Buşneag

Descrierea CIP a Bibliotecii Naționale

Dumitru Buşneag (coordonator),

Lecții de Algebra

527 p.; 21 cm.
Craiova – Editura Universitaria – 2002
Bibliogr.
512.54,55,56,58,553,516.62,64
ISBN **973 – 8043 –109 – 8**

Bun de tipar: 20.02.2002
Tipografia Universității din Craiova, Strada, Al. Cuza, nr.13
Craiova, România

Published in Romania by:
EDITURA UNIVERSITARIA CRAIOVA

ISBN: 973 – 8043 – 109 – 8

CUPRINS

pag.

CONTENTS

pag

CAPITOLUL 1: NOȚIUNI PRELIMINARII

§1 Mulțimi. Operații cu mulțimi

În cadrul acestei lucrări vom privi mulțimile în sensul în care ele au fost privite de către GEORG CANTOR - primul matematician care a inițiat studiul lor sistematic (punct de vedere cunoscut în matematică sub numele de *teoria naivă a mulțimilor).*

Despre paradoxurile ce le implică acest punct de vedere şi felul în care ele pot fi eliminate, rugăm cititorul să consulte lucrările [16] şi [30].

Definiția 1.1. Dacă A şi B sunt două mulțimi, vom spune că A este *inclusă* în B (sau că A este *submulțime* a lui B) dacă elementele lui A sunt şi elemente ale lui B; în acest caz vom scrie $A \subseteq B$ iar în caz contrar $A \not\subseteq B$.

Avem deci : $A \subseteq B \Leftrightarrow$ pentru orice $x \in A \Rightarrow x \in B$

$A \not\subseteq B \Leftrightarrow$ există $x \in A$ a.î. $x \notin B$.

Vom spune despre mulțimile A şi B că sunt *egale* dacă oricare ar fi x, $x \in A \Leftrightarrow x \in B$. Deci, $A = B \Leftrightarrow A \subseteq B$ şi $B \subseteq A$.

Vom spune că A este *inclusă strict* în B şi vom scrie $A \subset B$ dacă $A \subseteq B$ şi $A \neq B$.

Se acceptă existența unei mulțimi ce nu conține nici un element care se notează prin $\emptyset$ şi poartă numele de *mulțimea vidă*. Se observă că pentru orice mulțime A, $\emptyset \subseteq A$ (deoarece în caz contrar ar trebui să existe $x \in \emptyset$ a.î. $x \notin A$ – absurd.!).

O mulțime diferită de mulțimea vidă se zice *nevidă.*

Pentru o mulțime T, vom nota prin $\mathbf{P}(T)$ mulțimea submulțimilor sale (evident $\emptyset$, $T \in \mathbf{P}(T)$).

Următorul rezultat este imediat :

Dacă T este o mulțime oarecare iar A, B, C∈P(T), atunci :

(i) A⊆A

(ii) Dacă A⊆B şi B⊆A, atunci A=B

(iii) Dacă A⊆B şi B⊆C, atunci A⊆C.

În cadrul acestei lucrări vom utiliza deseori noțiunea de *familie* de elemente a unei mulțimi indexată de o mulțime nevidă de indici I (prin aceasta înțelegând o funcție definită pe mulțimea I cu valori în mulțimea respectivă).

Astfel, vom scrie de exemplu $(x_i)_{i\in I}$ pentru a desemna o familie de elemente ale unei mulțimi sau $(A_i)_{i\in I}$ pentru a desemna o familie de mulțimi indexată de mulțimea I. Pentru o mulțime T şi A, B∈**P**(T) definim :

$$A\cap B=\{x\in T \mid x\in A \text{ şi } x\in B\}$$

$$A\cup B=\{x\in T \mid x\in A \text{ sau } x\in B\}$$

$$A\setminus B=\{x\in T \mid x\in A \text{ şi } x\notin B\}$$

$$A\triangle B=(A\setminus B)\cup(B\setminus A).$$

Dacă $A\cap B=\emptyset$, mulțimile A şi B se zic *disjuncte*.

Operațiile $\cap$, $\cup$, $\setminus$ şi $\triangle$ poartă numele de *intersecție, reuniune, diferență* şi *diferență simetrică*.

În particular, $T\setminus A$ se notează prin $\complement_T(A)$ (sau $\complement(A)$ dacă nu este pericol de confuzie) şi poartă numele de *complementara lui A în T*.

În mod evident, pentru A, B∈**P**(T) avem:

$$A\setminus B=A\cap\complement_T(B)$$

$$A\triangle B=(A\cup B)\setminus(A\cap B)=(A\cap\complement_T(B))\cup(\complement_T(A)\cap B)$$

$$\complement_T(\emptyset)=T,\quad \complement_T(T)=\emptyset$$

$$A\cup\complement_T(A)=T,\ A\cap\complement_T(A)=\emptyset \text{ iar } \complement_T(\complement_T(A))=A.$$

De asemenea, pentru x∈T avem:

$$x\notin A\cap B \Leftrightarrow x\notin A \text{ sau } x\notin B$$

$$x\notin A\cup B \Leftrightarrow x\notin A \text{ şi } x\notin B$$

$$x\notin A\setminus B \Leftrightarrow x\notin A \text{ sau } x\in B$$

$x \notin A \triangle B \Leftrightarrow (x \notin A$ şi $x \notin B)$ sau $(x \in A$ şi $x \in B)$

$x \notin \complement_T(A) \Leftrightarrow x \in A.$

Din cele de mai înainte deducem imediat că dacă $A, B \in \mathbf{P}(T)$, atunci:

$$\complement_T(A \cap B) = \complement_T(A) \cup \complement_T(B) \text{ şi } \complement_T(A \cup B) = \complement_T(A) \cap \complement_T(B).$$

Aceste ultime două egalităţi sunt cunoscute sub numele de *relaţiile lui De Morgan.*

Pentru o familie nevidă $(A_i)_{i \in I}$ de submulţimi ale lui T definim:

$$\bigcap_{i \in I} A_i = \{x \in T \mid x \in A_i \text{ pentru orice } i \in I\} \text{ şi}$$

$$\bigcup_{i \in I} A_i = \{x \in T \mid \text{există } i \in I \text{ a.î. } x \in A_i\}.$$

Astfel, relaţiile lui De Morgan sunt adevărate într-un context mai general:

Dacă $(A_i)_{i \in I}$ este o familie de submulţimi ale mulţimii T, atunci:

$$C_T\left(\bigcap_{i \in I} A_i\right) = \bigcup_{i \in I} C_T(A_i) \text{ şi } C_T\left(\bigcup_{i \in I} A_i\right) = \bigcap_{i \in I} C_T(A_i).$$

Următorul rezultat este imediat:

Propoziţia 1.2. Dacă T o mulţime iar A, B, C∈P(T), atunci:

(i) A∩(B∩C)=(A∩B)∩C şi A∪(B∪C)=(A∪B)∪C

(ii) A∩B=B∩A şi A∪B=B∪A

(iii) A∩T=A şi A∪∅=A

(iv) A∩A=A şi A∪A=A.

Observaţia 1.3. 1. Din (i) deducem că operaţiile $\cup$ şi $\cap$ sunt *asociative*, din (ii) deducem că ambele sunt *comutative*, din (iii) deducem că T şi $\emptyset$ sunt elementele neutre pentru $\cap$ şi respectiv pentru $\cup$, iar din (iv) deducem că $\cap$ şi $\cup$ sunt operaţii *idempotente* pe $\mathbf{P}(T)$.

2. Prin dublă incluziune se probează imdiat că pentru oricare A, B, $C \in \mathbf{P}(T)$ avem:

$$A\cap(B\cup C)=(A\cap B)\cup(A\cap C) \quad \text{şi}$$
$$A\cup(B\cap C)=(A\cup B)\cap(A\cup C),$$

adică operațiile de intersecție şi reuniune sunt *distributive* una față de cealaltă.

Propoziția 1.4. Dacă A, B, C∈P(T), atunci:

(i) $A\triangle(B\triangle C)=(A\triangle B)\triangle C$

(ii) $A\triangle B=B\triangle A$

(iii) $A\triangle\emptyset=A$ **iar** $A\triangle A=\emptyset$

(iv) $A\cap(B\triangle C)=(A\cap B)\triangle(A\cap C)$.

*Demonstrație. (*i). Prin dublă incluziune se arată imediat că:

$A\triangle(B\triangle C)=(A\triangle B)\triangle C=[A\cap\complement_T(B)\cap\complement_T(C)]\cup[\complement_T(A)\cap B\cap\complement_T(C)]\cup$
$\cup[\complement_T(A)\cap\complement_T(B)\cap C]\cup(A\cap B\cap C)$.

(ii), (iii) sunt evidente.

(iv). Se probează fie prin dublă incluziune, fie ținând cont de distributivitatea intersecției față de reuniune. ■

Definiția 1.5. Fiind date două obiecte x şi y se numeşte *pereche ordonată* a obiectelor x şi y mulțimea notată (x, y) şi definită astfel:

$$(x, y)=\{\{x\},\{x, y\}\}.$$

Se verifică acum imediat că dacă x şi y sunt două obiecte a.î. $x\neq y$, atunci $(x, y)\neq(y, x)$ iar dacă (x, y) şi (u, v) sunt două perechi ordonate, atunci $(x, y)=(u, v) \Leftrightarrow x=u$ şi $y=v$; în particular, $(x, y)=(y, x) \Rightarrow x=y$.

Definiția 1.6. Dacă A şi B sunt două mulțimi, mulțimea notată $A\times B=\{(a, b) \mid a\in A$ şi $b\in B\}$ se va numi *produsul cartezian* al mulțimilor A şi B.

În mod evident:

$$A\times B\neq\emptyset \Leftrightarrow A\neq\emptyset \text{ şi } B\neq\emptyset$$

$$A\times B=\emptyset \Leftrightarrow A=\emptyset \text{ sau } B=\emptyset$$

$$A\times B=B\times A \Leftrightarrow A=B$$

$$A'\subseteq A \text{ şi } B'\subseteq B \Rightarrow A'\times B'\subseteq A\times B.$$

Dacă A, B, C sunt trei mulțimi vom defini produsul lor cartezian prin egalitatea : $A\times B\times C=(A\times B)\times C$.

Elementul ((a, b), c) din $A\times B\times C$ îl vom nota mai simplu prin (a, b, c).

Mai general, dacă $A_1, A_2, ..., A_n$ ($n\geq 3$) sunt mulțimi punem

$$A_1\times A_2\times ...\times A_n = ((...((A_1\times A_2)\times A_3)\times ...)\times A_n).$$

Dacă A este o mulțime finită, vom nota prin |A| numărul de elemente ale lui A. În mod evident, dacă A şi B sunt submulțimi finite ale unei mulțimi M atunci şi $A\cup B$ este submulțime finită a lui M iar

$$|A\cup B|=|A|+|B|-|A\cap B|.$$

Vom prezenta în continuare un rezultat mai general cunoscut sub numele de *principiul includerii şi excluderii*:

Propoziția 1.7. Fie M o mulțime finită iar $M_1, M_2, ..., M_n$ submulțimi ale lui M. Atunci :

$$\left|\bigcup_{i=1}^{n} M_i\right| = \sum_{1\leq i\leq n}|M_i| - \sum_{1\leq i<j\leq n}|M_i\cap M_j| + \sum_{1\leq i<j<k\leq n}|M_i\cap M_j\cap M_k| -$$
$$-....+(-1)^{n-1}|M_1\cap ...\cap M_n|.$$

Demonstrație. Facem inducție matematică după n. Pentru $n=1$ egalitatea din enunț se reduce la $|M_1|=|M_1|$, ceea ce este evident. Pentru $n=2$ trebuie demonstrată egalitatea :

$$(1) \quad |M_1\cup M_2|=|M_1|+|M_2|-|M_1\cap M_2|$$

care de asemenea este adevărată, deoarece elementele din $M_1\cap M_2$ apar atât la M_1 cât şi la M_2.

Presupunem egalitatea din enunț adevărată pentru oricare m submulțimi ale lui M cu $m<n$ şi o să o demonstrăm pentru n submulțimi $M_1, M_2, ..., M_n$.

Dacă notăm $N = \bigcup_{i=1}^{n-1} M_i$, atunci conform relației (1) putem scrie:

$$(2)\quad \left|\bigcup_{i=1}^{n} M_i\right| = |N \cup M_n| = |N| + |M_n| - |N \cap M_n|.$$

Însă $N \cap M_n = \left(\bigcup_{i=1}^{n-1} M_i\right) \cap M_n = \bigcup_{i=1}^{n-1} (M_i \cap M_n)$, deci aplicând ipoteza de inducție pentru $\bigcup_{i=1}^{n-1} (M_i \bigcap M_n)$ şi ținând seama de faptul că

$$(M_i \bigcap M_n) \bigcap (M_j \bigcap M_n) = (M_i \bigcap M_j) \bigcap M_n ,$$

$$(M_i \bigcap M_n) \bigcap (M_j \bigcap M_n) \bigcap (M_k \bigcap M_n) = (M_i \bigcap M_j \bigcap M_k) \bigcap M_n , \quad \text{etc,}$$

obținem:

$$(3)\quad \begin{aligned} |N \cap M_n| = \left|\bigcup_{i=1}^{n-1} (M_i \bigcap M_n)\right| &= \sum_{i=1}^{n-1} |M_i \bigcap M_n| - \sum_{1 \le i < j \le n-1} |M_i \bigcap M_j \bigcap M_n| + \\ &+ \sum_{1 \le i < j < k \le n-1} |M_i \bigcap M_j \bigcap M_k \bigcap M_n| - .... + (-1)^{n-2} \left|\bigcap_{i=1}^{n} M_i\right| \end{aligned}$$

Aplicând ipoteza de inducție şi pentru $|N|$ obținem:

$$(4)\quad \begin{aligned} |N| = \left|\bigcup_{i=1}^{n-1} M_i\right| &= \sum_{i=1}^{n-1} |M_i| - \sum_{1 \le i < j \le n-1} |M_i \bigcap M_j| + \\ &+ \sum_{1 \le i < j < k \le n-1} |M_i \bigcap M_j \bigcap M_k| - .... + (-1)^{n-2} \left|\bigcap_{i=1}^{n-1} M_i\right| \end{aligned}$$

astfel că ținând cont de (3) şi (4) relația (2) devine:

$$\left|\bigcup_{i=1}^{n} M_i\right| = |N| + |M_n| - |N \cap M_n| =$$

$$= \left(\sum_{i=1}^{n-1} |M_i| + |M_n|\right) - \left(\sum_{1\le i<j\le n-1} |M_i \bigcap M_j| + \sum_{i=1}^{n-1} |M_i \bigcap M_n|\right) +$$

$$+ \left(\sum_{1\le i<j<k\le n-1} |M_i \bigcap M_j \bigcap M_k| + \sum_{1\le i<j\le n-1} |M_i \bigcap M_j \bigcap M_n|\right) - \ldots +$$

$$+ \left[(-1)^{n-2} \left|\bigcap_{i=1}^{n-1} M_i\right|\right] -$$

$$- (-1)^{n-3} \sum_{1\le i_1<i_2<\ldots<i_{n-2}\le n-1} |M_{i_1} \bigcap M_{i_2} \bigcap \ldots \bigcap M_{i_{n-2}} \bigcap M_n| -$$

$$- (-1)^{n-2} \left|\bigcap_{i=1}^{n} M_i\right| = \sum_{i=1}^{n} |M_i| - \sum_{1\le i<j\le n} |M_i \bigcap M_j| +$$

$$+ \sum_{1\le i<j<k\le n} |M_i \bigcap M_j \bigcap M_k| - \ldots + (-1)^{n-1} \left|\bigcap_{i=1}^{n} M_i\right|.$$

Conform principiului inducției matematice, egalitatea din enunț este adevărată pentru orice număr natural n nenul. ■

§2 Relații binare pe o mulțime. Relații de echivalență

Definiția 2.1. Dacă A este o mulțime, numim *relație binară* pe A orice submulțime ρ a produsului cartezian A×A. Dacă a, b∈A şi (a, b)∈ρ vom spune că elementul a *este în relația* ρ cu b.

De asemenea, vom scrie aρb pentru a desemna faptul că (a, b)∈ρ.

Pentru mulțimea A vom nota prin **Rel** (A) mulțimea relațiilor binare de pe A (evident, **Rel** (A)=**P**(A×A)).

Relația Δ_A={ (a, a) | a∈A} poartă numele de *diagonala* produsului cartezian A×A.

Pentru ρ∈**Rel** (A) definim ρ^{-1}={(a, b)∈A×A | (b, a)∈ρ}.

În mod evident, $(\rho^{-1})^{-1}=\rho$ iar dacă mai avem $\rho'\in$**Rel** (A) a.î. $\rho\subseteq\rho'\Rightarrow \rho^{-1}\subseteq\rho'^{-1}$.

Definiția 2.2. Pentru $\rho, \rho'\in$Rel (A) definim *compunerea* lor $\rho\circ\rho'$ prin $\rho\circ\rho'=\{(a, b)\in A\times A \mid$ există $c\in A$ a.î. $(a, c)\in\rho'$ şi $(c, b)\in\rho\}$.

Rezultatul următor este imediat:

Propoziția 2.3. Fie $\rho, \rho', \rho''\in$Rel (A). Atunci:

(i) $\rho\circ\Delta_A=\Delta_A\circ\rho=\rho$

(ii) $(\rho\circ\rho')\circ\rho''=\rho\circ(\rho'\circ\rho'')$

(iii) $\rho\subseteq\rho'\Rightarrow \rho\circ\rho''\subseteq\rho'\circ\rho''$ şi $\rho''\circ\rho\subseteq\rho''\circ\rho'$

(iv) $(\rho\circ\rho')^{-1}=\rho'^{-1}\circ\rho^{-1}$

(v) $(\rho\cup\rho')^{-1}=\rho^{-1}\cup\rho'^{-1}$; mai general, dacă $(\rho_i)_{i\in I}$ este o familie de relații binare pe A, atunci

$$\left(\bigcup_{i\in I}\rho_i\right)^{-1}=\bigcup_{i\in I}\rho_i^{-1}\ .$$

Pentru $n\in\mathbb{N}$ şi $\rho\in$**Rel** (A) definim :

$$\rho^n=\begin{cases}\Delta_A \ \ pentru\ \ n=0\\ \underbrace{\rho\circ\rho\circ....\circ\rho}_{n\ ori}\ \ pentru\ \ n>1\end{cases}.$$

Se probează imediat că dacă m, $n\in\mathbb{N}$ atunci $\rho^m\circ\rho^n=\rho^{m+n}$.

Definiția 2.4. Vom spune despre o relație $\rho\in$Rel (A) că este:

i) *reflexivă* dacă $\Delta_A\subseteq\rho$

ii*) simetrică* dacă $\rho\subseteq\rho^{-1}$

iii) *antisimetrică* dacă $\rho\cap\rho^{-1}\subseteq\Delta_A$

iv) *tranzitivă* dacă $\rho^2\subseteq\rho$.

Rezultatul următor este imediat:

Propoziția 2.5. O relație $\rho \in Rel(A)$ este reflexivă (simetrică, antisimetrică, tranzitivă) dacă şi numai dacă ρ^{-1} este reflexivă (simetrică, antisimetrică, tranzitivă) .

Definiția 2.6. Vom spune despre o relație $\rho \in Rel(A)$ că este o *echivalență* pe A dacă este reflexivă, simetrică şi tranzitivă.

Vom nota prin **Echiv** (A) mulțimea relațiilor de echivalență de pe A. Evident, Δ_A, $A \times A \in$ **Echiv** (A).

Propoziția 2.7. Dacă $\rho \in$ Echiv (A) , atunci $\rho^{-1}=\rho$ şi $\rho^2=\rho$.

Demonstrație. Cum ρ este simetrică $\rho \subseteq \rho^{-1}$. Dacă $(a, b) \in \rho^{-1}$, atunci $(b, a) \in \rho \subseteq \rho^{-1} \Rightarrow (b, a) \in \rho^{-1} \Rightarrow (a, b) \in \rho$, adică $\rho^{-1} \subseteq \rho$, deci $\rho^{-1}=\rho$. Cum ρ este tranzitivă avem $\rho^2 \subseteq \rho$. Fie acum $(x, y) \in \rho$. Din $(x, x) \in \rho$ şi $(x, y) \in \rho \Rightarrow (x, y) \in \rho \circ \rho = \rho^2$, adică $\rho \subseteq \rho^2$, deci $\rho^2=\rho$. ■

Propoziția 2.8. Fie $\rho_1, \rho_2 \in$ Echiv (A). Atunci $\rho_1 \circ \rho_2 \in$ Echiv (A) dacă şi numai dacă $\rho_1 \circ \rho_2 = \rho_2 \circ \rho_1$. În acest caz $\rho_1 \circ \rho_2 = \bigcap_{\substack{\rho' \in Echiv(A) \\ \rho_1, \rho_2 \subseteq \rho'}} \rho'$.

Demonstrație. Dacă ρ_1 , $\rho_2 \in$ **Echiv** (A), atunci $(\rho_1 \circ \rho_2)^{-1}=\rho_1 \circ \rho_2$ conform Propoziției 2.7. Însă conform Propoziției 2.3. avem că $(\rho_1 \circ \rho_2)^{-1}= \rho_2^{-1} \circ \rho_1^{-1}= \rho_2 \circ \rho_1$, astfel că $\rho_1 \circ \rho_2 = \rho_2 \circ \rho_1$.

Invers, să presupunem că $\rho_1 \circ \rho_2 = \rho_2 \circ \rho_1$.

Cum $\Delta_A \subseteq \rho_1$, $\rho_2 \Rightarrow \Delta_A = \Delta_A \circ \Delta_A \subseteq \rho_1 \circ \rho_2$, adică $\rho_1 \circ \rho_2$ este reflexivă. Cum $(\rho_1 \circ \rho_2)^{-1}= \rho_2^{-1} \circ \rho_1^{-1} = \rho_2 \circ \rho_1 = \rho_1 \circ \rho_2$, deducem că $\rho_1 \circ \rho_2$ este şi simetrică. Din $(\rho_1 \circ \rho_2)^2=(\rho_1 \circ \rho_2) \circ (\rho_1 \circ \rho_2)=\rho_1 \circ (\rho_2 \circ \rho_1) \circ \rho_2= =\rho_1 \circ (\rho_1 \circ \rho_2) \circ \rho_2=\rho_1^2 \circ \rho_2^2= \rho_1 \circ \rho_2$ deducem că $\rho_1 \circ \rho_2$ este şi tranzitivă, adică este o echivalență pe A.

Să presupunem acum că $\rho_1 \circ \rho_2 = \rho_2 \circ \rho_1$ şi fie $\rho' \in$ **Echiv** (A) a.î. $\rho_1, \rho_2 \subseteq \rho'$.

Atunci $\rho_1 \circ \rho_2 \subseteq \rho' \circ \rho' = \rho'$, adică

$$\rho_1 \circ \rho_2 \subseteq \bigcap_{\substack{\rho' \in Echiv(A) \\ \rho_1, \rho_2 \subseteq \rho'}} \rho' \stackrel{def}{=} \theta$$

Cum ρ_1 , $\rho_2 \in$ **Echiv** (A) şi $\rho_1 \circ \rho_2 \in$ **Echiv** (A) $\Rightarrow \rho_1$, $\rho_2 \subseteq \rho_1 \circ \rho_2 \Rightarrow \theta \subseteq \rho_1 \circ \rho_2$ adică $\theta = \rho_1 \circ \rho_2$.■

Pentru $\rho \in$ **Rel** (A), definim *relaţia de ehivalenţă de pe A generată de* ρ ca fiind relaţia de echivalenţă

$$\langle \rho \rangle = \bigcap_{\substack{\rho' \in Echiv(A) \\ \rho \subseteq \rho'}} \rho' \ .$$

În mod evident, relaţia de echivalenţă $<\rho>$ este caracterizată de condiţiile $\rho \subseteq <\rho>$ iar dacă $\rho' \in$ **Echiv** (A) a.î. $\rho \subseteq \rho' \Rightarrow <\rho> \subseteq \rho'$ (altfel zis, $<\rho>$ este cea mai mică relaţie de echivalenţă ce include pe ρ).

Lema 2.9. Fie $\rho \in$ Rel(A) şi $\overline{\rho} = \Delta_A \cup \rho \cup \rho^{-1}$. Atunci relaţia $\overline{\rho}$ are următoarele proprietăţi:

(i) $\rho \subseteq \overline{\rho}$

(ii) $\overline{\rho}$ **este reflexivă şi simetrică**

(iii) dacă ρ' este o altă relaţie binară de pe A reflexivă şi simetrică a.î. $\rho \subseteq \rho'$, atunci $\overline{\rho} \subseteq \rho'$.

Demonstraţie. (i). este evidentă .

(ii). Cum $\Delta_A \subseteq \overline{\rho}$ deducem că $\overline{\rho}$ este reflexivă iar cum $\overline{\rho}^{-1} = (\Delta_A \cup \rho \cup \rho^{-1})^{-1} = \Delta_A^{-1} \cup \rho^{-1} \cup (\rho^{-1})^{-1} = \Delta_A \cup \rho \cup \rho^{-1} = \overline{\rho}$ deducem că $\overline{\rho}$ este şi simetrică.

(iii). Dacă ρ' este reflexivă şi simetrică a.î. $\rho \subseteq \rho'$, atunci $\rho^{-1} \subseteq \rho'^{-1} = \rho'$ şi cum $\Delta_A \subseteq \rho'$ deducem că $\overline{\rho} = \Delta_A \cup \rho \cup \rho^{-1} \subseteq \rho'$.■

Lema 2.10. Fie $\rho \in$ Rel(A) reflexivă şi simetrică iar $\overline{\rho} = \bigcup_{n \geq 1} \rho^n$.

Atunci $\overline{\rho}$ are următoarele proprietăţi :

(i) $\rho \subseteq \overline{\rho}$

(ii) $\overline{\rho}$ **este o echivalenţă pe A**

(iii) Dacă $\rho' \in$ **Echiv(A) a.î.** $\rho \subseteq \rho'$**, atunci** $\overline{\rho} \subseteq \rho'$**.**

Demonstraţie. (i). este evidentă.

(ii). Cum $\Delta_A \subseteq \rho \subseteq \overline{\rho}$ deducem că $\Delta_A \subseteq \overline{\rho}$, adică $\overline{\rho}$ este reflexivă. Deoarece ρ este simetrică şi pentru orice $n \in \mathbb{N}^*$ avem $(\rho^n)^{-1}=(\rho^{-1})^n=\rho^n$, deducem că

$$\overline{\rho}^{-1} = \left(\bigcup_{n\geq 1} \rho^n\right)^{-1} = \bigcup_{n\geq 1} \left(\rho^n\right)^{-1} = \bigcup_{n\geq 1} \rho^n = \overline{\rho},$$

adică $\overline{\rho}$ este şi simetrică. Fie acum $(x, y) \in \overline{\rho} \circ \overline{\rho}$; atunci există $z \in A$ a.î. $(x, z), (z, y) \in \overline{\rho}$, adică există $m, n \in \mathbb{N}^*$ a.î. $(x, z) \in \rho^m$ şi $(z, y) \in \rho^n$. Deducem imediat că $(x, y) \in \rho^n \circ \rho^m = \rho^{n+m} \subseteq \overline{\rho}$, adică $\overline{\rho}^2 \subseteq \overline{\rho}$, deci $\overline{\rho}$ este tranzitivă, adică $\overline{\rho} \in$ **Echiv** (A).

(iii). Fie acum $\rho' \in$ **Echiv** (A) a.î. $\rho \subseteq \rho'$**.** Cum $\rho^n \subseteq \rho'^n = \rho'$ pentru orice $n \in \mathbb{N}^*$ deducem că $\overline{\rho} = \bigcup_{n\geq 1} \rho^n \subseteq \rho'$. ■

Din Lemele 2.9. şi 2.10. deducem imediat:

Teorema 2.11. Dacă $\rho \in$ **Rel(A), atunci**

$$\langle \rho \rangle = \bigcup_{n\geq 1} \left(\Delta_A \cup \rho \cup \rho^{-1}\right)^n .$$

Propoziţia 2.12. Fie $\rho, \rho' \in$ **Rel (A). Atunci:**

(i) $(\rho \cup \rho')^2 = \rho^2 \cup \rho'^2 \cup (\rho \circ \rho') \cup (\rho' \circ \rho)$

(ii) Dacă $\rho, \rho' \in$ **Echiv (A) atunci** $\rho \cup \rho' \in$ **Echiv (A) dacă şi numai dacă** $\rho \circ \rho', \rho' \circ \rho \subseteq \rho \cup \rho'$**.**

Demonstraţie.

(i). Avem: $(x, y) \in (\rho \cup \rho')^2 = (\rho \cup \rho') \circ (\rho \cup \rho') \Leftrightarrow$ există $z \in A$ a.î. $(x, z) \in \rho \cup p'$ şi $(z, y) \in \rho \cup \rho' \Leftrightarrow [(x, z) \in \rho$ şi $(z, y) \in \rho]$ sau $[(x, z) \in \rho'$ şi $(z, y) \in \rho']$ sau $[(x, z) \in \rho'$ şi $(z, y) \in \rho]$ sau $[(x, z) \in \rho$ şi $(z, y) \in \rho']$

$\Leftrightarrow$ $(x, y)\in\rho^2$ sau $(x, y)\in\rho'^2$ sau $(x, y)\in\rho\circ\rho'$ sau $(x, y)\in\rho'\circ\rho$ $\Leftrightarrow$ $\Leftrightarrow(x, y)\in\rho^2\cup\rho'^2\cup(\rho\circ\rho')\cup(\rho'\circ\rho)$, de unde egalitatea cerută.

(ii).„$\Rightarrow$''. Avem că $\rho^2=\rho$, $\rho'^2=\rho'$ şi $(\rho\cup\rho')^2=\rho\cup\rho'$. Astfel, relația de la (i) devine: $\rho\cup\rho'=\rho\cup\rho'\cup(\rho\circ\rho')\cup(\rho'\circ\rho)$, deci $\rho\circ\rho'\subseteq\rho\cup\rho'$ şi $\rho'\circ\rho\subseteq\rho\cup\rho'$.

„$\Leftarrow$''. Utilizăm ipoteza din nou şi relația de la (i): $(\rho\cup\rho')^2=\rho^2\cup\rho'^2\cup(\rho\circ\rho')\cup(\rho'\circ\rho)=\rho\cup\rho'\cup(\rho\circ\rho')\cup(\rho'\circ\rho)\subseteq\rho\cup\rho'$, deci $\rho\cup\rho'$ este tranzitivă. Cum $\Delta_A\subseteq\rho$ şi $\Delta_A\subseteq\rho'\Rightarrow\Delta_A\subseteq\rho\cup\rho'$, adică $\rho\cup\rho'$ este reflexivă. Dacă $(x, y)\in\rho\cup\rho'\Rightarrow (x, y)\in\rho$ sau $(x, y)\in\rho'\Rightarrow (y, x)\in\rho$ sau $(y, x)\in\rho'\Rightarrow$ $(y, x)\in\rho\cup\rho'$, adică $\rho\cup\rho'$ este şi simetrică, deci o echivalență pe A. ■

Propoziția 2.13. Fie A o mulțime şi $\rho\in$Rel(A) având proprietățile:

(i) Pentru orice $x\in$A, există $y\in$A a.î. $(x, y)\in\rho$

(ii) $\rho\circ\rho^{-1}\circ\rho=\rho$

Atunci $\rho\circ\rho^{-1}$, $\rho^{-1}\circ\rho\in$Echiv (A).

Demonstrație.

Avem că $\rho\circ\rho^{-1}=\{(x, y)\mid$ există $z\in$A a.î. $(x, z)\in\rho^{-1}$ şi $(z, y)\in\rho\}$.

Deci, pentru a demonstra că $\Delta_A\subseteq\rho\circ\rho^{-1}$ ar trebui ca pentru orice $x\in$A, $(x, x)\in\rho\circ\rho^{-1}$ adică să existe $z\in$A a.î. $(z, x)\in\rho$, lucru asigurat de (i). Deducem că $\rho\circ\rho^{-1}$ este reflexivă (analog pentru $\rho^{-1}\circ\rho$).

Dacă $(x, y)\in\rho\circ\rho^{-1}\Rightarrow$ există $z\in$A a.î. $(x, z)\in\rho^{-1}$ şi $(z, y)\in\rho\Leftrightarrow$ există $z\in$A a.î. $(y, z)\in\rho^{-1}$ şi $(z, x)\in\rho\Leftrightarrow (y, x)\in\rho\circ\rho^{-1}$, adică $\rho\circ\rho^{-1}$ este simetrică (analog pentru $\rho^{-1}\circ\rho$). Cum $(\rho\circ\rho^{-1})\circ(\rho\circ\rho^{-1})=$ $=(\rho\circ\rho^{-1}\circ\rho)\circ\rho^{-1}=\rho\circ\rho^{-1}$ deducem că $\rho\circ\rho^{-1}$ este şi tranzitivă, deci este o echivalență. Analog pentru $\rho^{-1}\circ\rho$.■

Definiția 2.14. Dacă $\rho \in Echiv(A)$ şi $a \in A$, prin *clasa de echivalență* a lui a relativă la ρ înțelegem mulțimea

$$[a]_\rho = \{x \in A \mid (x, a) \in \rho\}$$

(cum ρ este în particular reflexivă deducem că $a \in [a]_\rho$, adică $[a]_\rho \neq \emptyset$ pentru orice $a \in A$).

Mulțimea $A/\rho = \{ [a]_\rho \mid a \in A \}$ poartă numele de *mulțimea factor* (sau *cât*) a lui A prin relația ρ.

Propoziția 2.15. Dacă $\rho \in Echiv(A)$, atunci:

(i) $\bigcup_{a \in A} [a]_\rho = A$

(ii) Dacă $a, b \in A$ atunci $[a]_\rho = [b]_\rho \Leftrightarrow (a, b) \in \rho$

(iii) Dacă $a, b \in A$, atunci $[a]_\rho = [b]_\rho$ sau $[a]_\rho \cap [b]_\rho = \emptyset$.

Demonstrație.

(i). Deoarece pentru orice $a \in A$, $a \in [a]_\rho$ deducem incluziunea de la dreapta la stânga; cum cealaltă incluziune este evidentă deducem egalitatea solicitată.

(ii). Dacă $[a]_\rho = [b]_\rho$, cum $a \in [a]_\rho$ deducem că $a \in [b]_\rho$ adică $(a, b) \in \rho$.

Fie acum $(a, b) \in \rho$ şi $x \in [a]_\rho$, adică $(x, a) \in \rho$. Datorită tranzitivității lui ρ deducem că $(x, b) \in \rho$, adică $x \in [b]_\rho$, deci $[a]_\rho \subseteq [b]_\rho$. Analog deducem că şi $[b]_\rho \subseteq [a]_\rho$, adică $[a]_\rho = [b]_\rho$.

(iii). Presupunem că $[a]_\rho \cap [b]_\rho \neq \emptyset$. Atunci există $x \in A$ a.î. $(x, a), (x, b) \in \rho$ şi astfel $(a, b) \in \rho$, deci $[a]_\rho = [b]_\rho$ (conform cu (ii)). ■

Definiția 2.16. Numim *partiție* a unei mulțimi M o familie $(M_i)_{i \in I}$ de submulțimi ale lui M ce verifică condițiile :

(i) Pentru $i, j \in I$, $i \neq j \Rightarrow M_i \cap M_j = \emptyset$

(ii) $\bigcup_{i \in I} M_i = M$ **.**

Observaţia 2.17. Din cele de mai înainte deducem că dacă ρ este o relaţie de echivalenţă pe mulţimea A, atunci mulţimea claselor de echivalenţă ale lui ρ pe A determină o partiţie a lui A.

§3 Relaţii funcţionale. Noţiunea de funcţie. Clase de funcţii.

Definiţia 3.1. Fie A şi B două mulţimi. O submulţime $R \subseteq A \times B$ se numeşte *relaţie funcţională* dacă :

(i) Pentru orice $a \in A$ există $b \in B$ a.î. $(a, b) \in R$

(ii) $(a, b), (a, b') \in R \Rightarrow b = b'$.

Numim *funcţie* (sau aplicaţie) un triplet $f = (A, B, R)$ unde A şi B sunt două mulţimi nevide iar $R \subseteq A \times B$ este o relaţie funcţională.

În acest caz, pentru fiecare element $a \in A$ există un unic element $b \in B$ a.î. $(a, b) \in R$. Convenim să notăm $b = f(a)$; elementul b se va numi *imaginea lui a* prin f. Mulţimea A se numeşte *domeniul (*sau *domeniul de definiţie* al lui f) iar B se numeşte *codomeniul* lui f şi spunem de obicei că f este o funcţie definită pe A cu valori în B scriind lucrul acesta prin $f: A \to B$ sau $A \xrightarrow{f} B$.

Relaţia funcţională R se mai numeşte şi *graficul* lui f (convenim să notăm pe R prin G_f, astfel că $G_f = \{(a, f(a)) \mid a \in A\}$.

Dacă $f : A \to B$ şi $f' : A' \to B'$ sunt două funcţii, vom spune că ele sunt *egale* (şi vom scrie $f = f'$) dacă $A = A'$, $B = B'$ şi $f(a) = f'(a)$ pentru orice $a \in A$. Pentru o mulţime A, funcţia $1_A : A \to A$, $1_A(a) = a$ pentru orice $a \in A$ poartă numele de *funcţia identică a lui A* (în particular, putem vorbi de funcţia identică a mulţimii vide $1_\emptyset$). Dacă $A = \emptyset$ atunci există o unică funcţie $f : \emptyset \to B$ (este de fapt incluziunea lui $\emptyset$ în B). Dacă $A \neq \emptyset$ şi $B = \emptyset$ atunci în mod evident nu există nici o funcţie de la A la B.

Dacă $f : A \to B$ este o funcţie iar $A' \subseteq A$ şi $B' \subseteq B$ atunci notăm:

$$f(A') = \{f(a) \mid a \in A'\} \text{ şi } f^{-1}(B') = \{a \in A \mid f(a) \in B'\}$$

(f (A′) se va numi *imaginea* lui A′ prin f iar $f^{-1}(B')$ *contraimaginea* lui B′ prin f).

În particular, notăm **Im**(f)=f (A). Evident, $f(\emptyset)=\emptyset$ şi $f^{-1}(\emptyset)=\emptyset$.

Definiția 3.2. Fiind date două funcții f:A→B şi g:B→C numim *compunerea* lor funcția notată g∘f:A→C şi definită prin (g∘f)(a)=g(f(a)) pentru orice a∈A.

Propoziția 3.3. Dacă avem trei funcții $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$ **atunci:**

(i) h∘(g∘f)=(h∘g)∘f

(ii) f∘1_A=1_B∘f=f.

Demonstrație. (i). Într-adevăr, avem că h∘(g∘f) şi (h∘g)∘f au pe A drept domeniu de definiție, pe D drept codomeniu şi pentru orice a∈A

$$(h\circ(g\circ f))(a)=((h\circ g)\circ f)(a)=h(g(f(a))).$$

(ii). este evidentă. ■

Propoziția 3.4. Fie f:A→B, A′, A′′⊆A, B′, B′′⊆B, $(A_i)_{i\in I}$, $(B_j)_{j\in J}$ două familii de submulțimi ale lui A şi respectiv B. Atunci:

(i) $A'\subseteq A''\Rightarrow f(A')\subseteq f(A'')$

(ii) $B'\subseteq B''\Rightarrow f^{-1}(B')\subseteq f^{-1}(B'')$

(iii) $f\left(\bigcap_{i\in I} A_i\right)\subseteq\bigcap_{i\in I} f(A_i)$

(iv) $f\left(\bigcup_{i\in I} A_i\right)=\bigcup_{i\in I} f(A_i)$

(v) $f^{-1}\left(\bigcap_{j\in J} B_j\right)=\bigcap_{j\in J} f^{-1}(B_j)$

(vi) $f^{-1}\left(\bigcup_{j\in J} B_j\right) = \bigcup_{j\in J} f^{-1}\left(B_j\right)$.

Demonstrație (i). Dacă b∈f(A′), atunci b=f(a) cu a∈A′ şi cum A′⊆A′′ deducem că b∈f(A′′), adică f(A′)⊆f(A′′).

(ii). Analog cu (i).

(iii). Deoarece pentru orice k∈I, $\bigcap_{i\in I} A_i \subseteq A_k$, conform cu (i) deducem că $f\left(\bigcap_{i\in I} A_i\right) \subseteq f\left(A_k\right)$ şi cum k este oarecare deducem că $f\left(\bigcap_{i\in I} A_i\right) \subseteq \bigcap_{i\in I} f\left(A_i\right)$.

(iv). Egalitatea cerută rezultă imediat din echivalențele :

$b\in f\left(\bigcup_{i\in I} A_i\right)$ ⇔ există $a\in\bigcup_{i\in I} A_i$ a.î. b=f(a) ⇔ există $i_0\in I$ a.î. $a\in A_{i_0}$ şi b=f(a)⇔ există $i_0\in I$ a.î. $b\in f(A_{i_0})$ ⇔ $b\in\bigcup_{i\in I} f\left(A_i\right)$.

(v). Totul rezultă din echivalențele $a\in f^{-1}\left(\bigcap_{j\in J} B_j\right)$ ⇔ $f(a)\in\bigcap_{j\in J} B_J$ ⇔ pentru orice j∈J, f(a)∈B_j ⇔ pentru orice j∈J, a∈$f^{-1}(B_j)$ ⇔$a\in\bigcap_{j\in J} f^{-1}\left(B_j\right)$.

(vi). Analog cu (iv). ■

Definiția 3.5. Despre o funcție f:A→B vom spune că este:

i*) injectivă,* dacă pentru orice a, a′∈A, a≠a′⇒f(a)≠f(a′) (echivalent cu f(a)=f(a′)⇒a=a′)

ii) *surjectivă,* dacă pentru orice b∈B, există a∈A a.î. b=f(a)

iii) *bijectivă,* dacă este simultan injectivă şi surjectivă.

Dacă f :A→B este bijectivă, funcția f^{-1}:B→A definită prin echivalența $f^{-1}(b)=a \Leftrightarrow b=f(a)$ (b∈B şi a∈A) poartă numele de *inversa* lui f.

Se verifică imediat că $f^{-1}\circ f=1_A$ şi $f\circ f^{-1}=1_B$.

Propoziția 3.6. Fie $f:A\to B$ şi $g:B\to C$ două funcții

(i) Dacă f şi g sunt injective (surjective; bijective) atunci g∘f este injectivă (surjectivă, bijectivă ; în acest ultim caz $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$)

(ii) Dacă g∘f este injectivă (surjectivă, bijectivă) atunci f este injectivă, (g este surjectivă; f este injectivă şi g este surjectivă).

Demonstrație.(i). Fie $a, a'\in A$ a.î. $(g\circ f)(a)=(g\circ f)(a')$**.** Atunci $g(f(a))=g(f(a'))$ şi cum g este injectivă deducem că $f(a)=f(a')$ iar cum şi f este injectivă deducem că $a=a'$, adică g∘f este injectivă.

Să presupunem acum că f şi g sunt surjective şi fie $c\in C$; cum g este surjectivă, $c=g(b)$ cu $b\in B$ şi cum şi f este surjectivă $b=f(a)$ cu $a\in A$ astfel că $c=g(b)=g(f(a))=(g\circ f)(a)$, adică g∘f este surjectivă.

Dacă f şi g sunt bijective atunci faptul că g∘f este bijectivă rezultă imediat din cele expuse mai sus. Pentru a proba în acest caz egalitatea $(g\circ f)^{-1} = f^{-1}\circ g^{-1}$, fie $c\in C$. Avem că $c=g(b)$ cu $b\in B$ şi $b=f(a)$ cu $a\in A$. Deoarece $(g\circ f)(a)=g(f(a))=g(b)=c$ deducem că $(g\circ f)^{-1}(c)=a=$ $=f^{-1}(b)=f^{-1}(g^{-1}(c))=(f^{-1}\circ g^{-1})(c)$, adică $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$.

(ii). Să presupunem că g∘f este injectivă şi fie $a, a'\in A$ a.î. $f(a)=f(a')$. Atunci $g(f(a))=g(f(a'))\Leftrightarrow(g\circ f)(a)=(g\circ f)(a')\Rightarrow a=a'$, adică f este injectivă.

Dacă g∘f este surjectivă, pentru $c\in C$, există $a\in A$ a.î. $(g\circ f)(a)=c \Leftrightarrow g(f(a))=c$, adică g este surjecție.

Dacă g∘f este bijecție atunci în particular g∘f este injecție şi surjecție, deci conform celor de mai sus cu necesitate f este injecție iar g surjecție. ■

Propoziția 3.7. Fie M şi N două mulțimi iar $f:M\to N$ o funcție. Între mulțimile P(M) şi P(N) se definesc funcțiile

f_* : P(M)→P(N), f^* : P(N)→P(M) prin $f_*(A)=f(A)$, ∀ A ∈P(M) şi $f^*(B)=f^{-1}(B)$, ∀ B∈P(N).

Următoarele afirmații sunt echivalente:

(i) f este injectivă

(ii) f_* este injectivă

(iii) $f^* \circ f_* = 1_{P(M)}$

(iv) f^* este surjectivă

(v) $f(A \cap B)=f(A) \cap f(B)$, ∀ A, B∈P(M)

(vi) $f(\complement_M A) \subseteq \complement_N f(A)$, ∀A∈P(M)

(vii) Dacă g, h:L →M sunt două funcții a.î. f∘g=f∘h, atunci g=h

(viii) Există o funcție g :N →M a.î. $g \circ f = 1_M$.

*Demonstrație.*Vom demonstra echivalența afirmațiilor astfel (i)⇒(ii)⇒(iii)⇒(iv)⇒(v)⇒(vi)⇒(vii)⇒(i) iar apoi (i)⇔(viii) .

(i)⇒(ii). Fie A, A′∈P(M) a.î. $f_*(A)=f_*(A') \Leftrightarrow f(A)=f(A')$.

Dacă x∈A, atunci f(x)∈f(A)⇒f(x)∈f(A′)⇒ există x′∈A′ a.î. f(x)=f(x′). Cum f este injectivă, rezultă x=x′∈A′, adică A⊆A′; analog A′⊆A, deci A=A′, adică f_* este injectivă.

(ii)⇒(iii). Pentru A∈P(M) trebuie demonstrat că $(f^* \circ f_*)(A)=A \Leftrightarrow f^{-1}(f(A))=A$. Incluziunea $A \subseteq f^{-1}(f(A))$ este valabilă pentru orice funcție f. Pentru cealaltă incluziune, dacă

$x \in f^{-1}(f(A)) \Rightarrow f(x) \in f(A) \Rightarrow$ există x′∈A a.î. $f(x)=f(x') \Rightarrow f_*(\{x\})=f_*(\{x'\}) \Rightarrow \{x\}=\{x'\} \Rightarrow x = x' \in A$, adică $f^{-1}(f(A)) \subseteq A$.

(iii)⇒(iv). Deoarece $f^* \circ f_* = 1_{P(M)}$, pentru orice A∈P(M), $f^*(f_*(A))=A$, deci notând $B=f_*(A) \in P(N)$ avem că $f^*(B)=A$, adică f^* este surjectivă.

(iv)⇒(v). Fie A, B∈P(M) şi A′, B′∈P(N) a.î. $A=f^{-1}(A')$ şi $B=f^{-1}(B')$. Atunci $f(A \cap B)=f(f^{-1}(A) \cap f^{-1}(B'))=f(f^{-1}(A' \cap B'))$.

Să arătăm că $f(f^{-1}(A')) \cap f(f^{-1}(B')) \subseteq f(f^{-1}(A' \cap B'))$.

Dacă $y\in f(f^{-1}(A'))\cap f(f^{-1}(B'))\Rightarrow y\in f(f^{-1}(A'))$ şi $y\in f(f^{-1}(B'))\Rightarrow$ există $x'\in f^{-1}(A')$ şi $x''\in f^{-1}(B')$ a.î. $y=f(x')=f(x'')$.

Cum $x'\in f^{-1}(A')$ şi $x''\in f^{-1}(B') \Rightarrow f(x')\in A'$ şi $f(x'')\in B'$, deci $y\in A'\cap B'$. Deoarece $y=f(x')\Rightarrow x'\in f^{-1}(A'\cap B')$, adică $y\in f(f^{-1}(A'\cap B'))$.

Astfel, $f(A\cap B)\supseteq f(A)\cap f(B)$ şi cum incluziunea $f(A\cap B)\subseteq f(A)\cap f(B)$ este adevărată pentru orice funcție deducem că $f(A\cap B)=f(A)\cap f(B)$.

(v)⇒(vi). Pentru $A\in P(M)$ avem

$f(A)\cap f(\complement_M A)=f(A\cap\complement_M A)=f(\emptyset)=\emptyset$, deci $f(\complement_M A)\subseteq\complement_N f(A)$.

(vi)⇒(vii). Fie $g, h : L\to M$ două funcții a.î. $f\circ g=f\circ h$ şi să presupunem prin absurd că există $x\in L$ a.î. $g(x)\neq h(x)$, adică $g(x)\in\complement_M\{h(x)\}$; atunci $f(g(x))\in f(\complement_M\{h(x)\})\subseteq\complement_N f(h(\{x\}))=\complement_N\{f(h(x))\}$ deci $f(g(x))\neq f(h(x)) \Leftrightarrow (f\circ g)(x)\neq(f\circ h)(x) \Leftrightarrow f\circ g\neq f\circ h$, ceea ce este absurd.

(vii)⇒(i). Fie $x, x'\in M$ a.î. $f(x)=f(x')$ şi să presupunem prin absurd că $x\neq x'$. Notând $L=\{x, x'\}$ şi definind $g, h : L\to M$, $g(x)=x$, $g(x')=x'$, $h(x)=x'$, $h(x')=x$, atunci $g\neq h$ şi totuşi $f\circ g=f\circ h$, ceea ce este absurd.

(i)⇒(viii). Definind $g:N\to M$, $g(y)=x$ dacă $y=f(x)$ cu $x\in M$ şi y_0 dacă $y\notin f(M)$, atunci datorită injectivității lui f, g este definită corect şi evident $g\circ f=1_M$.

(viii)⇒(i). Dacă $x, x'\in M$ şi $f(x)=f(x')$, atunci $g(f(x))=g(f(x'))\Rightarrow x=x'$, adică f este injectivă. ■

Propoziția 3.8. Cu notațiile de la propoziția precedentă, următoarele afirmații sunt echivalente:

(i) f este surjectivă

(ii) f_* este surjectivă

(iii) $f_*\circ f^*=1_{P(N)}$

(iv) f^* este injectivă

(v) $f(\complement_M A)\supseteq\complement_N f(A)$, $\forall A\in P(M)$

(vi) Dacă g, h:N→P sunt două funcţii a.î. g∘f=h∘f, atunci g=h

(vii) Există o funcţie g:N→M a.î. f∘g=1_N.

*Demonstraţie.*Vom demonstra echivalenţa afirmaţiilor astfel: (i)⇒(ii)⇒(iii)⇒(iv)⇒(v)⇒(vi)⇒(i) iar apoi (i)⇔(vii).

(i)⇒(ii). Fie B∈P(N) şi y∈B ; atunci există x_y∈M a.î. f(x_y)=y.

Notând A={x_y|y∈B}⊆M avem că f (A)=B ⇔f_*(A)=B.

(ii)⇒(iii). Avem de demonstrat că pentru orice B∈P(N), f (f^{-1}(B))=B . Incluziunea f (f^{-1} (B))⊆B este valabilă pentru orice funcţie f. Fie acum y∈B; cum f_* este surjectivă, există A⊆M a.î. f_*(A)={y}⇔f(A)={y}, deci există x∈A a.î. y=f(x) şi deoarece y∈B⇒ x∈f^{-1} (B)⇒y=f(x)∈f(f^{-1}(B)), de unde şi incluziunea B⊆f(f^{-1} (B)).

(iii)⇒(iv). Dacă B_1, B_2∈P(N) şi $f^*(B_1)=f^*(B_2)$, atunci $f_*(f^*(B_1))=f_*(f^*(B_2))$ ⇔$1_{P(N)}$ $(B_1)=1_{P(N)}$ (B_2)⇔$B_1=B_2$, adică f^* este injectivă.

(iv)⇒(v). Fie A⊆M ; a arăta că f($\complement_M$A)⊇$\complement_N$f (A), revine la f($\complement_M$A)∪f(A)=N ⇔ f($\complement_M$A∪A)=N⇔f(M)=N. Să presupunem prin absurd că există y_0∈N a.î. pentru orice x∈M, f(x)≠y_0 , adică f^{-1} ({y_0})=∅⇔f^*({y_0})=∅. Deoarece şi f^*(∅)=∅ ⇒ f^*({y_0})=f^*(∅) iar pentru că f^* este presupusă injectivă ar rezulta că {y_0}=∅, ceea ce este absurd.

(v)⇒(vi). În particular, pentru A=M ar trebui să avem

f($\complement_M$M)⊇$\complement_N$f (M)⇔ f(∅)⊇$\complement_N$f (M)⇔ ∅⊇$\complement_N$f (M)⇔f(M)=N.

Dacă g, h:N→P sunt două funcţii a.î. g∘f=h∘f, atunci pentru orice y∈N, există x∈M a.î. f(x)=y (căci f (M)=N) şi astfel g(y)=g(f(x))=(g∘f)(x)=(h∘f)(x)=h(f(x)) = h(y), adică g=h.

(vi)⇒(i). Presupunem prin absurd că există $y_0 \in N$ a.î. $f(x) \neq y_0$, pentru orice $x \in M$. Definim g, h : N→{0, 1} astfel : g(y)=0, pentru orice $y \in N$ şi $h(y) = \begin{cases} 0 \ \ pentru \ \ y \in N - \{y_0\} \\ 1 \ \ pentru \ \ y = y_0 \end{cases}$

Evident $g \neq h$ şi totuşi $g \circ f = h \circ f$, ceea ce este absurd, deci f este surjectivă.

(i)⇒(vii). Pentru fiecare $y \in N$ alegând câte un singur $x_y \in f^{-1}(\{y\})$, obținem astfel o funcție g : N→M, $g(y)=x_y$, pentru orice $y \in N$, ce verifică în mod evident relația $f \circ g = 1_N$.

(vii)⇒(i). Pentru $y \in N$, scriind că f(g(y))=y, rezultă y=f(x), cu $x=g(y) \in M$, adică f este surjectivă.■

Din propozițiile precedente obținem imediat:

Corolarul 3.9. Cu notațiile de la Propoziția 3.7., următoarele afirmații sunt echivalente:

(i) f este bijectivă

(ii) $f(\complement_M A) = \complement_N f(A), \ \forall A \in P(M)$

(iii) f_* **şi** f^* **sunt bijective**

(iv) Există o funcție $g: N \to M$ **a.î.** $f \circ g = 1_N$ **şi** $g \circ f = 1_M$**.**

Propoziția 3.10. Fie M o mulțime finită şi f:M→M o funcție. Următoarele afirmații sunt echivalente:

(i) f este injectivă

(ii) f este surjectivă

(iii) f este bijectivă .

Demonstrație. Vom demonstra următoarele implicații: (i)⇒(ii)⇒(iii)⇒(i).

(i)⇒(ii). Dacă f este injectivă, atunci f(M) şi M au acelaşi număr de elemente şi cum $f(M) \subseteq M$ rezultă că f (M)=M , adică f este şi surjectivă.

(ii)⇒(iii). Dacă f este surjectivă, atunci pentru orice element $y\in M$ va exista un unic element $x_y\in M$ a.î. $f(x_y)=y$ (căci în caz contrar ar rezulta contradicția că M ar avea mai multe elemente decât M), adică f este şi injectivă.

(iii)⇒(i). Evident. ■

Propoziția 3.11. Fie M şi N două mulțimi având m, respectiv n elemente. Atunci:

(i) Numărul funcțiilor definite pe M cu valori în N este egal cu n^m

(ii) Dacă m=n, atunci numărul funcțiilor bijective de la M la N este egal cu m!

(iii) Dacă m≤n, atunci numărul funcțiilor injective de la M la N este egal cu A_n^m

(iv) Dacă m≥n, atunci numărul funcțiilor surjective de la M la N este egal cu $n^m - C_n^1(n-1)^m + C_n^2(n-2)^m - \ldots + (-1)^{n-1}C_n^{n-1}$.

Demonstrație.(i). Facem inducție matematică după m; dacă m=1, mulțimea M va avea un singur element şi este clar că vom avea $n=n^1$ funcții de la M la N. Presupunem afirmația adevărată pentru mulțimile M ce au cel mult m-1 elemente.

Dacă M este o mulțime cu n elemente, putem scrie $M=M'\cup\{x_0\}$, cu $x_0\in M$ iar M' submulțime a lui M cu m-1 elemente.

Pentru orice $y\in N$ şi $g : M'\to N$ funcție, considerând $f_{g,y} : M\to N$, $f_{g,y}(x)=g(x)$ dacă $x\in M'$ şi y dacă $x=x_0$, deducem că oricărei funcții $g: M'\to N$ îi putem asocia n funcții distincte de la M la N ale căror restricții la M' sunt egale cu g. Aplicând ipoteza de inducție pentru funcțiile de la M' la N, deducem că de la M la N se pot defini $n\cdot n^{m-1}=n^m$ funcții.

(ii). Facem inducție matematică după m; dacă m =1, mulțimile M şi N vor avea câte un singur element şi vom avea o singură funcție bijectivă de la M la N.

Presupunem afirmația adevărată pentru toate mulțimile M' şi N' ambele având cel mult m-1 elemente şi fie M şi N mulțimi având fiecare

câte m elemente. Scriind $M=M'\cup\{x_0\}$, cu $x_0\in M$ iar M' submulțime a lui M cu m-1 elemente, atunci orice funcție bijectivă $f:M\to N$ este perfect determinată de valoarea $f(x_0)\in N$ precum şi de o funcție bijectivă $g:M'\to N'$, unde $N'=N\setminus\{f(x_0)\}$. Deoarece pe $f(x_0)$ îl putem alege în m moduri iar pe g în (m-1)! moduri (conform ipotezei de inducție) deducem că de la M la N putem defini $(m-1)!\cdot m=m!$ funcții bijective.

(iii). Dacă $f:M\to N$ este injectivă, atunci luând drept codomeniu pe $f(M)\subseteq N$, deducem că f determină o funcție bijectivă $\overline{f}:M\to f(M)$, $\overline{f}(x)=f(x)$, pentru orice $x\in M$, iar f(M) are m elemente. Reciproc, dacă vom alege în N o parte N′ a sa cu m elemente, atunci putem stabili m! funcții bijective de la M la N′ (conform cu (ii)). Cum numărul submulțimilor N′ ale lui N care au m elemente este egal cu C_n^m, rezultă că putem construi $m!\cdot C_n^m=A_n^m$ funcții injective de la M la N.

(iv). Să considerăm $M=\{x_1, x_2, ...,x_m\}$, $N=\{y_1, y_2, ...,y_n\}$ iar M_i mulțimea funcțiilor de la M la N a.î. y_i nu este imaginea nici unui element din M_i, i=1,2,...,n.

Astfel, dacă notăm prin F_m^n mulțimea funcțiilor de la M la N, mulțimea funcțiilor surjective S_m^n de la M la N va fi complementara mulțimii $M_1\cup M_2\cup..\ ...\cup M_n$ din F_m^n, deci conform Propoziției 1.7. avem egalitățile (1):

$$|S_m^n|=|F_m^n|-\left|\bigcup_{i=1}^n M_i\right|=n^m-\left|\bigcup_{i=1}^n M_i\right|=n^m-\sum_{i=1}^n|M_i|+\sum_{1\le i<j\le n}|M_i\cap M_j|-$$
$$-\sum_{1\le i<j<k\le n}|M_i\bigcap M_j\bigcap M_k|+....+(-1)^n|M_1\bigcap M_2\bigcap...\bigcap M_n|$$

Deoarece M_i este de fapt mulțimea funcțiilor definte pe M cu valori în $N\setminus\{y_i\}$, $M_i\cap M_j$ este mulțimea funcțiilor definite pe M cu valori în $N\setminus\{y_i, y_j\}$ ..., etc, conform punctului (i) avem că:

(2) $|M_i|=(n-1)^m$, $|M_i\cap M_j|=(n-2)^m$, ..., etc,

($|M_1\cap M_2\cap...\cap M_n|=0$, deoarece $M_1\cap M_2\cap...\cap M_n=\varnothing$).

Deoarece sumele ce apar în (1) au, respectiv, C_n^1, C_n^2, ..., C_n^n temeni egali, ținând cont de acest lucru şi de (2), relația (1) devine:

$$S_m^n = n^m - C_n^1(n-1)^m + C_n^2(n-2)^m - ... + (-1)^{n-1} C_n^{n-1}. \quad \blacksquare$$

Pentru o mulțime nevidă M şi A∈P(M) definim $\varphi_A : M \to \{0,1\}$,

$$\varphi_A(x) = \begin{cases} 0 \ \ daca \ x \notin A \\ 1 \ \ daca \ x \in A \end{cases}$$

pentru orice x∈M. Funcția φ_A poartă numele de *funcția caracteristică* a mulțimii A.

Propoziția 3.12. Dacă A, B∈P(M), atunci:

(i) $A=B \Leftrightarrow \varphi_A=\varphi_B$

(ii) $\varphi_\varnothing=0$, $\varphi_M=1$

(iii) $\varphi_{A\cap B}=\varphi_A \varphi_B$, $\varphi_A{}^2=\varphi_A$

(iv) $\varphi_{A\cup B}=\varphi_A+\varphi_B - \varphi_A \varphi_B$

(v) $\varphi_{A \setminus B}=\varphi_A - \varphi_A \varphi_B$, $\varphi_{C_M A}=1-\varphi_A$

(vi) $\varphi_{A \Delta B}=\varphi_A+\varphi_B - 2\varphi_A\varphi_B$.

Demonstrație.

(i).„⇒''. Evidentă.

„⇐''. Presupunem că $\varphi_A=\varphi_B$ şi fie x∈A; atunci $\varphi_A(x)= =\varphi_B(x)=1$, deci x∈B, adică A⊆B. Analog B⊆A, de unde A=B.

(ii). Evident.

(iii). Pentru x∈M putem avea următoarele situații: (x∉A, x∉B) sau (x∈A, x∉B) sau (x∉A, x∈B) sau (x∈A, x∈B). În fiecare situație în parte se verifică imediat relația $\varphi_{A\cap B}(x)=\varphi_A(x)\varphi_B(x)$.

Cum $A \cap A = A \Rightarrow \varphi_A = \varphi_A\varphi_A = \varphi_A{}^2$.

(iv), (v). Asemănător cu (iii).

(vi). Avem

$$\varphi_{A \Delta B} = \varphi_{(A \setminus B) \cup (B \setminus A)} = \varphi_{A \setminus B} + \varphi_{B \setminus A} - \varphi_{A \setminus B}\varphi_{B \setminus A} =$$

$$=\varphi_A-\varphi_A\varphi_B+\varphi_B-\varphi_B\varphi_A-\varphi_{(A\setminus B)\cap(B\setminus A)}=\varphi_A+\varphi_B-2\varphi_A\varphi_B$$

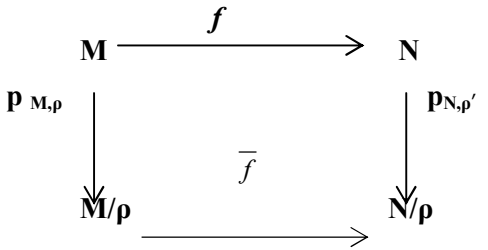
deoarece $(A\setminus B)\cap(B\setminus A)=\varnothing$. ■

Fie M o mulțime oarecare iar $\rho\in$**Echiv** (M). Funcția $p_{\rho,M}: M\to M/\rho$ definită prin $p_{\rho,M}(x)=[x]_\rho$ pentru orice $x\in M$ este surjectivă şi poartă numele de *surjecția canonică*.

Propoziția 3.13. Fie M şi N două mulțimi pe care s-au definit relațiile de echivalență ρ, respectiv ρ′ şi f : M→N o funcție având proprietatea:

$$(x, y)\in\rho \Rightarrow (f(x), f(y))\in\rho',\ \forall\ x, y\in M.$$

Atunci există o singură funcție $\overline{f}: M/\rho\to N/\rho'$ a. î. diagrama:



este comutativă (adică $p_{N,\rho'}\circ f=\overline{f}\circ p_{M,\rho}$, unde $p_{M,\rho}$, $p_{N,\rho}$, sunt surjecțiile canonice).

Demonstrație. Pentru $x\in M$, vom nota prin $[x]_\rho$ clasa de echivalență a lui x modulo relația ρ.

Pentru $x\in M$, definim: $\overline{f}([x]_\rho)=[f(x)]_{\rho'}$.

Dacă $x, y\in M$ a.î. $[x]_\rho=[y]_\rho \Leftrightarrow (x, y)\in\rho \Rightarrow [f(x), f(y)]\in\rho'$ (din enunț) $\Rightarrow [f(x)]_{\rho'}=[f(y)]_{\rho'}$, adică $\overline{f}$ este corect definită.

Dacă $x\in M$, atunci $(\overline{f}\circ p_{M,\rho})(x)=\overline{f}(p_{M,\rho}(x))=$

$=\overline{f}([x]_\rho)=[f[x]]_{\rho'}=p_{N,\rho'}(f(x))=(p_{N,\rho'}\circ f)(x)$, adică $p_{N,\rho'}\circ f=\overline{f}\circ p_{M,\rho}$.

Pentru a demonstra unicitatea lui $\overline{f}$, să presupunem că ar mai exista o funcție $\overline{f}'$: $M/\rho\to N/\rho'$ a.î. $p_{N,\rho'}\circ f=\overline{f}'\circ p_{M,\rho}$, şi fie $x\in M$.

Atunci $\overline{f}'([x]_\rho)=\overline{f}'(p_{M,\rho}(x))=(\overline{f}'\circ p_{M,\rho})(x)=(p_{N,\rho'}\circ f)(x)=$

$=p_{N,\rho'}(f(x))=[f(x)]_{\rho'}=\overline{f}'([x]_\rho)$, de unde deducem că $\overline{f}=\overline{f}'$. ■

Propoziția 3.14. Fie M şi N două mulțimi iar f :M→N o funcție ; notăm prin ρ_f relația binară de pe M definită astfel:

$$(x, y)\in\rho_f \Leftrightarrow f(x)=f(y) \quad (x, y\in M).$$

Atunci:

(i) ρ_f este relație de echivalență pe M

(ii) Există o unică funcție bijectivă $\overline{f}$: M / ρ_f→Im (f) a.î. i$\circ\overline{f}\circ p_{M,\rho_F}$ =f, i:Im (f) →N fiind incluziunea.

Demonstrație. (i). Evidentă (relația de egalitate fiind o echivalență pe M). (ii). Păstrând notația claselor de echivalență de la Propoziția 3.13., pentru x∈M definim $\bar{f}([x]_{\rho_f})=f(x)$. Funcția $\overline{f}$ este corect definită căci dacă x, y∈M şi $[x]_{\rho_f}=[y]_{\rho_f}\Leftrightarrow (x, y)\in\rho_f \Leftrightarrow f(x)=f(y)$ (de aici rezultă imediat şi injectivitatea lui $\overline{f}$) . Cum $\overline{f}$ este în mod evident şi surjectivă, deducem că $\overline{f}$ este bijectivă. Pentru a proba unicitatea lui $\overline{f}$, fie f_1 : M /ρ_f→Im (f) o altă funcție bijectivă a.î. i$\circ f_1\circ p_{M,\rho_F}$ =f şi x∈M. Atunci, $(i\circ f_1\circ p_{M,\rho_F})(x)=f(x) \Leftrightarrow$ $\Leftrightarrow f_1([x]_{\rho_f})=f(x)\Leftrightarrow f_1([x]_{\rho_f})=f(x)=\bar{f}([x]_{\rho_f})$, adică $f_1=\overline{f}$. ■

Propoziția 3.15. Fie M o mulțime finită cu m elemente. Atunci numărul $N_{m,k}$ al relațiilor de echivalență ce pot fi definite pe M a.î. mulțimea cât să aibă k elemente (k≤m) este dat de formula:

$$N_{m,k}=(1/k!)\cdot\left[k^m-C_k^1(k-1)^m+C_k^2(k-2)^m-\ldots+(-1)^{k-1}C_k^{k-1}\right].$$

Deci numărul relațiilor de echivalență ce pot fi definite pe mulțimea M este dat de formula $N=N_{m,1}+N_{m,2}+\ldots+N_{m,m}$.

Demonstrație. Dacă ρ este o relație de echivalență, ρ∈Echiv (M), atunci avem surjecția canonică $p_{M,\rho}$: M→M / ρ.

Dacă în general, f : M→N este o funcție surjectivă, atunci cum am stabilit în cazul Propoziției 3.14., aceasta dă naştere la următoarea relație de echivalență de pe M : $(x, y)\in\rho_f \Leftrightarrow f(x)=f(y)$. Mai mult, dacă g : N→N′ este o funcție bijectivă atunci relațiile ρ_f şi $\rho_{g\circ f}$ coincid căci $(x,y)\in\rho_{g\circ f}\Leftrightarrow(g\circ f)(x)=(g\circ f)(y)\Leftrightarrow g(f(x))=g(f(y))\Leftrightarrow f(x)=f(y)\Leftrightarrow$
$\Leftrightarrow(x, y)\in\rho_f$.

Deci, dacă N are k elemente, atunci k! funcții surjective de la M la N vor determina aceiaşi relație de echivalență pe M. Luând în particular N=M/ρ şi ținând cont de Propoziția 3.11. deducem că
$N_{m,k} = (1/k!)\cdot\left[k^m - C_k^1(k-1)^m + C_k^2(k-2)^m - \ldots + (-1)^{k-1}C_k^{k-1}\right]$. ■

Propoziția 3.16. Fie M o mulțime nevidă. Atunci funcția care asociază unei relații de echivalență definite pe M partiția lui M dată de relația de echivalență este bijectivă.

Demonstrație. Fie **Part** (M) mulțimea partițiilor lui M.

Vom nota prin f : **Echiv** (M)→**Part** (M) funcția ce asociază fiecărei relații de echivalență ρ de pe M, partiția lui M dată de clasele de echivalență modulo ρ: $f(\rho)=\{[x]_\rho \mid x\in M\}$.

Definim g : **Part** (M)→**Echiv** (M) astfel : dacă $P=(M_i)_{i\in I}$ este o partiție a lui M, definim relația g(P) pe M astfel :

$(x, y)\in g(P)\Leftrightarrow$ există i∈I a.î. x, y∈M_i .

Reflexivitatea şi simetria lui g(P) sunt imediate. Fie acum (x, y), (y, z)∈g(P). Există deci i_1 , $i_2\in I$ a. î. x, y∈M_{i_1} şi y, z∈M_{i_2} ; dacă $i_1\neq i_2$ ar rezulta că $M_{i_1}\bigcap M_{i_2}\neq\varnothing$ (căci ar conține pe y), ceea ce este absurd .

Deci $i_1=i_2=i$ şi astfel x, z∈M_i , adică (x, z) ∈ g(P) de unde concluzia că g (P) este şi tranzitivă, deci g(P)∈ **Echiv** (M), funcția g fiind astfel corect definită.

Să arătăm că dacă x∈M_i , atunci clasa de echivalență $\bar{x}$ modulo g (P) este egală cu M_i. Într-adevăr, y∈M_i ⇔ (x, y)∈g(P) ⇔ y∈$\bar{x}$ ⇔$M_i=\bar{x}$.

Deducem astfel că g este de fapt inversa lui f, adică f este bijectivă. ■

Suntem acum în măsură să facem anumite precizări legate de *mulțimea numerelor naturale.*

Definiția 3.17. 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 $0 \in P$ şi $(n \in P \Rightarrow s(n) \in P)$, atunci P=N .

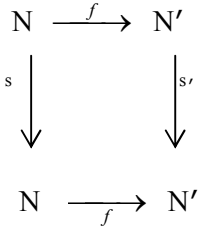
În cele ce urmează, acceptăm ca axiomă existența unui triplet Peano (cititorului dornic de aprofundarea acestei chestiuni îi recomandăm lucrarea [16]) .

Lema 3.18. Dacă (N, 0, s) este un triplet Peano, atunci $N=\{0\} \cup s(N)$.

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

Teorema 3.19. Fie (N, 0, s) un triplet Peano iar (N', $0'$, s') un alt triplet format dintr-o mulțime nevidă N', un element $0' \in N'$ şi o funcție $s':N' \to N'$. Atunci :

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



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 $R \subseteq N \times N'$ a.î. :

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

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 şi 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 $n \in N$ şi $f(n)=n' \in N'$, $(n , n') \in R_0$, 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 $n' \in N'$ a. î. $(n, n') \in R_0$ 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

$P=\{n \in N \mid \text{există } n' \in N' \text{ a. î. } (n, n') \in R_0\} \subseteq N$.

Cum $(0, 0') \in R_0$ deducem că $0 \in P$. Fie acum $n \in P$ şi $n' \in N'$ a.î. $(n, n') \in R_0$. Din definiția lui R_0 deducem că $(s(n), s'(n')) \in R_0$; obținem că $s(n) \in P$ şi cum (N, 0, s) este triplet Peano, deducem că P=N.

Pentru a doua parte, fie

$Q=\{n\in N$: dacă $n', n''\in N'$ 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 relația $R_1=R_0 \setminus\{(0, n')\}\subseteq N\times N'$. 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 $n', n''\in N'$ a. î. $(0, n'), (0 , n'')\in R_0$. Atunci, ținând cont de cele stabilite mai sus, deducem că $n'=n''=0'$, deci $0\in Q$.

Fie acum $n\in Q$ şi $n'\in N'$ a. î. $(n, n')\in R_0$; 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 relația $R_2 =R_0 \setminus\{(s (n), n'')\}$. 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 $f':N\to N'$ a.î. $f'(0)=0'$ şi $s'(f'(n))=f'(s(n))$ pentru orice $n\in N$.

Considerând $P=\{n\in N \mid f(n)=f'(n)\}\subseteq N$, 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 $P=\{n\in N \mid$ 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 $m\in N$ a. î. $f(0)=f(m)$ 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 $m\in N$ a.î. $f(m)=f(s(n))$.

Atunci $m\neq 0$ (căci în caz contrar ar rezulta că $0'=f(0)=f(s(n))=s'(f(n))$, absurd !), deci conform Lemei 3.18., $m=s(p)$ 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

$$P'=\{n'\in N' \mid \text{există } n\in N \text{ a. î. } n'=f(n)\}\subseteq N'.$$

Cum $f(0)=0'$ deducem că $0'\in P'$. Fie acum $n'\in P'$; atunci există $n\in N$ a.î. $n'=f(n)$. 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 . ■

Observaţia 3.20. Conform Teoremei 3.19. (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 $(\mathbb{N}, 0, s)$ pe care îl vom fixa ; elementele lui $\mathbb{N}$ le vom numi *numere naturale* .

Elementul 0 va purta numele de *zero* .

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 inducției matematice*).

Pe parcursul acestei lucrări vom construi – pornind de la o mulțime $\mathbb{N}$ a numerelor naturale – mulțimile numerelor *întregi* $\mathbb{Z}$, *raționale* $\mathbb{Q}$, *reale* $\mathbb{R}$ şi *complexe* $\mathbb{C}$, rezultând astfel rolul fundamental pe care îl joacă în matematică mulțimea numerelor naturale.

§4.Nucleul şi conucleul unei perechi de funcții

Definiția 4.1. Fie f, g : A→B o pereche de funcții. O pereche (K, i) formată dintr-o mulțime K şi o funcție i : K→A se numeşte *nucleul perechii (f, g)* dacă sunt verificate următoarele două condiții:

(i) $f\circ i=g\circ i$

(ii) Pentru oricare alt dublet (K', i') cu K' mulțime şi $i':K'\to A$ a.î. $f\circ i'= g\circ i'$ există o unică funcție $u : K'\to K$ a. î. $i\circ u=i'$.

Teorema 4.2. Pentru orice pereche de funcții f, g : A→B există un nucleu al perechii (f, g) unic până la o bijecție (unicitatea înseamnă că dacă (K, i) şi (K', i') sunt două nuclee pentru perchea (f, g) atunci există o bijecție $u : K\to K'$ a.î. $i'\circ u=i$).

Demonstrație. Să probăm la început existența nucleului şi pentru aceasta fie $K=\{x\in A\mid f(x)=g(x)\}$ iar $i : K\to A$ incluziunea (K putând fi chiar $\varnothing$).

În mod evident $f\circ i=g\circ i$. Fie acum (K', i') cu $i' : K'\to A$ a. î. $f\circ i'=g\circ i'$. Pentru $a\in K'$, cum $f(i'(a))=g(i'(a))$ deducem că $i'(a)\in K$. Definim atunci $u:K'\to K$ prin $u(a)=i'(a)$, pentru orice $a\in K'$ şi este clar că $i\circ u=i'$.

Dacă $u':K'\to K$ este o altă funcție a.î. $i\circ u'=i'$, atunci pentru $a\in K'$ avem $i(u'(a))=u(a)$, de unde $u'(a)=i'(a)=u(a)$, adică $u=u'$.

Să probăm acum unicitatea nucleului iar pentru aceasta fie (K, i) şi (K′, i′) două nuclee pentru perchea (f, g).

Cum (K′, i′) este nucleul perechii (f, g) deducem existența unei funcții u:K→K′ a.î. i′∘u=i.

Cum şi (K, i) este nucleul perechii (f, g) deducem existența unei funcții u′:K′→K a.î. i∘u′=i′.

Deducem imediat că i′∘(u∘u′)=i′ şi i∘(u′∘u)=i. Cum şi $i'\circ 1_{K'}=i'$ şi $i\circ 1_K=i$, ținând cont de unicitatea din Definiția 4.1., deducem că $u\circ u'=1_{K'}$ şi $u'\circ u=1_K$, adică u este bijecție şi i′∘u=i . ■

Observația 4.3. Vom nota (K, i) = Ker (f, g) (iar dacă nu este pericol de confuzie doar K=Ker (f, g)).

Definiția 4.4. Fiind dată o pereche de funcții f, g :A→B numim *conucleu* al perchii (f, g) pereche (P, p) formată dintr-o mulțime P şi o funcție p:B→P ce verifică următoarele două condiții :

(i) p∘f=p∘g

(ii) Pentru oricare alt dublet (P ′, p′) cu P ′ mulțime şi p′: B→P ′ a. î. p′∘f= p′∘g , există o unică funcție v :P→P ′ a.î. v∘p=p′.

Teorema 4.5. Pentru orice pereche de funcții f, g : A→B există un conucleu al perechii (f, g) unic până la o bijecție (unicitatea înseamnă că dacă (P, p) şi (P ′, p′) sunt două conuclee pentru perchea (f, g), atunci există o bijecție v:P→P ′ a.î. v∘p=p′).

Demonstrație. Vom proba doar existența conucleului perechii (f, g) deoarece unicitatea sa se probează analog cu unicitatea nucleului.

Pentru aceasta fie ρ={(f(x), g(x)) | x∈A } (care este o relație binară pe B) iar <ρ> relația de echivalență de pe B generată de ρ (a cărei construcție este descrisă în Teorema 2.11.). Să arătăm că perechea (B / <ρ>, $p_{<\rho>, B}$) este un conucleu al perechii (f, g). Deoarece pentru

orice $x\in A$ avem $(f(x), g(x))\in \rho\subseteq<\rho>$ deducem că $(f(x), g(x))\in<\rho>$ adică, $p_{<\rho>, B}(f(x))=p_{<\rho>, B}(g(x))$, deci $p_{<\rho>, B}\circ f=p_{<\rho>, B}\circ g$.

Fie acum (B', p') cu B' mulțime şi $p':B\to B'$ a.î. $p'\circ f=p'\circ g$. Atunci pentru orice $x\in A$, $p'(f(x))=p'(g(x))$, adică $(f(x), g(x))\in\rho_{p'}$ (vezi Propoziția 3.14.), deci $\rho\subseteq\rho_{p'}$. Cum $\rho_{p'}$ este relație de echivalență pe B iar $<\rho>$ este cea mai mică relație de echivalență de pe B ce conține pe ρ deducem că $<\rho>\subseteq\rho_{p'}$.

Conform Propoziției 3.13. există o funcție $\alpha : B/<\rho>\to B/\rho_{P'}$ a.î. $\alpha\circ p_{<\rho>, B}= p_{\rho_{p'},B}$. Fie $\beta:B/\rho_{P'}\to Im(p')$ bijecția a cărei existență ne este asigurată de Propoziția 3.14.. Avem că $p'=i'\circ\beta\circ p_{\rho_{p'},B}$, unde i': Im $(p')\to B'$ este incluziunea.

Dacă notăm $v=i'\circ\beta\circ\alpha$, atunci

$v\circ p_{\langle\rho\rangle,B}=(i'\circ\beta\circ\alpha)\circ p_{\langle\rho\rangle,B}=(i'\circ\beta)\circ(\alpha\circ p_{\langle\rho\rangle,B})=(i'\circ\beta)\circ p_{\rho_{p'},B}=$

$=i'\circ(\beta\circ p_{\rho_{p'},B})=p'$.

Dacă mai avem $v':B/<\rho>\to B'$ a.î. $v'\circ p_{\langle\rho\rangle,B}=p'$, atunci $v'\circ p_{\langle\rho\rangle,B}= v\circ p_{\langle\rho\rangle,B}$ şi cum $p_{\langle\rho\rangle,B}$ este surjecție deducem că $v'=v$ (conform Propoziției 3.8.). ■

Observația 4.6. Vom nota $(B, p_{\langle\rho\rangle,B})=$Coker (f, g) sau (B=Coker (f, g) dacă nu este pericol de confuzie).

§ 5. Mulțimi ordonate. Semilatici. Latici.

Definiția 5.1. Printr-o *mulțime ordonată* înțelegem un dublet (A, ≤) format dintr-o mulțime nevidă A şi o relație binară pe A notată tradițional prin "≤" care este reflexivă, antisimetrică şi tranzitivă. Vom spune că "≤" este o *ordine* pe A.

Pentru $x, y\in A$ vom scrie $x < y$ dacă $x\le y$, $x\ne y$. Dacă relația "≤" este doar reflexivă şi tranzitivă, vom spune despre ea că este o *ordine parțială* sau că (A, ≤) este o mulțime *parțial ordonată*.

Dacă pentru x, y∈A definim x ≥ y dacă şi numai dacă y ≤ x obţinem o nouă relaţie de ordine pe A. Dubletul (A, ≥) îl vom nota prin A° şi spunem că mulţimea ordonată A° este *duala* mulţimii A.

Fie $(A,\leq)$ o mulţime parţial ordonată iar ρ o relaţie de echivalenţă pe A. Vom spune despre ρ că este compatibilă cu preordinea $\leq$ de pe A dacă pentru oricare elemente x , y , z, t din A avem implicaţia $(x,y)\in\rho,(z,t)\in\rho$ şi $x\leq z\Rightarrow y\leq t.$

Dacă ρ este o relaţie de echivalenţă pe A compatibilă cu preordinea $\leq$, atunci pe mulţimea cât A/ρ se poate defini o ordine parţială astfel : $[x]_\rho\leq[y]_\rho\Leftrightarrow$ există $z\in[x]_\rho$ şi $t\in[y]_\rho$ a.î. $z\leq t$; vom numi această ordine parţială *preordinea cât.*

În cele ce urmează prin $(A,\leq)$ vom desemna o mulţime ordonată.

Când nu este pericol de confuzie prin mulţime ordonată vom specifica numai mulţimea subiacentă A (fără a mai pune în evidenţă relaţia $\leq$, aceasta subânţelegându-se).

Definiţia 5.2. Fie m, M ∈A şi S ⊆ A, S ≠ ∅.
Vom spune că:

i) m este *minorant* pentru S dacă pentru orice s∈S, m ≤ s (în caz că există, prin inf (S) vom desemna cel mai mare minorant al lui S)

ii) M este *majorant* pentru S dacă M este minorant pentru S în A°, adică pentru orice s∈S, s ≤ M (în caz că există, prin sup (S) vom desemna cel mai mic majorant al lui S).

Dacă $S=\{s_1, s_2, ..., s_n\}\subseteq A$ atunci vom nota inf (S)= $s_1\wedge s_2\wedge...\wedge s_n$ iar sup (S)= $s_1\vee s_2\vee..\vee s_n$ (evident, în cazul în care acestea există).

Ordinea "≤" de pe A se zice *totală* dacă pentru orice a, b∈A, a ≤ b sau b ≤ a; o submulţime total ordonată a lui A poartă numele de *lanţ*.

Pentru a, b∈A vom spune că b *urmează* pe a (sau că a este *urmat* de b) dacă a < b iar pentru a ≤ c ≤ b avem a=c sau c=b; vom utiliza în acest caz notaţia a ∠ b.

Pentru $a, b \in A$ vom nota:

$(a, b)=\{x \in A \mid a<x<b\}$

$[a, b]=\{x \in A \mid a \leq x \leq b\}$

$(a, b]=\{x \in A \mid a<x \leq b\}$

$[a, b)=\{x \in A \mid a \leq x<b\}$

şi vom numi astfel de submulţimi ale lui A *intervale* (respectiv deschise, închise, închise la dreapta şi deschise la stînga, închise la stînga şi deschise la dreapta).

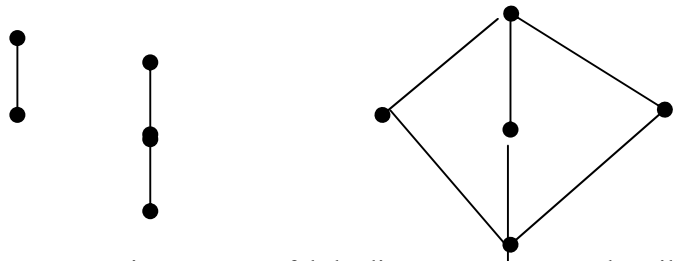
Mulţimile ordonate finite A pot fi reprezentate prin aşa zisele *diagrame Hasse*.

În acest sens, vom reprezenta fiecare element al lui A printr-un cerculeţ "•".

Dacă $a \angle b$ vom desena cerculeţul corespunzător lui b deasupra celui ce-l reprezintă pe a, unind cele două cercuţe printr-un segment (de remarcat faptul că intersecţia a două astfel de segmente poate să nu reprezinte un element al lui A).

Dintr-o astfel de diagramă putem să reconstituim relaţia "≤" ţinând cont de observaţia că $a \angle b$ dacă şi numai dacă pentru un şir finit de elemente $c_1, c_2, \ldots, c_n$ ale lui A avem $a = c_1 \angle c_2 \angle \ldots \angle c_{n-1} \angle c_n = b$.

Iată câteva exemple de diagrame Hasse:



Din păcate, astfel de diagrame sunt greu de utilizat în cazul mulţimilor ordonate infinite (cum ar fi de exemplu $\mathbb{Q}$ sau $\mathbb{R}$ cu ordonarea obişnuită).

Fie $(I, \leq)$ un lanţ iar $(A_i)_{i \in I}$ o familie de mulţimi ordonate (mutual disjuncte). Vom nota prin $\bigoplus_{i \in I} A_i$ mulţimea ordonată ce are drept mulţime subiacentă $\bigcup_{i \in I} A_i$ iar relaţia de ordonare este definită pentru x,

$y \in \bigoplus_{i \in I} A_i$ prin $x \le y$ dacă şi numai dacă $x \in A_i$, $y \in A_j$ şi $i < j$ sau $\{x, y\} \subset A_k$ iar $x \le y$ în A_k. Mulţimea ordonată $\bigoplus_{i \in I} A_i$ definită mai sus poartă numele de *suma ordinală* a familiei $(A_i)\ A_{i \in I}$.

Dacă $I=\{1, 2,..., n\}$ convenim să notăm

$$\bigoplus_{i \in I} A_i = A_1 \oplus A_2 \oplus ... \oplus A_n.$$

Dacă $(P_i, \le)_{1 \le i \le n}$ este o familie finită de mulţimi ordonate, atunci $P= \underset{1 \le i \le n}{\times} P_i$ devine în mod canonic mulţime ordonată, definind pentru $x=(x_i)_{1 \le i \le n}$, $y=(y_i)_{1 \le i \le n} \in P$, $x \le y$ $<\overset{def}{\Leftrightarrow}>$ există $1 \le s \le n$ a.î. $x_1 = y_1, \ldots, x_{s-1}=y_{s-1}$ şi $x_s<y_s$ (această ordonare se numeşte *ordonarea lexicografică*).

Definiţia 5.3. Vom spune despre A că este:

i*) inf – semilatice,* dacă pentru oricare două elemente $a, b \in A$ există $a \wedge b=\inf\{a, b\}$

ii) *sup – semilatice,* dacă pentru oricare două elemente $a, b \in A$ există $a \vee b=\sup\{a, b\}$

iii) *latice,* dacă este simultan inf şi sup-semilatice (adică pentru oricare două elemente $a, b \in A$ există $a \wedge b$ şi $a \vee b$)

iv) *inf – completă,* dacă pentru orice submulţime $S \subseteq A$ există inf (S)

v*) sup – completă,* dacă pentru orice submulţime $S \subseteq A$ există sup (S)

vi) completă dacă este simultan inf şi sup-completă (evident în acest caz se poate utiliza denumirea de *latice completă*)

vii) *inf - mărginită* dacă există un element notat tradiţional prin $0 \in A$ a.î. pentru orice $a \in A$, $0 \le a$

viii) *sup - mărginită* dacă există un element notat tradiţional prin $1 \in A$ a.î. pentru orice $a \in A$, $a \le 1$

ix) ***mărginită*** **dacă este simultan inf şi sup - mărginită (adică $0 \le a \le 1$ pentru orice $a \in A$); în acest caz 0 se zice element *inițial* (sau *prim*) al lui A iar 1 element *final* (sau *ultim*) al lui A**

x) ***condițional completă*** **dacă pentru orice submulțime nevidă şi mărginită S a sa există inf (S) şi sup (S).**

Observația 5.4.

1.Orice mulțime ordonată A care este inf-completă este latice completă.

Într-adevăr, fie $M \subseteq A$, M' mulțimea majoranților lui M iar $m=\inf(M')$. Cum pentru $x \in M$ şi $y \in M'$ avem $x \le y$ deducem că $x \le m$, adică $m \in M'$, astfel $m = \sup(M)$.

2. Dacă A este o latice completă, atunci $\inf(\emptyset) = \mathbf{1}$ iar $\sup(\emptyset) = \mathbf{0}$.

3. Pentru ca o latice L să fie condițional completă, este suficient ca pentru orice submulțime nevidă şi mărginită S a sa, să existe doar inf (S) (sau sup (S)).

Definiția 5.5. Un element $m \in A$ se zice:

i) ***minimal*** **dacă având $a \in A$ a.î. $a \le m$ deducem că $m = a$**

ii) ***maximal*** **dacă având $a \in A$ a.î. $m \le a$ deducem că $m = a$**

Dacă A are 0, un element $a \in A$ se zice *atom* dacă $a \neq 0$ şi având $x \in A$ a.î. $x \le a$, atunci $x = 0$ sau $x = a$ (deci $0 \angle a$).

Definiția 5.6. Dacă A este inf-semilatice (respectiv sup-semilatice) vom spune despre o submulțime $A' \subseteq A$ că este *inf-sub-semilatice* (respectiv *sup-sub-semilatice*), dacă pentru oricare două elemente $a, b \in A'$ avem $a \wedge b \in A'$ (respectiv $a \vee b \in A'$).

Dacă A este latice, $A' \subseteq A$ se va zice *sublatice,* dacă pentru oricare două elemente $a, b \in A'$ avem $a \wedge b$, $a \vee b \in A'$.

Exemple.

1. Fie $\mathbb{N}$ mulțimea numerelor naturale iar "$\mid$" relația de divizibilitate pe $\mathbb{N}$. Atunci "$\mid$" este o relație de ordine pe $\mathbb{N}$. Față de această ordine $\mathbb{N}$ devine latice în care pentru $m, n \in \mathbb{N}$, $m \wedge n$ = cel

mai mare divizor comun al lui m şi n iar $m \vee n$ = cel mai mic multiplu comun al lui m şi n.

Evident, pentru relaţia de divizibilitate, elementul $1 \in \mathbb{N}$ este element iniţial iar $0 \in \mathbb{N}$ este element final. Această ordonare nu este totală deoarece dacă avem două numere naturale m, n prime între ele (cum ar fi de exemplu 2 şi 3) nu avem $m \mid n$ şi nici $n \mid m$.

2. Dacă **K** este una din mulţimile de numere $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ sau $\mathbb{R}$, atunci **K** cu ordonarea naturală este o latice, iar ordonarea naturală este totală.

3. Fie M o mulţime iar **P**(M) mulţimea submulţimilor lui M. Atunci (**P** (M), $\subseteq$) este o latice completă cu prim şi ultim element (respectiv $\varnothing$ şi M).

Fie acum A, A′ două mulţimi ordonate (când nu este pericol de confuzie convenim să notăm prin "$\leq$" ambele relaţii de ordine de pe A şi A′) şi f:A→A′ o funcţie.

Definiţia 5.7. Vom spune despre f că este *morfism de mulţimi ordonate* (sau aplicaţie *izotonă*) dacă pentru orice a, b∈A cu $a \leq b$ avem $f(a) \leq f(b)$ (în anumite lucrări f se zice *monoton crescătoare*).

Dacă A, A′ sunt inf (sup) - semilatici vom spune despre f că este *morfism de inf (sup) - semilatici* dacă pentru oricare două elemente a, b∈A, $f(a \wedge b) = f(a) \wedge f(b)$ (respectiv $f(a \vee b) = f(a) \vee f(b)$).

Dacă A, A′ sunt latici, vom spune că f este *morfism de latici* dacă f este simultan morfism de inf şi sup-semilatici (adică pentru oricare două elemente a, b ∈A avem $f(a \wedge b) = f(a) \wedge f(b)$ şi $f(a \vee b) = f(a) \vee f(b)$).

În mod evident, morfismele de inf (sup) - semilatici sunt aplicaţii izotone iar dacă compunem două morfisme de acelaşi tip obţinem tot un morfism de acelaşi tip.

Dacă A, A′ sunt mulţimi ordonate iar f:A→A′ este *morfism de mulţimi ordonate*, atunci f se zice *izomorfism de mulţimi ordonate* dacă

există $g:A' \to A$ morfism de mulțimi ordonate a.î. $f \circ g = 1_{A'}$ şi $g \circ f = 1_A$. Acest lucru revine la a spune de fapt că f este o bijecție. În acest caz vom scrie $A \approx A'$.

Analog se defineşte noțiunea de *izomorfism de inf (sup)* - semilatici ca şi cea de *izomorfism de latici*.

În continuare vom stabili felul în care mulțimile preordonate induc mulțimi ordonate, iar pentru aceasta fie $(A, \leq)$ o mulțime parțial ordonată.

Se verifică imediat că relația ρ definită pe A prin: $(x, y) \in \rho \Leftrightarrow x \leq y$ şi $y \leq x$ este o echivalență pe A compatibilă cu preordinea $\leq$. Vom considera $\overline{A} = A/\rho$ împreună cu preordinea cât (definită la începutul paragrafului) şi să arătăm că acestă preordine este de fapt o ordine pe $\overline{A}$ (adică ρ este şi simetrică).

Într-adevăr, fie $[x]_\rho, [y]_\rho \in \overline{A}$ a.î. $[x]_\rho \leq [y]_\rho$ şi $[y]_\rho \leq [x]_\rho$ şi să demonstrăm că $[x]_\rho = [y]_\rho$. Atunci există $x', x'' \in [x]_\rho$, $y', y'' \in [y]_\rho$ a.î. $x' \leq y'$ şi $y'' \leq x''$.

Avem $(x', x), (x'', x), (y', y), (y'', y) \in \rho$ adică $x' \leq x, x \leq x', x'' \leq x, x \leq x'', y' \leq y, y \leq y', y'' \leq y$ şi $y \leq y''$.

Din $x \leq x', x' \leq y'$ şi $y' \leq y$ deducem că $x \leq y$ iar din $y \leq y'', y'' \leq x''$ şi $x'' \leq x$ deducem că $y \leq x$, adică $(x, y) \in \rho$, astfel că $[x]_\rho = [y]_\rho$.

Astfel, surjecția canonică $p_A : A \to \overline{A}$ este funcție izotonă.

Ținând cont de Propoziția 3.13. se verifică imediat faptul că mulțimea ordonată cât $(\overline{A}, \leq)$ împreună cu surjecția canonică $p_A : A \to \overline{A}$ verifică următoarea proprietate de universalitate:

Pentru orice mulțime ordonată $(B, \leq)$ ***şi funcție izotonă*** $f : A \to B$ ***există o unică aplicație izotonă*** $\bar{f} : \overline{A} \to B$ ***a.î.*** $\bar{f} \circ p_A = f$.

Definiția 5.8. Fie A o inf-semilatice şi F $\subseteq$A o submulțime nevidă a sa. Vom spune că F este *filtru* al lui A dacă F este o inf-sub-semi- latice şi pentru a, b $\in$A, dacă a $\leq$ b şi a$\in$F atunci b$\in$F.

Vom nota prin **F** (A) mulțimea filtrelor lui A.

Noțiunea dală celei de filtru este aceea de *ideal* pentru o sup-semilatice. Mai precis avem:

Definiția 5.9. Fie A o sup-semilatice iar $I \subseteq A$ o submulțime nevidă a sa. Vom spune că I este un *ideal* al lui A dacă I este sup-sub-semilatice a lui A şi pentru orice $a, b \in A$ cu $a \leq b$, dacă $b \in I$ atunci şi $a \in I$.

Vom nota prin **I** (A) mulțimea idealelor lui A.

Observația 5.10. Dacă A este latice, atunci noțiunile de filtru şi ideal au definiții precise în A (ținând cont de definițiile de mai sus, căci A este simultan inf şi sup-semilatice); evident în acest caz $A \in \mathbf{F}(A) \cap \mathbf{I}(A)$.

Cum intersecția oricărei familii de filtre (ideale) este de asemenea filtru (ideal), putem vorbi de *filtrul (idealul) generat de o mulțime nevidă.*

Dacă A este o inf(sup)-semilatice, pentru $\emptyset \neq S \subseteq A$ vom nota prin [S) ((S]) *filtrul(idealul) generat de S* (adică intersecția tuturor filtrelor (idealelor) lui A ce conțin pe S).

Propoziția 5.11. Dacă A este o inf-semilatice şi $S \subseteq A$ o submulțime nevidă a sa, atunci:

$$[S)=\{a \in A \mid \text{există } s_1, s_2, .., s_n \in S \text{ a.î. } s_1 \wedge s_2 \wedge .. \wedge s_n \leq a\}.$$

*Demonstrație.*Fie $F_S=\{a \in A \mid \text{există } s_1, s_2, .., s_n \in S \text{ a.î. } s_1 \wedge s_2 \wedge .. \wedge s_n \leq a\}$. Se probează imediat că $F_S \in \mathbf{F}(A)$ şi $S \subseteq F_S$, deci $[S) \subseteq F_S$.

Dacă $F' \in \mathbf{F}(A)$ a.î. $S \subseteq F'$ atunci $F_S \subseteq F'$ deci $F_S \subseteq \cap F' = [S)$,de unde $[S)=F_S$.■

Dual se demonstrează:

Propoziția 5.12. Dacă A este o sup-semilatice şi $S \subseteq A$ este o submulțime nevidă a sa, atunci:

$$(S]=\{a \in A \mid \text{există } s_1, s_2, .., s_n \in S \text{ a.î. } a \leq s_1 \vee s_2 \vee .. \vee s_n\}.$$

Astfel, $(F(A),\subseteq)$ şi $(I(A),\subseteq)$ sunt latici în care pentru F_1, $F_2\in F(A)$ (respectiv I_1, $I_2\in I(A)$) avem $F_1\wedge F_2=F_1\cap F_2$ iar $F_1\vee F_2=[F_1\cup F_2)$ (respectiv $I_1\wedge I_2=I_1\cap I_2$ iar $I_1\vee I_2=(I_1\cup I_2]$).

Dacă A este o inf (sup)-semilatice şi $a\in A$, vom nota prin [a) ((a]) filtrul (idealul) generat de {a}.

Conform celor de mai sus avem că: $[a)=\{x\in A|a\leq x\}$ şi $(a]=\{x\in A|x\leq a\}$ ([a), (a] poartă numele de *filtrul* (*idealul*) *principal* generat de a).

Teorema 5.13. Fie $(A, \leq)$ o mulţime ordonată. Atunci A este izomorfă cu o mulţime de submulţimi ale lui A (ordonată cu incluziunea).

Demonstraţie. Pentru fiecare $a\in A$ considerăm $M_a=\{x\in A|x\leq a\}\subseteq A$. Deoarece pentru a, $b\in A$, $a \leq b$ avem $M_a \subseteq M_b$ deducem că asocierea $a \to M_a$ pentru $a\in A$ descrie izomorfismul de mulţimi ordonate dorit. ■

Definiţia 5.14.

i) O mulţime ordonată în care orice submulţime nevidă a sa are un element iniţial se zice *bine ordonată* (evident o mulţime bine ordonată este inf-completă şi total ordonată)

ii) O mulţime ordonată în care orice submulţime total ordonată a sa are un majorant (minorant) se zice *inductiv (coinductiv)* ordonată.

După cum vom vedea în §9 $(\mathbb{N}, \leq)$ este un exemplu de mulţime bine ordonată.

În cele ce urmează, acceptăm că pentru orice mulţime M este verificată *axioma alegerii*:

Există o funcţie $s : P(M) \to M$ a.î. $s(S)\in S$ *pentru orice submulţime nevidă S a lui M*.

În continuare, reamintim un rezultat datorat lui Bourbaki şi câteva corolare importante ale acestuia (pentru demonstraţii recomandăm cititorului lucrarea [23]).

Lema 5.15. (*Bourbaki*). Dacă $(A, \leq)$ este o mulțime nevidă, inductiv ordonată şi $f : A \to A$ este o aplicație a.î. $f(a) \leq a$ pentru orice $a \in A$, atunci există $u \in A$ a.î. $f(u) = u$.

Corolar 1 (*Principiul lui Hansdorf de maximalitate*). Orice mulțime ordonată conține o submulțime total ordonată maximală.

Corolar 2 (*Lema lui Zorn*). Orice mulțime nevidă inductiv (coinductiv) ordonată are cel puțin un element maximal (minimal).

Corolar 3 (*Principiul elementului maximal (minimal)*). Fie $(A, \leq)$ o mulțime inductiv (coinductiv) ordonată şi $a \in A$. Există un element maximal (minimal) $m_a \in A$ a.î. $a \leq m_a$ ($m_a \leq a$).

Corolar 4 (*Lema lui Kuratowski*). Orice submulțime total ordonată a unei mulțimi ordonate este cuprinsă într-o submulțime total ordonată maximală.

Corolar 5 (*Teorema lui Zermelo*). Pe orice mulțime nevidă A se poate introduce o ordine față de care A este bine ordonată.

Corolar 6 (*Principiul inducției transfinite*). Fie $(A, \leq)$ o mulțime bine ordonată infinită şi P o proprietate dată. Pentru a demonstra că toate elementele mulțimii A au proprietatea P este suficient să demonstrăm că:

(i) Elementul inițial 0 al lui A are proprietatea P

(ii) Dacă pentru $a \in A$, toate elementele $x \in A$ a.î. $x < a$ au proprietatea P, atunci şi elementul a are proprietatea P.

Definiția 5.16. Vom spune despre o latice $(L, \leq)$ că este:

i) *modulară* dacă pentru oricare $x, y, z \in L$ cu $z \leq x$ avem $x \wedge (y \vee z) = (x \wedge y) \vee z$

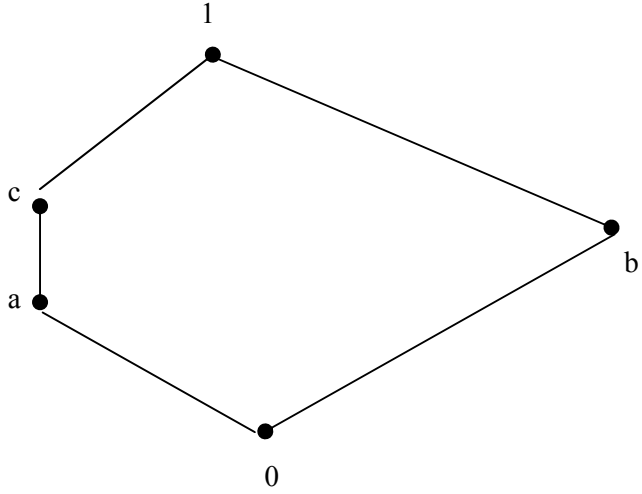
ii) *distributivă* dacă verifică una din următoarele două condiții echivalente:

1) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

2) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ pentru orice $x, y, z \in L$.

Să notăm că există latici ce nu sunt modulare.

Într-adevăr, dacă vom considera laticea notată tradițional prin $\mathbf{N_5}$:



observăm că $a \le c$, pe când $a \vee (b \wedge c) = a \vee \mathbf{0} = a$ iar $(a \vee b) \wedge c = \mathbf{1} \wedge c \neq a$, astfel că $c \wedge (b \vee a) \neq (c \wedge b) \vee a$, deci N_5 nu este modulară.

Teorema 5.17. (*Dedekind*). Pentru o latice L următoarele afirmații sunt echivalente:

(i) L este modulară

(ii) Pentru orice a, b, c∈L, dacă $c \le a$, atunci $a \wedge (b \vee c) \le (a \wedge b) \vee c$

(iii) Pentru orice a, b, c∈L avem $((a \wedge c) \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$

(iv) Pentru orice a, b, c∈L, dacă $a \le c$, atunci din $a \wedge b = c \wedge b$ şi $a \vee b = c \vee b$ deducem că $a = c$

(v) L nu are sublatici izomorfe cu N_5.

Demonstrație. Cum în orice latice, dacă $c \le a$, atunci $(a \wedge b) \vee c \le a \wedge (b \vee c)$, echivalența (i) $\Leftrightarrow$ (ii) este imediată.

(i) $\Rightarrow$ (iii). Rezultă din aceea că $a \wedge c \le c$.

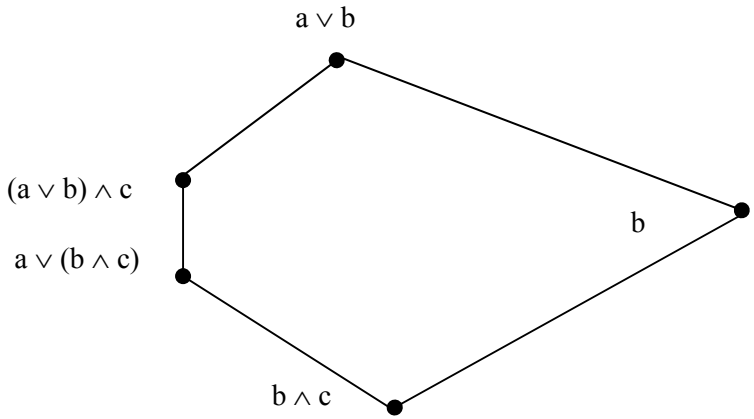
(iii) $\Rightarrow$ (i). Fie $a, b, c \in L$ a.î. $a \le c$. Atunci $a = a \wedge c$, deci $(a \vee b) \wedge c = ((a \wedge c) \vee b) \wedge c = (a \wedge c) \vee (b \wedge c) = a \vee (b \wedge c)$.

(i) $\Rightarrow$ (iv). Avem $a = a \vee (a \wedge b) = a \vee (c \wedge b) = a \vee (b \wedge c) =$ $=(a \vee b) \wedge c = (c \vee b) \wedge c = c$.

(iv) $\Rightarrow$ (v) Evident (ţinând cont de observaţia de mai înainte).

(v) $\Rightarrow$ (i) Să presupunem că L nu este modulară. Există atunci a, b, c în L a.î. $a \leq c$, iar $a \vee (b \wedge c) \neq (a \vee b) \wedge c$. Să observăm că $b \wedge c < a \vee (b \wedge c) < (a \vee b) \wedge c < a \vee b$, $b \wedge c < b < a \vee b$, $a \vee (b \wedge c) \leq b$ şi $b \leq (a \vee b) \wedge c$.

Obţinem în felul acesta diagrama Hasse a unei sublatici a lui L izomorfă cu $\mathbf{N_5}$:



(observând şi că $(a \vee (b \wedge c)) \vee b = a \vee ((b \wedge c) \vee b) = a \vee b$ şi $((a \vee b) \wedge c) \wedge b = ((a \vee b) \wedge b) \wedge c = b \wedge c$, ceea ce este absurd. ■

Pe parcursul acestei lucrări vom prezenta mai multe exemple de latici modulare.

§ 6. Latici distributive

Evident, orice latice distributivă este modulară. În cele ce urmează, prin **Ld** vom nota clasa laticilor distributive iar prin **Ld** (**0**, **1**) clasa laticilor distributive mărginite.

Exemple.

1. Dacă L este un lanţ, atunci $L \in$ **Ld** (**0**, **1**).

2. $(\mathbb{N}, |)$, $(\mathbf{P}(M), \subseteq) \in \mathbf{Ld}(\mathbf{0}, \mathbf{1})$.

Observația 6.1. Raționând inductiv după $n \in \mathbb{N}^*$, deducem că dacă $S_1, S_2, \ldots, S_n$ sunt submulțimi nevide ale unei latici distributive L, atunci: $\bigvee_{i=1}^{n}(\wedge S_i) = \wedge\left\{\bigvee_{i=1}^{n} f(i) \;\middle|\; f \in S_1 \times \ldots \times S_n\right\}$.

Teorema 6.2. Pentru $L \in \mathbf{L}$ următoarele afirmații sunt echivalente:

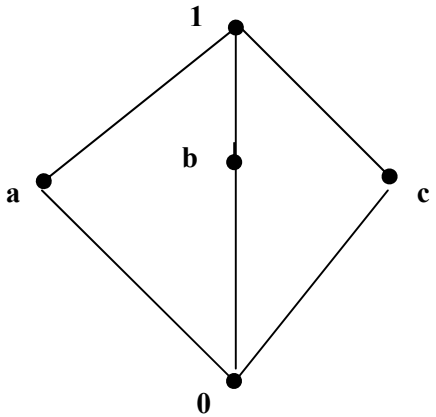
(i) $L \in \mathbf{Ld}$

(ii) $\mathbf{a \wedge (b \vee c) \leq (a \wedge b) \vee (a \wedge c)}$ **pentru orice** $\mathbf{a, b, c} \in L$

(iii) $\mathbf{(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \vee b) \wedge (b \vee c) \wedge (c \vee a)}$ **pentru orice** $\mathbf{a, b, c} \in L$

(iv) Pentru orice $\mathbf{a, b, c} \in L$**, dacă** $\mathbf{a \wedge c = b \wedge c}$ **şi** $\mathbf{a \vee c = b \vee c}$**, atunci** $\mathbf{a = b}$

(v) L **nu are sublatici izomorfe cu** $\mathbf{N_5}$ **sau** $\mathbf{M_3}$**, unde** $\mathbf{M_3}$ **are următoarea diagramă Hasse:**



Demonstrație. (i) $\Leftrightarrow$ (ii). Rezultă din aceea că pentru oricare elemente $a, b, c \in L$, $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$.

(i) $\Rightarrow$ (iii). Să presupunem că $L \in \mathbf{Ld}$ şi fie $a, b, c \in L$. Atunci $(a \vee b) \wedge (b \vee c) \wedge (c \vee a) = (((a \vee b) \wedge b) \vee ((a \vee b) \wedge c)) \wedge (c \vee a) =$

$=(b \vee ((a \wedge c) \vee (b \wedge c))) \wedge (c \vee a) = (b \vee (a \wedge c)) \wedge (c \vee a) =$
$=(b \wedge (c \vee a)) \vee ((a \wedge c) \wedge (c \vee a)) = ((b \wedge c) \vee (b \wedge a)) \vee (a \wedge c) =$
$=(a \wedge b) \vee (b \wedge c) \vee (c \wedge a)$.

(iii) $\Rightarrow$ (i). Deducem imediat că L este modulară, deoarece dacă a, b, $c \in L$ şi $a \leq c$, $(a \vee b) \wedge c = (a \vee b) \wedge ((b \vee c) \wedge c) = (a \vee b) \wedge (b \vee \vee c) \wedge (c \vee a) = (a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \wedge b) \vee (b \wedge c) \vee a =$
$=((a \wedge b) \vee a) \vee (b \wedge c) = a \vee (b \wedge c)$. Cu această observație, distributivitatea lui L se deduce astfel:

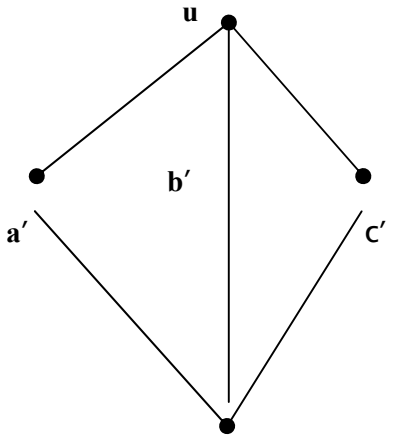
$a \wedge (b \vee c) = (a \wedge (a \vee b)) \wedge (b \vee c) = ((a \wedge (c \vee a)) \wedge (a \vee b) \wedge (b \vee c)$
$= a \wedge (a \vee b) \wedge (b \vee c) \wedge (c \vee a) = a \wedge ((a \wedge b) \vee (b \wedge c) \vee (c \wedge a)) =$
$=(a \wedge ((a \wedge b) \vee (b \wedge c))) \vee (c \wedge a) =$ (datorită modularității) =
$=a \wedge (b \wedge c)) \vee (a \wedge b) \vee (c \wedge a) =$ (datorită modularității) =
$=(a \wedge b) \vee (a \wedge c)$.

(i) $\Rightarrow$ (iv). Dacă $a \wedge c = b \wedge c$ şi $a \vee c = b \vee c$, atunci $a = a \wedge (a \vee c) = a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) = (a \wedge b) \vee (b \wedge c) = b \wedge (a \vee c) =$
$=b \wedge (b \vee c) = b$.

(iv) $\Rightarrow$ (v). Să admitem prin absurd că atât $\mathbf{N_5}$ cât şi $\mathbf{M_3}$ sunt sublatici ale lui L. În cazul lui $\mathbf{N_5}$ observăm că $b \wedge c = b \wedge a = \mathbf{0}$, $b \vee c = b \vee a = \mathbf{1}$ şi totuşi $a \neq c$ iar în cazul lui $\mathbf{M_3}$, $b \wedge a = b \wedge c = \mathbf{0}$, $b \vee a = b \vee c = \mathbf{1}$ şi totuşi $a \neq c$ - absurd!

(v) $\Rightarrow$ (i). Conform Teoremei 1.1, dacă L nu are sublatici izomorfe cu $\mathbf{N_5}$ atunci ea este modulară. Cum pentru oricare a, b, $c \in L$ avem: $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$, să presupunem prin absurd că există a, b, $c \in L$ a.î. $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) < < (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$. Notăm $d = (a \wedge b) \vee (b \wedge c) \vee (c \wedge a)$, $u = (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$, $a' = (d \vee a) \wedge u$, $b' = (d \vee b) \wedge u$ şi $c' = (d \vee c) \wedge u$.

Diagrama Hasse a mulțimii $\{d, a', b', c', u\}$ este:



Cum $\{d, a', b', c', u\} \subseteq L$ este sublatice, dacă vom verifica faptul că elementele d, a', b', c', u sunt distincte, atunci sublaticea $\{d, a', b', c', u\}$ va fi izomorfă cu $\mathbf{M_3}$ ceea ce va fi contradictoriu cu ipoteza pe care o acceptăm.

Deoarece $d < u$, vom verifica egalitățile $a' \vee b' = b' \vee c' = c' \vee a' = u$, $a' \wedge b' = b' \wedge c' = c' \wedge a' = d$ şi atunci va rezulta şi că cele 5 elemente d, a', b', c', u sunt distincte.

Datorită modularității lui L avem: $a' = d \vee (a \wedge u)$, $b' = d \vee (b \wedge u)$, $c' = d \vee (c \wedge u)$ iar datorită simetriei este suficient să demonstrăm doar că $a' \wedge c' = d$.

Într-adevăr, $a' \wedge c' = ((d \vee a) \wedge u) \wedge ((d \vee c) \wedge u) = (d \vee a) \wedge (d \vee c) \wedge u = ((a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \vee a) \wedge (d \vee c) \wedge u = ((b \wedge c) \vee a) \wedge (d \vee c) \wedge u = ((b \wedge c) \vee a) \wedge ((a \wedge b) \vee c) \wedge (a \vee b) \wedge (b \vee c) \wedge (c \vee a) = ((b \wedge c) \vee a) \wedge ((a \wedge b) \vee c) = (b \wedge c) \vee (a \wedge ((a \wedge b) \vee c)) =$ (datorită modularității) $= (b \wedge c) \vee (((a \wedge b) \vee c) \wedge a) = (b \wedge c) \vee ((a \wedge b) \vee (c \wedge a)) =$ (datorită modularității) $= d$. ■

Corolar 6.3. O latice L este distributivă dacă şi numai dacă pentru oricare două ideale I, J ∈ I (L), I ∨ J = {i ∨ j | i ∈ I şi j ∈ J}.

Demonstrație. Să presupun că L este distributivă. Ținând cont de Propoziția 5.12., pentru t∈I ∨ J există i ∈ I, j ∈ J a.î. t ≤ i ∨ j, astfel că t = (t ∧ i) ∨ (t ∧ j) = i′ ∨ j′ cu i′ = t ∧ i ∈ I iar j′ = t ∧ j ∈ J.

Pentru a proba afirmația reciprocă, să presupun prin absurd că L nu este distributivă şi să arătăm că există I, J∈**I** (L) ce nu verifică ipoteza.

Conform Teoremei 6.2., L conține elementele a, b, c care împreună cu **0** şi **1** formează laticile $\mathbf{N_5}$ sau $\mathbf{M_3}$.

Fie I = (b], J = (c]. Cum a ≤ b ∨ c deducem că a∈I ∨ J. Dacă am avea a=i ∨ j cu i∈I şi j∈J, atunci j ≤ c, deci j ≤ a ∧ c < b, adică j∈J şi astfel a = i ∨ j ∈I - absurd! ■

Corolar 6.4. Fie L∈Ld iar I, J∈I(L). Dacă I ∧J şi I∨J sunt ideale principale, atunci I şi J sunt ideale principale.

Demonstrație. Fie I ∧ J = (x] şi I ∨ J = (y]. Conform Corolarului 6.3., y = i ∨ j cu i∈I şi j∈J. Dacă c = x ∨ i şi b = x ∨ j, atunci c∈I şi b∈J. Să probăm că I = (c] şi J = (b].

Dacă prin absurd J≠(b], atunci există a∈I, a > b iar {x, a, b, c, y} este izomorfă cu $\mathbf{N_5}$ - absurd!

Analog, dacă I ≠ (c], găsim o sublatice a lui L izomorfă cu $\mathbf{M_3}$ ceea ce este din nou absurd! ■

Corolar 6.5. Fie L o latice oarecare şi x, y∈L. Atunci (x] ∧ (y]=(x ∧ y] iar (x ∨ y]⊆(x] ∨ (y]; dacă L∈Ld, atunci (x] ∨ (y] = (x ∨ y].

Demonstrație. Egalitatea (x] ∧ (y] = (x ∧ y] se probează imediat prin dublă incluziune iar incluziunea (x ∨ y]⊆(x] ∨ (y] rezultă

din Propoziția 5.12. Dacă $L \in \mathbf{Ld}$, atunci conform Corolarului 6.3., $(x] \vee (y] = \{i \vee j \mid i \in (x] \text{ şi } j \in (y]\} = \{i \vee j \mid i \leq x \text{ şi } j \leq y\}$, de unde rezultă imediat că $(x] \vee (y] \subseteq (x \vee y]$, deci $(x \vee y] = (x] \vee (y]$. ■

§ 7. Complement şi pseudocomplement într-o latice. Algebre Boole.

Definiția 7.1. **Fie L o latice mărginită. Vom spune că elementul $a \in L$ are un *complement* în L dacă există $a' \in L$ a.î. $a \wedge a' = 0$ şi $a \vee a' = 1$ (a' se va numi *complementul* lui a).**

Vom spune despre laticea L că este *complementată* dacă orice element al său are un complement.

Dacă L este o latice oarecare şi $a, b \in L$, $a \leq b$, prin *complementul relativ* al unui element $x \in [a, b]$ din intervalul $[a, b]$, înțelegem acel element $x' \in [a, b]$ (dacă există!) pentru care $x \wedge x' = a$ şi $x \vee x' = b$.

Vom spune despre o latice L că este *relativ complementată* dacă orice element al său admite un complement relativ în orice interval din L ce-l conține.

Lema 7.2. Dacă $L \in L(0, 1)$, atunci un element al lui L poate avea cel mult un complement.

Demonstrație. Fie $a \in L$ iar a', a'' doi complementi ai lui a. Atunci $a \wedge a' = a \wedge a'' = \mathbf{0}$ şi $a \vee a' = a \vee a'' = \mathbf{1}$, de unde $a' = a''$ (conform Teoremei 6.2, (iv)). ■

Lema 7.3. Orice latice L modulară şi complementată este relativ complementată.

Demonstrație. Fie $b, c \in L$, $b \leq c$, $a \in [b, c]$ şi $a' \in L$ complementul lui a în L. Dacă vom considera $a'' = (a' \vee b) \wedge c \in [b, c]$, atunci $a \wedge a'' = a \wedge [(a' \vee b) \wedge c] = [(a \wedge a') \vee (a \wedge b)] \wedge c = (a \wedge b) \wedge c = b \wedge c = b$ iar $a \vee a'' = a \vee [(a' \vee b) \wedge c] = (a \vee a' \vee b) \wedge (a \vee c) = \mathbf{1} \wedge c = c$, adică a'' este complementul relativ al lui a în **[b, c]**. ■

Lema 7.4. (*De Morgan*) Fie $L \in Ld(0, 1)$, $a, b \in L$ având complementii $a', b' \in L$. Atunci $a \wedge b$, $a \vee b$ au complementi în L şi anume $(a \wedge b)' = a' \vee b'$ iar $(a \vee b)' = a' \wedge b'$.

Demonstrație. Conform Lemei 7.2 şi principiului dualizării, este suficient să probăm că $(a \wedge b) \wedge (a' \vee b') = \mathbf{0}$ iar $(a \wedge b) \vee (a' \vee b') = \mathbf{1}$.

Într-adevăr, $(a \wedge b) \wedge (a' \vee b') = (a \wedge b \wedge a') \vee (a \wedge b \wedge b') = \mathbf{0} \vee \mathbf{0} = \mathbf{0}$ iar $(a \wedge b) \vee (a' \vee b') = (a \vee a' \vee b') \wedge (b \vee a' \vee b') = \mathbf{1} \wedge \mathbf{1} = \mathbf{1}$. ■

Observația 7.5. Dacă $L \in \mathbf{Ld}(\mathbf{0}, \mathbf{1})$ şi $a \in L$ are un complement $a' \in L$, atunci a' este cel mai mare element al lui L cu proprietatea că $a \wedge a' = \mathbf{0}$ (adică $a' = \sup(\{x \in L \mid a \wedge x = \mathbf{0}\})$.

Această observație ne conduce la:

Definiția 7.6. Fie L o inf-semilatice cu 0 şi $a \in L$. Un element $a^* \in L$ se zice *pseudocomplementul* lui a dacă $a^* = \sup(\{x \in L \mid a \wedge x = 0\})$.

Dacă orice element al lui L are pseudocomplement, vom spune că inf - semilaticea L este *pseudocomplementată*

O latice L se zice *pseudocomplementată,* dacă privită ca inf-semilatice este pseudocomplementată.

Lema 7.7. Dacă L este o latice modulară mărginită, atunci orice element ce are un complement a' îl va avea pe a' şi ca pseudocomplement.

Demonstrație. Într-adevăr, fie $a \in L$, a' un complement al lui a şi $b \in L$ a.î. $a' \le b$ şi $b \wedge a = \mathbf{0}$.

Atunci $b = b \wedge \mathbf{1} = b \wedge (a' \vee a) = a' \vee (b \wedge a) = a' \vee \mathbf{0} = a'$. ■

Teorema 7.8. Fie $L \in Ld\,(0)$ pseudocomplementată, $R(L) = \{a^* \mid a \in L\}$ iar $D(L) = \{a \in L \mid a^* = 0\}$.

Atunci, pentru $a, b \in L$ avem:

1) $a \wedge a^* = 0$ **iar** $a \wedge b = 0 \Leftrightarrow a \le b^*$

2) $a \le b \Rightarrow a^* \ge b^*$

3) $a \le a^{**}$

4) $a^* = a^{***}$

5) $(a \vee b)^* = a^* \wedge b^*$

6) $(a \wedge b)^{**} = a^{**} \wedge b^{**}$

7) $a \wedge b = 0 \Leftrightarrow a^{**} \wedge b^{**} = 0$

8) $a \wedge (a \wedge b)^* = a \wedge b^*$

9) $0^* = 1, \quad 1^* = 0$

10) $a \in R(L) \Leftrightarrow a = a^{**}$

11) $a, b \in R(L) \Rightarrow a \wedge b \in R(L)$

12) $\sup_{R(L)} \{a, b\} = (a \vee b)^{**} = (a^* \wedge b^*)^*$

13) $0, 1 \in R(L), 1 \in D(L)$ **şi** $R(L) \cap D(L) = \{1\}$

14) $a, b \in D(L) \Rightarrow a \wedge b \in D(L)$

15) $a \in D(L)$ **şi** $a \le b \Rightarrow b \in D(L)$

16) $a \vee a^* \in D(L)$.

Demonstrație. **1)** Rezultă din definiția lui a^*. Echivalența rezultă din definiția lui b^*.

2) Deoarece $b \wedge b^* = \mathbf{0}$, atunci pentru $a \le b$, deducem că $a \wedge b^* = \mathbf{0}$, adică $b^* \le a^*$.

3) Din $a \wedge a^* = \mathbf{0}$ deducem că $a^* \wedge a = \mathbf{0}$, adică $a \le (a^*)^* = a^{**}$.

4) Din $a \le a^{**}$ şi 2) deducem că $a^{***} \le a^*$ şi cum din 3) deducem că $a^* \le (a^*)^{**} = a^{***}$ rezultă că $a^* = a^{***}$.

5) Avem $(a \vee b) \wedge (a^* \wedge b^*) = (a \wedge a^* \wedge b^*) \vee (b \wedge a^* \wedge b^*) = = \mathbf{0} \vee \mathbf{0} = \mathbf{0}$. Fie acum $x \in L$ a.î. $(a \vee b) \wedge x = \mathbf{0}$. Deducem că $(a \wedge x) \vee (b \wedge x) = \mathbf{0}$, adică $a \wedge x = b \wedge x = \mathbf{0}$, de unde $x \leq a^*$, $x \leq b^*$, adică $x \leq a^* \wedge b^*$. Restul afirmațiilor se probează analog. ■

Observația 7.9.

1. Elementele lui R (L) se zic *regulate* iar cele ale lui D (L) *dense.*

2. Ținând cont de 4) şi 10) deducem că R (L) = $\{ a \in L / a^{**} = a\}$.

3. Din 14) şi 15) deducem că D (L) $\in \mathbf{F}$ (L).

Teorema 7.10. Fie $L \in Ld$ şi $a \in L$.
Atunci $f_a : L \to (a] \times [a)$, $f_a(x) = (x \wedge a, x \vee a)$ pentru $x \in L$ este un morfism injectiv în Ld. În cazul în care $L \in Ld$ (0, 1), atunci f_a este izomorfism în Ld (0, 1) dacă şi numai dacă a are un complement.

Demonstrație. Faptul că f_a este morfism de latici este imediat. Fie acum $x, y \in L$ a.î. $f_a(x) = f_a(y)$ adică $x \wedge a = y \wedge a$ şi $x \vee a = = y \vee a$. Cum $L \in \mathbf{Ld}$, atunci $x = y$ (conform Teoremei 6.2.), deci f_a este ca funcție o injecție, adică f_a este morfism injectiv în **Ld**.

Să presupunem acum că $L \in \mathbf{Ld}$ $(\mathbf{0}, \mathbf{1})$. Dacă f_a este izomorfism în **Ld** $(\mathbf{0}, \mathbf{1})$, atunci pentru $(\mathbf{0}, \mathbf{1}) \in (a] \times [a)$ va exista $x \in L$ a.î. $f(x) = (\mathbf{0}, \mathbf{1})$, adică $a \wedge x = \mathbf{0}$ şi $a \vee x = \mathbf{1}$, de unde $x = a'$.

Reciproc, dacă $a' \in L$ este complementul lui a, pentru $(u, v) \in (a] \times [a)$ alegând $x = (u \vee a') \wedge v$ deducem imediat că $f_a(x) = = (u, v)$, adică f_a este şi surjecție, deci izomorfism în **Ld** $(\mathbf{0}, \mathbf{1})$. ■

Definiția 7.11. Numim *latice Boole* orice latice complementată din Ld (0, 1).

Exemple.

1. Lanțul trivial $\mathbf{1} = \{\varnothing\}$ ca şi $\mathbf{2} = \{0, 1\}$ (în care $0' = 1$ şi $1' = 0$). De fapt **1** şi **2** sunt singurele lanțuri ce sunt latici Boole.

2. Pentru orice mulțime M, $(P(M), \subseteq)$ este o latice Boole în care pentru orice $X \subseteq M$, $X' = M \setminus X = C_M(X)$.

3. Fie $n \in \mathbb{N}$, $n \geq 2$ iar D_n mulțimea divizorilor naturali ai lui n.

Mulțimea ordonată $(D_n, |)$ este latice Boole $\Leftrightarrow$ n este liber de pătrate (în care caz pentru $p, q \in D_n$, $p \wedge q = (p, q)$, $p \vee q = [p, q]$, $\mathbf{0} = \mathbf{1}$, $\mathbf{1} = n$ iar $p' = n / p$).

4. Fie M o mulțime iar $\mathbf{2}^M = \{f : M \to \mathbf{2}\}$. Definim pe $\mathbf{2}^M$ relația de ordine $f \leq g \Leftrightarrow f(x) \leq g(x)$ pentru orice $x \in M$. Astfel $(\mathbf{2}^M, \leq)$ devine latice Boole (în care caz pentru $f \in \mathbf{2}^M$, $f' = \mathbf{1} - f$).

Definiția 7.12. Din punctul de vedere al Algebrei Universale, prin *algebră Boole* înțelegem o algebră $(B, \wedge, \vee, ', 0, 1)$ de tipul (2, 2, 1, 0, 0) (cu $\wedge$ şi $\vee$ operații binare, $'$ o operație unară iar $0, 1 \in B$ operații nule) a.î.

B_1: $(B, \wedge, \vee) \in$ Ld

B_2: Sunt verificate identitățile $x \wedge 0 = 0$, $x \vee 1 = 1$

$x \wedge x' = 0$, $x \vee x' = 1$.

În cele ce urmează prin **B** vom desemna clasa algebrelor Boole.

Dacă $B_1, B_2 \in \mathbf{B}$, $f : B_1 \to B_2$ va fi *morfism de algebre Boole* dacă f este morfism în **Ld** (**0**, **1**) şi în plus $f(x') = (f(x))'$ pentru orice $x \in B_1$.

Morfismele bijective din **B** se vor numi *izomorfisme*.

Propoziția 7.13. (*Glivenko*) Fie $(L, \wedge, *, 0)$ o inf-semilatice pseudocomplementată iar $R(L) = \{a^* \mid a \in L\}$. Atunci, cu ordinea indusă de pe L, R (L) devine algebră Boole.

Demonstrație. Ținând cont de Teorema 7.8. deducem că L este mărginită $(1 = 0^*)$ iar pentru $a, b \in R(L)$, $a \wedge b \in R(L)$ iar

sup R (L) $\{a, b\} = (a^* \wedge b^*)^*$ astfel că R (L) este latice mărginită şi sub-inf-semilatice a lui L.

Deoarece pentru $a \in R(L)$, $a \vee a^* = (a^* \wedge a^{**})^* = \mathbf{0}^* = \mathbf{1}$ şi $a \wedge a^* = \mathbf{0}$ deducem că a^* este complementul lui a în R (L). Mai rămâne de probat faptul că R (L) este distributivă.

Pentru $x, y, z \in R(L)$, $x \wedge z \leq x \vee (y \wedge z)$ şi $y \wedge z \leq x \vee (y \wedge z)$, deci $x \wedge z \wedge [x \vee (y \wedge z)]^* = \mathbf{0}$ şi $(y \wedge z) \wedge [x \vee (y \wedge z)]^* = \mathbf{0}$ astfel că $z \wedge [x \vee (y \wedge z)]^* \leq x^*, y^*$, adică $z \wedge [x \vee (y \wedge z)]^* \leq x^* \wedge y^*$ şi $z \wedge [x \vee (y \wedge z)]^* \wedge (x^* \wedge y^*)^* = \mathbf{0}$ ceea ce implică $z \wedge (x^* \wedge y^*) \leq \leq [x \vee (y \wedge z)]^{**}$. Cum partea stângă a acestei ultime inegalităţi este $z \wedge (x \vee y)$ iar partea dreaptă este $x \vee (y \wedge z)$ (în R (L)), deducem că $z \wedge (x \vee y) \leq x \vee (y \wedge z)$, adică R (L) este şi distributivă. ■

Lema 7.14. Fie $B \in \mathbf{B}$ şi $a, b \in B$ a.î. $a \wedge b = 0$ şi $a \vee b = 1$. Atunci $b = a'$.

Demonstraţie. Rezultă imediat din Lema 7.2. ■

Lema 7.15. Dacă $B \in \mathbf{B}$ şi $a, b \in B$, atunci $(a')' = a$, $(a \wedge b)' = a' \vee b'$ iar $(a \vee b)' = a' \wedge b'$.

Demonstraţie. Rezultă imediat din Lema 7.4.. ■

Propoziţia 7.16. Dacă M este o mulţime oarecare, atunci algebrele Boole 2^M şi P(M) sunt izomorfe.

Demonstraţie. Fie $X \in P(M)$ şi $\alpha_X : M \to \mathbf{2}$,

$$\alpha_X(x) = \begin{cases} 0 & \text{pentru } x \notin X \\ 1 & \text{pentru } x \in X \end{cases}$$

Se verifică imediat că asocierea $X \to \alpha_X$ defineşte un izomorfism de algebre Boole $\alpha : P(M) \to \mathbf{2}^M$. ■

Pentru $B \in \mathbf{B}$ şi $a \in B$, vom nota $I(a) = [\mathbf{0}, a]$.

Propoziția 7.17. Pentru orice $a \in B$**:**

(i) $(I(a), \wedge, \vee, *, 0, a) \in B$**, unde pentru** $x \in I(a)$, $x^* = x' \wedge a$

(ii) $\alpha_a : B \to I(a)$, $\alpha_a(x) = a \wedge x$ **pentru** $x \in B$ **este un morfism surjectiv din B**

(iii) $B \approx I(a) \times I(a')$.

Demonstrație.

(i). $I(a) \in \mathbf{Ld}(\mathbf{0}, \mathbf{1})$ (ca sublatice a lui B). Pentru $x \in I(a)$, $x \wedge x^* = x \wedge (x' \wedge a) = (x \wedge x') \wedge a = \mathbf{0} \wedge a = \mathbf{0}$ iar $x \vee x^* = x \vee (x' \wedge a) = (x \vee x') \wedge (x \vee a) = \mathbf{1} \wedge (x \vee a) = x \vee a = a$.

(ii). Dacă $x, y \in B$, atunci $\alpha_a(x \vee y) = a \wedge (x \vee y) = (a \wedge x) \vee (a \wedge y) = \alpha_a(x) \vee \alpha_a(y)$, $\alpha_a(x \wedge y) = a \wedge (x \wedge y) = (a \wedge x) \wedge (a \wedge y) = \alpha_a(x) \wedge \alpha_a(y)$, $\alpha_a(x') = a \wedge x' = (a \wedge a') \vee (a \wedge x') = a \wedge (a' \vee x') = a \wedge (a \wedge x)' = (\alpha_a(x))^*$, $\alpha_a(\mathbf{0}) = \mathbf{0}$ iar $\alpha_a(\mathbf{1}) = a$, adică α_a este morfism surjectiv în **B**.

(iii). Se verifică uşor că $\alpha : B \to I(a) \times I(a')$, $\alpha(x) = (a \wedge x, a' \wedge x)$ pentru $x \in B$ este morfism în **B**.

Pentru $(y, z) \in I(a) \times I(a')$, cum $\alpha(y \vee z) = (a \wedge (y \vee z), a' \wedge (y \vee z)) = ((a \wedge y) \vee (a \wedge z), (a' \wedge y) \vee (a' \wedge z)) = (y \vee \mathbf{0}, \mathbf{0} \vee z) = (y, z)$ deducem că α este surjecție. Fie acum $x_1, x_2 \in B$ a.î. $\alpha(x_1) = \alpha(x_2)$. Atunci $a \wedge x_1 = a \wedge x_2$ şi $a' \wedge x_1 = a' \wedge x_2$, deci $(a \wedge x_1) \vee (a' \wedge x_1) = (a \wedge x_2) \vee (a' \wedge x_2) \Leftrightarrow (a \vee a') \wedge x_1 = (a \vee a') \wedge x_2 \Leftrightarrow \mathbf{1} \wedge x_1 = \mathbf{1} \wedge x_2 \Leftrightarrow x_1 = x_2$, de unde concluzia că α este izomorfism în **B**. ■

§ 8. Produsul direct (suma directă) a unei familii de mulțimi

Definiția 8.1. Fie $(M_i)_{i \in I}$ **o familie nevidă de mulțimi. Numim** ***produsul direct*** **al acestei familii un dublet** $(P, (p_i)_{i \in I})$**, unde P este o**

mulțime nevidă iar $(p_i)_{i\in I}$ este o familie de funcții $p_i : P \to M_i$ pentru orice $i\in I$ a.î. este verificată următoarea proprietate de universalitate:

Pentru oricare alt dublet $(P', (p_i')_{i\in I})$ format din mulțimea P' şi familia de funcții $p_i': P' \to M_i$ $(i \in I)$, există o unică funcție $u: P' \to P$ a.î. $p_i \circ u = p_i'$, pentru orice $i \in I$.

Teorema 8.2. Pentru orice familie nevidă de mulțimi $(M_i)_{i\in I}$ există produsul său direct care este unic până la o bijecție.

Demonstrație. Unicitatea produsului direct. Dacă $(P, (p_i)_{i\in I})$ şi $(P', (p_i')_{i\in I})$ sunt două produse directe ale familiei $(M_i)_{i\in I}$, conform proprietății de universalitate există $u: P' \to P$ şi $v: P \to P'$ a. î $p_i \circ u = p_i'$ şi $p'_i \circ v = p_i$ pentru orice $i \in I$.

Deducem imediat că $p_i(uv) = p_i$ iar $p_i'(vu) = p_i'$ pentru orice $i \in I$. Cum şi $p_i 1_P = p_i$, $p_i' 1_{P'} = p_i'$ pentru orice $i \in I$, datorită unicității din proprietatea de universalitate deducem că $uv = 1_P$ şi $vu = 1_{P'}$, adică u este bijecție.

Existența produsului direct. Fie $P = \{f: I \to \bigcup_{i\in I} M_i / f(i) \in M_i$ pentru orice $i \in I\}$ iar $p_i : P \to M_i$, $p_i(f) = f(i)$ pentru $i \in I$ şi $f \in P$.

Se probează imediat că dubletul $(P, (p_i)_{i\in I})$ verifică proprietatea de universalitate a produsului direct de mulțimi $(M_i)_{i\in I}$. ■

Observația 8.3. În cele ce urmează, dubletul $(P, (p_i)_{i\in I})$ ce reprezintă produsul direct al familiei de mulțimi $(M_i)_{i\in I}$ se va nota prin $\prod_{i\in I} M_i$.

Pentru $j \in I$, $p_j: \prod_{i\in I} M_i \to M_j$ poartă numele de a j-a *proiecție*. De multe ori prin produs direct vom înțelege doar mulțimea subiacentă P (neglijând deci menționarea proiecțiilor).

Deoarece orice funcție f:I$\to \bigcup_{i\in I} M_i$ este determinată de f(i) pentru orice $i\in I$, notând $f(i) = x_i \in M_i$, vom scrie formal:

$$\prod_{i\in I} M_i = \{(x_i)_{i\in I} | x_i \in M_i \text{ pentru orice } i\in I\}$$

Astfel, în cazul în care I este finită I={1, 2, ..., n}, $\prod_{i\in I} M_i$ coincide de fapt cu $M_1 \times ....\times M_n$ definit în §1.

Astfel, $p_j: \prod_{i\in I} M_i \to M_j$ este definită prin $p_j((x_i)_{i\in I})=x_j$, $j\in I$. Fie acum $(M_i)_{i\in I}$ şi $(M_i')_{i\in I}$ două familii nevide de mulțimi iar $(f_i)_{i\in I}$ o familie de aplicații $f_i : M_i \to M_i'$, $(i\in I)$.

Aplicația $f: \prod_{i\in I} M_i \to \prod_{i\in I} M_i'$, $f((x_i)_{i\in I})=(f_i(x_i))_{i\in I}$ pentru orice $(x_i)_{i\in I}\in \prod_{i\in I} M_i$ poartă numele de *produsul direct* al familiei $(f_i)_{i\in I}$ de aplicații; vom nota $f = \prod_{i\in I} f_i$. Aplicația f este unică cu proprietatea că $p_i' f = f_i p_i$ pentru orice $i\in I$.

Se verifică imediat că $\prod_{i\in I} 1_{M_i} = 1_{\prod_{i\in I} M_i}$ şi că dacă mai avem o familie de mulțimi $(M_i'')_{i\in I}$ şi o familie $(f_i')_{i\in I}$ de aplicații cu $f_i' : M_i' \to M_i''$, $(i\in I)$ atunci

$$\prod_{i\in I}\left(f_i' \circ f_i\right) = \left(\prod_{i\in I} f_i'\right) \circ \left(\prod_{i\in I} f_i\right).$$

Propoziția 8.4. Dacă pentru orice $i\in I$, f_i este o funcție injectivă (surjectivă, bijectivă), atunci $f = \prod_{i\in I} f_i$ este injectivă (surjectivă, bijectivă).

Demonstrație. Într-adevăr, să presupunem că pentru orice $i\in I$, f_i este injectivă şi fie $\alpha, \beta\in\prod_{i\in I} M_i$ a.î. $f(\alpha)=f(\beta)$.

Atunci pentru orice $j\in I$, $f(\alpha)(j)=f(\beta)(j) \Leftrightarrow f_j(\alpha(j))= =f_j(\beta(j))$. Cum f_j este injectivă deducem că $\alpha(j)=\beta(j)$ iar cum j este oarecare deducem că $\alpha=\beta$, adică f este injectivă.

Să presupunem acum că pentru orice $i\in I$, f_i este surjectivă şi fie $\varphi\in\prod_{i\in I} M_i'$, adică $\varphi: I\to\bigcup_{i\in I} M_i'$ şi are proprietatea că $\varphi(j)\in M_j'$ pentru orice $j\in J$. Cum f_i este surjecție, există $x_j\in M_j$ a.î. $f_j(x_j)=\varphi(j)$. Dacă vom considera $\psi: I\to\bigcup_{i\in I} M_i$ definită prin $\psi(j)=x_j$ pentru orice $j\in I$, atunci $f(\psi)=\varphi$, adică f este surjectivă. ■

În cadrul teoriei mulțimilor, noțiunea duală celei de produs direct al unei familii de mulțimi este aceea de *sumă directă* (vom face mai tîrziu precizări suplimentare despre noțiunea de *dualizare* – vezi Definiția 1.4. de la Capitolul 5).

Definiția 8.5. Numim *sumă directă* a familiei (nevide) $(M_i)_{i\in I}$ de mulțimi, un dublet $(S, (\alpha_i)_{i\in I})$ format dintr-o mulțime nevidă S şi o familie de aplicații $\alpha_i: M_i\to S$ $(i\in I)$ ce verifică următoarea proprietate de universalitate:

Pentru oricare altă mulțime S′ şi familie $(\alpha'_i)_{i\in I}$ de aplicații cu $\alpha_i': M_i\to S'$ $(i\in I)$, există o unică aplicație $u: S\to S'$ a.î. $u\alpha_i=\alpha'_i$ pentru orice $i\in I$.

Teorema 8.6. Pentru orice familie $(M_i)_{i\in I}$ de mulțimi există şi este unică până la o bijecție suma sa directă.

Demonstrație. Unicitatea sumei directe se probează analog ca în cazul produsului direct.

Pentru a proba existența, pentru fiecare $i\in I$, considerăm $\overline{M_i}=M_i\times\{i\}$ şi $S=\bigcup_{i\in I}\overline{M_i}$ (observăm că pentru $i\neq j$, $\overline{M_i}\cap\overline{M_j}=\varnothing$).

Definind pentru orice $i \in I$, $\alpha_i : M_i \to S$ prin $\alpha_i(x) = (x, i)$ $(x \in M_i)$ se verifică imediat că dubletul $(S, (\alpha_i)_{i\in I})$ este suma directă a familiei $(M_i)_{i\in I}$ ■

Observația 8.7. Suma directă a familiei $(M_i)_{i\in I}$ o vom nota prin $\coprod_{i\in I} M_i$ (ea mai poartă numele şi de *reuniune disjunctă* a familiei $(M_i)_{i\in I}$).

Aplicațiile $(\alpha_i)_{i\in I}$, care sunt injecții, se vor numi *injecțiile canonice* (ca şi în cazul produsului direct, de multe ori când vorbim despre suma directă vom menționa doar mulțimea subiacentă, injecțiile canonice subânțelegîndu-se).

Ca şi în cazul produsului direct, dacă avem o familie de aplicații $(f_i)_{i\in I}$ aplicații cu $f_i : M_i \to M'_i$, $(i \in I)$ atunci aplicația $f : \coprod_{i\in I} M_i \to \coprod_{i\in I} M_i'$ definită prin $f((x, i)) = (f_i(x), i)$ pentru orice $i \in I$ şi $x \in M_i$ este unica aplicație cu proprietatea că $\alpha'_i f_i = f\alpha_i$ pentru orice $i \in I$; vom nota $f = \coprod_{i\in I} f_i$ şi vom numi pe f *suma directă* a aplicațiilor $(f_i)_{i\in I}$.

Se probează imediat că $\coprod_{i\in I} 1_{M_i} = 1_{\coprod_{i\in I} M_i}$ iar dacă mai avem o familie $(f'_i)_{i\in I}$ cu $f_i' : M_i' \to M_i''$ $(i \in I)$ atunci:

$$\coprod_{i\in I}\left(f_i' \circ f_i\right) = \left(\coprod_{i\in I} f_i'\right) \circ \left(\coprod_{i\in I} f_i\right).$$

Ca şi în cazul produsului direct al familiei de funcții $(f_i)_{i\in I}$ avem şi pentru $f = \coprod_{i\in I} f_i$ următorul rezultat:

Propoziția 8.8. Dacă pentru orice $i \in I$, f_i este o funcție injectivă (surjectivă, bijectivă), atunci $f = \coprod_{i\in I} f_i$ este injectivă (surjectivă, bijectivă).

§ 9 Numere cardinale. Operații cu numere cardinale.

Ordonarea numerelor cardinale

Definiția 9.1. Dacă A şi B sunt două mulțimi vom spune despre ele că sunt *cardinal echivalente* (sau mai simplu *echivalente*) dacă există o bijecție f A→B. Dacă A şi B sunt echivalente vom scrie A∼B (în caz contrar, vom scrieA≁B).

Propoziția 9.2. Relația de „∼'' este o echivalență pe clasa tuturor mulțimilor .

Demonstrație. Pentru orice mulțime A, A∼A căci funcția 1_A:A→A este o bijecție. Dacă A şi B sunt două mulțimi iar A∼B, atunci există f : A→B o bijecție. Cum şi f^{-1} : B→A este bijecție, deducem că B∼A, adică relația „∼'' este şi simetrică. Pentru a proba şi tranzitivitatea relației „∼'' fie A, B, C mulțimi a.î. A∼B şi B∼C, adică există f :A→B şi g :B→C bijecții. Cum g∘f : A →C este bijecție deducem că A∼C. ■

Teorema 9.3. (*Cantor*) Pentru orice mulțime A, A≁P(A).

Demonstrație. Să presupunem prin absurd că A∼P(A), adică există o bijecție f:A→P(A). Dacă vom considera mulțimea B={x∈A|x∉f(x)}, atunci cum B∈P(A) şi f este în particular surjecție, deducem că există a∈A a.î. B=f(a). Dacă a∈B, atunci a∉B - absurd, pe când dacă a∉B atunci a∉f(a), deci a∈B – din nou absurd!. ■

Teorema 9.4. (*Cantor, Bernstein*) Fie A_0, A_1, A_2 trei mulțimi a.î. $A_2 \subseteq A_1 \subseteq A_0$. Dacă $A_0 \sim A_2$, atunci $A_0 \sim A_1$.

Demonstrație. Cum $A_0 \sim A_2$, atunci există o bijecție $f:A_0 \to A_2$. Dacă vom considera mulțimile $A_i = f(A_{i-2})$ pentru $i \geq 3$, atunci în mod evident: $...A_{n+1} \subseteq A_n \subseteq ... \subseteq A_2 \subseteq A_1 \subseteq A_0$ (ținând cont de faptul că $A_2 \subseteq A_1 \subseteq A_0$). Să considerăm mulțimea $A = \bigcap_{i \geq 0} A_i = \bigcap_{i \geq 1} A_i$ şi să demonstrăm că

(1) $A_0 = \left[\bigcup_{i \geq 0} (A_i - A_{i+1})\right] \bigcup A$. Incluziunea de la dreapta la stânga este evidentă. Pentru a o proba pe cealaltă, fie $x \in A_0$. Dacă $x \in A$ atunci $x \in \left[\bigcup_{i \geq 0} (A_i - A_{i+1})\right] \bigcup A$. Dacă $x \notin A$, există $i \in \mathbb{N}$ a.î. $x \notin A_i$ şi cum $x \in A_0$, $i \geq 1$. Fie deci $n \geq 1$ cel mai mic număr natural pentru care $x \notin A_n$. Atunci $x \in A_{n-1}$ şi deci $x \in A_{n-1} - A_n$, de unde $x \in \left[\bigcup_{i \geq 0} (A_i - A_{i+1})\right] \bigcup A$. Astfel avem probată şi incluziunea de la stânga la dreapta, rezultând astfel egalitatea (1).

Analog se probează şi egalitatea: (2) $A_1 = \left[\bigcup_{i \geq 1} (A_i - A_{i+1})\right] \bigcup A$.

Dacă vom considera familiile de mulțimi $(B_i)_{i \in I}$ şi $(C_i)_{i \in I}$ definite astfel:

$$B_0 = A \quad \text{şi} \quad B_i = A_{i-1} - A_i \text{ pentru } i \geq 1$$

$$C_0 = A \quad \text{şi} \quad C_i = \begin{cases} A_{i+1} - A_{i+2}, & \textit{pentru } i \textit{ impar} \\ A_{i-1} - A_i, & \textit{pentru } i \textit{ par} \end{cases}$$

atunci se observă imediat că pentru $i, j \in \mathbb{N}$, $i \neq j \Rightarrow B_i \cap B_j = C_i \cap C_j = \varnothing$ iar din (1) şi (2) deducem că:

(3) $A_0 = \bigcup_{i \geq 0} B_i$ şi $A_1 = \bigcup_{i \geq 0} C_i$.

Considerăm de asemenea şi familia de funcții $(f_i)_{i \geq 0}$ cu $f_i : B_i \to C_i$ definită astfel

$$f_i = \begin{cases} 1_A, & pentru\ \ i = 0 \\ 1_{A_{i-1}-A_i}, & pentru\ \ i\ \ par \\ f_{|A_{i-1}-A_i}, & pentru\ \ i\ \ impar \end{cases}$$

(să observăm că pentru i impar, dacă $x \in A_{i-1}-A_i \Rightarrow f(x) \in A_{i+1}-A_{i+2}$, adică f_i este corect definită).

Dacă vom arăta că pentru orice $i \in \mathbb{N}$, f_i este bijectivă (suficient doar pentru i impar), atunci ținând cont de (3) vom deduce imediat că $A_0 \sim A_1$. Fie deci i impar şi $f_i = f_{|A_{i-1}-A_i}$. Deoarece f este bijectivă deducem imediat că f_i este injectivă. Pentru a proba surjectivitatea lui f_i fie $y \in A_{i+1}-A_{i+2}$, adică $y \in A_{i+1}$ şi $y \notin A_{i+2}$. Cum $A_{i+1} = f(A_{i-1})$, deducem că există $x \in A_{i-1}$ a.î. $y = f(x)$ şi deoarece $y \notin A_{i+2}$, deducem că $x \notin A_i$, adică $x \in A_{i-1}-A_i$. Astfel $y = f_i(x)$, adică f_i este şi surjectivă, deci bijectivă. Aşa după cum am observat anterior se poate construi imediat o bijecție de la A_0 la A_1, adică $A_0 \sim A_1$ şi cu aceasta teorema este complet demonstrată. ■

Corolarul 9.5. Fie A, B, A′, B′ mulțimi a.î. $A' \subseteq A$, $B' \subseteq B$ şi $A \sim B'$ iar $B \sim A'$. Atunci $A \sim B$.

Demonstrație. Cum $A \sim B'$ există o bijecție $f : A \to B'$ astfel că dacă vom considera $B'' = f(B')$ avem că $A' \sim B''$. Cum $B \sim A'$ deducem că $B'' \sim B$. Obținem astfel că $B'' \subseteq B' \subseteq B$ şi $B'' \sim B$. Conform Teoremei 9.4., $B' \sim B$ şi cum $B' \sim A$, deducem că $B \sim A$, adică $A \sim B$. ■

Definiția 9.6. Dacă A este o mulțime, prin *numărul cardinal* al lui A înțelegem clasa de echivalență a lui A (notată $\overline{\overline{A}}$) relativă la relația de echivalență $\sim$.

Deci $B \in \overline{\overline{A}} \Leftrightarrow A \sim B$.

Vom numi *secțiuni* ale lui $\mathbb{N}$ mulțimile de forma $S_n = \{0, 1, ..., n-1\}$ formate din n elemente $(n \in \mathbb{N}^*)$; convenim să notăm pentru

$n \in \mathbb{N}^*$, $n = \overline{\overline{S_n}}$. Convenim de asemenea să notăm 0=cardinalul mulțimii vide şi prin $\chi_0 (alef\ zero)$ cardinalul mulțimii numerelor naturale $\mathbb{N}$.

În continuare vom defini operațiile clasice cu numere cardinale : suma, produsul şi ridicarea la putere.

Definiția 9.7. Fie $(m_i)_{i \in I}$ o familie de numere cadinale, unde $m_i = \overline{\overline{M_i}}$ pentru orice $i \in I$. Definim *suma* (respectiv *produsul*) *familiei* $(m_i)_{i \in I}$ prin egalitatea $\sum_{i \in I} m_i = \overline{\overline{\coprod_{i \in I} M_i}}$ (respectiv $\prod_{i \in I} m_i = \overline{\overline{\prod_{i \in I} M_i}}$). Dacă I este o mulțime finită, I={1, 2, .., n} vom scrie $\sum_{i \in I} m_i = m_1 + ... + m_n$ (respectiv $\prod_{i \in I} m_i = m_1 .. . m_n$).

Observația 9.8. Din Propozițiile 8.8. şi respectiv 8.7. deducem că Definiția 9.7. este corectă (în sensul că $\sum_{i \in I} m_i$ nu depinde de modul de alegere a mulțimilor M_i pentru care $m_i = \overline{\overline{M_i}}$).

Definiția 9.9. Fie $m = \overline{\overline{M}}$ şi $n = \overline{\overline{N}}$ două numere cardinale. Definim n^m ca fiind numărul cardinal al mulțimii Hom (M, N)={f :M→N}.

Dacă mai avem două mulțimi M´şi N´ a.î. $m = \overline{\overline{M'}}$ şi $n = \overline{\overline{N'}}$ atunci există două bijecții f : M→M´ şi g : N→N´. Se verifică imediat că φ:**Hom** (M, N) →**Hom** (M´, N´) definită prin $\varphi(\alpha) = g \circ \alpha \circ f^{-1}$ pentru orice $\alpha \in$**Hom** (M, N) este bijecție, de unde deducem că Definiția 9.9. este corectă.

Observația 9.10. Principalele proprietăți ale operațiilor de adunare, înmulțire şi ridicare la putere a numerelor cardinale vor fi puse în evidență într-o viitoare lucrare, sub formă de exerciții propuse.

Definiția 9.11. Dacă $m = \overline{\overline{M}}$ şi $n = \overline{\overline{N}}$, vom spune că m este *mai mic sau egal* cu n (sau că n este *mai mare sau egal* cu m) şi vom scrie $m \leq n$, dacă există o submulțime $N' \subseteq N$ a.î. $M \sim N'$.

Vom spune că m este *strict mai mic* decât n (sau că n este *strict mai mare* ca m) şi vom nota $m < n$ dacă $m \leq n$ şi $m \neq n$.

Observaţia 9.12. Să presupunem că avem mulţimile M, N, P, Q a.î. $M \sim P$ şi $N \sim Q$ şi să mai presupunem că există $N' \subseteq N$ a.î. $M \sim N'$. Considerăm bijecţia $f : N \to Q$ şi să notăm cu $Q' = f(N')$. Deducem că $N' \sim Q'$, de unde $P \sim Q'$, adică Definiţia 9.11. este corectă (în sensul că definirea relaţiei $\leq$ nu depinde de alegerea reprezentanţilor).

Propoziţia 9.13. Fie m, n, p numere cardinale . Atunci:

(i) $m \leq m$

(ii) $m \not< m$

(iii) $m \leq n$ şi $n \leq m \Rightarrow m = n$

(iv) $m \leq n$ şi $n \leq p \Rightarrow m \leq p$

(v) $m < n$ şi $n < p \Rightarrow m < p$.

Demonstraţie. (i) şi (ii) sunt evidente.
(iii). Rezultă din Corolarul 9.5.

(iv). Să presupunem că $m = \overline{\overline{M}}$, $n = \overline{\overline{N}}$, $p = \overline{\overline{P}}$. Din ipotezăm avem că există $N' \subseteq N$ şi $P' \subseteq P$ a.î. $M \sim N'$ şi $N \sim P'$, adică avem bijecţia $f : N \to P'$. Dacă notăm $P'' = f(N')$, evident că $N' \sim P''$, deci $M \sim P''$, de unde deducem că $m \leq p$.

(v). Mai trebuie să probăm că dacă $m \neq p$, atunci $M \not\sim P$. Dacă $M \sim P$, atunci $N' \sim P$, deci $p \leq n$. Cum $n \leq p$, atunci din (iii) deducem că $n = p$ - absurd. ■

Observaţia 9.14. Ca şi în cazul operaţiilor cu numere cardinale, alte proprietăţi legate de compararea numerelor cardinale le vom pune în evidenţă sub formă de exerciţii propuse într-o viitoare lucrare.

Fie acum $m = \overline{\overline{M}}$ şi $\varphi : \mathbf{Hom}(M, \{0, 1\}) \to \mathbf{P}(M)$ definită prin $\varphi(f) = f^{-1}(\{1\})$, pentru orice $f : M \to \{0, 1\}$. Se probează imediat că φ este

o bijecţie, de unde deducem că **P**(M) ~ **Hom** (M, {0, 1}), adică $\overline{\overline{P(M)}} = 2^{\mathrm{m}}$. Din acest ultim rezultat şi Teorema 9. 3. deducem:

Corolarul 9. 15. Dacă m este un număr cardinal, atunci m < 2^{m}.

Acest Corolar ne arată că pentru un număr cardinal m obţinem următorul şir strict crescător de numere cardinale: $2 < 2^{2^m} < 2^{2^{2^m}} < \ldots$.

Cardinalul 2^{χ_0} îl vom nota prin c şi îl vom numi *puterea continuului.*

§10 Mulţimi numărabile. Mulţimi finite şi mulţimi infinite

Definiţia 10.1. Vom spune despre o mulţime M că este *numărabilă* dacă M ~ ℕ, adică $\overline{\overline{M}} = \chi_0$. Dacă $\overline{\overline{M}} \le \chi_0$ vom spune că M este *cel mult numărabilă* ; în caz contrar, spunem că M este *nenumărabilă.*

Propoziţia 10.2. Dacă M şi P sunt două mulţimi numărabile disjuncte, atunci M∪P este numărabilă.

Demonstraţie. Cum M şi P sunt numărabile avem două bijecţii f:ℕ→M şi g:ℕ→P. Se probează imediat că h:ℕ→M∪P,

$$h(n)=\begin{cases} f\left(\frac{n}{2}\right) & daca\ n\ este\ par \\ g\left(\frac{n+1}{2}\right) & daca\ n\ este\ impar \end{cases}$$

este bijecţie, de unde concluzia că M∪P este numărabilă.■

Corolar 10.3. O reuniune finită de mulţimi numărabile disjuncte este numărabilă.

Lema 10.4. Funcția *numărare diagonală* f : $\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ definită pentru (x, y)$\in\mathbb{N}\times\mathbb{N}$ prin f(x, y) $=\frac{(x+y+1)(x+y)}{2}+x$ este bijectivă.

Demonstrație. Să arătăm la început că dacă (x, y), (x´, y´)$\in\mathbb{N}\times\mathbb{N}$ şi f (x, y)=f (x´, y´), atunci x=x´ şi y=y´.

Să presupunem prin absurd că x≠x´ (de exemplu x > x´, adică x=x´+r cu r$\in\mathbb{N}$*). Obținem atunci egalitatea:

$$\frac{(x'+r+y+1)(x'+r+y)}{2}+r=\frac{(x'+y'+1)(x'+y')}{2}$$

de unde deducem că

$$(x'+r+y+1)(x'+r+y)<(x'+y'+1)(x'+y')$$

şi astfel y´>r+y. Alegând y´=r+y+s cu s$\in\mathbb{N}$* obținem că $\frac{z(z-1)}{2}+r=\frac{(z+s)(z+s+1)}{2}$, unde z=x´+r+y+1, lucru absurd deoarece $\frac{z(z-1)}{2}+r<\frac{z(z-1)}{2}+z=\frac{(z+1)z}{2}\le\frac{(z+s)(z+s-1)}{2}$.

Prin urmare x=x´ iar egalitatea f (x, y)=f (x´, y´) devine

$$\frac{(x'+y+1)(x'+y)}{2}=\frac{(x'+y'+1)(x'+y')}{2}$$

de unde obținem imediat că y=y´, adică f este injectivă.

Pentru a proba surjectivitatea lui f vom arăta prin inducție matematică că pentru orice n$\in\mathbb{N}$ există x, y$\in\mathbb{N}$ a.î. f (x, y)=n. Avem că 0=f (0, 0) şi să presupunem că n=f (x, y) cu x, y$\in\mathbb{N}$.

Dacă y$\in\mathbb{N}$* avem n+1=f (x, y)+1=$\frac{(x+y+1)(x+y)}{2}$ +x+1=

=f(x+1, y-1) pe când dacă y=0 avem

n+1=$\frac{x(x+1)}{2}+x+1=\frac{(x+1)(x+2)}{2}$ =f (0, x+1).

Dacă x=y=0, atunci n=0 , deci n+1=1=f (0, 1). ■

Corolar 10.5. $\chi_0 \cdot \chi_0 = \chi_0$.

Propoziția 10.6. $\mathbb{Z}$, $\mathbb{Z}^*$ **şi** $\mathbb{Q}$ **sunt mulțimi numărabile.**

Demonstrație. Se probează imediat că f:$\mathbb{Z}\to\mathbb{N}$

$$f(x)=\begin{cases}2x \ \ daca \ \ x\geq 0\\ -2x-1 \ \ daca \ \ x<0\end{cases}$$

şi g:$\mathbb{Z}\to\mathbb{Z}^*$,
$$g(x)=\begin{cases}x+1 \ \ daca \ x\geq 0\\ x \ \ daca \ \ x<0\end{cases}$$

sunt bijective. Să probăm acum că şi $\mathbb{Q}$ este numărabilă. Cum $\mathbb{N}\subseteq\mathbb{Q}$ deducem că $\overline{\overline{Q}}\geq\chi_0$. Să considerăm f:$\mathbb{Z}\times\mathbb{Z}^*\to\mathbb{Q}$, $f(x,y)=\frac{x}{y}$ pentru orice x, y$\in\mathbb{Z}\times\mathbb{Z}^*$.
Cum f este surjectivă, conform Propoziției 3.8. de la Capitolul 1, există g:$\mathbb{Q}\to\mathbb{Z}\times\mathbb{Z}^*$ a.î. $f\circ g=1_{\mathbb{Q}}$. Conform Propoziției 3.7. de la Capitolul 1, deducem că g este injectivă, adică $\overline{\overline{Q}}\leq\overline{\overline{Z\times Z^*}}=\chi_0\cdot\chi_0=\chi_0$, de unde egalitatea $\overline{\overline{Q}}=\chi_0$, adică $\mathbb{Q}$ este numărabilă. ■

Propoziția 10.7. Mulțimea $\mathbb{R}$ **a numerelor reale este nenumărabilă**.

Demonstrație. Deoarece f :$\mathbb{R}\to(0,\ 1)$, $f(x)=\frac{1}{2}+\frac{1}{\pi}arctg\ x$ este bijectivă, este suficient să arătăm că intervalul (0, 1) nu este o mulțime numărabilă iar pentru aceasta să arătăm că orice funcție f :$\mathbb{N}\to(0,1)$ nu este surjectivă (*procedeul diagonal al lui Cantor*).

Pentru fiecare n $\in\mathbb{N}$ putem scrie pe f (n) ca fracție zecimală: f (n)=0, $a_{n1}\ a_{n2}$ ..... a_{nn} .... cu $a_{ij}\in\{0,\ 1,\ ...\ ,\ 9\}$.

Dacă vom considera b$\in(0,1)$

$$b=0,\ b_1\ b_2\ ....b_n\ ...$$

unde pentru orice $k\in\mathbb{N}^*$ $b_k\notin\{0, 9, a_{k\,k}\}$, atunci $b\notin$**Im**(f), adică f nu este surjectivă. ■

Definiția 10.8. Vom spune despre o mulțime M că este *infinită :*

(i) ***în sens Dedekind*, dacă există $M'\subset M$ a.î. $M'\sim M$**

(ii) ***în sens Cantor,* dacă conține o submulțime numărabilă**

(iii) ***în sens obișnuit,* dacă $M \nsim S_n$ pentru orice $n\in\mathbb{N}^*$ (unde $S_n=\{1, 2, ..., n\}$) .**

Teorema 10.9. Cele trei definiții ale mulțimilor infinite din cadrul Definiției 10.8. sunt echivalente două câte două.

Demonstrație. (i)⇒(ii). Fie M o mulțime infinită în sens Dedekind ; atunci există $M'\subset M$ şi o bijecție $f:M\to M'$**.** Cum $M'\subset M$, există $x_0\in M$ a.î. $x_0\notin M'$. Construim prin recurență şirul de elemente $x_1=f(x_0)$, $x_2=f(x_1)$, ..., $x_n=f(x_{n-1})$, ... şi să arătăm că funcția $\varphi:\mathbb{N}\to M$ $\varphi(n)=x_n$ pentru orice $n\in\mathbb{N}$ este injectivă. Pentru aceasta vom demonstra că dacă n, $n'\in\mathbb{N}$, $n\neq n'$, atunci $\varphi(n)\neq\varphi(n')$. Vom face lucrul acesta prin inducție matematică după n.

Dacă n=0, atunci $n'\neq 0$, de unde $\varphi(0)=x_0$ şi $\varphi(n')=f(x_{n'-1})\in$ $\in M'$ şi cum $\varphi(0)=x_0\notin M'$ deducem că $\varphi(n')\neq\varphi(0)$. Să presupunem acum că pentru orice $n\neq m'$ $\varphi(n)\neq\varphi(m')$ şi să alegem acum $n'\neq n+1$. Dacă $n'=0$, atunci $\varphi(n')=\varphi(0)=x_0\notin M'$ şi $x_{n+1}=f(x_n)\in M'$**,** deci $\varphi(n+1)\neq\varphi(n')$. Dacă $n'\neq 0$, atunci $\varphi(n')=f(x_{n'-1})$ şi $\varphi(n+1)=f(x_n)$. Cum $n'-1\neq n$, atunci $x_{n'-1}\neq x_n$ şi cum f este injectivă deducem că $f(x_{n'-1})\neq f(x_n)$, adică $\varphi(n')\neq\varphi(n+1)$. Rezultă deci că φ este injectivă şi deci $\varphi(\mathbb{N})\subseteq M$ este o submulțime numărabilă.

(ii)⇒(i). Fie M o mulțime infinită în sensul Cantor, adică există $M'\subseteq M$ a.î. $M'\sim\mathbb{N}$ (fie $f:\mathbb{N}\to M'$ o funcție bijectivă). Se observă imediat că $\varphi : M\to M\setminus\{f(0)\}$ definită prin

$$\varphi(x)=\begin{cases} x \ \ daca \ \ x \notin M' \\ f(n+1) \ \ daca \ \ x=f(n) \ \ cu \ \ n \in N \end{cases}$$

este bine definită şi să arătăm că φ este chiar bijecție.

Fie deci x, x′ ∈ M a.î. φ (x) = φ (x′).

Deoarece M=M′∪ (M \ M′) şi φ (x) = φ (x′), atunci x, x′∈ ∈M′ sau x, x′∉ M′. Dacă x, x′∉ M′, atunci în mod evident din φ (x) = =φ(x′) deducem că x=x′. Dacă x, x′∈ M′, atunci dacă x=f(k), x′=f(t) deducem că f (k+1)=f (t+1), de unde k+1=t+1 ⇔ k=t ⇒x=x′.

Să arătăm acum că φ este surjectivă. Pentru aceasta fie y ∈ M \ {f (0)} . Dacă y∉M′ atunci y=φ (y), iar dacă y∈M′ , atunci y=f (n) cu n∈ℕ. Cum y≠f (0), atunci n≠0⇒ n≥1 deci putem scrie y=f (n-1+1)=φ (n-1).

(ii)⇒(iii). Această implicație este evidentă deoarece $\mathbb{N} \sim S_n$ pentru orice n∈ℕ* .

(iii)⇒(ii). Vom utiliza următorul fapt: dacă M este o mulțime infinită în sens obişnuit, atunci pentru orice n∈ℕ* există o funcție injectivă φ:S_n →M.

Vom proba lucrul acesta prin inducție matematică referitor la n.

Pentru n=1 există o funcție injectivă φ:S_1→M (deoarece M≠Ø). Să presupunem acum că pentru n∈ℕ* există φ:S_n→M injectivă. Cum am presupus că M este infinită în sens obişnuit, atunci φ (S_n) ≠ M, deci există x_0∈M a.î. x_0 ∉ φ (S_n).

Atunci ψ :S_{n+1}→M, $\psi(x)=\begin{cases} \varphi(x) \ \ pentru \ \ x \in S_n \\ x_0 \ \ pentru \ \ x=n+1 \end{cases}$ este în mod evident funcție injectivă.

Să trecem acum la a demonstra efectiv implicația (iii)⇒(ii). Din rezultatul expus anterior deducem că :

$$M_k=\{\varphi:S_k \rightarrow M \mid \varphi \text{ este injecție}\} \neq \emptyset$$

pentru orice k∈ℕ*. Cum pentru k≠k′ , $S_k \cap S_{k'}=\emptyset$, deducem că $M_k \cap M_{k'}=\emptyset$. Conform axiomei alegerii aplicată mulțimii

$T=\{ M_k : k\in\mathbb{N} \}$, există $S\subseteq T$ a.î. $S\cap M_k\neq\emptyset$ şi este formată dintr-un singur element. Atunci $M'=\bigcup_{\varphi\in S}\mathrm{Im}(\varphi)$ este o submulțime numărabilă a lui M. ■

CAPITOLUL 2: GRUPURI

§1. Operații algebrice. Monoizi. Morfisme de monoizi. Produse directe finite de monoizi

Definiția 1.1. Fiind dată o multime nevidă M, numim ***operatie algebrică*** (internă) sau ***lege de compoziție*** (internă) pe M orice funcție $\varphi:M\times M\to M$.

Pentru uşurința scrierii vom nota pentru $x, y\in M$ pe $\varphi(x, y)$ (care se mai numeşte şi ***compusul*** lui x cu y) prin xoy sau pur şi simplu prin xy (convenim să spunem că am notat operația algebrică φ ***multiplicativ***).

În anumite situații folosim pentru φ şi notația ***aditivă*** „+”.

Exemple **1. Dacă T este o mulțime nevidă iar M=P(T), în capitolul precedent am definit pe M operațiile algebrice de intersecție, reuniune, diferență şi diferența simetrică.**

2. Dacă A este o mulțime nevidă iar Hom**(A)={f:A→A}, atunci pe** Hom**(A) avem operația de compunere a funcțiilor: φ :** Hom**(A)** × Hom**(A)** → Hom**(A), φ(f, g) = fog pentru orice f, g ∈** Hom**(A).**

Pe parcursul acestei lucrări vom mai pune în evidență alte mulțimi şi operații algebrice pe acestea (inclusiv mulțimile numerelor întregi $\mathbb{Z}$, raționale $\mathbb{Q}$, reale $\mathbb{R}$ şi complexe $\mathbb{C}$ precum şi operațiile de adunare şi înmulțire pe acestea).

Definiția 1.2. Dacă M este mulțime nevidă, vom spune despre o operație algebrică de pe M (notată multiplicativ) că este:

(i) ***comutativă*** – dacă pentru oricare $x, y\in M$, $xy=yx$

(ii) ***asociativă*** – dacă pentru oricare $x, y, z\in M$, $(xy)z=x(yz)$.

Operaţiile de intersecţie, reuniune şi diferenţă simetrică sunt exemple de operaţii ce sunt simultan comutative şi asociative, pe când compunerea funcţiilor nu este operaţie comutativă fiind însă asociativă.

Dacă o operaţie algebrică de pe M este asociativă, atunci pentru a scrie compunerea a trei elemente x, y, z din M (sau mai multe) nu mai este necesar să folosim parantezele, astfel că în loc să scriem (xy)z sau x(yz) vom scrie xyz.

Pentru n elemente $x_1,\ldots,x_n$ ($n\in\mathbb{N}$) din M utilizăm de multe ori notaţiile:

$x_1x_2\ldots\ldots x_n=\prod_{i=1}^{n} x_i$ (când operaţia algebrică asociativă este notată multiplicativ) sau

$x_1+x_2+\ldots+x_n \quad =\sum_{i=1}^{n} x_i$ (când aceeaşi operaţie algebrică asociativă este notată aditiv).

Dacă $x_1=x_2=\ldots=x_n=x$ şi $n\in\mathbb{N}^*$ convenim să notăm $x_1x_2\ldots x_n=x^n$ dacă operaţia algebrică este notată multiplicativ şi $x_1+x_2+\ldots+x_n = nx$ dacă ea este notată aditiv.

Definiţia 1.3. Fie M o mulţime nevidă pe care avem o operaţie algebrică. Vom spune că un element $e\in M$ este ***element neutru*** pentru operaţia algebrică respectivă dacă pentru orice $x\in M$, $xe = ex = x$.

Observaţia 1.4.

1. Dacă o operaţie algebrică de pe M ar avea două elemente neutre e, $e'\in M$, atunci $ee'=e$ (dacă gândim pe e' element neutru) şi tot $ee'=e'$ (dacă gândim pe e element neutru) astfel că $e=e'$. Deci, elementul neutru al unei operaţii algebrice (dacă există !) este unic.

2. În cazul adoptării notaţiei multiplicative pentru o operaţie algebrică, elementul său neutru (dacă există) va fi notat prin 1, iar în cazul adoptării notaţiei aditive acesta se va nota prin 0.

Exemple **1. Dacă $T\neq\emptyset$, atunci pentru operațiile algebrice $\cap,\cup$ şi Δ de pe $M=P(T)$ elementele neutre sunt T, $\emptyset$ şi respectiv $\emptyset$.**

2. Dacă $A\neq\emptyset$, atunci pentru compunerea funcțiilor de pe $Hom(A)$, 1_A este elementul neutru.

Definiția 1.5. Un dublet $(M, \cdot)$ format dintr-o mulțime nevidă M şi o operație algebrică pe M se zice ***semigrup*** dacă operația algebrică respectivă este asociativă. Dacă operația algebrică are şi element neutru, semigrupul $(M, \cdot)$ se zice ***monoid***. Dacă operația algebrică este comutativă, monoidul se zice ***comutativ***.

De multe ori, în cazul unui semigrup se specifică doar mulțimea subiacentă M (fară a se mai specifica operația algebrică de pe M; dacă este pericol de confuzie atunci şi aceasta trebuie neapărat menționată).

Exemple **1.Dacă $T\neq\emptyset$ şi $M=P(T)$, atunci $(M, \cap)$, $(M, \cup)$ şi (M, Δ) sunt monoizi comutativi.**

2.Dacă $A\neq\emptyset$, atunci $(Hom(A),o)$ este monoid necomutativ.

Reamintim că în §3 de la Capitolul 1 am introdus mulțimea $\mathbb{N}$ a numerelor naturale. În continuare vom defini două operații algebrice pe $\mathbb{N}$: *adunarea* (notată „+") şi *înmulțirea* (notată „·") în raport cu care $\mathbb{N}$ devine monoid.

Teorema 1.6. Există o unică operație algebrică pe $\mathbb{N}$ pe care o vom nota prin „+" şi o vom numi *adunarea numerelor naturale* **a. î. pentru orice $m, n\in\mathbb{N}$ să avem :**

A_1 : $0+m=m$

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

Demonstrație. Să probăm la început unicitatea şi pentru aceasta să presupunem că mai există o operație algebrică $\oplus$ pe $\mathbb{N}$ ce verifică A_1 şi A_2.

Fie $P=\{n\in\mathbb{N} \mid n+m=n\oplus m$, 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 3.19 de la Capitolul 1 există o unică funcţie $f_m: \mathbb{N} \to \mathbb{N}$ a. î. $f_m(0)=m$ 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 $s(n)+m= f_m(s(n))=s(f_m(n))=s(n+m)$. ■

Observaţia 1.7. Axiomele A_1–A_2 poartă numele de *axiomele adunării numerelor naturale*.

Propoziţia 1.8. Pentru orice $m, n \in \mathbb{N}$ avem

A_1^0 **: $m+0=m$**

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.■

Propoziţia 1.9. Dubletul $(\mathbb{N}, +)$ este monoid comutativ cu proprietatea de simplificare.

Demonstraţie. 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 (deoarece s este injecție). Deducem că P=ℕ, adică adunarea numerelor naturale este comutativă .

Pentru a demonstra asociativitatea adunării numerelor naturale, să considerăm

$P=\{n\in\mathbb{N}: (n+m)+p=n+(m+p)$ 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 $s(n)+(m+p)=s(n+(m+p))$ şi 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 $0\in P$ şi 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 $s(p)\in P$ şi astfel din nou $P=\mathbb{N}$. ■

Observația 1.10. Dacă $n\in\mathbb{N}$, atunci $s(n)=s(n+0)=n+s(0)=n+1$.

Propoziția 1.11. Dacă $m, n\in\mathbb{N}$ şi $m+n=0$, atunci $m=n=0$.

Demonstrație. Dacă $m \neq 0$ sau $n \neq 0$, atunci, conform Lemei 3.18 de la Capitolul 1 există $p, q\in\mathbb{N}$ a. î. $m = s(p)$ sau $n = s(q)$. În primul caz, obținem că $m+n = s(p)+n = s(p+n) \neq 0$ – absurd ! şi analog în al doilea caz. Deci $m = n = 0$. ■

Propoziția 1.12. Există o unică operație algebrică pe $\mathbb{N}$ notată „$\cdot$" şi numită *înmulțirea numerelor naturale* **a.î. 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 3.19 de la Capitolul 1 există o unică funcție $g_m:\mathbb{N}\to\mathbb{N}$ a.î. $g_m(0)=0$ şi $f_m\circ g_m = g_m\circ s$.

Definim $m\cdot n=g_m(n)$ şi 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 şi I_2 se probează analog ca în cazul adunării. ■

Observația 1.13. I_1 şi 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 1.14. Înmulțirea numerelor naturale este distributivă la stânga față de adunarea numerelor naturale.

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

Ținând cont de 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 $P=\mathbb{N}$. ■

Propoziția 1.15. Dubletul ($\mathbb{N}$, ·) este monoid comutativ. Dacă $m, n\in\mathbb{N}$ şi $mn=0$, atunci $m=0$ sau $n=0$.

Demonstrație. Pentru a proba asociativitatea înmulțirii fie $P=\{p\in\mathbb{N} : (mn)p=m(np)$ 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 1.14.), 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 înmulțirii numerelor naturale.

Pentru a proba comutativitatea înmulțirii 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 $P=\mathbb{N}$.

Fie acum $m, n\in\mathbb{N}$ a.î. $mn=0$ şi să presupunem că $m\neq 0$. Atunci $m=s(k)$ cu $k\in\mathbb{N}$ (conform Lemei 3.18 de la Capitolul 1) şi cum $0=mn=s(k)n=kn+n$ trebuie ca $n=n\cdot k=0$ (conform Propoziției 1.11). ■

Definiția 1.16. 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 $p\in\mathbb{N}$ a.î. $m+p=n$; 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 1.17. Dacă $m, n\in\mathbb{N}$ şi $m<n$, atunci $s(m)\leq n$.

Demonstrație. Deoarece $m<n$, există $p\in\mathbb{N}^*$ a.î. $m+p=n$. Cum $p\in\mathbb{N}^*$, există $k\in\mathbb{N}$ a. î. $p=s(k)$ (conform Lemei 3.18 de la Capitolul I). 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 1.18. Pentru orice $n\in\mathbb{N}$, $n<s(n)$.

Propoziția 1.19. Dubletul $(\mathbb{N}, \leq)$ este o mulțime total ordonată.

Demonstrație. Deoarece pentru orice $n\in\mathbb{N}$, $n+0=n$ deducem că $n\leq n$, adică relația $\leq$ este reflexivă. Fie acum $m, n\in\mathbb{N}$ a. î. $m\leq n$ şi $n\leq m$. Atunci există $p, q\in\mathbb{N}$ a.î. $m+p=n$ şi $n+q=m$. Deducem că $n+(p+q)=n$, de

unde p+q=0 (conform Propoziției 1.9.), iar de aici p=q=0 (conform Propoziției 1.11.), adică m=n, deci relația $\leq$ este antisimetrică .

Fie acum m, n, p$\in\mathbb{N}$ a. î. m$\leq$n şi n$\leq$p. Atunci există r, s$\in\mathbb{N}$ a. î. m+r=n şi n+s=p. Deducem imediat că m+(r+s)=p, adică m$\leq$p, deci relația $\leq$ este şi tranzitivă, adică $\leq$ este o relație de ordine pe $\mathbb{N}$.

Pentru a proba că ordinea $\leq$ de pe $\mathbb{N}$ este totală, fie m$\in\mathbb{N}$ fixat iar

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

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 1.17. avem s(n)$\leq$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 $\leq$ de pe $\mathbb{N}$ este totală. ■

Observația 1.20. Relația de ordine $\leq$ definită anterior pe $\mathbb{N}$ poartă numele de *ordinea naturală* de pe $\mathbb{N}$.

Teorema 1.21. Dubletul ($\mathbb{N}$, $\leq$) este o mulțime bine ordonată.

Demonstrație. Trebuie să demonstrăm că orice submulțime nevidă A$\subseteq\mathbb{N}$ are un cel mai mic element. Pentru aceasta fie:

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

Evident $0\in P$. Dacă pentru orice $n\in P$ ar rezulta $s(n)\in P$, atunci am deduce că $P=\mathbb{N}$, astfel că alegând un $x_0\in A$ atunci $x_0\in P$, deci $s(x_0)\in P$. În particular ar rezulta că $s(x_0)\leq x_0$ – absurd !.

Deducem că $P\neq\mathbb{N}$, adică există $a\in P$ a.î. $s(a)\notin P$. Vom demonstra că $a\in A$ şi că a este cel mai mic element al lui A.

Dacă $a\notin A$, atunci pentru orice $x\in A$ avem a<x, de unde $s(a)\leq x$ (conform Lemei 1.17.), adică $s(a)\in P$ – absurd !, deci $a\in A$ şi cum a $\in P$ deducem că a $\leq$x pentru orice $x\in A$, adică a este cel mai mic element al lui A . ■

Corolar 1.22. Orice şir descrescător de numere naturale este staționar.

Demonstrație. 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 1.21 mulțimea A are un cel mai mic element a_k; atunci pentru orice $m\geq k$ avem $a_m \geq a_k$ şi cum $a_k \geq a_m$ deducem că $a_m = a_k$, adică şirul $(a_n)_{n\in\mathbb{N}}$ este staționar . ■

Corolar 1.23. În $\mathbb{N}$ nu putem găsi un şir strict descrescător şi infinit de numere naturale.

Corolar 1.24. Fie $P\subseteq\mathbb{N}$ a.î. pentru orice $n\in\mathbb{N}$ $(x<n \Rightarrow x\in P) \Rightarrow n\in P$. Atunci $P=\mathbb{N}$.

Demonstrație. Fie $A=\mathbb{N}\setminus P\subseteq\mathbb{N}$ şi să presupunem prin absurd că $A\neq\emptyset$. Conform Teoremei 1.21. mulțimea A va avea un cel mai mic element $a\in A$. Cum pentru $x\in\mathbb{N}$, $x<a \Rightarrow x\notin A \Rightarrow x\in P$, conform ipotezei, adică $a\in P$ şi astfel $a\notin A$ – absurd !. Deci $A=\emptyset$, de unde $P=\mathbb{N}$. ■

Corolar 1.25. (*Teorema împărțirii 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 a.î. $m=n\cdot c+r$ şi $r<n$.

Demonstrație. Fie $A=\{s\in\mathbb{N}$: există $p\in\mathbb{N}$ a.î. $m=np+s\}\subseteq\mathbb{N}$.
Deoarece $m=0\cdot m+m$ deducem că $m\in A$, adică $A\neq\emptyset$. Conform Teoremei 1.21. mulțimea A posedă un cel mai mic element $r\in A$. Atunci, există $c\in\mathbb{N}$ a.î. $m=c\cdot n+r$ şi să demonstrăm că $r<n$.

Dacă prin absurd $r\not<n$, atunci conform Propoziției 1.19., $r\geq n$, adică există $u\in\mathbb{N}$ a.î. $r=n+u$. 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 $r=r'$. ■

Observaţia 1.26. Numărul c poartă numele de *câtul împărţirii lui m la n* iar r se zice *restul* acestei împărţiri .

Teorema 1.27. Fie m, n, m′, n′, p∈ℕ a.î. m≤n şi m′≤n′. Atunci: (i) m+m′≤ n+n′ şi mm′≤ nn′
(ii) mp≤ np şi $m^p\le n^p$.

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

(ii). Se deduce analog ca şi (i) ţinând cont de (i) precum şi de regulile de calcul din ℕ stabilite mai înainte. ■

Să revenim acum la cazul general al semigrupurilor. Următorul rezultat este imediat.

Propoziţia 1.28. Dacă M este un semigrup, $x\in M$ iar $m, n\in\mathbb{N}^*$, atunci $x^m\cdot x^n=x^{m+n}$ iar $(x^m)^n=x^{mn}$.

Dacă mai avem $y\in M$ a.î. $xy=yx$, atunci $(xy)^n=x^ny^n$.

Definiţia 1.29. Dacă M, M′ sunt monoizi, o funcţie $f:M\to M'$ se zice ***morfism de monoizi*** dacă $f(1)=1$ şi $f(xy)=f(x)f(y)$ pentru orice $x, y\in M$.

Vom nota prin Mon **clasa monoizilor iar pentru M, M′∈**Mon **vom nota prin** $\mathrm{Hom}_{\mathrm{Mon}}$**(M, M′) (sau mai simplu** Hom**(M, M′) dacă nu este pericol de confuzie) toate morfismele de monoizi de la M la M′, adică** Hom**(M, M′)={f:M→M′/ f este morfism de monoizi}.**

Propoziția 1.30. Dacă M, M′, M″ sunt monoizi iar $f\in Hom(M, M')$ şi $g\in Hom(M', M'')$, atunci $gof\in Hom(M, M'')$.

Demonstrație. **Cum $f(1)=g(1)$, $(gof)(1)=g(f(1))=g(1)=1$ iar pentru $x, y\in M$ avem $(gof)(xy)=g(f(xy))=g(f(x)f(y))=g(f(x))g(f(y))=$ $=(gof)(x)(gof)(y)$, adică $gof \in Hom(M, M'')$.■**

Definiția 1.31. Dacă M şi M′ sunt doi monoizi, numim ***izomorfism de monoizi*** un morfism $f\in Hom(M, M')$ care ca funcție este bijecție; în acest caz vom spune despre monoizii M, M′ că sunt ***izomorfi*** şi vom scrie $M\approx M'$.

Se deduce imediat că dacă $f\in Hom(M, M')$ este izomorfism de monoizi, atunci şi $f^{-1}:M'\to M$ este morfism de monoizi.

Definiția 1.32. Fie $(M, \cdot)$ un monoid. Vom spune despre un element $x\in M$ că este ***inversabil*** (sau ***simetrizabil***) dacă există $x'\in M$ a.î. $xx'=x'x=1$.

Să observăm că dacă x' există atunci el este unic deoarece dacă ar mai exista $x''\in M$ a.î. $xx''=x''x=1$, atunci $x'(xx'')=x'1=x'$ şi $x'(xx'')=(x'x)x''=1x''=x''$, adică $x'=x''$.

Elementul x' poartă numele de *inversul* (sau *simetricul*) lui x. În cazul notației multiplicative vom nota $x'=x^{-1}$ iar în cazul notației aditive vom nota $x'=-x$ (iar $-x$ se va numi *opusul* lui x). În cele ce urmează (până la specificări suplimentare) vom considera monoizi multiplicativi.

Pentru monoidul $(M, \cdot)$ prin $U(M, \cdot)$ (sau mai simplu $U(M)$ dacă nu se creează confuzii prin nespecificarea operației algebrice de pe M) vom nota mulțimea elementelor inversabile din M (adică $U(M)=\{x\in M$ / există $x'\in M$ a.î. $xx'=x'x=1\}$).

Evident, dacă $x\in U(M)$, atunci $(x^{-1})^{-1}=x$.

Pentru exemplele de monoizi de până acum avem: $U(P(T),\cap)=\{T\}$, $U(P(T),\cup)=\{\varnothing\}$, $U(P(T),\Delta)=P(T)$, $U(\mathbb{N},+)=\{0\}$, $U(\mathbb{N},\cdot)=\{1\}$, iar pentru o mulțime $A\neq\varnothing$, $U(Hom(A),o)=\{f:A\to A$ / f este bijecție$\}$. Convenim să notăm $\sum(A)=\{f\in Hom(A)$ / f este bijecție$\}$ şi să numim un element $f\in\sum(A)$ ca fiind o *permutare* asupra elementelor lui A.

Propoziția 1.33. Fie $(M, \cdot)$ un monoid şi $x, y \in U(M)$. Atunci $1 \in U(M)$, $xy \in U(M)$ iar $(xy)^{-1}=y^{-1}x^{-1}$.

Demonstrație. **Din $1 \cdot 1=1 \cdot 1=1$ deducem că $1 \in U(M)$ iar din $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x \cdot 1 \cdot x^{-1} = xx^{-1} = 1$ şi $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y =$ $= y^{-1} \cdot 1 \cdot y = y^{-1}y = 1$ deducem că $xy \in U(M)$ iar $(xy)^{-1}=y^{-1}x^{-1}$.■**

Observația 1.34.

Raționând inductiv după n deducem că dacă $x_1,\ldots,x_n \in U(M)$ $(n \geq 2)$, atunci $x_1 \cdot x_2 \cdot \ldots \cdot x_n \in U(M)$ iar $(x_1 \cdot x_2 \cdot \ldots \cdot x_n)^{-1}=x_n^{-1}\ldots x_2^{-1}x_1^{-1}$.

Fie acum M_1, M_2, …, M_n monoizi iar

$$M = M_1 \times \ldots \times M_n = \{(x_1, \ldots, x_n) / x_i \in M_i , 1 \leq i \leq n\}.$$

Pentru $x=(x_1,\ldots,x_n)$, $y=(y_1,\ldots,y_n) \in M$ definim $xy=(x_1y_1,\ldots,x_ny_n)$ iar pentru fiecare $1 \leq i \leq n$ considerăm $p_i : M \to M_i$ definit prin $p_i(x)=x_i$ pentru orice $x=(x_1,\ldots,x_n) \in M$ (p_i se zice a i-a *proiecție* a lui M pe M_i sau *proiecția de indice i*).

Propoziția 1.35. Dacă $M_1,\ldots,M_n$ sunt monoizi, atunci $(M, \cdot)$ este monoid, $U(M)=U(M_1) \times \ldots \times U(M_n)$, pentru fiecare $1 \leq i \leq n$, $p_i \in Hom(M,M_i)$ şi în plus este verificată următoarea proprietate de universalitate : *Pentru oricare monoid M' şi familie de morfisme de monoizi $(p_i')_{1 \leq i \leq n}$ cu $p_i' \in Hom(M', M_i)$, $1 \leq i \leq n$, există un unic $u \in Hom(M', M)$ a.î. $p_i ou=p_i'$.*

Demonstrație. **Asociativitatea operației de înmulțire de pe M rezultă din asociativitatea fiecărei operații de înmulțire de pe M_i iar elementul neutru este $1=(1,\ldots,1)$.**

Dacă $x \in U(M)$, $x=(x_1,\ldots,x_n)$, atunci există $y \in M$, $y=(y_1,\ldots,y_n)$ a.î. $xy=yx=1 \Leftrightarrow (x_1y_1,\ldots,x_ny_n)=(y_1x_1,\ldots,y_nx_n)=(1,\ldots,1) \Leftrightarrow x_iy_i = y_ix_i = 1$ pentru orice $1 \leq i \leq n \Leftrightarrow x_i \in U(M_i)$ pentru orice $1 \leq i \leq n \Leftrightarrow$ $\Leftrightarrow x \in U(M_1) \times \ldots \times U(M_n)$, de unde egalitatea (de mulțimi).

$$U(M)= U(M_1) \times \ldots \times U(M_n).$$

Dacă $x=(x_1,\ldots,x_n)$, $y=(y_1,\ldots,y_n)\in M$ şi $1 \leq i \leq n$, atunci $xy=(x_1y_1,\ldots,x_ny_n)$, deci $p_i(xy)=x_i y_i=p_i(x)p_i(y)$, adică $p_i \in \mathrm{Hom}(M, M_i)$.

Să verificăm acum proprietatea de universalitate, iar pentru aceasta fie M' un alt monoid şi pentru $1 \leq i \leq n$ să considerăm $p_i' \in \mathrm{Hom}(M', M_i)$. Pentru $x \in M'$, definim $u: M' \to M$ prin $u(x)=(p_1'(x),\ldots,p_n'(x))$ şi se verifică imediat că $u \in \mathrm{Hom}(M', M)$ iar $p_i ou = p_i'$, pentru orice $1 \leq i \leq n$.

Fie acum $u' \in \mathrm{Hom}(M', M)$ a.î. $p_i ou' = p_i'$ pentru orice $1 \leq i \leq n$. Atunci pentru orice $x \in M'$ avem $p_i(u'(x)) = p_i'(x)$, adică $u'(x)=(p_1'(x),\ldots,p_n'(x))=u(x)$, de unde $u=u'$.■

Definiția 1.36. Monoidul $M=M_1 \times \ldots \times M_n$ împreună cu proiecțiile $(p_i)_{1\leq i\leq n}$ poartă numele de ***produsul direct*** al monoizilor M_1, M_2, …, M_n (când nu este pericol de confuzie nu vom mai specifica proiecțiile).

§2. Grup. Calcule într-un grup. Subgrup. Subgrup generat de o mulțime. Grup ciclic. Ordinul unui element într-un grup

Definiția 2.1. Vom spune despre un monoid M că este ***grup*** dacă U(M)=M. Altfel zis, dubletul (M, ·) format dintr-o mulțime M şi o operație algebrică pe M este grup dacă operația algebrică este asociativă, admite element neutru şi orice element din M este inversabil.

Grupul M se va zice *comutativ* (sau *abelian*) dacă operația algebrică este comutativă.

Exemple: **1. Dacă T este o mulțime nevidă atunci (P(T), Δ) este grup comutativ.**

2. Dacă A este o mulțime nevidă, atunci ($\sum$(A) , o) este grup (în general necomutativ).

3. Mai general, dacă (M, ·) este un monoid atunci (U (M), ·) este grup.

În cele ce urmează prin $(G, \cdot)$ **vom desemna un grup multiplicativ (dacă nu este pericol de confuzie nu vom mai specifica operaţia algebrică). Cardinalul mulţimii G se va nota** $|G|$ **şi se va numi *ordinul* grupului G .**

În consecinţă, elementul neutru al lui G va fi notat cu 1 iar pentru $x \in G$ **inversul său va fi notat prin** x^{-1} **.**

Analog ca în cazul semigrupurilor, dacă pentru $x \in G$ **definim** $x^0 = 1$**, atunci** $(x^{-1})^{-1} = x$ **iar dacă** $m, n \in \mathbb{N}$**, atunci** $x^m x^n = x^{m+n}$ **şi** $(x^m)^n = = x^{mn}$**. De asemenea, dacă** $x, y \in G$ **şi** $xy = yx$**, atunci pentru orice** $n \in \mathbb{N}$ $(xy)^n = x^n y^n$**.**

Definiţia 2.2. O submulţime nevidă S a lui G se zice ***subgrup*** al lui G dacă S împreună cu restricţia operaţiei algebrice de pe G la S formează grup.

Vom nota prin $L(G)$ **mulţimea subgrupurilor lui G; pentru a exprima că** $H \in L(G)$ **vom indica lucrul acesta scriind că** $H \leq G$**.**

Propoziţia 2.3. Pentru o mulţime nevidă S a lui G următoarele afirmaţii sunt echivalente:

(i) $S \in L(G)$

(ii) $1 \in S$ şi pentru orice $x, y \in S$, $xy \in S$ şi $x^{-1} \in S$

(iii) pentru orice $x, y \in S$, $x^{-1}y \in S$.

Demonstraţie. **Implicaţiile (i)$\Rightarrow$(ii) şi (ii)$\Rightarrow$(iii) sunt imediate.**

(iii)$\Rightarrow$(i). Cum $S \neq \emptyset$ **există** $x_0 \in S$ **şi atunci** $1 = x_0^{-1} x_0 \in S$**. Alegând un element oarecare** $x \in S$**, cum** $1 \in S$ **avem că şi** $x^{-1} = x^{-1} 1 \in S$ **adică** $(S, \bullet)$ **este grup.** ■

În mod evident, $\{1\} \in L(G)$ **şi** $G \in L(G)$**. Oricare alt subgrup S al lui G diferit de** $\{1\}$ **şi G se zice *propriu*. Subgrupul** $\{1\}$ **se zice *subgrup nul* şi se notează de obicei prin** 0.

Propoziţia 2.4. Fie $(S_i)_{i \in I}$ o familie nevidă de subgrupuri ale lui G . Atunci, $\bigcap_{i \in I} S_i \in L(G)$.

Demonstrație. **Fie** $S=\bigcap_{i\in I} S_i$ **şi x, y** $\in$**S . Atunci pentru orice i**$\in$**I, x, y**$\in S_i$ **şi cum** $S_i \leq G$ **avem că** $x^{-1}y \in S_i$ **, adică** $x^{-1}y \in S$**, deci** $S \leq G$.■

Observația 2.5. **În ceea ce priveşte reuniunea a două subgrupuri ale lui G să demonstrăm că dacă H, K**$\in L(G)$**, atunci** $H \cup K \in L(G) \Leftrightarrow$ $\Leftrightarrow H \subseteq K$ **sau** $K \subseteq H$**. Implicația de la dreapta la stânga fiind evidentă să presupunem că** $H \cup K \in L(G)$ **şi totuşi** $H \not\subset K$ **şi** $K \not\subset H$ **, adică există** $x \in H$ **astfel încât** $x \notin K$ **şi** $y \in K$ **astfel încât** $y \notin H$**. Considerând elementul z=xy atunci cum am presupus că** $H \cup K \in L(G)$ **ar trebui ca** $z \in H \cup K$**. Dacă** $z \in H$**, atunci cum** $y=x^{-1}z$ **am deduce că** $y \in H$ **– absurd. Dacă** $z \in K$ **atunci ar rezulta că** $x=zy^{-1} \in K$ **– absurd !.**

Din cele expuse mai înainte deducem că în general, dacă H, K$\in L(G)$ **nu rezultă cu necesitate că şi** $H \cup K \in L(G)$**. Este una din rațiunile pentru care vom introduce noțiunea ce urmează.**

Definiția 2.6. Dacă M este o submulțime nevidă a lui G, prin ***subgrupul lui G generat de M*** înțelegem cel mai mic subgrup al lui G (față de relația de incluziune) ce conține pe M şi pe care îl vom nota prin <M>. Altfel zis

$$<M>= \bigcap_{\substack{S\in L(G)\\ M\subseteq S}} S .$$

Dacă $M \in L(G)$**, în mod evident <M>=M.**

Propoziția 2.7. Dacă $M \subseteq G$ este o submulțime nevidă, atunci $<M> = \{x_1 \ldots x_n \mid n \in \mathbb{N}$ iar $x_i \in M$ sau $x_i^{-1} \in M$ pentru orice $1 \leq i \leq n \}$.

Demonstrație. **Fie** $H=\{x_1 \ldots x_n \mid n \in \mathbb{N}$ **iar** $x_i \in M$ **sau** $x_i^{-1} \in M$ **pentru orice** $1 \leq i \leq n \}$ **şi x, y**$\in$**H, adică** $x=x_1 \ldots x_n$, $y=y_1 \ldots y_m$ **cu** x_i **sau** x_i^{-1} **în M şi** y_j **sau** y_j^{-1} **în M pentru** $1 \leq i \leq n$ **şi** $1 \leq j \leq m$**.**

Cum $x^{-1}y = x_n^{-1} \ldots x_1^{-1}\ y_1 \ldots y_m$ **deducem că** $x^{-1}y \in H$**, adică** $H \leq G$**. Deoarece** $M \subseteq H$ **iar <M> este cel mai mic subgrup al lui G ce conține pe M deducem că** $<M> \subseteq H$ **.**

Fie acum S≤G astfel încât M⊆S. Atunci H⊆S, deci H⊆ $\bigcap_{\substack{S\le G \\ M\subseteq S}} S$ =<M>, de unde egalitatea <M>=H.■

Corolar 2.8. **<x>={x^n | n∈ℕ}∪{$(x^{-1})^n$ | n∈ℕ}.**

Definiția 2.9. <x> poartă numele de ***grupul ciclic*** generat de x. ***Ordinul*** unui element x∈G notat o(x) se definește ca fiind o(x)=|<x>|. Evident, o(1)=1 iar dacă x≠1 și o(x)=n, atunci n este cel mai mic număr natural pentru care x^n=1. Dacă o(x)=∞, atunci x^n≠1, pentru orice n≥1.

Observația 2.10. **1. Dacă** $x \in G$ **este de ordin finit și există** $n \in \mathbb{N}^*$ **a.î.** $x^n = 1$**, atunci o(x)**$\mid n$**.**

Într-adevăr, împărțind pe n la o(x) găsim c, r $\in \mathbb{N}$ **a.î** $n = c \cdot o(x) + r$ **și** $r < o(x)$.

Din $x^{o(x)} = x^n = 1$ **deducem imediat că și** $x^r = 1$**, adică r = 0 (ținând cont de minimalitatea lui o(x)), deci o(x)**$\mid n$**.**

2. Dacă $x, y \in G$**, a.î. o(x) și o(y) sunt finite, xy = yx și (o(x), o(y)) = 1, atunci o(xy) = o(x)o(y).**

Într-adevăr, dacă notăm m = o(x), n = o(y) și p = o(xy), din $x^m = y^n = 1$ **deducem că** $(xy)^{mn} = x^{mn} \cdot y^{mn} = 1$**, adică p** $\mid mn$**. Din o(xy) = p deducem că** $(xy)^p = 1$**, deci** $x^p = y^{-p}$ **iar de aici** $x^{np} = (y^n)^{-p} = 1$**, adică** $m \mid np$ **și cum (m,n) = 1 deducem că** $m \mid p$**. Analog** $n \mid p$ **și cum (m,n) = 1 deducem că** $mn \mid p$**, adică p = mn.**

3. Din cele de mai înainte deducem recursiv că dacă $x_1, x_2, ..., x_n \in G$ **(**$n \ge 2$**) și cele n elemente comută între ele iar ordinele a oricare două (diferite) sunt prime între ele, atunci** $o(x_1 ... x_n) = o(x_1) ... o(x_n)$.

Propoziția 2.11. (L(G), ⊆) este latice completă.

Demonstrație. **În mod evident 0={1}, 1=G iar pentru H, K∈L(G), H∧K=H∩K iar H∨K=<H∪K>. Dacă $(S_i)_{i\in I}$ este o familie oarecare de subgrupuri ale lui G, atunci $\bigwedge_{i\in I} S_i = \bigcap_{i\in I} S_i \in L(G)$ iar $\bigvee_{i\in I} S_i = <\bigcup_{i\in I} S_i> \in L(G)$.■**

§3. Centralizatorul unui element într-un grup. Centrul unui grup. Teorema lui Lagrange. Indicele unui subgrup într-un grup. Ecuația claselor

Definiția 3.1. Pentru $x\in G$ vom nota $C_G(x) = \{ y\in G : xy=yx \}$ şi $Z(G)= \bigcap_{x\in G} C_G(x)$. $C_G(x)$ se numeşte ***centralizatorul lui*** x în G iar Z(G) ***centrul*** lui G; în mod evident $Z(G)= \{ x\in G ; xy = yx$, pentru orice $y\in G \}$.

Propoziția 3.2. Pentru orice $x\in G$, $C_G(x)\leq G$.

Demonstrație. **Dacă $y, z \in C_G(x)$, atunci $yx = xy$ şi $zx =xz$. Deducem imediat că $y^{-1}x = xy^{-1}$ iar $(y^{-1}z)x = y^{-1}(zx) = y^{-1}(xz) = (y^{-1}x)z = =(xy^{-1})z = x(y^{-1}z)$, adică $y^{-1}z \in C_G(x)$, deci $C_G(x) \leq G$.■**

Corolar 3.3. $Z(G)\leq G$.

Demonstrație. **Avem $Z(G)= \bigcap_{x\in G} C_G(x)$ şi conform Propoziției 2.4., $Z(G)\leq G$.■**

Fie acum $H\leq G$ şi $x\in G$.

Definim $xH = \{ xh : h\in H \}$ şi $Hx = \{hx : h\in H \}$. Mulțimea xH (Hx) poartă numele de *clasa la stânga (dreapta)* a lui x în raport cu H.

Propoziția 3.4. Dacă $x, y\in G$ şi $H\leq G$ atunci

(i) $xH = yH \Leftrightarrow x^{-1}y \in H$
(ii) $Hx = Hy \Leftrightarrow xy^{-1} \in H$.

Demonstrație. **(i). Să presupunem că $xH = yH$. Cum $1 \in H$, $x = x \cdot 1 \in xH = yH$, adică $x = yh$ cu $h \in H$. Deducem că $y^{-1}x = h \in H$ şi cum $h^{-1} \in H$ avem că $h^{-1} = x^{-1}y \in H$. Reciproc, fie $x^{-1}y = h \in H$ şi $z \in xH$, adică $z = xk$ cu $k \in H$. Cum $x = yh^{-1}$ avem $z = (yh^{-1})k = y(h^{-1}k)$, adică $z \in yH$ (căci $h^{-1}k \in H$), deci $xH \subseteq yH$. Analog deducem că şi $yH \subseteq xH$, de unde $xH = yH$.**

(ii). Ca şi în cazul (i).■

Corolar 3.5. Dacă $H \leq G$, atunci pentru $x \in G$, $xH = H$ (sau $Hx = H$) $\Leftrightarrow x \in H$. În particular, $1 \cdot H = H$.

Vom nota $(G/H)_s = \{xH : x \in G\}$ şi $(G/H)_d = \{Hx : x \in G\}$

Propoziția 3.6. $(G/H)_s$ şi $(G/H)_d$ sunt partiții ale lui G.

Demonstrație. **Este suficient să probăm pentru $(G/H)_s$. Deoarece pentru orice $x \in G$ avem $x = x \cdot 1 \in xH$ deducem că $\bigcup_{x \in G} xH = G$.**

Fie acum $x, y \in G$ şi să demonstrăm că $xH = yH$ sau $xH \cap yH = \emptyset$. Avem că $x^{-1}y \in H$ sau $x^{-1}y \notin H$. Dacă $x^{-1}y \in H$, conform Propoziției 3.4, $xH = yH$.

Să presupunem acum că $x^{-1}y \notin H$. Dacă ar exista $z \in xH \cap yH$, atunci $z = xh = yk$ cu $h, k \in H$ şi am deduce imediat că $x^{-1}y = hk^{-1} \in H$ -absurd. Deci în cazul $x^{-1}y \notin H$ avem $xH \cap yH = \emptyset$. ■

Propoziția 3.7. Funcția $f : (G/H)_s \to (G/H)_d$, $f(xH) = Hx^{-1}$ pentru orice $x \in G$ este o bijecție .

Demonstrație. **Pentru $x, y \in G$ echivalențele $xH = yH \Leftrightarrow x^{-1}y \in H \Leftrightarrow x^{-1}(y^{-1})^{-1} \in H \Leftrightarrow Hx^{-1} = Hy^{-1}$ (conform Propoziției 3.4) ne arată că f este corect definită şi că este injectivă. Cum surjectivitatea lui f este imediată, deducem că f este bijecție.■**

Din propoziția precedentă deducem că $|(G/H)_s| = |(G/H)_d|$; acest număr cardinal se notează $|G:H|$ şi poartă numele de *indicele* lui H în G.

Lema 3.8. Dacă $H \leq G$ şi $x \in G$, atunci $|xH| = |Hx| = |H|$.

Demonstrație. **Este suficient să arătăm că mulțimile xH şi H sunt echipotente iar în acest sens definim $f_x : H \to xH$, $f_x(h) = xh$ pentru orice $h \in H$.**

Dacă $h, k \in H$ şi $f_x(h) = f_x(k)$ atunci $xh=xk$ deci $h=k$ adică f este injectivă. Cum f_x este în mod evident şi surjectivă, deducem că f_x este o bijecție şi astfel $|xH| = |H|$.■

Teorema 3.9. Dacă $H \leq G$, atunci

$$|G| = |H| \cdot |G:H| .$$

Demonstrație. **Cum $(G/H)_s$ este o partiție a lui G avem $|G| = \sum_{x \in G} |xH|$ (sumarea făcându-se după clase distincte).**

Ținând cont de Lema 3.8. deducem că $|G| = |H| \cdot |G:H|$.

În cazul în care G este un grup finit, atunci $|G|$, $|H|$ şi $|G : H|$ sunt numere naturale iar relația $|G| = |H| \cdot |G:H|$ arată că $|H|$ este un divizor al lui $|G|$.

Obținem astfel:

Corolar 3.10. (*Lagrange*) Ordinul oricărui subgrup al unui grup finit divide ordinul grupului.

Corolar 3.11. Dacă G este un grup finit de ordin n, atunci $x^n = 1$ pentru orice $x \in G$.

Demonstrație. **Dacă $k=o(x)$, atunci $x^k = 1$ şi $k|n$ (conform teoremei lui Lagrange), adică $n=kt$ cu $t \in \mathbb{N}$. Atunci $x^n = x^{kt} = (x^k)^t = 1^t = 1$.■**

Definiția 3.12. Vom spune despre elementele x, $y \in G$ că sunt ***conjugate*** în G şi vom scrie $x \sim y$ dacă există $a \in G$ a. î. $x=a^{-1}ya$.

Propoziția 3.13. Relația de conjugare $\sim$ este o echivalență pe G.

Demonstrație. **Deoarece pentru orice $x \in G$, $x=1^{-1}x1$ deducem că $x \sim x$, adică relația $\sim$ este reflexivă. Dacă $x, y \in G$ şi $x \sim y$, atunci există $a \in G$ astfel încât $x=a^{-1}ya$. Cum $y=axa^{-1}=(a^{-1})^{-1}\, xa^{-1}$ deducem că şi $y \sim x$, adică relația $\sim$ este şi simetrică.**

Fie acum x, y, z astfel încât $x \sim y$ şi $y \sim z$. Atunci există $a, b \in G$ astfel încât $x=a^{-1}ya$ şi $y=b^{-1}zb$. Deducem că $x=a^{-1}(b^{-1}zb)a = (a^{-1}b^{-1})\, z\, (ba) = (ba)^{-1}\, z\, (ba)$, adică $x \sim z$ şi astfel $\sim$ este şi tranzitivă, deci o relație de echivalență pe G.■

În conformitate cu notațiile de la Capitolul 1, pentru $x \in G$ prin $[x]_\sim$ vom desemna clasa de echivalență a lui x în raport cu relația $\sim$ care se mai zice şi *clasa de conjugare a lui x* (altfel zis $[x]_\sim$ este mulțimea conjugaților lui x în G, adică $[x]_\sim=\{axa^{-1} : a \in G\}$).

Propoziția 3.14. Pentru orice $x \in G$, $|[x]_\sim|=|G : C_G(x)|$.

Demonstrație. **Fie $H=C_G(x)$. Dacă $a, b \in G$ atunci din echivalențele $axa^{-1}=bxb^{-1} \Leftrightarrow xa^{-1}b=a^{-1}bx \Leftrightarrow a^{-1}b \in H \Leftrightarrow aH=bH$ deducem că funcția $f:[x]_\sim \to (G/H)_s$, $f(axa^{-1}) = aH$ pentru orice $a \in G$ este corect definită şi injectivă. Cum în mod evident f este şi surjecție deducem că f este bijecție, adică $|[x_\sim]|=|(G/H)_s|=|G : H|=$ $=|G : C_G(x)|$.■**

Deoarece $\{[x]_\sim\}_{x \in G}$ formează o partiție a lui G deducem că $G = \bigcup_{x \in G} [x]_\sim$ (vom lua reuniunea după elementele $x \in G$ ce nu sunt conjugate între ele). Să remarcăm şi faptul că dacă $x \in Z(G)$, atunci $[x]_\sim=\{x\}$. Astfel, $|G|=\sum_{x \in G} |[x]_\sim|$ (sumarea făcându-se după elementele neconjugate). Scriind

$$|G| = \sum_{x \in Z(G)} |[x]_{\sim}| + \sum_{x \notin Z(G)} |[x]_{\sim}| = \sum_{x \in Z(G)} |\{x\}| + \sum_{x \notin Z(G)} |[x]_{\sim}|$$

şi ţinând cont de Propoziţia 3.13 obţinem relaţia

$|G| = |Z(G)| + \sum_{x \notin Z(G)} |G:C_G(x)|$ **, cunoscută sub numele de *ecuaţia claselor.***

În continuare vom aplica ecuaţia claselor în special în cazul în care grupul G este finit.

§4. Subgrupuri normale. Factorizarea unui grup printr-un subgrup normal

Definiţia 4.1. Vom spune despre un subgrup H al lui G că este ***normal* în G** dacă $xH = Hx$ pentru orice $x \in G$ şi vom scrie $H \trianglelefteq G$ pentru a desemna faptul acesta.

Vom nota prin $L_0(G)$ mulţimea subgrupurilor normale ale lui G. Evident, $L_0(G) \subseteq L(G)$, $\{1\}, G \in L_0(G)$ iar dacă G este comutativ, atunci $L_0(G) = L(G)$.

Propoziţia 4.2. Pentru $H \in L(G)$ următoarele afirmaţii sunt echivalente

(i) $H \in L_0(G)$

(ii) Pentru orice $x \in G$, $xHx^{-1} \subseteq H$ (unde $xHx^{-1} = \{xhx^{-1} : h \in H\}$).

***Demonstraţie.* (i) $\Rightarrow$ (ii). Dacă $H \trianglelefteq G$ şi $x \in G$, atunci $xH = Hx$, deci pentru $h \in H$, $xh = kx$ cu $k \in H$ astfel că $xhx^{-1} = k \in H$.**

(ii)$\Rightarrow$(i). Fie $x \in G$. Din $xHx^{-1} \subseteq H$ deducem imediat că $xH \subseteq Hx$. Înlocuind pe x cu x^{-1} deducem că $x^{-1}H \subseteq Hx^{-1}$, de unde $Hx \subseteq xH$, adică $xH = Hx$, deci $H \in L_0(G)$.■

Propoziţia 4.3. $L_0(G)$ este sublatice modulară marginită a lui L(G).

***Demonstraţie.* Am văzut că {1} şi G fac parte din $L_0(G)$. Fie acum $H, K \in L_0(G)$, $x \in G$ şi $h \in H \cap K$. Atunci $xhx^{-1} \in H$, K deci**

$xhx^{-1} \in H \cap K$, adică $H \cap K \in L_0(G)$. Să arătăm acum că $H \vee K = HK = KH$ (unde $HK = \{hk \mid h \in H, k \in K\}$). Avem

$HK = \bigcup_{x \in H} xK = \bigcup_{x \in H} Kx = KH$.

În mod evident $H, K \subseteq HK$ iar dacă alegem $S \leq G$ astfel încât $H, K \subseteq S$ atunci $HK \subseteq S$, adică $HK = KH = H \vee K$. Pentru a arăta că $HK \trianglelefteq G$, fie $x \in G$, $h \in H$ şi $k \in K$.

Scriind $x(hk)x^{-1} = (xhx^{-1})(xkx^{-1})$, cum $xhx^{-1} \in H$ şi $xkx^{-1} \in K$, deducem că $x(hk)x^{-1} \in HK$, adică $HK \trianglelefteq G$, deci şi $H \vee K \in L_0(G)$. Am demonstrat deci că $L_0(G)$ este sublatice (mărginită) a lui $L(G)$. Pentru a proba că $L_0(G)$ este modulară fie $H, K, L \in L_0(G)$ astfel încât $H \subseteq K$ şi să arătăm că $K \wedge (H \vee L) = H \vee (K \wedge L)$. Ţinînd cont de cele stabilite anterior este suficient să probăm incluziunea $K \cap (HL) \subseteq H(K \cap L)$ (cealaltă fiind evidentă) iar pentru aceasta fie $x \in K \cap (HL)$. Atunci $x \in K$ şi $x \in HL$ ceea ce implică $x = yz$ cu $y \in H$ şi $z \in L$. Avem $z = y^{-1}x \in K$ şi cum $z \in L$ deducem că $z \in K \cap L$.

Cum $y \in H$ rezultă $x = yz \in H(K \cap L)$, adică avem $K \cap (LH) \subseteq H(K \cap L)$.■

Am văzut că o intersecţie finită de subgrupuri normale ale lui G este de asemenea un subgrup normal al lui G. Analog se probează faptul că dacă $(H_i)_{i \in I}$ este o familie oarecare de subgrupuri normale ale lui G, atunci $\bigcap_{i \in I} H_i$ este de asemenea subgrup normal al lui G, astfel că, fiind dată o mulţime nevidă $M \subseteq G$ putem vorbi de *subgrupul normal al lui G generat de M* ca fiind intersecţia tuturor subgrupurilor normale ale lui G ce conţin pe M. Convenim să notăm acest subgrup normal prin [M], adică $[M] = \bigcap_{\substack{H \in L_0(G) \\ M \subseteq H}} H$.

Propoziţia 4.4. Dacă $M \subseteq G$ este o mulţime nevidă, atunci
$[M] = \langle \{a^{-1}xa \mid a \in G \text{ şi } x \in M\} \rangle$.

Demonstraţie. **Fie $K = \langle \{a^{-1}xa \mid a \in G \text{ şi } x \in M\} \rangle$. În mod evident $M \subseteq K$. Ţinând cont de Propoziţia 2.7, un element din K este de forma $x_1 \ldots x_n$ cu $x_i \in M'$ sau $x_I^{-1} \in M'$ unde $M' = \{a^{-1}xa \mid a \in G$ şi**

$x \in M\}$. Pentru a proba apartenența $K \in L_0(G)$, fie $a \in G$ şi $y \in K$. Atunci $y=y_1 \ldots y_n$ cu $y_i \in M'$ sau $y_i^{-1} \in M'$ astfel că scriind $a^{-1}ya = a^{-1}y_1 \ldots y_n a = (a^{-1}y_1a)(a^{-1}y_2a) \ldots (a^{-1}y_na)$ deducem că $a^{-1}ya \in K$, deci $K \trianglelefteq G$. Cum $[M]$ este cel mai mic subgrup normal al lui G ce conține pe M deducem că $[M] \subseteq K$.

Fie acum $H \in L_0(G)$ astfel încât $M \subseteq H$. Dacă alegem $a \in G$ şi $x \in M$, atunci $x \in H$ şi cum $H \trianglelefteq G$ deducem că $a^{-1}xa \in H$, adică $K \subseteq H$. Atunci $K \subseteq \bigcap_{\substack{H \in L_0(G) \\ M \subseteq H}} H = [M]$, de unde egalitatea $[M]=K$.■

Dacă $H \trianglelefteq G$, atunci $(G/H)_s=(G/H)_d=G/H$.

Pentru $xH, yH \in G/H$ (cu $x,y \in G$) definim $(xH)(yH)=(xy)H$ şi să arătăm că față de această operație algebrică G/H devine grup.

Dacă mai avem $x', y' \in G$ astfel încât $xH=x'H$ şi $yH=y'H$ atunci $x^{-1}x', y^{-1}y' \in H$. Pentru a proba că $(xy)H=(x'y')H$ scriem

$(xy)^{-1}(x'y')=y^{-1}x^{-1}x'y'=[y^{-1}(x^{-1}x')y](y^{-1}y')$, de unde deducem că $(xy)^{-1}(x'y') \in H$, adică $(xy)H=(x'y')H$ şi astfel înmulțirea pe G/H este corect definită. Ea este şi asociativă deoarece pentru $xH, yH, zH \in G/H$ cu $x, y, z \in G$ avem $(xH)[(yH)(zH)]=(xH)[(yz)H]=[x(yz)]H=[(xy)z]H=[(xy)H](zH)=$

$=[(xH)(yH)](zH)$ Elementul neutru va fi $1H=H$ iar pentru $xH \in G/H$ avem $(x^{-1}H)(xH)=(x^{-1}xH)=H$ şi $(xH)(x^{-1}H)=(xx^{-1})H=H$, de unde deducem că $(xH)^{-1}=x^{-1}H$.

Definiția 4.5. Grupul $(G/H, \cdot)$ poartă numele de ***grupul factor*** al lui G prin subgrupul normal H. Aplicația $p_H: G \to G/H$, $p_H(x)=xH$ pentru orice $x \in G$ poartă numele de ***surjecția canonică***.

Observația 4.6. **1. În mod evident $|G/H|=|G:H|$, astfel că dacă G este finit, $|G/H|=|G|:|H|$.**

2. Dacă $H \leq G$ şi $|G:H|=2$, atunci $H \trianglelefteq G$, (deoarece alegând $x \in G \setminus H$, din $H \cap xH = H \cap Hx = \varnothing$ şi $H \cup xH = H \cup Hx = G$ deducem că $xH=Hx$).

În continuare vom prezenta un alt mod de a introduce grupul factor G / H când H⊴G.

Să presupunem la început că H este doar subgrup al lui G (fără a fi normal).

Pe G definim două relații ρ_H^s şi ρ_H^d astfel:

(x, y)$\in \rho_H^s$ $\Leftrightarrow$ $x^{-1}y \in H$ şi (x, y)$\in \rho_H^d$ $\Leftrightarrow$ $xy^{-1} \in H$.

Se verifică imediat că ρ_H^s şi ρ_H^d sunt relații de echivalență pe G iar pentru x∈G, $[x]_{\rho_H^s} = xH$ şi $[x]_{\rho_H^d} = Hx$.

În cazul în care H⊴G , atunci $\rho_H^s = \rho_H^d \stackrel{\text{def}}{=} \rho_H$ şi să arătăm că ρ_H este o congruență pe G (adică compatibilă cu structura de grup a lui G). Pentru aceasta fie x, x′, y, y′∈G a.î. (x, x′), (y, y′)$\in \rho_H$ şi să arătăm că şi (xy, x′y′)$\in \rho_H$. Avem $(xy)^{-1}(x'y') = y^{-1}x^{-1}x'y' =$ $= [y^{-1}(x^{-1}x')y](y^{-1}y')$ şi cum $x^{-1}x', y^{-1}y' \in H$ iar H⊴G (adică $y^{-1}(x^{-1}x')y \in H$) deducem imediat că $(xy)^{-1}(x'y') \in H$ adică, (xy, x′y′)$\in \rho_H$. Astfel G / $\rho_H = \{[x]_{\rho_H}\}_{x\in G} = \{xH\}_{x\in G} = G/H$ şi de aici construcția grupului factor G / H continuă ca mai înainte.

Observația 4.7. **Am văzut că dacă H⊴G, atunci ρ_H este o congruență pe G (adică o relație de echivalență pe G compatibilă cu structura de grup a lui G).**

Se poate arăta imediat că asocierea H $\rightsquigarrow \rho_H$ stabileşte o bijecție între L_0(G) şi congruențele de pe G. Într-adevăr, dacă ρ este o congruență pe G, atunci se arată uşor că $[1]_\rho = \{x \in G \mid (x,1) \in \rho\} \in L_0$(G) şi astfel, asocierea $\rho \rightsquigarrow [1]_\rho$ este inversa funcției H $\rightsquigarrow \rho_H$ (de mai înainte).

§5 Morfisme de grupuri. Compunerea morfismelor de grupuri. Monomorfisme, epimorfisme, izomorfisme de grupuri. Nucleul şi conucleul unui morfism de grupuri. Nucleul şi conucleul unei perechi de morfisme

de grupuri

Definiția 5.1. Dacă G şi G′ sunt două grupuri, vom spune că o funcție f:G→G′ este ***morfism*** de grupuri dacă pentru orice x, y∈G, f(xy)=f(x)f(y).

Vom nota Hom_{Gr}**(G, G′)={f:G→G′ | f este morfism de grupuri}. Dacă nu este pericol de confuzie în loc de** Hom_{Gr}**(G, G′) vom scrie** Hom**(G, G′).**

Exemple. **1. Funcția** 1_G**:G→G este morfism de grupuri.**

2. f : G→G′, f(x)=1 pentru orice x∈G este de asemenea morfism de grupuri (numit *morfismul nul*).

3. Dacă H⊴G atunci p_H **:G→G/H,** p_H**(x)=xH pentru orice x∈G este morfism surjectiv de grupuri (numit morfismul *surjectiv canonic*).**

Pe parcursul acestei lucrări vom prezenta mai multe exemple de morfisme de grupuri.

Observația 5.2. **Ca şi în cazul monoizilor se demonstrează imediat că dacă G, G′, G″ sunt grupuri şi f∈**Hom**(G,G′), g∈**Hom**(G′,G″), atunci gof∈**Hom**(G,G″).**

Propoziția 5.3. **Dacă G, G′ sunt grupuri şi f∈**Hom**(G, G′), atunci f(1)=1 şi** $f(x^{-1}) = (f(x))^{-1}$ **pentru orice x∈G.**

Demonstrație. **Din 1=1·1 deducem că f(1)=f(1·1)=f(1)·f(1) iar de aici că f(1) =1. Dacă x∈G, cum** $xx^{-1} = 1$ **deducem** $1 = f(1) = f(xx^{-1}) = = f(x)\, f(x^{-1})$**, de unde** $f(x^{-1})=f(x)^{-1}$**.■**

Propoziția 5.4. Fie G, G′ grupuri iar f∈Hom(G, G′).

(i) Dacă H≤G atunci f(H)≤G′

(ii) Dacă H⊴G şi f este funcție surjectivă, atunci f(H)⊴G′

(iii) Dacă H′≤G′, atunci $f^{-1}(H')$≤G

(iv) Dacă $H' \trianglelefteq G'$, atunci $f^{-1}(H') \trianglelefteq G$.

Demonstrație. **(i). Dacă $x', y' \in f(H)$, atunci $x'=f(x)$, $y'=f(y)$ cu $x, y \in H$ şi cum $x'^{-1}y' = (f(x))^{-1} f(y) = f(x^{-1}y)$ iar $x^{-1}y \in H$ deducem că $x'^{-1}y' \in f(H)$, adică $f(H) \leq G'$.**

(ii). Dacă $x' \in G'$ şi $h' \in f(H)$ atunci cum f este surjecție $x'=f(x)$ cu $x \in G$ şi $h'=f(h)$ cu $h \in H$. Deoarece $x'h'x'^{-1} = f(xhx^{-1})$ iar $xhx^{-1} \in H$ (căci $H \trianglelefteq G$) deducem că $x'h'x'^{-1} \in f(H)$, adică $f(H) \trianglelefteq G$.

(iii). Dacă $x, y \in f^{-1}(H')$, atunci $f(x), f(y) \in H'$ şi cum $H' \leq G'$ deducem că $f(x)^{-1} f(y) = f(x^{-1}y) \in H'$, adică $x^{-1}y \in f^{-1}(H')$, deci $f^{-1}(H') \leq G$.

(iv). Fie $x \in G$ şi $y \in f^{-1}(H')$ (adică $f(y) \in H'$). Cum $H' \trianglelefteq G'$ avem $f(x)f(y)f(x)^{-1} \in H'$ sau $f(xyx^{-1}) \in H'$, deci $xyx^{-1} \in f^{-1}(H')$, adică $f^{-1}(H') \trianglelefteq G$.■

Observația 5.5. Dacă $f \in Hom(G, G')$, conform propoziției precedente deducem că $f^{-1}(\{1\}) \trianglelefteq G$ iar $f(G) \leq G'$. Convenim să notăm $f^{-1}(\{1\}) = Ker(f)$ şi să-l numim *nucleul* lui f iar $f(G) = Im(f)$ şi să-l numim *imaginea* lui f.

Astfel, pentru orice $f \in Hom(G, G')$, $Ker(f) \trianglelefteq G$ iar $Im(f) \leq G'$.

Propoziția 5.6. Dacă G, G′ sunt grupuri iar $f \in Hom(G, G')$, următoarele afirmații sunt echivalente:

(i) f este funcție injectivă
(ii) $Ker(f) = \{1\}$
(iii) Pentru orice grup G″ şi $\alpha, \beta \in Hom(G'', G)$, dacă $f\circ\alpha = f\circ\beta$, atunci $\alpha = \beta$.

Demonstrație. **(i) $\Rightarrow$ (ii). Evident $\{1\} \subseteq Ker(f)$. Dacă $x \in Ker(f)$ atunci $f(x)=1=f(1)$ şi cum f este injecție deducem că $x=1$, adică $Ker(f)=\{1\}$.**

(ii)$\Rightarrow$(i). Dacă $x, y \in G$ astfel încât $f(x)=f(y)$, cum $f(x^{-1}y) = (f(x))^{-1}f(y)=1$ deducem că $x^{-1}y \in Ker(f)=\{1\}$, adică $x^{-1}y=1$ deci $x=y$, rezultând astfel că f este injecție.

(i)$\Rightarrow$(iii). Evidentă

(iii)⇒(i). Să presupunem prin absurd că f nu este injectivă (deşi verifică (iii)). Cum (i) ⇔ (ii), deducem că Ker(f)≠{1}. Dacă notăm G″=Ker(f) şi considerăm α, β:G″→ G, α=incluziunea iar β= morfismul nul (adică β(x)=1 pentru orice x∈G″), atunci α≠β şi foα=foβ (căci ambele dau morfismul nul) – absurd !.■

Observaţia 5.7. Datorită propoziţiei precedente (şi ţinând cont de felul în care se vor defini în Capitolul 5 *monomorfismele* într-o categorie oarecare) vom numi morfismele injective de grupuri ***monomorfisme.*** **Monomorfismele se mai zic *şi scufundări.***

Propoziţia 5.8. Dacă G, G′ sunt grupuri iar f∈Hom(G, G′), atunci în ipoteza că G′ este comutativ, următoarele afirmaţii sunt echivalente:

(i) f este surjecţie

(ii) Im(f)=G′

(iii) Pentru orice grup G″ şi orice morfisme α, β∈Hom(G′,G″), dacă αof=βof, atunci α=β.

Demonstraţie. **Echivalenţa (i) ⇔ (ii) este imediată.**

(i)⇒(iii). Dacă y∈G′ cum f este surjecţie există x∈G astfel încât f(x)=y. Atunci (αof)(x)=(βof)(x) ⇔ α(f(x))= β(f(x)) ⇔ α(y)=β(y), adică α=β.

(iii)⇐(i). Să presupunem că f verifică (iii) şi totuşi nu este surjectivă, adică Im(f)≠G′. Alegând G″=G′/Im(f) (lucru posibil deoarece prin ipoteză G′ este comutativ şi deci Im(f)⊴G′) avem că G″≠{1} şi astfel alegând α=$p_{Im(f)}$:G′→G″ şi β= morfismul nul de la G′ la G″ avem că α≠β deşi αof=βof (căci ambele compuneri dau morfismul nul) – absurd.■

Observaţia 5.9. Datorită propoziţiei precedente (şi din aceleaşi raţiuni ca în cazul Observaţiei 5.7) morfismele surjective f∈Hom(G, G′) cu G′ comutativ se mai zic şi ***epimorfisme*** (cu atât mai mult cu cât vom arăta mai târziu că putem renunţa la restricţia ca G′ să fie comutativ).

Definiția 5.10. Dacă G, G′ sunt grupuri, vom spune că $f \in Hom(G, G')$ este ***izomorfism*** de grupuri dacă există $g \in Hom(G', G)$ astfel încât $gof=1_G$ şi $fog=1_{G'}$. În acest caz vom spune despre grupurile G şi G′ că sunt ***izomorfe*** şi vom scrie $G \approx G'$.

Se verifică imediat că morfismul f este izomorfism de grupuri dacă şi numai dacă f este bijecție.

Vom privi noțiunile de nucleu şi conucleu ale unui morfism de grupuri într-un context mai general. În acest sens vom introduce noțiunea de *nucleu* şi *conucleu* a unei perechi de morfisme de grupuri şi vom proba existența lor (analog ca în cadrul §4 de la Capitolul1).

Definiția 5.11. Fie $f, g: G_1 \to G_2$ o pereche de morfisme de grupuri . Un dublet notat prin Ker(f, g)=(G, i) şi format dintr-un grup G şi un morfism de grupuri $i: G \to G_1$ se zice ***nucleul perechii (f, g)*** dacă îndeplineşte următoarele condiții:

(i) foi=goi

(ii) Dacă (G′, i′) este un alt dublet format dintr-un grup G′ şi un morfism de grupuri $i': G' \to G_1$ a.î. foi′=goi′, atunci există un unic morfism de grupuri $u: G' \to G$ astfel încât iou=i′.

Teorema 5.12. Pentru orice pereche de morfisme de grupuri $f, g: G_1 \to G_2$ există Ker(f, g) care este unic până la un izomorfism de grupuri.

Demonstrație. **Demonstrația unicității fiind asemănătoare cu cea de la nucleul unei perechi de funcții (§4, Capitolul 1) vom proba doar existența nucleului.**

În acest sens vom considera $K = \{x \in G_1 \mid f(x) = g(x)\}$ şi să arătăm că $K \leq G_1$. Dacă $x, y \in K$, atunci f(x)=g(x), f(y)=g(y) şi cum $f(xy^{-1})=f(x)f(y)^{-1}= g(x)g(y)^{-1}= g(xy^{-1})$ deducem că $xy^{-1} \in K$, adică $K \leq G_1$. Morfismul $i: K \to G_1$ va fi incluziunea şi în mod evident foi=goi.

Dacă mai avem un alt dublet (K′, i′) cu K′ grup şi $i': K' \to G_1$ morfism de grupuri astfel încât foi′=goi′, atunci pentru orice $x \in K'$, $f(i'(x)) \in K$ astfel că $u: K' \to K$, $u(x)=i'(x)$ pentru orice $x \in K'$ va fi unicul morfism de grupuri pentru care iou=i′.■

Definiția 5.13 Fie f, g:$G_1 \to G_2$ o pereche de morfisme de grupuri. Un dublet notat prin Coker(f, g)=(G, p) format dintr-un grup G şi un morfism de grupuri p:$G_2 \to G$ se zice ***conucleu al perechi (f,g)*** dacă îndeplineşte următoarele condiții:

(i) pof=pog

(ii) Dacă(G′, p′) este un alt dublet format dintr-un grup G′ şi un morfism de grupuri p′:$G_2 \to G'$ astfel încât p′of=p′og, atunci există un unic morfism de grupuri u:$G \to G'$ astfel încât uop=p′.

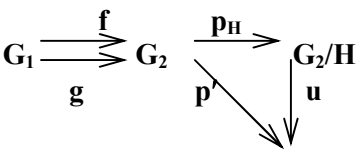
Teorema 5.14. Pentru orice pereche de morfisme de grupuri f, g:$G_1 \to G_2$ există Coker(f, g) care este unic până la un izomrfism de grupuri.

Demonstrație. **Cum probarea unicității conucleului se face ca pentru funcții (§4, Capitolul 1), să probăm doar existența conucleului. În acest sens vom considera M=$\{f(x)g(x)^{-1} \mid x \in G_1\}$, H=[M]= subgrupul normal al lui G_2 generat de M (vezi Propoziția 4.4) iar $p_H : G_2 \to G_2/H$ morfismul surjectiv canonic şi să probăm că (G=G_2/H, p_H)=Coker(f, g). Conform Propoziției 4.4, H=[M]= $<\{a^{-1} f(x)g(x)^{-1}a \mid a \in G_2, x \in G_1\}>$.**

Deoarece pentru orice $x \in G_1$, $f(x)g(x)^{-1} \in M \subseteq H$, deducem că H(f(x))=H(g(x)), adică $p_H(f(x))=p_H(g(x))$, deci $p_H$of=$p_H$og.

Fie acum (G′, p′) un alt dublet format dintr-un grup G′ şi un morfism p′:$G_2 \to G'$ astfel încât p′of=p′og. Atunci pentru orice $x \in G_1$ $p'(f(x))=p'(g(x)) \Leftrightarrow f(x)g(x)^{-1} \in$ Ker p′ de unde deducem că $M \subseteq$Ker(p′) şi deci şi H=[M]$\subseteq$Ker(p′) (căci Ker(p′)$\trianglelefteq G_2$ iar H este cel mai mic subgrup normal al lui G_2 ce conține pe M).

Avem deci diagrama



cu H$\subseteq$Ker(p′). Definim u:$G_2/H \to G'$ prin u(xH)=p′(x) pentru orice $x \in G_2$.

Dacă mai avem $y \in G_2$ astfel încât $xH=yH$ atunci $x^{-1}y \in H \subseteq Ker(p')$, adică $x^{-1} y \in Ker(p)$ deci $p'(x)=p'(y)$ şi astfel u este corect definită. În mod evident u este morfism de grupuri şi $uop_H=p'$.

Dacă mai avem $u': G_2 / H \to G'$ astfel încât $u'op_H=p'$, atunci pentru orice $x \in G_2$ avem $u'(p_H(x))= u(p_H(x))$, adică $u'=u$.■

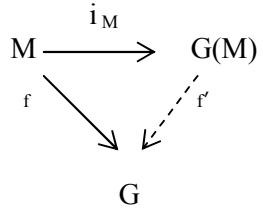
Observaţia 5.15. Dacă $f:G_1 \to G_2$ este un morfism de grupuri, atunci considerând morfismul nul $1:G_1 \to G_2$ definit prin $1(x)=1$ pentru orice $x \in G_1$, avem că $Ker(f)=Ker(f, 1)$ iar $Coker(f)=Coker(f, 1)$.

§6.Teorema lui Malţev. Grupul $(\mathbb{Z},+)$.
Subgrupurile lui $(\mathbb{Z},+)$. Clasele de resturi modulo n

În vederea construirii mulţimii numerelor întregi $\mathbb{Z}$, vom prezenta la început o teoremă a 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 6.1. (*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 $f':G(M) \to G$ a.î. diagrama



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

Demonstrație. Pe mulțimea $M' = M \times M$ definim relația $(x, y) \sim (x', y') \overset{def}{\Leftrightarrow} xy' = yx'$ şi să probăm că $\sim$ este o echivalență pe M' compatibilă cu structura de monoid a lui M' (adică $\sim$ este o congruență pe monoidul produs $M' = M \times M$). În mod evident, relația $\sim$ 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 relația $\sim$ este şi tranzitivă, de unde concluzia că $\sim$ este o echivalență pe M' .

Fie acum $(x, y), (x', y'), (a, b), (a', b') \in M'$ a.î. $(x, y) \sim (a, b)$ 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 relația $\sim$ este o congruență pe monoidul produs M' în care reamintim că operația de compunere se definește 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 echivalență în $G(M)$.

Datorită faptului că relația $\sim$ este o congruență 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 $[1, 1]$, 1 fiind elementul neutru al lui M). Deoarece pentru $[x, y] \in G(M)$, $[x, y] \cdot [y, x] = [xy, xy] = [1, 1]$ deducem că $[y, x] = [x, y]^{-1}$, adică $G(M)$ este grup (comutativ).

Definim $i_M : M \to G(M)$ prin $i_M(x) = [x, 1]$ pentru orice $x \in M$. Pentru $x, y \in M$ avem $i_M(x) \cdot i_M(y) = [x, 1] \cdot [y, 1] = [xy, 1] = i_M(xy)$ adică i_M este morfism de monoizi. Dacă $i_M(x) = i_M(y)$, atunci $[x, 1] = [y, 1] \Leftrightarrow$ $\Leftrightarrow x1 = y1 \Leftrightarrow x = y$, 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 un grup comutativ oarecare şi $f : M \to G$ un morfism de monoizi. Pentru $[x, y] \in G(M)$,

definim $f'([x, y])=f(x)f(y)^{-1}$. Observăm că dacă $[x, y]=[x', y']$, atunci $xy'=x'y$, deci $f(x)f(y')=f(x')f(y) \Leftrightarrow f(x)f(y)^{-1}=f(x')f(y')^{-1}$, adică f' este corect definită.

Să probăm acum că f' este morfism de grupuri.

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

$=f(x)f(x')[f(y)\cdot f(y')]^{-1}=(f(x)f(y)^{-1})(\ f(x')f(y')^{-1})=f'([x,\ y])f'([x',\ y'])$. Pentru $x\in M$ avem $(f'\circ i_M)(x)=f'(i_M\ (x))=\ f'([x,1])=f(x)f(1)^{-1}=f(x)$, 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 $f'':G(M)\to G$ a.î. $f''\circ i_M=f$. Atunci, pentru $[x, y]\in G(M)$ avem

$[x,y]=[x,1]\cdot[1,y]=[x,1]\cdot[y,1]^{-1}$, de unde $f''([x,\ y])=f''([x,1]\cdot[y,1]^{-1})\ =$

$=f''(i_M\ (x)i_M(y)^{-1})=f''(i_M\ (x))(f''(i_M\ (y))^{-1}=f(x)(f(y))^{-1}=f'([x,\ y])$, adică $f''=f'$. ■

Observația 6.2.

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 $f'([x,\ y])=1$, atunci $f(x)(f(y))^{-1}=1$, deci $f(x)=f(y)$, de unde $x=y$, adică $[x, y]=[x, x]=1$.

2. Dacă pe mulțimea dubletelor (G, f) cu G grup abelian şi $f:M\to G$ morfism injectiv de monoizi definim relația $(G, f)\leq(G', f')\Leftrightarrow$ există $h:G\to G'$ a.î. h este morfism injectiv de grupuri şi $h\circ f=f'$, atunci se verifică imediat că relația de mai sus este o relație de ordine iar dubletul $(G(M), i_M)$ din Teorema lui Malțev este cel mai mic element față de această relație de ordine.

Definiția 6.3. Considerând monoidul ($\mathbb{N}$, +) (ce are proprietatea de simplificare conform Propoziției 1.9.) şi urmând tehnica dată de Teorema lui Malțev, mulțimea subiacentă grupului aditiv (G($\mathbb{N}$), +) se notează prin $\mathbb{Z}$ şi poartă numele de *mulțimea numerelor întregi* iar grupul ($\mathbb{Z}$, +) *grupul aditiv al numerelor întregi* **.**

Ținând 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 submulțime a lui $\mathbb{Z}$.

Fie acum $z=[m, n]\in\mathbb{Z}$. Dacă $m=n$, atunci $z=0$. Dacă $m<n$, atunci există $p\in\mathbb{N}^*$ a.î. $m+p=n$ (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 $q\in\mathbb{N}^*$ a.î. $n+q=m$ şi astfel $z=[q, 0]$ identificându-se cu numărul natural q.

Ținând 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 $\mathbb{Z}=\{0 , \pm1 , \pm2 , \ldots.\}$.

Lema 6.4. Fie $x, y, z, t, x', y', z', t'\in\mathbb{N}$ a.î. $[x, y]=[x', y']$ 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

$$[xz+yt, xt+yz]=[x'z'+y't', x't'+y'z']\Leftrightarrow$$

$$(xz+yt)+(x't'+y'z')=(xt+yz)+(x'z'+y't')\Leftrightarrow$$

$x(z-t)+y(t-z)=x'(z'-t')+y'(t'-z')\Leftrightarrow(x-y)(z-t)=(x'-y')(z'-t')$ ceea ce este adevărat deoarece $x-y=x'-y'$ şi $z-t=z'-t'$. ■

Fie acum $\alpha=[x, y]$ şi $\beta=[z, t]$ două numere întregi.

Definind $\alpha\cdot\beta=[xz+yt, xt+yz]$, conform Lemei 6.4. deducem că această definiție este corectă .

Propoziția 6.5. $(\mathbb{Z}, \cdot)$ este monoid comutativ, înmulțirea este distributivă față de adunare iar dacă $\alpha,\alpha'\in\mathbb{Z}$ şi $\alpha\alpha'=0$, atunci $\alpha=0$ sau $\alpha'=0$.

Demonstrație. Pentru a demonstra că $(\mathbb{Z}, \cdot)$ este monoid comutativ fie $\alpha=[x, y]$, $\alpha'=[x', y']$, $\alpha''=[x'', y'']$ trei elemente oarecare din $\mathbb{Z}$. Atunci :

$\alpha(\alpha'\alpha'')=[x,y][x'x''+y'y'',x'y''+y'x'']=[x(x'x''+y'y'')+y(x'y''+y'x''),$
$x(x'y''+y'x'')+y(x'x''+y'y'')]=[xx'x''+xy'y''+x'yy''+x''yy',$
$xx'y''+xx''y'+x'x''y+yy'y'']$ iar

$\mathbf{(\alpha\alpha')\alpha''=[xx'+yy',\ xy'+x'y][x'', y'']}$

$\mathbf{=[(xx'+yy')x''+(xy'+x'y)y'', (xx'+yy')y''+(xy'+x'y)x'']}$

$\mathbf{=[xx'x''+xy'y''+x'yy''+x''yy', xx'y''+xx''y'+x'x''y+yy'y''] ,}$

de unde deducem că $\alpha(\alpha'\alpha'')=(\alpha\alpha')\alpha''$ adică înmulțirea numerelor întregi este asociativă.

În mod evident, $\alpha\alpha'=\alpha'\alpha$ (deoarece înmulțirea numerelor naturale este comutativă), adică înmulțirea numerelor întregi este comutativă.

Deoarece $\alpha[1, 0]=[x, y][1, 0]=[x, y]=\alpha$, 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,

$\mathbf{\alpha(\alpha'+\alpha'')=[x, y][x'+x'' , y'+y'']}$

$\mathbf{=[x\,(x'+x'')+y(y'+y''),\ x(y'+y'')+y\,(x'+x'')]}$

$\mathbf{=[xx'+xx''+yy'+yy'', xy'+xy''+yx'+yx'']}$ **iar**

$\mathbf{\alpha\alpha'+\alpha\alpha''=[x, y][x',y']+[x, y]\,[x'', y'']}$

$\mathbf{=[xx'+yy', xy'+yx']+[xx''+yy'', xy''+yx'']}$

$\mathbf{=[xx'+yy'+xx''+yy'',\ xy'+yx'+xy''+yx'']}$ **de unde se observă că $\alpha(\alpha'+\alpha'')=\alpha\alpha'+\alpha\alpha''$.**

Fie $\alpha\alpha'=0=[0, 0]$ cu $\alpha\neq0$ (adică $x\neq y$). Atunci $xx'+yy'=xy'+x'y$, de unde $(x-y)(x'-y')=0$ şi cum $x-y\neq0$, atunci $x'-y'=0$, adică $x'=y'$ (conform Propoziției 1.15.), deci $\alpha'=0$.■

Definiția 6.6. Pentru $x, y \in \mathbb{Z}$ definim $x \leq y \Leftrightarrow y-x \in \mathbb{N}$.

Teorema 6.7. Dubletul $(\mathbb{Z}, \leq)$ 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 $m, n \in \mathbb{N}$ a.î. $y-x=m$ şi $x-y=n$, de unde $m+n=0$ şi deci $m=n=0$ (conform Propoziției 1.11.), adică $x=y$.

Dacă $x \leq y$ şi $y \leq z$, atunci există $m, n \in \mathbb{N}$ a.î. $x+m=y$ 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 $(-\mathbb{N}^*) \cap \mathbb{N}=\emptyset$. ■

Observația 6.8. 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 6.9. Fie $x, y, z \in \mathbb{Z}$ a.î. $x \leq y$.
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 $xz \geq yz$. ■

Observația 6.10. 1. Dacă G este un grup, $x \in G$ şi $n \in \mathbb{Z}$ atunci definim

$$x^n = \begin{cases} x^n \ \ daca \quad n \in N \\ \left(x^{-1}\right)^{-n} daca \quad n \in Z \setminus N \end{cases}$$

Se probează imediat că dacă $x \in G$ şi $m, n \in \mathbb{Z}$ atunci $x^m x^n = x^{m+n}$ şi $(x^m)^n = x^{mn}$. De asemenea, dacă $x, y \in G$, $xy = yx$ şi $n \in \mathbb{Z}$, atunci $(xy)^n = x^n y^n$.

2. Tinând cont de cele mai înainte, Propoziția 2.7 capătă următoarea formă:

Dacă $M \subseteq G$ este o mulțime nevidă, atunci

$$\langle M \rangle = \{ x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n} \mid n \in \mathbb{N}, \varepsilon_1, \ldots \varepsilon_n \in \mathbb{Z} \text{ iar } x_1, \ldots x_n \in M \}.$$

Dacă $M=\{x\}$, atunci $\langle x \rangle = \{x^n : n \in \mathbb{Z}\}$ (vezi Corolarul 2.8).

Să caracterizăm acum subgrupurile grupului $(\mathbb{Z},+)$ iar în acest sens pentru $n \in \mathbb{N}$, notăm $n\mathbb{Z}=\{nk : k \in \mathbb{Z}\}$.

Teorema 6.11. Următoarele afirmații sunt echivalente

(i) $H \leq (\mathbb{Z},+)$

(ii) Există $n \in \mathbb{N}$ astfel încât $H=n\mathbb{Z}$.

Demonstrație. **(ii) $\Rightarrow$ (i). Să arătam că dacă $H=n\mathbb{Z}$, atunci $H \leq (\mathbb{Z},+)$ iar pentru aceasta fie $x, y \in H$, adică $x=nk$, $y=nt$ cu $k, t \in \mathbb{Z}$. Atunci $x-y=n(k-t) \in H$, adică $H \leq (\mathbb{Z}+)$.**

(i)$\Rightarrow$(ii). Fie $H \leq (\mathbb{Z},+)$. Dacă $H=\{0\}$, atunci $H=0\mathbb{Z}$. Să presupunem că există $x \in H$ astfel încât $x \neq 0$. Dacă $x>0$, atunci $x \in \mathbb{N}^* \cap H$ iar dacă $x<0$, atunci $-x \in \mathbb{N}^* \cap H$ (căci $H \leq (\mathbb{Z},+)$). În concluzie $A=\mathbb{N}^* \cap H \subseteq \mathbb{N}$ şi $A \neq \emptyset$. Conform Teoremei 1.21. A are un cel mai mic element n şi să demonstrăm că $H=n\mathbb{Z}$.

Cum $n \in H \cap \mathbb{N}^*$ şi $H \leq (\mathbb{Z},+)$, atunci pentru orice $k \in \mathbb{Z}$, $nk \in H$, adică $n\mathbb{Z} \subseteq H$.

Pentru cealaltă incluziune, fie $m \in H$. Atunci $m \geq n$ şi conform teoremei împărțirii cu rest din $\mathbb{N}$ (Corolar 1.25.) există c, $r \in \mathbb{N}$ astfel încât $m=cn+r$ iar $0 \leq r < n$. Deducem că $r=m-cn$ şi cum m,

$n \in H$ iar $c \in \mathbb{N}$, atunci $r \in H$, deci cu necesitate $r=0$ (altfel din $r<n$ am contrazice minimalitatea lui n). În concluzie $m=cn \in n\mathbb{Z}$, adică $H \subseteq n\mathbb{Z}$, deci $H=n\mathbb{Z}$.■

Fie $n \in \mathbb{N}$, $n \geq 2$ şi $\rho_n \subseteq \mathbb{Z} \times \mathbb{Z}$ definită prin $(x,y) \in \rho_n \Leftrightarrow n \mid x-y$.

Deoarece pentru orice $x \in \mathbb{Z}$, $n|x-x=0$ deducem că ρ_n este reflexivă iar dacă $n|x-y$, atunci $n|y-x$, adică $(y,x) \in \rho_n$ astfel că ρ_n este şi simetrică. Dacă $(x,y), (y,z) \in \rho_n$, atunci $n \mid x-y$, $y-z$ şi atunci $n \mid (x-y)+(y-z)=x-z$, deci $(x,z) \in \rho_n$, adică ρ_n este şi tranzitivă, deci o echivalenţă pe $\mathbb{Z}$.

Dacă $x \in \mathbb{Z}$, atunci împărţind pe x la n avem $x=cn+r$ cu $c \in \mathbb{Z}$ şi $r \in \{0,1,\ldots,n-1\}$

Atunci $x-r=cn$ adică $(x, r) \in \rho_n$ şi deci $[x]_{\rho_n} = [r]_{\rho_n}$ astfel că

$\mathbb{Z}/\rho_n = \{[0]_{\rho_n}, [1]_{\rho_n}, \ldots, [n-1]_{\rho_n}\}$

Pentru a respecta tradiţia notaţiilor, vom nota $\mathbb{Z}/\rho_n = \mathbb{Z}_n$ iar $[k]_{\rho_n} = \hat{k}$ pentru orice $k \in \{0,1,\ldots,n-1\}$ (dacă nu este pericol de confuzie); astfel $\mathbb{Z}_n = \{\hat{0}, \hat{1}, \ldots, \widehat{n-1}\}$ iar $\hat{k} = \{k+cn \mid c \in \mathbb{Z}\}$ pentru orice $k \in \{0,1,\ldots,n-1\}$.

Elementele lui $\mathbb{Z}_n$ se numesc *clasele de resturi modulo n.*

Observaţia 6.12. **Dacă notăm $H=n\mathbb{Z}$ am văzut că $H \leq (\mathbb{Z},+)$ iar cum $(\mathbb{Z},+)$ este grup comutativ, de fapt $H \trianglelefteq (\mathbb{Z},+)$.**

Deoarece pentru orice $0 \leq k \leq n-1$, $\hat{k} = \{k+cn \mid c \in \mathbb{Z}\}$, ţinând cont de cele expuse la §4, de fapt $\hat{k} = k+H$, astfel că $\mathbb{Z}_n = \mathbb{Z}/H$.

Astfel, dacă pentru $\hat{k}, \hat{t} \in \mathbb{Z}_n$ definim $\hat{k} + \hat{t} = \widehat{k+t}$ atunci $(\mathbb{Z}_n, +)$ devine grup (comutativ) în care elementul neutru este $\hat{0}$ iar $-\hat{k} =$

$\widehat{n-k}$ **pentru orice 0≤k≤n-1. Deducem imediat că** $\mathbb{Z}_n=<\hat{1}>$**, adică (**$\mathbb{Z}_n$ **,+) este un grup ciclic cu n elemente.**

Să definim acum şi înmulțirea claselor de resturi modulo n, **pentru** $\hat{k},\hat{t}\in\mathbb{Z}$ **prin** $\hat{k}\cdot\hat{t}=\widehat{kt}$**.**

Dacă $\hat{k}=\hat{k'}$ **şi** $\hat{t}=\hat{t'}$**, atunci n | k-k′ şi n | t-t′, astfel că dacă scriem kt-k′t′=k(t-t′)+t′(k-k′) deducem că n | kt-k′t′** $\Leftrightarrow \widehat{kt}=\widehat{k't'}$**, adică înmulțirea claselor de resturi este corect definită.**

Propoziția 6.13. ($\mathbb{Z}_n$, ·) este monoid comutativ iar

$$U(\mathbb{Z}_n,\cdot)=\{\hat{k} \mid (k,n)=1\}.$$

Demonstrație. **Asociativitatea înmulțirii pe** $\mathbb{Z}_n$ **este imediată (ea reducându-se la asociativitatea înmulțirii pe** $\mathbb{Z}$ **) . Elementul neutru este** $\hat{1}$ **deoarece** $\hat{k}\cdot\hat{1}=\hat{k}$**, pentru orice** $\hat{k}\in\mathbb{Z}_n$ **. Dacă** $\hat{k}\in U$ **(**$\mathbb{Z}_n$ **,·) atunci există** $\hat{t}\in\mathbb{Z}_n$ **a.î.** $\hat{k}\cdot\hat{t}=\hat{1}$ $\Leftrightarrow$ **n | kt-1, de unde cu necesitate (k, n)=1.**

Reciproc, dacă (k, n)=1, atunci există $\alpha,\beta\in\mathbb{Z}$ **a.î.** $\alpha k+\beta n=1$ **(vezi [4]), de unde** $\hat{\alpha}\cdot\hat{k}=\hat{1}$**, adică** $\hat{k}\in U(\mathbb{Z}_n,\cdot)$**, iar** $\hat{k}^{-1}=\hat{\alpha}$**.**■

Observația 6.14. Funcția $\varphi:\mathbb{N}^*\to\mathbb{N}$, definită prin $\varphi(1)=\varphi(2)=1$ iar pentru $n\geq 3$, $\varphi(n)$=numărul numerelor naturale m a.î. $m<n$ şi $(m, n)=1$ poartă numele de ***indicatorul lui Euler***. Astfel, pentru $n>2$, $|U(\mathbb{Z}_n,\cdot)|=\varphi(n)$.

Propoziția 6.15. Fie G un grup ciclic, $G=<x>$, $x\neq 1$. Dacă $o(x)=\infty$, atunci $G\approx(\mathbb{Z},+)$ pe când dacă $o(x)=n$ $(n\geq 2)$ atunci $G\approx(\mathbb{Z}_n,+)$.

Demonstrație. **Dacă $o(x)=\infty$, atunci $x^k\neq 1$ pentru orice $k\in\mathbb{Z}^*$ iar $G=\{x^k : k\in\mathbb{Z}\}$.**

Definim $f: (\mathbb{Z}, +)\to (G, \cdot)$, $f(k)=x^k$ pentru orice $k\in\mathbb{Z}$. Dacă $k, t\in\mathbb{Z}$ şi $k\neq t$, atunci $x^k\neq x^t$ (căci în caz contrar ar rezulta că $x^{k-t}=1$ sau $x^{t-k}=1$, după cum $k>t$ sau $t>k$), adică $f(k)\neq f(t)$, deci f este funcție injectivă. În mod evident f este surjectivă, adică bijectivă. Deoarece $f(k+t)=x^{k+t}=x^k\cdot x^t = f(k)\cdot f(t)$ pentru orice $k, t\in\mathbb{Z}$ deducem că f este şi morfism de grupuri adică izomorfism de grupuri şi deci $G\approx(\mathbb{Z}, +)$.

Dacă $o(x)=n$, atunci $G=\{1, x, x^2,\ldots, x^{n-1}\}$ şi atunci definim $f: (\mathbb{Z}_n, +)\to(G,\cdot)$ prin $f(\hat{k})= x^k$ pentru orice $0\leq k\leq n-1$.

Dacă $x^k = x^t$ (cu $0\leq k,t\leq n-1$) atunci presupunând că $k>t$ deducem că $n| k-t$ şi astfel $\hat{k}=\hat{t}$, adică f este injectivă. In mod evident f este şi surjectivă, adică f este bijectivă.

Deoarece $f(\hat{k}+\hat{t})=f(\widehat{k+t})= x^{k+t}=x^k\cdot x^t=f(\hat{k})\cdot f(\hat{t})$ pentru orice $\hat{k},\hat{t}\in\mathbb{Z}_n$ deducem că f este şi morfism de grupuri, adică izomorfism de grupuri.■

§7. Teoremele de izomorfism pentru grupuri

Vom începe cu o teoremă cunoscută sub numele de *teorema fundamentală de izomorfism pentru grupuri:*

Teorema 7.1. Dacă G, G′ sunt grupuri iar $f\in\mathrm{Hom}(G, G')$, atunci $G/\mathrm{Ker}(f)\approx\mathrm{Im}(f)$.

Demonstrație. **Dacă notăm $H=\mathrm{Ker}(f)$ atunci $H=\{x\in G \mid f(x)=1\}\trianglelefteq G$ iar $G/\mathrm{Ker}(f)=\{x\ \mathrm{Ker}\ f \mid x\in G\}=\{xH \mid x\in G\}$.**

Definim $\varphi: G/\mathrm{Ker}(f)\to\mathrm{Im}(f)$ prin $\varphi(xH)=f(x)$ pentru orice $x\in G$. Dacă $x, y\in G$, atunci din echivalențele $xH=yH \Leftrightarrow x^{-1}y\in H \Leftrightarrow$ $\Leftrightarrow f(x^{-1}y)=1 \Leftrightarrow f(x)=f(y)$ deducem că φ este corect definită şi

injectivă. Surjectivitatea lui φ fiind imediată deducem că φ este bijecție.

Cum φ ((xH)(yH)) = φ((xy)H) = f(xy) = f(x)f(y) = φ(xH)φ(yH) pentru orice xH, yH∈G/H deducem că φ este şi morfism de grupuri, adică φ este izomorfism de grupuri.■

Corolar 7.2. Dacă G, G′ sunt grupuri iar $f \in Hom(G, G')$ un morfism surjectiv de grupuri, atunci $G/Ker(f) \approx G'$.

Corolar 7.3. Fie G un grup, H, K subgrupuri ale lui G a.î. $K \trianglelefteq G$. Atunci $HK \leq G$, $H \cap K \trianglelefteq H$ iar $HK / K \approx H / H \cap K$.

În plus, dacă şi $H \trianglelefteq G$, atunci $HK \trianglelefteq G$ (unde reamintim că $HK=\{hk / h \in H$ şi $k \in K\}$).

Demonstrație. **Cum $K \trianglelefteq G$, $xK=Kx$ pentru orice $x \in G$ şi prin urmare *HK*=** $\bigcup_{x \in H} Kx = \bigcup_{x \in H} xK$ **=*KH*.**

Dacă $x, y \in HK$, $x=h_1k_1$ şi $y=h_2k_2$ cum $h_1, h_2 \in H$ şi $k_1, k_2 \in K$ atunci scriind:
$xy^{-1}=(h_1k_1)(h_2k_2)^{-1}=(h_1k_1)(h_2^{-1}k_2^{-1})=[h_1(k_1k_2^{-1})h_1^{-1}](h_1h_2^{-1})$ deducem că $xy^{-1} \in KH=HK$ (căci din H, $K \leq G$ şi $K \trianglelefteq G$ deducem pe rând că h_1, $h_2^{-1} \in K$, $h_1(k_1k_2^{-1})h_1^{-1} \in K$ și $h_1h_2^{-1} \in H$), adică $HK \leq G$.

În mod evident $K \trianglelefteq HK$ şi să considerăm $\varphi: H \to HK/K$, $\varphi(x)=xK$ pentru orice $x \in H$ (evident φ este corect definită deoarece pentru $x \in H$ avem $x \in HK$ şi $xK \in HK/K$), care este morfism de grupuri.

Deoarece orice element din HK/K este de forma $(xy)K=x(yK)=xK=\varphi(x)$ (cu $x \in H$ şi $y \in K$) deducem că φ este morfism surjectiv de grupuri.
În plus, $Ker\ \varphi=\{x \in H / \varphi(x)=1\}=\{x \in H / xK=K\}=\{x \in H / x \in K\}=H \cap K$.
Conform Corolarului 7.2. deducem că $H/Ker\varphi \approx HK/K \Leftrightarrow$ $\Leftrightarrow H/H \cap K \approx HK/K$. Dacă şi $H \trianglelefteq G$, atunci pentru orice $x \in G$ avem $x(HK)=(xH)K=(Hx)K=H(xK)=H(Kx)=(HK)x$, adică $HK \trianglelefteq G$.■

Să facem acum preparativele pentru a demonstra o altă teoremă de izomorfism importantă din teoria grupurilor cunoscută sub numele de *teorema de corespondență* pentru grupuri.

Fie deci G un grup, $H \trianglelefteq G$ iar $p_H:G\to G/H$ morfismul surjectiv canonic ($p_H(x)=xH$ pentru orice $x\in G$). Dacă avem $K\leq G$ a.î. $H\subseteq K$ (deci $H\leq K$), atunci $p_H(K)=\{xH \mid x\in K\}=K/H$ şi conform Propoziției 5.4., $K/H\leq G/H$, adică $K/H\in L(G/H)$. Să notăm $L(G;H)=\{K\in L(G)/H\subseteq K\}$ şi să definim $\alpha:L(G;H)\to L(G/H)$, $\alpha(K)=p_H(K)=K/H$ pentru orice $K\in L(G;H)$.

Suntem acum în măsură să enunțăm şi să demonstrăm *teorema de corespondență* pentru grupuri:

Teorema 7.4. Fie G un grup, $H\trianglelefteq G$ iar K, K_1, $K_2\in L(G;H)$. Atunci:

(i) $\alpha:L(G;H)\to L(G/H)$, $\alpha(K)=p_H(K)=K/H$ este izomorfism laticeal

(ii) $K\trianglelefteq G \Leftrightarrow \alpha(K)=K/H\trianglelefteq G/H$ şi în acest caz $G/K \approx (G/H)/(K/H)$.

***Demonstrație.* (i). Să arătăm la început că α este bijecție izotonă. Dacă $S\in L(G/H)$, atunci $p_H^{-1}(S)\leq G$ şi cum $1\in S$, $H=\mathrm{Ker}\, p_H = p_H^{-1}(\{1\})\subseteq p_H^{-1}(S)$, adică $p_H^{-1}(S)\in L(G;H)$. Obținem astfel funcția $\beta:L(G/H)\to L(G;H)$, $\beta(S)=p_H^{-1}(S)$ pentru orice $S\in L(G;H)$.**

Vom demonstra că $\alpha\circ\beta=1_{L(G/H)}$ şi $\beta\circ\alpha=1_{L(G;H)}$, de unde va rezulta că α este bijectivă.

Fie deci $S\in L(G/H)$. Atunci $(\alpha\circ\beta)(S)=\alpha(\beta(S))=p_H(p_H^{-1}(S))$ şi să demonstrăm că $p_H(p_H^{-1}(S))=S$ (de unde va rezulta că $\alpha\circ\beta=1_{L(G/H)}$).

Incluziunea $p_H(p_H^{-1}(S))\subseteq S$ este evidentă.

Fie acum $s\in S$; cum p_H este funcție surjectivă deducem că există $x\in G$ a.î. $s=p_H(x)$, de unde rezultă că $x\in p_H^{-1}(S)$ şi $s=p_H(x)\in p_H(p_H^{-1}(S))$, adică $S\subseteq p_H(p_H^{-1}(S))$, de unde egalitatea $p_H(p_H^{-1}(S))=S$.

De asemenea, pentru $K\in L(G;H)$, $(\beta\circ\alpha)(K)=\beta(\alpha(K))=p_H^{-1}(p_H(K))$ şi să demonstrăm că $p_H^{-1}(p_H(K))=K$ (de unde va rezulta egalitatea $\beta\circ\alpha=1_{L(G;H)}$). Incluziunea $K\subseteq p_H^{-1}(p_H(K))$ este evidentă. Pentru

cealaltă incluziune fie $x\in K$. Atunci $p_H(x)\in p_H(K)$ şi găsim $y\in K$ a.î. $p_H(x)=p_H(y)$.

Deducem că $x^{-1}y\in Ker\ p_H=H\subseteq K$ şi deci $x\in Ky=K$ (deoarece $y\in K$), de unde şi incluziunea $p_H^{-1}(p_H(K))\subseteq K$, adică avem egalitatea $p_H^{-1}(p_H(K))=K$. Dacă $K_1\leq K_2$ atunci în mod evident $\alpha(K_1)\leq\alpha(K_2)$. Reciproc, dacă $\alpha(K_1)\leq\alpha(K_2)$, atunci $K_1=\beta(\alpha(K_1))=p_H^{-1}(\alpha(K_1))\leq$ $\leq p_H^{-1}(\alpha(K_2))=\beta(\alpha(K_2))=K_2$. Cum probarea faptului că α este chiar morfism laticeal este imediată, rezultă că α este de fapt izomorfism de latici.

(ii). Să presupunem că dacă $K\in L(G;H)$, atunci $K\trianglelefteq G$ şi să considerăm $\varphi:G/H\to G/K$, $\varphi(xH)=xK$, pentru orice $x\in G$. Dacă avem $x,y\in G$ a.î. $xH=yH$, atunci $x^{-1}y\in H$ şi cum $H\subseteq K$ deducem că $x^{-1}y\in K$, adică $xK=yK$ şi deci φ este corect definită ; în mod evident φ este morfism surjectiv de grupuri.

Avem $x\in H=Ker\varphi \Leftrightarrow \varphi(xH)=1 \Leftrightarrow xK=K \Leftrightarrow x\in K$, deci Ker $\varphi=K/H$, de unde concluzia că $K/H\trianglelefteq G/H$.

Conform Corolarului 7.2. de la teorema fundamentală de izomorfism pentru grupuri avem $(G/H)/Ker\ \varphi \approx G/K \Leftrightarrow (G/H)/(K/H)\approx G/K$.

Reciproc, dacă $K/H\trianglelefteq G/H$, atunci putem considera $G\xrightarrow{p_H} G/H\xrightarrow{p_{K/H}}(G/H)/(K/H)$ iar cum $K=Ker(p_{K/H}op_H)$ deducem că $K\trianglelefteq G$.■

Ca un corolar al teoremei de corespondență pentru grupuri putem să caracterizăm subgrupurile grupului $(\mathbb{Z}_n,+)$ pentru $n\geq 2$. După cum am văzut mai înainte $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}$. Conform teoremei de corespondență pentru grupuri orice subgrup al lui $\mathbb{Z}_n$ va fi de forma $K/n\mathbb{Z}$ unde $K\leq(\mathbb{Z},+)$ a.î. $n\mathbb{Z}\subseteq K$ şi în plus $\mathbb{Z}_n/(K/n\mathbb{Z})\approx\mathbb{Z}/K$.

Conform Teoremei 6.11., $K=d\mathbb{Z}$ cu d divizor natural al lui n.

Prin urmare, orice subgrup H al lui $\mathbb{Z}_n$ este de forma $H=(d\mathbb{Z})/(n\mathbb{Z})$ unde $d>0$ şi $d|n$ iar $\mathbb{Z}_n/H=\mathbb{Z}/d\mathbb{Z}=\mathbb{Z}_d$. Pentru un astfel de grup H avem $|\mathbb{Z}_n:H|=|\mathbb{Z}_d|=d$ iar conform teoremei lui Lagrange

$|H|=|\mathbb{Z}_n|/|\mathbb{Z}_n:H|=n/d$. În plus K este grup ciclic, anume $K=<\hat{d}>$, unde $\hat{d}=d+n\mathbb{Z}\in\mathbb{Z}_n$.

Pentru exemplificare să considerăm n=12. Divizorii lui 12 sunt 1, 2, 3, 4, 6, 12, deci subgrupurile lui $\mathbb{Z}_{12}$ sunt:

1 $\mathbb{Z}/12\mathbb{Z} = \mathbb{Z}_{12} = \{\hat{0}, \hat{1},..., \hat{11}\}$

2 $\mathbb{Z}/12\mathbb{Z} = \{\hat{0}, \hat{2}, \hat{4}, \hat{6}, \hat{8}, \hat{10}\}$

3 $\mathbb{Z}/12\mathbb{Z} = \{\hat{0}, \hat{3}, \hat{6}, \hat{9}\}$

4 $\mathbb{Z}/12\mathbb{Z} = \{\hat{0}, \hat{4}, \hat{8}\}$

6 $\mathbb{Z}/12\mathbb{Z} = \{\hat{0}, \hat{6}\}$ **şi**

12 $\mathbb{Z}/12\mathbb{Z} = \{\hat{0}\}$**.**

§8. Produse directe finite de grupuri. Teorema chinezească a resturilor. Numărul tipurilor de grupuri abeliene finite

Fie $G_1, G_2, \ldots, G_n$ $(n\geq 2)$ grupuri (multiplicative) iar $G = G_1 \times \ldots \times G_n = \{(x_1, \ldots, x_n) \mid x_i \in G_i, 1 \leq i \leq n\}$.

Definind pentru $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in G$, $xy = (x_1y_1, \ldots, x_ny_n)$, aşa cum am arătat în §1, G devine monoid în care $1=(1,\ldots,1)$.

Deoarece $(x_1,...,x_n)(x_1^{-1},...,x_n^{-1}) = (x_1x_1^{-1},...,x_nx_n^{-1}) = (1,...,1) = 1 = (x_1^{-1}x_1, ..., x_n^{-1}x_n) = (x_1^{-1},...,x_n^{-1})(x_1,...,x_n)$ deducem că $(x_1^{-1},...,x_n^{-1}) = x^{-1}$, de unde concluzia că G devine grup.

Ca şi în cazul monoizilor, pentru fiecare $1 \leq i \leq n$, $p_i : G \to G_i$, $p_i(x)=x_i$ pentru orice $x=(x_1,\ldots,x_n)\in G$ este morfism surjectiv de grupuri iar dubletul $(G,(p_i)_{1\leq i\leq n})$ verifică următoarea proprietate de universalitate:

Pentru oricare grup G' şi orice familie de morfisme de grupuri, $(p'_i)_{1\le i\le n}$ cu $p'_i : G\to G'_i$ pentru $1\le i \le n$, există un unic morfism de grupuri $u : G'\to G$ a.î. $p_iou=p'_i$ pentru orice $1\le i \le n$.

Grupul G (împreună cu morfismele, $(p_i)_{1\le i\le n}$) poartă numele de *produsul direct* al grupurilor $G_1, \dots , G_n$.

Propoziția 8.1 Dacă $G_1,\dots,G_n$ sunt grupuri, atunci $Z(G_1 \times \dots \times G_n)= Z(G_1) \times \dots \times Z(G_n)$ astfel că $G_1 \times \dots \times G_n$ este grup comutativ dacă şi numai dacă fiecare dintre grupurile $G_1 \dots G_n$ este comutativ .

Demonstrație. Dacă $x,y \in G = G_1 \times \dots \times G_n$, $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$ atunci $xy = yx \Leftrightarrow (x_1y_1, \dots, x_ny_n) = (y_1x_1, \dots, y_nx_n) \Leftrightarrow$ $\Leftrightarrow x_1y_1 = y_1x_1 , \dots , x_ny_n = y_nx_n$, de unde egalitatea

$$Z(G)=Z(G_1) \times \dots \times Z(G_n). \blacksquare$$

Propoziția 8.2. Fie G_1, G_2 două grupuri.

Atunci $G_1\times\{1\}, \{1\}\times G_2 \trianglelefteq G_1\times G_2$.

Demonstrație. Fie $x=(x_1,x_2)\in G_1\times G_2$ şi $y=(x,1)\in G_1\times\{1\}$. Atunci $x^{-1}yx = (x_1^{-1},x_2^{-1})(x,1)(x_1,x_2) = (x_1^{-1}xx_1, x_2^{-1}x_2) = (x_1^{-1}xx_1,1) \in$ $\in G_1\times\{1\}$, de unde concluzia că $G_1\times\{1\}\trianglelefteq G_1\times G_2$.

Analog se probează că $\{1\} \times G_2 \trianglelefteq G_1 \times G_2$.$\blacksquare$

Teorema 8.3. Fie G un grup, $H, K \trianglelefteq G$ a.î. $H\cap K = \{1\}$ şi $HK=G$. Atunci $G \approx H \times K$.

Demonstrație. Reamintim că $HK=\{hk \mid h\in H, k\in K\}$. Să probăm acum că pentru orice $x\in G$, elementele $h\in H$ şi $k\in K$ pentru care $x=hk$ sunt unice. Într-adevăr, dacă mai avem h',k' a.î. $h'\in H$, $k'\in K$ şi $x = hk = h'k'$, atunci $h'^{-1}h=k'k^{-1} \in H\cap K = \{1\}$, de unde $h'^{-1}h = k'k^{-1} = 1 \Leftrightarrow h=h'$, $k=k'$.

Fie acum $h\in H$, $k\in K$ şi $x = h^{-1}k^{-1}hk$. Cum $K\trianglelefteq G$ deducem că $h^{-1}k^{-1}h\in K$, astfel că $x = h^{-1}k^{-1}hk = (h^{-1}k^{-1}h)k\in K$ şi cum analog se arată că $x\in H$, deducem că $x\in H\cap K=\{1\}$, adică $x=1$ şi astfel $hk=kh$.

Fie acum $x\in G$. Atunci există $h\in H$, $k\in K$, unice a.î. $x=hk$ şi definim $f:G\to H\times K$, $f(x)=(h,k)$. Dacă mai avem $x'=h'k'$ cu $h'\in H$, $k'\in K$ atunci $xx'=(hk)(h'k') = h(kh')k' = h(h'k)k' = (hh')(kk')$, de unde concluzia că $f(xx')=(hh',kk')=(h,k)(h'k')=f(x)f(x')$, adică f este morfism de grupuri. Cum în mod evident f este funcție bijectivă, deducem că f este izomorfism de grupuri, adică $G\approx H\times K$.■

Teorema 8.4. Fie G_1,G_2 grupuri, $G=G_1\times G_2$, $H_1\trianglelefteq G_1$, $H_2\trianglelefteq G_2$. Atunci $H_1\times H_2\trianglelefteq G$ iar $G/(H_1\times H_2)\approx G_1/H_1\times G_2/H_2$ **.**

Demonstrație. Fie $p_{H_1}:G_1\to G_1/H_1$ şi $p_{H_2}:G_2\to G_2/H_2$ morfismele surjective canonice de grupuri şi $f:G\to\left(G_1/H_1\right)\times\left(G_2/H_2\right)$, $f(x)=\left(p_{H_1}(x),p_{H_2}(x)\right)$ pentru orice $x\in G$. Se arată imediat că f este morfism surjectiv de grupuri, $\operatorname{Ker} f = H_1\times H_2$, de unde ținând cont de teorema fundamentală de izomorfism pentru grupuri deducem că $H_1\times H_2\trianglelefteq G$ iar

$$G/Ker(f)\approx \operatorname{Im}(f)\Leftrightarrow G/(H_1\times H_2)\approx G/H_1\times G/H_2\ .\blacksquare$$

Corolar 8.5. Dacă $G=G_1\times G_2$, atunci $G/(G_1\times\{1\})\approx G_2$ **.**

Teorema 8.6. Fie $m,n\in\mathbb{N}$, $m,n\geq 2$ şi $(m,n)=1$.
Atunci $\mathbb{Z}_m\times\mathbb{Z}_n\approx\mathbb{Z}_{mn}$ (ca grupuri aditive).

Demonstrație. Fie $\mathbb{Z}_m=\{\hat{0},\hat{1},\ldots,\widehat{m-1}\}$, $\mathbb{Z}_n=\{\overline{0},\overline{1},\ldots,\overline{n-1}\}$ iar $\mathbb{Z}_{mn}=\left\{\overline{\overline{0}},\overline{\overline{1}},\ldots,\overline{\overline{mn-1}}\right\}$ şi $f:\mathbb{Z}_{mn}\to\mathbb{Z}_m\times\mathbb{Z}_n$,

$f(\overline{\overline{x}}) = (\hat{x}, \overline{x})$ pentru orice x∈{0,1, … , mn-1}. Cum (m,n)=1 avem echivalențele $\overline{\overline{x}} = \overline{\overline{y}} \Leftrightarrow mn \mid x - y \Leftrightarrow m \mid x - y şi\ n \mid x - y \Leftrightarrow \hat{x} = \hat{y}\ şi\ \overline{x} = \overline{y}$ de unde concluzia că f este bine definită şi injectivă.

Cum $|\mathbb{Z}_m \times \mathbb{Z}_n| = |\mathbb{Z}_{mn}| = mn$, deducem că f este o bijecție. Deoarece probarea faptului că f este şi morfism de grupuri aditive este imediată, deducem că f este izomorfism de grupuri.■

Corolar 8.7. Dacă $m_1, m_2, \ldots, m_n \geq 2$ sunt numere naturale a.î. pentru $i \neq j$, $(m_i, m_j)=1$, atunci $Z_{m_1} \times \ldots \times Z_{m_n} \approx Z_{m_1 m_2 \ldots m_n}$ (ca grupuri aditive).

Observația 8.8. Teorema 8.6. mai este cunoscută în literatura matematică şi sub numele de *teorema chinezească a resturilor***.**

Lema 8.9. Dacă M şi N sunt doi monoizi a.î. M ≈ N, atunci U(M) ≈ U(N) (ca izomorfism de grupuri).

Demonstrație. Cum M≈N există f:M→N izomorfism de monoizi. Dacă x∈**U**(M), atunci există y∈M a.î. xy=yx=1. Deducem că imediat că f(x)f(y)=f(y)f(x)=1, adică f(x)∈**U**(N), astfel că $\bar{f}$:**U**(M)→**U**(N), $\bar{f} = f_{|U(M)}$ este corect definită. Dacă x,y∈**U**(M), atunci xy∈**U**(M) şi cum $\bar{f}$ (xy) = f(xy) = f(x)f(y) = $\bar{f}$ (x) $\bar{f}$ (y), deducem că f este morfism de grupuri. Datorită bijectivității lui f deducem imediat şi bijectivitatea lui $\bar{f}$, de unde izomorfismul de grupuri **U**(M)≈**U**(N).■

Lema 8.10. Dacă m.n∈ℕ, m,n≥2 şi (m,n)=1 atunci

$(\mathbb{Z}_m, \cdot) \times (\mathbb{Z}_n, \cdot) \approx (\mathbb{Z}_{mn}, \cdot)$ (izomorfism de monoizi).

Demonstrație. Ca şi în demonstrația Teoremei 8.6. fie

$$\mathbb{Z}_m = \{\hat{0}, \hat{1}, \ldots, \widehat{m-1}\},\ \mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\},\ \mathbb{Z}_{mn} = \{\overline{\overline{0}}, \overline{\overline{1}}, \ldots, \overline{\overline{mn-1}}\}$$

şi $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $f(\overline{\overline{x}}) = (\hat{x}, \overline{x})$ pentru orice $x \in \{0,1, \ldots, mn-1\}$. Dacă mai avem $y \in \{0,1, \ldots, mn-1\}$, atunci $\overline{\overline{x}} = \overline{\overline{y}} \Leftrightarrow mn \mid x-y \Leftrightarrow m \mid x-y$ şi $n \mid x-y$ (căci $(m, n) = 1$) $\Leftrightarrow \hat{x} = \hat{y}$ şi $\overline{x} = \overline{y}$, de unde deducem că $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $f(\hat{x}) = (\hat{x}, \overline{x})$ este corect definită şi injectivă. În mod evident, din $\overline{\overline{x}}\,\overline{\overline{y}} = \overline{\overline{xy}}$ deducem că

$$f(\overline{\overline{x}}\,\overline{\overline{y}}) = f(\overline{\overline{xy}}) = (\hat{xy}, \overline{xy}) = (\hat{x}, \overline{x}) \cdot (\hat{y}, \overline{y}) = f(\overline{\overline{x}}) f(\overline{\overline{y}})$$

iar $f(\overline{\overline{1}}) = (\hat{1}, \overline{1}) = 1$ (în $\mathbb{Z}_m \times \mathbb{Z}_n$), adică f este morfism de monoizi. Cum $|\mathbb{Z}_m \times \mathbb{Z}_n| = |\mathbb{Z}_{mn}| = mn$ deducem că f este surjecție, adică bijecție, deci izomorfism de monoizi.■

Corolar 8.11. Dacă $m, n \in \mathbb{N}$, $m, n \geq 2$ şi $(m, n)=1$, atunci $\varphi(mn)=\varphi(m)\varphi(n)$.

Demonstrație. Conform Lemei 8.10. avem izomorfismul de monoizi $(\mathbb{Z}_m,\cdot) \times (\mathbb{Z}_n,\cdot) \approx (\mathbb{Z}_{mn},\cdot)$.

Conform Lemei 8.9 avem izomorfism de grupuri $\mathbf{U}[(\mathbb{Z}_m,\cdot) \times (\mathbb{Z}_n,\cdot)] \approx \mathbf{U}(\mathbb{Z}_{mn},\cdot)$. Însă $\mathbf{U}[(\mathbb{Z}_m,\cdot) \times (\mathbb{Z}_n,\cdot)] =$
$= \mathbf{U}(\mathbb{Z}_m,\cdot) \times \mathbf{U}(\mathbb{Z}_n,\cdot)$, de unde $\mathbf{U}(\mathbb{Z}_m,\cdot) \times \mathbf{U}(\mathbb{Z}_n,\cdot) \approx \mathbf{U}(\mathbb{Z}_{mn},\cdot)$.

Totul rezultă acum din Observația 6.15. deoarece
$|\mathbf{U}(\mathbb{Z}_m,\cdot) \times \mathbf{U}(\mathbb{Z}_n,\cdot)| = |\mathbf{U}(\mathbb{Z}_m,\cdot)| \cdot |\mathbf{U}(\mathbb{Z}_n,\cdot)| = \varphi(m)\varphi(n)$ iar $|\mathbf{U}(\mathbb{Z}_{mn},\cdot)| =$
$= \varphi(mn)$.■

Corolar 8.12. Dacă $m_1, \ldots, m_n \geq 2$ $(n \geq 2)$ iar pentru $i \neq j$, $(m_i, m_j)=1$, atunci $\varphi(m_1 m_2 \ldots m_n)=\varphi(m_1)\varphi(m_2) \ldots \varphi(m_n)$.

Corolar 8.13. Dacă $n \in \mathbb{N}$, $n \geq 2$ iar $n = p_1^{k_1} \ldots p_t^{k_t}$ este descompunerea lui n în factori primi distincți, atunci

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_t}\right).$$

Demonstrație. Deoarece pentru i≠j, $\left(p_i^{k_i}, p_j^{k_j}\right)=1$, deducem (ținând cont de Corolarul 8.11.) că:

$$\varphi(n)=\varphi\left(p_1^{k_1}\ldots p_t^{k_t}\right)=\varphi\left(p_1^{k_1}\right)\ldots\varphi\left(p_t^{k_t}\right)=$$
$$=\left(p_1^{k_1}-p_1^{k_1-1}\right)\ldots\left(p_t^{k_t}-p_t^{k_t-1}\right)=$$
$$=p_1^{k_1}\ldots p_t^{k_t}\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_t}\right)=n\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_t}\right).\blacksquare$$

Dacă $n\in\mathbb{N}^*$, prin *partiție* a lui n înțelegem un sistem ordonat de numere naturale $(m_1, m_2, \ldots, m_k)$ a.î. $m_1\geq m_2\geq\ldots\geq m_k$ iar $m_1+m_2+\ldots+m_k=n$; vom nota prin k_n numărul partițiilor lui n.

Iată, pentru n≤6 toate partițiile distincte ale lui n:

n=1 : (1) , deci $k_1=1$

n=2 : (2), (1,1) , deci $k_2=2$

n=3 : (3), (2,1), (1,1,1) , deci $k_3=3$

n=4 : (4), (3,1), (2,2), (2,1,1), (1,1,1,1) , deci $k_4=5$

n=5 : (5), (4,1), (3,2), (3,1,1), (2,2,1), (2,1,1,1), (1,1,1,1,1) , deci $k_5=7$

n=6 : (6), (5,1), (4,2), (4,1,1), (3,3), (3,2,1), (3,1,1,1), (2,2,2), (2,2,1,1), (2,1,1,1,1), (1,1,1,1,1,1) , deci $k_6=11$.

Observația 8.14. Din teorema de structură a grupurilor abeliene finit generate (vezi [22, p.99]) deducem că dacă p este un număr prim iar $n\in\mathbb{N}^*$ atunci există k_n tipuri de grupuri abeliene finite de ordin p^n.

Mai general, dacă $n=p_1^{n_1}\ldots p_t^{n_t}$ **este descompunerea lui n în produse distincte de numere prime, atunci ținând cont şi de Corolarul 10.7 deducem că numărul tipurilor de grupuri abeliene de ordin n este egal cu** $k_{n_1}\ldots k_{n_t}$ **.**

Astfel, există $k_4 = 5$ tipuri de grupuri abeliene de ordin p^4 (cu p prim):

$\mathbb{Z}_{p^4}$ - corespunzător partiției (4)

$\mathbb{Z}_{p^3}\times\mathbb{Z}_p$ - corespunzător partiției (3,1)

$\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ - corespunzător partiției (2,2)

$\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$- corespunzător partiției (1,1,1,1)

iar dacă p şi q sunt numere prime distincte, atunci există $k_3 \cdot k_3 = 9$ tipuri de grupuri abeliene de ordin p^3q^3:

$\mathbb{Z}_{p^3} \times \mathbb{Z}_{q^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_{q^3}$, $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q^3}$, $\mathbb{Z}_{p^3} \times \mathbb{Z}_{q^2} \times \mathbb{Z}_q$,

$\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_{q^2} \times \mathbb{Z}_q$, $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q^2} \times \mathbb{Z}_q$, $\mathbb{Z}_{p^3} \times \mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{Z}_q$,

$\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{Z}_q$, $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{Z}_q$.

Observația 8.15. 1. Cum $4=2^2$, conform Observației 8.14. există există două tipuri de grupuri cu 4 elemente: $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$.

2. Considerând $K = \{1, a, b, c\}$ cu elementele multiplicându-se după regula $a^2 = b^2 = c^2 = 1$, $ab = ba = c$, $bc = cb = a$ şi $ca = ac = b$, obținem un grup izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2$ numit *grupul lui Klein*.

§9. Teorema lui Cauchy pentru grupuri finite. Grupul diedral D_n de grad n. Structura grupurilor finite cu 2p elemente (p prim, p≥3)

În cadrul acestui paragraf, prin p vom desemna un număr prim (p≥2).

Teorema 9.1. (*Cauchy*) Dacă G este un grup finit a.î. p | |G| , atunci există x∈G a.î. o(x)=p (echivalent cu există H≤G a.î. | H | = p).

Demonstrație. Cazul 1: G comutativ. Vom face inducție matematică după cardinalul grupurilor finite G cu proprietatea că p | |G|. Dacă |G| = p , atunci G este ciclic şi orice element x∈G, x≠1, are ordinul p. Să presupunem afirmația adevărată pentru orice grup comutativ G′ cu proprietatea că |G′|<|G| şi p | |G′| şi s-o demonstrăm pentru grupul comutativ G (în ipoteza p | |G|). Pentru aceasta alegem x∈G, x≠1. Dacă p | o(x), atunci o(x)=tp cu t∈$\mathbb{N}^*$ iar din $x^{o(x)}=1$ deducem că $x^{tp}=1 \Leftrightarrow (x^t)^p=1$ adică $o(x^t)=1$. Dacă p ∤ o(x), atunci alegem $H=<x>=\{1, x, \ldots, x^{o(x)-1}\}$ care este subgrup normal al lui G (G fiind

presupus comutativ). Dacă vom considera $G'=G/H$ atunci $|G'|=|G|:o(x)<|G|$ şi cum $p \mid |G|$ iar $(p,o(x))=1$ deducem că $p \mid |G'|$. Aplicând ipoteza de inducţie lui G' deducem că există un element $yH \in G'$ a.î. $o(yH)=p$. Din $(yH)^p=H$ deducem că $y^pH=H$, adică $y^p \in H$, deci $y^p=x^t$ cu $1 \le t \le o(x)-1$. Deducem imediat că $y^{o(x)p}=1$ şi astfel elementul $z=y^{o(x)} \in G$ va avea ordinul p.

Cazul 2: G necomutativ. Vom reduce acest caz tot la Cazul 1 iar în acest sens vom utiliza ecuaţia claselor pentru grupul G expusă în §3 al acestui capitol:

$|G| = |Z(G)| + \sum_{x \notin Z(G)} |G : C_G(x)|$ (sumarea făcându-se după elementele $x \in G \setminus Z(G)$ pentru care clasa de conjugare $[x]_{\sim}$ este netrivială).

Dacă există un element $x \notin Z(G)$ a.î. $p \mid |C_G(x)|$ atunci ca şi în cazul 1 facem inducţie după $|G|$ (aplicând ipoteza de inducţie lui $G'=C_G(x)$).

Dacă $p \nmid |C_G(x)|$ pentru orice $x \notin Z(G)$, atunci cum $|G : C_G(x)| = \frac{|G|}{|C_G(x)|}$ deducem că $p \mid |G : C_G(x)|$ şi cum $p \mid |G|$, din ecuaţia claselor deducem că $p \mid |Z(G)|$. Cum $Z(G)$ este comutativ , conform Cazului 1 există un element în $Z(G)$ (deci în G) a.î. ordinul lui este p şi astfel teorema este complet demonstrată.■

Definiţia 9.2. Vom spune despre un grup G că este *p – grup* **dacă ordinul oricărui element al său este o putere naturală a lui p.**

Corolar 9.3. Dacă G este un grup finit , atunci G este p – grup dacă şi numai dacă | G | este o putere naturală a lui p.

Demonstraţie „⇒”. Dacă prin absurd există un număr prim q a.î. $q \neq p$ şi $q \mid |G|$, atunci conform teoremei lui Cauchy, există $x \in G$ a.î. $o(x)=q$ contrazicând faptul că G este p – grup.

„⇐”. Totul rezultă din teorema lui Lagrange (vezi §3).■

Corolar 9.4. Dacă G este un p – grup finit atunci $Z(G) \neq \{1\}$.

Demonstraţie. Scriem din nou ecuaţia claselor pentru grupul G:

$| G | = | Z(G) | + \sum_{x \notin Z(G)} | G : C_G(x) |$ (unde reamintim că suma se face după acele elemente $x \notin Z(G)$ pentru care clasa de conjugare $[x]_{\sim}$ este netrivială). Conform Corolarului 9.3, $|G|=p^n$ cu $n \geq 1$ iar pentru $x \notin Z(G)$ pentru care $[x]_{\sim}$ este netrivială avem $| G : C_G(x) | = p^m$ cu $m \geq 1$ astfel că din ecuația claselor deducem că $p \mid Z(G)|$, adică $| Z(G) | \geq p$ şi astfel Z(G) este netrivial.■

Lema 9.5. Dacă G este un grup a.î. G/Z(G) este ciclic, atunci G este comutativ.

Demonstrație. Fie H=Z(G) iar G/Z(G) = <xH> cu $x \in G$. Dacă $y,z \in G$ atunci $yH=x^mH$ iar $zH=x^nH$ cu $m,n \in \mathbb{N}$, de unde $y=x^mh_1$, $z=x^nh_2$ cu $h_1,h_2 \in H=Z(G)$. Atunci $yz=x^{m+n}h_1h_2$ iar $zy=x^{n+m}h_2h_1$ şi cum $h_1h_2=h_2h_1$ şi m+n=n+m deducem că yz=zy, adică G este comutativ.■

Corolar 9.6. Dacă G este un grup cu p^2 elemente, atunci G este comutativ.

Demonstrație. Cum $Z(G) \leq G$, $| Z(G) | \in \{1, p, p^2\}$. Conform Corolarului 9.4, $|Z(G)| \neq 1$ iar dacă $|Z(G)| = p^2$, atunci G = Z(G), adică G este comutativ. Rămâne să analizăm doar cazul $|Z(G)|=p$. În acest caz, cum $| G / Z(G) | = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$ iar p este prim, deducem că G/Z(G) este ciclic şi conform Lemei 9.5. ajungem şi în acest caz la concluzia că G este comutativ.■

Definiția 9.7. Dacă n≥1 este un numar natural, prin *grupul diedral de grad n* **înțelegem un grup D_n cu 2n elemente generat de două elemente s şi r ce satisfac conditiile: $s^2=1$, $r^n=1$ şi $srs=r^{-1}$. În concluzie, $|D_n|=2n$ iar $D_n=\{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$.**

Teorema 9.8. Presupunem că p este un număr prim ≥3. Dacă G este un grup cu 2p elemente , atunci G este ciclic (izomorf cu $(\mathbb{Z}_{2p},+)$) sau diedral (izomorf cu D_p).

Demonstrație. Cum | G | = 2p iar 2 şi p sunt numere prime (p≥3) atunci (conform Teoremei 9.1.) există s, r∈G a.î. $s^2 = 1$ şi $r^p = 1$. Considerând H = < r > avem | H | = p şi cum $|G:H| = \frac{2p}{p} = 2$ deducem (conform Observației 4.6.) că H⊴G, astfel că $srs^{-1} \in H$, deci $srs = r^i$ cu $0 \le i \le p-1$. Deducem imediat că

$$r^{i^2} = (r^i)^i = (srs)^i = sr^i s = s(srs)s = s^2 r s^2 = r \ ,$$

deci p | i^2-1 =(i - 1)(i +1) . Dacă p | i-1, atunci srs = r ⇔ sr = rs şi atunci G va fi comutativ .

Din teorema de structură o grupurilor abeliene finit generate şi teorema chinezească a resturilor deducem că $G \approx \mathbb{Z}_2 \times \mathbb{Z}_p \approx \mathbb{Z}_{2p}$.

Dacă p | i+1, atunci $srs=r^{-1}$ şi obținem astfel descrierea grupului diedral D_p.■

În continuare vom prezenta un rezultat ce arată în esență că pentru p – grupuri finite funcționează reciproca teoremei lui Lagrange.

Mai precis vom demonstra:

Teorema 9.9. Fie G un p-grup, | G | = p^m cu m∈ℕ. Atunci pentru orice 0 ≤ i ≤ m există un subgrup normal G_i în G a.î. | G_i | =p^i şi 1 = G_0 < G_1 < … < G_m = G.

Demonstrație. Facem inducție matematică după m (afirmația fiind evidentă pentru m=0,1).

Să presupumen m>1 şi că afirmația din enunț este adevărată pentru orice grup G′ de ordin p^{m-1} şi fie G un grup a.î. | G | = p^m . Conform Corolarului 9.4, Z(G)≠1 şi fie z∈Z(G), z≠1. Cum o(z) | | G | = =p^m, fie o(z)=p^n cu n≥1 iar G_1=<$z^{p^{n-1}}$>. Cum $z^{p^{n-1}} \ne 1$ şi $(z^{p^{n-1}})^p = z^{p^n} = 1$ deducem că o($z^{p^{n-1}}$)=p şi astfel | G_1 |=p. Cum z∈Z(G) deducem că G_1≤Z(G) şi atunci în mod evident $G_1 \trianglelefteq G$. Alegând G′=G/G_1 , cum |G′| = p^m/p = p^{m-1} putem aplica ipoteza de inducție lui G′, deci există grupurile G′$_0$,G′$_1$,…G′$_{m-1}$ normale în G′, a.î. G′$_0$<G′$_1$<… ..<G′$_{m-1}$=G′ şi |G′$_i$| = p^i pentru orice 0≤i≤m-1.

Conform teoremei de corespondenţă pentru grupuri (vezi Teorema 7.4.) avem $G'_i = G_{i+1}/G_1$ cu $G_{i+1} \trianglelefteq G$ a.î. $G_1 \subseteq G_i$. In plus, $G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_m = G$ şi pentru orice $0 \le i \le m-1$, $|G_{i+1}| = |G'_i| \cdot |G_1| = p^i \cdot p = p^{i+1}$. Alegând $G_0 = 1$, subgrupurile $G_0, G_1, \ldots, G_m$ satisfac condiţiile din enuţul teoremei. ■

§10. Grupuri de permutări. Teorema lui Cayley.

Grupurile S_n şi A_n.

Fie M o mulţime nevidă iar $\Sigma(M) = \{f \in \mathbf{Hom}(M) \mid f \text{ este bijectivă}\}$. După cum am văzut în §1 al acestui capitol $(\mathbf{Hom}(M), \circ)$ este monoid iar $\Sigma(M)$ apare acum ca grupul unităţilor monoidului **Hom**(M).

Convenim să numim grupul $\Sigma(M)$ ca fiind *grupul permutărilor asupra elementelor mulţimii M.*

Dacă M este o mulţime cu n elemente (exemplul clasic fiind $M = \{1,2,\ldots,n\}$ cu $n \ge 1$), atunci grupul $\Sigma(M)$ se notează prin S_n şi se va numi *grupul permutărilor asupra unei mulţimi cu n elemente sau grup simetric de grad n.* (vom vedea mai departe că pentru grupul S_n natura elementelor mulţimii M joacă un rol secundar, numărul elementelor lui M fiind lucrul important).

Astfel, un element σ al lui S_n se va prezenta de multe ori sub forma unui tabel $\begin{pmatrix} 1 & \ldots & n \\ \sigma(1) & \ldots & \sigma(n) \end{pmatrix}$.

Vom nota prin e_n sau simplu prin e (dacă nu este pericol de confuzie) permutarea identică din S_n.

Tinând cont de Propoziţia 3.11. de la Capitolul 1, deducem că $|S_n| = n!$.

Teorema 10.1.(*Cayley*) Orice grup G este izomorf cu un subgrup al grupului de permutări Σ (G).

Demonstraţie. Pentru $x \in G$ se probează imediat că $\theta_x : G \to \Sigma(G)$, $\theta_x(y) = xy$ pentru orice $y \in G$ este un element din $\Sigma(G)$. Să arătăm acum că $\varphi : G \to \Sigma(G)$, $\varphi(x) = \theta_x$ pentru orice $x \in G$ este un morfism injectiv de

grupuri. Dacă x, $y \in G$ şi $\varphi(x)=\varphi(y)$, atunci $\theta_x=\theta_y$ deci în particular $\theta_x(1)=\theta_y(1) \Leftrightarrow x\cdot 1=y\cdot 1 \Leftrightarrow x=y$, de unde deducem că φ este ca funcţie o injecţie.

De asemenea, $\varphi(x) \circ \varphi(y) = \theta_x \circ \theta_y$ iar dacă $z \in G$ avem $(\theta_x \circ \theta_y)(z) = \theta_x(\theta_y(z)) = x(yz) = (xy)z = \theta_{xy}(z)$, adică $\theta_x \circ \theta_y = \theta_{xy} = \varphi(xy)$, deci $\varphi(x) \circ \varphi(y) = \varphi(xy)$, adică $\varphi \in \mathbf{Hom}(G, \Sigma(G))$. Deducem că $G \approx \varphi(G) \leq \Sigma(G)$.■

Suntem acum în măsură să arătăm că putem renunţa la condiţia de comutativitate a lui G′ din Propoziţia 5.8. (mai precis la demonstrarea implicaţiei (iii)⇒(i)). Să presupunem deci că G , G′ sunt grupuri, f:G→G′ este morfism de grupuri cu proprietatea că pentru orice grup G′′ şi oricare morfisme α, β: G′→G′′ , dacă $\alpha \circ f = \beta \circ f$ atunci α=β şi să arătăm că f este surjecţie. Fie $H=f(G) \leq G'$ şi să presupunem prin absurd că H≠G′. Dacă [G′:H]=2, atunci $H \trianglelefteq G'$, (conform Observaţiei 4.6.) şi alegînd G′′=G′/H , $\alpha = p_H : G' \to G''$ morfismul surjectiv canonic iar β : G′→G′′ morfismul nul, atunci $\alpha \circ f = \beta \circ f$ şi totuşi α≠β-absurd!.

Să presupunem acum că [G′:H]>2 şi fie $T=(G'/H)_d$ mulţimea claselor la dreapta ale lui G′ relative la H iar $G''=\sum(G')$-grupul permutărilor lui G′.

Vom construi şi în acest caz două morfisme de grupuri α, β: G′→G′′ , a.î. α≠β şi totuşi $\alpha \circ f = \beta \circ f$, contrazicând faptul că f este surjecţie.

Alegem $\alpha : G' \to G''=\sum(G')$ ca fiind morfismul lui Cayley (vezi Teorema 10.1.), (adică $\alpha(x)=\theta_x$, cu $\theta_x : G' \to G'$, $\theta_x(y)=xy$, oricare ar fi $x, y \in G'$).

Pentru a construi pe β, fie $\pi : G' \to T$ surjecţia canonică, (adică $\pi(x)=Hx \stackrel{def}{=} \hat{x}$, oricare ar fi $x \in G'$) iar $s : T \to G'$ o secţiune a lui π (deci $\pi \circ s = 1_T$, adică $s(\hat{x}) \in \hat{x}$, oricare ar fi $\hat{x} \in T$; existenţa lui s ne este asigurată de Propoziţia 3.8., (vii) de la Capitolul 1).

Cum $|T|=|G':H|\geq 3$, există o permutare $\sigma : T\to T$ a.î. $\sigma(\hat{e})=\hat{e}$ şi $\sigma\neq 1_T$. Dacă $x\in G$, cum $s(\hat{x})\in\hat{x}\Rightarrow xs(\hat{x})^{-1}\in H$.

Definim $\tau : G'\to H$ prin $\tau(x)=xs(\hat{x})^{-1}$, oricare ar fi $x\in G'$. Atunci $\lambda : G'\to G'$, $\lambda(x)=\tau(x)\cdot s(\sigma(\hat{x}))=xs(\hat{x})^{-1}s(\sigma(\hat{x}))$ oricare ar fi $x\in G'$ este o permutare a lui G' (adică $\lambda\in G''$).

Într-adevăr, dacă $x, y\in G'$ şi $\lambda(x)=\lambda(y)$, atunci

(1) $xs(\hat{x})^{-1}s(\sigma(\hat{x}))=ys(\hat{y})^{-1}s(\sigma(\hat{y}))$.

Cum $xs(\hat{x})^{-1}$, $ys(\hat{y})^{-1}\in H\Rightarrow s(\sigma(\hat{x}))=s(\sigma(\hat{y}))\Rightarrow(\pi\circ s)(\sigma(\hat{x}))=$ $=(\pi\circ s)(\sigma(\hat{y}))\Rightarrow\sigma(\hat{x})=\sigma(\hat{y})\Rightarrow\hat{x}=\hat{y}$ iar din (1) deducem că $x=y$.

Fie acum $y\in G'$; există $\hat{z}\in T$ a.î $\hat{y}=\sigma(\hat{z})$. Cum $s(\hat{y})\in\hat{y}=Hy$, atunci există $h\in H$ a.î. $s(\hat{y})=hy$. Dacă notăm $x_1=s(\hat{z})$ şi $x=h^{-1}x_1$, atunci (cum $\hat{x}=\hat{x}_1$ căci $xx_1^{-1}=h\in H$) avem $\lambda x=xs(\hat{x})^{-1}s(\sigma(\hat{x}))=h^{-1}x_1s(\hat{x}_1)^{-1}s(\sigma(\hat{x}_1))=h^{-1}x_1s(\hat{x}_1)^{-1}s(\sigma(\hat{z}))=$ $=h^{-1}x_1s(\hat{x}_1)^{-1}s(\hat{y})=h^{-1}x_1s(\hat{x}_1)^{-1}hy$. Cum $x_1=s(\hat{z})\in\hat{z}$, $\hat{x}_1=\hat{z}$ şi deci $s(\hat{x}_1)=s(\hat{z})=x_1$, astfel că $\lambda(x)=h^{-1}x_1x_1^{-1}hy=y$, adică λ este şi surjecţie, deci $\lambda\in G''$.

Să definim acum $\beta : G'\to G''=\sum(G')$ prin $\beta(x)=\lambda^{-1}\circ\alpha(x)\circ\lambda$ pentru orice $x\in G'$. În mod evident β este morfism de grupuri. Avem $\alpha\neq\beta$ căci dacă $\alpha=\beta$, atunci $\alpha(x)\circ\lambda=\lambda\circ\alpha(x)$, oricare ar fi $x\in G'\Leftrightarrow$ $(\alpha(x)\circ\lambda)(y)=(\lambda\circ\alpha(x))(y)$, oricare ar fi $y\in G'\Leftrightarrow x\lambda(y)=\lambda(xy)$ oricare ar fi $y\in G'\Leftrightarrow xys(\hat{y})^{-1}s(\sigma(\hat{y}))=xys\left(\hat{xy}\right)^{-1}s\left(\sigma\left(\hat{xy}\right)\right)$, oricare ar fi $y\in G'\Leftrightarrow$

$\Leftrightarrow s(\hat{y})^{-1}s(\sigma(\hat{y}))=s\left(\hat{xy}\right)^{-1}s\left(\sigma\left(\hat{xy}\right)\right)$ oricare ar fi $y\in G'$.

Alegând acum $x=y^{-1}$ obţinem că $s(\hat{y})^{-1}s(\sigma(\hat{y}))=s(\hat{e})^{-1}s(\sigma(\hat{e}))=s(\hat{e})^{-1}s(\hat{e})=e$, de unde $s(\hat{y})=s(\sigma(\hat{y}))$.

Cum s este injectivă deducem că $\hat{y}=\sigma(\hat{y})$ şi cum y este oarecare deducem că $\sigma=1_T$ - absurd!. Deci $\alpha\neq\beta$.

Să arătăm acum că $\alpha\circ f=\beta\circ f$ şi contradicția va fi evidentă urmînd a concluziona că f este surjecție.

Într-adevăr, $\alpha\circ f=\beta\circ f\Leftrightarrow(\alpha\circ f)x=(\beta\circ f)x$, oricare ar fi $x\in G \Leftrightarrow$ $\Leftrightarrow\alpha(f(x))=\beta(f(x))$, oricare ar fi $x\in G \Leftrightarrow \theta_{f(x)}=\lambda^{-1}\circ\alpha(f(x))\circ\lambda$, oricare ar fi $x\in G\Leftrightarrow \lambda\circ\theta_{f(x)}=\theta_{f(x)}\circ\lambda$ oricare ar fi $x\in G\Leftrightarrow$

$\Leftrightarrow (\lambda\circ\theta_{f(x)})(y)=(\theta_{f(x)}\circ\lambda)(y)$, oricare ar fi $x\in G$ şi $y\in G' \Leftrightarrow$

$\Leftrightarrow \lambda(f(x)\,y)=f(x)\,\lambda(y)$, oricare ar fi $x\in G$ şi $y\in G' \Leftrightarrow$

$\Leftrightarrow \tau(f(x)y)s(\sigma(\overset{\wedge}{f(x)y}))=f(x)ys(\hat{y})^{-1}s(\sigma(\hat{y}))$, oricare ar fi $x\in G$ şi

$y\in G' \Leftrightarrow f(x)ys(\overset{\wedge}{f(x)y})^{-1}\ s(\sigma(\overset{\wedge}{f(x)y}))=f(x)ys(\hat{y})^{-1}s(\sigma(\hat{y}))$, oricare

ar fi $x\in G$ şi $y\in G' \Leftrightarrow s(\overset{\wedge}{f(x)y})^{-1}\ s(\sigma(\overset{\wedge}{f(x)y}))=s(\hat{y})^{-1}s(\sigma(\hat{y}))$, oricare ar fi $x\in G$ şi $y\in G'$ ceea ce este evident deoarece pentru $x\in G$,

$f(x)\in f(G)=H$ şi deci $\overset{\wedge}{f(x)y}=\hat{y}$, oricare ar fi $y\in G'$.

În continuare ne vom ocupa de studiul grupului S_n cu $n\geq 2$. Evident, grupul S_2 având 2 elemente este comutativ pe când începând cu $n\geq 3$, S_n nu mai este comutativ.

Definiția 10.2. Numim *ciclu de lungime k* **($2\leq k\leq n$) o permutare $\sigma\in S_n$ pentru care există elementele distincte $i_1,i_2,\ldots,i_k$ din $\{1,2,\ldots,n\}$ a.î. $\sigma(i_1)=i_2$, $\sigma(i_2)=i_3$, …, $\sigma(i_k)=i_1$ iar $\sigma(i)=i$ pentru orice $i\in\{1,2,\ldots,n\}\setminus\{i_1,i_2,\ldots,i_k\}$.** Convenim să notăm un astfel de ciclu σ prin $\sigma=(i_1\ i_2\ \ldots\ i_k)$ sau $\sigma=(i_1,i_2,\ldots,i_k)$ (dacă există pericol de confuzie).

Ciclii de lungime 2 se mai numesc şi *transpoziţii.*

De exemplu, în S_5

$$(1\ 3\ 5)=\begin{pmatrix}1&2&3&4&5\\3&2&5&4&1\end{pmatrix} \text{ iar } (2\ 4)=\begin{pmatrix}1&2&3&4&5\\1&4&3&2&5\end{pmatrix}.$$

Dacă $\sigma = (i_1\ i_2\ \dots\ i_k)$ este un ciclu de lungime k, convenim să numim mulţimea $\{i_1,i_2, \dots, i_k\}$ ca fiind *orbita* lui σ .

Dacă $\tau = (j_1\ j_2\ \dots\ j_t)$ este un alt ciclu de lungime t din S_n , vom spune că σ şi τ sunt *ciclii disjuncţi* dacă $\{i_1, i_2, \dots, i_k\} \cap \{j_1, j_2, \dots, j_t\}=\emptyset$.

Propoziţia 10.3. Dacă σ, τ sunt ciclii disjuncţi din S_n, atunci $\sigma\tau=\tau\sigma$.

Demonstraţie. Dacă $i \in \{1, 2, \dots, n\} \setminus (\{i_1, i_2, \dots, i_k\} \cup \{j_1,j_2, \dots, j_t\})$, atunci $(\sigma\tau)(i) = =(\tau\sigma)(i) =i$. Să presupunem că $i\in\{i_1, i_2, \dots, i_k\}$, să zicem de exemplu că $i=i_1$. Atunci $(\sigma\tau)(i)=\sigma(\tau(i))=\sigma(i)=\sigma(i_1)=i_2$, iar $(\tau\sigma)(i)=\tau(\sigma(i))=\tau(i_2)=i_2$ de unde concluzia că $(\sigma\tau)(i)=(\tau\sigma)(i)$. Analog se arată că $(\sigma\tau)(i)=(\tau\sigma)(i)$ dacă $i\in\{j_1, j_2, \dots, j_t\}$, de unde deducem egalitatea $\sigma\tau = \tau\sigma$.

În esenţă am folosit faptul că dacă $i\notin\{i_1, i_2, \dots, i_k\}$ atunci $\tau(i)=i$ iar dacă $j\notin\{j_1, j_2, \dots, j_t\}$, atunci $\sigma(j)=j$.■

Observaţia 10.4. Deoarece pentru orice $2\le k\le n$ avem $(i_1\ i_2\ \dots\ i_k) = (i_2\ i_3\ \dots\ i_k\ i_1) = \dots = (i_k\ i_1\ \dots\ i_{k-1})$ deducem că în S_n există $\frac{1}{k}\cdot A_n^k$ ciclii distincţi de lungime k.

Propoziţia 10.5. Ordinul oricărui ciclu de lungime k ($2\le k\le n$) este k . Dacă σ,τ sunt 2 ciclii disjuncţi de lungimi k şi respectiv t ($2\le k, t\le n$), atunci $o(\sigma\tau)=[k,t]$. În particular, dacă $(k,t)=1$, atunci $o(\sigma t)=o(\sigma)\cdot o(\tau)$.

Demonstraţie. Trebuie în prima parte să demonstrăm că $\sigma^k(i)=i$ pentru orice $i\in\{1,2, \dots ,n\}$, unde $\sigma=(i_1, i_2, \dots , i_k)$ este un ciclu de lungime k.

Dacă $i\in\{1,2,\dots,n\}\setminus\{i_1,i_2,\dots,i_k\}$, atunci în mod evident $\sigma^k(i)=i$. Dacă $i\in\{i_1,i_2,\dots,i_k\}$, de exemplu $i=i_1$, atunci $\sigma^2(i)=\sigma(\sigma(i))=\sigma(\sigma(i_1))=\sigma(i_2)=i_3$, deci $\sigma^{k-1}(i)=i_k\neq i$ iar $\sigma^k(i)=i$ şi analog pentru orice $i\in\{i_1,i_2,\dots,i_k\}$, $i\neq i_1$, de unde concluzia că $\sigma^k=e$ iar k este cel mai mic număr natural cu această proprietate, adică $o(\sigma)=k$.

Fie $\sigma=(i_1\ i_2\ \dots\ i_k)$, $\tau=(j_1\ j_2\ \dots\ j_t)$ ciclii disjuncţi de lungime k şi respectiv t ($2\le k,\ t\le n$), $\varepsilon=\sigma\tau=\tau\sigma$, $s=[k,t]$ iar $r=o(\varepsilon)$. Va trebui să demonstrăm că r=s.

Deoarece k,t | s deducem că $\varepsilon^s=e$, adică r|s. Cum $\varepsilon^r=e$ deducem că $\sigma^r\tau^r=e$ adică $\sigma^r=\tau^{-r}$. Dacă am avea $\sigma^r\neq e$, atunci există $i\in\{i_1,i_2,\dots,i_k\}$ a.î. $\sigma^r(i)\neq i$. Cum $\sigma^r=\tau^{-r}$ deducem că şi $\tau^r(i)\neq i$, adică $i\in\{j_1,j_2,\dots,j_t\}$ – absurd ! . În concluzie $\sigma^r=\tau^r=e$, de unde deducem k|r şi t|r. Cum s=[k,t] deducem că s|r, adică s=r.■

Corolar 10.6. Dacă $\sigma_1,\dots\sigma_k$ sunt ciclii disjuncţi doi câte doi din S_n de lungimi $t_1,\dots,t_k$, atunci $o(\sigma_1\dots\sigma_k)=[t_1,\dots,t_k]$.

Teorema 10.7. Orice permutare $\sigma\in S_n$, $\sigma\neq e$ se descompune în mod unic în produs de ciclii disjuncţi (exceptând ordinea în care aceştia sunt scrişi) .

Demonstraţie. Fie $t=|\{\ i\in\{1,2,\dots,n\}\mid\sigma(i)\neq i\ \}|$; cum $\sigma\neq e$ deducem că există $i\in\{1,2.,\dots,n\}$ a.î . $\sigma(i)\neq i$ şi astfel şi $\sigma(\sigma(i))\neq\sigma(i)$, de unde concluzia că $t\ge 2$. Vom face acum inducţie matematică după t. Dacă t=2 totul este clar căci în acest caz σ se reduce la o transpoziţie.

Să presupunem acum teorema adevărată pentru toate permutările ce schimbă efectiv mai putin de t indici şi să arătăm că dacă σ este o permutare ce schimbă efectiv t indici atunci σ se descompune în produs de ciclii disjuncţi. Alegem $i_0\in\{1,2,\dots,n\}$ pentru care $\sigma(i_0)\neq i_0$ şi fie $q=o(\sigma)$. Alegând $i_1=\sigma(i_0)$, $i_2=\sigma(i_1)$, … ,$i_{k+1}=\sigma(i_k)$, … se vede că $i_k=\sigma^k(i_0)$ pentru orice $k\ge 1$. Cum $\sigma^q=e$ deducem că $\sigma^q(i_0)=i_0$, deci $i_q=i_0$. Putem alege atunci cel mai mic numar natural m cu proprietatea că $i_m=i_0$. Atunci numerele $i_0,i_1,\dots,i_{m-1}$ sunt distincte între ele.

Într-adevăr, dacă $i_r=i_s$ cu $0\le r,\ s<m$, atunci $\sigma^r(i_0)=\sigma^s(i_0)$. Dacă r>s, notând $p=r-s$ obţinem $\sigma^p(i_0)=i_0$ şi deci $i_p=i_0$ contrazicând alegerea lui m (căci p<m).

Analog dacă r<s. Cu $i_0,i_1, \ldots ,i_{m-1}$ formăm ciclul $\tau=(i_0 i_1 \ldots i_{m-1})$ şi să considerăm permutarea $\sigma'=\tau^{-1}\sigma$. Dacă avem un i a.î. $\sigma(i)=i$, atunci $i \notin \{ i_0,i_1, \ldots , i_{m-1}\}$ şi deci $\tau^{-1}(i)=i$ de unde $\sigma'(i)=i$. Cum $i_1=\sigma(i_0)$, $i_2=\sigma(i_1)$, … , $i_0=\sigma(i_{m-1})$ deducem că pentru orice $i \in \{ i_0,i_1, \ldots ,i_{m-1}\}$ avem $\sigma'(i)=i$.

Rezultă că σ' schimbă efectiv mai puţin de t-m elemente iar cum $m \geq 2$ atunci t-m<t, deci putem aplica ipoteza de inducţie lui σ'. Rezultă atunci că putem scrie $\sigma'=\tau_2 \ldots \tau_s$ cu $\tau_2 \ldots \tau_s$ ciclii disjuncţi. Punând $\tau_1=\tau$ obţinem că $\sigma= \tau_1\tau_2 \ldots \tau_s$ iar τ_1 este disjunct faţă de ceilalţi ciclii. Din modul efectiv de descompunere de mai înainte deducem că scrierea lui σ sub forma $\sigma= \tau_1\tau_2 \ldots \tau_s$ este unic determinată.■

Observaţia 10.8. Dacă $\sigma=(i_1, i_2, \ldots ,i_k)$ este un ciclu de lungime k din S_n ($2 \leq k \leq n$), atunci se probează imediat prin calcul direct că avem următoarele descompuneri ale lui σ în produs de transpoziţii:

$\sigma=(i_1i_2)(i_2i_3)\ldots(i_{k-1}i_k)=(i_1i_k)(i_1i_{k-1}) \ldots (i_1i_2)$.

Din Teorema 10.7 şi Observaţia 10.8 deducem imediat următorul rezultat:

Corolar 10.9. Orice permutare $\sigma \in S_n$ ($n \geq 2$) este un produs de transpoziţii (să observăm că dacă $\sigma=e$, atunci $\sigma=(12)(12)$).

Definiţia 10.10. Fie $\sigma \in S_n$. *Signatura lui* σ **este numărul** $\operatorname{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$ **; evident,** $\operatorname{sgn}(\sigma) \in \{\pm 1\}$ **.**

O *inversiune* **a lui σ este o pereche (ij) cu $1 \leq i < j \leq n$ a.î. $\sigma(i)>\sigma(j)$. Dacă r este numărului de inversiuni ale lui σ, atunci evident $\operatorname{sgn}(\sigma) = (-1)^r$. Dacă r este par spunem că σ este** *permutare pară* **iar dacă r este impar spunem că σ este** *permutare impară* **.**

Vom nota prin A_n mulţimea permutărilor pare.

Astfel, $\sigma \in S_n$ este pară $\Leftrightarrow \operatorname{sgn}(\sigma)=1$ şi impară $\Leftrightarrow \operatorname{sgn}(\sigma)=-1$.

Propoziţia 10.11. Dacă $\sigma,\tau \in S_n$, atunci $\operatorname{sgn}(\sigma \circ \tau)=\operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$.

Demonstrație. Avem $\operatorname{sgn}(\sigma \circ \tau) = \prod_{1 \le i < j \le n} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{i - j}$

$$= \prod_{1 \le i < j \le n} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \cdot \frac{\tau(i) - \tau(j)}{i - j} =$$

$$= \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j} \cdot \prod_{1 \le i < j \le n} \frac{\tau(i) - \tau(j)}{i - j} = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau) \quad \blacksquare$$

Corolar 10.12. Pentru orice n≥2, $A_n \trianglelefteq S_n$ iar $|A_n| = \frac{n!}{2}$.

Demonstrație. Din Propoziția 10.11. deducem că funcția sgn : $S_n \to \{\pm 1\}$ este un morfism surjectiv de la grupul $(S_n, \circ)$ la grupul multiplicativ $(\{\pm 1\}, \cdot)$.
Deoarece Ker(sgn) = $\{\sigma \in S_n \mid \operatorname{sgn}(\sigma)=1\} = A_n$ deducem imediat că $A_n \trianglelefteq S_n$. Conform Corolarului 7.2. de la teorema fundamentală de izomorfism pentru grupuri deducem că $S_n/A_n \approx \{\pm 1\}$, de unde concluzia că $|S_n/A_n| = 2 \Leftrightarrow |S_n| : |A_n| = 2 \Leftrightarrow |A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.■

Observația 10.13. Orice transpoziție (rs) cu 1≤r≤n este o permutare impară . Într-adevăr, inversiunile sale sunt de forma (r,i) cu r<i<s sau (i,s) cu r<i<s astfel că numărul lor este egal cu 2(s-r)-1. Astfel dacă $\sigma \in S_n$ şi scriem pe σ ca un produs de transpoziții $\sigma = t_1 t_2 \ldots t_m$, atunci $\operatorname{sgn}(\sigma) = \operatorname{sgn}(t_1) \operatorname{sgn}(t_2) \ldots \operatorname{sgn}(t_m) = (-1)^m$ şi deci σ va fi permutare pară sau impară după cum m este par sau impar.

În particular, dacă $\sigma = (i_1\ i_2\ \ldots.\ i_k)$ cum $\sigma = (i_1 i_2)(i_2 i_3)\ldots(i_{k-1} i_k)$ deducem că $\operatorname{sgn}(\sigma) = (-1)^{k-1}$.

Teorema 10.14. Două permutări $\alpha, \beta \in S_n$ sunt conjugate în S_n dacă şi numai dacă ele au aceeaşi structură ciclică.

Demonstraţie. „$\Rightarrow$” . Dacă α, β sunt conjugate în S_n, atunci există $\gamma \in S_n$ a.î. $\beta=\gamma\alpha\gamma^{-1}$. Însă $\gamma\alpha\gamma^{-1}$ are aceeaşi structură ciclică cu α (căci dacă α= … (i_1 i_2 … i_k) … , atunci $\gamma\alpha\gamma^{-1}$= …($\gamma(i_1)$ $\gamma(i_2)$ …. $\gamma(i_k)$)… de unde concluzia că α şi β au aceeaşi structură ciclică.

Faptul că $\gamma\alpha\gamma^{-1}$ acţionează asupra lui α de maniera descrisă mai sus se probează astfel : se descompune α în ciclii disjuncţi $\alpha = c_1c_2 \dots c_t$ şi se observă că $\gamma\alpha\gamma^{-1}=(\gamma c_1\gamma^{-1})\ (\gamma c_2\gamma^{-1})\ \dots\ (\gamma c_t\gamma^{-1})$ iar dacă de exemplu $c_1=(i_1i_2 \dots i_k)$, atunci $\gamma c_1\gamma^{-1}=[\gamma(i_1i_2)\gamma^{-1}]\ [\gamma(i_2i_3)\gamma^{-1}] \dots [\gamma(i_{k-1}i_k)\gamma^{-1}]$, totul reducându-se astfel la a proba de exemplu că $\gamma(i_1i_2)\gamma^{-1}=(\gamma(i_1)\gamma(i_2)) \Leftrightarrow$ $\Leftrightarrow \gamma\circ(i_1i_2)=(\gamma(i_1)\gamma(i_2))\circ\gamma$.

Dacă $i\in\{1,2, \dots,n\} \setminus \{i_1,i_2\}$ atunci $\gamma(i)\neq\gamma(i_1),\gamma(i_2)$ şi $(\gamma\circ(i_1,i_2))(i)=\gamma((i_1,i_2)(i))=\gamma(i)$ iar $((\gamma(i_1)\gamma(i_2))\circ\gamma)(i) =(\gamma(i_1)\gamma(i_2))(\gamma(i))= \gamma(i)$ iar dacă de exemplu $i=i_1$ atunci $(\gamma\circ(i_1i_2))(i_1)= \gamma((i_1i_2)(i_1))=\gamma(i_2)$ iar $((\gamma(i_1)\gamma(i_2))\circ\gamma)(i_1)=(\gamma(i_1)\gamma(i_2))(\gamma(i_1))= \gamma(i_2)$, de unde egalitatea dorită.

„$\Leftarrow$”. Să presupunem acum că α şi β au aceeaşi structură ciclică şi să construim γ a.î. $\beta=\gamma\alpha\gamma^{-1}$.

Vom face lucrul acesta pe un exemplu concret (la general raţionîndu-se analog) . Să presupunem că suntem în S_5 şi avem α = (1 5) (4 2 3) şi β = (3 4)(2 1 5) . Ţinând cont de felul în care acţionează $\gamma\alpha\gamma^{-1}$ asupra lui α deducem că: $\gamma = \begin{pmatrix} 1\,5\,4\,2\,3 \\ 3\ 4\,2\,1\,5 \end{pmatrix} = (1\,3\,5\,4\,2)$. ■

Ţinând cont de Observaţia 10.4 şi de Teorema 10.14 , putem determina cu uşurinţă numărul permutărilor α din S_n de o structură ciclică dată.

De exemplu numărul de permutări din S_4 de forma (1 2)(3 4) este $\frac{1}{2}\left(\frac{4\times3}{2}\times\frac{2\times1}{2}\right)=3$ (factorul $\frac{1}{2}$ apărând datorită egalităţii (a b)(c d)=(c d)(a b) pentru {a,b,c,d}={1,2,3,4}) .Găsim astfel pentru S_4 următorul tabel de structură:

Structura ciclică	Numărul lor	Ordinul	Paritatea
(1)	1	1	pară
(12)	$\frac{4\times 3}{2}=6$	2	impare
(123)	$\frac{4\times 3\times 2}{3}=8$	3	pare
(1234)	$\frac{4!}{4}=6$	4	impare
(12)(34)	$\frac{1}{2}\left(\frac{4\times 3}{2}\times\frac{2\times 1}{2}\right)=3$	2	pare

Se observă că 1+6+8+6+3=24=4!.

Putem acum prezenta un rezultat care ne arată că reciproca teoremei lui Lagrange pentru grupuri finite este falsă.

Teorema 10.15 Grupul A_4 (care are ordinul 12) nu conține subgrupuri de ordin 6.

Demonstrație. Din tabelul de structură pentru S_4 deducem că A_4 constă din 8 ciclii de lungime 3, trei produse de transpoziții disjuncte şi permutarea identică. Aceste elemente sunt : (1 2 3), (1 3 2), (2 3 4), (2 4 3), (3 4 1), (3 1 4), (4 1 2), (4 2 1), (1 4)(2 3), (1 2)(3 4), (1 3)(2 4)

mod evident, $C_{S_4}(\alpha)=\{e, \alpha, \alpha^{-1}\}$ şi cum $e, \alpha, \alpha^{-1}\in A_4$ deducem că $|C_{A_4}(\alpha)| = 3$ deci $|A_4 : C_{A_4}(\alpha)| = \frac{12}{3} = 4$. Deducem că α va avea 4 conjugaţi în A_4 şi cum $H\trianglelefteq A_4$, cei patru conjugaţi ai lui α sunt în H. Tot din tabelul de structură al lui S_4 şi A_4 deducem că H trebuie să conţină un element β de ordin 2 (căci dacă ar mai conţine un ciclu de lungime 3 atunci ar mai conţine încă 4 conjugaţi ai acestuia depăşind numărul de 6 elemente ce am presupus a fi în H).

Deoarece β este pară avem β=(a b)(c d) astfel că până acum am descoperit 6 elemente din H: 4 ciclii de lungime 3, e şi β. Deoarece $H\trianglelefteq A_4$ alegând $\gamma=(a\ c\ b)\in A_4$, ar trebui ca şi $\gamma\beta\gamma^{-1}=(c\ a)(b\ d)\in H$ şi cum $\gamma\beta\gamma^{-1}\neq\beta$ am deduce că H conţine cel puţin 7 elemente – absurd!.

Deci A_4 nu conţine subgrupuri de ordin 6.■

§11. Teoremele lui Sylow. Aplicaţii : caracterizarea grupurilor cu pq elemente (p şi q numere prime distincte) şi 12 elemente

În cadrul acestui paragraf prin G vom desemna un grup finit. Conform teoremei lui Lagrange ordinul oricărui subgrup al lui G divide ordinul lui G. După cum am demonstrat în §10 (Teorema 10.15) reciproca teoremei lui Lagrange este falsă (în sensul că există grupuri finite cu proprietatea că pentru un anumit divizor al grupului respectiv grupul nu are subgrupuri de ordin egal cu acel divizor). Există în teoria grupurilor anumite rezultate pe care le vom prezenta în continuare (datorate matematicianului L. Sylow (1832-1918)) şi care permit să se stabilească existenţa subgrupurilor de ordin p^n ale lui G (cu p prim şi $n\in\mathbb{N}^*$) şi care dau informaţii importante despre aceste subgrupuri. Astfel, teoremele lui Sylow sunt de importanţă fundamentală în teoria grupurilor finite. Deoarece prezenta monografie nu este un tratat de teoria grupurilor vom prezenta doar enunţurile acestor teoreme, cititorul dornic de a vedea cum se demonstrează acestea putând consulta de exemplu lucrările [20], [21] sau [22] (după ce în prealabil s-a pus la punct cu anumite chestiuni legate de acţiuni ale grupurilor pe mulţimi).

Definiţia 11.1. Fie p un număr prim şi să presupunem că $|G| = p^m r$ cu $m\in\mathbb{N}$, $r\in\mathbb{N}^*$ şi (p,r)=1. Numim *p- subgrup Sylow* al lui G orice subgrup al lui G de ordin p^m. Pentru $H\leq G$ vom nota

$N_G(H)=\{g\in G \mid gH=Hg\}$. În mod evident avem $H\trianglelefteq N_G(H)\leq G$ şi pentru orice subgrup $K\leq G$ a.î. $H\trianglelefteq K$ avem $K\leq N_G(H)$, deci $N_G(H)$ este cel mai mare subgrup al lui G (față de incluziune) ce conține H ca subgrup normal) . În particular, $H\trianglelefteq G \Leftrightarrow N_G(H)=G$.

Subgrupul $N_G(H)$ poartă numele de *normalizatorul* lui H în G .

Iată acum enunțul teoremelor lui Sylow:

Teorema 11.2. (*Prima teoremă a lui Sylow*) Pentru orice grup finit G şi orice număr prim p există un p-subgrup Sylow al lui G.

Teorema 11.3. (*A doua teoremă a lui Sylow*) Fie G un grup finit şi p un număr prim . Dacă H este un p-subgrup Sylow al lui G iar K este un p-subgrup al lui G, atunci există $g\in G$ a.î. $K \leq g^{-1}Hg$. În particular, dacă K este p-subgrup Sylow al lui G, atunci $K=g^{-1}Hg$.

Teorema 11.4. (*A treia teoremă a lui Sylow*) Dacă notăm prin n_p numărul p-subgrupurilor Sylow distincte ale lui G, atunci $n_p = |G:N_G(H)|$ (unde H este un p-subgrup Sylow particular al lui G), n_p divide $|G:H|$ iar $n_p\equiv 1(\text{mod } p)$.

În continuare vom prezenta câteva aplicații ale acestor teoreme urmând ca în finalul paragrafului să prezentăm un tabel cu caracterizarea grupurilor finite cu cel mult 15 elemente.

Teorema 11.5. Fie p şi q numere prime distincte, p>q şi să presupunem că $|G| = pq$.

(i) Dacă $q \nmid p-1$ atunci G este ciclic

(ii) Dacă $q \mid p-1$ atunci G este generat de două elemente a şi b satisfăcând condițiile $a^q=b^p=1$, $a^{-1}ba=b^r$ cu $r\not\equiv 1 \pmod p$ însă $r^q\equiv 1 \pmod p$.

Demonstrație. (i). Conform teoremei lui Cauchy pentru grupuri finite, G conține un element b de ordin p; fie $H=\langle b\rangle$. Cum H este un p-subgrup Sylow, atunci conform celei de a treia teoreme a lui Sylow numărul conjugaților lui H (adică a subgrupurilor de forma gHg^{-1} cu

$g \in G$) este de forma 1+up cu $u \in \mathbb{N}$. Însă 1+up=$|G:N_G(H)|$ şi trebuie să dividă |G|=pq. Cum (1+up, p)=1 atunci 1+up | q iar cum q<p deducem că u=0, deci $H \trianglelefteq G$.

De asemenea, există un element $a \in G$ al cărui ordin este q; fie K = <a>. Ca şi mai înainte K este q-subgrup Sylow al lui G astfel că | G : $N_G(H)$ |=1+kq cu $k \in \mathbb{N}$. Cum 1+kq | p iar prin ipoteză q $\nmid$ p-1 deducem că k=0.

Astel $K \trianglelefteq G$, deci $G \approx H \times K \approx \mathbb{Z}_p \times \mathbb{Z}_q \approx \mathbb{Z}_{pq}$, deci G este ciclic în acest caz.

(ii). Să presupunem că q | p-1 . Atunci K nu mai este subgrup normal în G. Cum $S \trianglelefteq G$, $a^{-1}ba=b^r$ cu $r \in \mathbb{N}$.

Putem presupune $r \not\equiv 1 \pmod p$ (căci în caz contrar ne reântoarcem la cazul comutativ). Prin inducţie se arată uşor că $a^{-j}ba^j = b^{r^j}$. În particular pentru j=q avem $b = b^{r^q}$, adică $r^q \equiv 1 \pmod p$.■

Corolar 11.6. Orice grup cu 15 elemente este ciclic (deci izomorf cu ($\mathbb{Z}_{15}$, +)).

Demonstraţie. Totul rezultă din Teorema 11.4. pentru p=5 şi q=3 observând că q=3 $\nmid$ p-1 = 4.■

Definiţia 11.7. Un grup de ordin 8 având doi generatori a şi b ce satisfac relaţiile $a^4=1$, $b^2=a^2$ şi $b^{-1}ab=a^{-1}$ se notează prin Q şi poartă numele de *grupul quaternionilor.*

Teorema 11.8. Grupurile Q şi D_4 sunt singurele grupuri necomutative de ordin 8.

Demonstraţie. Dacă G este un grup necomutativ cu 8 elemente atunci G nu conţine elemente de ordin 8 şi nu toate elementele sale au ordinul 2, de unde concluzia că G conţine un element a de ordin 4.

Alegem $b \in G$ a.î. $b \notin <a>$. Cum |G : <a>| = 2 deducem că $<a> \trianglelefteq G$ şi $G/<a> \approx \mathbb{Z}_2$, de unde cu necesitate $b^2 \in <a>$. Dacă $b^2=a$ sau $b^2=a^3$ atunci o(b)=8 - contradicţie, deci avem doar cazurile $b^2 = a^2$ sau

$b^2 = 1$. Cum $\langle a\rangle \trianglelefteq G$ deducem ca $b^{-1}ab \in \langle a\rangle$ iar cum $o(a^2)=2$ avem doar posibilitățile $b^{-1}ab=a$ sau $b^{-1}ab=a^3$.

Cazul $b^{-1}ab=a$ îl excludem căci el implică ab=ba, adică G este comutativ astfel că avem doar situațiile :

(i) $a^4 = 1$, $b^2 = a^2$ şi $b^{-1}ab=a^3 =a^{-1}$ sau

(ii) $a^4 = 1$, $b^2 = 1$ şi $b^{-1}ab=a^3 =a^{-1}$.

În cazul (i) avem descrierea lui Q (deci $G\approx Q$) iar în cazul (ii) avem descrierea lui D_4 deci ($G\approx D_4$).■

În continuare vom caracteriza grupurile finite cu 12 elemente, iar pentru aceasta avem nevoie să introducem un nou tip de grup finit.

Definiția 11.9. Dacă $n\in\mathbb{N}$, $n \geq 2$ prin *grup diciclic de ordin 4n* **(notat DI_n) înțelegem un grup cu 4n elemente :**

$$\mathbf{DI_n=\{1, x, \ldots, x^{2n-1}, y, xy, \ldots, x^{2n-1}y\}}$$

ale cărui elemente le multiplicăm astfel:

$$\mathbf{x^a x^b = x^{a+b}}$$
$$\mathbf{x^a(x^b y) = x^{a+b}y}$$
$$\mathbf{(x^a y)\, x^b = x^{a-b}y}$$
$$\mathbf{(x^a y)\,(x^b y) = x^{a-b+n}}$$

unde $0\leq a, b\leq 2n-1$ iar puterile lui x sunt considerate modulo 2n.

Se observă că pentru n=2, $DI_2 = Q$ (grupul quaternionilor).

Suntem acum în măsură să prezentăm teorema de structură a grupurilor finite cu 12 elemente:

Teorema 11.10. Fie G un grup finit cu 12 elemente.

(i) Dacă G este comutativ, atunci G este izomorf cu $\mathbb{Z}_{12}$ sau $\mathbb{Z}_6 \times \mathbb{Z}_2$

(ii) Dacă G este necomutativ atunci G este izomorf cu D_3, DI_3 sau A_4.

Demonstrație. (i). Rezultă din teorema de structură a grupurilor abeliene finit generate (vezi Observația 8.14).

(ii). Fie t numărul subgrupurilor Sylow distincte ale lui G cu 3 elemente. Conform teoremelor lui Sylow $t\equiv 1 \pmod 3$ şi $t|4$.

Astfel , G are fie un singur subgrup de ordin 3 (care trebuie să fie subgrup normal) fie 4 subgrupuri (conjugate). Tot conform teoremelor lui Sylow deducem că G trebuie să aibă unul sau 3 subgrupuri de ordin 4.

Cazul 1. Presupunem că G conține un singur subgrup (normal) H de ordin 3 generat de x.

Dacă K este un subgrup al lui G de ordin 4 atunci K este ciclic ($K\approx\mathbb{Z}_4$) sau K este izomorf cu grupul lui Klein ($K\approx\mathbb{Z}_2\times\mathbb{Z}_2$).

(a) Să analizăm cazul când K este ciclic, K=<y>.

Cum $H\cap K=\{1\}$, atunci clasele H, Hy, Hy^2, Hy^3 sunt toate distincte şi HK=G.

Cum $H\trianglelefteq G$ deducem că $yxy^{-1}\in H$.

(1) Dacă $yxy^{-1}=x$, atunci xy=yx, deci G este comutativ şi avem

$$G\approx H\times K\approx\mathbb{Z}_3\times\mathbb{Z}_4\approx\mathbb{Z}_{12}.$$

(2) Dacă $yxy^{-1}=x^2$, atunci $yx=x^2y$, de unde $y^2x=yx^2y=x^2yxy=x^4y^2=xy^2$.

Astfel, $xy^2=y^2x$ şi dacă considerăm $z=xy^2$ avem că o(z)=6.

De asemenea $z^3=x^3y^6=y^2$ şi $yz=yxy^2=y^3x=y^2x^2y=z^{-1}y$.

Cum o(y)=4, $y\notin$ <z> şi deci clasele <z> , <z>y dau o partiție a lui G.

Multiplicând în acest caz elementele lui G ca în cazul grupului diciclic şi anume $z^az^b=z^{a+b}$, $z^a(z^by)=z^{a+b}y$, $(z^ay)z^b=z^{a-b}y$, $(z^ay)(z^by)=$ $=z^{a-b}y^2=z^{a-b+3}$ (unde puterile lui z se reduc modulo 6) obținem în acest caz că $G\approx DI_3$.

(b) Să presupunem că K este grupul lui Klein (deci $K\approx\mathbb{Z}_2\times\mathbb{Z}_2$) şi să notăm elementele sale cu 1,u,v,w unde w=uv şi $u^2=v^2=1$. Atunci $H\cap K=\{1\}$ iar clasele H, Hu, Hv, Hw partiționează pe G, de unde HK=G. Cum $H\trianglelefteq G$ avem $uxu^{-1}=x^a$, $vxv^{-1}=x^b$, $wxw^{-1}=x^{ab}$ unde a, b, $ab\in\{\pm 1\}$.

(3) Dacă a=b=ab=1, cum G este abelian,

$$G\approx H\times K\approx\mathbb{Z}_3\times\mathbb{Z}_2\times\mathbb{Z}_2\approx\mathbb{Z}_6\times\mathbb{Z}_2.$$

(4) Să considerăm cazul când două dintre a, b, ab sunt egale cu –1 iar al treilea egal cu 1.

Renumerotând u, v, w (dacă este necesar) putem presupune că a = 1 şi b = -1. Atunci ux=xu iar z=ux are ordinul 6. Astfel, G=<z,v> iar $z^6=1, v^2=1$ iar $vz=z^{-1}v \Leftrightarrow vzv=z^{-1}$ de unde concluzia că în acest caz $G\approx D_6$.

*Cazul 2.*Să presupunem că G conține 4 subgrupuri (conjugate) de ordin 3.

Elementele nenule (diferite de 1) ale celor 4 subgrupuri de ordin 3 ne dau 8 elemente diferite de 1 ale lui G restul de 4 urmând a forma singurul subgrup K de ordin 4 al lui G.

(c) Să arătăm că grupul K nu poate fi ciclic.

Presupunem prin absurd că totuşi K este ciclic, K=<y> şi fie $x\in G\setminus K$. Atunci o(x)=3 iar clasele K, Kx şi Kx^2 dau o partiție a lui G. Cum $K\trianglelefteq G$ avem că $xyx^{-1}\in K$. Dacă $xyx^{-1}=y$, atunci ar rezulta că G este comutativ (în contradicție cu faptul că G conține 4 subgrupuri conjugate distincte de ordin 3).

De asemenea $xyx^{-1}\neq y^2$ (căci y şi y^2 au ordine diferite).

În sfârşit, dacă am avea $xyx^{-1}=y^3$, atunci $y=x^3yx^{-3}=y^{27}=y^3$ – absurd, de unde concluzia că grupul K nu este ciclic.

(d) Atunci K trebuie să fie grupul lui Klein. Considerând ca mai sus K={1, u, v, w}, fie $x\in G$ a.î. o(x)=3. Atunci clasele K, Kx, Kx^2 sunt toate distincte astfel că G=<u, v, x>. Conjugarea prin x permută cele 3 elemente u, v, w între ele (căci $K\trianglelefteq G$) iar permutarea este sau identică sau un 3-ciclu (deoarece $x^3=1$).

(5) Nu putem avea permutarea identică căci în acest caz G ar deveni comutativ (caz studiat deja).

(6) Renumerotând eventual, putem presupune că $xux^{-1}=v$, $xvx^{-1}=w$, $xwx^{-1}=u$ şi atunci considerând asocierile $u\leftrightarrow(12)(34)$, $v\leftrightarrow(13)(24)$, $x\leftrightarrow(234)$ obținem un izomorfism între G şi A_4.

În concluzie avem 5 tipuri de grupuri cu 12 elemente, 2 comutative ($\mathbb{Z}_{12}$, $\mathbb{Z}_6\times\mathbb{Z}_2$) şi 3 necomutative ($D_6$, DI_3 şi A_4).■

Suntem acum în măsură să prezentăm tabelul de caracterizare a grupurilor cu cel mult 15 elemente:

Nr. elem	Nr. tipuri	Reprezentanți	Rezultatul care dă caracterizarea
2	1	$\mathbb{Z}_2$	Propoziția 6.16.
3	1	$\mathbb{Z}_3$	Propoziția 6.16.
4	2	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$	Observația 8.15
5	1	$\mathbb{Z}_5$	Propoziția 6.16.
6	2	$\mathbb{Z}_6$, D_3	Teorema 9.12.
7	1	$\mathbb{Z}_7$	Propoziția 6.16.
8	5	3 tipuri comutative : $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ 2 tipuri necomutative: Q , D_4	Observația 8.14. , Teorema 11.8.
9	2	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$	Observația 8.14.
10	2	$\mathbb{Z}_{10}$, $\mathbf{D_5}$	Teorema 9.12.
11	1	$\mathbb{Z}_{11}$	Propoziția 6.16.
12	5	2 comutative: $\mathbb{Z}_{12}$,$\mathbb{Z}_4 \times \mathbb{Z}_3$ 3 necomutative : D_6, DI_3, A_4	Observația 8.14. , Teorema 11.10.
13	1	$\mathbb{Z}_{13}$	Propoziția 6.16.
14	2	$\mathbb{Z}_{14}$, D_7	Terorema 9.12.
15	1	$\mathbb{Z}_{15}$	Corolar 11.6.

CAPITOLUL 3 : INELE ŞI CORPURI

§1. Inel. Exemple. Reguli de calcul într-un inel. Divizori ai lui zero. Domenii de integritate. Caracteristica unui inel

Definiția 1.1. O mulțime nevidă A, împreună cu două operații algebrice notate tradițional prin „+" şi „· " se zice *inel* dacă:

(i) (A,+) este grup comutativ

(ii (A,·) este semigrup

(iii) Înmulțirea este distributivă la stânga şi la dreapta față de adunare, adică pentru oricare x, y, z $\in$A avem:

x(y+z)=xy+xz şi (x+y)z=xz+yz.

În cele ce urmează (dacă nu este pericol de confuzie) când vom vorbi despre un inel A vom pune în evidență doar mulțimea A (operațiile de adunare şi înmulțire subânțelegându-se).

Astfel, prin 0 vom nota elementul neutru al operației de adunare iar pentru a$\in$A, prin – a vom desemna opusul lui a.

Dacă operația de înmulțire de pe A are element neutru (pe care îl vom nota prin 1) vom spune despre inelul A că este *unitar.*

Dacă A este un inel unitar şi 0=1 vom spune despre A că este *inelul nul*; în caz contrar vom spune că A este *inel nenul*.

Dacă înmulțirea de pe A este comutativă, vom spune despre inelul A că este comutativ. Convenim să notăm A^*=A\{0}.

Exemple. 1. Din cele stabilite în §6 de la Capitolul 2 deducem că ($\mathbb{Z}$,+,·) este inel comutativ unitar.

2. Dacă vom considera A=2$\mathbb{Z}$={2n : n$\in\mathbb{Z}$} atunci (A,+,·) este exemplu de inel comutativ neunitar (căci 1$\notin$2$\mathbb{Z}$).

3. Dacă n$\in\mathbb{N}$, n$\geq$2 atunci ($\mathbb{Z}_n$, +, ·) este exemplu de inel unitar comutativ finit cu n elemente (vezi §6 de la Capitolul 2).

4. Fie A un inel şi m, n$\in\mathbb{N}^*$. Un tablou de forma

$$\alpha = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \dots & \dots & \dots \\ \alpha_{m1} & \dots & \alpha_{mn} \end{pmatrix}$$

cu m limii şi n coloane, format din elemente ale lui A se zice *matrice cu m linii şi n coloane*; convenim să notăm o astfel de matrice şi sub formă mai condensată $\alpha = (\alpha_{ij})_{\substack{1\le i\le m \\ 1\le j\le n}}$.

Dacă m=n notăm $M_{m,n}(A)=M_n(A)$; o matrice din $M_n(A)$ se zice *pătratică de ordin n*.

Pentru $\alpha, \beta \in M_{m,n}(A)$, $\alpha=(\alpha_{ij})_{\substack{1\le i\le m \\ 1\le j\le n}}$ şi $\beta=(\beta_{ij})_{\substack{1\le i\le m \\ 1\le j\le n}}$ definim:

$$\alpha+\beta=(\alpha_{ij}+\beta_{ij})_{\substack{1\le i\le m \\ 1\le j\le n}}.$$

Asociativitatea adunării matricelor este imediată, elementul neutru este matricea $O_{m,n}$ din $M_{m,n}(A)$ ce are toate elementele egale cu 0, iar opusa matricei α este matricea $-\alpha=(-\alpha_{ij})_{\substack{1\le i\le m \\ 1\le j\le n}}$, de unde concluzia că $(M_{m,n}(A), +)$ este grup (abelian).

Pentru m, n, $p\in\mathbb{N}^*$, $\alpha\in M_{m,n}(A)$, $\beta\in M_{n,p}(A)$, $\alpha=(\alpha_{ij})_{\substack{1\le i\le m \\ 1\le j\le n}}$, $\beta=(\beta_{jk})_{\substack{1\le j\le n \\ 1\le k\le p}}$ definim $\alpha\beta=(\gamma_{ik})_{\substack{1\le i\le m \\ 1\le k\le p}}$, unde $\gamma_{ik}=\sum_{j=1}^{n}\alpha_{ij}\beta_{jk}$ pentru $1\le i\le m$ şi $1\le k\le p$.

În mod evident, $\alpha\beta\in M_{m,p}(A)$.

Să demonstrăm că dacă m, n, p, $q\in\mathbb{N}^*$ şi $\alpha\in M_{m,n}(A)$, $\beta\in M_{n,p}(A)$, $\gamma\in M_{p,q}(A)$, atunci $(\alpha\beta)\gamma=\alpha(\beta\gamma)$. Într-adevăr, fie $\alpha\beta=(\delta_{ik})_{\substack{1\le i\le m \\ 1\le k\le p}}$, cu $\delta_{ik}=\sum_{j=1}^{n}\alpha_{ij}\beta_{jk}$ şi $(\alpha\beta)\gamma=(\varepsilon_{it})_{\substack{1\le i\le m \\ 1\le t\le q}}$ cu $\varepsilon_{it}=\sum_{k=1}^{p}\delta_{ik}\gamma_{kt}$ $=\sum_{k=1}^{p}\left(\sum_{j=1}^{n}\alpha_{ij}\beta_{jk}\right)\gamma_{kt}=\sum_{k=1}^{p}\sum_{j=1}^{n}\alpha_{ij}\beta_{jk}\gamma_{kt}$.

Dacă $\beta\gamma=(\delta'_{jt})_{\substack{1\le j\le n \\ 1\le t\le q}}$ cu $\delta'_{jt}=\sum_{k=1}^{p}\beta_{jk}\gamma_{kt}$ iar $\alpha(\beta\gamma)=(\varepsilon'_{it})_{\substack{1\le i\le m \\ 1\le t\le q}}$, atunci $\varepsilon'_{it}=\sum_{j=1}^{n}\alpha_{ij}\delta'_{jt}=\sum_{j=1}^{n}\alpha_{ij}\sum_{k=1}^{p}\beta_{jk}\gamma_{kt}=\sum_{j=1}^{n}\sum_{k=1}^{p}\alpha_{ij}\beta_{jk}\gamma_{kt}$, de unde egalitatea $(\alpha\beta)\gamma=\alpha(\beta\gamma)$.

Ținând cont de distributivitatea înmulțirii de pe A față de adunare, deducem imediat că dacă $\alpha \in M_{m,n}(A)$ şi $\beta,\gamma \in M_{n,p}(A)$ atunci $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$ iar dacă α, $\beta \in M_{m,n}(A)$ şi $\gamma \in M_{n,p}(A)$ atunci $(\alpha+\beta)\gamma=\alpha\gamma+\beta\gamma$.

Sumând cele de mai sus, deducem că dacă $n \in \mathbb{N}$, $n \geq 2$, atunci $(M_n(A),+,\cdot)$ este un inel (numit *inelul matricelor pătratice de ordin n cu elemente din A*).

Dacă inelul A este unitar, atunci şi inelul $(M_n(A),+,\cdot)$ este unitar, elementul neutru fiind matricea I_n ce are pe diagonala principală 1 şi în rest 0.

Să remarcăm faptul că în general, chiar dacă A este comutativ, $M_n(A)$ nu este comutativ.

Observația 1.2. 1. Dacă A este inel unitar, rezultă că adunarea de pe A este comutativă.

Într-adevăr, calculând pentru a, $b \in A$, (a+b)(1+1) în două moduri (ținând cont de distributivitatea la stânga şi la dreapta a înmulțirii față de adunare) obținem egalitatea a + a + b + b =a + b + a + +b, de unde a+b=b+a.

2. Notarea generică cu litera A a unui inel oarecare se explică prin aceea că în limba franceză noțiunea matematică corespunzătoare se traduce prin *anneaux*.

În anumite cărți un inel oarecare se notează prin R (de la faptul că în limba engleză noțiunea matematică de inel se traduce prin *ring*).

Propoziția 1.3. Dacă A este un inel, atunci:

(i) $a \cdot 0 = 0 \cdot a = 0$, **pentru orice** $a \in A$

(ii) $a(-b)=(-a)b=-(ab)$ **şi** $(-a)(-b)=ab$, **pentru orice** $a, b \in A$

(iii) $a(b-c)=ab-ac$ **şi** $(a-b)c=ac-bc$, **pentru orice** $a, b, c \in A$

(iv) $a(b_1+\ldots+b_n)=ab_1+\ldots+ab_n$ **şi** $(a_1+\ldots+a_n)b=a_1b+\ldots+a_nb$, **pentru orice** $a, b, a_i, b_i \in A$, $1 \leq i \leq n$

(v) Dacă $a, b \in A$, $n \in \mathbb{N}^*$ **şi** $ab=ba$ **avem egalitățile:**

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1})$$

$$a^{2n+1} + b^{2n+1} = (a+b)(a^{2n} - a^{2n-1}b + \ldots - ab^{2n-1} + b^{2n}).$$

Demonstrație. (i). Totul rezultă din 0+0=0.

(ii). Totul rezultă din (i) şi din aceea că b+(-b)=0.

(iii). Rezultă din (ii).

(iv). Se face inducţie matematică după n.

(v). Se fac calculele în membrul drept.■

Observaţia 1.4. Definind pentru a∈A şi n∈$\mathbb{Z}$

$$\mathbf{na} = \begin{cases} \underbrace{a+\ldots+a}_{n\ ori} & \textbf{dacă } n>0 \\ \mathbf{0} & \textbf{dacă } n=0 \\ \underbrace{(-a)+\ldots+(-a)}_{-n\ ori} & \textbf{dacă } n<0, \end{cases}$$

atunci (vi). a(nb)=(na)b=n(ab) pentru orice a, b∈A şi n∈$\mathbb{Z}$

(vii). Dacă A este un inel unitar, a, b∈A, ab=ba şi n∈$\mathbb{N}^*$, avem egalitatea $(a+b)^n=\sum_{k=0}^{n} C_n^k a^{n-k}b^k$ **(prin definiţie a^0=1).**

Egalitatea de la (vi) rezultă din (iv) iar (vii) se demonstrează prin
inducţie matematică după n ţinând cont de faptul că $C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$ pentru orice n∈$\mathbb{N}^*$ şi 0≤ k ≤n.

Definiţia 1.5. Prin *unităţile* U(A) ale inelului unitar A înţelegem unităţile monoidului (A, ·), adică U(A)={a∈A| există b∈A a.î. ab=ba=1}.

În mod evident, (**U**(A), ·) este grup.

De exemplu, **U**($\mathbb{Z}$)={±1} iar dacă A este inel unitar şi n∈$\mathbb{N}$, n≥2, atunci **U**($M_n(A)$)={M∈$M_n(A)$| det(M)≠0}.

Grupul (**U**($M_n(A)$,·) se notează prin **GL**$_n$(A) şi se numeşte *grupul liniar general de grad n peste A.*

Definiţia 1.6. Un element a∈A se zice *divizor al lui zero* la stânga (dreapta) dacă există b∈A* a.î. ab=0 (ba=0).

Exemple 1. Dacă A=$M_2(\mathbb{Z})$, atunci din $\begin{pmatrix}1&0\\1&0\end{pmatrix}\begin{pmatrix}0&0\\1&1\end{pmatrix}=O_2$ deducem

că $\begin{pmatrix}10\\10\end{pmatrix}$ este divizor al lui zero la stânga iar $\begin{pmatrix}00\\11\end{pmatrix}$ este divizor al lui zero la dreapta.

Dacă $n\in\mathbb{N}$, $n \geq 2$ nu este un număr prim iar $n=n_1n_2$ cu n_1, n_2 diferiți de 1 şi n, atunci în inelul $(\mathbb{Z}_n, +, \cdot)$ avem egalitatea $\hat{n}_1 \cdot \hat{n}_2 = \hat{n} = \hat{0}$, adică $\hat{n}_1$ şi $\hat{n}_2$ sunt divizori ai lui zero.

2. În orice inel A, elementul 0 este divizor al lui zero la stânga şi la dreaptaA.

Propoziția 1.7. Fie A un inel şi a, b, c∈A.

(i) Dacă A este unitar şi a∈U(A), atunci a nu este divizor al lui zero (nici la dreapta nici la stânga)

(ii) Dacă a nu este divizor al lui zero la stânga (dreapta) şi ab=ac (ba=ca), atunci b=c.

Demonstrație. (i). Dacă a∈U(A), atunci există b∈A a.î. ab=ba=1. Dacă a ar fi divizor al lui zero, de exemplu la stânga, atunci există $c\in A^*$ a.î. ac=0. Deducem imediat că b(ac)=b·0=0 ⇔ (ba)c=0 ⇔ 1·c=0 ⇔ c=0 - absurd. Analog dacă a este divizor al lui zero la dreapta.

(ii). Din ab=ac deducem că a(b-c)=0 şi cum am presupus că a nu este divizor al lui zero la stânga, cu necesitate b-c=0, adică b=c. ■

Definiția 1.8. Numim *domeniu de integritate* (sau *inel integru*), un inel comutativ, nenul şi fără divizori ai lui zero, diferiți de zero.

Inelul întregilor $(\mathbb{Z}, +,\cdot)$ este un exemplu de inel integru (vezi §6 de la Capitolul 2) .

Definiția 1.9. Un element a∈A se zice *nilpotent* dacă există $n\in\mathbb{N}^*$ a.î. $a^n = 0$.

Vom nota prin **N**(A) mulțimea elementelor nilpotente din inelul A (evident $0\in\mathbf{N}(A)$).

De exemplu, în inelul $A=M_2(\mathbb{Z})$ dacă alegem $M=\begin{pmatrix}01\\00\end{pmatrix}$ cum

$M^2=O_2$, deducem că $M\in$**N(M$_2$($\mathbb{Z}$))**. De asemenea, cum în inelul $\mathbb{Z}_8$ avem $\hat{2}^3=\hat{8}=\hat{0}$ deducem că $\hat{2}\in$**N($\mathbb{Z}_8$)**.

În mod evident, dacă $a\in$**N(**A**)**, atunci a este divizor al lui zero la dreapta şi la stânga.

Să presupunem că A este un inel unitar nenul. Dacă elementul 1 are ordinul infint în grupul (A,+) vom spune că A este un inel de *caracteristică 0* (vom scrie **car(**A**)**=0). În mod evident, a spune că **car(**A**)**=0 revine la aceea că $n\cdot 1\neq 0$ pentru orice $n\in\mathbb{N}^*$.

Dacă ordinul lui 1 în grupul (A,+) este p vom spune că inelul A are *caracteristică* p şi vom scrie **car(**A**)**=p (acest lucru revine la a spune că p este cel mai mic număr natural nenul cu proprietatea că $p\cdot 1=0$).

De exemplu, inelul întregilor este un inel de caracteristică 0, pe când $\mathbb{Z}_3$ este un inel de caracteristică 3.

Observaţia 1.10. Dacă inelul A este domeniu de integritate de caracteristică p, atunci p este un număr prim.

Într-adevăr, dacă p nu ar fi prim, atunci putem scrie $p=p_1p_2$ cu p_1, p_2 numere naturale mai mici decât p şi diferite de 1 şi p. Cum $p\cdot 1=0$ iar $(p_1p_2)\cdot 1=(p_1\cdot 1)(p_2\cdot 1)$ obţinem că $(p_1\cdot 1)(p_2\cdot 1)=0$ şi cum A este domeniu de integritate deducem că $p_1\cdot 1=0$ sau $p_2\cdot 1=0$, contrazicând minimalitatea lui p cu proprietatea că $p\cdot 1=0$.

§2. Subinele şi ideale

Definiţia 2.1. Dacă (A,+,·) este un inel, vom spune că o submulţime nevidă A′ a lui A este *subinel* al lui A dacă restricţiile operaţiilor de adunare şi înmulţire de pe A la A' îi conferă lui A' structură de inel.

Acest lucru revine la a spune că $A'\leq(A,+)$ (adică pentru orice $a,b\in A'\Rightarrow a-b\in A'$) şi că pentru orice $a, b\in A'\Rightarrow ab\in A'$.

Observaţia 2.2. Dacă A este inel unitar, vom spune că o submulţime nevidă A' a lui A este *subinel unitar* al lui A dacă A' este subinel al lui A şi $1\in A'$.

De exemplu, {0} şi A sunt subinele ale lui A. Oricare alt subinel al lui A diferit de {0} şi A se zice *propriu.*

Cum orice subinel A al inelului întregilor $\mathbb{Z}$ este în particular subgrup al grupului ($\mathbb{Z}$, +) cu necesitate există $n\in\mathbb{N}$ a.î. $A=n\mathbb{Z}$ (conform Teoremei 6.11. de la Capitolul 2).

În mod evident, pentru $a, b\in A$ avem $ab\in A$, de unde concluzia că subinelele lui ($\mathbb{Z}$, +) sunt submulţimile de forma $n\mathbb{Z}=\{nk : k\in\mathbb{Z}\}$ cu $n\in\mathbb{N}$.

În cele ce urmează prin **I(**A**)** vom nota mulţimea subinelelor lui A.

Propoziţia 2.3. Dacă $(A_i)_{i\in I}$ este o familie de subinele ale lui A, atunci $\bigcap_{i\in I} A_i \in$I(A).

Demonstraţie. Fie $A'=\bigcap_{i\in I} A_i \neq\varnothing$ (căci $0\in A'$) şi $a, b\in A'$. Atunci $a, b\in A_i$ pentru orice $i\in I$ şi cum A_i este subinel al lui A deducem că $a-b$, $ab\in A_i$, adică $a-b$, $ab\in A'$. Dacă A este unitar, cum $1\in A_i$ pentru orice $i\in I$ deducem că $1\in\bigcap_{i\in I} A_i = A'$. ■

Observaţia 2.4. În general, o reuniune de subinele ale unui inel nu este cu necesitate un subinel. De exemplu, $2\mathbb{Z}$ şi $3\mathbb{Z}$ sunt subinele ale lui ($\mathbb{Z}$, +, ·) pe când $A=2\mathbb{Z}\cup 3\mathbb{Z}$ nu este subinel al lui $\mathbb{Z}$ deoarece 2, $3\in A$ iar $3-2=1\notin A$.

Definiţia 2.5. Fie A un inel şi M $\subseteq$A o submulţime nevidă. Prin *subinelul lui A generat de mulţimea M* vom înţelege cel mai mic subinel al lui A (faţă de incluziune) ce conţine pe M; dacă vom nota prin [M] acest subinel, atunci în mod evident $[M]=\bigcap_{\substack{A'\in I(A)\\ M\subseteq A'}} A'$.

Propoziţia 2.6. Dacă A este un inel, atunci (I(A), $\subseteq$) este o latice completă.

Demonstrație. Dacă $F=(A_i)_{i\in I}$ este o familie de elemente din **I(**A**)**, atunci $\inf(F)=\bigcap_{i\in I} A_i$ iar $\sup(F)=[\bigcup_{i\in I} A_i]$. ■

Propoziția 2.7. Fie A, B două inele comutative a.î. A este subinel al lui B şi $b\in B\backslash A$. Atunci, $[A\cup\{b\}]=\{a_0+a_1b+\ldots+a_nb^n \mid n\in\mathbb{N}$ şi $a_0,a_1,\ldots,a_n\in A\}$.

Demonstrație. Să notăm prin $A[b]=\{a_0+a_1b+\ldots+a_nb^n \mid n\in\mathbb{N}$ şi $a_0,a_1,\ldots,a_n\in A\}$. Se verifică imediat prin calcul că A[b] este subinel al lui B ce conține pe $A\cup\{b\}$.

Cum $[A\cup\{b\}]$ este cel mai mic subinel al lui B ce contine pe $A\cup\{b\}$ avem incluziunea $[A\cup\{b\}]\subseteq A[b]$.

Fie acum B' $\in$**I(**B**)** a.î. $A\cup\{b\}\subseteq$ B'. Deducem imediat că $A[b]\subseteq$ B' şi cum B' este oarecare obținem că $A[b]\subseteq\cap$ B'$=[A\cup\{b\}]$, de unde egalitatea dorită.■

Definiția 2.8. Fie A un inel iar $I\subseteq A$ o submulțime nevidă a sa. Vom spune că I este un *ideal stâng (drept)* al lui A dacă:

(i) $I\leq(A,+)$ (adică pentru orice $a,b\in I\Rightarrow a-b\in I$)

(ii) Pentru orice $a\in A$ şi $x\in I$ avem $ax\in I$ ($xa\in I$).

Dacă I este un ideal simultan stâng şi drept vom spune despre el că este *bilateral.*

Vom nota prin $\mathbf{Id_s}$**(**A**)** ($\mathbf{Id_d}$**(**A**)**) mulțimea idealelor stângi (drepte) ale lui A iar prin $\mathbf{Id_b}$**(**A**)** mulțimea idealelor bilaterale ale lui A.

În cazul când A este comutativ, în mod evident $\mathbf{Id_s}$**(**A**)**=$\mathbf{Id_d}$**(**A**)**=$\mathbf{Id_b}$**(**A**)** şi convenim să notăm prin **Id(**A**)** mulțimea idealelor lui A.

Observația 2.9. 1. Ținând cont de definiția subinelului unui inel deducem că orice ideal este subinel. Reciproca nu este adevărată.

Într-adevăr, în inelul unitar $M_n(\mathbb{Z})$ al matricelor pătratice de ordin n ($n\geq2$) mulțimea S a matricelor superior triunghiulare (adică acele matrice din $M_n(\mathbb{Z})$ ce au toate elementele de sub diagonala principală egale cu zero) este subinel unitar după cum se verifică imediat prin calcul, dar nu este ideal stâng sau drept al lui $M_n(\mathbb{Z})$ căci în

general produsul dintre o matrice superior triunghiulară din S şi o altă matrice din $M_n(\mathbb{Z})$ nu este superior triunghiulară.

2. Nu orice ideal stâng este în acelaşi timp şi ideal drept sau invers.

Într-adevăr, dacă $n\in\mathbb{N}$, $n\geq 2$, atunci în inelul $M_n(\mathbb{Z})$ mulțimea $I=\{A=(a_{ij})\in M_n(\mathbb{Z})|\ a_{i1}=0$ pentru orice $1\leq i\leq n\}$ este ideal stâng fără a fi ideal drept iar $J=\{A=(a_{ij})\in M_n(\mathbb{Z})|\ a_{1j}=0$ pentru orice $1\leq j\leq n\}$ este ideal drept fără a fi ideal stâng.

3. Dacă I este un ideal al unui inel comutativ şi unitar A şi $n\in\mathbb{N}$, $n\geq 2$, atunci $M_n(I)$ este ideal bilateral al lui $M_n(A)$.

4. Dacă A este un inel unitar şi comutativ, atunci $\mathbf{N}(A)\in\mathbf{Id}(A)$. Într-adevăr, dacă $x\in\mathbf{N}(A)$ atunci există $n\in\mathbb{N}$ a.î. $x^n=0$, astfel că dacă $a\in A$, $(ax)^n=a^nx^n=a^n\cdot 0=0$, deci $ax\in\mathbf{N}(A)$. Dacă mai avem $y\in\mathbf{N}(A)$, atunci există $m\in\mathbb{N}$ a.î. $y^m=0$. Se deduce imediat că $(x-y)^{m+n}=0$, adică $x-y\in\mathbf{N}(A)$.

5. Dacă $x\in\mathbf{U}(A)$ şi $y\in\mathbf{N}(A)$, atunci $x+y\in\mathbf{U}(A)$. Într-adevăr, scriind $x+y=x(1+x^{-1}y)$, cum $x^{-1}y = z\in\mathbf{N}(A)$, pentru a proba că $x+y\in\mathbf{U}(A)$ este suficient să arătăm că dacă $z\in\mathbf{N}(A)$, atunci $1+z\in\mathbf{U}(A)$. Scriind din nou $1+z=1-(-z)$, cum $t = -z\in\mathbf{N}(A)$, totul s-a redus la a proba că dacă $t\in\mathbf{N}(A)$, atunci $1-t\in\mathbf{U}(A)$. Acest lucru este imediat, deoarece din $t\in\mathbf{N}(A)$ deducem existența unui număr natural n a.î. $t^n=0$ şi astfel $1=1-0=1-t^n = (1-t)(1+t+t^2+\ldots+t^{n-1})$, de unde concluzia că $1-t\in\mathbf{U}(A)$ iar $(1-t)^{-1}=1+t+t^2+\ldots+t^{n-1}$.

Propoziția 2.10. Dacă $(I_i)_{i\in K}$ este o familie de ideale stângi (drepte, bilaterale) ale lui A atunci, $\bigcap_{i\in K} I_i$ este de asemenea un ideal stâng (drept, bilateral) al lui A.

Demonstrație. Fie $I=\bigcap_{i\in K} I_i$ şi să presupunem că toate idealele I_i sunt stângi. Dacă $a, b\in I$, atunci $a, b\in I_i$ pentru orice $i\in K$ şi cum I_i este ideal avem că $a-b\in I_i$, adică $a-b\in I$. Dacă $a\in A$ şi $b\in I$ atunci $b\in I_i$ pentru orice $i\in K$ şi cum I_i este ideal stâng al lui A avem că $ab\in I_i$, de unde $ab\in I$. Analog se demonstrează în celelalte cazuri.■

Definiția 2.11. Fie A un inel oarecare iar $M \subseteq A$ o submulțime nevidă a sa. Vom nota $<M>_s$ ($<M>_d$, $<M>$) cel mai mic ideal stâng (drept, bilateral) al lui A ce conține pe M. Deci $< M >_s = \bigcap_{\substack{I \in Id_s(A) \\ M \subseteq I}} I$, $< M >_d = \bigcap_{\substack{I \in Id_d(A) \\ M \subseteq I}} I$ **iar** $< M > = \bigcap_{\substack{I \in Id_b(A) \\ M \subseteq I}} I$ **.**

Propoziția 2.12. Fie A un inel unitar şi $M \subseteq A$ o submulțime nevidă.

Atunci: (i) $< M >_s = \{\sum_{i=1}^{n} a_i x_i \,\big|\, n \in \mathrm{N}^*, a_i \in A,\ \ x_i \in M,\ 1 \le i \le n\}$

(ii) $< M >_d = \{\sum_{i=1}^{n} x_i a_i \,\big|\, n \in \mathrm{N}^*, a_i \in A,\ \ x_i \in M,\ 1 \le i \le n\}$

(iii) $< M >= \{\sum_{i=1}^{n} a_i x_i b_i \,\big|\, n \in \mathrm{N}^*, a_i, b_i \in A,\ \ x_i \in M,\ 1 \le i \le n\}$ **.**

Demonstrație. Este suficient să probăm doar egalitatea de la (i), celelalte făcându-se analog, iar pentru aceasta să notăm cu I_s mulțimea din partea dreaptă de la (i). Se verifică imediat că $I_s \in Id_s(A)$ şi că $M \subseteq I_s$ (căci A fiind unitar putem scrie pentru $x \in M$, $x = 1 \cdot x$). Cum $<M>_s$ este cel mai mic ideal stâng al lui A ce conține pe M, cu necesitate $<M>_s \subseteq I_s$. Dacă $I \in Id_s(A)$ a.î. $M \subseteq I$, atunci $I_s \subseteq \cap I = <M>_s$, de unde egalitatea $<M>_s = I_s$. ■

Observația 2.13. În particular dacă M={a} atunci idealul stâng (drept, bilateral) generat de M se numeşte *idealul principal stâng (drept, bilateral)* generat de a şi atunci avem $<a>_s = \{ba \mid b \in A\} \overset{\text{def}}{=} Aa$,

$$<a>_d = \{ab \mid b \in A\} \overset{\text{def}}{=} aA.$$

Dacă A este un inel comutativ şi unitar, atunci idealul principal generat de {a} se notează simplu prin <a> şi avem deci $<a> = Aa = aA$.

Pentru a=0 avem $<0> = \{0\}$ iar pentru a=1 avem $<1> = A$. Avem în mod evident $<a> = A \Leftrightarrow a \in \mathbf{U}(A)$.

Corolar 2.14. Dacă A este un inel oarecare unitar, atunci în raport cu incluziunea $Id_s(A)$, $Id_d(A)$ şi $Id_b(A)$ sunt latici complete.

Demonstrație. Analog ca în cazul subinelelor, infimul unei familii de ideale este egal cu intersecția lor iar supremul va fi idealul generat de reuniunea lor. ■

Fie acum I_1, I_2 două ideale stângi (drepte, bilaterale) ale unui inel unitar A.

Din Propoziția 2.12. deducem imediat că:

$$<I_1 \cup I_2>_s = <I_1 \cup I_2>_d = <I_1 \cup I_2> = \{x+y \mid x \in I_1, y \in I_2\}.$$

Convenim să notăm $\{x+y \mid x \in I_1, y \in I_2\}$ prin I_1+I_2 şi să numim acest ideal *suma idealelor* I_1 şi I_2.

Dacă $(I_i)_{i \in K}$ este o familie oarecare de ideale stângi (drepte, bilaterale) ale inelului unitar A, se constată cu ajutorul Propoziției 2.12. că :

$$< \bigcup_{i \in K} I_i >_s = < \bigcup_{i \in K} I_i >_d =$$

$$= < \bigcup_{i \in K} I_i > = \{ \sum_{i \in K} a_i \Big| a_i \in I_i \ \ pentru \ \ i \in K \ \ \ iar \ \ \{i \in K \big| a_i \neq 0\} \ \ este \ \ finita\}$$

convenim să notăm această ultimă mulțime prin $\sum_{i \in K} I_i$ şi s-o numim *suma idealelor* $(I_i)_{i \in K}$.

Fie A un inel unitar iar I_1, I_2 două ideale stângi (drepte, bilaterale).

Definiția 2.15. Definim produsul $I_1 \cdot I_2$ al idealelor I_1 şi I_2 prin $I_1 \cdot I_2 = <\{ ab \mid a \in I_1, b \in I_2\}>_s$ (respectiv $<\{ab \mid a \in I_1, b \in I_2\}>_d$, $<\{ab \mid a \in I_1, b \in I_2\}>$, după cum idealele sunt stângi, drepte sau bilaterale).

Observația 2.16. Se constată imediat că:

$$I_1 I_2 = \{ \sum_{i=1}^{n} a_i b_i \Big| n \in N^*, a_i \in I_1, \ \ b_i \in I_2, \ 1 \leq i \leq n\} \subseteq I_1 \cap I_2.$$

Inductiv se poate acum defini produsul unui număr finit de ideale ale lui A.

În particular, dacă I este un ideal al lui A şi $n \in \mathbb{N}^*$, atunci I^n este idealul lui A generat de produsele de forma $a_1a_2....a_n$ cu $a_i \in I$ pentru orice $1 \leq i \leq n$.

Să presupunem că inelul A este unitar şi comutativ.

Propoziția 2.17. (i) (Id(A), $\cap$), (Id(A),+), (Id(A),·) sunt monoizi comutativi.

(ii) Dacă I, J, K $\in$Id(A), atunci I(J+K)=IJ+IK.

Demonstrație. (i). În mod evident, operațiile de intersecție, adunare şi produs de pe **Id**(A) sunt asociative şi comutative. Elementul neutru al intersecției şi produsului este idealul A=<1> iar al sumei este idealul nul <0>.

(ii). Cum J, K $\subseteq$J+K în mod evident IJ, IK$\subseteq$I(J+K) şi deci IJ+IK$\subseteq$I(J+K).

Cealaltă incluziune rezultă din distributivitatea înmulțirii față de adunarea de pe A. ■

Definiția 2.18. Idealele I, J$\in$Id(A) se numesc *coprime* dacă I+J=<1>=A (echivalent cu a spune că există x$\in$I şi y$\in$J a.î. x+y=1).

Propoziția 2.19. Fie I, J $\in$Id(A) . Atunci

(i) (I+J)(I$\cap$J)$\subseteq$IJ

(ii) Dacă I şi J sunt coprime, atunci I$\cap$J=IJ.

Demonstrație. (i). Ținând cont de Propoziția 2.17. (ii) avem:

$$(I+J)(I\cap J)=I(I\cap J)+J(I\cap J)\subseteq IJ.$$

(ii). Dacă I şi J sunt coprime, atunci I+J=<1>=A şi astfel din (i) deducem că I$\cap$J$\subseteq$IJ şi cum IJ$\subseteq$I$\cap$J avem că I$\cap$J=IJ. ■

Observația 2.20. Inductiv se arată că dacă I_1, I_2, ..., I_n ($n \geq 2$) sunt ideale ale lui A a.î. I_j şi I_k sunt coprime pentru orice $j \neq k$, atunci $I_1 \cap I_2 \cap ... \cap I_n = I_1 I_2 ... I_n$. ■

Fie I, J∈**Id**(A) şi (I : J)={x∈A: xJ⊆I} (unde xJ={xy: y∈J}).

Propoziția 2.21. (I : J)∈Id(A).

Demonstrație. Dacă x, y∈(I : J), atunci xJ, yJ ⊆ I şi astfel xJ-yJ=(x-y)J⊆I, de unde deducem că x-y∈(I : J). Dacă a∈A şi x∈(I : J) atunci xJ⊆I iar cum I este ideal al lui A deducem că a(xJ)=(ax)J⊆I, adică ax∈(I : J) şi astfel (I : J)∈**Id**(A). ■

Definiția 2.22. Idealul (I : J) poartă numele de *idealul cît al lui I prin J*. În particular (0 : J) se numeşte *anulatorul* lui J şi se mai notează şi prin Ann(J). Dacă J={x} convenim să notăm prin (I : x) idealul (I : <x>) iar Ann(x)=Ann(<x>).

În mod evident, mulțimea divizorilor lui zero din A va fi $\bigcup_{x\in A^*} Ann(x)$.

Propoziția 2.23. Fie I, J, K ideale ale lui A iar $(I_s)_{s\in S}$, $(J_t)_{t\in T}$ două familii de ideale ale lui A. Atunci:

(i) I⊆(I : J)

(ii) (I : J)J⊆I

(iii) ((I : J) : K)=(I : JK)=((I : K) : J)

(iv) $(\bigcap_{s\in S} I_s$ **:J)=** $\bigcap_{s\in S}$ **(I_s : J)**

(v) (I : $\sum_{t\in T} J_t$ **)=** $\bigcap_{t\in T}$ **(I : J_t).**

Demonstrație. (i). Dacă x∈I, atunci în mod evident pentru orice y∈J, xy∈I, adică xJ⊆I, deci x∈(I : J). Cum x este ales oarecare deducem incluziunea I⊆(I : J).

(ii). Fie x∈(I : J)J ; atunci $x=\sum_{i=1}^{n} y_i z_i$ cu y_i∈(I : J) şi z_i∈J $1\le i\le n$. Cum y_i∈(I : J) deducem că y_iJ⊆I, adică y_iz_i∈I pentru $1\le i\le n$ deci şi x∈I , adică (I : J)J⊆I.

(iii). Cele două egalități se probează imediat prin dublă incluziune.

(iv). Avem $x\in(\bigcap_{s\in S} I_s : J) \Leftrightarrow xJ \subseteq \bigcap_{s\in S} I_s \Leftrightarrow xJ \subseteq I_s$ pentru orice $s\in S \Leftrightarrow x\in(I_s : J)$ pentru orice $s\in S \Leftrightarrow x\in \bigcap_{s\in S} (I_s : J)$, de unde egalitatea solicitată.

(v). Dacă $x\in(I : \sum_{t\in T} J_t)$, atunci $x(\sum_{t\in T} J_t)\subseteq I$. Cum pentru orice $t\in T$, $J_t\subseteq \sum_{t\in T} J_t$ deducem că $xJ_t \subseteq I$, adică $x\in(I : J_t)$ deci $x\in \bigcap_{t\in T} (I : J_t)$, obținând astfel incluziunea $(I : \sum_{t\in T} J_t)\subseteq \bigcap_{t\in T} (I : J_t)$. Cum incluziunea inversă este evidentă, deducem egalitatea solicitată. ■

§3. Morfisme de inele. Izomorfisme de inele. Transportul subinelelor şi idealelor prin morfisme de inele. Produse directe de inele

Fie A şi B două inele în care (pentru a simplifica scrierea) operațiile sunt notate pentru ambele prin „+" şi „·" .

Definiția 3.1. O funcție f : A→B se zice *morfism de inele* dacă pentru oricare a, b∈A avem egalitățile:

(i) f(a+b) =f(a)+f(b)

(ii) f(a·b) = f(a)·f(b).

Dacă A şi B sunt inele unitare, vom spune că f este *morfism de inele unitare* dacă este morfism de inele şi în plus

(iii) f(1)=1.

Observaţia 3.2. 1. Cum în particular f este morfism de grupuri aditive avem f(0)=0 şi f (-a) = -f(a), pentru orice $a\in A$.

2. Se verifică imediat că $f : \mathbb{Z}\to M_2(\mathbb{Z})$, $f(n)=\begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}$ pentru orice $n\in\mathbb{Z}$ este morfism de inele fără a fi însă morfism de inele unitare (căci $f(1)=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\neq I_2$).

3. Dacă A şi B sunt inele unitare şi f : A→B este un morfism surjectiv de inele, atunci f este şi morfism de inele unitare.

Într-adevăr, dacă $b\in B$ este un element oarecare există $a\in A$ a.î. f(a) = b. Cum $a\cdot 1 = 1\cdot a = a$, deducem că f(a) f(1) = f(1) f(a) = f(a) $\Leftrightarrow$ $\Leftrightarrow$ $b\cdot f(1)=f(1)\cdot b=b$, iar din unicitatea elementului 1 din B deducem cu necesitate că f(1)=1.

Vom nota prin **Hom(**A, B**)** mulţimea morfismelor de inele de la A la B; în mod evident $1_A\in$**Hom(**A, A**)**, iar dacă C este un alt inel, $f\in$**Hom(**A, B**),** $g\in$**Hom(**B, C**),** atunci $g\circ f\in$**Hom(**A, C**).**

Definiţia 3.3. Vom spune despre inelele A şi B că sunt *izomorfe* (şi vom nota A≈B) dacă există f∈Hom(A, B), g∈Hom(B, A) a.î. $f\circ g=1_B$ şi $g\circ f=1_A$. În acest caz despre f şi g vom spune că sunt *izomorfisme de inele*.

În particular, un izomorfism de inele este o aplicaţie bijectivă.

Reciproc, dacă $f:A\to B$ este un morfism bijectiv de inele, atunci ca în cazul morfismelor de grupuri (de la Capitolul 1) se arată uşor că $f^{-1}:B\to A$ este morfism de inele şi cum $f\circ f^{-1}=1_B$ iar $f^{-1}\circ f=1_A$ deducem că $f\in$**Hom**(A, B**)** este izomorfism de inele dacă şi numai dacă f este morfism bijectiv de inele.

Propoziţia 3.4. Fie A şi B două inele iar f∈Hom(A, B).

(i) Dacă A' ⊆ A este subinel al lui A, atunci f(A') este subinel al lui B.

(ii) Dacă B' este subinel al lui B, atunci f^{-1}(B') este subinel al lui A.

Demonstrație. (i). Fie a, b∈f(A'); atunci a=f(a'), b=f(b') cu a', b'∈A'.

Cum a-b=f(a'-b') şi ab=f(a'·b') iar a'-b', a'·b'∈A' deducem că a-b, ab∈f(A'), adică f(A') este subinel al lui B.

(ii). Dacă a', b'∈f^{-1}(B'), atunci f(a'), f(b')∈B' şi cum f(a')-f(b')=f(a'-b'), f(a')f(b')=f(a'·b') iar B' este presupus subinel al lui B, deducem că a'-b', a'·b'∈ f^{-1} (B'), adică f^{-1}(B') este subinel al lui A.■

Observația 3.5. Din propoziția precedentă deducem în particular că f(A) (pe care îl vom nota prin **Im(f)** şi îl vom numi *imaginea lui f*) este subinel al lui B şi $f^{-1}(\{0\})$ (pe care îl vom nota prin **Ker(f)** şi îl vom numi *nucleul lui f*) este *subinel* al lui A.

Propoziția 3.6. Fie A şi B două inele, f∈Hom(A, B) un morfism surjectiv de inele, iar $I_f(A)=\{S∈I(A):Ker(f)⊆S\}$. Atunci funcția $F:Id_f(A)→Id(B)$, F(S)=f(S) pentru orice S∈I_f(A) este un izomorfism de mulțimi ordonate.

Demonstrație. Definim G: Id(B)→Id_f(A) prin G(B') = f^{-1}(B') pentru orice B'∈Id(B). (conform Propoziției 3.4. funcția G este corect definită). Faptul că F şi G sunt morfisme de mulțimi ordonate (adică păstrează incluziunea) este imediat.

Ca şi în cazul Teoremei 7.4. de la Capitolul 2 (Teorema de corespondență pentru grupuri) se arată că $F∘G=1_{Id(B)}$ şi $G∘F=1_{Id_f(A)}$, de unde concluzia propoziției. ■

Propoziția 3.7. Fie f∈Hom(A, B) un morfism de inele.

(i) Dacă f este funcție surjectivă iar I este un ideal stâng (drept, bilateral) al lui A, atunci f(I) este ideal stâng (drept, bilateral) al lui B

(ii) Dacă I' este ideal stâng (drept, bilateral) al lui B, atunci f^{-1}(I') este ideal stâng (drept, bilateral) al lui A.

Demonstrație. (i). Să presupunem de exemplu că I este ideal stâng (în celelalte situații demonstrația făcându-se asemănător).

Dacă a,b∈f(I), atunci a=f(a'), b=f(b') cu a', b'∈I şi cum a-b= =f(a') - f(b')=f(a'-b'), iar a'-b'∈I deducem că a-b∈f(I).

Dacă $c \in B$ atunci, cum f este surjecție, există $c' \in A$ a.î. $c=f(c')$ şi astfel $ca=f(c')f(a')=f(c'a') \in f(I)$ (căci $c'a' \in I$). Deci f(I) este ideal stâng al lui B.

(ii). Să presupunem de exemplu că I' este ideal stâng al lui B şi fie $a, b \in f^{-1}(I')$. Atunci $f(a), f(b) \in I'$ şi cum $f(a)-f(b)=f(a-b) \in I'$ deducem că $a-b \in f^{-1}(I')$. Dacă $c \in A$, cum $f(ca)=f(c)f(a) \in I'$ deducem că $ca \in f^{-1}(I')$, adică $f^{-1}(I')$ este ideal stâng al lui A. Analog în celelalte cazuri. ■

Observația 3.8. În particular, deducem că **Ker(f)** este ideal bilateral al lui A, (adică $\text{Ker}(f) \in \mathbf{Id_b}(A)$).

Fie acum $(A_i)_{i \in I}$ o familie de inele iar $A=\prod_{i \in I} A_i$ mulțimea subiacentă a produsului direct al mulțimilor subiacente $(A_i)_{i \in I}$ (vezi §8 de la Capitolul 1).

Reamintim că $A=\{ (x_i)_{i \in I} : x_i \in A_i$ pentru orice $i \in I\}$.

Pentru două elemente $x=(x_i)_{i \in I}$ şi $y=(y_i)_{i \in I}$ din A definim adunarea şi înmulțirea lor prin: $x+y=(x_i+y_i)_{i \in I}$ şi $x \cdot y=(x_i \cdot y_i)_{i \in I}$.

Propoziția 3.9. (A, +,·) este inel.

Demonstrație. Faptul că (A, +) este grup abelian rezultă imediat: asociativitatea adunării de pe A este dată de asociativitatea adunării de pe fiecare inel A_i, elementul neutru este $0=(a_i)_{i \in I}$ cu $a_i=0$ pentru orice $i \in I$, iar opusul elementului $x=(x_i)_{i \in I}$ este $-x=(-x_i)_{i \in I}$.

Dacă $x=(x_i)_{i \in I}$, $y=(y_i)_{i \in I}$, $z=(z_i)_{i \in I}$ sunt trei elemente din A, atunci $(x+y)z=((x_i+y_i)z_i)_{i \in I}=(x_i z_i+y_i z_i)_{i \in I}=(x_i z_i)_{i \in I}+(y_i z_i)_{i \in I}=xz+yz$ şi analog $z(x+y)=zx+zy$, probând astfel distributivitatea la stânga şi dreapta a înmulțirii față de adunarea de pe A. Asociativitatea înmulțirii de pe A este dată de asociativitatea înmulțirii de pe fiecare inel A_i ($i \in I$).

■

Observaţia 3.10. 1. Dacă pentru orice $i\in I$ inelul A_i este unitar atunci şi inelul A este unitar (elementul neutru fiind $1=(b_i)_{i\in I}$ cu $b_i=1$ pentru orice $i\in I$).

2. Dacă pentru orice $i\in I$ inelul A_i este comutativ, atunci şi inelul A este comutativ.

Pentru fiecare $i\in I$ considerăm funcţia $p_i : A\to A_i$ dată de $p_i((x_j)_{j\in I})=x_i$. (p_i poartă numele de *proiecţia de indice i* sau *proiecţia lui A pe* A_i).

Se verifică imediat că pentru fiecare $i\in I$, p_i este morfism surjectiv de inele (iar dacă $(A_i)_{i\in I}$ sunt inele unitare, atunci p_i este morfism surjectiv de inele unitare).

Propoziţia 3.11. Dubletul $(A, (p_i)_{i\in I})$ verifică următoarea proprietate de universalitate: ***Pentru orice inel A´ şi orice familie de morfisme de inele*** $(p_i')_{i\in I}$ ***, cu*** $p_i':A'\to A_i$ ***pentru orice*** $i\in I$ ***există un unic morfism de inele*** $f:A'\to A$ ***a.î.*** $p_i\circ f=p_i'$ ***pentru orice*** $i\in I$.

Demonstraţie. Pentru $x\in A'$ definim $f(x)=(p_i'(x))_{i\in I}$ şi în mod evident f este morfism de inele (deoarece pentru orice $i\in I$, p_i' este morfism de inele) şi $p_i\circ f=p_i'$ pentru orice $i\in I$. Pentru a proba unicitatea lui f cu proprietatea din enunţ, fie $f':A'\to A$ un alt morfism de inele a.î. $p_i\circ f'=p_i'$ pentru orice $i\in I$. Atunci, pentru orice $x\in A'$ $p_i(f'(x))=p_i'(x)$, adică $f'(x)=(p_i'(x))_{i\in I}=f(x)$, de unde concluzia că $f=f'$.

Dacă inelele $(A_i)_{i\in I}$ sunt unitare atunci şi A este unitar şi proprietatea de universalitate este valabilă considerând în loc de morfisme de inele, morfisme unitare de inele. ■

Definiţia 3.12. Dubletul $(A, (p_i)_{i\in I})$ ce verifică proprietatea de universalitate din Propoziţia 3.11. poartă numele de *produsul direct* al familiei de inele $(A_i)_{i\in I}$ şi se notează prin $\prod_{i\in I} A_i$ (de multe ori

se omit morfismele structurale $(p_i)_{i\in I}$ dacă nu este pericol de confuzie).

Dacă I={1, 2, ..., n} convenim să notăm $\prod_{i\in I} A_i$ prin $A_1\times A_2\ldots\times A_n$.

Propoziția 3.13. Dacă $(A_i)_{i\in I}$ este o familie de inele unitare şi $A=\prod_{i\in I} A_i$, atunci $U(A)=\prod_{i\in I} U(A_i)$ (în partea dreaptă fiind produsul direct al mulțimilor $U(A_i)_{i\in I}$).

Demonstrație. Fie $x=(x_i)_{i\in I}\in A$. Atunci din echivalențele: $x\in U(A) \Leftrightarrow$ există $x'=(x_i')_{i\in I}\in A$ a.î. $xx'=x'x=1 \Leftrightarrow x_ix_i'=x_i'x_i=1$ pentru orice $i\in I \Leftrightarrow x_i\in U(A_i)$ pentru orice $i\in I \Leftrightarrow x\in\prod_{i\in I} U(A_i)$ deducem egalitatea din enunț (ca egalitate de mulțimi!). ■

De exemplu, $U(\mathbb{Z}\times\mathbb{Z})=\{(1, -1), (1, 1), (-1, 1), (-1, -1)\}$.

Observația 3.14. Analog ca în cazul grupurilor (vezi Teorema 8.6. de la Capitolul 2) pentru $m, n\in\mathbb{N}^*$, $(m, n)=1$ avem izomorfismul de inele $\mathbb{Z}_m\times\mathbb{Z}_n\approx\mathbb{Z}_{mn}$.

§4. Factorizarea unui inel printr-un ideal bilateral. Teoremele de izomorfism pentru inele

Reamintim că pentru un inel A, prin $\mathbf{Id_b(A)}$ am desemnat mulțimea idealelor bilaterale ale lui A.

Pentru $I\in\mathbf{Id_b(A)}$, cum (A, +) este grup abelian avem că $I\trianglelefteq(A,+)$ astfel că putem vorbi de $A/I = \{x+I|\ x\in A\}$ şi de grupul abelian (A/I, +) unde pentru $x,y\in A$, $(x+I)+(y+I)=(x+y)+I$. (vezi §4 de la Capitolul 2).

Vom defini acum pe grupul factor A/I o nouă operație algebrică :

$(x+I)(y+I)=xy+I$, pentru orice $x, y\in A$ (pe care convenim să o numim *înmulțire*).

Propoziția 4.1. (A/I,+, ·) este inel. Dacă A este unitar (comutativ) atunci şi A/I este unitar (comutativ).

Demonstrație. Să arătăm la început că înmulțirea pe A/I este corect definită şi în acest sens să considerăm x, y, x′, y′∈A a.î. x+I=x′+I şi y+I=y′+I. Scriind xy-x′y′=x(y-y′)+(x-x′)y′ deducem că xy-x′y′∈I, adică xy+I=x′y′+I.

Să alegem acum x, y, z∈I şi să notăm $\hat{x}$=x+I, $\hat{y}$ = y+I, $\hat{z}$ = z+I.

Atunci $\hat{x}(\hat{y}\,\hat{z})=\widehat{x(yz)}$ iar $(\hat{x}\,\hat{y})\hat{z}=\widehat{(xy)z}$, de unde deducem că $\hat{x}(\hat{y}\hat{z})=(\hat{x}\hat{y})\hat{z}$, adică înmulțirea pe A/I este asociativă, deci (A/I, ·) este semigrup.

De asemenea, $\hat{x}(\hat{y}+\hat{z})=\widehat{x(y+z)}$ = $\widehat{xy+xz}=\widehat{xy}+\widehat{xz}=\hat{x}\hat{y}+\hat{x}\hat{z}$ şi analog $(\hat{x}+\hat{y})\hat{z}=\hat{x}\,\hat{z}+\hat{y}\,\hat{z}$, de unde concluzia că (A/I, +, ·) este inel.

Dacă inelul A este unitar, atunci şi A/I este unitar, elementul neutru pentru înmulțire fiind $\hat{1}$=1+I deoarece pentru orice element x+I∈ A/I avem (1+I)(x+I)=(x+I)(1+I)=x+I.

Dacă A este inel comutativ, atunci $\hat{x}\,\hat{y}=\widehat{xy}=\widehat{yx}=\hat{y}\,\hat{x}$, de unde concluzia că şi A/I este comutativ.■

Definiția 4.2. Inelul (A/I, +, ·) poartă numele de *inel factor* (spunem că am *factorizat* inelul A prin idealul bilateral I).

Surjecția canonică p_I:A→A/I, p_I(x)=x+I pentru orice x∈A (care este morfism de grupuri aditive) este de fapt morfism de inele deoarece pentru x,y∈A avem p_I(xy)=xy+I=(x+I)(y+I)=p_I(x)p_I(y).

Dacă A este inel unitar, atunci cum p_I(1)=1+I=$\hat{1}$ iar $\hat{1}$ este elementul neutru al înmulțirii din A/I, deducem că p_I este morfism de inele unitare.

Deoarece pentru x∈I, x∈Ker(p_I) ⇔ x+I=I ⇔ x∈I, deducem că Ker(p_I)=I.

În continuare vom prezenta *teoremele de izomorfism pentru inele.*

Vom începe (ca şi în cazul grupurilor) cu o teoremă importantă cunoscută sub numele de *Teorema fundamentală de izomorfism pentru inele*:

Teorema 4.3. Dacă A, A′ sunt două inele, f∈Hom(A, A′), atunci Ker(f)∈Id_b(A) (conform Observaţei 3.8.) şi A/Ker(f) ≈ Im(f).

Demonstraţie. Pentru x∈A, definim: φ : **A/Ker(f)**→Im(f) prin φ(x+Ker(f))=f(x). Dacă mai avem y∈A, atunci din şirul de echivalenţe x+Ker(f)=y+Ker(f) ⇔ x-y∈Ker(f) ⇔f(x)=f(y) deducem că φ este corect definită şi ca funcţie este injecţie. Cum surjectivitatea lui φ este evidentă, deducem că φ este bijecţie. Deoarece pentru x, y∈A avem : φ [(x+Ker(f))+(y+Ker(f))]=f(x+y)=f(x)+f(y)=φ[x+Ker(f)]+φ [y+Ker(f)] şi φ [(x+Ker(f))(y+Ker(f))] =φ [xy+Ker(f)] = f(xy) = f(x)f(y) = = φ [x+Ker(f)] φ [y+Ker(f)] deducem că φ este morfism de inele şi cum mai sus am probat că este şi bijecţie, rezultă că φ este izomorfism de inele.■

Corolar 4.4. Dacă A, A′ sunt inele şi f∈Hom(A,A′) este un morfism surjectiv de inele, atunci A/Ker(f) ≈ A′.

Corolar 4.5. Fie A un inel, A′ ⊆ A un subinel iar I∈Id_b(A). Atunci A′+I={x+y| x∈A′, y∈I} este subinel al lui A, I∈Id_b(A′+I), A′∩I∈Id_b(A′) şi avem următorul izomorfism de inele:

$$A'/(A'\cap I) \approx (A'+I)/I \,.$$

Demonstraţie Fie a,b∈A′+I, a=x+y, b=z+t, x,z∈A′ şi y,t∈I. Atunci a-b=(x-z)+(y-t)∈A′+I iar ab=(x+y)(z+t)=xz+(xt+yz+yt)∈A′+I, de unde concluzia că A′+I este subinel al lui A. Faptul că I∈Id_b(A′+I) este evident.

Să considerăm acum φ:A′→(A′+I)/I, φ(x)=x+I care este în mod evident morfism de inele. Dacă avem un element (x+y)+I din (A′+I)/I cu x∈A′ şi y∈I, atunci cum (x+y)-x=y∈I deducem că (x+y)+I=x+I=φ(x), adică φ este surjecţie.

Din şirul de echivalenţe: $x\in Ker(\varphi) \Leftrightarrow \varphi(x)=0 \Leftrightarrow x+I=I$, pentru orice $x\in A' \Leftrightarrow x\in I$, pentru orice $x\in A' \Leftrightarrow x\in A'\cap I$ deducem că $A'\cap I=Ker(\varphi)\in Id_b(A')$.

Conform Corolarului 4.4. avem izomorfismele de inele:

$$A/Ker(\varphi) \approx Im(\varphi) \Leftrightarrow A'/(A'\cap I) \approx (A'+I)/I.\blacksquare$$

Corolar 4.6. Fie A un inel, $I\in Id_b(A)$ iar J un subinel al lui A ce include pe I. Atunci $J\in Id_b(A) \Leftrightarrow J/I\in Id_b(A/I)$. În acest caz avem izomorfismul canonic: $A/J\approx (A/I)/(J/I)$ **.**

Demonstraţie. Echivalenţa $J\in Id_b(A) \Leftrightarrow J/I \in Id_b(A/I)$ este imediată. Fie acum $A \xrightarrow{p_I} A/I \xrightarrow{p_{J/I}} (A/I)/(J/I)$ iar $\varphi : A\to (A/I)/(J/I)$, $\varphi=p_{J/I}\circ p_I$.

În mod evident φ este morfism surjectiv de inele (fiind compunerea morfismelor surjective canonice).

Cum $Ker\varphi=\{a\in A|\varphi(a)=0\}=\{a\in A|p_{J/I}(a+I)=0\}=\{a\in A|(a+I)+J/I=J/I\}=$

$=\{a\in A|\ a+I\in J/I\}=\{a\in A|\ a\in J\}=J$, izomorfismul căutat rezultă acum din Corolarul 4.4. ■

§5. Corp. Subcorp. Subcorp prim. Morfisme de corpuri. Caracteristica unui corp

Definiţia 5.1. Vom spune despre un inel unitar K că este *corp* dacă $U(K)=K^*$ (unde $K^*=K\setminus\{0\}$). Astfel, $(K, +, \cdot)$ este corp dacă:

(i) $(K, +)$ este grup

(ii) $(K^*, \cdot)$ este grup

(iii) Înmulţirea este distributivă la stânga şi la dreapta faţă de adunare.

Din cele stabilite în Capitolul 2 deducem că dacă $n\in\mathbb{N}$, $n\geq 2$, atunci $(\mathbb{Z}_n,+,\cdot)$ este corp dacă şi numai dacă n este prim.

Pe parcursul acestui capitol vom pune în evidenţă mai multe exemple de corpuri (vezi §6, 7, 8, 9) .

În mod evident, într-un corp K nu există divizori ai lui zero nenuli după cum nu există nici ideale diferite de $\{0\}$ şi K (căci dacă prin absurd ar exista de exemplu un ideal I la stânga a.î. $\{0\} \subset I \subset K$

atunci am avea $a \in I$ a.î. $a \neq 0$ şi cum K este corp am deduce că $a^{-1}a=1 \in I$, adică I=K - absurd!).

Reciproc, dacă un inel unitar A are doar idealele {0} şi A atunci A este corp. Într-adevăr, dacă $a \in A^*$, atunci considerând idealele aA şi Aa trebuie ca aA=Aa=A, adică ab=ca=1, cu b, $c \in A$, de unde b=c şi ab=ba=1, adică a este inversabil şi astfel A devine corp.

Definiția 5.2. Fiind dat corpul K, o submulțime nevidă k a lui K se zice *subcorp* al lui K dacă restricțiile operațiilor de adunare şi înmulțire de pe K la k conferă lui k structură de corp. În acest caz spunem despre K că este o *extindere* a lui k (vezi §6 ,7).

Propoziția 5.3. Fie K un corp iar $k \subseteq K$ o submulțime nevidă a sa. Atunci k este *subcorp* al lui K dacă şi numai dacă :

(i) oricare ar fi $x, y \in k \Rightarrow x-y \in k$

(ii) oricare ar fi $x, y \in k$ cu $y \neq 0 \Rightarrow xy^{-1} \in k$.

Demonstrație. Echivalența celor două afirmații rezultă din faptul că (k, +) şi $(k^*, \cdot)$ trebuie să fie subgrupuri ale grupurilor (K, +) şi respectiv $(K^*, \cdot)$. Să observăm că elementele unitate din K şi k coincid.■

Propoziția 5.4. Dacă $p \geq 2$ este un număr prim, atunci $\mathbb{Z}_p$ şi $\mathbb{Q}$ nu au alte subcorpuri în afară de ele însele.

Demonstrație. Într-adevăr, dacă $F \subseteq \mathbb{Z}_p$ este un subcorp al lui $\mathbb{Z}_p$ atunci F este subinel al lui $\mathbb{Z}_p$. Ştim însă că subinelele şi idealele lui $\mathbb{Z}_p$ coincid iar cum $\mathbb{Z}_p$ este corp, singurele sale ideale sunt {0} şi $\mathbb{Z}_p$, deci singurul subcorp al lui $\mathbb{Z}_p$ este $\mathbb{Z}_p$.

Fie acum $F \subseteq \mathbb{Q}$ un subcorp. Cum $1 \in F$ deducem că pentru orice $n \in \mathbb{N}$, $n \in F$ (deoarece $n=\underbrace{1+...+1}_{n \text{ ori}}$), adică $\mathbb{N} \subseteq F$.Cum $0 \in F$ deducem că pentru orice $n \in \mathbb{N}$, $0 - n = -n \in F$, adică şi $\mathbb{Z} \subseteq F$. Dacă avem $m, n \in \mathbb{Z}$, $n \neq 0$, atunci $mn^{-1}=m/n \in F$ (căci F este presupus subcorp al lui $\mathbb{Q}$), adică $\mathbb{Q} \subseteq F$, de unde $\mathbb{Q}=F$.■

În paragraful 1 am definit noţinea de *caracteristică* a unui inel. Cum corpurile sunt în particular inele această definiţie rămâne valabilă şi pentru corpuri.

Astfel, dacă k este un corp iar pentru orice $n\in\mathbb{N}^*$, $n\cdot 1_k\neq 0$ atunci corpul k se zice de *caracteristică 0* (scriem car(k)=0) iar dacă n este cel mai mic număr natural nenul pentru care $n\cdot 1_k=0$ atunci spunem că corpul k este de *caracteristică n* (se scrie car(k)=n). Analog ca în cazul inelelor (vezi Observaţia 1.10.) se demonstrează că dacă car(k)=n, atunci n este un număr prim.

Propoziţia 5.5. Dacă K este un corp iar $(K_i)_{i\in I}$ o familie nevidă de subcorpuri ale lui K, atunci $\bigcap_{i\in I} K_i$ este subcorp al lui K.

Demonstraţie. Fie $K'=\bigcap_{i\in I} K_i$ şi $x, y\in K'$. Atunci $x, y\in K_i$ pentru orice $i\in I$ şi cum fiecare K_i este subcorp al lui K avem că $x-y\in K_i$, adică $x-y\in\bigcap_{i\in I} K_i = K'$.

Dacă $y\neq 0$, atunci $xy^{-1}\in K_i$ pentru orice $i\in I$ şi cum K_i este subcorp al lui K deducem că $xy^{-1}\in\bigcap_{i\in I} K_i = K'$, adică K′ este subcorp al lui K.■

Definiţia 5.6. Un corp care nu are alte subcorpuri în afară de el însuşi se numeşte *corp prim*.

Mai înainte am văzut că $\mathbb{Q}$ este corp prim ca şi $\mathbb{Z}_p$ (cu $p\geq 2$ prim) precum şi intersecţia tuturor subcorpurilor unui corp.

Definiţia 5.7. Dacă K, K′ sunt două corpuri, numim *morfism de corpuri* orice morfism unitar de inele $f:K\to K'$.

Deci, $f : K\to K'$ este morfism de corpuri dacă şi numai dacă $f(1)=1$ şi $f(x+y)=f(x)+f(y)$, $f(xy)=f(x)f(y)$ pentru orice $x, y\in K$.

În particular, deducem că $f(0)=0$, $f(-x) = -f(x)$ pentru orice $x\in K$ iar dacă $x\in K^*$, atunci $f(x^{-1}) = (f(x))^{-1}$.

Observaţia 5.8. Orice morfism de corpuri $f : K\to K'$ este ca funcţie o injecţie.

Într-adevăr, dacă vom considera $x, y\in K$ a.î. $f(x)=f(y)$ şi presupunem prin absurd că $x-y\neq 0$, cum $x-y\in K^*$, există $z\in K^*$ a.î.

(x-y)z=1. Deducem imediat că : f(x-y)f(z)= f(1)=1 $\Leftrightarrow$ (f(x)-f(y))f(z)=1 $\Leftrightarrow$ 0·f(z)=1 $\Leftrightarrow$ 0=1-absurd, deci x-y=0 $\Rightarrow$x = y.■

Definiția 5.9. Un morfism de corpuri f:K$\to$K′ se zice *izomorfism de corpuri* dacă există g:K′$\to$K a.î. g$\circ$f=1_K şi f$\circ$g=$1_{K'}$. În acest caz vom scrie K$\approx$K′. Se probează imediat că f este izomorfism de corpuri dacă şi numai dacă f este morfism bijectiv de corpuri.

Ținând cont de Observația 5.8. deducem că morfismul f : K$\to$K′ este izomorfism de corpuri dacă şi numai dacă f este surjecție.

Propoziția 5.10. Orice corp prim este izomorf sau cu corpul $\mathbb{Q}$ al numerelor raționale sau cu un anumit corp $\mathbb{Z}_p$ cu p prim.

Demonstrație. Fie P un corp prim şi f : $\mathbb{Z}\to$P, f(n)=n·1_P pentru orice n$\in\mathbb{Z}$, care în mod evident este morfism unitar de inele. Atunci Ker (f) este ideal al lui $\mathbb{Z}$ şi deci există n$\in\mathbb{N}$ a.î. Ker (f)=n$\mathbb{Z}$.

Avem acum două cazuri:

1. Ker (f)={0}. Atunci f este morfism injectiv de la $\mathbb{Z}$ la P şi să considerăm $\overline{P}$ ={(m·1_P)(n·1_P)$^{-1}$ | m, n$\in\mathbb{Z}$, n$\neq$0} $\subseteq$ P. Să verificăm că $\overline{P}$ este subcorp al lui P iar pentru aceasta fie x, y$\in\overline{P}$, x= (m·1_P)(n·1_P)$^{-1}$, y=(r·1_P)(s·1_P)$^{-1}$ cu m, n, r, s$\in\mathbb{Z}$ iar n, s$\in\mathbb{Z}^*$.
Atunci x-y = (m·1_P)(n·1_P)$^{-1}$ - (r·1_P)(s·1_P)$^{-1}$ =(ms-nr)·1_P [(ns)·1_P]$^{-1}\in\overline{P}$ iar dacă y$\in\overline{P}^*$ (adică r$\in\mathbb{Z}^*$) atunci xy^{-1}= (ms)·1_P·[(nr)·1_P]$\in\overline{P}$.

Deoarece P este corp prim avem că $\overline{P}$ =P şi se verifică imediat că g:$\mathbb{Q}\to$P, g(m/n)=(m·1_P)(n·1_P)$^{-1}$ pentru orice m/n$\in\mathbb{Q}$ este izomorfism de copuri, de unde concluzia că P$\approx\mathbb{Q}$.

2. Ker(f)$\neq${0}. Atunci Ker(f)=n$\mathbb{Z}$ cu n$\in\mathbb{N}^*$. Conform Teoremei fundamentale de izomorfism pentru inele (vezi Teorema 4.3.) avem că $\mathbb{Z}$/Ker(f) $\approx$ Im(f) $\Leftrightarrow$ $\mathbb{Z}_n\approx$Im(f) . Cum Im(f) este subinel al corpului P deducem că Im(f) este domeniu de integritate deci şi $\mathbb{Z}_n$ va fi domeniu de integritate, deci corp.

Astfel Im (f) este subcorp al lui P şi cum P este prim avem că P=Im(f) şi deci $\mathbb{Z}_n\approx$P. ■

Observaţia 5.11. 1. Din Propoziţia precedentă deducem că un corp K este de caracteristică zero dacă şi numai dacă subcorpul prim al lui K este izomorf cu corpul $\mathbb{Q}$ al numerelor raţionale şi este de caracteristică p ($p\in\mathbb{N}^*$ fiind un număr prim) dacă şi numai dacă subcorpul prim al lui K este izomorf cu corpul $\mathbb{Z}_p$. În acest ultim caz corpul K poate fi privit ca un $\mathbb{Z}_p$-spaţiu vectorial. Deducem imediat că dacă K este finit, atunci $|K| = p^t$ cu $t\in\mathbb{N}^*$.

2. Dacă K este o extindere a lui k (adică k este subcorp al lui K) atunci k şi K au aceeaşi caracteristică. În particular, dacă există un morfism de corpuri $f : k\to K$ atunci k şi K au aceeaşi caracteristică.

3. Conform unei celebre teoreme a lui Wedderburn orice corp finit este comutativ.

Propoziţia 5.12. Fie K un corp comutativ cu car(K)=p ($p\geq 2$ număr prim). Atunci, pentru orice $x, y\in K$ avem:

(i) $px=0$

(ii) $(xy)^p=x^py^p$

(iii) $(x\pm y)^p=x^p\pm y^p$ (semnele se corespund).

Demonstraţie. (i). Avem $px=p(1_Kx)=(p\cdot 1_K)x=0\cdot x=0$

(ii). Este evidentă deoarece $xy=yx$.

(iii). Cum p este prim $p\mid C_p^k$ pentru orice $1\leq k\leq p-1$ şi astfel dezvoltând după binomul lui Newton avem $(x+y)^p=x^p+y^p$ iar $(x-y)^p=x^p+(-1)^p y^p$. Dacă $p>2$, atunci cum p este prim (deci cu necesitate impar) deducem că $(x-y)^p = x^p - y^p$ iar dacă p=2, cum $2y^2 = 0$ avem $(x-y)^2=x^2+y^2=x^2-y^2$. ■

Observaţia 5.13. Din propoziţia precedentă deducem că funcţia $\varphi_p:K\to K$, $\varphi_p(x)=x^p$ este morfism de corpuri. Morfismul φ_p poartă numele de *morfismul lui Frobenius*.

§6. Inele de fracţii. Construcţia corpului $\mathbb{Q}$ al numerelor raţionale

În cadrul acestui paragraf prin A vom desemna un inel unitar comutativ.

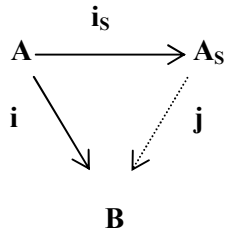
Definiţia 6.1. O submulţime nevidă $S \subseteq A$ se zice *sistem multiplicativ* dacă $1 \in S$ şi $a, b \in S \Rightarrow ab \in S$ (adică înmulţirea de pe A conferă lui S structură de monoid).

Teorema 6.2. Fie $S \subseteq A$ un sistem multiplicativ format din nondivizori ai lui zero. Atunci există un inel unitar şi comutativ A_S, un morfism injectiv de inele unitare $i_S: A \to A_S$ a. î. :

1) Pentru orice $s \in S \Rightarrow i_S(s) \in U(A_S)$

2) Pentru orice $\alpha \in A_S$, există $a \in A$, $s \in S$ a.î. $\alpha = i_S(a)[i_S(s)]^{-1}$

3) Dacă mai există un inel unitar şi comutativ B şi un morfism injectiv de inele $i: A \to B$ a.î. pentru orice $s \in S \Rightarrow i(s) \in U(B)$, atunci există un unic morfism de inele unitare $j: A_S \to B$ a.î. diagrama



este comutativă (adică $j \circ i_S = i$).

Demonstraţie. Să construim la început inelul A_S şi morfismul injectiv de inele unitare $i_S: A \to A_S$. În acest sens pe produsul cartezian de mulţimi $A \times S$ definim relaţia $(a,s) \sim (a',s') \Leftrightarrow as' = a's$. În mod evident, relaţia $\sim$ este reflexivă şi simetrică. Pentru a proba tranzitivitatea relaţiei $\sim$ fie $(a, s), (a', s'), (a'',s'') \in A \times S$ a.î. $(a, s) \sim (a', s')$ şi $(a', s') \sim (a'', s'')$, adică $as' = a's$ şi $a's'' = a''s'$. Deducem imediat că $as's'' = a'ss'' = (a's'')s = (a''s')s \Rightarrow (as'')s' = (a''s)s' \Rightarrow as'' = a''s$ (căci s' nu este divizor al lui zero), adică relaţia $\sim$ este şi tranzitivă, deci o echivalenţă pe $A \times S$.

Clasa de echivalență a elementului $(a, s)\in A\times S$ o vom nota prin $\frac{a}{s}$ şi o vom numi *fracție* iar mulțimea factor $(A\times S)/\sim$ o vom nota prin A_S.

Deci $A_S=\{\frac{a}{s} \mid a\in A$ şi $s\in S\}$. Cum S nu conține divizori ai lui zero avem că $0\notin S$.

Pentru $\frac{a}{s}, \frac{b}{t} \in A_S$ definim $\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st}$ şi $\frac{a}{s}\cdot\frac{b}{t}=\frac{ab}{st}$. Dacă $\frac{a}{s}=\frac{a'}{s'}$ şi $\frac{b}{t}=\frac{b'}{t'}$ atunci $as'=a's$ şi $bt'=b't$ de unde deducem imediat că $(at+bs)(t's')=as'tt'+bt'ss'=a'stt'+b'tss'=(a't'+b's')ts$, deci

$\frac{at+bs}{ts}=\frac{a't'+b's'}{t's'} \Leftrightarrow \frac{a}{s}+\frac{b}{t}=\frac{a'}{s'}+\frac{b'}{t'}$ (altfel zis, adunarea fracțiilor este corect definită). Cum şi $(ab)(s't') = (a'b')(st)$ deducem că $\frac{a}{s}\cdot\frac{b}{t}=\frac{a'}{s'}\cdot\frac{b'}{t'}$ deci şi înmulțirea fracțiilor este corect definită.

Să arătăm acum că $(A_S, +, \cdot)$ este inel comutativ unitar.

Dacă $\frac{a}{s},\frac{b}{t},\frac{c}{u}\in A_S$, atunci

$(\frac{a}{s}+\frac{b}{t})+\frac{c}{u}=\frac{at+bs}{st}+\frac{c}{u}=\frac{(at+bs)u+c(st)}{(st)u}=\frac{atu+bsu+cst}{stu}$ iar

$\frac{a}{s}+(\frac{b}{t}+\frac{c}{u})=\frac{a}{s}+\frac{bu+ct}{tu}=\frac{a(tu)+(bu+ct)s}{s(tu)}=\frac{atu+bus+cts}{stu}$, de unde deducem că $\left(\frac{a}{s}+\frac{b}{t}\right)+\frac{c}{u}=\frac{a}{s}+\left(\frac{b}{t}+\frac{c}{u}\right)$, adică adunarea pe A_S este asociativă. Cum adunarea şi înmulțirea pe A sunt comutative deducem imediat că adunarea fracțiilor este comutativă.

Deoarece pentru orice $\frac{a}{s}\in A_S$, $\frac{a}{s}+\frac{0}{1}=\frac{a\cdot 1+s\cdot 0}{s\cdot 1}=\frac{a}{s}=\frac{0}{1}+\frac{a}{s}$, deducem că $\frac{0}{1}$ este elementul neutru pentru adunarea fracțiilor.

Deoarece $\frac{a}{s}+\frac{-a}{s}=\frac{as-as}{s^2}=\frac{0}{s^2}=\frac{0}{1}$ deducem că $-(\frac{a}{s})=\frac{-a}{s}$ adică orice fracție are o opusă . Am probat până acum faptul că (A_S, +) este grup abelian.

Deoarece $(\frac{a}{s}\cdot\frac{b}{t})\frac{c}{u}=\frac{(ab)c}{(st)u}=\frac{a(bc)}{s(tu)}=\frac{a}{s}(\frac{b}{t}\cdot\frac{c}{u})$ deducem că înmulțirea fracțiilor este asociativă . Deoarece inelul A este comutativ, deducem că şi înmulțirea fracțiilor este comutativă, adică (A_S, ·) este monoid comutativ.

Deoarece $\frac{a}{s}\cdot\frac{1}{1}=\frac{1}{1}\cdot\frac{a}{s}=\frac{a}{s}$ deducem că $\frac{1}{1}$ este elementul neutru pentru înmulțirea fracțiilor. Să remarcăm faptul că dacă $\frac{a}{s}\in A_S$ şi $t\in S$, atunci $\frac{at}{st}=\frac{a}{s}$, de unde concluzia că o fracție poate fi "simplificată" prin factori din S.

Astfel $\frac{1}{1}=\frac{s}{s}$, pentru orice $s\in S$.

Deoarece $(\frac{a}{s}+\frac{b}{t})\cdot\frac{c}{u}=\frac{at+bs}{st}\cdot\frac{c}{u}=\frac{atc+bsc}{stu}$ iar

$$\frac{a}{s}\cdot\frac{c}{u}+\frac{b}{t}\cdot\frac{c}{u}=\frac{ac}{su}+\frac{bc}{tu}=\frac{actu+bcsu}{sutu}=\frac{(atc+bsc)u}{(stu)u}=\frac{atc+bsc}{stu}$$

deducem că $(\frac{a}{s}+\frac{b}{t})\frac{c}{u}=\frac{a}{s}\cdot\frac{c}{u}+\frac{b}{t}\cdot\frac{c}{u}$, adică înmulțirea este distributivă față de adunare, probând astfel că (A_S, +, ·) este un inel.

Definim $i_S:A\to A_S$ prin $i_S(a)=\frac{a}{1}$ pentru orice $a\in A$. Dacă $a,b\in A$, atunci

$$i_S(a)+i_S(b)=\frac{a}{1}+\frac{b}{1}=\frac{a+b}{1}=i_S(a+b),$$

$$i_S(a)\cdot i_S(b)=\frac{a}{1}\cdot\frac{b}{1}=\frac{ab}{1}=i_S(ab)$$

iar $i_S(1)=\frac{1}{1}=1$, de unde concluzia că i_S este morfism de inele unitare.

Dacă $i_S(a)=i_S(b) \Rightarrow \alpha=\frac{a}{1}=\frac{b}{1} \Rightarrow a\cdot 1=b\cdot 1 \Rightarrow a=b$, adică i_S este morfism injectiv de inele.

Dacă $s\in S$, cum $i_S(s)=\frac{s}{1}$ iar $\frac{s}{1}\cdot\frac{1}{s}=\frac{s}{s}=1$, deducem că $i_S(s)\in U(A_S)$ (probând astfel 1) din enunț). Astfel, dacă $\alpha\in A_S$, $\alpha=\frac{a}{s}$ cu $a\in A$ şi $s\in S$ scriind $\alpha=\frac{a}{1}\cdot\frac{1}{s}= i_S(a)\ (i_S(s))^{-1}$ răspundem astfel la chestiunea 2) din enunț.

Pentru a soluționa şi chestiunea 3), fie B un inel cu proprietățile din enunț şi $\alpha=\frac{a}{s}\in A_S$. Definim $j(\alpha)=i(a)(i(s))^{-1}$.

Dacă mai avem $a'\in A$ şi $s'\in S$ a.î. $\alpha=\frac{a}{s}=\frac{a'}{s'}$, atunci $as'=a's \Rightarrow$ $\Rightarrow i(a)i(s')=i(a')i(s) \Rightarrow i(a)(i(s))^{-1}=i(a')(i(s'))^{-1}$, adică j este corect definită. Dacă $a\in A$, atunci $j(i_S(a))=j(\frac{a}{1})=i(a)(i(1))^{-1}=i(a)$ adică $j\circ i_S=i$.

Fie acum $\alpha=\frac{a}{s}$ şi $\beta=\frac{a'}{s'}$ două elemente din A_S. Atunci $\alpha+\beta=\frac{as'+a's}{ss'}$ şi $\alpha\beta=\frac{aa'}{ss'}$, astfel că:

$j(\alpha+\beta)=i(as'+a's)(i(ss'))^{-1}=(i(a)i(s')+i(a')i(s))\cdot[i(s)i(s')]^{-1}=$
$=i(a)i(s')(i(s))^{-1}(i(s'))^{-1}+i(a')i(s)(i(s))^{-1}(i(s'))^{-1}=i(a)(i(s))^{-1}+i(a')(i(s'))^{-1}=$
$=j(\alpha)+j(\beta)$
$j(\alpha\beta)=i(aa')(i(ss'))^{-1}=i(a)i(a')(i(s))^{-1}(i(s'))^{-1}=(i(a)(i(s))^{-1})\cdot(i(a')(i(s'))^{-1})=$
$=j(\alpha)j(\beta)$ şi $j(1)=j(\frac{1}{1})=i(1)\ (i(1))^{-1}=1$, de unde concluzia că j este morfism de inele unitare.

Dacă mai avem un morfism de inele unitare $k:A_S\to B$ a.î. $k\circ i_S=i$ atunci pentru $\alpha\in A_S$, conform cu 1) există $a\in A$ şi $s\in S$ a.î. $\alpha=i_S(a)(i_S(s))^{-1}$.

Atunci $k(\alpha)=k(i_S(a)(i_S(s))^{-1})=k(i_S(a))(k(i_S(s)))^{-1}=$
$=(k\circ i_S)(a)((k\circ i_S)(s))^{-1}=i(a)(i(s))^{-1}=j(\alpha)$, de unde deducem că $j=k$.■

Definiția 6.3. Inelul A_S din Teorema 6.2. poartă numele de *inelul de fracții al lui A relativ la sistemul multiplicativ S* (sau cu numitorii în S) şi se mai notează şi prin $S^{-1}A$.

Dacă S este mulțimea tuturor nondivizorilor lui zero, atunci A_S se numeşte *inelul total de fracții al lui A*.

Observația 6.4. Să presupunem că A este domeniu de integritate (adică este comutativ şi nu are divizori ai lui zero diferiți de 0). Considerând $S=A^*=A\setminus\{0\}$, atunci dacă $\frac{a}{s}\in A^*_S$ deducem că $\alpha\in A^*$, deci $\frac{s}{a}\in A_S$. Din $\frac{a}{s}\cdot\frac{s}{a}=\frac{as}{as}=\frac{1}{1}=1$ deducem că $\frac{s}{a}=(\frac{a}{s})^{-1}$, adică A_S este corp, numit *corpul total de fracții al domeniului de integritate A*.

Definiția 6.5. Corpul total de fracții al inelului $(\mathbb{Z}, +, \cdot)$ se notează prin $\mathbb{Q}$ şi poartă numele de *corpul numerelor raționale*.

În continuare, pornind de la corpul numerelor raționale $(\mathbb{Q}, +, \cdot)$ vom construi corpul numerelor reale $(\mathbb{R}, +, \cdot)$.

§7. Construcția corpului $\mathbb{R}$ al numerelor reale

Relațiile de ordine de pe inelul $\mathbb{Z}$ şi corpul $\mathbb{Q}$ se înscriu într-un context mai general pe care îl vom prezenta în cele ce urmează şi care ne va fi de folos şi pentru ordinea naturală de pe mulțimea numerelor reale $\mathbb{R}$.

Definiția 7.1. Dacă A este un domeniu de integritate (adică un inel comutativ unitar fără divizori ai lui zero), prin *ordonare* pe A înțelegem o submulțime nevidă $P\subseteq A$ a.î. :

Ord 1: Pentru orice $x\in A$ avem în mod exclusiv $x\in P$ sau $x=0$ sau $-x\in P$

Ord 2: Dacă x, y∈P atunci x+y, xy∈P.

În acest caz vom spune că inelul A este *ordonat* de P iar P este mulțimea elementelor *pozitive* ale lui A.

Să presupunem acum că A este ordonat de P. Cum $1\neq 0$ şi $1=1^2=(-1)^2$ deducem că $1\in P$ (adică 1 este pozitiv).

Ținând cont de **Ord 2** deducem inductiv că pentru orice $n\in\mathbb{N}^*$, $\underbrace{1+1+\ldots+1}_{de\ n\ ori}$ este pozitiv.

Un element $x\in A$, $x\neq 0$, $x\notin P$ (adică $-x\in P$) se zice *negativ* .

Dacă x, y∈A sunt negative, atunci xy este pozitiv (căci –x, $-y\in P$ iar $(-x)(-y)=xy\in P$).

Analog deducem că dacă x este negativ iar y este pozitiv, atunci xy este negativ şi că pentru orice $x\neq 0$ din A, x^2 este pozitiv.

Dacă A este corp, cum pentru $x\neq 0$ pozitiv avem $xx^{-1}=1$ deducem că şi x^{-1} este pozitiv**.**

Fie acum $A'\subseteq A$ un subinel iar $P'=P\cap A'$. Se verifică imediat că A′ este ordonat de P′ (P′ se va numi *ordonarea indusă* de P pe A′) .

Mai general, fie A′, A două inele ordonate iar P′, P respectiv mulțimile elementelor pozitive din A′ şi A .

Dacă $f:A'\to A$ este un morfism injectiv de inele, vom spune că f *păstrează ordinea* dacă pentru orice $x\in P'$ deducem că $f(x)\in P$ (echivalent cu a zice că $P'\subseteq f^{-1}(P)$).

Fie acum x, y∈A. Definim $x<y$ (sau $y>x$) prin $y-x\in P$.

Astfel $x>0$ înseamnă $x\in P$ iar $x<0$ înseamnă că $-x\in P$ (spunem atunci că x este *negativ*).

Se verifică imediat că dacă x, y, z∈A, atunci :

IN_1: Dacă $x<y$ şi $y<z$, atunci $x<z$.

IN_2: Dacă $x<y$ şi $z>0$, atunci $xz<yz$.

IN_3: Dacă $x<y$ atunci $x+z<y+z$.

IN_4: Dacă A este corp, $x>0$, $y>0$ şi $x<y$ atunci $y^{-1}<x^{-1}$.

Dacă x, y∈A definim x≤y prin x<y sau x=y. Fie acum A un domeniu de integritate ordonat de P iar K corpul său total de fracții.

Dacă $P_K=\{\frac{a}{b}\in K|\ a, b>0\ \}$, atunci P_K defineşte o ordonare pe K. Într-adevăr, dacă x∈K, x≠0, $x=\frac{a}{b}$ atunci putem presupune că b>0 (deoarece $x=\frac{a}{b}=\frac{-a}{-b}$). Dacă a>0, atunci $x\in P_K$. Dacă –a>0 atunci $-x=\frac{-a}{b}\in P_K$.

Nu putem avea simultan $x,-x\in P_K$ căci scriind $x=\frac{a}{b}$ şi $-x=\frac{c}{d}$, cu a, b, c, d∈A şi a, b, c, d >0, atunci $-\frac{a}{b}=\frac{c}{d}$ deci –(ad)=bc, absurd (căci bc∈P şi ad∈P). Deci P_K satisface **Ord 1.**

Cum $xy=\frac{ac}{bd}$ (iar ac, bd >0) şi $x+y=\frac{ad+bc}{bd}$ (iar ad+bc, bd>0) deducem că P_K satisface şi **Ord 2** .

Observația 7.2. $\mathbb{N}^*$ **este o ordonare pe** $\mathbb{Z}$**.**

Fie acum A un inel ordonat. Pentru x∈A definim :

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

(|x| poartă numele de *valoarea absolută* sau *modulul* lui x).

Lema 7.3. Pentru orice x ∈A, | x | este unicul element z∈A a.î. z≥0 şi $z^2=x^2$.

Demonstrație Să observăm că $|x|^2=x^2$ şi |x| ≥0 pentru orice x∈A. Pe de altă parte, dacă a∈A şi a >0 atunci există cel mult două elemente z∈A a.î. $z^2=a$ (căci conform Corolarului 4.9. de la Capitolul 4,

polinomul $X^2-a\in A[X]$ are cel mult două rădăcini în A). Dacă $w^2=a$, atunci $w\neq 0$ şi $(-w)^2=w^2=a$, deci există cel mult un $z\in A$ pozitiv a.î. $z^2=a$ şi cu aceasta lema este probată . ■

Definiția 7.4. Pentru a ≥ 0, definim elementul $\sqrt{a}$ ca fiind acel element z ≥ 0 a.î. $z^2=a$ (evident, dacă un astfel de z există !).

Se verifică acum uşor că dacă pentru a, b $\geq 0, \sqrt{a}, \sqrt{b}$ există, atunci $\sqrt{ab}$ există şi $\sqrt{ab}=\sqrt{a}\cdot\sqrt{b}$.

Evident, pentru orice $x\in A$, $|x|=\sqrt{x^2}$.

Lema 7.5. Dacă A este un inel ordonat, atunci

VA_1: Pentru orice $x\in A$, $|x|\geq 0$, iar $|x|>0$ dacă $x\neq 0$

VA_2 : Pentru orice $x, y\in A$, $|xy|=|x|\cdot|y|$

VA_3 : Pentru orice $x, y\in A$, $|x+y|\leq |x|+|y|$.

Demonstrație. Cum VA_1 şi VA_2 sunt imediate, să probăm pe VA_3 : $|x+y|^2=(x+y)^2=x^2+2xy+y^2\leq |x|^2+2|xy|+|y|^2=$
$=|x|^2+2|x|\cdot|y|+|y|^2=(|x|+|y|)^2$, de unde $|x+y|\leq |x|+|y|$. ■

Fie acum K un corp comutativ ordonat pentru care există un morfism (injectiv) de corpuri $f:\mathbb{Q}\to K$ (deci K va fi de caracteristică 0).

Se arată imediat că dacă $x\in\mathbb{Z}$, atunci

$$f(x)=\begin{cases}\underbrace{1_K+\ldots+1_K}_{de\ x\ ori}, & \text{dacă } x\geq 0\\ 0, & \text{dacă } x=0\\ \underbrace{(-1_K)+\ldots+(-1_K)}_{de\ -x\ ori}, & \text{dacă } x<0\end{cases}.$$

Mai mult, dacă $x\in\mathbb{Z}^*$, cum în $\mathbb{Q}$ avem $x\cdot\frac{1}{x}=1$ deducem că $1_K=f(1)=f\left(x\cdot\frac{1}{x}\right)=f(x)\cdot f\left(\frac{1}{x}\right)$, de unde $f\left(\frac{1}{x}\right)=f(x)^{-1}$ în K. Atunci dacă $x=\frac{m}{n}\in\mathbb{Q}$ avem $f(x)=f\left(\frac{m}{n}\right)=f\left(m\cdot\frac{1}{n}\right)=m\cdot f\left(\frac{1}{n}\right)=m\cdot\left(n\cdot 1_K\right)^{-1}$. Rezultă că f este unic determinat ; vom identifica atunci pe $\mathbb{Q}$ cu un subcorp al lui K (f se va numi scufundarea canonică a lui $\mathbb{Q}$ în K).

Dacă $x=\frac{m}{n}$, $y=\frac{m'}{n'}\in\mathbb{Q}$ (cu n, n′>0) şi x≤y, atunci mn′-m′n≤0, deci m′n-mn′≥0, iar $f(x)=m(n1_K)^{-1}$, $f(y)=m'(n'1_K)^{-1}$. Din m′n-mn′≥0 şi $1_K\geq 0$ deducem că $(m'n-mn')1_K\geq 0 \Leftrightarrow m'(n1_K)-m(n'1_K)\geq 0 \Leftrightarrow m'(n1_K)\geq m(n'1_K)$, de unde $m'(n'1_K)^{-1}\geq m(n\,1_K)^{-1}\Leftrightarrow f(y)\geq f(x)$.

Obținem astfel următorul rezultat :

Teorema 7.6. Dacă K este un corp ordonat de caracteristică 0, atunci scufundarea canonică a lui $\mathbb{Q}$ în K, f :$\mathbb{Q}\to$K, $f\left(\frac{m}{n}\right)=m\cdot\left(n\cdot 1_K\right)^{-1}$, (cu n>0) păstrează ordinea.

În continuare prin K vom desemna un corp comutativ ordonat de caracteristică 0 iar un element $x\in\mathbb{Z}$ îl vom identifica cu $f(x)=x\cdot 1_K$.

Definiția 7.7. Un şir de elemente $(x_n)_{n\geq 0}$ din K se zice *şir Cauchy* dacă pentru orice $\varepsilon\in$K, ε>0, există $n_\varepsilon\in\mathbb{N}$ a.î. pentru orice m, n$\in\mathbb{N}$, m, n≥n_ε să avem $|x_n-x_m|<\varepsilon$.

Vom spune despre şirul $(x_n)_{n\geq 0}$ că este *convergent* la un element x∈K, dacă pentru orice ε∈K, ε>0, există $n_\varepsilon\in\mathbb{N}$ a.î. pentru orice n≥n_ε să avem $|x_n-x|<\varepsilon$.

Observaţia 7. 8.

1.Să presupunem că şirul $(x_n)_{n\geq 0}$ este convergent la două elemente x,y∈K. Atunci pentru ε∈K, ε>0 şi n∈ℕ* suficient de mare avem :

$$| x-y | \leq | x-x_n + x_n-y | \leq | x-x_n | + | x_n - y | \leq 2\varepsilon$$

iar cum ε este oarecare deducem că | x-y |=0 (căci dacă | x-y |≠0, atunci | x-y | >0 şi am avea | x-y |< | x-y | , absurd !).

Dacă $(x_n)_{n\geq 0}$ este convergent la un element x∈K, vom scrie

$$x = \lim_{n\to\infty} x_n .$$

2. Orice şir convergent este şir Cauchy.

Definiţia 7.9. Corpul ordonat K în care orice şir Cauchy este convergent se zice *complet* .

Definiţia 7.10. Corpul ordonat K se numeşte *arhimedean* dacă pentru orice x∈K, există n∈ℕ a.î. $x \leq n\cdot 1_K$.

Teorema 7.11. Corpul ℚ al numerelor raţionale nu este complet .

Demonstraţie. Într-adevăr, să considerăm şirul $(x_n)_{n\geq 0}$ de numere raţionale dat prin $x_0=1$ şi $x_{n+1} = \frac{4+3x_n}{3+2x_n}$ pentru orice n≥0. Prin inducţie matematică relativă la n se probează că $x_n^2<2$, şi că $(x_n)_{n\geq 0}$ este crescător (căci $x_{n+1} - x_n = \frac{4+3x_n}{3+2x_n} - x_n = \frac{2\left(2-x_n^{\,2}\right)}{3+2x_n} > 0$) iar de aici că el este şir Cauchy.

Dacă acest şir ar avea limita $l\in\mathbb{Q}$, atunci cu necesitate $l = \frac{4+3l}{3+2l}$, de unde $l^2=2$, absurd căci $l\notin\mathbb{Q}$. Deci $(x_n)_{n\geq 0}$ nu are limită în ℚ, adică corpul ℚ nu este complet. ■

Pentru K corp ordonat şi $S \subseteq K$, prin *majorant* al lui S în K înțelegem un element $z \in K$ a.î. $x \leq z$, pentru orice $x \in S$.

Prin marginea superioară a lui S, notată prin sup(S) înțelegem cel mai mic majorant al lui S din K (evident dacă acesta există).

Teorema 7.12. Fie K un corp arhimedean complet. Atunci orice submulțime nevidă S a lui K ce admite un majorant are margine superioară.

Demonstrație. Pentru $n \in \mathbb{N}$, fie

$$T_n = \{y \in \mathbb{Z} \mid ny \leq x \text{ pentru orice } x \in S\}.$$

Atunci T_n este mărginită de orice element de forma nx cu $x \in S$ şi este nevidă deoarece dacă b este un majorant al lui S, atunci orice întreg y a.î. $nb \leq y$ este în T_n (deoarece K este arhimedean) .

Fie y_n cel mai mic element al lui T_n. Atunci există $x_n \in S$ a.î. $y_n - 1 < nx_n \leq y_n$, de unde $\frac{y_n}{n} - \frac{1}{n} < x_n \leq \frac{y_n}{n}$.

Să notăm $z_n = \frac{y_n}{n}$ şi să demonstrăm că şirul $(z_n)_{n \in \mathbb{N}}$ este Cauchy. Pentru aceasta fie m, $n \in \mathbb{N}$ a.î. $\frac{y_n}{n} \leq \frac{y_m}{m}$ atunci $\frac{y_m}{m} - \frac{1}{m} < \frac{y_n}{n} \leq \frac{y_m}{m}$ căci în caz contrar, $\frac{y_n}{n} \leq \frac{y_m}{m} - \frac{1}{m}$, deci $\frac{y_m}{m} - \frac{1}{m}$ este majorant pentru S, ceea ce este absurd căci x_m este mai mare.

Atunci $\left| \frac{y_n}{n} - \frac{y_m}{m} \right| \leq \frac{1}{n}$ de unde deducem că $(z_n)_{n \in \mathbb{N}}$ este Cauchy.

Fie $w = \lim_{n \to \infty} z_n$ şi să demonstrăm la început că w este un majorant pentru S.

Să presupunem prin absurd că există $x \in S$ a.î. $w < x$. Există atunci $n \in \mathbb{N}$ a.î. $| z_n - w | \leq \frac{x - w}{2}$ astfel că $x - z_n = x - w + w - z_n \geq x - w -$

$-|\ w-z_n\ | \geq x-w-\frac{x-w}{2} \geq \frac{x-w}{2} > 0$ deci $x > z_n$ contrazicând faptul că z_n este majorant al lui S.

Să demonstrăm acum că $w = \sup S$.

Fie $u < w$; atunci există $n \in \mathbb{N}$ suficient de mare a.î. $|\ z_n - x_n\ | \leq \frac{1}{4} < \frac{w-u}{4}$.

Putem alege n suficient de mare a.î. $|\ z_n - w\ | \leq \frac{w-u}{4}$ căci $\lim_{n\to\infty} z_n = w$.

Astfel, $x_n - u = w-u+x_n-z_n+z_n-w \geq w-u-|\ x_n-z_n\ |-|\ z_n-w\ | \geq$

$\geq w-u-\frac{w-u}{4}-\frac{w-u}{4} \geq \frac{w-u}{4} > 0$, deci $u < x_n$ (adică u nu este majorant– absurd !). ■

În continuare vom prezenta construcția *corpului numerelor reale cu ajutorul şirurilor Cauchy de numere raționale* (definite mai înainte într-un context mai general).

Definiția 7.13. Un şir de numere raționale $\gamma=(c_n)_{n\geq 0}$ se zice *şir nul* dacă pentru orice $\varepsilon \in \mathbb{Q}$, $\varepsilon > 0$, există $n_\varepsilon \in \mathbb{N}$ a.î. pentru orice $n \geq n_\varepsilon$, $|\ c_n\ | \leq \varepsilon$ (adică $\lim_{n\to\infty} c_n = 0$).

Dacă $\alpha=(a_n)_{n\geq 0}$ şi $\beta=(b_n)_{n\geq 0}$ sunt două şiruri de numere raționale, definim suma şi produsul lor prin $\alpha+\beta=(a_n+b_n)_{n\geq 0}$ şi respectiv $\alpha\beta=(a_n b_n)_{n\geq 0}$

Lema 7.14. Orice şir Cauchy $\alpha=(a_n)_{n\geq 0}$ de numere raționale este mărginit.

Demonstrație. Există $k \in \mathbb{N}$ a.î. pentru orice $n \geq k$, $|\ a_n - a_k\ | \leq 1$, de unde $|\ a_n\ | \leq |a_k|+1$. Alegând $M = \max(|\ a_0\ |, \ldots, |a_{k-1}|, |\ a_k\ |+1)$ deducem că $|a_n\ | \leq M$ pentru orice $n \in \mathbb{N}$. ■

În cele ce urmează prin $\mathbf{C}(\mathbb{Q})$ vom nota mulțimea șirurilor Cauchy de numere raționale.

Propoziția 7.15. $(\mathbf{C}(\mathbb{Q}), +, \cdot)$ este inel unitar comutativ.

Demonstrație. Fie $\alpha=(x_n)_{n\geq 0}$, $\beta=(y_n)_{n\geq 0}$, $\mathbf{0}=(0, 0, \ldots)$ și $\mathbf{1}=(1, 1, \ldots)$. Să demonstrăm la început că $\alpha+\beta$ și $\alpha\beta$ sunt din $\mathbf{C}(\mathbb{Q})$.

Pentru $\varepsilon\in\mathbb{Q}_+^*$, există $n_\varepsilon', n_\varepsilon''\in\mathbb{N}$ a.î. pentru orice $m, n \geq n_\varepsilon'$ să avem $|x_m-x_n|<\frac{\varepsilon}{2}$ și pentru orice $m, n \geq n_\varepsilon''$, $|y_m-y_n|<\frac{\varepsilon}{2}$. Alegând $n_\varepsilon=\max(n_\varepsilon', n_\varepsilon'')$, deducem că pentru orice $m, n \geq n_\varepsilon$, $|x_m-x_n|$, $|y_m-y_n|<\frac{\varepsilon}{2}$, astfel că $|(x_m+y_m)-(x_n+y_n)|=|(x_m-x_n)+(y_m-y_n)| \leq$ $\leq|x_m-x_n|+|y_m-y_n|<\frac{\varepsilon}{2}+\frac{\varepsilon}{2}=\varepsilon$, adică $\alpha+\beta\in\mathbf{C}(\mathbb{Q})$.

Pentru cazul produsului $\alpha\beta$ vom ține cont de Lema 7.14. Conform acesteia, există $M_1, M_2\in\mathbb{Q}_+^*$ a.î. $|x_n|\leq M_1$ și $|y_n|\leq M_2$ pentru orice $n\in\mathbb{N}$.

Notând $M=\max(M_1, M_2)$ și alegând $\varepsilon\in\mathbb{Q}_+^*$, există $n_\varepsilon', n_\varepsilon''\in\mathbb{N}$ a.î.

$$|x_m-x_n|\leq\frac{\varepsilon}{2M}, \text{ pentru } m, n \geq n_\varepsilon' \text{ și}$$

$$|y_m-y_n|\leq\frac{\varepsilon}{2M}, \text{ pentru } m, n \geq n_\varepsilon''.$$

Astfel, pentru $m, n \geq n_\varepsilon=\max(n_\varepsilon', n_\varepsilon'')$, avem

$|x_my_m-x_ny_n|=|x_m(y_m-y_n)+y_n(x_m-x_n)|=|x_m||y_m-y_n|+|y_n||x_m-x_n| \leq$

$\leq M\cdot\frac{\varepsilon}{2M}+M\cdot\frac{\varepsilon}{2M}=\varepsilon$, adică și $\alpha\beta\in\mathbf{C}(\mathbb{Q})$.

În mod evident, $-\alpha=(-x_n)_{n\geq 0}\in\mathbf{C}(\mathbb{Q})$ ca și $\mathbf{0}, \mathbf{1}\in\mathbf{C}(\mathbb{Q})$.

Deducem acum imediat că $(\mathbf{C}(\mathbb{Q}), +, \cdot)$ este inel comutativ și unitar. ■

În continuare, vom nota prin

$$\mathbf{N}(\mathbb{Q})=\{(x_n)_{n\geq 0}\in \mathbf{C}(\mathbb{Q}) \mid \lim_{n\to\infty} x_n = 0\}\ .$$

Lema 7.16. N(ℚ) este ideal al inelului C(ℚ).

Demonstrație. Analog ca în cazul sumei din propoziția precedentă, se demonstrează imediat că dacă $\alpha, \beta\in\mathbf{N}(\mathbb{Q})$, atunci $\alpha-\beta\in\mathbf{N}(\mathbb{Q})$.

Fie acum $\alpha=(a_n)_{n\geq 0}\in\mathbf{C}(\mathbb{Q})$ şi $\beta=(b_n)_{n\geq 0}\in\mathbf{N}(\mathbb{Q})$. Conform Lemei 7.14. există $M\in\mathbb{Q}_+^*$ a.î. $|a_n|\leq M$ pentru orice $n\in\mathbb{N}$.

Deoarece $\beta=(b_n)_{n\geq 0}\in\mathbf{N}(\mathbb{Q})$ pentru $\varepsilon\in\mathbb{Q}_+^*$, există $n_\varepsilon\in\mathbb{N}$ a.î. pentru orice $n\geq n_\varepsilon$ să avem $|b_n|\leq\frac{\varepsilon}{M}$.

Atunci pentru $n\geq n_\varepsilon$, $|a_n b_n|=|a_n||b_n|\leq M\cdot\frac{\varepsilon}{M}=\varepsilon$, astfel că $\alpha\beta\in\mathbf{N}(\mathbb{Q})$, adică $\mathbf{N}(\mathbb{Q})$ este ideal al inelului comutativ $\mathbf{C}(\mathbb{Q})$. ■

Lema 7.17. Fie $\alpha\in\mathbf{C}(\mathbb{Q})$ a.î. $\alpha\notin\mathbf{N}(\mathbb{Q})$, $\alpha=(a_n)_{n\geq 0}$. Atunci există $c\in\mathbb{Q}_+^*$ şi $n_0\in\mathbb{N}$ a.î. pentru orice $n\geq n_0$, $|a_n|\geq c$.

Demonstrație. Dacă prin absurd lema nu ar fi adevărată, atunci pentru $\varepsilon\in\mathbb{Q}_+^*$ există o infinitate de numere naturale $n_1<n_2<\ldots$ a.î. $|a_{n_i}|<\frac{\varepsilon}{3}$ pentru orice $i\geq 1$.

Cum $\alpha\in\mathbf{C}(\mathbb{Q})$, există $p\in\mathbb{N}$ a.î. pentru orice m, $n\geq p$ să avem $|a_n-a_m|\leq\frac{\varepsilon}{3}$. Fie $n_i\geq p$; atunci pentru orice $m\geq p$, $|a_m|\leq|a_m-a_{n_i}|+|a_{n_i}|\leq\frac{2\varepsilon}{3}$ şi pentru orice m, $n\geq p$, $|a_n|\leq|a_n-a_m|+|a_m|\leq\frac{\varepsilon}{3}+\frac{2\varepsilon}{3}=\varepsilon$, adică $\alpha\in\mathbf{N}(\mathbb{Q})$, absurd ! . ■

Teorema 7.18. (C(ℚ) / N(ℚ) , +, ·) este corp comutativ.

Demonstrație. Faptul că **C(ℚ) / N(ℚ)** este inel comutativ rezultă din aceea că **C(ℚ)** este inel comutativ iar **N(ℚ)** este ideal în **C(ℚ)** (vezi §4).

Fie acum $\alpha \in \mathbf{C}(\mathbb{Q})$ a.î. $\alpha \notin \mathbf{N}(\mathbb{Q})$ şi $\overline{\alpha} = \alpha + \mathbf{N}(\mathbb{Q}) \in \mathbf{C}(\mathbb{Q}) / \mathbf{N}(\mathbb{Q})$. Vom demonstra că există $\overline{\beta} \in \mathbf{C}(\mathbb{Q})/\mathbf{N}(\mathbb{Q})$ a.î. $\overline{\alpha} \cdot \overline{\beta} = \overline{1}$, unde $\overline{1} = \mathbf{1} + \mathbf{N}(\mathbb{Q})$ (reamintim că $\mathbf{1} = (1, 1, \ldots) \in \mathbf{C}(\mathbb{Q})$).

Cum $\alpha \notin \mathbf{N}(\mathbb{Q})$, conform Lemei 7.17. există $\varepsilon \in \mathbb{Q}_+^*$ şi $n_0 \in \mathbb{N}$ a.î. pentru orice $n \geq n_0$, $|a_n| \geq \varepsilon$. În particular, deducem că pentru $n \geq n_0$, $a_n \neq 0$.

Fie $\beta = (b_n)_{n \geq 0}$ cu

$$b_n = \begin{cases} 1 & \text{dacă } 0 \leq n \leq n_0 \\ a_n^{-1} & \text{dacă } n \geq n_0 \end{cases}$$

Să arătăm că $\beta \in \mathbf{C}(\mathbb{Q})$ şi că $\overline{\alpha} \cdot \overline{\beta} = \overline{1}$.

Putem alege deci $c \in \mathbb{Q}_+^*$ şi $n_0 \in \mathbb{N}$ a.î. pentru orice $n \geq n_0$, $|a_n| \geq c > 0$; de unde va rezulta că $\frac{1}{|a_n|} \leq \frac{1}{c}$.

Pentru $\varepsilon \in \mathbb{Q}_+^*$ există $p \geq n_0$ a.î. pentru orice m, n ≥ p să avem

$$|a_n - a_m| \leq \varepsilon c^2 .$$

Atunci pentru orice m, n ≥ p avem

$$\left| \frac{1}{a_n} - \frac{1}{a_m} \right| = \left| \frac{a_m - a_n}{a_m \cdot a_n} \right| \leq \frac{\varepsilon \cdot c^2}{c^2} = \varepsilon \text{ , adică } \beta \in \mathbf{C}(\mathbb{Q}).$$

Cum $\alpha\beta$ diferă de **1** numai într-un număr finit de termeni (eventual pentru $n \leq n_0$) deducem că $\alpha\beta - \mathbf{1} \in \mathbf{N}(\mathbb{Q})$, adică $\overline{\alpha} \cdot \overline{\beta} = \overline{1}$, deci $\overline{\beta} = \left(\overline{\alpha}\right)^{-1}$, adică **C(ℚ) / N(ℚ)** este corp . ■

Definiția 7.19. Mulțimea C(ℚ) / N(ℚ) se notează prin ℝ şi poartă numele de *mulțimea numerelor reale.*

Corpul (ℝ,+, ·) poartă numele de *corpul numerelor reale*.

Deoarece se probează imediat că funcția $i_{\mathbb{Q}}:\mathbb{Q}\to\mathbb{R}$, $i_{\mathbb{Q}}(a) = \overline{(a,a,....)}$ pentru orice $a \in\mathbb{Q}$ este morfism de corpuri (deci în particular funcție injectivă) putem privi pe ℚ ca subcorp al lui ℝ.

Elementele din $\mathbf{I}=\mathbb{R}\setminus\mathbb{Q}$ se zic *numere iraționale.*

Lema 7.20. Pentru $\alpha=(a_n)_{n\geq 0} \in \mathbf{C}(\mathbb{Q})$ este verificată doar una din condițiile :

(1) $\alpha\in\mathbf{N}(\mathbb{Q})$

(2) Există $c\in\mathbb{Q}_+^*$ a.î. pentru n suficient de mare să avem $a_n \geq c$

(3)Există $c\in\mathbb{Q}_+^*$ a.î. pentru n suficient de mare să avem $a_n \leq -c$

Demonstrație. Evident (2) şi (3) se exclud reciproc.

Să presupunem acum că $\alpha\notin\mathbf{N}(\mathbb{Q})$. Conform Lemei 7.20. există $n_0\in\mathbb{N}$ şi $c\in\mathbb{Q}_+^*$ a.î. pentru orice $n \geq n_0$, $|a_n| \geq c$ astfel că $a_n \geq c$ dacă $a_n > 0$ şi $a_n \leq -c$ dacă $a_n<0$.

Să presupunem acum că $a_n>0$ pentru suficient de mulți n şi $a_m<0$ pentru suficient de mulți m. Pentru astfel de n şi m avem $a_n-a_m\geq 2c>0$ ceea ce contrazice faptul că $\alpha\in\mathbf{C}(\mathbb{Q})$.

Deci (2) sau (3) în sens disjunctiv trebuie să aibă loc . ■

Fie $P=\{\overline{\alpha} \mid \alpha\in\mathbf{C}(\mathbb{Q})$ şi verifică (2) din Lema 7.20.$\}\subseteq\mathbb{R}$

Lema 7.21. P este o ordonare pe ℝ.

Demonstrație. Conform Lemei 7.20. deducem că P satisface **Ord 1**.

Fie acum $\alpha=(a_n)_{n\geq 0}$ şi $\beta=(b_n)_{n\geq 0} \in\mathbf{C}(\mathbb{Q})$ a.î. $\overline{\alpha},\overline{\beta}\in P$.

Există $c_1, c_2\in\mathbb{Q}_+^*$ şi $n_1, n_2\in\mathbb{N}$ a.î. pentru $n\geq n_1$, $a_n \geq c_1$ şi pentru $n\geq n_2$, $b_n \geq c_2$.

Pentru $n \geq \max(n_1, n_2)$, $a_n+b_n \geq c_1+c_2 >0$ şi $a_nb_n \geq c_1c_2 >0$ astfel că $\alpha+\beta$, $\alpha\beta$ verifică (2) din Lema 7.20., adică $\overline{\alpha}+\overline{\beta}, \overline{\alpha}\cdot\overline{\beta} \in P$, deci P satisface şi **Ord 2**.

Observaţia 7.22.

1. Din cele de mai sus deducem că dacă $\overline{\alpha}, \overline{\beta} \in \mathbb{R}$, $\alpha=(x_n)_{n\geq 0}$, $\beta=(y_n)_{n\geq 0}$, atunci $\overline{\alpha} \leq \overline{\beta}$ este echivalent cu aceea că $\overline{\beta}-\overline{\alpha} \in P$, adică $\overline{(\beta-\alpha)} \in P$, deci cu existenţa lui $n_0 \in \mathbb{N}$ şi $c \in \mathbb{Q}_+^*$ a.î. $y_n-x_n \geq c$ pentru orice $n \geq n_0$.

Convenim să numim ordinea de mai înainte *ordonarea naturală* de pe $\mathbb{R}$.

2. Pentru $a \in \mathbb{Q}$ convenim să notăm pe $i_{\mathbb{Q}}(a)$ prin $\overline{a}$, adică $\overline{a} = \overline{(a, a, ...)}$.

Teorema 7.23. Ordonarea naturală de pe $\mathbb{R}$ (dată de P) este arhimedeană.

Demonstraţie. Conform Definiţiei 7.10., pentru $\alpha=(a_n)_{n\geq 0} \in C(\mathbb{Q})$ va trebui să demonstrăm că există $m_\alpha \in \mathbb{N}$ a.î. $\overline{\alpha} \leq \overline{m_\alpha}$. Conform Lemei 7.14. există $M \in \mathbb{Q}_+^*$ a.î. $a_n \leq M$ pentru orice $n \in \mathbb{N}$. Alegând $m_\alpha \in \mathbb{N}$ a.î. $M \leq m_\alpha$ deducem că $a_n \leq m_\alpha$ pentru orice $n \in \mathbb{N}$, adică $\overline{\alpha} \leq \overline{m_\alpha}$. ■

Următorul rezultat este imediat.

Lema 7.24. Dacă $\alpha=(a_n)_{n\geq 0} \in C(\mathbb{Q})$ şi există $c \in \mathbb{Q}_+^*$ şi $n_0 \in \mathbb{N}$ a.î. pentru orice $n \geq n_0$, $|a_n| \leq c$, atunci $\left|\overline{\alpha}\right| \leq \overline{c}$.

Observaţie 7.25. Conform Teoremei 7.23., fiind dat $\varepsilon \in \mathbb{R}$, $\varepsilon>0$, există $\varepsilon_1 \in \mathbb{Q}_+^*$ a.î. $\varepsilon<\varepsilon_1$ astfel că în definiţia limitei unui şir din $\mathbb{R}$ nu contează dacă ε este real sau raţional.

Lema 7.26. Fie $\alpha=(a_n)_{n\geq 0} \in C(\mathbb{Q})$. Atunci $\overline{\alpha} = \lim\limits_{n\to\infty} \overline{a_n}$ (adică orice şir Cauchy de numere raţionale converge în $\mathbb{R}$).

Demonstrație. Fie $\varepsilon\in\mathbb{Q}_+^*$. Există $n_0\in\mathbb{N}$ a.î. pentru orice m, n $\geq$ n_0, $|a_m - a_n| \leq \varepsilon$. Atunci pentru $m\geq n_0$ avem $|\overline{\alpha} - \overline{a_m}| = \left|\overline{\alpha - a_m}\right| \leq \overline{\varepsilon}$ (căci $\alpha - a_m = (a_n - a_m)_{n\geq 0}$), adică $\overline{\alpha} = \lim_{n\to\infty} \overline{a_n}$. ■

Teorema 7.27. Corpul $\mathbb{R}$ este complet .

Demonstrație. Fie $(x_n)_{n\geq 0}$ un şir Cauchy de numere reale.

Conform Lemei 7.26., pentru orice $n\in\mathbb{N}$ găsim $a_n\in\mathbb{Q}$ a.î. $|x_n - \overline{a_n}| < \frac{1}{n}$ (în partea dreaptă este vorba de fapt de $(\overline{n})^{-1}$!)

Cum $(x_n)_{n\geq 0}$ este Cauchy, deducem că fiind dat $\varepsilon>0$ (de exemplu $\varepsilon\in\mathbb{Q}$) există $n_0\in\mathbb{N}$ a.î. pentru orice m, n $\geq$ n_0 să avem $|x_n - x_m| \leq \frac{\varepsilon}{3}$.

Fie $n_1\in\mathbb{N}$, $n_1\geq n_0$ a.î. $\frac{1}{n_1} \leq \frac{\varepsilon}{3}$. Atunci pentru orice m, n $\geq$ n_1 avem

$$\left|\overline{a_n} - \overline{a_m}\right| = \left|\overline{a_n} - x_n + x_n - x_m + x_m - \overline{a_m}\right| \leq \left|\overline{a_n} - x_n\right| + \left|x_n - x_m\right| + \left|x_m - \overline{a_m}\right| \leq$$

$$\leq \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon .$$ Adică $\left(\overline{a_n}\right)_{n\geq 0}$ este şir Cauchy de numere raționale. Conform Lemei 7.26. există $x = \lim_{n\to\infty} \overline{a_n}$ în $\mathbb{R}$. Deoarece pentru n suficient de mare $|x_n - x| \leq |x_n - \overline{a_n}| + |\overline{a_n} - x|$ deducem că $x = \lim_{n\to\infty} x_n$, adică $\mathbb{R}$ este complet. ■

Definiția 7.28. Un corp ordonat K se zice *complet ordonat* dacă orice parte nevidă minorată a sa are o margine inferioară.

Observație 7.29. Fie K un corp complet ordonat şi $A\subset K$, $A\neq\emptyset$, A majorată. Atunci $-A$ este minorată, sup A există şi sup (A)=- inf ($-$ A).

Lema 7.30. Dacă x, y$\in\mathbb{Q}$, atunci :

(i) $x \le y \Leftrightarrow i_{\mathbb{Q}}(x) \le i_{\mathbb{Q}}(y)$

(ii) $x < y \Leftrightarrow i_{\mathbb{Q}}(x) < i_{\mathbb{Q}}(y)$

(iii) pentru orice $\alpha \in \mathbb{R}$ **există** $x, y \in \mathbb{Z}$ **a.î.** $i_{\mathbb{Q}}(x) \le \alpha \le i_{\mathbb{Q}}(y)$ **.**

Demonstrație. (i). Să presupunem că $x \le y$, adică $y-x \ge 0$. Cum $i_{\mathbb{Q}}(y)-i_{\mathbb{Q}}(x)=i_{\mathbb{Q}}(y-x)$ deducem că $i_{\mathbb{Q}}(y) \ge i_{\mathbb{Q}}(x) \Leftrightarrow i_{\mathbb{Q}}(x) \le i_{\mathbb{Q}}(y)$. Reciproc, să presupunem că $i_{\mathbb{Q}}(x) \le i_{\mathbb{Q}}(y)$, adică $i_{\mathbb{Q}}(y-x) \ge 0 \Rightarrow y-x \in P$, deci pentru $\varepsilon>0$, $y-x>\varepsilon>0 \Rightarrow y \ge x \Leftrightarrow x \le y$.

(ii). Rezultă din injectivitatea lui $i_{\mathbb{Q}}$.

(iii). Fie $\alpha \in \mathbb{R}$ şi $(x_n)_{n\ge 0} \in \alpha$. Atunci $(x_n)_{n\ge 0} \in \mathbf{C(\mathbb{Q})}$, deci pentru $\varepsilon \in \mathbb{Q}_+^*$ există $n_\varepsilon \in \mathbb{N}$ a.î. $|x_n - x_{n_\varepsilon}| < \varepsilon$ pentru orice $n \ge n_\varepsilon$ sau $x_{n_\varepsilon} - \varepsilon < x_n < x_{n_\varepsilon} + \varepsilon$ pentru orice $n \ge n_\varepsilon$.

Luând $x, y \in \mathbb{Z}$ a.î. $x < x_{n_\varepsilon} - \varepsilon$ şi $x_{n_\varepsilon} + \varepsilon < y$ deducem că $x_n - x > 0$ şi $y - x_n > 0$ pentru orice $n \ge n_\varepsilon$ deci

$$(x_n)_{n\ge 0} - (x, x, \ldots.) = (x_n - x)_{n\ge 0} \in P \quad \text{şi}$$

$$(y, y, \ldots.) - (x_n)_{n\ge 0} = (y - x_n)_{n\ge 0} \in P,$$

adică $i_{\mathbb{Q}}(x) \le \alpha \le i_{\mathbb{Q}}(y)$.

Lema 7.31. Fie $\alpha, \beta \in \mathbb{R}$ **şi** $(u_n)_{n\ge 0}, (v_n)_{n\ge 0} \in \mathbf{C(\mathbb{Q})}$ **a.î.**

$$i_{\mathbb{Q}}(u_m) \le \alpha \le \beta \le i_{\mathbb{Q}}(v_m)$$

pentru orice $m \in \mathbb{N}$ **şi** $(u_m)_{m\ge 0} - (v_m)_{m\ge 0} \in \mathbf{N(\mathbb{Q})}$ **. Atunci** $\alpha = \beta$ **.**

Demonstrație. Fie $\varepsilon>0$. Există $m_0 \in \mathbb{N}$ a.î. $|v_{m_0} - u_{m_0}| < \frac{\varepsilon}{3}$. Fie acum $(x_n)_{n\ge 0} \in \alpha$ şi $(y_n)_{n\ge 0} \in \beta$. Din condiția (1) deducem că $i_{\mathbb{Q}}(u_m) \le \alpha$, deci pentru $m = m_0$ avem $(x_n - u_{m_0})_{n\ge 0} \in P$ prin urmare există $n_\varepsilon' \in \mathbb{N}$ a.î. $x_n - u_{m_0} > -\frac{\varepsilon}{3}$ pentru $n \ge n_\varepsilon'$.

Tot din (1) rezultă că $\beta \le i_{\mathbb{Q}}(v_m)$ deci pentru $m=m_0$ avem $(v_{m_0}-y_n)_{n\ge 0}\in P$, adică există $n_\varepsilon''\in\mathbb{N}$ a.î. $v_{m_0}-y_n>-\frac{\varepsilon}{3}$, pentru orice $n\ge n_\varepsilon''$, de unde

$$y_n-x_n< v_{m_0}+\frac{\varepsilon}{3}-u_{m_0}+\frac{\varepsilon}{3}=v_{m_0}-u_{m_0}+\frac{2\varepsilon}{3}\le$$

$$\le\left|v_{m_0}-u_{m_0}\right|+\frac{2\varepsilon}{3}\le\frac{\varepsilon}{3}+\frac{2\varepsilon}{3}=\varepsilon,$$ prin urmare, $y_n-x_n<\varepsilon$ pentru orice $n\ge\max(n_\varepsilon', n_\varepsilon'')$. Dar $\alpha\le\beta$. Atunci $(y_n-x_n)_{n\ge 0}\in P$, deci există $n_\varepsilon'''\in\mathbb{N}$ a.î. $y_n-x_n>-\varepsilon$, pentru orice $n\ge n_\varepsilon'''$.

Atunci $|x_n-y_n|<\varepsilon$ pentru orice $n\ge\max(n_\varepsilon', n_\varepsilon'', n_\varepsilon''')$, de unde $\alpha=\beta$.■

Teorema 7.32. Corpul $(\mathbb{R},\le)$ este complet ordonat .

Demonstrație. Fie $A\subset\mathbb{R}$ nevidă şi minorată iar A_0 mulțimea minoranților lui A. Cum $A_0\neq\emptyset$, există $\beta\in A_0$ a.î. $\beta\le\alpha$ pentru orice $\alpha\in A$. Din Lema 7.31., (iii) rezultă existența unui $z\in\mathbb{Z}$ a.î. $i_{\mathbb{Q}}(z)\le\beta$, adică $i_{\mathbb{Q}}(z)\in A_0$.

Fie $x_0=\max\{z\in\mathbb{Z} \mid i_{\mathbb{Q}}(z)\in A_0\}$; atunci $i_{\mathbb{Q}}(x_0)\in A_0$ şi $i_{\mathbb{Q}}(x_0+1)\notin A_0$. Presupunem că am obținut un $x_k\in\mathbb{Q}$ $(k\ge 0)$ a.î. $i_{\mathbb{Q}}(x_k)\in A_0$ şi $i_{\mathbb{Q}}(x_k+\frac{1}{10^k})\notin A_0$

Notând $n_k=\max\{0\le n\le 9 \mid i_{\mathbb{Q}}(x_k)+\frac{n}{10^{k+1}}\in A_0\}$ şi

$x_{k+1}=x_k+\frac{n_k}{10^{k+1}}$ se obține, prin inducție, un şir $(x_k)_{k\ge 0}\in\mathbb{Q}$ a.î.

(1) $i_{\mathbb{Q}}(x_k)\in A_0$ pentru orice $k\in\mathbb{N}$;

(2) $i_{\mathbb{Q}}(x_k+\frac{1}{10^k})\notin A_0$ pentru orice $k\in\mathbb{N}$;

(3) $x_{k+1}=x_k+\frac{n_k}{10^{k+1}}$.

Din (3) şi din definiția lui n_k rezultă $x_{k+1} = x_k + \frac{n_k}{10^{k+1}}$, de unde pentru n >k obținem $x_n - x_k = x_n - x_{n-1} + x_{n-1} - x_{n-2} + ... + x_{k+1} - x_k \leq$

$$\leq \frac{9}{10^n} + \frac{9}{10^{n-1}} + ... + \frac{9}{10^{k+1}} = \frac{9}{10^{k+1}}\left(1 + \frac{1}{10} + ... + \frac{1}{10^{n-k-1}}\right) = \frac{9}{10^{k+1}} \cdot \frac{1 - \frac{1}{10^{n-k}}}{1 - \frac{1}{10}} <$$

$$< \frac{9}{10^{k+1}} \cdot \frac{10}{9} = \frac{1}{10^k}$$

deci $(x_n)_{n\geq 0} \in \mathbf{C}(\mathbb{Q})$. Fie $\alpha = \overline{(x_n)_{n\geq 0}} \in \mathbb{R}$ şi să demonstrăm că $\alpha = \inf A$.

Pentru aceasta vom demonstra că

$$(*)\ i_{\mathbb{Q}}(x_k) \leq \alpha \leq i_{\mathbb{Q}}\left(x_k + \frac{1}{10^k}\right) \text{ pentru orice } k \in \mathbb{N}.$$

Din (3) deducem că $x_0 \leq x_1 \leq \ldots \leq x_k \leq \ldots$, deci $(x_n - x_k)_{n\geq 0} \in P$ pentru orice $k \in \mathbb{N}$, adică $i_{\mathbb{Q}}(x_k) \leq \overline{(x_n)_{n\geq 0}} = \alpha$ pentru orice $k \in \mathbb{N}$.

Am demonstrat mai înainte că $x_n - x_k < \frac{1}{10^k}$, pentru n>k, adică $\left(x_k + \frac{1}{10^k}\right) - x_n > 0$ pentru n >k, deci $\alpha \leq i_{\mathbb{Q}}\left(x_k + \frac{1}{10^k}\right)$ pentru orice $k \in \mathbb{N}$.

Am arătat astfel inegalitățile $(*)$.

Să demonstrăm acum că α este minorant al lui A. Să presupunem că există $\gamma \in A$ a.î. $\gamma < \alpha$. Atunci $i_{\mathbb{Q}}(x_k) \leq \gamma \leq \alpha \leq i_{\mathbb{Q}}\left(x_k + \frac{1}{10^k}\right)$ pentru orice $k \in \mathbb{N}$.

Dar $\lim_{k\to\infty}\left(x_k + \frac{1}{10^k} - x_k\right) = \lim_{k\to\infty} \frac{1}{10^k} = 0$, de unde ținând cont de Lema 7.31. deducem că $\gamma = \alpha$, absurd, deci $\alpha \in A_0$.

Să arătăm acum că α este cel mai mare minorant al lui A. Presupunem că există $\beta \in A_0$ a.î. $\alpha < \beta$. Din (3) deducem că pentru fiecare $k \in \mathbb{N}$ există $\alpha_k \in A$ a.î. $\alpha_k < i_{\mathbb{Q}}\left(x_k + \frac{1}{10^k}\right)$. Cum β este minorant al lui A

şi $\alpha_k \in A$ deducem că $\beta \le \alpha_k$ de unde $i_{\mathbb{Q}}(x_k) \le \alpha \le \beta \le i_{\mathbb{Q}}(x^k + \frac{1}{10^k})$ de unde deducem că $\alpha = \beta$, absurd!. Deci $\alpha = \inf A$. ■

§8 . Construcția corpului $\mathbb{C}$ al numerelor complexe

Scopul acestui paragraf este de a identifica corpul $\mathbb{R}$ al numerelor reale cu un subcorp al unui corp comutativ $\mathbb{C}$ în care ecuația $x^2 = -1$ are soluție.

Pentru aceasta vom considera $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ iar pentru $(x, y), (z, t) \in \mathbb{C}$ definim :

$$(x, y) + (z, t) = (x+z, y+t)$$

$$(x, y) \cdot (z, t) = (xz-yt, xt+yz).$$

Teorema 8.1. ($\mathbb{C}$, +, ·) este corp comutativ în care ecuația $x^2 = -1$ are soluție.

Demonstrație. Faptul că ($\mathbb{C}$, +) este grup abelian se probează imediat (elementul neutru este (0, 0), iar pentru $(x, y) \in \mathbb{C}$, $-(x, y) = (-x, -y)$).

În mod evident înmulțirea este comutativă.

Pentru a proba că ($\mathbb{C}^*$, ·) este grup, fie $(x, y), (z, t), (r, s) \in \mathbb{C}$. Deoarece $(x, y)[(z, t)\cdot(r, s)] = [(x, y)(z, t)]\cdot(r, s) = (xzr-xts-yzs-ytr, xzs+xtr+yzr-yts)$ deducem că înmulțirea este asociativă.

Cum $(x, y)(1, 0) = (1, 0)(x, y) = (x, y)$ deducem că elementul neutru față de înmulțire este (1, 0). Fie acum $(x, y) \in \mathbb{C}^*$ (adică $x \neq 0$ sau $y \neq 0$). Egalitatea $(x, y)(x', y') = (1, 0)$ este echivalentă cu $xx' - yy' = 1$ şi

$xy'+yx'=0$, de unde $x'=\frac{x}{x^2+y^2}$ şi $y'=-\frac{y}{x^2+y^2}$, adică $(x, y)^{-1}=$

$=\left(\frac{x}{x^2+y^2}, -\frac{y}{x^2+y^2}\right)$.

Cum pentru $(x, y), (z, t), (r, s)\in\mathbb{C}$, $(x, y)\cdot[(z, t)+(r, s)]=$ $=(x, y)\cdot(z, t)+(x, y)\cdot(r, s)=(xz+xr-yt-ys, xt+xs+yz+yr)$ deducem că înmulţirea este distributivă faţă de adunare, adică $(\mathbb{C}, +, \cdot)$ este corp comutativ.

Să notăm $i=(0, 1)$. Cum $i^2=(0, 1)(0, 1)=(-1, 0)=-(1, 0)$ deducem că ecuaţia $x^2=-1$ are soluţie în $\mathbb{C}$. ■

Observaţia 8.2. Se probează imediat că $i_{\mathbb{R}}:\mathbb{R}\to\mathbb{C}$, $i_{\mathbb{R}}(x)=(x, 0)$ pentru orice $x\in\mathbb{R}$, este morfism de corpuri (deci funcţie injectivă). În felul acesta $\mathbb{R}$ poate fi privit ca subcorp al lui $\mathbb{C}$.

Am construit astfel şirul de mulţimi $\mathbb{N}\subseteq\mathbb{Z}\subseteq\mathbb{Q}\subseteq\mathbb{R}\subseteq\mathbb{C}$.

Deoarece pentru $z=(x, y)\in\mathbb{C}$ putem scrie $z=(x, 0)+(y, 0)(0, 1)$, ţinând cont de identificările anterioare deducem că z se poate scrie (formal) sub forma $z=x+iy$ (cu $i=(0, 1)$ iar $i^2=-1$).

Mulţimea $\mathbb{C}$ poartă numele de *mulţimea numerelor complexe*, iar $(\mathbb{C}, +, \cdot)$ *corpul numerelor complexe.* Elementele din $\mathbb{C}\setminus\mathbb{R}$ se zic *pur imaginare*.

Dacă $z=x+iy\in\mathbb{C}$ cu $x, y\in\mathbb{R}$, atunci x se zice *partea reală* a lui z iar yi *partea imaginară* a lui z (y se numeşte *coeficientul părţii imaginare*).

Pentru $z\in\mathbb{C}$, $z=x+iy$, definim $\bar{z}=x-iy$ (ce se va numi *conjugatul* lui z) şi $|z|=\sqrt{x^2+y^2}$ ($|z|$ poartă numele de *modulul* lui z).

Propoziţia 8.3. Fie $z, z_1, z_2\in\mathbb{C}$. Atunci

(i) $z\in\mathbb{R} \Leftrightarrow z=\bar{z}$

(ii) $\overline{\bar{z}}=z$, $z\cdot\bar{z}=|z|^2$

(iii) $\overline{z_1 \pm z_2} = \overline{z_1} \pm \overline{z_2}$, $\overline{z_1 z_2} = \overline{z_1}\ \overline{z_2}$, $\overline{\left(\frac{z_1}{z_2}\right)} = \frac{\overline{z_1}}{\overline{z_2}}$ **(cu $z_2 \neq 0$)**

(iv) $|z| = |\overline{z}|$, $|z_1 + z_2| \leq |z_1| + |z_2|$, $|z_1\ z_2| = |z_1|\ |z_2|$, $\left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}$ **(cu $z_2 \neq 0$).**

Demonstrație. (i). Fie z=a+ib. Dacă $z \in \mathbb{R}$, atunci b=0, deci $\overline{z} = a = z$ iar dacă $z = \overline{z}$ atunci b =-b adică b=0, deci $z \in \mathbb{R}$.

(ii). şi (iii). sunt evidente.

(iv). Să probăm doar inegalitatea $|z_1+z_2| \leq |z_1|+|z_2|$ (celelalte probându-se imediat). Alegem $z_1=x_1+iy_1$ şi $z_2=x_2+iy_2$ cu $x_1, x_2, y_1, y_2 \in \mathbb{R}$ şi astfel

$|z_1+z_2| \leq |z_1|+|z_2| \Leftrightarrow \sqrt{(x_1+x_2)^2+(y_1+y_2)^2} \leq \sqrt{x_1^2+y_1^2} + \sqrt{x_2^2+y_2^2} \Leftrightarrow$

$x_1^2 + x_2^2 + 2x_1x_2 + y_1^2 + y_2^2 + 2y_1y_2 \leq x_1^2 + y_1^2 + x_2^2 + y_2^2 +$

$+ 2\sqrt{(x_1^2+y_1^2)(x_2^2+y_2^2)}$

$\Leftrightarrow (x_1x_2 + y_1y_2)^2 \leq (x_1^2+y_1^2)(x_2^2+y_2^2) \Leftrightarrow (x_1y_2 - x_2y_1)^2 \geq 0$ ceea ce este evident.

Egalitate avem dacă $\frac{x_1}{y_1} = \frac{x_2}{y_2} = \lambda$ cu $\lambda \in \mathbb{R}$, adică $z_1 = \lambda\ z_2$. ■

Observația 8.4. Asociind fiecărui număr complex z=a+ib matricea $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ se probează imediat că corpul $(\mathbb{C},+,\cdot)$ este izomorf cu corpul $\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a,\ b \in \mathbb{R} \right\}$, operațiile de adunare şi înmulțire fiind cele obişnuite din $M_2(\mathbb{R})$.

§.9. Construcția corpului H al quaternionilor

În inelul $(M_2(\mathbb{C}), +, \cdot)$ să considerăm mulțimea:

$$\mathbf{H} = \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} | \alpha, \beta \in \mathbb{C} \right\}$$

(unde reamintim că pentru $\alpha \in C$, $\overline{\alpha}$ reprezintă conjugatul lui α).

Propoziția 9.1. (H, +, ·) este subinel al lui $M_2(\mathbb{C})$.

Demonstrație. Fie $M=\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$ și $N=\begin{pmatrix} \gamma & \delta \\ -\overline{\delta} & \overline{\gamma} \end{pmatrix}$ două elemente din **H**. Atunci $M-N=\begin{pmatrix} \alpha-\gamma & \beta-\delta \\ \overline{-(\beta-\delta)} & \overline{\alpha-\gamma} \end{pmatrix} \in \mathbf{H}$,

$MN=\begin{pmatrix} \alpha\gamma-\beta\overline{\delta} & \alpha\delta+\beta\overline{\gamma} \\ \overline{-\alpha\delta+\beta\overline{\gamma}} & \overline{\alpha\gamma-\beta\overline{\delta}} \end{pmatrix} \in \mathbf{H}$ și $I_2=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ -\overline{0} & \overline{1} \end{pmatrix} \in \mathbf{H}$, de unde concluzia că **H** este subinel (unitar) al lui $M_2(\mathbb{C})$.■

Corolarul 9.2. (H, +, ·) este corp.

Demonstrație. Ținând cont de Propoziția 9.1. mai avem de demonstrat faptul că dacă $M \in \mathbf{H}$, $M=\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \neq O_2$, atunci există $N \in \mathbf{H}$ a.î. $MN=NM=I_2$. Din $M \neq O_2$ deducem că $\Delta = \alpha\overline{\alpha}+\beta\overline{\beta} = |\alpha|^2 + |\beta|^2 \neq 0$. Considerând $N=\begin{pmatrix} \alpha' & \beta' \\ -\overline{\beta}' & \overline{\alpha}' \end{pmatrix} \in \mathbf{H}$, unde $\alpha' = \overline{(\alpha/\Delta)}$ și $\beta' = -\frac{\beta}{\Delta}$ avem:

$$MN=\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}\begin{pmatrix} \alpha' & \beta' \\ -\overline{\beta}' & \overline{\alpha}' \end{pmatrix}=\begin{pmatrix} \alpha\alpha'-\beta\overline{\beta}' & \alpha\beta'+\beta\overline{\alpha}' \\ \overline{-(\alpha\beta'+\beta\overline{\alpha}')} & \overline{\alpha\alpha'-\beta\overline{\beta}'} \end{pmatrix} \text{ iar}$$

$$\alpha\alpha' - \beta\overline{\beta}' = \alpha\overline{\left(\frac{\alpha}{\Delta}\right)} + \beta\overline{\left(\frac{\beta}{\Delta}\right)} = \frac{\alpha\overline{\alpha} + \beta\overline{\beta}}{\Delta} = \frac{|\alpha|^2 + |\beta|^2}{\Delta} = \frac{\Delta}{\Delta} = 1$$

$$\alpha\beta' + \beta\overline{\alpha}' = -\alpha\left(\frac{\beta}{\Delta}\right) + \beta\left(\frac{\alpha}{\Delta}\right) = -\frac{\alpha\beta}{\Delta} + \frac{\alpha\beta}{\Delta} = 0,$$

de unde $MN=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=I_2$ şi analog $NM=I_2$, adică $M^{-1}=N$.■

Definiția 9.3. Corpul H poartă numele de *corpul quaternionilor* (elementele lui H se vor numi *quaternioni*).

Dacă vom considera $j_{\mathbb{R}}:\mathbb{R}\to\mathbf{H}$ definit prin $j_{\mathbb{R}}(a)=\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ pentru orice $a\in\mathbb{R}$ se verifică imediat că $j_{\mathbb{R}}$ este morfism de corpuri (deci funcție injectivă), astfel numărul real **a** se identifică cu quaternionul $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$.

Să notăm $I=\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ şi $K=\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Prin calcul se verifică egalitățile:

$$I^2=J^2=K^2=-I_2,\ IJ=-JI=K,\ JK=-KJ=I,\ KI=-IK=J$$

(de unde o primă concluzie ce se desprinde este că **H** este un corp necomutativ).

Dacă $\alpha=a_0+a_1i$ şi $\beta=b_0+b_1i\in\mathbb{C}$, putem scrie:

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}=\begin{pmatrix} a_0+a_1i & b_0+b_1i \\ -b_0+b_1i & a_0-a_1i \end{pmatrix}=\begin{pmatrix} a_0 & 0 \\ 0 & a_0 \end{pmatrix}+\begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}+$$

$$\begin{pmatrix} b_0 & 0 \\ 0 & b_0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}+\begin{pmatrix} b_1 & 0 \\ 0 & b_1 \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}=a_0I_2+a_1I+b_0J+b_1K$$ (dacă ținem cont de identificarea oricărui număr real **a** cu quaternionul $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$). Astfel, orice quaternion $h\in\mathbf{H}$ poate fi scris, în mod unic, sub forma $h=a+bI+cJ+dK$ cu $a, b, c, d\in\mathbb{R}$ (identificând pe aI_2 cu a).

Observaţia 9.4. În corpul **H** ecuaţia $x^2+1=0$ are o infinitate de soluţii şi anume toţi quaternionii $h=aI+bJ+cK$ cu a, b, $c\in\mathbb{R}$ şi $a^2+b^2+c^2=1$.

§10. Ideale prime. Ideale maximale

În cadrul acestui paragraf prin A vom desemna un inel unitar şi comutativ.

Definiţia 10.1. Un ideal $\wp$ al lui A se zice *prim* dacă $\wp \neq A$ şi dacă avem a,b∈A a.î. ab∈ $\wp$, atunci a∈$\wp$ sau b∈$\wp$.

Exemple 1. Dacă A este un domeniu de integritate, atunci idealul nul (0) este prim.

2. Pentru inelul $\mathbb{Z}$ idealele prime sunt (0) şi $p\mathbb{Z}$ cu $p\geq 2$ număr prim.

Propoziţia 10.2. Un ideal $\wp$ al lui A este prim dacă şi numai dacă A/$\wp$ este domeniu de integritate.

Demonstraţie. Dacă $\wp \subset$ A este ideal prim, atunci $\wp\neq$A, deci A/$\wp$ este inel nenul şi cum A este comutativ şi unitar deducem că şi A/$\wp$ este comutativ şi unitar. Fie acum $\hat{a} = a + \wp$, $\hat{b} = b + \wp \in$A/$\wp$ a.î. $\hat{a}\,\hat{b} = \hat{0} \Leftrightarrow ab \in \wp$. Cum $\wp$ este prim deducem că $a \in \wp \Leftrightarrow \hat{a} = \hat{0}$ sau $b \in \wp \Leftrightarrow \hat{b} = \hat{0}$, adică A/$\wp$ nu are divizori ai lui zero nenuli.

Reciproc, dacă A/$\wp$ este domeniu de integritate, atunci A/$\wp$ este nenul şi deci $\wp\neq$A. Dacă $a, b \in$A a.î. $ab \in \wp$, atunci $\hat{ab} = \hat{0} \Leftrightarrow \hat{a}\,\hat{b} = \hat{0}$ şi cum A/$\wp$ nu are divizori nenuli ai lui zero deducem că $\hat{a} = \hat{0} \Leftrightarrow a \in \wp$ sau $\hat{b} = \hat{0} \Leftrightarrow b \in \wp$.■

Propoziția 10.3. Fie A, A′ două inele unitare şi comutative iar f:A→A′ un morfism de inele unitare. Atunci:

(i) Dacă $\wp' \subset A'$ este ideal prim în A′, $f^{-1}(\wp')$ este ideal prim în A

(ii) Dacă în plus f este morfism surjectiv şi $\wp \subset A$ ideal prim, a.î. $Ker(f) \subseteq \wp$, atunci $f(\wp)$ este ideal prim in A′.

Demonstrație. (i). Conform Propoziției 3.7. deducem că $f^{-1}(\wp')$ este ideal în A (evident $f^{-1}(\wp') \neq A$, căci $\wp' \neq A'$). Dacă a, b∈A a.î. $ab \in f^{-1}(\wp')$ atunci $f(ab) \in \wp' \Leftrightarrow f(a)f(b) \in \wp'$. Cum $\wp'$ este prim în A′ deducem că $f(a) \in \wp'$ sau $f(b) \in \wp'$, de unde concluzia că $a \in f^{-1}(\wp')$ sau $b \in f^{-1}(\wp')$, adică $f^{-1}(\wp')$ este ideal prim în A.

(ii). Cum f este surjecție, conform Propoziției 3.7. deducem că $f(\wp)$ este ideal al lui A′ (propriu, deoarece $\wp \neq A$). Fie acum a′, b′∈A′ a.î. a′b′∈$f(\wp)$. Atunci există a, b∈A a.î. a′=f(a) şi b′=f(b) altfel că a′b′∈$f(\wp) \Rightarrow f(a)f(b) \in f(\wp) \Rightarrow f(ab) \in f(\wp) \Rightarrow f(ab)=f(c)$ cu $c \in \wp \Rightarrow ab\text{-}c \in Ker(f) \subseteq \wp \Rightarrow ab\text{-}c \in \wp$ şi $c \in \wp \Rightarrow ab \in \wp$. Deoarece $\wp$ este prim în A deducem că $a \in \wp$ sau $b \in \wp$, adică a′∈$f(\wp)$ sau b′∈$f(\wp)$, de unde concluzia că $f(\wp)$ este prim în A′.■

Definiția 10.4. Un ideal $m \subset A$ se zice *maximal* dacă $m \neq A$ şi m este element maximal în laticea Id(A) (adică oricare ar fi I∈Id(A) a.î. $m \subseteq I \subseteq A$ rezultă m=I sau I=A**).**

Exemple 1. În orice corp K, idealul (0) este maximal .

2. Pentru idealul $\mathbb{Z}$, idealele maximale coincid cu cele prime (adică sunt de forma $p\mathbb{Z}$ cu p≥2 număr prim).

Într-adevăr, dacă p≥2 este număr prim, atunci $p\mathbb{Z} \neq \mathbb{Z}$ şi dacă $I=n\mathbb{Z}$ este un alt ideal al lui $\mathbb{Z}$ pentru care $p\mathbb{Z} \subseteq n\mathbb{Z} \subseteq \mathbb{Z}$, atunci n|p, de unde n∈{±1, ±p}, adică $I=p\mathbb{Z}$ sau $I=\mathbb{Z}$. Reciproc, dacă $p\mathbb{Z}$ este ideal maximal, atunci $p\mathbb{Z} \neq \mathbb{Z}$ şi deci p≠±1. Dacă n∈$\mathbb{Z}$ a.î. n|p, atunci $p\mathbb{Z} \subseteq n\mathbb{Z}$

$\subseteq \mathbb{Z}$ şi cum $p\mathbb{Z}$ este maximal rezultă $n\mathbb{Z}=p\mathbb{Z}$ sau $n\mathbb{Z}=\mathbb{Z}$, adică $n = \pm p$ sau $n = \pm 1$, adică p este prim.

Propoziția 10.5. Fie $m \subset A$ un ideal maximal a.î. $m \neq A$. Următoarele afirmații sunt echivalente:

(i) m este ideal maximal

(ii) Pentru orice $a \in A \setminus m$ avem $m + \langle a \rangle = A$

(iii) A / m este corp.

Demonstrație. (i)$\Rightarrow$(ii). Deoarece pentru $a \in A \setminus m$ avem $m \subset m + \langle a \rangle$ iar m este maximal deducem cu necesitate că $m + \langle a \rangle = A$.

(ii)$\Rightarrow$(iii). Fie $\hat{a} = a + m \in (A/m)^*$, adică $a \notin m$. Atunci $a \in A \setminus m$ şi deci $m + \langle a \rangle = A$, adică $1 = x + ba$ cu $x \in m$ şi $b \in A$. Deducem imediat că $\hat{b}\,\hat{a} = \hat{1}$, adică $\hat{a}$ este inversabil, deci A/m este corp.

(iii)$\Rightarrow$(i). Să presupunem prin absurd că m nu este maximal, adică există $I \in \mathbf{Id}(A)$ a.î. $I \neq A$ şi $m \subseteq I$. Există deci $a \in I$ a.î. $a \notin m$.

Atunci $\hat{a} \in (A/m)^*$ şi cum A/m este presupus corp deducem existența unui $b \in A \setminus m$ a.î. $\hat{a}\,\hat{b} = \hat{1} \Leftrightarrow ab - 1 \in m$. Cum $m \subset I$ deducem că $ab - 1 \in I$ şi cum $a \in I$ rezultă $1 \in I$, adică $I = A$ - absurd !.■

Corolar 10.6. Orice ideal maximal al lui A este prim.

Demonstrație. Dacă m este ideal maximal al lui A, atunci conform Propoziției 10.5., A/m este corp (deci domeniu de integritate) şi atunci m este prim conform Propoziției 10.2.■

Observația 10.7. **Reciproca Corolarului 10.6. nu este în general adevărată. Contraexemplul ne este oferit de inelul $\mathbb{Z}$ în care (0) este prim fără a fi însă maximal (căci (0) este cuprins în orice ideal al lui $\mathbb{Z}$).**

Propoziția 10.8. Fie A, A′ două inele unitare şi comutative iar $f: A \to A'$ un morfism surjectiv de inele unitare.

(i) Dacă $m' \subset A'$ este ideal maximal în A′, atunci $f^{-1}(m')$ este ideal maximal în A

(ii) Dacă $m \subset$A ideal maximal în A a.î. Ker(f) $\subseteq m$, atunci f(m) este ideal maximal în A′.

Demonstrație. (i). Fie I∈Id(A) a.î. $f^{-1}(m') \subseteq I \subseteq$A. Atunci $m' \subseteq$ f(I) şi cum m' este maximal în A′ deducem că m'=f (I) sau f (I)=A′, adică $f^{-1}(m')$=I sau I=f^{-1}(A′)=A, adică $f^{-1}(m)$ este ideal maximal în A.

(ii). Fie I′∈Id(A′) a.î. f(m) $\subseteq$ I $\subseteq$A′. Atunci $m \subseteq f^{-1}(I) \subseteq \subseteq f^{-1}(A')$=A şi cum m este maximal în A deducem că $m = f^{-1}(I)$ sau f^{-1}(I)=A, adică $f^{-1}(m)$=I sau I=f (A)=A′, adică f (m) este ideal maximal în A′.■

Teorema 10.9. (*Krull*) Orice ideal I ≠A al inelului A este conținut într-un ideal maximal.

Demonstrație. Să considerăm mulțimea

$$P_I=\{J \in Id(A) \mid I \subseteq J \text{ şi } J \neq A\}.$$

Cum I∈P_I deducem că $P_I \neq \emptyset$. Se verifică imediat că (P_I, $\subseteq$) este o mulțime inductiv ordonată. Conform Lemei lui Zorn (vezi Corolarul 2 la Lema 5.15. de la Capitolul 1) P_I are cel puțin un element maximal m. Atunci m este ideal maximal al lui A ce conține pe I. ■

Corolarul 10.10. Orice element neinversabil al lui A este conținut într-un ideal maximal al lui A.

Demonstrație. Fie a∈A**U**(A). Atunci I=<a>≠A şi conform Teoremei 10.9. există un ideal maximal m a.î. I $\subseteq m$, de unde a∈ m. ■

Corolarul 10.11. Orice inel A (comutativ şi unitar) are cel puțin un ideal maximal.

Demonstrație. În Teorema 10.9. considerăm I=(0).■

Definiția 10.12. Un inel comutativ şi unitar ce are un singur ideal maximal se zice *inel local*.

Exemplu. Corpurile comutative sunt în particular inele locale.

Propoziția 10.13. Pentru inelul comutativ A următoarele afirmații sunt echivalente:

(i) A este local

(ii) Dacă a, b∈A şi a+b=1 atunci a sau b este inversabil

(iii) Mulțimea A\ U(A)∈Id(A).

Demonstrație.(i)⇒(ii). Fie m singurul ideal maximal al lui A şi a, b∈A a.î a+b=1. Să presupunem prin absurd că de exemplu a nu este inversabil. Atunci <a>≠A şi conform Teoremei 10.9., <a> $\subseteq m$, adică a $\in m$. Cum m≠A avem că 1 $\notin m$ deci a+b $\notin m$ şi cu necesitate b $\notin$ **U**(A).

(ii)⇒(iii). Fie x,y∈A**U**(A) şi să presupunem prin absurd că x-y∈**U**(A). Atunci există z∈A a.î. z(x-y)=1 ⇔ zx+(-zy)=1. Deducem că zx∈**U**(A) sau -zy∈**U**(A) şi cum z∈**U**(A) deducem că x∈**U**(A) sau y∈**U**(A)- absurd!, deci obligatoriu x-y∈A**U**(A). Dacă a∈A şi x∈A**U**(A) atunci în mod evident ax∈A**U**(A), adică A**U**(A)∈**Id**(A).

(iii)⇒(i). Să presupunem că A**U**(A)∈**Id**(A) şi fie m un ideal maximal al lui A. Cum 1∈**U**(A) deducem că A**U**(A)≠A. Cum m ≠A, orice element al lui m este neinversabil, deci m ⊆A**U**(A)⊆A. Atunci m=A**U**(A), adică A are un singur ideal maximal, deci este inel local. ■

Observația 10.14. Un inel cu un număr finit de ideale maximale se zice *semi-local.*

În cadrul Observației 2.9. am stabilit că mulțimea **N**(A) a elementelor nilpotente ale lui A formează un ideal ce poartă numele de *nilradicalul* lui A.

Propoziția 10.15. N(A) este egal cu intersecția tuturor idealelor prime ale lui A.

Demonstrație. Fie $\mathcal{N}$ intersecția tuturor idealelor prime ale lui A; vom proba egalitatea **N**(A) = $\mathcal{N}$ prin dublă incluziune.

Dacă $x \in N(A)$, atunci există n∈$\mathbb{N}^*$, a.î. $x^n = 0$ astfel că dacă $\wp$ este un ideal prim oarecare al lui A avem $x^n = 0 \in \wp$, de unde concluzia că $x \in \wp$, adică $x \in \cap \wp = \mathcal{N}$, deci **N**(A) $\subseteq \mathcal{N}$.

Fie $a \notin N(A)$ iar I_a familia idealelor I ale lui A cu proprietatea că pentru orice n∈$\mathbb{N}^*$, $a^n \notin I$ (familia I_a este nevidă deoarece din presupunerea $x \notin N(A)$ deducem că idealul nul $0 \in I_a$).

Se verifică imediat că mulțimea $(I_a, \subseteq)$ este inductivă şi atunci conform lemei lui Zorn (Corolarul 2 la Lema 5.15 de la Capitolul 1) în I_a există un element maximal $\wp$ despre care vom arăta că este prim.

Dacă x,y $\notin \wp$, atunci cum $\wp$ este inclus strict în idealele $\wp + \langle x \rangle$ şi $\wp + \langle y \rangle$ deducem că aceste ultime două ideale nu fac parte din I_a , astfel că vom găsi $m,n \in \mathbb{N}^*$ a.î. $a^m \in \wp + \langle x \rangle$ şi $a^n \in \wp + \langle y \rangle$.

Deducem imediat că $a^{m+n} \in \wp + \langle xy \rangle$, adică $\wp + \langle xy \rangle \in I_a$, deci $xy \notin \wp$, adică $\wp$ este prim. Cum $a \notin \wp$ deducem că $a \notin \mathcal{N}$, adică $\mathcal{N} \subseteq N(A)$, de unde egalitatea **N**(A)=$\mathcal{N}$. ■

Definiția 10.16. ***Radicalul Jacobson*** **al inelului A se defineşte ca fiind intersecția J(A) a tuturor idealelor maximale ale lui A.**

Avem următoarea caracterizare a lui J(A):

Propoziția 10.17. $x \in J(A) \Leftrightarrow 1 - xy \in U(A)$ ***pentru orice*** $y \in A$**.**

Demonstrație. "$\Rightarrow$". Fie $x \in J(A)$ şi să presupunem prin absurd că există $y \in A$ a.î. $1 - xy \notin U(A)$. Conform Corolanului 10.10 există un ideal maximal m al lui A a.î. $1 - xy \in m$. Cum $x \in J(A) \subseteq m$ deducem că $xy \in m$ adică $1 \in m$ – absurd !.

"$\Leftarrow$". Să presupunem că $x \notin J(A)$, adică există un ideal maximal m al lui A a.î. $x \notin m$. Atunci $<m \cup \{x\}>$ = A, deci $1 = a + xy$ cu $a \in m$ şi $y \in A$. Deducem că $1 - xy = a \in m$**,** ceea ce este absurd deoarece m nu conține unități ale lui A. ■

Propoziția 10.18. (i) Dacă $\wp_1$, ..., $\wp_n$ sunt ideale prime ale lui A şi I $\in$Id(A) a.î. I$\subseteq \bigcup_{i=1}^{n} \wp_i$, atunci există i$\in${1, 2., ..., n} a.î. I$\subseteq\wp_i$

(ii) Dacă I_1, I_2,..., I_n sunt ideale ale lui A iar $\wp$ este ideal prim al lui A a.î. $\bigcap_{i=1}^{n} I_i \subseteq \wp$, atunci există 1$\leq$i$\leq$n a.î. $I_i \subseteq \wp$

Dacă $\wp = \bigcap_{i=1}^{n} I_i$ atunci există 1$\leq$i$\leq$n a.î. $\wp = I_i$.

Demonstrație. (i). Vom demonstra prin inducție matematică după n$\geq$1 implicația I $\not\subseteq \wp_i$ (1$\leq$i$\leq$n) $\Rightarrow$I$\not\subseteq \bigcup_{i=1}^{n} \wp_i$ (care pentru n=1 este

evidentă). Fie $n\geq 1$ şi să presupunem implicaţia adevărată pentru n-1 şi fie pentru fiecare $1\leq i\leq n$, $x_i\in I$ a.î. $x_i\notin \wp_j$ pentru orice $j\neq i$. Dacă pentru un anumit i_0 $(1\leq i_0\leq n)$, $x_{i_0}\notin \wp_{i_0}$, atunci $x_{i_0}\notin \bigcup_{i=1}^{n}\wp_i$ şi totul este clar. Să presupunem acum că $x_i\in\wp_i$ pentru orice $1\leq i\leq n$. Pentru orice $1\leq i\leq n$ să considerăm elementul $y_i=\prod_{\substack{1\leq j\leq n\\ j\neq i}} x_j \in I$. Cum $\wp_i$ este ideal prim deducem că $y_i\notin\wp_i$ şi $y_i\in\wp_j$ pentru orice $1\leq i,j\leq n$, $i\neq j$. Considerând elementul $y=\sum_{i=1}^{n} y_i$ deducem că $y\in I$ şi $y\notin\wp_i$ pentru orice $1\leq i\leq n$, adică $I\not\subseteq\bigcup_{i=1}^{n}\wp_i$.

(ii). Presupunem că $\bigcap_{i=1}^{n} I_i\subseteq\wp$ şi totuşi $I_i\not\subseteq\wp$ pentru orice $1\leq i\leq n$ adică există $x_i\in I_i$ a.î. $x_i\notin\wp$.

Atunci $\prod_{i=1}^{n} x_i\in\prod_{i=1}^{n} I_i\subseteq\bigcap_{i=1}^{n} I_i$ (conform Observaţiei 2.16.). Cum $\wp$ este prim, $\prod_{i=1}^{n} x_i\notin\wp$, de unde concluzia că $\bigcap_{i=1}^{n} I_i\not\subseteq\wp$- absurd !.

Dacă $\bigcap_{i=1}^{n} I_i=\wp$ atunci conform celor de mai înainte există $1\leq i\leq n$ a.î. $I_i\subseteq\wp$. Cum $\wp\subseteq I_i$ deducem că $\wp=I_i$. ■

Definiţia 10. 19. Dacă $I\in Id(A)$, atunci prin *radicalul lui I* înţelegem mulţimea $r(I)=\{x\in A \mid \text{există } n\in\mathbb{N}^* \text{ a.î. } x^n\in I\}$. Considerând $p_I:A\to A/I$ morfismul surjectiv canonic şi nilradicalul $N(A/I)$ al lui A/I, atunci cum $r(I)=p_I^{-1}(N(A/I))$ deducem că $r(I)\in Id(A)$ (conform Propoziţiei 3.7.).

Propoziţia 10. 20. Dacă $I, J\in Id(A)$, atunci

(i) $I\subseteq r(I)$ iar dacă $I\subseteq J\Rightarrow r(I)\subseteq r(J)$

(ii) $r(r(I))=r(I)$

(iii) $r(IJ)= r(I\cap J)= r(I)\cap r(J)$

(iv) $r(I)=A \Leftrightarrow I=A$

(v) $r(I+J)=r(r(I)+ r(J))$

(vi) Dacă I este prim atunci pentru orice $n\in\mathbb{N}^*$, $r(I^n)= I$.

Demonstrație. (i).Evident.

(ii). Din $I\subseteq r(I) \Rightarrow r(I) \subseteq r(r(I))$. Dacă $x\in r(r(I))$ atunci există $n\in\mathbb{N}^*$ a.î. $x^n\in r(I)$, adică există $m\in\mathbb{N}^*$ a.î. $\left(x^n\right)^m \in I \Leftrightarrow x^{mn}\in I$, deci $x\in r(I)$, de unde şi incluziunea $r(r(I)) \subseteq r(I)$ ceea ce ne asigură egalitatea de la (ii).

(iii). Egalitatea $r(I\cap J)=r(I)\cap r(J)$ este evidentă. Cum $IJ\subseteq I\cap J$ (conform Observației 2.16.) deducem că $r(IJ)\subseteq r(I\cap J)$. Dacă $x\in r(I\cap J)$ atunci există $n\in\mathbb{N}^*$ a.î. $x^n\in I\cap J \Leftrightarrow$ şi $x^n\in I$ şi $x^n\in J$. Cum $x^{2n}=x^nx^n\in IJ$ deducem că $x\in r(IJ)$, adică $r(I\cap J) \subseteq r(IJ)$, de unde egalitatea $r(IJ)= =r(I\cap J)$.

(iv). Evidentă.

(v). Ținând cont de (i) deducem că $I \subseteq r(I)$ şi $J \subseteq r(J)$, apoi $I+J \subseteq r(I) +r(J)$, deci $r(I+J) \subseteq r(r(I) +r(J))$.

Fie acum $x\in r(I+J) \subseteq r(r(I) +r(J))$ şi $n\in\mathbb{N}^*$ a.î. $x^n\in r(I)+r(J)$. Există atunci $y\in r(I)$ şi $z\in r(J)$, $p, q\in\mathbb{N}^*$ a.î. $y^p\in I$, $z^q\in J$ şi $x^n=y+z$. Deducem că $x^{npq}=(y+z)^{pq}$ dezvoltând cu ajutorul binomului lui Newton membrul drept putem găsi $y' \in I$ şi $z'\in J$ a.î. $(y+z)^{pq}=y'+z'$ şi astfel $x^{npq} =(y'+z')\in I+J$, deci $x\in r(I+J)$. Obținem astfel şi incluziunea $r(r(I)+r(J))\subseteq r(I+J)$, de unde egalitatea cerută.

(vi). Fie $n\in\mathbb{N}^*$. Dacă $x\in r(I^n)$ atunci există $m\in\mathbb{N}$ a.î. $x^m\in I^n= \underbrace{I\ldots I}_{n\ ori} = \left\{ \sum_{finita} x_1....x_n \middle| x_1,....,x_n \in I \right\} \subseteq I$ deci $x^m\in I$, şi cum I este prim deducem că $x\in I$, adică $r(I^n)\subseteq I$. Cum incluziunea $I\subseteq r(I^n)$ este evidentă deducem că $r(I^n)=I$. ■

§ 11. Divizibilitatea în inele

În cadrul acestui paragraf prin A vom desemna un domeniu de integritate (adică un inel unitar comutativ nenul fără divizori ai lui zero nenuli).

Definiția 11.1. Vom spune că elementul a∈A *divide* elementul b∈B (sau că b este un *multiplu* al lui a sau că a este *divizor* al lui b) dacă există c∈A a.î. b=ac.

Dacă a nu divide b vom scrie a∤b.

În mod evident, relația de divizibilitate de pe A este o relație de preordine. Ea nu este însă în general o relație de ordine. Un contraexemplu imediat ne este oferit de inelul întregilor $\mathbb{Z}$ în care 1|-1 şi -1|1, însă 1≠-1.

Ținând cont de cele stabilite la începutul § 5 de la Capitolul 1 deducem că relația a∼b ⇔ a|b şi b|a este o echivalență pe A compatibilă cu relația de divizibilitate. Relația ∼ de pe A definită mai sus poartă numele de *relația de asociere în divizibilitate* (dacă a∼b vom spune că a este *asociat* cu b în divizibilitate).

Reamintim că pentru a∈A prin <a> am notat idealul principal generat de a (conform Observației 2.13., $<a>=\{ab \mid b\in A\}\overset{def}{=}aA$).

Rezultatul următor este imediat.

Propoziția 11.2. Relația de divizibilitate de pe A are următoarele proprietăți:

(i) Dacă a, b∈A, a|b ⇔ Ab⊆Aa

(ii) Dacă a, b∈A, a∼b ⇔există u∈U(A) a.î. a=ub ⇔ Aa=Ab

(iii) Dacă a, b_i∈A, (1≤i≤n) şi a|b_i pentru orice 1≤i≤n, atunci a|$c_1b_1+\ldots+c_nb_n$ pentru oricare elemente $c_1, c_2, \ldots, c_n$∈A.

Demonstrație. (i) „⇒”**.** Dacă a|b atunci există c∈A a.î. b=ca, deci pentru orice d∈A, db=d(ca)=(dc)a, de unde incluziunea Ab⊆Aa.

„⇐”**.** Cum b∈Ab ⊆Aa deducem că b∈Aa deci există c∈A a.î. b=ca, adică a|b.

(ii). Dacă $a \sim b$, atunci $a|b$ şi $b|a$, deci există c, $d \in A$ a.î. $b=ac$ şi $a=db$. Deducem imediat că $a=a(cd)$ şi cum A este domeniu de integritate avem că $cd=1$; analog $dc=1$, de unde concluzia că c, $d \in U(A)$ şi astfel o implicație de la prima echivalență este probată.

Fie acum $u \in U(A)$ a.î. $a=ub$. Atunci $b=u^{-1}a$, de unde concluzia că $a|b$ şi $b|a$, probând astfel complet prima echivalență.

Echivalența $a \sim b \Leftrightarrow Aa=Ab$ este imediată ținând cont de (i).

(iii). Evidentă, ținând cont de regulile de calcul într-un inel. ■

Corolarul 11.3. Dacă $a \in A$ atunci următoarele afirmații sunt echivalente:

(i) $a \sim 1$

(ii) $a \in U(A)$

(iii) $Aa=A$

(iv) $a|b$ pentru orice $b \in A$.

Definiția 11.4. Fie $a, b \in A$; un element $d \in A$ se zice *cel mai mare divizor comun* (prescurtat c.m.m.d.c) al elementelor a şi b dacă îndeplineşte următoarele condiții:

i) $d|a$ şi $d|b$

ii) Dacă mai avem $d' \in A$ a.î. $d'|a$ şi $d'|b$ atunci $d'|d$.

Observația 11.5. 1. Se deduce imediat că d_1 şi d_2 verifică condițiile i) şi ii) din definiția de mai înainte dacă şi numai dacă $d_1 \sim d_2$. Din acest motiv vom nota cu (a, b) sau c.m.m.d.c (a, b) orice element din A ce este cel mai mare divizor comun al elementelor a şi b (adică nu vom face nici o distincție între elementele asociate în divizibilitate).

2. Dacă (a, b)=1 vom spune despre a şi b că sunt *prime între ele.*

3. Deoarece pentru oricare trei elemente a, b, $c \in A$, obținem imediat din Definiția 11.4. că (a, (b, c))=((a, b), c), deducem că putem extinde noțiunea de c.m.m.d.c la un număr finit de elemente $a_1, a_2, \ldots, a_n$ ale lui A ($n \geq 2$) raționând inductiv după n.

Astfel, $(a_1, a_2, a_3) = ((a_1, a_2), a_3)$,

$(a_1, a_2, a_3, a_4) = ((a_1, a_2 a_3), a_4)$ ş.a.m.d.

Propoziția 11.6. Presupunem că în A pentru oricare două elemente există un c.m.m.d.c al lor. Atunci:

(i) $(a, b)=a \Leftrightarrow a|b$

(ii) $(a, 0)=a$

(iii) Dacă $(a, b)=d$ cu $a, b \in A^*$ şi $a=da', b=db'$, atunci $(a', b')=1$

(iv) $(ac, bc)=(a, b)c$

(v) Dacă $aA+bA=dA$, atunci $d=(a, b)$.

În particular, dacă în A suma oricăror două ideale principale este ideal principal, atunci în A oricare două elemente au un c.m.m.d.c.

Demonstrație. (i) şi (ii) sunt evidente.

(iii). Alegem $d'=(a', b')$ şi deducem imediat că $dd'|a$ şi $dd'|b$ iar cum $d=(a, b)$ obținem că $dd'|d$, adică există $c \in A$ a.î. $dd'c=d$. Deoarece $d \in A^*$ iar A este domeniu de integritate deducem că $d'c=1$ adică $d'|1$ (deci $d' \sim 1$), ceea ce ne arată că $(a', b')=1$.

(iv). Fie $d=(a, b)$ şi $d' =(ac, bc)$ (evident putem presupune că $d, c \in A$ în cazul $c=0$ sau $d=0$ totul rezultând din (ii)).

Cum $d=(a, b)$ putem scrie $a=da'$ şi $b=db'$ (cu $a', b' \in A$) astfel că $ac=(dc)a'$ şi $bc=(dc)b'$, de unde deducem că $dc|d'$, adică $dcd''=d'$ (cu $d'' \in A$).

Cum $d'=(ac, bc)$ deducem că $ac=d'a''$ şi $bc=d'b''$ (cu $a'', b'' \in A$). Obținem imediat că $ac=dcd''a''$ şi $bc=dcd''b''$ sau $dca'=dcd''a''$ şi $dcb'=dcd''b''$. Cum $dc \neq 0$ atunci $a'=d''a''$ şi $b'=d''b''$ ceea ce implică $d''|a'$ şi $d''|b'$. Deoarece $(a', b')=1$ (conform cu (iii)), atunci $d''|1$ adică $d' \sim dc$ ceea ce trebuia probat.

(v). Din $aA+bA=dA$ deducem că $aA, bA \subseteq dA$, adică $d|a$ şi $d|b$. Dacă mai avem $d' \in A$ a.î. $d'|a$ şi $d'|b$, cum $d=ax+by$ cu $x, y \in A$, deducem că $d'|d$, adică $d=(a, b)$. ■

Corolar 11.7. Presupunem că în inelul A pentru oricare două elemente a şi b există (a, b). Dacă a, b, c $\in$A a.î. a$|$bc şi (a, b)=1, atunci a$|$c.

Demonstraţie. Din (a, b)=1 şi Propoziţia 11.6. (iv), deducem că (ac, bc)=(a, b)c=c, adică a$|$c. ■

Definiţia 11.8. Dacă a, b$\in$A, un element m$\in$A se zice *cel mai mic multiplu comun* al elementelor a şi b (vom scrie prescurtat că m=c.m.m.m.c (a, b) sau m=[a, b] dacă îndeplineşte următoarele condiţii:

i) a$|$m şi b$|$m

ii) Dacă mai avem m′$\in$A a.î. a$|$m′ şi b$|$m′, atunci m$|$m′.

Observaţia 11.9. 1. Ca şi în cazul celui mai mare divizor comun se deduce imediat că dacă m şi m′ verifică condiţiile i) şi ii) din Definiţia 11.8., atunci m $\sim$ m′ (adică există u$\in$**U**(A) a.î. m=um′) .

2. Deoarece pentru oricare trei elemente a, b, c$\in$A, obţinem imediat că [a, [b, c]]=[[a, b], c], deducem că putem extinde noţiunea de c.m.m.m.c la un număr finit de elemente a_1, a_2, …, a_n ale lui A ($n\geq 2$) raţionând inductiv după n.

Astfel, $[a_1, a_2, a_3] = [[a_1, a_2], a_3]$

$[a_1, a_2, a_3, a_4] = [[a_1, a_2 a_3], a_4]$ ş.a.m.d.

3. Dacă vom considera A împreună cu relaţia de divizibilitate „$|$'' (care este o preordine pe A), atunci faţă de această ordine $(a, b)=a\wedge b$ iar $[a, b]=a\vee b$.

Legătura între c.m.m.d.c şi c.m.m.m.c ne este oferită de:

Teorema 11.10. Pentru domeniul de integritate A următoarele afirmaţii sunt echivalente:

(i) Pentru oricare două elemente a, b$\in$A există (a, b)

(ii) Pentru oricare două elemente a, b$\in$A există [a, b]

(iii) Intersecţia oricăror două ideale principale ale lui A este un ideal principal.

Demonstrație. (i)⇒(ii). Fie a, b∈A; dacă a=0 sau b=0, atunci [a, b]=0, astfel că putem presupune a≠0 şi b≠0. Dacă d=(a, b), atunci a=da′ şi b=db′ cu (a′, b′)=1. Să demonstrăm că dacă alegem m= $\frac{ab}{d}$ =ab′=a′b, atunci m=[a, b]. Avem în mod evident că a|m şi b|m şi fie m′∈A a.î. a|m′ şi b|m′. Atunci există a′′, b′′∈A a.î. m′=aa′′=bb′′; deducem imediat că da′a′′=db′b′′ şi cum d≠0 rezultă că a′a′′=b′b″ . Cum (a′, b′)=1, atunci din Propoziția 11.2. rezultă că a′′=(a′a′′, b′a′′)=(b′b′′, b′a′′) şi deci b′|a′′, adică a′′=b′a_1, astfel că m′=aa′′=ab′a_1=ma_1, deci m|m′, de unde concluzia că m=[a, b].

(ii)⇒(i). Putem presupune că a≠0 şi b≠0 şi fie m=[a, b]. Atunci m=aa′=bb′ cu a′, b′∈A.

Cum a|ab şi b|ab, deducem că m|ab, adică ab=md cu d∈A şi să demonstrăm că d=(a, b). Cum ab=aa′ d=bb′d obținem imediat că b=a′d şi a=b′d, deci d|a şi d|b.

Fie acum d′∈A a.î. d′|a şi d′|b, adică a=d′a′′ şi b=d′b′′ cu a′′, b′′∈A. Alegând m′=d′a′′b′′=ab′′=ba′′ avem că a|m′ şi b|m′, de unde deducem că m|m′, adică m′=mc cu c∈A şi astfel d′m′=d′mc. Cum d′m′=d'^2 a′′b′′=(d′a′′)(d′b′′)=ab, obținem că ab=d′mc sau md=d′mc şi astfel d=d′c , adică d′=d.

(ii)⇒(iii). Dacă m=[a, b], atunci Am⊆Aa şi Am⊆Ab, deci Am⊆Aa∩Ab. Dacă m′∈Aa∩Ab, atunci a|m′ şi b|m′, deci m|m′, adică m′∈Am, de unde şi incluziunea Aa∩Ab⊆Am, adică Aa∩Ab=Am.

(iii)⇒(ii). Se arată imediat că dacă Aa∩Ab=Am, atunci m=[a, b]. ■

Corolar 11.11. Dacă este verificată una din condițiile echivalente ale Teoremei 11.10, atunci pentru oricare două elemente a, b∈A avem egalitatea (a, b)[a, b]=ab.

Definiția 11.12. Vom spune despre un element $p \in A^* \setminus U(A)$ că este : i) *prim* dacă având a, b∈A a.î. $p \mid ab \Rightarrow p \mid a$ sau $p \mid b$

ii) *ireductibil* dacă p nu are divizori proprii (adică din p=ab cu a, b∈A deducem că unul dintre elementele a sau b este din U(A) iar celălalt este asociat în divizibilitate cu p).

Deducem imediat că dacă p este prim (ireductibil), atunci oricare alt element asociat cu p în divizibilitate este prim (ireductibil).

Propoziția 11.13. Orice element prim este ireductibil.

Demonstrație. Fie p∈A un element prim iar pentru a proba că p este ireductibil fie a, b∈A a.î. p=ab. Deducem imediat că p|a sau p|b. Dacă p|a, cum a|p deducem că p∼a, deci există u∈**U**(A) a.î. a=pu ceea ce împreună cu p=ab implică p=pub, de unde 1=ub, adică b∈**U**(A), deci p este ireductibil. ■

Observația 11.14. Există domenii de integritate în care anumite elemente ireductibile nu sunt prime.

Într-adevăr, în inelul $\mathbb{Z}[i\sqrt{5}]=\{a+ib\sqrt{5} \mid a, b\in\mathbb{Z}\}$ elementul 3 este ireductibil fără a fi însă prim. Pentru a proba acest lucru vom considera funcția $\varphi: \mathbb{Z}[i\sqrt{5}]\to\mathbb{N}$, $\varphi(a+ib\sqrt{5})=a^2+5b^2$. Prin calcul direct se probează că dacă z, $z' \in\mathbb{Z}[i\sqrt{5}]$ $\varphi(zz')=\varphi(z)\varphi(z')$ iar $z\in\mathbf{U}(\mathbb{Z}[i\sqrt{5}])\Leftrightarrow \varphi(z)=1\Leftrightarrow z=\pm 1$. Să arătăm că 3 este element ireductibil în inelul $\mathbb{Z}[i\sqrt{5}]$ iar pentru aceasta să presupunem că $3=z_1z_2$ unde $z_j=a_j+ib_j\sqrt{5}$, cu $a_j, b_j\in\mathbb{Z}$, j=1, 2. Din $\varphi(3)=\varphi(z_1z_2)=\varphi(z_1)\varphi(z_2)$ obținem că

$$9=\left(a_1^2+5b_1^2\right)\left(a_2^2+5b_2^2\right), \text{ adică } a_1^2+5b_1^2\in\{1, 3, 9\}.$$

Egalitatea $a_1^2+5b_1^2=1$, implică $a_1=\pm 1$ şi $b_1=0$, adică $z_1\in \mathbf{U}(\mathbb{Z}[i\sqrt{5}])$. Egalitatea $a_1^2+5b_1^2=3$ este imposibilă iar egalitatea $a_1^2+5b_1^2=9$ implică $\varphi(z_2)=1$, adică z_2 este inversabil în $\mathbb{Z}[i\sqrt{5}]$. Să arătăm acum că 3 nu este element prim în $\mathbb{Z}[i\sqrt{5}]$. Într-adevăr, dacă 3 ar fi prim, atunci cum $3\,|\,6=\left(1+i\sqrt{5}\right)\left(1-i\sqrt{5}\right)$ am deduce că $3\,|\,1+i\sqrt{5}$ sau $3\,|\,1-i\sqrt{5}$, adică $1+i\sqrt{5}=3\left(a+ib\sqrt{5}\right)$ sau $1-i\sqrt{5}=3\left(a'+ib'\sqrt{5}\right)$ cu $a, a', b, b'\in\mathbb{Z}$. Obţinem $3a=1$ sau $3a'=1$ –absurd!.■

CAPITOLUL 4 : INELE DE POLINOAME

§1. Inelul polinoamelor într-o nedeterminată

În cele ce urmează prin A vom desemna un inel unitar şi comutativ.

Prin $A^{\mathbb{N}}$ vom nota mulţimea funcţiilor $f:\mathbb{N}\to A$. Pentru uşurinţa scrierii vom reprezenta o funcţie $f:\mathbb{N}\to A$ în felul următor : $f=(a_0, a_1, ...,a_n,...)$ unde pentru orice $i\in\mathbb{N}$, $a_i=f(i)\in A$ (f se mai numeşte şi *şir* de elemente din A).

În mod evident, dacă mai avem $g:\mathbb{N}\to A$, $g=(b_0, b_1, ..., b_n,...)$, atunci $f=g$ dacă şi numai dacă $a_i=b_i$, pentru orice $i\in\mathbb{N}$.

Pentru $f, g\in A^{\mathbb{N}}$, $f=(a_0, a_1, ..., a_n, ...)$ şi $g=(b_0, b_1, ..., b_n, ...)$ definim f+g, $fg\in A^{\mathbb{N}}$ prin $(f+g)(i)=f(i)+g(i)$ şi $(fg)(i)=\sum_{k=0}^{i} f(k)g(i-k)$ pentru orice $i\in\mathbb{N}$.

Altfel zis, $f+g=(a_0+b_0, a_1+b_1, ..., a_n+b_n, ...)$ şi $fg=(c_0, c_1, ..., c_n, ...)$ unde $c_i=\sum_{k=0}^{i} a_k b_{i-k}$ pentru orice $i\in\mathbb{N}$. Astfel, $c_0=a_0b_0$, $c_1=a_0b_1+a_1b_0$, ..., $c_n=a_0b_n+a_1b_{n-1}+...+a_{n-1}b_1+a_nb_0$, …

Propoziția 1.1. ($A^{\mathbb{N}}$, +,·) este inel unitar comutativ.

Demonstrație. Faptul că ($A^{\mathbb{N}}$, +) este grup comutativ este imediat: asociativitatea şi comutativitatea adunării de pe $A^{\mathbb{N}}$ rezultă din asociativitatea şi comutativitatea adunării de pe A, elementul neutru este şirul nul **0**=(0, 0, ..., 0, ...) (ce are toate componentele egale cu zero), iar pentru $f = (a_0, a_1, ..., a_n, ...) \in A^{\mathbb{N}}$ opusul său -f este dat de $-f = (-a_0, -a_1, ..., -a_n, ...)$.

Comutativitatea înmulțirii de pe $A^{\mathbb{N}}$ rezultă din comutativitatea înmulțirii de pe A. Pentru a proba asociativitatea înmulțirii de pe $A^{\mathbb{N}}$, fie $f = (a_0, a_1, ..., a_n, ...)$, $g = (b_0, b_1, ..., b_n, ...)$, $h = (c_0, c_1, ..., c_n, ...)$ trei elemente oarecare din $A^{\mathbb{N}}$ şi să probăm că (fg)h=f(gh). Într-adevăr, pentru $n \in \mathbb{N}$ avem :

$$((fg)h)(n) = \sum_{i=0}^{n} (fg)(i)h(n-i) = \sum_{i=0}^{n} (\sum_{j=0}^{i} f(j)g(i-j))h(n-i)$$

$= \sum_{j+k+t=n} f(j)g(k)h(t)$ şi analog $(f(gh))(n) = \sum_{j+k+t=n} f(j)g(k)h(t)$, de unde ((fg)h)(n)=(f(gh))(n), adică (fg)h=f(gh).

Dacă notăm **1**=(1, 0, ..., 0, ...)$\in A^{\mathbb{N}}$, atunci pentru orice $f \in A^{\mathbb{N}}$ avem $f \cdot \mathbf{1} = \mathbf{1} \cdot f = f$, de unde concluzia că **1** este elementul neutru pentru înmulțirea de pe $A^{\mathbb{N}}$. Deoarece înmulțirea de pe A este distributivă față de adunarea de pe A deducem imediat că dacă f, g, h $\in A^{\mathbb{N}}$ şi $n \in \mathbb{N}$, atunci (f(g+h))(n)=f(n)(g(n)+h(n))=f(n)g(n)+f(n)h(n)=(fg)(n)+(fh)(n)= =(fg+fh)(n), adică f(g+h)=fg+fh, altfel zis înmulțirea de pe $A^{\mathbb{N}}$ este distributivă față de adunarea de pe $A^{\mathbb{N}}$ şi cu aceasta propoziția este demonstrată. ■

Observația 1.2. 1. Dacă vom considera $i_A : A \to A^{\mathbb{N}}$, $i_A(a)=(a, 0, 0,...,0,...)$ pentru orice $a \in A$, atunci i_A este morfism injectiv de inele unitare, astfel că putem identifica orice element $a \in A$ cu elementul (a, 0,..., 0, ...) din $A^{\mathbb{N}}$ şi astfel putem privi pe A ca subinel unitar al inelului $A^{\mathbb{N}}$.

2. Dacă $X = (0, 1, 0, ..., 0, ...) \in A^{\mathbb{N}}$, atunci pentru orice $n \in \mathbb{N}$ avem $X^n = (\underbrace{0,...,0}_{nori}, 1, 0, ...)$, astfel că dacă $f=(a_0, a_1, ..., a_n, ...) \in A^{\mathbb{N}}$, atunci folosind adunarea şi înmulţirea definite pe $A^{\mathbb{N}}$ ca şi identificările stabilite în prima parte a acestei observaţii avem:

$f= (a_0, a_1, ..., a_n, ...) = (a_0, 0, ...) + (0, a_1, 0, ...) + ... = (a_0, 0, ...) + +(a_1, 0, ...) (0, 1, 0,...) + (a_2, 0, ...) (0, 0, 1, 0, ...) +...+ (a_n, 0, ...) (\underbrace{0,0,...,0}_{nori}, 1, 0, ...) +... =(a_0, 0, ...) + (a_1, 0, ...) X + (a_2, 0, ...) X^2+...+ +(a_n, 0, ...) X^n+...= a_0+a_1X+...+a_nX^n+...$

Obţinem astfel scrierea obişnuită a unei serii formale. Această observaţie ne permite să dăm următoarea definiţie :

Definiţia 1.3. Inelul $(A^{\mathbb{N}}, +, \cdot)$ se *numeşte inelul seriilor formale în nedeterminata X cu coeficienţi din A* şi se notează prin A[[X]].

Un element f din A[[X]] se va scrie condensat sub forma $f=\sum_{i\geq 0} a_i X^i$ (aceasta fiind doar o notaţie, fără sens de adunare).

Definiţia 1.4. O serie formală $f = \sum_{i\geq 0} a_i X^i \in A[[X]]$ cu proprietatea că $\{ i \in \mathbb{N} \mid a_i \neq 0\}$ este finită se numeşte *polinom* cu coeficienţi în A.

Vom nota prin A[X] mulţimea polinoamelor cu coeficienţi în A. Polinoamele de forma aX^n cu $a \in A^*$ se zic *monoame*.

Astfel, dacă $f=\sum_{i\geq 0} a_i X^i \in A[X]$, atunci există $n \in \mathbb{N}$ a.î. $a_i=0$ pentru orice $i \in \mathbb{N}$, $i \geq n+1$; în acest caz vom scrie $f=a_0+a_1X+...+a_nX^n$ sau $f=\sum_{i=0}^{n} a_i X^i$.

În cazul *polinomului nul*, $a_i=0$ pentru orice $i \in \mathbb{N}$; dacă nu este pericol de confuzie convenim să notăm prin **0** polinomul nul.

Observația 1.5. Fie $f=\sum_{i=0}^{n} a_i X^i$, $g=\sum_{i=0}^{m} b_i X^i$ două polinoame din A[X]. Cum în particular f şi g sunt funcții de la $\mathbb{N}$ la A deducem că f=g dacă şi numai dacă m=n şi $a_i=b_i$ pentru orice $0 \le i \le n$.

În particular, f=**0** dacă şi numai dacă $a_i=0$ pentru orice $0 \le i \le n$ şi $f \neq 0$ dacă şi numai dacă există $0 \le i \le n$ a.î. $a_i \neq 0$.

Definiția 1.6. Pentru polinomul nul $0 \in A[X]$ definim *gradul* său ca fiind $-\infty$ iar pentru $f \in A[X]$, $f \neq 0$ definim *gradul* lui f ca fiind

$$\mathbf{grad(f)=max\{i \mid a_i \neq 0\}.}$$

Astfel, dacă $f \neq 0$ şi $grad(f)=n \ge 1$, atunci f se poate scrie sub forma

$$f=a_0+a_1X+...+a_nX^n \text{ şi } a_n \neq 0.$$

În acest caz, a_n se zice *coeficientul dominant* al lui f; dacă $a_n=1$, f se mai zice *monic*.

Dacă grad(f)=0, atunci f=a cu $a \in A$; spunem în acest caz că f este *polinom constant*.

Propoziția 1.7. A[X] este subinel al inelului A[[X]].

Demonstrație. Fie $f=a_0+a_1X+...+a_nX^n$ şi $g=b_0+b_1X+...+b_mX^m$ două polinoame din A[X] de grade n şi respectiv m. Dacă de exemplu $n \le m$, atunci $f-g=(a_0-b_0)+(a_1-b_1)X+...+(a_n-b_n)X^n+(-b_{n+1})X^{n+1}+...+(-b_m)X^m \in A[X]$ iar $fg=a_0b_0+(a_0b_1+a_1b_0)X+...+a_nb_mX^{n+m} \in A[X]$. De asemenea, polinomul constant $\mathbf{1} \in A[X]$. ■

Definiția 1.8. Inelul A[X] poartă numele de *inelul polinoamelor în nedeterminata X cu coeficienți în inelul A* sau mai pe scurt, *inelul polinoamelor într-o nedeterminată.*

Propoziția 1.9. Dacă $f, g \in A[X]$, atunci:
(i) $grad(f+g) \le max\{grad(f), grad(g)\}$
(ii) $grad(fg) \le grad(f) + grad(g)$.

Demonstrație. Dacă f=g=**0** totul este clar. De asemenea, dacă de exemplu f=**0** şi $g \neq \mathbf{0}$ (ținând cont de convențiile de calcul cu $\pm\infty$).

Dacă $f\neq \mathbf{0}$ şi $g\neq \mathbf{0}$ inegalităţile de la (i) şi (ii) rezultă imediat din felul în care se efectuează f+g şi fg (vezi demonstraţia Propoziţiei 1.7.). ■

Observaţia 1.10.

1. Fie $f=a_o+a_1X+...+a_nX^n$ şi $g=b_0+b_1X+...+b_mX^m$ două polinoame din A[X] de grade n şi respectiv m (adică $a_n\neq 0$ şi $b_m\neq 0$). Dacă a_n şi b_m nu sunt divizori ai lui zero în A, cum $fg=a_0b_0+(a_0b_1+a_1b_0)X+...+a_nb_mX^{n+m}$ deducem că $a_nb_m\neq 0$ şi astfel grad(fg)=grad(f)+grad(g). Astfel, dacă A este domeniu de integritate, atunci pentru orice f, g∈A[X], grad(fg)=grad(f)+grad(g). Dacă A nu este domeniu de integritate, atunci inegalitatea (ii) de la Propoziţia 1.9. poate fi strictă. Într-adevăr, dacă $A=\mathbb{Z}_4$, $f=g=\hat{2}X$, atunci grad(f)=grad(g)=1, pe când $fg=\hat{4}X^2=0$ şi astfel grad(fg)=-∞ <1.

Propoziţia 1.11. Fie $f=a_0+a_1X+...+a_nX^n\in \mathbf{A}[X]$. Atunci:

(i) $f\in \mathbf{U}(A[X]) \Leftrightarrow a_0\in \mathbf{U}(A)$ iar $a_1, ..., a_n\in \mathbf{N}(A)$ (reamintim că prin N(A) am notat mulţimea elementelor nilpotente din A)

(ii) f este divizor al lui zero în A[X] $\Leftrightarrow$ există $a\in A^*$ a.î. af=0.

Demonstraţie. (i). "$\Rightarrow$". Dacă $f\in \mathbf{U}(A[X])$, atunci există $g=b_0+b_1X+...+b_mX^m\in A[X]$ a.î. $fg=1 \Leftrightarrow$

$$(*)\quad \begin{cases} a_0b_0=1 \\ a_0b_1+a_1b_0=0 \\ a_0b_2+a_1b_1+a_2b_0=0 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n-1}b_m+a_nb_{m-1}=0 \\ a_nb_m=0 \end{cases}$$

Din prima egalitate din (∗) deducem că $a_0\in \mathbf{U}(A)$. Înmulţind ambii membrii ai penultimei egalităţi din (∗) cu a_n şi ţinând cont de ultima egalitate deducem că $a_n^2b_{m-1}=0$. Inductiv deducem că $a_n^{m+1}b_0=0$, de unde $a_n^{m+1}=0$ (căci $b_0\in \mathbf{U}(A)$), adică $a_n\in \mathbf{N}(A)$. Atunci $a_nX^n\in \mathbf{N}(A[X])$ şi cum $f\in \mathbf{U}(A[X])$ deducem (ţinând cont de Observaţia 2.9. de la Capitolul 3) că $f_1=f-a_nX^n\in \mathbf{U}(A[X])$. Cum $f_1=a_0+a_1X+...+a_{n-1}X^{n-1}$

deducem că $a_{n-1} \in \mathbf{N}(A)$. Raţionând acum inductiv deducem că a_{n-2}, ..., a_2, $a_1 \in \mathbf{N}(A)$.

"$\Leftarrow$". Să presupunem că $a_0 \in \mathbf{U}(A)$ (deci $a_0 \in \mathbf{U}(A[X])$) şi a_1, a_2, ..., $a_n \in \mathbf{N}(A)$. Atunci a_1, ..., $a_n \in \mathbf{N}(A[X])$ şi cum $\mathbf{N}(A[X])$ este ideal în A[X] (conform Observaţiei 2.9. de la Capitolul 3) deducem că a_1X, a_2X^2, $a_nX^n \in \mathbf{N}(A[X])$ deci şi $a_1X+a_2X^2+...+a_nX^n \in \mathbf{N}(A[X])$. Cum $a_0 \in \mathbf{U}(A[X])$ iar $f=a_0+(a_1X+...+a_nX^n)$ deducem că $f \in \mathbf{U}(A[X])$ (conform Observaţiei 2.9. de la Capitolul 3).

(ii). "$\Leftarrow$". Evidentă.

"$\Rightarrow$". Să presupunem că f este divizor al lui zero în A[X] şi fie $g=b_0+b_1X+...+b_mX^m \in A[X]$ un polinom nenul de grad minim pentru care fg=0. Atunci $a_nb_m=0$ şi cum $g_1=a_ng=a_nb_0+a_nb_1+...+a_nb_{m-1}X^{m-1}$ are gradul $\leq$ m-1<m şi $g_1f=0$, datorită minimalităţii lui m deducem că $g_1=\mathbf{0}$, adică $a_nb_0=a_nb_1=...=a_nb_{m-1}=0$. Inductiv se arată că $a_{n-k}g=0$ pentru $0 \leq k \leq n$ şi deci $a_ib_j=0$ pentru orice $0 \leq i \leq n$, $0 \leq j \leq m$. Cum $g \neq \mathbf{0}$ există $0 \leq j \leq m$ a.î. $b_j \neq 0$.

Cum $b_ja_i=0$ pentru orice $0 \leq i \leq n$ deducem că $b_jf=\mathbf{0}$. ■

Corolar 1.12. Dacă A este domeniu de integritate atunci

(i) $f=a_0+a_1X+...+a_nX^n \in \mathbf{U}(A[X]) \Leftrightarrow a_1=a_2=...=a_n=0$ iar $a_0 \in \mathbf{U}(A)$ (altfel zis, $f \in \mathbf{U}(A[X])$ dacă şi numai dacă $f=a_0$, cu $a_0 \in \mathbf{U}(A)$).

(ii) A[X] este domeniu de integritate.

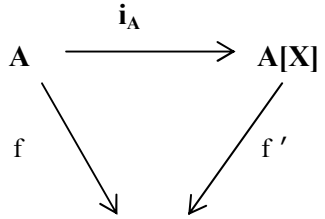
Demonstraţie.(i). Rezultă imediat din Propoziţia 1.11., (i) deoarece în cazul în care A este domeniu de integritate, $\mathbf{N}(A)=\{0\}$.

(ii). Să arătăm că dacă $f \in A[X]$ este divizor al lui 0 în A[X], atunci f=0. Alegem $f=a_0+a_1X+...+a_nX^n \in A[X]$ şi conform Propoziţiei 1.11. (ii), există $b \in A^*$ a.î. $bf=0 \Leftrightarrow ba_i=0$, pentru orice $0 \leq i \leq n$. Cum $b \in A^*$ iar A este domeniu de integritate deducem că $a_i=0$ pentru orice $0 \leq i \leq n$, adică f=0. ■

Aplicaţia $i_A:A \to A[X]$, $i_A(a)=a$ pentru orice $a \in A$ este morfism injectiv de inele unitare (numit *morfismul canonic de scufundare* al lui A în A[X]).

În continuare vom prezenta o proprietate importantă a inelului de polinoame A[X], numită ***proprietatea de universalitate*** a inelelor de polinoame într-o nedeterminată.

Teorema 1.13. Pentru orice inel unitar, comutativ B, orice element $b \in B$ şi orice morfism de inele $f \in Hom(A, B)$, există un unic morfism de inele unitare $f' \in Hom(A[X], B)$ a.î. $f'(X)=b$ iar diagrama:



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

Demonstraţie. Fie $P=a_0+a_1X+...+a_nX^n \in A[X]$ şi să arătăm că dacă definim $f'(P)=f(a_0)+f(a_1)b+...+f(a_n)b^n$, atunci f' este morfismul de inele căutat. Avem $f'(1)=f(1)=1$, iar dacă mai avem $Q=b_0+b_1X+...+b_mX^m \in A[X]$ cu $m \leq n$, atunci scriind şi pe Q sub forma $Q=b_0+b_1X+...+b_nX^n$ cu $b_{m+1}=...=b_n=0$, avem

$P+Q=\sum_{i=1}^{n}(a_i+b_i)X^i$, $PQ=\sum_{i=0}^{m+n}c_iX^i$ cu $c_i=\sum_{k=0}^{i}a_kb_{i-k}$ $(0 \leq i \leq m+n)$ astfel că

$f'(P+Q)=\sum_{i=0}^{n}f(a_i+b_i)b^i=\sum_{i=0}^{n}(f(a_i)+f(b_i))b^i=$

$=\sum_{i=0}^{n}f(a_i)b^i+\sum_{i=0}^{n}f(b_i)b^i=f'(P)+f'(Q)$ iar $f'(PQ)=\sum_{i=0}^{m+n}f(c_i)b^i$.

Cum $c_i=\sum_{k=0}^{i} a_k b_{i-k}$ pentru orice $0\le i\le m+n$ avem $f(c_i)=\sum_{k=0}^{i} f(a_k)f(b_{i-k})$ astfel că $f'(PQ)=\sum_{i=0}^{m+n}(\sum_{k=0}^{i} f(a_k)f(b_{i-k}))b^i =$ $=f'(P)f'(Q)$, adică $f'\in$**Hom**$(A[X], B)$.

Dacă $a\in A$, atunci $(f'\circ i_A)(a)=f'(i_A(a))=f'(a)$, adică $f'\circ i_A=f$.

Să presupunem acum că mai avem $f''\in$**Hom**$(A[X], B)$ a.î. $f''(X)=b$ şi $f''\circ i_A=f$. Atunci, pentru $P=a_0+a_1X+...+a_nX^n\in A[X]$ avem $f''(P)=f''(a_0+a_1X+...+a_nX^n)=f''(a_0)+f''(a_1)f''(X)+...+f''(a_n)(f(X))^n =$ $=f(a_0)+f(a_1)b+...+f(a_n)b^n=f'(P)$, adică $f''=f'$. ■

Definiția 1.14. Dacă $f=a_0+a_1X+...+a_nX^n\in A[X]$, atunci $\tilde{f}:A\to A$, $\tilde{f}(a)=a_0+a_1a+...+a_na^n$ pentru orice $a\in A$ poartă numele de *funcția polinomială ataşată lui f.* Vom spune despre o funcție $g:A\to A$ că este *polinomială* dacă există $f\in A[X]$ a.î. $g=\tilde{f}$.

Observația 1.15. 1. Dacă $f, g\in A[X]$ şi $f=g$ (ca polinoame), atunci în mod evident $\tilde{f}=\tilde{g}$ (ca funcții).

2. Reciproca primei observații nu este adevărată pentru orice inel A.

Într-adevăr, considerând $A=\mathbb{Z}_2$, $f=\hat{1}+X$, $g=\hat{1}+X^2$, atunci $\tilde{f}(\hat{0})=\tilde{g}(\hat{0})=\hat{1}$, $\tilde{f}(\hat{1})=\tilde{g}(\hat{1})=\hat{0}$, deci $\tilde{f}=\tilde{g}$, pe când $f\neq g$.

3. Se probează imediat că dacă $f, g\in A[X]$, atunci $\widetilde{f\pm g}=\tilde{f}\pm\tilde{g}$ şi $\widetilde{fg}=\tilde{f}\tilde{g}$.

§2. Inelul polinoamelor în mai multe nedeterminate

În paragraful precedent am construit inelul polinoamelor într-o nedeterminată. În cadrul acestui paragraf vom construi inductiv inelul

polinoamelor într-un număr finit de nedeterminate punând apoi în evidență principalele proprietăți ale unor astfel de polinoame. Reamintim că prin A am desemnat un inel unitar comutativ.

Definiția 2.1. Inelul polinoamelor în nedeterminatele $X_1, X_2, ..., X_n$ ($n \geq 2$) cu coeficienți în inelul A, notat prin $A[X_1, X_2, ..., X_n]$ se defineşte inductiv astfel: $A[X_1]$ este inelul polinoamelor în nedeterminata X_1 cu coeficienți din A, $A[X_1, X_2]$ este inelul polinoamelor în nedeterminata X_2 cu coeficienți din inelul $A[X_1]$ şi în general $A[X_1, X_2, ..., X_n]$ este inelul polinoamelor în nedeterminata X_n cu coeficienți din inelul $A[X_1, ..., X_{n-1}]$.

Astfel, o dată construit $A[X_1]$ avem $A[X_1, X_2]=A[X_1][X_2]$, ..., $A[X_1, X_2, ..., X_n]=A[X_1, X_2, ..., X_{n-1}][X_n]$. Analog, plecând de la inelul seriilor formale $A[[X_1]]$ se construieşte inductiv inelul $A[[X_1, ..., X_n]]$ al seriilor formale cu coeficienți din A prin $A[[X_1, ..., X_n]]= =A[[X_1, ..., X_{n-1}]] [[X_n]]$.

Dacă $f \in A[X_1, ..., X_n]=A[X_1, ..., X_{n-1}][X_n]$, atunci $f=f_0+f_1X_n+...+f_{t_n} X^{t_n}$ cu $f_i \in A[X_1, ..., X_{n-1}]$ pentru $0 \leq i \leq t_n$. Scriind la rândul lor pe $f_0, f_1, ..., f_{t_n}$ ca polinoame în X_{n-1} cu coeficienți în $A[X_1, ..., X_{n-2}]$, ş.a.m.d., deducem că f se scrie ca o sumă finită de forma (∗) $f = \sum_{i_1,...,i_n=0}^{t_1,t_2,...,t_n} a_{i_1 i_2 ... i_n} X_1^{i_1} ... X_n^{i_n}$ (în care $a_{i_1 ... i_n} \in A$ se numesc *coeficienții* lui f).

Observația 2.2. Făcând inducție matematică după n se arată imediat că scrierea lui f sub forma (∗) este unică (echivalent cu a arăta că $f = \mathbf{0}$ dacă şi numai dacă toți coeficienții $a_{i_1 i_2 ... i_n}=0$).

Definiția 2.3. Un polinom de forma $aX_1^{i_1} ... X_n^{i_n}$ cu $a \in A^*$ iar $i_1, i_2, ..., i_n \in \mathbb{N}$ se numeşte *monom* iar prin gradul său înțelegem numărul natural $i_1+i_2+...+i_n$ (convenim să scriem $grad(aX_1^{i_1} ... X_n^{i_n})= = i_1+...+i_n$).

Astfel, un polinom $f \in A[X_1, ..., X_n]$ se scrie în mod unic ca sumă finită de monoame nenule din $A[X_1, ..., X_n]$.

$$f=\sum_{i_1,\ldots,i_n=0}^{t_1,\ldots,t_n} a_{i_1\ldots i_n} X_1^{i_1}\ldots X_n^{i_n}\ .$$

Monoamele nenule din scrierea lui f se numesc *termenii* lui f.

Gradul lui f se defineşte astfel:

$$\text{grad}(f)=\begin{cases} -\infty\ , \text{ dacă } f=\mathbf{0} \\ \\ \text{maximul gradelor termenilor săi, dacă } f\neq \mathbf{0}. \end{cases}$$

Astfel, dacă $f=2X_1^2-3X_1X_2^2+4X_1X_2X_3\in\mathbb{Z}[X_1, X_2, X_3]$, atunci

$$\text{grad}(f)=\max\{2, 1+2, 1+1+1\}=\max\{2, 3, 3\}=3.$$

Observăm deci că în cadrul unui polinom f de mai multe variabile pot să apară termeni diferiţi (în cazul exemplului nostru fiind monoamele $-3X_1X_2^2$ şi $4X_1X_2X_3$) care însă să aibă acelaşi grad, astfel că nu putem vorbi de un termen bine individualizat de grad maxim (ca în cazul polinoamelor de o singură nedeterminată în care termenii se pot ordona după puterile nedeterminatei).

Pentru monoamele nenule ale unui polinom de mai multe variabile putem defini o ordonare cu ajutorul ordonării lexicografice (vezi §5 de la Capitolul 1). Mai precis, dacă $n\geq 2$, $M_1=aX_1^{i_1}\ldots X_n^{i_n}$, $M_2=bX_1^{j_1}\ldots X_n^{j_n}\in A[X_1, \ldots, X_n]$ cu $a, b\in A^*$, atunci definim $M_1\leq M_2 \Leftrightarrow$

$\Leftrightarrow (i_1, \ldots, i_n)\leq(j_1, \ldots, j_n)$ (în ordonarea lexicografică de pe $\mathbb{N}^n$!).

Astfel, $M_1\leq M_2 \Leftrightarrow$ există $1\leq k\leq n$ a.î. $i_1=i_2,\ldots,i_k=j_k$ şi $i_{k+1}<j_{k+1}$.

De exemplu, în $\mathbb{Z}[X_1, X_2, X_3]$: $2X_1^2X_2^3X_3^4\leq -4X_1^2X_2^3X_3^5$, $X_1\leq X_1X_2X_3$.

În general, având un polinom nenul $f\in A[X_1, \ldots, X_n]$, cum acesta se poate scrie ca sumă finită de monoame nenule din $A[X_1, \ldots, X_n]$, cu ajutorul ordonării lexicografice de pe $A[X_1, \ldots, X_n]$ putem individualiza un monom nenul care să fie cel mai mare în ordonarea lexicografică. Acest termen se numeşte *termenul principal* al polinomului f (convenim să-l notăm prin $t_p(f)$).

Astfel, dacă în $\mathbb{Z}[X_1, X_2, X_3]$ considerăm polinoamele $f=X_1+X_2+X_3$, $g=X_1X_2+X_2X_3+X_3X_1$ şi $h=X_1X_2^2X_3-4X_1X_2^2X_3^4$ atunci $t_p(f)=X_1$, $t_p(g)=X_1X_2$ iar $t_p(h)=-4X_1X_2^2X_3^4$.

Observaţia 2.4. 1. Cum ordonarea lexicografică este o relaţie de ordine (parţială) pe $A[X_1, ..., X_n]$, dacă avem M_1, M_2, N_1, N_2 patru monoame nenule din $A[X_1, ..., X_n]$ a.î. $M_1 \le M_2$ şi $N_1 \le N_2$, atunci $M_1N_1 \le M_2N_1$ şi $M_1N_1 \le M_2N_2$.

2. În consecinţă, dacă produsul termenilor principali a două polinoame nenule din $A[X_1, ..., X_n]$ este un monom nenul, atunci acesta este termenul principal al produsului celor două polinoame.

Să revenim acum asupra problemei gradului unui polinom din $A[X_1,...,X_n]$.

Definiţia 2.5. Dacă toţi termenii unui polinom f din $A[X_1, ..., X_n]$ au acelaşi grad, vom spune despre f că este *polinom omogen* sau *formă*.

Fiind date două polinoame omogene f şi g din $A[X_1, ..., X_n]$ atunci produsul lor fg este sau polinomul nul sau un polinom omogen de grad egal cu grad(f)+grad(g).

Observaţia 2.6. Orice polinom nenul $f \in A[X_1, ..., X_n]$ de grad n se poate scrie în mod unic sub forma $f=f_0+f_1+...+f_n$ unde fiecare f_i, $0 \le i \le n$ este sau nul sau polinom omogen de grad i. Polinoamele omogene nenule f_i, $0 \le i \le n$ din scrierea lui f de mai sus se numesc *componentele omogene* ale polinomului f.

Propoziţia 2.7. Pentru orice $f, g \in A[X_1, ..., X_n]$ avem:
(i) $grad(f+g) \le max\{ grad(f), grad(g) \}$
(ii) $grad(fg) \le grad(f)+grad(g)$.

Demonstraţie. Atât (i) cât şi (ii) sunt clare dacă ţinem cont de scrierea polinoamelor f şi g ca sume de polinoame omogene. ■

Propoziţia 2.8. Dacă A este domeniu de integritate, atunci şi $A[X_1, ..., X_n]$ este domeniu de integritate iar în acest caz pentru orice $f, g \in A[X_1,...,X_n]$ avem $grad(fg)=grad(f)+grad(g)$.

Demonstrație. Vom face inducție matematică după n, pentru n=1 totul fiind clar dacă ținem cont de cele stabilite în paragraful precedent.

Cum $A[X_1, ..., X_n]=A[X_1, ..., X_{n-1}][X_n]$, dacă presupunem că $A[X_1, ..., X_{n-1}]$ este domeniu de integritate, atunci şi $A[X_1, ..., X_n]$ va fi domeniu de integritate.

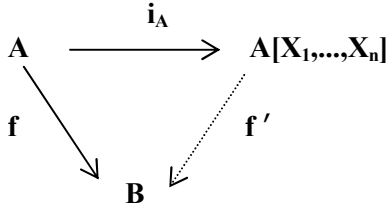
Fie acum f, g polinoame nenule din $A[X_1, ..., X_n]$ de grad m şi respectiv n. Atunci scriem pe f şi g sub forma $f=f_0+f_1+...+f_m$, $g=g_0+g_1+...+g_n$ cu $f_m \neq 0$, $g_n \neq 0$ iar f_i, g_i sunt sau nule sau polinoame omogene de grad i, respectiv j, $0 \leq i \leq m-1$, $0 \leq j \leq n-1$. Avem $fg=\sum_{k=0}^{m+n} h_k$ cu $h_k=\sum_{i+j=k} f_i g_j$ $(0 \leq k \leq m+n)$. Cum $A[X_1, ..., X_n]$ este domeniu de integritate avem $h_{m+n}=f_m g_n$, de unde relația grad(fg)=grad(f)+grad(g). ■

Funcția $i_A: A \to A[X_1, ..., X_n]$ definită prin $i_A(a)=a$ pentru orice $a \in A$ este un morfism injectiv de inele unitare (numit *morfismul canonic* de scufundare a lui A în $A[X_1, ..., X_n]$).

Să observăm că în notarea morfismului canonic de scufundare a lui A în $A[X_1, ..., X_n]$ ar fi trebuit să amintim şi de n. Nu am făcut lucrul acesta pentru a nu complica notația, însă dacă este pericol de confuzie vom face şi lucrul acesta.

Suntem acum în măsură să prezentăm *proprietatea de universalitate* a inelelor de polinoame în mai multe nedeterminate (de fapt o generalizare a Teoremei 1.13.).

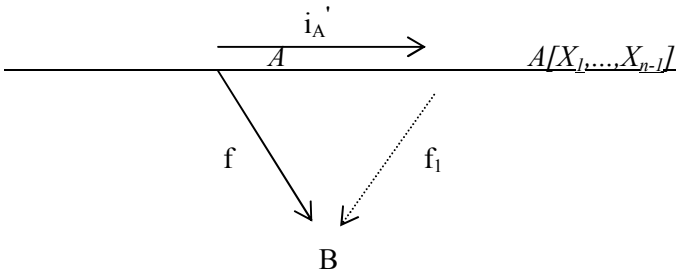
Teorema 2.9. Fie $n \in \mathbb{N}$, $n \geq 2$, B un inel unitar comutativ, $f: A \to B$ un morfism de inele unitare şi $b_1, ..., b_n \in B$. Atunci există un unic morfism de inele unitare $f' : A[X_1, ..., X_n] \to B$ a.î. $f'(X_i)=b_i$ pentru orice $1 \leq i \leq n$ iar diagrama



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

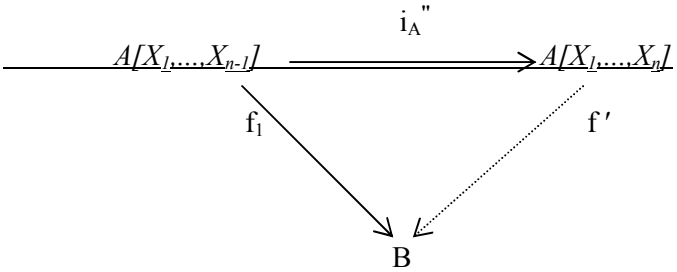
Demonstrație. Facem inducție matematică după n (pentru n=1 rezultatul fiind adevărat conform Teoremei 1.13.).

Să presupunem acum afirmația din enunț adevărată pentru n-1 şi să o demonstrăm pentru n. Avem deci un unic morfism de inele unitare $f_1: A[X_1,...,X_{n-1}] \to B$ a.î. $f_1(X_i)=b_i$, $1 \le i \le n-1$ şi diagrama



este comutativă, adică $f_1 \circ i_A' = f$ (i_A' fiind morfismul canonic de la A la $A[X_1,...,X_{n-1}]$).

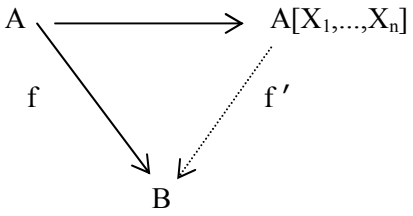
Cum $A[X_1,...,X_n]=A[X_1,...,X_{n-1}][X_n]$, conform Teoremei 1.13. avem un morfism de inele unitare $f': A[X_1, ..., X_n] \to B$ a.î. $f'(X_n)=b_n$ şi diagrama



este comutativă (adică $f' \circ i_A'' = f_1$), unde i_A'' este morfismul canonic de la $A[X_1, ..., X_{n-1}]$ la $A[X_1, ..., X_{n-1}][X_n]=A[X_1, ..., X_n]$.

În mod evident, $i_A = i_A'' \circ i_A'$ şi obținem din cele două diagrame comutative de mai înainte diagrama comutativă

i_A

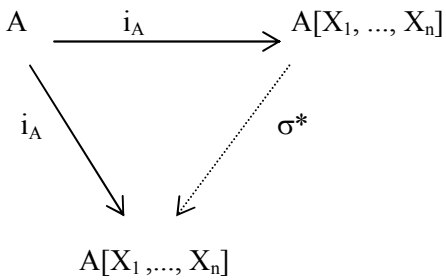


În mod evident $f'(X_i)=b_i$ pentru orice $1 \le i \le n$. Unicitatea lui f' rezultă din unicitatea lui f_1 şi a faptului că $f' \circ i_A''=f_1$.

Conform principiului inducţiei matematice teorema este adevărată pentru orice $n \in \mathbb{N}$, $n \ge 1$. ■

§3. Polinoame simetrice

Păstrând notaţiile de la paragrafele precedente, dacă $\sigma \in S_n$ este o permutare ($n \ge 2$) atunci conform proprietăţii de universalitate a inelului de polinoame $A[X_1, ..., X_n]$, există un unic morfism de inele unitare $\sigma^*: A[X_1, ..., X_n] \to A[X_1, ..., X_n]$ a.î. $\sigma^*(X_i)=X_{\sigma(i)}$ pentru orice $1 \le i \le n$ iar diagrama



este comutativă (adică pentru orice $a \in A$, $\sigma^*(a)=a$). În general, dacă avem $f \in A[X_1, ..., X_n]$, $f=\sum_{i_1,i_2,...,i_n=0}^{t_1,t_2,...,t_n} a_{i_1 i_2 ... i_n} X_1^{i_1} ... X_n^{i_n}$, atunci

$$\sigma^*(f)=\sum_{i_1,i_2,...,i_n=0}^{t_1,t_2,...,t_n} a_{i_1 i_2 ... i_n} X_{\sigma(1)}^{i_1} ... X_{\sigma(n)}^{i_n}.$$

Dacă avem de exemplu $f=X_1^2-2X_1X_2-X_2X_3^2\in\mathbb{Z}[X_1,X_2,X_3]$ iar $\sigma=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\in S_3$, atunci $\sigma^*(f)=X_3^2-2X_3X_1-X_1X_2^2$.

Observația 3.1. 1. Dacă $\sigma,\tau\in S_n$, atunci $(\sigma\tau)^*=\sigma^*\circ\tau^*$.

2. Dacă $e\in S_n$ este permutarea identică, atunci $e^*=1_{A[X_1,\ldots,X_n]}$.

3. Dacă $\sigma\in S_n$, atunci $\sigma^*:A[X_1,\ldots,X_n]\to A[X_1,\ldots,X_n]$ este izomorfism de inele unitare (ținând cont de prima parte a acestei observații deducem că inversul lui σ^* este $(\sigma^{-1})^*$).

Definiția 3.2. Vom spune că un polinom $f\in A[X_1,\ldots,X_n]$ $(n\geq 2)$ este *simetric* dacă pentru orice $\sigma\in S_n$, $\sigma^*(f)=f$, altfel zis, oricum am permuta (schimba) variabilele lui f acesta rămâne neschimbat (spunem că f rămâne invariant la σ).

Cum orice permutare din S_n este un produs de transpoziții (Corolarul 10.9. de la Capitolul 2), atunci un polinom din $A[X_1,\ldots,X_n]$ este simetric dacă şi numai dacă f rămâne invariant la orice transpoziție din S_n. Vom nota prin $\mathbf{S}(A[X_1,\ldots,X_n])$ mulțimea polinoamelor simetrice din $A[X_1,\ldots,X_n]$.

Propoziția 3.3. $S(A[X_1,\ldots,X_n])$ este subinel unitar al inelului $A[X_1,\ldots,X_n]$.

Demonstrație. În mod evident, polinoamele constante din $A[X_1,\ldots,X_n]$ (deci şi **1**) fac parte din $\mathbf{S}(A[X_1,\ldots,X_n])$ iar dacă f, $g\in\mathbf{S}(A[X_1,\ldots,X_n])$ şi $\sigma\in S_n$, cum σ^* este morfism de inele unitare avem $\sigma^*(f-g)=\sigma^*(f)-\sigma^*(g)=f-g$ şi $\sigma^*(fg)=\sigma^*(f)\sigma^*(g)=fg$, de unde deducem că f-g, $fg\in\mathbf{S}(A[X_1,\ldots,X_n])$, adică $\mathbf{S}(A[X_1,\ldots,X_n])$ este subinel unitar al lui $A[X_1,\ldots,X_n]$.

Observația 3.4. După cum am văzut în paragraful precedent, orice polinom $f\in A[X_1,\ldots,X_n]$ se scrie în mod unic sub forma $f=f_0+f_1+\ldots+f_k$ unde fiecare f_i este un polinom omogen de grad i $(0\leq i\leq k)$ din $A[X_1,\ldots,X_n]$. Astfel, dacă $\sigma\in S_n$, atunci $\sigma^*(f)=\sigma^*(f_0+f_1+\ldots+f_k)=\sigma^*(f_0)+\sigma^*(f_1)+\ldots+\sigma^*(f_k)$. Deoarece $\sigma^*(f_i)$,

$0 \le i \le k$ este tot un polinom omogen de grad i, deducem din unicitatea scrierii lui f sub forma $f=f_0+f_1+...+f_k$ că $\sigma^*(f)=f \Leftrightarrow \sigma^*(f_i)=f_i$ pentru orice $0 \le i \le k$.

Altfel zis, un polinom f din $A[X_1, ..., X_n]$ este simetric dacă şi numai dacă fiecare componentă omogenă a sa este un polinom simetric.

Această observaţie ne permite ca de multe ori atunci când raţionăm relativ la un polinom $f \in \mathbf{S}(A[X_1, ..., X_n])$ să-l considerăm şi omogen.

Să considerăm acum polinoamele $\mathbf{S_1, S_2, ..., S_n}$ din $A[X_1, ..., X_n]$ definite prin :

$$\mathbf{S_1}=X_1+X_2+...+X_n=\sum_{1\le i\le n} X_i$$

$$\mathbf{S_2}=X_1X_2+X_1X_3+...+X_{n-1}X_n=\sum_{1\le i<j\le n} X_iX_j$$

.....

$$\mathbf{S_n}=X_1X_2...X_n.$$

Propoziţia 3.5. $\mathbf{S_1}, \mathbf{S_2}, ..., \mathbf{S_n} \in \mathbf{S}(A[X_1, ..., X_n])$.

Demonstraţie. Vom considera polinomul $g=(X-X_1)(X-X_2)...(X-X_n)$ din $A[X_1, ..., X_n, X]$ care se mai poate scrie şi sub forma $g=X^n-\mathbf{S_1}X^{n-1}+\mathbf{S_2}X^{n-2}-...+ +(-1)^n\mathbf{S_n}$.

Pentru $\sigma \in S_n$ avem morfismul de inele unitare $\sigma^*:A[X_1, ..., X_n] \to A[X_1, ..., X_n]$ cu ajutorul căruia şi al Teoremei 2.9. găsim morfismul unitar de inele $\sigma^{**}:A[X_1, ..., X_n, X] \to A[X_1, ..., X_n, X]$ pentru care $\sigma^{**}(X_i)=X_{\sigma(i)}=\sigma^*(X_i)$ pentru orice $1 \le i \le n$, $\sigma^{**}(X)=X$ şi $\sigma^{**}(a)=a$ pentru orice $a \in A$.

De fapt, dacă vom considera permutarea σ' din S_{n+1} cu proprietatea că $\sigma'(i)=\sigma(i)$ pentru orice $1 \le i \le n$ şi $\sigma(n+1)=n+1$, atunci numerotând eventual pe X prin X_{n+1}, σ^{**} este de fapt σ'^*.

Atunci $\sigma^{**}(g)=\sigma^{**}((X-X_1)...(X-X_n))=\sigma^{**}(X-X_1)...\sigma^{**}(X-X_n)=$ $=(X-X_{\sigma(1)})...(X-X_{\sigma(n)})=(X-X_1)...(X-X_n)=g$ iar pe de altă parte $\sigma^{**}(g)=\sigma^{**}(X^n-\mathbf{S_1}X^{n-1}+\mathbf{S_2}X^{n-2}-...+(-1)^n\mathbf{S_n})=X^n-\sigma^*(\mathbf{S_1})X^{n-1}+\sigma^*(\mathbf{S_2})X^{n-2}-$ $-...+(-1)^n\sigma^*(\mathbf{S_n})$.

Comparând cele două expresii ale lui $\sigma^{**}(g)$ deducem că $\sigma^*(S_i)=S_i$ pentru orice $1\le i\le n$, adică $S_i\in S(A[X_1, ..., X_n])$ pentru orice $1\le i\le n$. ■

Definiția 3.6. Polinoamele $S_1, S_2, ..., S_n$ poartă numele de *polinoamele simetrice fundamentale* din $A[X_1, ..., X_n]$.

Reamintim că în paragraful precedent pentru $f\in A[X_1, ..., X_n]$ prin $t_p(f)$ am notat termenul principal al lui f (adică acel monom nenul care în ordonarea lexicografică este cel mai mare termen al lui f).

Propoziția 3.7. Fie $f\in S(A[X_1, ... ,X_n])$ şi să presupunem că $t_p(f)=aX_1^{i_1}X_2^{i_2}...X_n^{i_n}$ cu $a\in A^*$. Atunci cu necesitate $i_1\ge i_2\ge ...\ge i_n$.

Demonstrație. Să presupunem prin absurd că pentru un $1\le k\le n$ avem $i_k<i_{k+1}$ şi să considerăm monomul $M=aX_1^{i_1}...X_{k-1}^{i_{k-1}}X_k^{i_{k+1}}X_{k+1}^{i_k}...X_n^{i_n}$. Cum f este simetric cu necesitate M face parte dintre termenii lui f. Contradicția provine din aceea că, relativ la ordonarea lexicografică, $t_p(f) < M$ - absurd. ■

Observația 3.8. Dacă $X_1^{i_1}...X_n^{i_n}$ este un monom din $A[X_1, ..., X_n]$ pentru care $i_1\ge i_2\ge ...\ge i_n$, atunci există doar un număr finit de monoame $X_1^{j_1}X_2^{j_2}...X_n^{j_n}$ a.î. $j_1\ge j_2\ge ...\ge j_n$ şi $X_1^{j_1}X_2^{j_2}...X_n^{j_n} < X_1^{i_1}X_2^{i_2}...X_n^{i_n}$ (deoarece din $j_1\le i_1$ deducem că avem un număr finit de moduri de alegere a lui j_1 iar pentru fiecare j_1 ales există cel mult j_1^{n-1} posibilități de alegere a lui $(j_2,...,j_n)$ a.î. $j_1\ge j_2\ge ...\ge j_n$).

Suntem acum în măsură să prezentăm un rezultat important legat de polinoamele simetrice cunoscut sub numele de *Teorema fundamentală a polinoamelor simetrice:*

Teorema 3.9. Pentru orice $f\in S(A[X_1,...,X_n])$ există un unic $g\in A[X_1,...,X_n]$ a.î. $f=g(S_1, ..., S_n)$, unde $S_1, ..., S_n$ sunt polinoamele simetrice fundamentale.

Demonstrație. Ținând cont de Observația 3.4. putem presupune că f este şi omogen; fie grad(f)=m. Dacă $t_p(f)=aX_1^{i_1}...X_n^{i_n}$, atunci conform Propoziției 3.7. avem că $i_1 \geq i_2 \geq ... \geq i_n$. Ținând cont de faptul că pentru orice $1 \leq i \leq n$, $t_p(\mathbf{S_i})=X_1X_2...X_i$ şi de Observația 3.4. de la paragraful precedent deducem că :

$t_p(\mathbf{S_1}^{i_1-i_2}\mathbf{S_2}^{i_2-i_3}...\mathbf{S_{n-1}}^{i_{n-1}-i_n}\mathbf{S_n}^{i_n})=$

$=X_1^{i_1-i_2}(X_1X_2)^{i_2-i_3}...(X_1X_2...X_{n-1})^{i_{n-1}-i_n}(X_1X_2...X_n)^{i_n}$

$=X_1^{(i_1-i_2)+(i_2-i_3)+...+(i_{n-1}-i_n)+i_n}X_2^{(i_2-i_3)+...+(i_{n-1}-i_n)+i_n}...X_n^{i_n}=$

$=X_1^{i_1}X_2^{i_2}...X_n^{i_n}=t_p(f).$

Astfel, dacă vom considera $f_1=f-a\mathbf{S_1}^{i_1-i_2}\mathbf{S_2}^{i_2-i_3}...\mathbf{S_{n-1}}^{i_{n-1}-i_n}\mathbf{S_n}^{i_n}$, $t_p(f_1)<t_p(f)$ (în ordonarea lexicografică).

Continuăm acum procedeul pentru f_1. Dacă $bX_1^{j_1}...X_n^{j_n}=t_p(f_1)$ atunci $j_1 \geq j_2 \geq ... \geq j_n$ şi dacă vom considera

$f_2=f_1-b\mathbf{S_1}^{j_1-j_2}\mathbf{S_2}^{j_2-j_3}...\mathbf{S_{n-1}}^{j_{n-1}-j_n}\mathbf{S_n}^{j_n}$, atunci $t_p(f_2) < t_p(f_1) < t_p(f)$ şi astfel procedeul va continua. Ținând cont de Observația 3.8., acest procedeu se va sfârşi după un număr finit de paşi.

Astfel, $f=a\mathbf{S_1}^{i_1-i_2}\mathbf{S_2}^{i_2-i_3}...\mathbf{S_{n-1}}^{i_{n-1}-i_n}\mathbf{S_n}^{i_n}+f_1=$

$=a\mathbf{S_1}^{i_1-i_2}\mathbf{S_2}^{i_2-i_3}...\mathbf{S_{n-1}}^{i_{n-1}-i_n}\mathbf{S_n}^{i_n}+b\mathbf{S_1}^{j_1-j_2}\mathbf{S_2}^{j_2-j_3}...\mathbf{S_{n-1}}^{j_{n-1}-j_n}\mathbf{S_n}^{j_n}+f_2=$

$=...$ şi deci alegând

$g=aX_1^{i_1-i_2}X_2^{i_2-i_3}...X_{n-1}^{i_{n-1}-i_n}X_n^{i_n}+bX_1^{j_1-j_2}X_2^{j_2-j_3}...$

$....X_{n-1}^{j_{n-1}-j_n}X_n^{j_n}+... \in A[X_1,...,X_n]$ avem că $f=g(\mathbf{S_1}, \mathbf{S_2}, ..., \mathbf{S_n})$.

Să demonstrăm acum unicitatea lui g. Acest lucru revine la a demonstra că dacă $g \in A[X_1, ..., X_n]$, $g=\sum a_{i_1i_2...i_n}X_1^{i_1}...X_n^{i_n}$ şi $g(\mathbf{S_1}, ..., \mathbf{S_n})=0$, atunci toți coeficienții $a_{i_1i_2...i_n}=0$.

Să presupunem prin absurd că există un coeficient $a_{i_1i_2...i_n} \neq 0$. Atunci polinomul $\mathbf{S_1}^{i_1}\mathbf{S_2}^{i_2}...\mathbf{S_n}^{i_n}$ are ca termen principal $t_p(\mathbf{S_1}^{i_1}\mathbf{S_2}^{i_2}...\mathbf{S_n}^{i_n})=X_1^{j_1}X_2^{j_2}...X_n^{j_n}$ cu $j_1=i_1+...+i_n$, $j_2=i_2+...+i_n,...$, $j_n=i_n$ iar $\text{grad}(t_p)=\sum_{k=1}^{n} j_k=\sum_{k=1}^{n} ki_k$.

Deducem de aici că dacă

$\mathbf{S_1}^{i_1}\mathbf{S_2}^{i_2}...\mathbf{S_n}^{i_n} \neq \mathbf{S_1}^{j_1}\mathbf{S_2}^{j_2}...\mathbf{S_n}^{j_n}$ atunci $t_p(\mathbf{S_1}^{i_1}\mathbf{S_2}^{i_2}...\mathbf{S_n}^{i_n}) \neq t_p(\mathbf{S_1}^{j_1}\mathbf{S_2}^{j_2}...\mathbf{S_n}^{j_n})$. Deci termenii principali în $X_1, X_2, ..., X_n$ ai diferitelor monoame distincte în $\mathbf{S_1}, \mathbf{S_2}, ..., \mathbf{S_n}$ care apar în expresia lui g, nu se reduc.

Dacă $X_1^{t_1}...X_n^{t_n}$ este cel mai mare termen principal, atunci înlocuind $\mathbf{S_1}, ..., \mathbf{S_n}$ prin expresiile lor în $X_1, ..., X_n$ apare un polinom în $X_1, ..., X_n$ egal cu zero dar care are un termen $a_{t_1...t_n}X_1^{t_1}...X_n^{t_n}$ nenul - absurd!

Cu aceasta teorema este complet demonstrată. ■

Aplicații: 1. Să exprimăm pe $f=(-X_1+X_2+X_3)(X_1-X_2+X_3)(X_1+X_2-X_3)$ (care în mod evident aparține lui $\mathbf{S}(\mathbb{Z}[X_1, X_2, X_3])$ ca polinom din $\mathbb{Z}[X_1, X_2, X_3]$ de polinoamele simetrice fundamentale $\mathbf{S_1}, \mathbf{S_2}, \mathbf{S_3}$. Avem că $t_p(f)=-X_1^3$ astfel că exponenții termenilor principali ai polinoamelor $f_1, f_2, ...$ care vor rămâne după eliminarea succesivă a termenilor principali (ca în procedeul descris în Teorema 3.9.) vor fi (3, 0, 0), (2, 1, 0) şi (1, 1, 1).

Deci $f= -\mathbf{S_1}^3+a\mathbf{S_1}^{2-1}\mathbf{S_2}^{1-0}\mathbf{S_3}^0+b\mathbf{S_1}^{1-1}\mathbf{S_2}^{1-1}\mathbf{S_3}^1= -\mathbf{S_1}^3+a\mathbf{S_1}\mathbf{S_2}+b\mathbf{S_3}$ unde $a, b \in \mathbb{Z}$.

Alegând de exemplu $X_1=X_2=1$ şi $X_3=0$ obținem că $f(1, 1, 0)=0$, $S_1=2, S_2=1, S_3=0$ deci $0= -8+2a$, adică $a = 4$.

Alegând $X_1=X_2=X_3=1$, atunci $f(1, 1, 1)=1$, $S_1=3, S_2=3, S_3=1$ şi astfel obținem $1= -27+36+b$, de unde $b = -8$.

Deci $f = -\mathbf{S_1}^3+4\mathbf{S_1}\mathbf{S_2}-8\mathbf{S_3}$, astfel că alegând $g = -X_1^3+4X_1X_2-8X_3$ avem $f=g(\mathbf{S_1}, \mathbf{S_2}, \mathbf{S_3})$.

2. Tot ca aplicație la Teorema fundamentală a polinoamelor simetrice (Teorema 3.9.) vom arăta cum se exprimă în funcție de polinoamele simetrice fundamentale $S_1, ..., S_n$, polinoamele $P_k= X_1^k+...+X_n^k$ $(k\in\mathbb{N})$.

Vom proba la început aşa-zisele *formule ale lui Newton.*

Teorema 3.10. (*Newton*) Dacă A este un domeniu de integritate, atunci pentru orice n, k $\in\mathbb{N}^*$ au loc formulele:

$$(-1)^{k-1}P_k + (-1)^{k-2}P_{k-1}S_1 + \ldots + P_1S_{k-1} = kS_k$$

(convenim ca pentru k >n să alegem $S_k=0$).

Demonstrație. Vom demonstra la început că formulele din enunț sunt adevărate pentru $k\geq n$, adică pentru orice $k\geq n$ avem :

(1) $P_k - P_{k-1}S_1 + P_{k-2}S_2 + \ldots + (-1)^{n-1}P_{k-n+1}S_{n-1} + (-1)^n P_{k-n}S_n = 0$

Pentru aceasta vom considera polinomul

$$f = f(X) = \prod_{i=1}^{n}(X - X_i) = X^n - S_1X^{n-1} + S_2X^{n-2} + \ldots + (-1)^n S_n$$

Înlocuind pe X cu X_i, $1\leq i\leq n$ se obțin relațiile:

$$X_i^n - S_1X_i^{n-1} + S_2X_i^{n-2} + \ldots + (-1)^n S_n = 0$$

pentru $1\leq i\leq n$, de unde prin înmulțire cu X_i^{k-n} se obțin relațiile:

$$X_i^k - S_1X_i^{k-1} + S_2X_i^{k-2} + \ldots + (-1)^n S_nX_i^{k-n} = 0$$

(pentru $1\leq i\leq n$).

Sumând după i=1, 2, ..., n obținem relațiile (1).

Să demonstrăm acum relațiile (1) pentru k<n iar pentru aceasta vom proba prin inducție matematică după m=n-k că polinomul

$$f_k = f_k(X_1,\ldots,X_n) = (-1)^{k-1}P_k + (-1)^{k-2}P_{k-1}S_1 + \ldots + P_1S_{k-1} + kS_k$$

este nul.

În cazul m=0 (adică n=k) acest lucru rezultă din (1) (deoarece $P_0=n$).

Să observăm acum că polinomul f_k fiind simetric în X_1, ..., X_n atunci şi polinomul $f_k(X_1, \ldots, X_{n-1}, 0)$ va fi simetric în X_1, ..., ,X_{n-1}. Dacă notăm polinoamele simetrice fundamentale în nedeterminatele X_1, ..., X_{n-1} cu S_1', ..., S_{n-1}' avem:

$$S_k(X_1, \ldots, X_{n-1}, 0) = S_k'(X_1, \ldots, X_{n-1}).$$

Cum şi $f_k(X_1, \ldots, X_{n-1}, 0) = f_k'(X_1, \ldots, X_{n-1})$ atunci

$$f_k(X_1,\ldots,X_{n-1},0) = (-1)^{k-1}P_k' + (-1)^{k-2}P_{k-1}'S_1' + \ldots + P_1'S_{k-1}' + kS_k' =$$

$= f_k X_1, ..., X_{n-1}$. Conform ipotezei de inducție $f_k(X_1, ..., X_n)=0$, deci $f_k(X_1, ..., X_n)$ este divizibil prin X_n. Cum este polinom simetric deducem imediat că f_k este divizibil prin $X_1, ..., X_{n-1}$, deci şi prin produsul $X_1 ... X_{n-1}X_n$, adică putem scrie

(2) $f_k(X_1, ..., X_n)= S_n(X_1, ..., X_n) f'_k(X_1, ..., X_n)$.

Deoarece $f_k(X_1, ..., X_n)$ este un polinom omogen de grad k, k<n şi $S_n(X_1, ..., X_n)$, este omogen de grad n, egalitatea (2) nu este posibilă decît dacă $f'_k(X_1, ..., X_n)=0$ şi atunci va rezulta că $f_k(X_1, ..., X_n)=0$.

Conform principiului inducției matematice avem că pentru orice k<n $f_k(X_1, ..., X_n)=0$ şi astfel relațiile lui Newton sunt probate şi pentru k<n ■.

Observația 3.11. Scriind formula lui Newton sub formă explicită:

$$P_1 = S_1$$
$$P_1S_2 - P_2 = 2S_3$$
$$P_1S_2 - P_2S_1 + P_3 = 3S_3$$
$$.....$$
$$P_1S_{k-1} - P_2S_{k-2} + ... + (-1)^{k-1}P_k = kS_k$$

şi interpretând aceste relații ca un sistem liniar în necunoscutele $P_1, ..., P_k$ obținem în final expresia lui P_k în funcție de $S_1, .., S_k$:

$$P_k = \begin{vmatrix} S_1 & 1 & 0 & ..... & 0 \\ 2S_2 & S_1 & 1 & ..... & 0 \\ 3S_3 & S_2 & S_1 & ..... & 0 \\ ..... & ..... & ..... & ..... & ..... \\ kS_k & S_{k-1} & S_{k-2} & ..... & S_1 \end{vmatrix}.$$

§4. Rădăcini ale polinoamelor cu coeficienți într-un corp. Teorema fundamentală a algebrei. Polinoame ireductibile. Rezolvarea ecuațiilor algebrice de grad 3 şi 4

În cadrul acestui paragraf toate corpurile considerate vor fi comutative. Dacă k, K sunt două corpuri a.î. k este subcorp al lui K vom spune că K este o *extindere* a lui k.

Definiția 4.1. Fie k un corp, K o extindere a sa şi $M \subseteq K$ o submulțime oarecare. Intersecția tuturor subcorpurilor lui K ce conțin $k \cup M$ se notează prin k(M) şi se spune că este corpul obținut prin *adjuncționarea* la k a elementelor lui M. Dacă $M=\{ \alpha_1, ..., \alpha_n \}$ vom scrie $k(M)=k(\alpha_1, ..., \alpha_n)$.

O extindere K a lui k se zice de *tip finit* dacă există o submulțime finită $M \subseteq K$ a.î. k(M)=K ; dacă există un element $x \in K$ a.î. K=k(x) atunci K se zice *extindere simplă* a lui k.

Dacă $k \subseteq K$ este o extindere de corpuri, vom spune despre un element $\alpha \in K$ că este *algebric* peste k dacă există un polinom nenul $f \in k[x]$ a.î. $\widetilde{f}(\alpha)=0$ (reamintim că $\widetilde{f}: k \to k$ este funcția polinomială ataşată lui f). În caz contrar, spunem că α este *transcendent* peste k.

O extindere K a unui corp k se zice *algebrică* dacă orice element al lui K este algebric peste k. Dacă orice element dintr-o extindere a lui k, care este algebric peste k, aparține lui k, vom spune despre k că este *algebric închis*.

Teorema 4.2. (*Teorema împărțirii cu rest*) Fie K un corp comutativ, f, $g \in K[X]$ cu $g \neq 0$. Atunci există şi sunt unice două polinoame q, $r \in K[X]$ a.î. f=gq+r şi grad(r)<grad(g).

Demonstrație. Fie $f=a_0+a_1X+...+a_nX^n$ şi $g=b_0+b_1X+...+b_mX^m$ cu $b_m \neq 0$ şi $m \geq 0$. Vom demonstra existența polinoamelor q şi r prin inducție matematică după gradul lui f (adică după n).

Dacă grad(g) > n, putem alege q=0 şi r=f.

Dacă grad(g) ≤ n, considerăm polinomul $f_1=f-b_m^{-1}a_nX^{n-m}g$. Cum grad($f_1$)<n, conform ipotezei de inducție există q_1, $r_1 \in K[X]$ a.î. $f_1=gq_1+r_1$ cu grad(r_1)<grad(g). Obținem $f-b_m^{-1} a_n X^{n-m} g = gq_1+r_1$, de unde $f=g(q_1+b_m^{-1}a_nX^{n-m})+r_1$, de unde se observă că alegând $q=q_1+b_m^{-1} a_n X^{n-m}$ şi $r=r_1$ avem f=gq+r şi grad(r)<grad(g). Conform principiului inducției matematice partea de existență din teoremă este demonstrată.

Pentru a proba unicitatea lui q şi r, să presupunem că mai există $q', r' \in K[X]$ a.î. $f=gq'+r'$ şi grad(r')<grad(g). Cum f=gq+r deducem că $gq'+r'=gq+r \Leftrightarrow g(q'-q)=r-r'$. Dacă $q'=q$, atunci în mod evident şi $r'=r$. Dacă $q' \neq q$, atunci cum $b_m \neq 0$ din egalitatea $g(q'-q)=r-r'$ deducem că gradul polinomului $g(q'-q)$ este mai mare sau egal cu n pe când gradul lui $r-r'$ este strict mai mic decât n - absurd! . În concluzie, $r = r'$ şi $q = q'$. ■

Definiția 4.3. Polinoamele q şi r din enunțul Teoremei 4.2. poartă numele de *câtul* **şi respectiv** *restul* **împărțirii lui f la g.**

Dacă r=0 spunem că g *divide* f şi scriem $\mathbf{g \mid f}$.

Observația 4.4. În cazul în care corpul K din enunțul Teoremei 4.2. se înlocuieşte cu un inel oarecare A, atunci teorema împărțirii cu rest în A[X] capătă forma :

Fie A un inel comutativ f, $g \in A[X]$, $f=a_0+a_1X+...+a_nX^n$, $g=b_0+b_1X+...+b_mX^m$ de grade n, respectiv m≥0 (deci $b_m \neq 0$) şi k = max(n-m+1, 0). Atunci există polinoamele q şi r din A[X] a.î. $b_m^k f=gq+r$ cu grad(r)<m. În plus, dacă b_m nu este divizor al lui zero, atunci q şi r sunt unic determinate.

Demonstrația este asemănătoare cu cea a Teoremei 4.2..

Conform Definiției 11.12. de la Capitolul 3, un polinom $f \in A[X]$ se zice *ireductibil* în A[X] dacă $f \in A[X] \setminus \mathbf{U}(A[X])$ şi f nu are divizori proprii.

Dacă presupunem că A este domeniu de integritate, atunci conform Corolarului 1.12, (ii), A[X] va fi de asemenea domeniu de integritate iar $\mathbf{U}(A[X])=\mathbf{U}(A)$. Astfel, dacă $f \in A[X] \setminus \mathbf{U}(A[X])$ (adică f este un polinom diferit de polinomele constante a cu $a \notin \mathbf{U}(A)$), atunci f

este ireductibil în A[X] dacă şi numai dacă f nu are divizori proprii (adică din f=gh cu g, h∈A[X] deducem că unul dintre polinoamele g sau h este polinom constant cu constanta respectivă din U(A) iar celălalt este asociat în divizibilitate cu f).

În particular, dacă k este un corp comutativ, atunci f∈(k[X])* este ireductibil în k[X] dacă şi numai dacă din f=gh, cu g, h∈(k[X])* deducem că g sau h face parte din k*.

Un polinom f∈A[X] care nu este ireductibil în A[X] se va zice *reductibil* în A[X].

Propoziția 4.5. (*Bézout*) Fie A un inel comutativ unitar, f∈A[X] şi a∈A. Atunci următoarele afirmații sunt echivalente:

(i) a este rădăcină a lui f (adică $\widetilde{f}$ (a)=0)

(ii) X-a | f.

Demonstrație. (i)⇒(ii). Fie f=$a_0+a_1X+...+a_nX^n$ ∈A[X] şi să presupunem că $\widetilde{f}$(a)=0 ⇔ $a_0+a_1a+...+a_na^n$=0. Putem deci scrie f=$(a_0+a_1X+...+a_nX^n)-(a_0+a_1a+...+a_na^n)=a_1(X-a)+a_2(X^2-a^2)+...+a_n(X^n-a^n)$ şi cum pentru orice k∈ℕ, $X^k-a^k=(X-a)(X^{k-1}+aX^{k-2}+...+a^{k-2}X+a^{k-1})$ (adică X-a | X^k-a^k) deducem imediat că X-a | f.

(ii)⇒(i). Dacă X-a | f atunci putem scrie f=(X-a)g cu g∈A[X] şi cum $\widetilde{f}=\widetilde{(x-a)}\,\widetilde{g}$ (vezi Observația 1.15) deducem că $\widetilde{f}$(a)=(a-a)$\widetilde{g}$(a)= =0·$\widetilde{g}$(a)=0. ■

Observația 4.6. Din propoziția de mai înainte deducem că dacă A este un inel integru, atunci un polinom de grad ≥2 din A[X] care are o rădăcină în A este reductibil. Reciproca acestei afirmații (în sensul că orice polinom reductibil are cel puțin o rădăcină în A) nu este adevărată după cum ne putem convinge considerând polinomul f=$(1+X^2)(1+X^4)$∈ℤ[X] care deşi este reductibil în ℤ[X] nu are nici o rădăcină în ℤ. Afirmația rămâne totuşi adevărată pentru polinoamele de grad 2 şi 3 cu coeficienți într-un corp (căci în acest caz cel puțin un

factor al său este de gradul 1 şi orice polinom de gradul 1 are o rădăcină în corpul coeficienților).

Definiția 4.7. Fie $f \in A[X]$, $f \neq 0$ şi $a \in A$. Vom spune despre a că este *rădăcină multiplă de ordin i* pentru f dacă $(X-a)^i \mid f$ şi $(X-a)^{i+1} \nmid f$. Numărul i poartă numele de *ordinul de multiplicitate* **al lui a (a spune că i=0 revine de fapt la a spune că a nu este rădăcină pentru f).**

Atunci când numărăm rădăcinile unui polinom şi nu facem specificarea expresă că sunt sau nu distincte, vom număra fiecare rădăcină, de atâtea ori cât este ordinul său de multiplicitate.

Propoziția 4.8. Fie A un domeniu de integritate.

(i) Dacă $a \in A$ este rădăcină multiplă pentru polinoamele nenule $f, g \in A[X]$ cu ordine de multiplicitate i respectiv j, atunci a este rădăcină multiplă de ordin i+j pentru fg

(ii) Dacă $a_1, ..., a_k$ sunt rădăcini distincte din A ale polinomului nenul $f \in A[X]$ cu ordinele de multiplicitate $i_1, ..., i_k$ atunci f se scrie sub forma $f=(X-a_1)^{i_1}...(X-a_k)^{i_k} g$ cu $g \in A[X]$.

Demonstrație. (i). Putem scrie $f=(X-a)^i f_1$ şi $g=(X-a)^j g_1$ cu $f_1, g_1 \in A[X]$ iar $\widetilde{f_1}(a) \neq 0$, $\widetilde{g_1}(a) \neq 0$. Atunci $fg=(X-a)^i f_1 (X-a)^j g_1 = (X-a)^{i+j} f_1 g_1$

şi $\widetilde{f_1 g_1}(a)=\widetilde{f_1}(a)\ \widetilde{g_1}(a) \neq 0$ (căci A este domeniu de integritate), de unde concluzia că a este rădăcină multiplă de ordin i+j pentru fg.

(ii). Facem inducție matematică după k (pentru k=1 afirmația fiind evidentă dacă ținem cont de Propoziția 4.5.). Să presupunem afirmația adevărată pentru k-1 şi s-o probăm pentru k. Există deci $f_1 \in A[X]$ a.î. $f=(X-a_1)^{i_1}...(X-a_{k-1})^{i_{k-1}} f_1$.

Cum $\widetilde{f}(a_k)=0$ iar A este domeniu de integritate deducem că $\widetilde{f_1}(a_k)=0$ şi ordinul de multiplicitate al lui a_k în cadrul lui f_1 este acelaşi ca în cadrul lui f, adică $f_1=(X-a_k)^{i_k} g$ şi astfel $f=(X-a_1)^{i_1}...(X-a_k)^{i_k} g$. ■

Corolar 4.9. (i) Dacă A este un domeniu de integritate şi f∈A[X] cu grad(f)=n≥1, atunci f are în A cel mult n rădăcini

(ii) Dacă K este un corp comutativ, atunci orice subgrup finit al grupului (K*, ·) este ciclic.

Demonstraţie. (i). Rezultă imediat din Propoziţia 4.8. (ii).

(ii). Fie G≤K* a.î. |G|=n. Pentru a proba că G este ciclic este suficient să arătăm că în G găsim un element de ordin n.

Fie $n = p_1^{r_1} \ldots p_t^{r_t}$ descompunerea lui n în factori primi distincţi. Pentru orice 1≤i≤t există un element $x_i \in G$ a.î. $x_i^{n/p_i} \neq 1$ căci în caz contrar polinomul $X_i^{n/p_i} - 1 \in K[X]$ ar avea mai multe rădăcini decât gradul său (absurd conform cu)i)).

Să arătăm că dacă notăm $y_i = x_i^{n/p_i^{r_i}}$, atunci $o(y_i) = p_i^{r_i}$ pentru orice 1≤i≤t. Într-adevăr, $y_i^{p_i^{r_i}} = x_i^n = 1$ (conform Corolarului 3.11. de la Capitolul 2). Conform Observaţiei 2.10. de la Capitolul 2 deducem că $o(y_i)$ divide $p_i^{r_i}$ adică $o(y_i) = p_i^s$ cu $1 \leq s \leq r_i$. Dacă $s < r_i$, ar rezulta că $y_i^{p_i^{r_i-1}} = x_i^{n/p_i} = 1$ în contradicţie cu alegerea elementului x_i. Atunci $s = r_i$ şi astfel $o(y_i) = p_i^{r_i}$ pentru orice 1≤i≤t. Ţinând cont din nou de Observaţia 2.10. de la Capitolul 2 deducem că dacă notăm $y = y_1 \cdot \ldots \cdot y_t$, atunci $o(y) = p_1^{r_1} \cdot \ldots \cdot p_t^{r_t} = n$. ■

Propoziţia 4.10. (*Relaţiile lui Viète*) Fie A un domeniu de integritate şi f∈A[X] un polinom de grad n, $f = a_0 + a_1X + \ldots + a_nX^n$ (deci $a_n \neq 0$). Dacă $x_1, \ldots, x_n$ sunt rădăcinile lui f în A, atunci

$$a_n(x_1 + \ldots + x_n) = -a_{n-1}$$

$$a_n(x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n) = a_{n-2}$$

.....

$$a_n(x_1x_2\ldots x_k + x_1x_2\ldots x_{k-1}x_{k+1} + \ldots + x_{n-k+1}x_{n-k+2}\ldots x_n) = (-1)^k a_{n-k}$$

.....

$$a_n(x_1\ldots x_n) = (-1)^n a_0.$$

Demonstrație. Conform Propoziției 4.8., (ii), putem scrie $f=(X-x_1)...(X-x_n)g$; identificând coeficientul lui X^n în ambii membrii deducem că $g=a_n$, astfel că $f=a_n(X-x_1)...(X-x_n)=$
$=a_nX^n-a_n(x_1+...+x_n)X^{n-1}+a_n(x_1x_2+x_1x_3+...+x_{n-1}x_n)X^{n-2}+...+(-1)^k a_n(x_1...x_k+$
$+x_1...x_{k-1}x_{k+1}+...+x_{n-k+1}x_{n-k+2}...x_n)X^{n-k}+...+(-1)^n a_nx_1...x_n.$
Identificând coeficienții lui X^k $(0\le k\le n)$ din cele două scrieri ale lui f obținem relațiile din enunț dintre rădăcinile şi coeficienții lui f. ■

Corolar 4.11. Dacă A este corp comutativ, atunci relațiile dintre rădăcinile şi coeficienții lui f devin:

$$\begin{cases} x_1+...+x_n=-a_{n-1}a_n^{-1} \\ x_1x_2+x_1x_3+...+x_{n-1}x_n=a_{n-2}a_n^{-1} \\ ..... \\ x_1x_2...x_k+x_1x_2...x_{k-1}x_{k+1}+...+x_{n-k+1}x_{n-k+2}...x_n=(-1)^k a_{n-k}a_n^{-1} \\ ..... \\ x_1x_2...x_n=(-1)^n a_0a_n^{-1} \end{cases}$$

Corolar 4.12. (*Wilson*). Dacă $p\ge 2$ este un număr prim, atunci $(p-1)!+1\equiv 0 \pmod p$.

Demonstrație. În $\mathbb{Z}_p[X]$ considerăm polinomul $f=X^{p-1}-1$. Ținând cont de faptul că $(\mathbb{Z}_p^*, \cdot)$ este un grup (comutativ) cu p-1 elemente, conform Corolarului 3.11. de la Capitolul 2 avem că pentru orice $\hat{x}\in\mathbb{Z}_p^*$, $\hat{x}^{p-1}=\hat{1}$ şi astfel, ținând cont de Corolarul 4.9. rădăcinile lui f sunt $\hat{1}, \hat{2}, ..., \overset{\wedge}{p-1}$.

Conform ultimei relații a lui Viète avem $\hat{1}\,\hat{2}.....\overset{\wedge}{p-1}=(-1)^{p-1}(-\hat{1}) \Leftrightarrow$

$\overset{\wedge}{(p-1)}!+1=\hat{0} \Leftrightarrow (p-1)!+1\equiv 0\ (p)$. ■

Propoziția 4.13. Fie k un corp comutativ iar f∈k[X] cu grad(f)≥ 1. Atunci există o extindere $\bar{k}$ a lui k a.î. f să aibă cel puțin o rădăcină în $\bar{k}$.

Demonstrație. Cum grad(f) ≥1 deducem că f∉**U**(k[X]) (vezi Propoziția 1.11.).
Atunci idealul < f > este diferit de k[X] şi conform Teoremei 10.9. de la Capitolul 3, există un ideal maximal m al lui k[X] a.î. < f > $\subseteq m$. Considerând

$$k \xrightarrow{i_k} k[X] \xrightarrow{p} k[X]/m \overset{def}{=} \bar{k}$$

(unde i_k este morfismul canonic de scufundare a lui k în k[X] iar p este morfismul surjectiv canonic de inele). Cum m este ideal maximal în inelul k[X], $\bar{k}$ este corp (vezi Propoziția 10.5. de la Capitolul 3). Notând $\bar{p} = p \circ i_k$ obținem un morfism de corpuri $\bar{p} : k \to \bar{k}$. Dacă alegem f=a_0+a_1X+...+$a_n$$X^n$ şi notăm $\bar{p}$ (f)= $\bar{p}$ (a_0)+ $\bar{p}$ (a_1)X+...+ $\bar{p}$ (a_n)X^n ∈ $\bar{k}$ [X], atunci pentru

a=p(X)= $\hat{X} \in \bar{k}$ avem $\widetilde{\bar{p}(f)}$ (a)=0 adică a∈ $\bar{k}$ este o rădăcină a lui $\bar{p}$ (f). Cum $\bar{p}$ este în particular o funcție injectivă, k poate fi privit ca subcorp al lui $\bar{k}$ (k fiind de fapt izomorf cu $\bar{p}$ (k)), deci în mod canonic şi f poate fi privit ca făcând parte din $\bar{k}$ [X]. ■

Corolar 4.14. Dacă k este un corp comutativ iar f∈k[X] este un polinom de grad ≥1, atunci există o extindere K a lui k în care f are toate rădăcinile.

Demonstrație. Se face inducție matematică după n=grad(f) ținând cont la pasul de inducție de Propoziția 4.13. şi Propoziția 4.5. ■

Observația 4.15. 1. Dacă k este un corp, f∈k[X] este de grad ≥1 iar K este o extindere a lui k în care f are toate rădăcinile α_1, ..., α_n , atunci k(α_1, ..., α_n) este numit *corpul de descompunere* **al lui f.**

2. Fie $f \in k[X]$ de grad ≥ 1 şi K o extindere a lui k în care f are rădăcinile $x_1, ..., x_n$. Atunci pentru orice polinom simetric $g \in k[x_1, ..., x_n]$, $\widetilde{g}(x_1, ..., x_n) \in k$.

Într-adevăr, deoarece $g \in \mathbf{S}(k[X_1,...,X_n])$, conform teoremei fundamentale a polinoamelor simetrice (Teorema 3.9.) există $h \in k[X_1,...,X_n]$ a.î. $g=h(S_1, ..., S_n)$. Conform relațiilor lui Viète, $\widetilde{S}_i(x_1,...,x_n) \in k$ pentru $1 \leq i \leq n$ şi astfel

$$\widetilde{g}(x_1,...,x_n)=\widetilde{h}(\widetilde{S}_1(x_1,...,x_n), ..., \widetilde{S}_n(x_1,...,x_n)) \in k.$$

Suntem acum în măsură să prezentăm un rezultat deosebit de important în algebră cunoscut sub numele de *teorema fundamentală a algebrei* :

Teorema 4.16. (*D'Alembert - Gauss*). Orice polinom de grad ≥ 1 din $\mathbb{C}[X]$ are cel puțin o rădăcină în $\mathbb{C}$ (adică corpul numerelor complexe $\mathbb{C}$ este algebric închis).

Demonstrație. Fie $f=a_0+a_1X+...+a_nX^n \in \mathbb{C}[X]$ cu $n \geq 1$ şi $a_n \neq 0$. Considerând $\bar{f}=\bar{a}_0+\bar{a}_1X+...+\bar{a}_nX^n$ (unde pentru $z \in \mathbb{C}$ prin $\bar{z}$ desemnăm conjugatul său) atunci $f\,\bar{f}=b_0+b_1X+...+b_{2n}X^{2n}$ unde $b_j=\sum_{k=0}^{j} a_k\bar{a}_{j-k}$, $0 \leq j \leq 2n$.

Deoarece $\bar{b}_j=\sum_{k=0}^{j}\bar{a}_k a_{j-k}=b_j$, deducem că $b_j \in \mathbb{R}$ $(0 \leq j \leq 2n)$ astfel că $f\,\bar{f} \in \mathbb{R}[X]$. Dacă admitem teorema adevărată pentru polinoamele din

$\mathbb{R}[X]$, atunci există $\alpha \in \mathbb{C}$ a.î. $\widetilde{(f\,\bar{f})}(\alpha)=0 \Leftrightarrow \widetilde{f}(\alpha)\,\widetilde{\bar{f}}(\alpha)=0 \Leftrightarrow \widetilde{f}(\alpha)\,\widetilde{f}(\bar{\alpha})=0$ (căci $\widetilde{\bar{f}}(\alpha)=\widetilde{f}(\bar{\alpha})$) de unde concluzia că α sau $\bar{\alpha}$ sunt rădăcini ale lui f.

În concluzie, putem presupune $f \in \mathbb{R}[X]$.

Dacă grad(f) este impar, cum $\widetilde{f}:\mathbb{R}\to\mathbb{R}$ este funcție continuă iar la $\pm\infty$ ia valori de semne contrarii deducem că există $\alpha\in\mathbb{R}$ a.î. $\widetilde{f}(\alpha)=0$.

Să presupunem acum că grad(f)=2^n r cu $n\in\mathbb{N}$ şi $r\in\mathbb{N}^*$, r impar. Prin inducție matematică după n vom arăta că există $\alpha\in\mathbb{C}$ a.î. $\widetilde{f}(\alpha)=0$.

Dacă n=0, atunci grad(f) este impar şi după cum am văzut mai înainte există $\alpha\in\mathbb{R}$ a.î. $\widetilde{f}(\alpha)=0$.

Să presupunem afirmația adevărată pentru toate polinoamele $g\in\mathbb{R}[X]$ cu proprietatea că n-1 este exponentul maxim al lui 2 în descompunerea în factori primi a gradului lui g şi fie $f\in\mathbb{R}[X]$ cu grad(f)=2^n r cu n, $r\in\mathbb{N}$, r impar.

Conform Corolarului 4.14., există o extindere K a lui $\mathbb{C}$ în care f are toate rădăcinile $x_1, ..., x_m$ (unde m=grad(f)).

Pentru $a\in\mathbb{R}$ arbitrar considerăm $z_{ij}^a=x_ix_j+a(x_i+x_j)$, $1\le i<j\le m$.

Dacă vom considera polinomul

$g_a=\prod_{1\le i<j\le m}(X-z_{ij}^a)$, atunci grad(g_a)=$C_m^2=\frac{m(m-1)}{2}$ şi cum m=grad(f)=2^kr (cu k, $r\in\mathbb{N}$, r impar) avem că grad (g_a)=$\frac{2^k r(2^k r-1)}{2}$ = =2^{k-1}r (2^kr-1)=2^{k-1} r′ unde r′=r (2^kr-1) este număr natural impar.

Să observăm că coeficienții lui g_a sunt polinoame simetrice fundamentale de z_{ij}^a. Mai mult, având în vedere expresiile lui z_{ij}^a, $1\le i<j\le m$ rezultă că aceşti coeficienți, ca polinoame de $x_1, ..., x_m$ sunt simetrice deoarece orice permutare a acestora are ca efect schimbarea elementelor z_{ij}^a între ele ($1\le i<j\le m$). Ținând cont de Observația 4.15. deducem că $g_a\in\mathbb{R}[X]$. Aplicând ipoteza de inducție lui g_a deducem că există o pereche (i, j) cu $1\le i<j\le m$ a.î. $z_{ij}^a\in\mathbb{C}$.

Făcând pe a să parcurgă mulțimea infinită $\mathbb{R}$ a numerelor reale, cum mulțimea perechilor (i, j) cu $1\le i<j\le m$ este finită, deducem că există a, $b\in\mathbb{R}$, $a\neq b$ a.î. $z_{ij}^a, z_{ij}^b\in\mathbb{C}$.

Din $z_{ij}^{a}=x_ix_j+a(x_i+x_j)$ şi $z_{ij}^{b}=x_ix_j+b(x_i+x_j)$ deducem că $z_{ij}^{a}-z_{ij}^{b}=(a-b)(x_i+x_j)\in\mathbb{C}$, adică $x_i+x_j\in\mathbb{C}$.

Atunci şi $x_ix_j\in\mathbb{C}$, adică $x_i,\ x_j\in\mathbb{C}$ şi cu aceasta teorema este demonstrată. ■

Observaţia 4.17. 1. Din Teorema 4.16. şi Propoziţia 4.5. deducem imediat că în $\mathbb{C}[X]$ polinoamele ireductibile sunt cele de gradul 1.

2. Dacă $f=a_0+a_1X+...+a_nX^n\in\mathbb{R}[X]$ $(n\geq 1)$ şi $\alpha\in\mathbb{C}$ este o rădăcină a lui f, atunci $\widetilde{f}(\alpha)=0$ şi se verifică imediat că şi $\widetilde{f}(\overline{\alpha})=0$, adică rădăcinile lui f care sunt din $\mathbb{C}\setminus\mathbb{R}$ sunt conjugate două câte două (mai mult, ele au acelaşi ordin de multiplicitate).

3. Dacă $z=a+bi\in\mathbb{C}$, $b\neq 0$ şi $\bar{z}=a-bi$ atunci $(X-z)(X-\bar{z})=$ $=X^2-2aX+(a^2+b^2)\in\mathbb{R}[X]$. De aici deducem imediat că un polinom $f\in\mathbb{R}[X]$ este ireductibil în $\mathbb{R}[X]$ dacă şi numai dacă f este de gradul 1 sau este de forma aX^2+bX+c cu $a, b, c\in\mathbb{R}$ şi $b^2-4ac<0$.

Din observaţia de mai înainte deducem că problema ireductibilităţii este interesantă doar în $\mathbb{Z}[X]$ (pentru $\mathbb{Q}[X]$ această problemă se reduce imediat la $\mathbb{Z}[X]$).

În continuare vom prezenta un criteriu suficient de ireductibilitate pentru polinoamele din $\mathbb{Z}[X]$, cunoscut sub numele de c*riteriul de ireductibilitate al lui Eisenstein:*

Propoziţia 4.18. (*Eisenstein***) Fie $f=a_0+a_1X+...+a_nX^n\in\mathbb{Z}[X]$ de grad ≥ 1 şi să presupunem că există $p\in\mathbb{N}$ un număr prim a.î. $p\mid a_0$, $a_1, ..., a_{n-1}$, $p\nmid a_n$ şi $p^2\nmid a_0$.**

Atunci f este ireductibil în $\mathbb{Z}[X]$.

Demonstraţie. Să presupunem prin absurd că f este reductibil în $\mathbb{Z}[X]$, adică putem scrie $f=(b_0+b_1X+...+b_mX^m)(c_0+c_1X+...+c_kX^k)$ cu $m, k\geq 1$ şi $m+k=n$. Identificând coeficienţii lui f deducem că

$$(*)\ \begin{cases} a_0 = b_0c_0 \\ a_1 = b_0c_1 + b_1c_0 \\ a_2 = b_0c_2 + b_1c_1 + b_2c_0 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n-1} = b_{m-1}c_k + b_mc_{k-1} \\ a_n = b_mc_k \end{cases}$$

Cum $p \mid a_0$ iar $p^2 \nmid a_0$ deducem că $p \mid b_0$ şi $p \nmid c_0$ sau $p \mid c_0$ şi $p \nmid b_0$. Să presupunem de exemplu că $p \mid b_0$ şi $p \nmid c_0$.

Dacă ţinem cont de relaţiile (*) deducem din aproape în aproape că $p \mid b_1$, $p \mid b_2$, ..., $p \mid b_{m-1}$ şi din ultima relaţie din (*) am deduce că $p \mid a_n$ -absurd!. Analog, dacă $p \nmid b_0$ şi $p \mid c_0$ am deduce că $p \mid c_1$, $p \mid c_2$, ..., $p \mid c_{k-1}$ şi din ultima relaţie din (*) am deduce că $p \mid a_n$ -absurd. ■

Observaţia 4.19. Alegând un număr prim $p \geq 2$ şi $n \in \mathbb{N}^*$ atunci conform criteriului de ireductibilitate al lui Eisenstein polinomul $X^n - pX + p \in \mathbb{Z}[X]$ este un polinom ireductibil din $\mathbb{Z}[X]$.

Deci pentru orice $n \geq 1$ în $\mathbb{Z}[X]$ găsim o infinitate de polinoame ireductibile de grad n.

În continuare vom prezenta metode de rezolvare a ecuaţiilor algebrice de grade 3 şi 4 cu coeficienţi din $\mathbb{C}$ (adică a ecuaţiilor de forma $\widetilde{f}(x)=0$ cu $f \in \mathbb{C}[X]$ iar grad(f)=3 sau 4).

1. Să considerăm la început ecuaţia algebrică de grad 3 cu coeficienţi din $\mathbb{C}$ scrisă sub forma

$$(1)\quad x^3+ax^2+bx+c=0 \quad \text{cu} \quad a \in \mathbb{C}.$$

Dacă în (1) înlocuim $y=x+\frac{a}{3}$ obţinem o ecuaţie algebrică în y de forma:

$$(2)\quad y^3+py+q=0 \text{ cu } p, q \in \mathbb{C}.$$

Fie acum θ o rădăcină a lui (2) (eventual într-o extindere K a lui $\mathbb{C}$, conform Corolarului 4.14.) iar x_1, x_2 rădăcinile ecuaţiei

(3) $x^2 - \theta x - \frac{p}{3} = 0.$

Conform relațiilor lui Viète avem

(4) $x_1+x_2=\theta$ şi $x_1x_2=\frac{-p}{3}$.

Înlocuind pe θ în (2) avem că $\theta^3+p\theta+q=0$ astfel că dacă ținem cont de (4) obținem $x_1^3+x_2^3=(x_1+x_2)^3-3x_1x_2(x_1+x_2)=\theta^3+p\theta=-q$ şi cum $x_1^3x_2^3=\frac{-p^3}{27}$ obținem că x_1^3 şi x_2^3 sunt rădăcinile ecuației $x^2+qx-\frac{p^3}{27}=0$, adică $x_1^3=-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$ şi $x_2^3=-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$ de unde deducem :

$x_1^{(j)}=\varepsilon_j\sqrt[3]{\frac{-q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$ şi $x_2^{(t)}=\varepsilon_t\sqrt[3]{\frac{-q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$, $0\le j, t\le 2$, în care $\varepsilon_0, \varepsilon_1, \varepsilon_2$ sunt rădăcinile ecuației $x^3-1=0$.

Cum rădăcinile ecuației $x^3-1=0$ sunt 1 şi $\varepsilon, \varepsilon^2$ (cu $\varepsilon=\frac{-1+i\sqrt{3}}{2}$) deducem că rădăcinile ecuației (2) sunt

$$\begin{cases} \theta_1=\sqrt[3]{\frac{-q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{\frac{-q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}} \\ \theta_2=\varepsilon\sqrt[3]{\frac{-q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\varepsilon^2\sqrt[3]{\frac{-q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}} \\ \theta_3=\varepsilon^2\sqrt[3]{\frac{-q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\varepsilon\sqrt[3]{\frac{-q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}} \end{cases}$$

Astfel, rădăcinile lui (1) vor fi $x_i=\theta_i-\frac{a}{3}$, $1\le i\le 3$.

2. Să considerăm acum ecuația algebrică de grad 4 cu coeficienți din $\mathbb{C}$:

(5) $x^4+ax^3+bx^2+cx+d=0$ $(a, b, c, d \in \mathbb{C})$.

Notând $y=x+\frac{a}{4}$ obținem că y verifică o ecuație de forma

(6) $y^4+py^2+qy+r=0$ cu p, q, $r\in\mathbb{C}$.

Fie α un element dintr-o extindere K a lui $\mathbb{C}$ a.î. scriind pe (6) sub forma (7) $(y^2+\frac{p}{2}+\alpha)^2-[2\alpha y^2-qy+(\alpha^2+p\alpha-r+\frac{p^2}{4})]=0$ şi cel de al doilea termen să fie pătrat perfect, adică α să verifice ecuația de gradul 3:

$$q^2-8\alpha(\alpha^2+p\alpha-r+\frac{p^2}{4})=0 \Leftrightarrow$$

(8) $8\alpha^3+8p\alpha^2+(2p^2-8r)\alpha-q^2=0.$

Pentru α ce verifică ecuația (8), ecuația (7) devine:

(9) $(y^2+\frac{p}{2}+\alpha)^2-2\alpha(y-\frac{q}{4\alpha})^2=0$

iar rădăcinile lui (9) sunt rădăcinile ecuațiilor $y^2-\theta y+(\frac{p}{2}+\alpha+\frac{q}{2})=0$

$$y^2+\theta y+(\frac{p}{2}+\alpha-\frac{q}{2})=0$$

cu θ rădăcină a ecuației $x^2-2\alpha=0$.

Astfel, rezolvarea unei ecuații algebrice de grad 4 se reduce la rezolvarea unei ecuații de gradul 3 şi a două ecuații algebrice de grad 2.