Fundamentele algebrice ale informaticii

pentru anul I Informatică (zi + ID) începînd cu anul universitar 2005/2006

CURSUL nr. 1

§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)*.

Definiția1.1.. 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 $A, B, C\in\mathbf{P}(T)$, atunci :

(i) $A\subseteq A$

(ii) Dacă $A\subseteq B$ şi $B\subseteq A$, atunci $A=B$

(iii) Dacă $A\subseteq B$ şi $B\subseteq C$, atunci $A\subseteq C$.

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, $B\in\mathbf{P}(T)$ 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:

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

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

$\complement_T(\varnothing)=T,\ \complement_T(T)=\varnothing$

$A\cup\complement_T(A)=T,\ A\cap\complement_T(A)=\varnothing$ iar $\complement_T(\complement_T(A))=A$.

De asemenea, pentru x∈T avem:

$x\notin A\cap B \Leftrightarrow x\notin A$ sau $x\notin B$

$x\notin A\cup B \Leftrightarrow x\notin A$ şi $x\notin B$

$x\notin A\setminus B \Leftrightarrow x\notin A$ 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∈**P**(T), atunci:

$\complement_T(A\cap B)=\complement_T(A)\cup\complement_T(B)$ 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:

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

$\bigcup_{i\in I} A_i = \{x\in T \mid$ există $i\in I$ 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 ∪ şi ∩ sunt *asociative*, din (ii) deducem că ambele sunt *comutative*, din (iii) deducem că T şi ∅ sunt elementele neutre pentru ∩ şi respectiv pentru ∪**,** iar din (iv) deducem că ∩ şi ∪ sunt operaţii *idempotente* pe **P**(T).

2. Prin dublă incluziune se probează imdiat că pentru oricare A, B, C∈**P**(T) avem:

$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$ şi

$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$,

adică operaţiile de intersecţie şi reuniune sunt *distributive* una faţă de cealaltă.

Propoziţia1.4. Dacă A, B, C∈P(T), atunci:

(i) A△(B△C)=(A△B)△C

(ii) A△B=B△A

(iii) A△∅=A iar A △A=∅

(iv) A∩(B△C)=(A∩B)△(A∩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. ■

Din cele de mai inainte deducem ca dacă T este o mulțime oarecare , atunci $(P(T), \triangle, \cap)$ este inel Boolean .

Definiția1.5. 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, $(x, y)=(y, x) \Rightarrow x=y$.

Definiția1.6. 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*:

Propoziția1.7. Fie M o mulțime finită iar $M_1, M_2, ..., M_n$ submulțimi ale lui M. Atunci :

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

$$-....+(-1)^{n-1}|M_1\cap ...\cap M_n|$$

§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 $\Delta_A=\{(a, a) \mid a\in A\}$ poartă numele de *diagonala* produsului cartezian A×A.

Pentru ρ∈**Rel** (A) definim $\rho^{-1}=\{(a, b)\in A\times A \mid (b, a)\in\rho\}$.

În mod evident, $(\rho^{-1})^{-1}=\rho$ iar dacă mai avem ρ′∈**Rel** (A) a.î. ρ⊆ρ′⇒ $\rho^{-1}\subseteq\rho'^{-1}$.

Definiția2.2. Pentru ρ, ρ′∈Rel (A) definim *compunerea* lor ρ∘ρ′ prin ρ∘ρ′={(a, b)∈A×A | există c∈A a.î. (a, c)∈ρ′ şi (c, b)∈ρ}.

Rezultatul următor este imediat:

Propoziția 2.3. Fie ρ, ρ′, ρ′′∈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∈ℕ şi ρ∈**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 ∈ℕ atunci $\rho^m\circ\rho^n=\rho^{m+n}$.

Definiți 2.3. Vom spune despre o relație ρ∈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:

Propoziția2.4. O relație ρ∈Rel(A) este reflexivă (simetrică, antisimetrică, tranzitivă) dacă şi numai dacă ρ^{-1} este reflexivă (simetrică, antisimetrică, tranzitivă) .

Definiția 2.5. Vom spune despre o relație ρ∈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 2.6. 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 $\rho^2=\rho$. ■

Lema 2.7. Fie $\rho\in$Rel(A) şi $\overline{\rho}=\Delta_A\cup\rho\cup\rho^{-1}$. Atunci relația $\overline{\rho}$ are următoarele proprietăți:

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

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

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

Demonstrație. (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 2.8. Fie $\rho\in$Rel(A) reflexivă şi simetrică iar $\overline{\rho}=\bigcup_{n\geq 1}\rho^n$. Atunci $\overline{\rho}$ are următoarele proprietăți :

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

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

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

Demonstrație. (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 de mai sus deducem imediat:

Teorema 2.9. Dacă $\rho\in$Rel(A), atunci

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

Definiția 2.10. Dacă ρ∈Echiv (A) şi a∈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∈A).

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

Propoziția 2.11. Dacă ρ∈Echiv (A), atunci:

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

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

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

Demonstrație.

(i). Deoarece pentru orice a∈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)∈ρ.

Fie acum (a, b)∈ρ şi $x\in[a]_\rho$, adică (x, a)∈ρ. Datorită tranzitivității lui ρ deducem că (x, b)∈ρ, 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∈A a.î. (x, a), (x, b)∈ρ şi astfel (a, b)∈ρ, deci $[a]_\rho=[b]_\rho$ (conform cu (ii)). ■

Definiția 2.12. 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∈I, $i\neq j\Rightarrow M_i\cap M_j=\emptyset$;

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

Observația 2.13. Din cele de mai înainte deducem că dacă ρ este o relație de echivalență pe mulțimea A, atunci mulțimea claselor de echivalență ale lui ρ pe A determină o partiție a lui A.

Definiția 2.13. 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 scrie$A\nsim B$).

Propoziția 2.14. 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. ■

Definiția 2.15. Dacă A este o mulțime, prin *numărul cardinal* al lui A înțelegem clasa de echivalență a lui A (notată |A|) relativă la relația de echivalență ∼.

Deci $B\in|A|\Leftrightarrow A\sim B$.

Vom numi *secțiuni* ale lui ℕ mulțimile de forma $S_n=\{0, 1, ..., n-1\}$ formate din n elemente ($n\in\mathbb{N}^*$); convenim să notăm pentru $n\in\mathbb{N}^*$, $n=|S_n|$. Convenim de asemenea să notăm 0=cardinalul mulțimii vide şi prin χ_0 (alef zero) cardinalul mulțimii numerelor naturale ℕ.

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 $n|x-y$, $y-z$ şi atunci $n|(x-y)+(y-z)=x-z$, 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 $\hat{k}=\{k+cn|c\in\mathbb{Z}\}$ pentru orice $k\in\{0,1,\ldots,n-1\}$.

Elementele lui $\mathbb{Z}_n$ se numesc *clasele de resturi modulo n.*

CURSUL nr. 2 :

§1.Mulţimi ordonate.Lema Zorn

Definiţia 1.1. Printr-o *mulţime ordonată* înţelegem un dublet $(A,\leq)$ format dintr-o mulţime nevidă A şi o relaţie binară pe A notată tradiţional prin "$\leq$" care este reflexivă, antisimetrică şi tranzitivă. Vom spune că "$\leq$" este o *ordine* pe A.

Pentru $x, y\in A$ vom scrie $x<y$ dacă $x\leq y$, $x\neq y$. Dacă relaţia "$\leq$" este doar reflexivă şi tranzitivă, vom spune despre ea că este o *ordine parţială* sau că $(A,\leq)$ este o mulţime *parţial ordonată*.

Dacă pentru $x, y\in A$ definim $x\geq y$ dacă şi numai dacă $y\leq x$ obţinem o nouă relaţie de ordine pe A. Dubletul $(A,\geq)$ 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 1.2. Fie $m, M\in A$ şi $S\subseteq A$, $S\neq\emptyset$.

Vom spune că:

i) m este *minorant* pentru S dacă pentru orice $s\in S$, $m\leq s$ (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 $s\in S$, $s\leq M$ (în caz că există, prin sup (S) vom desemna cel mai mic majorant al lui S).

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

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

Pentru $a, b\in A$ vom spune că b *urmează* pe a (sau că a este *urmat* de b) dacă $a<b$ iar pentru $a\leq c\leq b$ avem $a=c$ sau $c=b$; vom utiliza în acest caz notaţia $a\angle b$.

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).

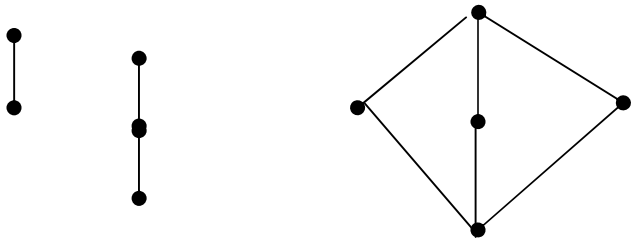
Mulţimile ordonate finite A pot fi reprezentate prin aşa zisele *diagrame Hasse*.

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).

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

Definiţi1.3. Un element $m\in A$ se zice:

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

ii) ***maximal*** **dacă având $a\in A$ a.î. $m \leq a$ 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. $x \leq a$, atunci $x = 0$ sau $x = a$ (deci $0 \angle a$).

Definiţie.

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.

$(\mathbb{N}, \leq)$ 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 .

Lema 1.4.(*Bourbaki*). Dacă $(A, \leq)$ este o mulţime nevidă, inductiv ordonată şi $f : A \to A$ este o aplicaţie 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.

CURSUL nr. 3

§1.Semilatici. Latici.Filtre.Ideale.Morfisme de latici.Latici distributive.Latici modulare

Definiția 1.1. 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 submulțime $S \subseteq A$ există inf (S)

v) *sup – completă,* dacă pentru orice submulțime $S \subseteq A$ 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 tradițional prin $0 \in A$ a.î. pentru orice $a \in A$, $0 \leq a$

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

ix) *mărginită* dacă este simultan inf şi sup - mărginită (adică $0 \leq a \leq 1$ 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).

Observația1.2.

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 $x \leq y$ deducem că $x \leq m$, 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 condiţional completă, este suficient ca pentru orice submulţime nevidă şi mărginită S a sa, să existe doar $\inf(S)$ (sau $\sup(S)$).

Definiţia 1.3. Dacă A este inf-semilatice (respectiv sup-semilatice) vom spune despre o submulţime $A' \subseteq A$ 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 $\mathbb{N}$ mulţimea numerelor naturale iar "$|$" relaţia de divizibilitate pe $\mathbb{N}$. Atunci "$|$" este o relaţie de ordine pe $\mathbb{N}$. Faţă 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 $\emptyset$ 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 $f: A \to A'$ o funcţie.

Definiţia1.4. Vom spune despre f că este *morfism de mulţimi ordonate* (sau aplicaţie *izotonă*) dacă pentru orice a, $b \in A$ 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, $b \in A$, $f(a \wedge b) = f(a) \wedge f(b)$ (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, $b \in A$ 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 $f: A \to A'$ este *morfism de mulţimi ordonate*, atunci f se zice *izomorfism de mulţimi ordonate* dacă există $g: A' \to A$ morfism de mulţimi 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 bijecţie. În acest caz vom scrie $A \approx A'$.

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

Definiţia 1.5. Fie A o inf-semilatice şi $F \subseteq A$ o submulţime 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) mulţimea filtrelor lui A.

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

Definiţia1.6. Fie A o sup-semilatice iar $I \subseteq A$ o submulţime 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) mulţimea idealelor lui A.

Observaţia1.7. Dacă A este latice, atunci noţiunile de filtru şi ideal au definiţii precise în A (ţinând cont de definiţiile 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 intersecţia oricărei familii de filtre (ideale) este de asemenea filtru (ideal), putem vorbi de *filtrul (idealul) generat de o mulţime 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 intersecţia tuturor filtrelor (idealelor) lui A ce conţin pe S).

Propoziţia1.8. Dacă A este o inf-semilatice şi $S \subseteq A$ o submulţime nevidă a sa, atunci:

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

*Demonstraţie.*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:

Propoziţia1.9. Dacă A este o sup-semilatice şi $S \subseteq A$ este o submulţime 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: $[a)=\{x \in A \mid a \leq x\}$ şi $(a]=\{x \in A \mid x \leq a\}$ ([a), (a] poartă numele de *filtrul* (*idealul*) *principal* generat de a).

Definiţia1.10. Vom spune despre o latice $(L, \leq)$ că este:

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

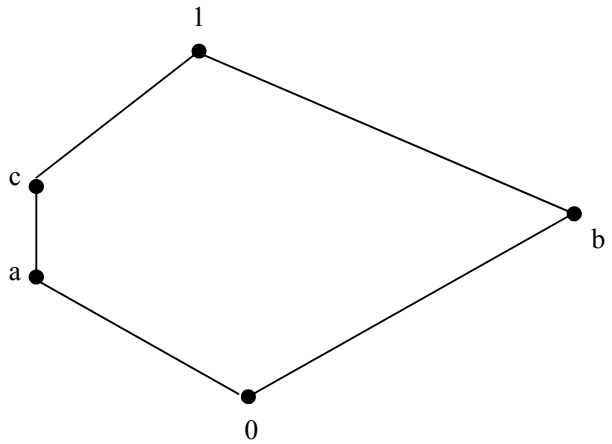
ii) *distributivă* dacă verifică una din următoarele două condiţii echivalente:

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 tradiţional prin $\mathbf{N_5}$:



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

Teorema 1.11. (*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 $a \wedge c \le c$.

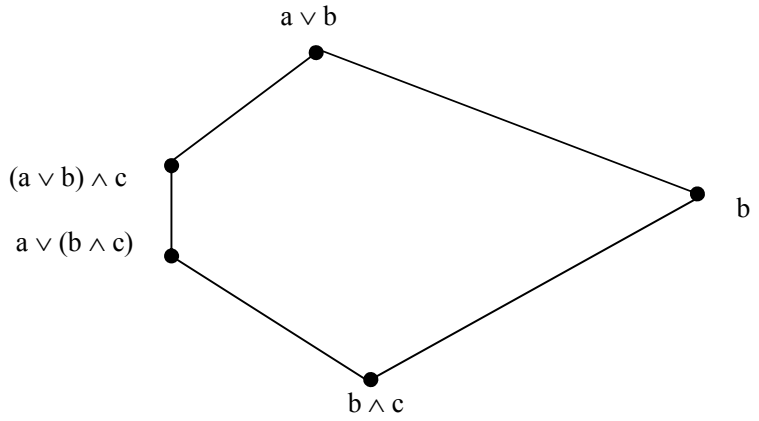
(iii) $\Rightarrow$ (i). Fie $a, b, c \in L$ a.î. $a \le c$. Atunci $a = a \wedge c$, deci $(a \vee b) \wedge c = ((a \wedge c) \vee b) \wedge c = (a \wedge c) \vee (b \wedge c) = a \vee (b \wedge c)$.

(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 observația de mai înainte).

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

Obținem 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.

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 lanț, atunci $L \in$ **Ld** (**0**, **1**).

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

Teorema 1.12. Pentru $L \in L$ următoarele afirmații sunt echivalente:

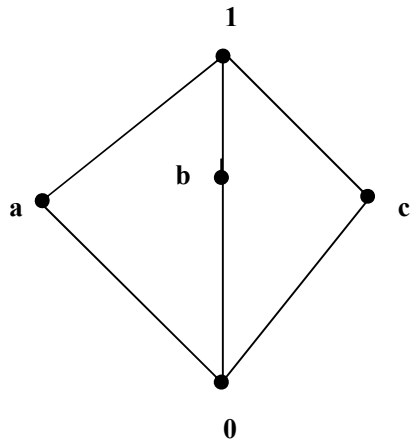
(i) $L \in$ **Ld**

(ii) $a \wedge (b \vee c) \le (a \wedge b) \vee (a \wedge c)$ **pentru orice** $a, b, c \in L$

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

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

(v) L **nu are sublatici izomorfe cu N_5 sau M_3, unde 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:

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

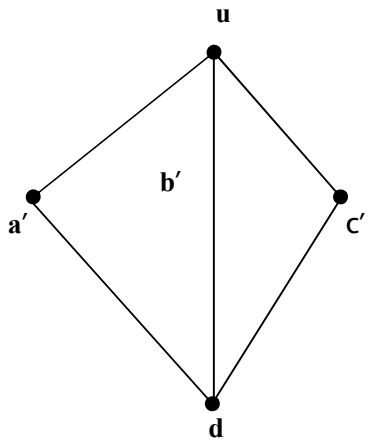
$=(a \wedge ((a \wedge b) \vee (b \wedge c))) \vee (c \wedge a) =$ (datorită modularității) $= a \wedge (b \wedge c)) \vee (a \wedge b) \vee (c \wedge a) =$ (datorită modularității) $= (a \wedge b) \vee (a \wedge c)$.

(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, $a' \wedge c' = ((d \vee a) \wedge u) \wedge ((d \vee c) \wedge u) = (d \vee a) \wedge (d \vee c) \wedge u = ((a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \vee a) \wedge (d \vee c) \wedge u = =((b \wedge c) \vee a) \wedge (d \vee c) \wedge u = ((b \wedge c) \vee a) \wedge ((a \wedge b) \vee c) \wedge \wedge (a \vee b) \wedge (b \vee c) \wedge (c \vee a) = ((b \wedge c) \vee a) \wedge ((a \wedge b) \vee c) = (b \wedge c) \vee (a \wedge ((a \wedge b) \vee c)) =$ (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 1.13. Fie L o latice oarecare şi $x, y \in L$. Atunci
$(x] \wedge (y] = (x \wedge y]$ iar $(x \vee y] \subseteq (x] \vee (y]$; dacă $L \in \mathbf{Ld}$, atunci $(x] \vee (y] = (x \vee y]$.

Demonstrație. Egalitatea $(x] \wedge (y] = (x \wedge y]$ se probează imediat prin dublă incluziune iar incluziunea $(x \vee y] \subseteq (x] \vee (y]$ este imediata. Dacă $L \in \mathbf{Ld}$, atunci $(x] \vee (y] = \{i \vee j \mid i \in (x] \text{ şi } j \in (y]\} = \{i \vee j \mid i \leq x \text{ şi } j \leq y\}$, de unde rezultă imediat că $(x] \vee (y] \subseteq (x \vee y]$, deci $(x \vee y] = (x] \vee (y]$. ■

CURSUL nr. 4

§1.Algebre Boole.

Definiția1. 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 1.2. 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 $a' = a''$ ■

Lema 1.3. 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 $[b, c]$. ■

Lema1.4. (*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. 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 1.5. 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:

Definiția1.6. 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 1.7.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. $a' \leq b$ 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 1.8. 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 $a \wedge b = 0 \Leftrightarrow a \leq b^*$
2) $a \leq b \Rightarrow a^* \geq b^*$
3) $a \leq a^{**}$
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) $0^* = 1$, $1^* = 0$

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 $a \leq b \Rightarrow b \in D(L)$

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

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

2) Deoarece $b \wedge b^* = 0$, atunci pentru $a \leq b$, deducem că $a \wedge b^* = 0$, adică $b^* \leq a^*$.

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

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

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

Observație 1.9.

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 $D(L) \in \mathbf{F}(L)$.

Teorema1.10. 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 $x = y$, 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 $\mathbf{Ld}(\mathbf{0}, \mathbf{1})$, 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 $\mathbf{Ld}(\mathbf{0}, \mathbf{1})$. ■

Definiția1.11. 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 $f \le g \Leftrightarrow f(x) \le g(x)$ pentru orice $x \in M$. Astfel $(\mathbf{2}^M, \le)$ devine latice Boole (în care caz pentru $f \in \mathbf{2}^M$, $f' = \mathbf{1} - f$).

Definiția1.12. 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***.**

Propoziția1.13. (*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. Deducem imediat 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 $x, y, z \in R(L)$, $x \wedge z \le x \vee (y \wedge z)$ şi $y \wedge z \le x \vee (y \wedge z)$, 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 $z \wedge [x \vee (y \wedge z)]^* \le x^*, y^*$, adică $z \wedge [x \vee (y \wedge z)]^* \le x^* \wedge y^*$ şi $z \wedge [x \vee (y \wedge z)]^* \wedge (x^* \wedge y^*)^* = \mathbf{0}$ ceea ce implică $z \wedge (x^* \wedge y^*) \le [x \vee (y \wedge z)]^{**}$. Cum partea stângă a acestei ultime inegalități este $z \wedge (x \vee y)$ iar partea dreaptă este $x \vee (y \wedge z)$ (în $R(L)$), deducem că $z \wedge (x \vee y) \le x \vee (y \wedge z)$, adică $R(L)$ este şi distributivă. ■

Propoziția1.14. Fie $B \in \mathbf{B}$ şi $a, b \in B$ a.î. $a \wedge b = 0$ şi $a \vee b = 1$. Atunci $b = a'$
Dacă $B \in \mathbf{B}$ şi $a, b \in B$, atunci $(a')' = a$, $(a \wedge b)' = a' \vee b'$ iar $(a \vee b)' = a' \wedge b'$.

Demonstrație. Rezultă imediat din cele de mai inainte ■

Propoziția1.15. Dacă M este o mulțime oarecare, atunci algebrele Boole $\mathbf{2}^M$ şi $P(M)$ sunt izomorfe.

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

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

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

§2.Legătura dintre inelele Boole şi algebrele Boole.

Definiția 2.1. Un inel $(A, +, \cdot, -, 0, 1)$ se zice *Boolean* dacă $a^2 = a$ pentru orice $a \in A$.

Exemple 1. 2 este inel Boolean (în care $1 + 1 = 0$).

2. $(P(X), \Delta, \cap, ', \emptyset, X)$ cu X mulțime oarecare iar Δ diferența simetrică de mulțimi.

Lema 2.2. Dacă A este inel Boolean, atunci pentru orice $a \in A$, $a + a = 0$ iar A este comutativ.

Demonstrație. Din $a + a = (a + a)^2$ deducem că $a + a = a + a + a + a$, adică $a + a = \mathbf{0}$, deci $-a = a$.

Pentru $a, b \in A$, din $a + b = (a + b)^2$ deducem că $a + b = a^2 + ab + ba + +b^2$ adică $ab + ba = \mathbf{0}$ de unde $ab = -(ba) = ba$. ■

Legătura dintre algebrele Boole şi inelele Boole ne este oferită de:

Propoziția 2.3. (i) Dacă $(A, +, \cdot, -, 0, 1)$ este un inel Boole, atunci relația "$\leq$" de pe A definită prin $a \leq b \Leftrightarrow ab = a$ conferă lui A structură de algebră Boole, unde pentru $a, b \in A$, $a \wedge b = ab$, $a \vee b = a + b + ab$ iar $a' = 1 + a$.

(ii) Reciproc, dacă $(A, \wedge, \vee, ', 0, 1)$ este o algebră Boole, atunci A devine inel Boole față de operațiile $+, \cdot$ definite pentru $a, b \in A$ prin $a + b = (a \wedge b') \vee (a' \wedge b)$ şi $a \cdot b = a \wedge b$ iar $-a = a$.

Demonstrație. (i) Faptul că $(A, \leq)$ este mulțime ordonată se probează imediat. Fie acum $a, b \in A$. Deoarece $a(ab) = a^2 b = ab$ şi $b(ab) = ab^2 = ab$ deducem că $ab \leq a$ şi $ab \leq b$. Fie acum $c \in A$ a.î. $c \leq a$ şi $c \leq b$, adică $ca = c$ şi $cb = c$. Atunci $c^2 ab = c^2 \Leftrightarrow cab = c \Leftrightarrow c \leq ab$, de unde concluzia că $ab = a \wedge b$.

Analog se probează că $a \vee b = a + b + ab$.

Deoarece $a \wedge (b \vee c) = a(b + c + bc) = ab + ac + abc$ iar $(a \wedge b) \vee (a \wedge c) = (ab) \vee (ac) = ab + ac + a^2 bc = ab + ac + abc$ deducem că $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, adică $A \in \mathbf{Ld}$. Deoarece pentru $a \in A$, $a \wedge a' = a \wedge (\mathbf{1} + a) = a(\mathbf{1} + a) = a + a^2 = a + a = \mathbf{0}$ şi $a \vee a' = a \vee (\mathbf{1} + a) = a + \mathbf{1} + a + a(\mathbf{1} + a) = a + \mathbf{1} + a + a + +a^2 = \mathbf{1} + a + a + a + a = \mathbf{1}$ deducem că $(A, \wedge, \vee, ', \mathbf{0}, \mathbf{1})$ este latice Boole.

(ii) Pentru $a, b, c \in A$ avem

1. $a + (b + c) = [a \wedge (b + c)'] \vee [a' \wedge (b + c)] =$
$= \{a \wedge [(b \wedge c') \vee (b' \wedge c)]'\} \vee \{a' \wedge [(b \wedge c') \vee (b' \wedge c)]\} =$
$= \{a \wedge [(b' \vee c) \wedge (b \vee c')]\} \vee \{(a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c)\} =$
$= \{a \wedge [(b' \wedge c') \vee (c \wedge b)]\} \vee \{(a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c)\} =$
$= (a \wedge b' \wedge c') \vee (a \wedge b \wedge c) \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c) =$
$= (a \wedge b \wedge c) \vee (a \wedge b' \wedge c') \vee (b \wedge c' \wedge a') \vee (c \wedge a' \wedge b')$

Cum forma finală este simetrică în a, b şi c deducem că $a + (b + c) = (a + b) + c$.

2. $a + b = (a \wedge b') \vee (a' \wedge b) = (b \wedge a') \vee (a \wedge b') = b + a$.
3. $a + \mathbf{0} = (a \wedge \mathbf{0}') \vee (a' \wedge \mathbf{0}) = (a \wedge \mathbf{1}) \vee \mathbf{0} = a$.
4. $a + a = (a' \wedge a) \vee (a \wedge a') = \mathbf{0} \vee \mathbf{0} = \mathbf{0}$, deci $-a = a$.
5. $a(bc) = a \wedge (b \wedge c) = (a \wedge b) \wedge c = (ab)c$
6. $a \cdot \mathbf{1} = a \wedge \mathbf{1} = a$.
7. $a(b + c) = a \wedge [(b \wedge c') \vee (b' \wedge c)] = (a \wedge b \wedge c') \vee (a \wedge b' \wedge c)$ iar $(ab) + (ac) = (a \wedge b) + (a \wedge c) = [(a \wedge b) \wedge (a \wedge c)'] \vee [(a \wedge b)' \wedge (a \wedge c)] = [a \wedge b \wedge (a' \vee c')] \vee [(a' \vee b') \wedge (a \wedge c)] = [(a \wedge b \wedge a') \vee (a \wedge b \wedge c')] \vee [(a \wedge c \wedge a') \vee (a \wedge c \wedge b')] = (a \wedge b \wedge c') \vee (a \wedge c \wedge b')$, de unde deducem că $a(b + c) = ab + ac$.

Din 1-7 deducem că $(A, +, \cdot, -, \mathbf{0}, \mathbf{1})$ este inel Boolean unitar. ■

Teorema 2.4. Fie $(B_1, +, \cdot)$, $(B_2, +, \cdot)$ două inele Boole iar $(B_1, \wedge, \vee, ', 0, 1)$, $(B_2, \wedge, \vee, ', 0, 1)$ algebrele Boole induse de aceste.

Atunci $f : B_1 \to B_2$ este morfism de inele (unitare) dacă şi numai dacă f este morfism de algebre Boole.

Demonstrație. Totul rezultă din definiția morfismelor de inele şi de latici Boole ■

Teorema 2.5. Fie B_1 şi B_2 două algebre Boole iar $f : B_1 \to B_2$ o funcție. Următoarele condiții sunt echivalente:

(i) f este morfism de algebre Boole;

(ii) f este morfism de latici mărginite;

(iii) f este morfism de inf-semilatici şi $f(x') = (f(x))'$ pentru orice $x \in B_1$;

(iv) f este morfism de sup-semilatici şi $f(x') = (f(x))'$ pentru orice $x \in B_1$.

Demonstrație. (i) $\Rightarrow$ (ii). Evident.

(ii) $\Rightarrow$ (i). $f(x) \wedge f(x') = f(x \wedge x') = f(\mathbf{0}) = \mathbf{0}$ şi analog $f(x) \vee f(x') = f(x \vee x') = f(\mathbf{1}) = \mathbf{1}$, deci $f(x') = (f(x))'$.

(iii) $\Rightarrow$ (i). f este morfism de sup – semilatici deoarece $f(x \vee y) = f(x'' \vee y'') = f((x' \wedge y')') = (f(x' \wedge y'))' = (f(x') \wedge f(y'))' = ((f(x))' \wedge (f(y))')' = f(x)'' \vee f(y)'' = f(x) \vee f(y)$.

Atunci $f(\mathbf{0}) = f(x \wedge x') = f(x) \wedge (f(x))' = \mathbf{0}$ şi analog $f(\mathbf{1}) = \mathbf{1}$, deci f este morfism de algebre Boole.

(i) $\Rightarrow$ (iii). Evident.

(iv). Este afirmația duală lui (iii) şi deci echivalența (iv) $\Leftrightarrow$ (i) se demonstrează analog ca şi echivalența (i) $\Leftrightarrow$ (iii). ■

Teorema 2.6. Fie $f : B_1 \to B_2$ un morfism de algebre Boole iar $Ker(f) = = f^{-1}\{0\} = \{x \in B_1 | f(x) = 0\}$. Atunci $Ker(f) \in I(B_1)$ iar f este ca funcție o injecție dacă şi numai dacă $Ker(f) = \{0\}$.

Demonstrație. Fie $x \in Ker(f)$ şi $y \in B_1$ a.î. $y \le x$. Atunci, f fiind izotonă $\Rightarrow f(y) \le f(x) = \mathbf{0} \Rightarrow f(y) = \mathbf{0} \Rightarrow y \in Ker(f)$. Dacă $x, y \in Ker(f)$ atunci în mod evident şi $x \vee y \in Ker(f)$, adică $Ker(f) \in I(B_1)$.

Să presupunem că $Ker(f) = \{\mathbf{0}\}$ şi fie $x, y \in Ker(f)$ a.î. $f(x) = f(y)$. Atunci $f(x \wedge y') = f(x) \wedge f(y') = f(x) \wedge f(y)' = f(x) \wedge f(x)' = \mathbf{0}$, deci $x \wedge y' \in Ker(f)$, adică $x \wedge y' = \mathbf{0}$, deci $x \le y$. Analog se arată că $y \le x$, de unde $x = y$.

Implicația reciprocă este evidentă (deoarece $f(\mathbf{0}) = \mathbf{0}$). ■

Teorema 2.7. Fie $f : B_1 \to B_2$ un morfism de algebre Boole. Următoarele afirmații sunt echivalente:

(i) f este izomorfism de algebre Boole;

(ii) f este surjectiv şi pentru orice $x, y \in B_1$ avem $x \le y \Leftrightarrow f(x) \le f(y)$;

(iii) f este inversabilă şi f^{-1} este un morfism de algebre Boole.

Demonstrație. (i) $\Rightarrow$ (ii). f izomorfism $\Rightarrow$ f surjecție.

Orice morfism de latici este o funcție izotonă, deci $x \le y \Rightarrow f(x) \le f(y)$.

Fie $f(x) \le f(y)$. Atunci $f(x) = f(x) \wedge f(y) = f(x \wedge y)$ şi cum f este injectivă $\Rightarrow x = x \wedge y$, de unde $x \le y$.

(ii) $\Rightarrow$ (iii). Arătăm că f este injectivă. Fie $f(x) = f(y) \Rightarrow f(x) \le f(y)$ şi $f(y) \le f(x) \Rightarrow x \le y$ şi $y \le x \Rightarrow x = y$. Cum f este şi surjecție, rezultă că f este bijecție, deci este inversabilă. Să demonstrăm de exemplu că $f^{-1}(x \wedge y) = f^{-1}(x) \wedge \wedge f^{-1}(y)$, oricare ar fi $x, y \in B_2$. Din $x, y \in B_2$ şi f surjecție rezultă că există x_1 şi $y_1 \in B_1$ a.î. $f(x_1) = x$ şi $f(y_1) = y$, deci $f^{-1}(x \wedge y) = f^{-1}(f(x_1) \wedge f(y_1)) = f^{-1}(f(x_1 \wedge y_1)) = x_1 \wedge y_1 = f^{-1}(f(x_1)) \wedge f^{-1}(f(y_1)) = f^{-1}(x) \wedge f^{-1}(y)$.

Analog $f^{-1}(x \vee y) = f^{-1}(x) \vee f^{-1}(y)$ şi $f^{-1}(x') = (f^{-1}(x))'$.

(iii) $\Rightarrow$ (i). Evident. ■

Teorema 2.8. Într-o algebră Boole $(B, \wedge, \vee, ', 0, 1)$, pentru $x, y \in B$ definim:

$x \to y = x' \vee y$ şi $x \leftrightarrow y = (x \to y) \wedge (y \to x) = (x' \vee y) \wedge (y' \vee x)$.

Atunci pentru orice $x, y, z \in B$ avem:

(i) $x \le y \Leftrightarrow x \to y = 1$;

(ii) $x \to 0 = x', 0 \to x = 1, x \to 1 = 1, 1 \to x = x, x \to x = 1, \quad x' \to x = x, x \to x' = x'$;

(iii) $x \to (y \to x) = 1$;

(iv) $x \to (y \to z) = (x \to y) \to (x \to z)$;
(v) $x \to (y \to z) = (x \wedge y) \to z$;
(vi) Dacă $x \le y$, atunci $z \to x \le z \to y$ şi $y \to z \le x \to z$;
(vii) $(x \to y) \wedge y = y$, $x \wedge (x \to y) = x \wedge y$;
(viii) $(x \to y) \wedge (y \to z) \le x \to z$;
(ix) $((x \to y) \to y) \to y = x \to y$;
(x) $(x \to y) \to y = (y \to x) \to x = x \vee y$;
(xi) $x \to y = \sup \{ z \in B : x \wedge z \le y \}$;
(xii) $x \to (y \wedge z) = (x \to y) \wedge (x \to z)$;
(xiii) $(x \vee y) \to z = (x \to z) \wedge (y \to z)$;
(xiv) $x \wedge (y \to z) = x \wedge [(x \wedge y) \to (x \wedge z)]$;
(xv) $x \leftrightarrow y = 1 \Leftrightarrow x = y$.

Demonstrație. (i). Dacă $x \to y = 1$ atunci $x' \vee y = 1 \Leftrightarrow x \le y$.
(iii). $x \to (y \to x) = x' \vee (y' \vee x) = 1 \vee y' = 1$
Analog celelalte relații . ■

CURSUL nr. 5

§1.Filtre într-o algebră Boole.

Aşa cum am menționat anterior, prin filtru într-o algebră Boole $(B, \wedge, \vee, ', 0, 1)$ înțelegem un filtru al laticei $(B, \wedge, \vee, 0, 1)$. Ca şi în cazul laticilor vom nota prin **F(B)** mulțimea filtrelor lui **B**. Un filtru maximal propriu al lui **B** se va numi (ca şi în cazul laticilor) *ultrafiltru*.

Ca şi în cazul laticilor deducem:

Teorema.1.1. (i) În orice algebră Boole B există ultrafiltre;

(ii) Orice element $x \neq 0$ este conținut într-un ultrafiltru.

Corolar 1.2. Fie B o algebră Boole şi $x, y \in B$, $x \neq y$. Atunci există un ultrafiltru U al lui B a.î. $x \in U$ şi $y \notin U$.

Demonstrație. Dacă $x \neq y$, atunci $x \not\le y$ şi $y \not\le x$.

Considerăm că $x \not\le y$. Atunci $x \wedge y' \neq 0$ (căci dacă $x \wedge y' = 0$, atunci $x \le y$). Conform Teoremei 1, (ii), cum $x \wedge y' \neq 0$ există un ultrafiltru U al lui B a.î. $x \wedge y' \in U$. Cum $x \wedge y' \le x$, y' şi U este în particular filtru deducem că $x, y' \in U$. Cum $U \neq B$ deducem că $y \notin U$. ■

Teorema 1.3. Fie $(B, \wedge, \vee, ', 0, 1)$ o algebră Boole iar $F \in F(B)$. Pe B definim următoarele relații binare:

$$x \sim_F y \Leftrightarrow \text{există } f \in F \text{ a.î. } x \wedge f = y \wedge f,$$
$$x \approx_F y \Leftrightarrow x \leftrightarrow y \in F.$$

Atunci:

(i) $\sim_F = \approx_F \overset{not}{=} \rho_F$;
(ii) ρ_F **este o congruență pe B;**
(iii) Dacă pentru $x \in B$ notăm prin x/F clasa de echivalență a lui x relativă la ρ_F, $B/F = \{x/F \mid x \in B\}$, atunci definind pentru $x, y \in B$, $x/F \wedge y/F =$ $= (x \wedge y)/F$, $x/F \vee y/F = (x \vee y)/F$ şi $(x/F)' = x'/F$, atunci $(B/F, \wedge, \vee, ', 0, 1)$ devine în mod canonic algebră Boole (unde $0 = \{0\}/F = \{ x \in B \mid x' \in F \}$ iar $1 = \{1\}/F = F$).

Demonstrație. (i). Fie $x \sim_F y \Leftrightarrow$ există $f \in F$ a.î. $x \wedge f = y \wedge f$.

Atunci $x' \vee (x \wedge f) = x' \vee (y \wedge f) \Rightarrow (x' \vee x) \wedge (x' \vee f) = (x' \vee y) \wedge (x' \vee f) \Rightarrow x' \vee f = (x' \vee y) \wedge (x' \vee f)$. Cum $f \in F$, F filtru şi $f \leq x' \vee f$ rezultă că $x' \vee f \in F \Rightarrow x' \vee y \in F$. Analog $x \vee y' \in F$, deci $x \leftrightarrow y \in F$, adică $x \approx_F y$.

Invers, dacă $x \approx_F y \Rightarrow x \leftrightarrow y \in F \Rightarrow (x' \vee y) \wedge (x \vee y') \in F \Rightarrow x' \vee y, x \vee y' \in F \Rightarrow$ există $f_1, f_2 \in F$ a .î. $x' \vee y = f_1$ şi $x \vee y' = f_2$. Atunci $x \wedge f_1 = x \wedge (x' \vee y) = (x \wedge x') \vee (x \wedge y) = x \wedge y$ şi analog $y \wedge f_2 = x \wedge y$, deci dacă $f = f_1 \wedge f_2 \in F$, atunci $x \wedge f = y \wedge f$.

(ii). Demonstrăm că ρ_F este o relaţie de congruenţă.

-*reflexivitatea*: $x \rho_F x$ deoarece $x' \vee x = \mathbf{1} \in F$.

- *simetria*: $x \rho_F y \Rightarrow (x' \vee y) \wedge (x \vee y') \in F \Rightarrow y \rho_F x$.

- *tranzitivitatea*: $x \rho_F y$ şi $y \rho_F z$ implică $x' \vee y, x \vee y', y' \vee z, y \vee z' \in F$. Atunci $x' \vee z = x' \vee z \vee (y \wedge y') = (x' \vee z \vee y) \wedge (x' \vee z \vee y') \geq (x' \vee y) \wedge (y' \vee z)$. Deoarece $x' \vee y, y' \vee z \in F$ atunci $x' \vee z \in F$. Analog $x \vee z' \in F$, deci $x \rho_F z$.

Astfel am demonstrat că ρ_F este o relaţie de echivalenţă.

Demonstrăm compatibilitatea lui ρ_F cu operaţiile $\wedge, \vee, '$.

Fie $x \rho_F y$ şi $z \rho_F t$. Atunci $x' \vee y, z' \vee t \in F \Rightarrow (x' \vee y) \wedge (z' \vee t) \in F$. Avem $(x' \vee y) \wedge (z' \vee t) \leq (x' \vee y \vee t) \wedge (z' \vee t \vee y) = (x' \wedge z') \vee (y \vee t) = (x \vee z)' \vee (y \vee t)$, deci $(x \vee z)' \vee (y \vee t) \in F$.

Analog $(y \vee t)' \vee (x \vee z)$, deci $(x \vee z) \rho_F (y \vee t)$.

Fie $x \rho_F y$. Atunci $x \leftrightarrow y \in F$ şi $x' \leftrightarrow y' = (x'' \vee y') \wedge (y'' \vee x') = (x \vee y') \wedge (x' \vee y) = x \leftrightarrow y$, deci $x' \rho_F y'$.

Fie $x \rho_F y$ şi $z \rho_F t$. Conform celor de mai sus $x' \rho_F y'$ şi $z' \rho_F t'$ şi cum ρ_F este compatibilă cu $\vee$, avem $(x' \vee z') \rho_F (y' \vee t') \Leftrightarrow (x \wedge z)' \rho_F (y \wedge t)' \Leftrightarrow (x \wedge z) \rho_F (y \wedge t)$.

Cu aceasta am stabilit că ρ_F este o congruenţă.

(iii). Totul rezultă din faptul că ρ_F este o congruenţă pe B . ■

Teorema 1.4. Fie B_1, B_2 două algebre Boole iar $f : B_1 \to B_2$ este un morfism de algebre Boole. Notăm prin $F_f = f^{-1}(\{1\}) = \{x \in B_1 : f(x) = 1\}$. Atunci:

(i) $F_f \in F(B_1)$;

(ii) f ca funcţie este injecţie $\Leftrightarrow F_f = \{1\}$;

(iii) $B_1 / F_f \approx Im(f)$ (unde $Im(f) = f(B_1)$).

Demonstraţie. (i). Se verifică imediat prin dualizarea teoremei corespunzatoare de lalatici.

(ii). Dacă f este injectivă şi $x \in F_f$ atunci din $f(x) = \mathbf{1} = f(\mathbf{1}) \Rightarrow x = \mathbf{1}$. Dacă $F_f = \{\mathbf{1}\}$ şi $f(x) = f(y)$, atunci $f(x' \vee y) = f(x \vee y') = \mathbf{1}$, deci $x' \vee y = x \vee y' = \mathbf{1}$, adică $x \leq y$ şi $y \leq x$, deci $x = y$.

(iii). Considerăm aplicaţia $\alpha : B_1/F_f \to f(B_1)$ definită prin $\alpha (x/F_f) = f(x)$, pentru orice $x/F_f \in B_1/F_f$.

Deoarece pentru $x, y \in B_1$: $x/F_f = y/F_f \Leftrightarrow x \sim_{F_f} y \Leftrightarrow (x' \vee y) \wedge (x \vee y') \in F_f$ (conform Teoremei 1) $\Leftrightarrow f((x' \vee y) \wedge (x \vee y')) = \mathbf{1} \Leftrightarrow f(x' \vee y) = f(x \vee y') = \mathbf{1} \Leftrightarrow f(x) = f(y) \Leftrightarrow \alpha(x/F_f) = \alpha (y/F_f)$, deducem că α este corect definită şi injectivă.

Avem : $\alpha (x/F_f \vee y/F_f) = \alpha ((x \vee y) / F_f) = f(x \vee y) = f(x) \vee f(y) = \alpha (x/F_f) \vee \alpha (x/F_f)$; analog se arată că $\alpha (x/F_f \wedge y/F_f) = \alpha (x/F_f) \wedge (y/F_f)$ şi $\alpha (x'/F_f) = (\alpha (x/F_f))'$, deci α este morfism de latici Boole.

Fie $y = f(x) \in f(B_1)$, $x \in B_1$; atunci $x/F_f \in B_1/F_f$ şi $\alpha (x/F_f) = f(x) = y$, deci α este surjectiv, adică izomorfism. ■

Teorema 1.5 . Pentru un filtru propriu F al unei algebre Boole B următoarele afirmaţii sunt echivalente:

(i) F este ultrafiltru;

(ii) Pentru orice $x \in B \setminus F$ avem că $x' \in F$.

Demonstraţie. Să observăm că nu putem avea $x, x' \in F$ deoarece atunci $x \wedge x' = \mathbf{0} \in F$, adică $F = B$, absurd.

(i) $\Rightarrow$ (ii). Presupunem că F este ultrafiltru şi că $x \notin F$. Atunci $[F \cup \{x\}) = B$. Deoarece $\mathbf{0} \in B$, există $x_1, \ldots, x_n \in F$ a.î. $x_1 \wedge \ldots \wedge x_n \wedge x = \mathbf{0}$, deci $x_1 \wedge \ldots \wedge x_n \leq x'$, de unde concluzia că $x' \in F$ (căci $x_1 \wedge \ldots \wedge x_n \in F$ şi F este un filtru).

(ii) $\Rightarrow$ (i). Să presupunem că există un filtru propriu F_1 a.î. $F \subsetneq F_1$, adică există $x \in F_1 \setminus F$. Atunci $x' \in F$, deci $x' \in F_1$ şi cum $x \in F_1$ deducem că $\mathbf{0} \in F_1$, deci $F_1 = B$, absurd. Deci F este ultrafiltru. ■

Teorema 1.6. Pentru un filtru propriu F al unei algebre Boole B următoarele afirmaţii sunt echivalente:

(i) F este ultrafiltru;

(ii) $0 \notin F$ şi pentru orice elemente $x, y \in B$ dacă $x \vee y \in F$ atunci $x \in F$ sau $y \in F$ (adică F este *filtru prim*).

Demonstraţie. (i) $\Rightarrow$ (ii). Presupunem că $x \vee y \in F$ şi $x \notin F$.

Atunci $[F \cup \{x\}) = B$ şi atunci cum $\mathbf{0} \in B$ există $z \in F$ a.î. $z \wedge x = \mathbf{0}$. Deoarece $z, x \vee y \in F$ rezultă că $z \wedge (x \vee y) = (z \wedge x) \vee (z \wedge y) = \mathbf{0} \vee (z \wedge y) = z \wedge y \in F$. Cum $z \wedge y \leq y$ deducem că $y \in F$.

(ii) $\Rightarrow$ (i). Cum pentru orice $x \in B$, $x \vee x' = 1$, deducem că $x \in F$ sau $x' \in F$ şi atunci F este un ultrafiltru. ■

Teorema 1.7. Pentru un filtru propriu F al unei algebre Boole B următoarele afirmaţii sunt echivalente:

(i) F este ultrafiltru;

(ii) $B/F \approx 2$.

Demonstraţie. (i) $\Rightarrow$ (ii). Reamintim că $B/F = \{x/F \mid x \in B\}$ (vezi Teorema 3). Fie $x \in B$ a.î. $x/F \neq \mathbf{1}$. Atunci $x \notin F$,deci $x' \in F$, adică $x'/F = \mathbf{1}$. Dar $(x/F)' = x'/F$, deci $x/F = (x/F)'' = \mathbf{1}' = \mathbf{0}$, de unde concluzia că $B/F = = \{\mathbf{0}, \mathbf{1}\} \approx \mathbf{2}$.

(ii) $\Rightarrow$ (i). Dacă $x \notin F$ atunci $x/F \neq \mathbf{1}$, deci $x/F = \mathbf{0}$ iar $x'/F = (x/F)' = \mathbf{0}' = \mathbf{1}$, adică $x' \in F$ şi deci F este ultrafiltru. ■

Teorema 1.8. (*Stone*). Pentru orice algebră Boole B există o mulţime M a.î. B este izomorfă cu o subalgebră Boole a algebrei Boole $(P(M), \subseteq)$.

Demonstraţie. Vom nota prin $M = U_B$ mulţimea ultrafiltrelor lui B iar despre $u_B : B \to P(U_B)$, $u_B(x) = \{F \in U_B : x \in F\}$ vom arăta că este morfism injectiv de algebre Boole (astfel că B va fi izomorfă cu $u_B(B)$)

Dacă $x, y \in B$ şi $x \neq y$ atunci există $F \in U_B$ a.î. $x \in F$ şi $y \notin F$, adică $F \in u_B(x)$ şi $F \notin u_B(y)$, deci $u_B(x) \neq u_B(y)$.

În mod evident $u(0) = \varnothing$ şi $u(1) = U_B$.

Fie acum $x, y \in B$ şi $F \in U_B$. Avem: $F \in u_B(x \wedge y) \Leftrightarrow x \wedge y \in F \Leftrightarrow x \in F$ şi $y \in F$ deci $u_B(x \wedge y) = u_B(x) \wedge u_B(y)$.

Deducem că $u_B(x \vee y) = u_B(x) \vee u_B(y)$, iar apoi $u_B(x') = (u_B(x))'$, adică u_B este şi morfism de algebre Boole. ■

CURSUL nr. 6

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

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

Pentru uşurinţa 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 operaţia algebrică φ *multiplicativ*).

În anumite situaţii folosim pentru φ şi notaţia *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: $\varphi : Hom(A) \times Hom(A) \to Hom(A)$, $\varphi(f, g) = fog$ pentru orice $f, g \in Hom(A)$.

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).

Definiția1.2. 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 $x, y, z \in M$, $(xy)z = x(yz)$.**

Operațiile de intersecție, reuniune şi diferență simetrică sunt exemple de operații ce sunt simultan comutative şi asociative, pe când compunerea funcțiilor nu este operație comutativă fiind însă asociativă.

Dacă o operație 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 notațiile:

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

$x_1+x_2+\ldots+x_n = \sum_{i=1}^{n} x_i$ (când aceeaşi operație 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 operația algebrică este notată multiplicativ şi $x_1+x_2+\ldots+x_n = nx$ dacă ea este notată aditiv**.**

Definiție Fie M o mulțime nevidă pe care avem o operație algebrică. Vom spune că un element $e \in M$ este ***element neutru*** pentru operația algebrică respectivă dacă pentru orice $x \in M$, $xe = ex = x$.

Observație 1.3.

(i). Dacă o operație 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 operații algebrice (dacă există !) este unic.

(ii). În cazul adoptării notației multiplicative pentru o operație algebrică, elementul său neutru (dacă există) va fi notat prin 1, iar în cazul adoptării notației 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 1.4. Un dublet (M, ·) 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, ·) 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 (fără 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.

Să revenim acum la cazul general al semigrupurilor.

Următorul rezultat este imediat:

Propoziția 1.5. 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 $(xy)^n = x^n y^n$.

Definiția1.6.. Dacă M, M′ sunt monoizi, o funcție $f:M \to M'$ 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 $M, M' \in Mon$ vom nota prin $Hom_{Mon}(M, M')$ (sau mai simplu $Hom(M, M')$ dacă nu este pericol de confuzie) toate morfismele de monoizi de la M la M′, adică $Hom(M, M') = \{f:M \to M' / f \text{ este morfism de monoizi}\}$.

Propoziția1.7. 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 $gof \in Hom(M, M')$.■

Definiția1.8. **Dacă M şi M′ sunt doi monoizi, numim *izomorfism de monoizi* un morfism $f \in Hom(M, M')$ pentru care există $g \in Hom(M', M)$ a.î. $f \circ g = 1_{M'}$ şi $g \circ f = 1_M$; în acest caz vom spune despre monoizii M, M′ că sunt *izomorfi* şi vom scrie $M \approx M'$.**

Se deduce imediat că $f \in Hom(M, M')$ este izomorfism de monoizi dacă şi numai dacă f este bijecție; atunci $f^{-1}:M' \to M$ este morfism de monoizi.

Definiția1.9. 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 $x^{-1} \in U(M)$ iar $(x^{-1})^{-1}=x$.

Pentru exemplele de monoizi de până acum avem: $U(P(T),\cap)=\{T\}$, $U(P(T),\cup)=\{\emptyset\}$, $U(P(T),\Delta)=P(T)$, $U(\mathbb{N},+)=\{0\}$, $U(\mathbb{N},\cdot) = \{1\}$, iar pentru o mulțime $A \neq \emptyset$, $U(Hom(A),o)=\{f:A \to A$ / 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.

Propoziția1.10.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 $(xy)^{-1}=y^{-1}x^{-1}$.■

Observație. 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 $M_1, M_2, \ldots, M_n$ 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 1.11. 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 $1 \leq i \leq n\Leftrightarrow x\in U(M_1) \times\ldots\times U(M_n)$, 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 $p_i \in Hom(M, M_i)$.

Să verificăm acum proprietatea de universalitate, iar pentru aceasta fie M′ un alt monoid şi pentru $1 \leq i \leq n$ să considerăm $p_i'\in Hom(M', M_i)$. Pentru $x\in M'$, definim $u:M'\to M$ prin $u(x)=(p_1'(x),\ldots,p_n'(x))$ şi se verifică imediat că $u\in Hom(M', M)$ iar $p_iou=p_i'$, pentru orice $1\leq i \leq n$.

Fie acum $u'\in Hom(M', M)$ a.î. $p_iou'=p_i'$ 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 1.12. 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 $M_1, M_2, \ldots, M_n$ (când nu este pericol de confuzie nu vom mai specifica proiecțiile).

CURSUL nr. 7

§1. Grup. Calcule într-un grup. Subgrup.
Subgrup generat de o mulțime. Grup ciclic.
Ordinul unui element într-un grup.

Definiția1.1. Vom spune despre un monoid M că este *grup* dacă U(M)=M. Altfel zis, dubletul $(M, \cdot)$ 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 $(P(T), \Delta)$ este grup comutativ.

2. Dacă A este o mulțime nevidă, atunci $(\sum(A) , o)$ este grup (în general necomutativ).

3. Mai general, dacă $(M, \cdot)$ este un monoid atunci $(U (M), \cdot)$ este grup.

În cele ce urmează prin $(G, \cdot)$ vom desemna un grup multiplicativ (dacă nu este pericol de confuzie nu vom mai specifica operația algebrică). Cardinalul mulțimii G se va nota $|G|$ şi se va numi *ordinul* grupului G .

În consecință, 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 $n \in \mathbb{N}$ $(xy)^n = x^n y^n$.

Definiția1.2. O submulțime nevidă S a lui G se zice *subgrup* al lui G dacă S împreună cu restricția operației algebrice de pe G la S formează grup.

Vom nota prin L(G) mulțimea subgrupurilor lui G; pentru a exprima că $H \in L(G)$ vom indica lucrul acesta scriind că $H \leq G$.

Propoziția1.3. Pentru o mulțime nevidă S a lui G următoarele afirmații 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 $x, y \in S$, $x^{-1}y \in S$.

Demonstrație. Implicațiile (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.

Propoziția1.4. 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 $S \leq G$.■

Observația1.5. În ceea ce priveşte reuniunea a două subgrupuri ale lui G să demonstrăm că dacă $H, K \in L(G)$, atunci $H \cup K \in L(G) \Leftrightarrow H \subseteq K$ 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.

Definiția1.6. 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

$$\langle M \rangle = \bigcap_{\substack{S \in L(G) \\ M \subseteq S}} S .$$

Dacă $M \in L(G)$, în mod evident $\langle M \rangle = M$.

Propoziția1.7. Dacă $M \subseteq G$ este o submulțime nevidă, atunci $\langle M \rangle = \{x_1 \ldots x_n \mid n \in \mathbb{N}$ iar $x_i \in M$ sau $x_i^{-1} \in M$ pentru orice $1 \leq i \leq n\}$.

Demonstrație. Fie $H=\{x_1 \dots x_n \mid n\in\mathbb{N}$ iar $x_i \in M$ sau $x_i^{-1} \in M$ pentru orice $1\le i\le n\}$ şi $x, y\in H$, adică $x=x_1 \dots x_n$, $y=y_1 \dots y_m$ cu x_i sau x_i^{-1} în M şi y_j sau y_j^{-1} în M pentru $1\le i\le n$ şi $1\le j\le m$.

Cum $x^{-1}y = x_n^{-1} \dots x_1^{-1}\ y_1 \dots y_m$ deducem că $x^{-1}y\in H$, adică $H\le G$. 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 $S\le G$ astfel încât $M\subseteq S$. Atunci $H\subseteq S$, deci $H\subseteq \bigcap_{\substack{S\le G\\ M\subseteq S}} S = <M>$, de unde egalitatea $<M>=H$.■

Corolar 1.8 . $<x>=\{x^n \mid n\in\mathbb{N}\}\cup\{(x^{-1})^n \mid n\in\mathbb{N}\}$.

Definiție. $<x>$ poartă numele de *grupul ciclic* generat de x. *Ordinul* unui element $x\in G$ notat o(x) se defineşte ca fiind $o(x)=|<x>|$. Evident, $o(1)=1$ iar dacă $x\ne 1$ şi $o(x)=n$, atunci n este cel mai mic număr natural pentru care $x^n=1$. Dacă $o(x)=\infty$, atunci $x^n\ne 1$, pentru orice $n\ge 1$.

Observația 1.9.

1. Dacă $x\in G$ este de ordin finit şi 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 $n=c\cdot o(x)+r$ şi $r<o(x)$.

Din $x^{o(x)}=x^n=1$ deducem imediat că şi $x^r=1$, 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) şi o(y) sunt finite, xy = yx şi (o(x), o(y)) = 1, atunci o(xy) = o(x)o(y).

Într-adevăr, dacă notăm m = o(x), n = o(y) şi 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 $m\mid np$ şi cum (m,n) = 1 deducem că $m\mid p$. Analog $n\mid p$ şi cum (m,n) = 1 deducem că $mn\mid p$, adică p = mn.

3. Din cele de mai înainte deducem recursiv că dacă $x_1, x_2, \dots, x_n\in G$ $(n\ge 2)$ şi cele n elemente comută între ele iar ordinele a oricare două (diferite) sunt prime între ele, atunci $o(x_1 \dots x_n)=o(x_1)\dots o(x_n)$.

Propoziția1.10. $(L(G), \subseteq)$ este latice completă.

Demonstrație. În mod evident $0=\{1\}$, $1=G$ iar pentru H, $K\in L(G)$, $H\wedge K=H\cap K$ iar $H\vee K=<H\cup K>$. 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 $\bigvee_{i\in I} S_i = <\bigcup_{i\in I} S_i> \in L(G)$.■

§2.Subgrupuri normale. Factorizarea unui grup printr-un subgrup normal

Definiția 2.1. 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 $L_0(G)$ mulțimea subgrupurilor normale ale lui G. Evident, $L_0(G)\subseteq L(G)$, $\{1\}$, $G\in L_0(G)$ iar dacă G este comutativ, atunci $L_0(G)= L(G)$.

Propoziția 2.2. Pentru $H\in L(G)$ următoarele afirmații sunt echivalente

(i) $H\in L_0(G)$

(ii) Pentru orice $x\in G$, $xHx^{-1}\subseteq H$ (unde $xHx^{-1}=\{xhx^{-1} : h\in H\}$).

Demonstrație. (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)⇒(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 $H\in L_0(G)$.■

Propoziția 2.3. $L_0(G)$ este sublatice modulară marginită a lui L(G).

Demonstrație. 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 $K\cap(LH)\subseteq H(K\cap L)$.■

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 2.4. 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 2.5.

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 $H\cap xH = H\cap Hx=\emptyset$ 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 $H\trianglelefteq G$.

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 $x\in G$, $[x]_{\rho_H^s}=xH$ şi $[x]_{\rho_H^d}=Hx$.

În cazul în care $H\trianglelefteq G$, atunci $\rho_H^s=\rho_H^d\overset{\text{def}}{=}\rho_H$ 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, $y'\in G$ 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 $H \trianglelefteq G$ (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 construcţia grupului factor G/H continuă ca mai înainte.

Observaţia 2.6. Am văzut că dacă $H \trianglelefteq G$, atunci ρ_H este o congruenţă pe G (adică o relaţie de echivalenţă pe G compatibilă cu structura de grup a lui G).

Se poate arăta imediat că asocierea $H \rightsquigarrow \rho_H$ stabileşte o bijecţie între $L_0(G)$ şi congruenţele de pe G. Într-adevăr, dacă ρ este o congruenţă 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 funcţiei $H \rightsquigarrow \rho_H$ (de mai înainte).

CURSUL nr. 8

§1.Morfisme de grupuri. Compunerea morfismelor de grupuri. Monomorfisme, epimorfisme, izomorfisme de grupuri.

Definiţia 1.1. Dacă G şi G′ sunt două grupuri, vom spune că o funcţie f:G→G′ este *morfism* de grupuri dacă pentru orice x, y∈G, f(xy)=f(x)f(y).

Vom nota $Hom_{Gr}(G, G') = \{f: G \to G' \mid f \text{ este morfism de grupuri}\}$. Dacă nu este pericol de confuzie în loc de $Hom_{Gr}(G, G')$ vom scrie $Hom(G, G')$.

Exemple.

1. Funcţia $1_G: G \to G$ este morfism de grupuri.

2. $f: G \to G'$, $f(x)=1$ pentru orice $x \in G$ este de asemenea morfism de grupuri (numit *morfismul nul*).

3. Dacă $H \trianglelefteq G$ atunci $p_H: G \to G/H$, $p_H(x)=xH$ pentru orice $x \in G$ este morfism surjectiv de grupuri (numit morfismul *surjectiv canonic*).

Observaţia.1.2. Ca şi în cazul monoizilor se demonstrează imediat că dacă G, G′, G″ sunt grupuri şi $f \in Hom(G,G')$, $g \in Hom(G',G'')$, atunci $gof \in Hom(G,G'')$.

Propoziţia 1.3. Dacă G, G′ sunt grupuri şi $f \in Hom(G, G')$, atunci $f(1)=1$ şi $f(x^{-1}) = (f(x))^{-1}$ pentru orice $x \in G$.

Demonstraţie. Din $1=1\cdot 1$ deducem că $f(1)=f(1\cdot 1)=f(1)\cdot f(1)$ iar de aici că $f(1)=1$. Dacă $x \in G$, cum $xx^{-1} = 1$ deducem $1 = f(1) = f(xx^{-1}) = = f(x)\, f(x^{-1})$, de unde $f(x^{-1})=f(x)^{-1}$.■

Propoziţia 1.4. Fie G, G′ grupuri iar $f \in Hom(G, G')$.

(i) Dacă $H \le G$ atunci $f(H) \le G'$

(ii) Dacă $H \trianglelefteq G$ şi f este funcţie surjectivă, atunci $f(H) \trianglelefteq G'$

(iii) Dacă $H' \le G'$, atunci $f^{-1}(H') \le G$

(iv) Dacă $H' \trianglelefteq G'$, atunci $f^{-1}(H') \trianglelefteq G$.

Demonstraţie. (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 $f(H) \le G'$.

(ii). Dacă $x' \in G'$ şi $h' \in f(H)$ atunci cum f este surjecţie $x'=f(x)$ 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 $f^{-1}(H') \trianglelefteq G$.■

Observaţia 1.5. Dacă $f \in Hom(G, G')$, conform propoziţiei 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 $Im(f) \leq G'$.

Propoziţia 1.6. Dacă G, G′ sunt grupuri iar $f \in Hom(G, G')$, următoarele afirmaţii sunt echivalente:

(i) f este funcţie injectivă

(ii) $Ker(f) = \{1\}$

(iii) Pentru orice grup G″ şi $\alpha, \beta \in Hom(G'', G)$, dacă $fo\alpha = fo\beta$, atunci $\alpha = \beta$.

Demonstraţie. (i) $\Rightarrow$ (ii). Evident $\{1\} \subseteq Ker(f)$. Dacă $x \in Ker(f)$ atunci $f(x) = 1 = f(1)$ şi cum f este injecţie 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 injecţie.

(i)$\Rightarrow$(iii). Evidentă

(iii)$\Rightarrow$(i). Să presupunem prin absurd că f nu este injectivă (deşi verifică (iii)). Cum (i) $\Leftrightarrow$ (ii), deducem că $Ker(f) \neq \{1\}$. Dacă notăm $G'' = Ker(f)$ şi considerăm $\alpha, \beta: G'' \to G$, α=incluziunea iar β= morfismul nul (adică $\beta(x) = 1$ pentru orice $x \in G''$), atunci $\alpha \neq \beta$ şi $fo\alpha = fo\beta$ (căci ambele dau morfismul nul) – absurd !.■

Observaţia 1.7. Datorită propoziţiei precedente vom numi morfismele injective de grupuri *monomorfisme.* Monomorfismele se mai zic şi *scufundări.*

Propoziţia 1.8. Dacă G, G′ sunt grupuri iar $f \in Hom(G, G')$, 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 $\alpha, \beta \in Hom(G', G'')$, dacă $\alpha of = \beta of$, atunci $\alpha = \beta$.

Demonstraţie. Echivalenţa (i) $\Leftrightarrow$ (ii) este imediată.

(i)$\Rightarrow$(iii). Dacă $y \in G'$ cum f este surjecţie există $x \in G$ astfel încât $f(x) = y$. Atunci $(\alpha of)(x) = (\beta of)(x) \Leftrightarrow \alpha(f(x)) = \beta(f(x)) \Leftrightarrow \alpha(y) = \beta(y)$, adică $\alpha = \beta$.

(iii)$\Leftarrow$(i). Să presupunem că f verifică (iii) şi totuşi nu este surjectivă, adică $Im(f) \neq G'$. Alegând $G'' = G'/Im(f)$ (lucru posibil deoarece prin ipoteză G′ este comutativ şi deci $Im(f) \trianglelefteq G'$) avem că $G'' \neq \{1\}$ şi astfel alegând $\alpha = p_{Im(f)}: G' \to G''$ şi β= morfismul nul de la G′ la G″ avem că $\alpha \neq \beta$ deşi $\alpha of = \beta of$ (căci ambele compuneri dau morfismul nul) – absurd.■

Observaţia 1.9. Datorită propoziţiei precedente morfismele surjective $f \in Hom(G, G')$ cu G′ comutativ se mai zic şi *epimorfisme.*

Definiţia 1.10. 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 $G \approx G'$.

§2.Teoremele de izomorfism pentru grupuri

Vom începe cu o teoremă cunoscută sub numele de *teorema fundamentală de izomorfism pentru grupuri:*

Teorema.2.1. Dacă G, G′ sunt grupuri iar f∈Hom(G, G′), atunci G/Ker(f)≈Im(f).

Demonstrație. Dacă notăm H=Ker(f) atunci H={x∈G | f(x)=1}⊴G iar G/Ker(f)={x Ker f | x∈G}={xH | x∈G}.

Definim φ:G/Ker(f)→Im(f) prin φ(xH)=f(x) pentru orice x∈G. Dacă x, y∈G, atunci din echivalențele xH=yH ⇔ $x^{-1}y$∈H ⇔ f($x^{-1}y$)=1 ⇔ 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 grupu**ri.**■

Corolar 2.2. Dacă G, G′ sunt grupuri iar f∈Hom(G, G′) un morfism surjectiv de grupuri, atunci G/Ker(f)≈G′.

Corolar 2.3. Fie G un grup, H, K subgrupuri ale lui G a.î K ⊴G. Atunci HK ≤ G, H∩K ⊴H iar HK / K ≈ H / H∩K.

În plus, dacă şi H ⊴ G, atunci HK⊴ G (unde reamintim că HK={hk / h∈H şi k∈K}).

Demonstrație. Cum K⊴G, xK=Kx pentru orice x∈G şi prin urmare $HK=\bigcup_{x\in H} Kx = \bigcup_{x\in H} xK = KH$

.

Dacă x, y∈HK, x=h_1k_1 şi y=h_2k_2 cum h_1, h_2∈H şi k_1, k_2∈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}∈KH=HK (căci din H, K≤G şi K⊴G deducem pe rând că h_1,h_2^{-1}∈K, $h_1(k_1k_2^{-1})h_1^{-1}$∈K şi $h_1h_2^{-1}$∈H), adică HK≤G.

În mod evident K⊴HK şi să considerăm φ:H→HK/K, φ(x)=xK pentru orice x∈H (evident φ este corect definită deoarece pentru x∈H avem x∈HK şi xK∈HK/K), care este morfism de grupuri.

Deoarece orice element din HK/K este de forma (xy)K=x(yK)=xK=φ(x) (cu x∈H şi y∈K) deducem că φ este morfism surjectiv de grupuri.

În plus, Ker φ={x∈H / φ(x)=1}={x∈H / xK=K}={x∈H / x∈K}=H∩K.

Deducem că H/Kerφ ≈ HK/K ⇔H/H∩K≈HK/K. Dacă şi H⊴G, atunci pentru orice x∈G avem x(HK)=(xH)K=(Hx)K=H(xK)=H(Kx)=(HK)x, adică HK⊴G.■

§3.Grupuri de permutări. Teorema lui Cayley. Grupurile S_n şi A_n.

Fie M o mulțime nevidă iar Σ(M)={f∈**Hom**(M) | f este bijectivă}. După cum am văzut în §1 al acestui capitol (**Hom**(M),∘) este monoid iar Σ(M) apare acum ca grupul unităților monoidului **Hom**(M).

Convenim să numim grupul Σ(M) ca fiind *grupul permutărilor asupra elementelor mulțimii M.*

Dacă M este o mulțime cu n elemente (exemplul clasic fiind M={1,2,…,n} cu n≥1), atunci grupul Σ(M) se notează prin S_n şi se va numi *grupul permutărilor asupra unei mulțimi cu n elemente sau grup simetric de grad n.* (vom vedea mai departe că pentru grupul S_n natura elementelor mulțimii 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 $\begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$.

Vom nota prin e_n sau simplu prin e (dacă nu este pericol de confuzie) permutarea identică din S_n.

Avem că $|S_n| = n!$.

Teorema 3.1.(*Cayley*) Orice grup G este izomorf cu un subgrup al grupului de permutări Σ (G).

Demonstrație. 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 funcție o injecție.

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 $\varphi\in$ **Hom** $(G, \Sigma(G))$. Deducem că $G\approx\varphi(G)\le\Sigma(G)$.■

În continuare ne vom ocupa de studiul grupului S_n cu $n\ge 2$. Evident, grupul S_2 având 2 elemente este comutativ pe când începând cu $n\ge 3$, S_n nu mai este comutativ.

Definiția 3.2. Numim *ciclu de lungime k* **$(2\le k\le n)$ o permutare $\sigma\in S_n$ pentru care există elementele distincte $i_1,i_2,\dots,i_k$ din $\{1,2,\dots,n\}$ a.î. $\sigma(i_1)=i_2$, $\sigma(i_2)= i_3$, …, $\sigma(i_k)=i_1$ iar $\sigma(i)=i$ pentru orice $i\in\{1,2,\dots,n\}\setminus\{i_1,i_2,\dots,i_k\}$.** Convenim să notăm un astfel de ciclu σ prin $\sigma = (i_1\ i_2\ \dots\ i_k)$ sau $\sigma = (i_1,i_2, \dots, i_k)$ (dacă există pericol de confuzie).

Ciclii de lungime 2 se mai numesc şi *transpoziții.*

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 mulțimea $\{i_1,i_2, \dots, i_k\}$ 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 disjuncți* dacă $\{i_1, i_2, \dots, i_k\}\cap\{j_1, j_2, \dots, j_t\}=\emptyset$.

Propoziția 3.3. Dacă σ, τ sunt ciclii disjuncți din S_n, atunci $\sigma\tau=\tau\sigma$.

Demonstrație. 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 esență 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 $\sigma(j)=j$.■

Observația 3.4. 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 distincți de lungime k.

Propoziția 3.5. Ordinul oricărui ciclu de lungime k $(2\le k\le n)$ este k . Dacă σ,τ sunt 2 ciclii disjuncți 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 $o(\sigma t)=o(\sigma)\cdot o(\tau)$.

Demonstrație. 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 $\sigma^{k-1}(i) = i_k \ne i$ 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 disjuncți 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 3.6. Dacă $\sigma_1, \dots \sigma_k$ sunt ciclii disjuncți 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 3.7.. Orice permutare $\sigma\in S_n$, $\sigma\neq e$ se descompune în mod unic în produs de ciclii disjuncți (exceptând ordinea în care aceştia sunt scrişi) .

Demonstrație. 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 inducție matematică după t. Dacă t=2 totul este clar căci în acest caz σ se reduce la o transpoziție.

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 disjuncți. 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 obținem $\sigma^p(i_0)=i_0$ şi deci $i_p=i_0$ contrazicând alegerea lui m (căci p<m).

Analog dacă r<s. Cu $i_0,i_1, \dots, i_{m-1}$ formăm ciclul $\tau =(i_0 i_1 \dots i_{m-1})$ şi să considerăm permutarea $\sigma'=\tau^{-1}\sigma$. Dacă avem un i a.î. $\sigma(i)=i$, atunci $i\notin \{ i_0,i_1, \dots , i_{m-1}\}$ 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 $i\in\{ i_0,i_1, \dots ,i_{m-1}\}$ avem $\sigma'(i)=i$.

Rezultă că σ′ schimbă efectiv mai puțin de t-m elemente iar cum $m\ge 2$ atunci t-m<t, deci putem aplica ipoteza de inducție lui σ′. Rezultă atunci că putem scrie $\sigma'=\tau_2 \dots \tau_s$ cu $\tau_2 \dots \tau_s$ ciclii disjuncți. Punând $\tau_1=\tau$ obținem că $\sigma= \tau_1\tau_2 \dots \tau_s$ iar τ_1 este disjunct față de ceilalți ciclii. Din modul efectiv de descompunere de mai înainte deducem că scrierea lui σ sub forma $\sigma= \tau_1\tau_2 \dots \tau_s$ este unic determinată.■

Observația 3.8. Dacă $\sigma=(i_1, i_2, \dots ,i_k)$ este un ciclu de lungime k din S_n ($2\le k\le n$), atunci se probează imediat prin calcul direct că avem următoarele descompuneri ale lui σ în produs de transpoziții:

$\sigma=(i_1i_2)(i_2i_3)\dots(i_{k-1}i_k)=(i_1i_k)(i_1i_{k-1}) \dots (i_1i_2)$.

Din cele de mai sus deducem imediat următorul rezultat:

Corolar 3.9. Orice permutare $\sigma\in S_n$ ($n\ge 2$) este un produs de transpoziții (să observăm că dacă σ=e, atunci σ=(12)(12)).

Definiție 3.10. Fie $\sigma\in S_n$. *Signatura lui σ* **este numărul** $\operatorname{sgn}(\sigma)=\prod_{1\le i<j\le n}\frac{\sigma(i)-\sigma(j)}{i-j}$**; evident,** $\operatorname{sgn}(\sigma)\in\{\pm 1\}$ **.**

O *inversiune* a lui σ este o pereche (ij) cu $1\le i<j\le n$ 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 mulțimea permutărilor pare.

Astfel, $\sigma\in S_n$ este pară $\Leftrightarrow \operatorname{sgn}(\sigma)=1$ şi impară $\Leftrightarrow \operatorname{sgn}(\sigma)=-1$.

Propoziția 3.11. Dacă $\sigma,\tau\in S_n$, atunci $\operatorname{sgn}(\sigma\circ\tau)=\operatorname{sgn}(\sigma)\cdot\operatorname{sgn}(\tau)$.

Demonstrație. Avem $\operatorname{sgn}(\sigma\circ\tau)=\prod_{1\le i<j\le n}\frac{\sigma(\tau(i))-\sigma(\tau(j))}{i-j}$

$$=\prod_{1\le i<j\le n}\frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)}\cdot\frac{\tau(i)-\tau(j)}{i-j}=$$
$$=\prod_{1\le i<j\le n}\frac{\sigma(i)-\sigma(j)}{i-j}\cdot\prod_{1\le i<j\le n}\frac{\tau(i)-\tau(j)}{i-j}=\operatorname{sgn}(\sigma)\cdot\operatorname{sgn}(\tau)\ \blacksquare$$

Corolar 3.12. Pentru orice $n\ge 2$, $A_n\trianglelefteq S_n$ 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 $\operatorname{Ker}(\operatorname{sgn})=\{\sigma\in S_n \mid \operatorname{sgn}(\sigma)=1\}=A_n$ deducem imediat că $A_n\trianglelefteq S_n$. Conform primului Corolar 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 3.13. Orice transpoziție (rs) cu $1\le r\le n$ 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 $\sigma=t_1t_2\dots t_m$, atunci $\operatorname{sgn}(\sigma)=\operatorname{sgn}(t_1)\operatorname{sgn}(t_2)\dots\operatorname{sgn}(t_m)=(-1)^m$ şi deci σ va fi permutare pară sau impară după cum m este par sau impar.

În particular, dacă $\sigma=(i_1\ i_2\ \dots\ i_k)$ cum $\sigma=(i_1i_2)(i_2i_3)\dots(i_{k-1}i_k)$ deducem că $\operatorname{sgn}(\sigma)=(-1)^{k-1}$.

Teorema 3.14. Două permutări $\alpha,\beta\in S_n$ sunt conjugate în S_n dacă şi numai dacă ele au aceeaşi structură ciclică.

Demonstrație. „⇒” . 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 $\alpha=\dots(i_1\ i_2\ \dots\ i_k)\dots$, atunci $\gamma\alpha\gamma^{-1}=\dots(\gamma(i_1)\ \gamma(i_2)\ \dots.\ \gamma(i_k))\dots$ de unde concluzia că α şi β au aceeaşi structură ciclică.

Faptul că $\gamma\alpha\gamma^{-1}$ acționează asupra lui α de maniera descrisă mai sus se probează astfel : se descompune α în ciclii disjuncți $\alpha=c_1c_2\dots c_t$ 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 $\gamma(i)\ne\gamma(i_1),\gamma(i_2)$ 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.

„⇐”. 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 raționîndu-se analog) . Să presupunem că suntem în S_5 şi avem $\alpha=(1\ 5)(4\ 2\ 3)$ şi $\beta=(3\ 4)(2\ 1\ 5)$. Ținând cont de felul în care acționează $\gamma\alpha\gamma^{-1}$ asupra lui α deducem că: $\gamma=\begin{pmatrix}1&5&4&2&3\\3&4&2&1&5\end{pmatrix}=(1\,3\,5\,4\,2)$. ■

CURSUL nr. 9

§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 ∈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∈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 $A^*=A\setminus\{0\}$.

Exemple.

1. Din cele stabilite în §6 de la Capitolul 2 deducem că $(\mathbb{Z},+,\cdot)$ este inel comutativ unitar.

2. Dacă vom considera $A=2\mathbb{Z}=\{2n : n\in\mathbb{Z}\}$ atunci $(A,+,\cdot)$ este exemplu de inel comutativ neunitar (căci $1\notin 2\mathbb{Z}$).

3. Dacă $n\in\mathbb{N}$, $n\geq 2$ atunci $(\mathbb{Z}_n, +, \cdot)$ 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 $\alpha=(\alpha_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}$.

Dacă m=n notăm $M_{m,n}(A)=M_n(A)$; o matrice din $M_n(A)$ se zice *pătratică de ordin n*.

Pentru $\alpha, \beta\in M_{m,n}(A)$, $\alpha=(\alpha_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}$ şi $\beta=(\beta_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}$ definim:

$$\alpha+\beta=(\alpha_{ij}+\beta_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}.$$

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 $-\alpha=(-\alpha_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}$, de unde concluzia că $(M_{m,n}(A), +)$ este grup (abelian).

Pentru m, n, $p\in\mathbb{N}^*$, $\alpha\in M_{m,n}(A)$, $\beta\in M_{n,p}(A)$, $\alpha=(\alpha_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}$, $\beta=(\beta_{jk})_{\substack{1\leq j\leq n\\ 1\leq k\leq p}}$ definim $\alpha\beta=(\gamma_{ik})_{\substack{1\leq i\leq m\\ 1\leq k\leq p}}$, unde $\gamma_{ik}=\sum_{j=1}^{n}\alpha_{ij}\beta_{jk}$ pentru $1\leq i\leq m$ şi $1\leq k\leq p$.

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 $\varepsilon_{it}=\sum_{k=1}^{p}\delta_{ik}\gamma_{kt}$ $=\sum_{k=1}^{p}(\sum_{j=1}^{n}\alpha_{ij}\beta_{jk})\gamma_{kt}=\sum_{k=1}^{p}\sum_{j=1}^{n}\alpha_{ij}\beta_{jk}\gamma_{kt}$.

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 $(\alpha\beta)\gamma=\alpha(\beta\gamma)$.

Ţinând cont de distributivitatea înmulţirii de pe A faţă 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 $n\in\mathbb{N}$, $n\ge 2$, 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.

Observaţia 1.2. 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 (ţinând cont de distributivitatea la stânga şi la dreapta a înmulţirii faţă de adunare) obţinem 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 noţiunea matematică corespunzătoare se traduce prin *anneaux.*

În anumite cărţi un inel oarecare se notează prin R (de la faptul că în limba engleză noţiunea matematică de inel se traduce prin *ring*).

Propoziţia 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 $a, b, a_i, b_i\in A$, $1\le i\le n$

(v) Dacă $a, b\in A$, $n\in\mathbb{N}^*$ şi $ab=ba$ avem egalităţile:
$a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\ldots+ab^{n-2}+b^{n-1})$
$a^{2n+1}+b^{2n+1}=(a+b)(a^{2n}-a^{2n-1}b+\ldots-ab^{2n-1}+b^{2n})$.

Demonstraţie. (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$\in$A şi n$\in\mathbb{Z}$

$$na=\begin{cases}\underbrace{a+\ldots+a}_{n\ ori} & \text{dacă } n>0\\ 0 & \text{dacă } n=0\\ \underbrace{(-a)+\ldots+(-a)}_{-n\ ori} & \text{dacă } n<0,\end{cases}$$

atunci (vi). a(nb)=(na)b=n(ab) pentru orice a, b$\in$A şi n$\in\mathbb{Z}$

(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 definiție a^0=1).

Egalitatea de la (vi) rezultă din (iv) iar (vii) se demonstrează prin inducție matematică după n ținând 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.

Definiția 1.6. Prin *unitățile* U(A) ale inelului unitar A înțelegem unitățile 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*.

Definiția 1.7. 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 $\begin{pmatrix}1&0\\1&0\end{pmatrix}$ este divizor al lui zero la stânga iar $\begin{pmatrix}0&0\\1&1\end{pmatrix}$ este divizor al lui zero la dreapta.

Dacă n∈$\mathbb{N}$, n ≥ 2 nu este un număr prim iar n=n_1n_2 cu n_1, n_2 diferiți de 1 şi n, atunci în inelul ($\mathbb{Z}_n$, +, ·) 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 1.8. 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∈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 1.10. Numim *domeniu de integritate* (sau *inel integru*), un inel comutativ, nenul şi fără divizori ai lui zero, diferiți de zero.

Inelul întregilor ($\mathbb{Z}$, +,·) este un exemplu de inel integru .

Definiția 1.11. Un element a∈A se zice *nilpotent* dacă există n∈$\mathbb{N}^*$ a.î. $a^n = 0$.

Vom nota prin **N**(A) mulțimea elementelor nilpotente din inelul A (evident 0∈**N**(A)).

De exemplu, în inelul A=$M_2(\mathbb{Z})$ dacă alegem M=$\begin{pmatrix}0&1\\0&0\end{pmatrix}$ cum $M^2=O_2$, deducem că M∈**N(**$M_2(\mathbb{Z})$**).** De asemenea, cum în inelul $\mathbb{Z}_8$ avem $\hat{2}^3 = \hat{8} = \hat{0}$ deducem că $\hat{2}$ ∈**N(**$\mathbb{Z}_8$**).**

În mod evident, dacă a∈**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 1.12. 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. $A=n\mathbb{Z}$.

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 $(\mathbb{Z}, +, \cdot)$ 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 iar $I\subseteq A$ o submulţime 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 $\mathbf{Id_s(A)=Id_d(A)=Id_b(A)}$ şi convenim să notăm prin $\mathbf{Id(A)}$ mulțimea idealelor lui A.

Observația 2.6.

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 ($n\geq 2$) 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 2.7. 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 2.8. Fie A un inel oarecare iar $M\subseteq A$ o submulțime nevidă a sa. Vom nota $\langle M\rangle_s$ ($\langle M\rangle_d$, $\langle M\rangle$) cel mai mic ideal stâng (drept, bilateral) al lui A ce conține pe M. Deci $\langle M\rangle_s=\bigcap_{\substack{I\in Id_s(A)\\ M\subseteq I}} I$, $\langle M\rangle_d=\bigcap_{\substack{I\in Id_d(A)\\ M\subseteq I}} I$ **iar** $\langle M\rangle=\bigcap_{\substack{I\in Id_b(A)\\ M\subseteq I}} I$.

Propoziția 2.9. Fie A un inel unitar şi $M\subseteq A$ o submulțime nevidă.

Atunci: (i) $\langle M\rangle_s=\{\sum_{i=1}^{n} a_i x_i \,|\, n\in\mathrm{N}^*, a_i\in A,\ x_i\in M,\ 1\leq i\leq n\}$

(ii) $\langle M\rangle_d=\{\sum_{i=1}^{n} x_i a_i \,|\, n\in\mathrm{N}^*, a_i\in A,\ x_i\in M,\ 1\leq i\leq n\}$

(iii) $\langle M\rangle=\{\sum_{i=1}^{n} a_i x_i b_i \,|\, n\in\mathrm{N}^*, a_i, b_i\in A,\ x_i\in M,\ 1\leq i\leq n\}$.

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 2.10. 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 $<a>_s = \{ba \mid b \in A\} \overset{def}{=} Aa$,

$$<a>_d = \{ab \mid b \in A\} \overset{def}{=} aA.$$

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 2.11. 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.

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 imediat că :

$$< \bigcup_{i \in K} I_i >_s = < \bigcup_{i \in K} I_i >_d =$$

$$= < \bigcup_{i \in K} I_i > = \{ \sum_{i \in K} a_i \Big| a_i \in I_i \ pentru \ \ i \in K \ \ iar \ \ \{i \in K | a_i \neq 0\} \ este \ \ finita \}$$ convenim să notăm această ultimă mulțime prin $\sum_{i \in K} I_i$ şi s-o numim *suma idealelor* $(I_i)_{i \in K}$.

§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∈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∈$\mathbb{Z}$ 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∈B este un element oarecare există a∈A a.î. f(a) = b. Cum a·1 = 1·a = a, deducem că f(a) f(1) = f(1) f(a) = f(a) ⇔

⇔ b·f(1)=f(1)·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∈**Hom(**A, B**),** g∈**Hom(**B, C**),** atunci g∘f∈**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∘g=1_B şi g∘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→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→A este morfism de inele şi cum f∘f^{-1}=1_B iar f^{-1}∘f=1_A deducem că f∈**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.

Demonstraţie. (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.■

Observaţia 3.5. Din propoziţia 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.

Propoziţia 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 funcţia F:Id_f(A)→Id(B), F(S)=f(S) pentru orice S∈I_f(A) este un izomorfism de mulţimi ordonate.

Demonstraţie. Definim G: Id(B)→Id_f(A) prin G(B') = f^{-1}(B') pentru orice B'∈Id(B). (in mod evident funcţia G este corect definită). Faptul că F şi G sunt morfisme de mulţimi ordonate (adică păstrează incluziunea) este imediat.

Ca şi în cazul grupurilor se arată că F∘G=$1_{Id(B)}$ şi G∘F=$1_{Id_f(A)}$, de unde concluzia propoziţiei.

■

Propoziţia 3.7. Fie f∈Hom(A, B) un morfism de inele.

(i) Dacă f este funcţie 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 $a,b\in f(I)$, atunci $a=f(a')$, $b=f(b')$ cu $a', b'\in I$ şi cum $a-b= =f(a') - f(b')=f(a'-b')$, iar $a'-b'\in I$ deducem că $a-b\in f(I)$.

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 3.9. În particular, deducem că **Ker(f)** este ideal bilateral al lui A, (adică $\mathrm{Ker}(f)\in\mathbf{Id_b}(A)$).

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 $A=\{(x_i)_{i\in I}: x_i\in A_i \text{ pentru orice } i\in I\}$.

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 3.10. (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 ($i\in I$). ■

Observația 3.11.

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 funcția $p_i: A\to A_i$ dată de $p_i((x_j)_{j\in I})=x_i$. (p_i poartă numele de *proiecția de indice i* sau *proiecția 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).

Propoziția 3.12. 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 $i\in I$.***

Demonstrație. 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 enunț, 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. ■

Definiția 3.13 . Dubletul $(A, (p_i)_{i\in I})$ ce verifică proprietatea de universalitate de mai sus 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 3.14. 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 3.15. Analog ca în cazul grupurilor 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 $x,y\in A$, $(x+I)+(y+I)=(x+y)+I$.

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.. $(A/I,+,\cdot)$ 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 $x, y, x', y'\in A$ a.î. $x+I=x'+I$ şi $y+I=y'+I$. Scriind $xy-x'y'=x(y-y')+(x-x')y'$ deducem că $xy-x'y'\in I$, adică $xy+I=x'y'+I$. Să alegem acum $x, y, z\in I$ 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 $(A/I, \cdot)$ este semigrup.

De asemenea, $\hat{x}(\hat{y}+\hat{z})=\widehat{x(y+z)}=\widehat{xy+xz}=\hat{x}\hat{y}+\hat{x}\hat{z}$ şi analog $(\hat{x}+\hat{y})\hat{z}=\hat{x}\,\hat{z}+\hat{y}\,\hat{z}$, de unde concluzia că $(A/I, +, \cdot)$ 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 $x+I\in A/I$ avem $(1+I)(x+I)=(x+I)(1+I)=x+I$.

Dacă A este inel comutativ, atunci $\hat{x}\,\hat{y}=\hat{xy}=\hat{yx}=\hat{y}\,\hat{x}$, 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 $p_I:A\to A/I$, $p_I(x)=x+I$ pentru orice $x\in A$ (care este morfism de grupuri aditive) este de fapt morfism de inele deoarece pentru $x,y\in A$ 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 $x\in I$, $x\in Ker(p_I)\Leftrightarrow x+I=I\Leftrightarrow x\in I$, 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, $f\in Hom(A, A')$, atunci $Ker(f)\in Id_b(A)$ şi $A/Ker(f)\approx Im(f)$.

Demonstrație. Pentru $x\in A$, definim: φ : **A/Ker(f)**$\to$Im(f) prin $\varphi(x+Ker(f))=f(x)$. Dacă mai avem $y\in A$, atunci din şirul de echivalențe $x+Ker(f)=y+Ker(f)\Leftrightarrow x-y\in Ker(f)\Leftrightarrow f(x)=f(y)$ deducem că φ este corect definită şi ca funcție este injecție. Cum surjectivitatea lui φ este evidentă, deducem că φ este bijecție. Deoarece pentru $x, y\in A$ avem :

$\varphi[(x+Ker(f))+(y+Ker(f))]=f(x+y)=f(x)+f(y)=\varphi[x+Ker(f)]+\varphi[y+Ker(f)]$ şi $\varphi[(x+Ker(f))(y+Ker(f))]=\varphi[xy+Ker(f)]=f(xy)=f(x)f(y)=$

$=\varphi[x+Ker(f)]\,\varphi[y+Ker(f)]$ deducem că φ este morfism de inele şi cum mai sus am probat că este şi bijecție, rezultă că φ este izomorfism de inele.■

Corolar.4.4. Dacă A, A′ sunt inele şi $f\in Hom(A,A')$ este un morfism surjectiv de inele, atunci $A/Ker(f)\approx A'$.

Corolar.4.5. Fie A un inel, $A'\subseteq A$ un subinel iar $I\in Id_b(A)$. Atunci $A'+I=\{x+y|\ x\in A', y\in I\}$ este subinel al lui A, $I\in Id_b(A'+I)$, $A'\cap I\in Id_b(A')$ şi avem următorul izomorfism de inele:

$$A'/(A'\cap I)\approx (A'+I)/I\ .$$

Demonstrație Fie $a,b\in A'+I$, $a=x+y$, $b=z+t$, $x,z\in A'$ şi $y,t\in I$. Atunci $a-b=(x-z)+(y-t)\in A'+I$ iar $ab=(x+y)(z+t)=xz+(xt+yz+yt)\in A'+I$, de unde concluzia că A′+I este subinel al lui A. Faptul că $I\in Id_b(A'+I)$ este evident.

Să considerăm acum $\varphi:A'\to(A'+I)/I$, $\varphi(x)=x+I$ care este în mod evident morfism de inele. Dacă avem un element $(x+y)+I$ din $(A'+I)/I$ cu $x\in A'$ şi $y\in I$, atunci cum $(x+y)-x=y\in I$ deducem că $(x+y)+I=x+I=\varphi(x)$, adică φ este surjecție.

Din şirul de echivalențe: $x\in Ker(\varphi)\Leftrightarrow\varphi(x)=0\Leftrightarrow x+I=I$, 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 avem izomorfismele de inele:

$$A/Ker(\varphi)\approx Im(\varphi)\ \Leftrightarrow\ A'/(A'\cap I)\approx(A'+I)/I.$$■

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: $A/J\approx(A/I)/(J/I)$ **.**

Demonstrație. Echivalența $J\in Id_b(A) \Leftrightarrow J/I \in Id_b\ (A/I)$ 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 ■

CURSUL nr. 10

§1.Corp. Subcorp. Subcorp prim.
Morfisme de corpuri. Caracteristica unui corp

Definiția 1.1. Vom spune despre un inel unitar K că este *corp* dacă $U(K)=K^*$ (unde $K^*=K\setminus\{0\}$). Astfel, (K, +, ·) este corp dacă:

(i) (K, +) este grup

(ii) (K*, ·) este grup

(iii) Înmulțirea este distributivă la stânga şi la dreapta față de adunare.

Din cele stabilite anterior deducem că dacă $n\in\mathbb{N}$, $n\geq 2$, atunci $(\mathbb{Z}_n,+,\cdot)$ este corp dacă şi numai dacă n este prim. .

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 1.2. 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 .

Propoziția 1.3. 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.■

Definiția 1.4. 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 $f(x^{-1}) = (f(x))^{-1}$.

Observația 1.5. Orice morfism de corpuri $f : K\to K'$ este ca funcție o injecție.

Într-adevăr, dacă vom considera x, y∈K a.î. f(x)=f(y) şi presupunem prin absurd că x-y≠0, cum x-y∈K^*, există z∈K^* a.î. (x-y)z=1. Deducem imediat că : f(x-y)f(z)= f(1)=1 ⇔ (f(x)-f(y))f(z)=1 ⇔ 0·f(z)=1 ⇔ 0=1-absurd, deci x-y=0 ⇒x = y.■

Definiția 1.6. Un morfism de corpuri f:K→K′ se zice *izomorfism de corpuri* dacă există g:K′→K a.î. g∘f=1_K şi f∘g=$1_{K'}$. În acest caz vom scrie K≈K′. Se probează imediat că f este izomorfism de corpuri dacă şi numai dacă f este morfism bijectiv de corpuri.

Ținând cont de observația de mai sus deducem că morfismul f : K→K′ este izomorfism de corpuri dacă şi numai dacă f este surjecție.

Propoziția 1.7. Fie K un corp comutativ cu car(K)=p (p≥2 număr prim). Atunci, pentru orice x, y∈K avem:

(i) px=0

(ii) $(xy)^p=x^py^p$

(iii) $(x\pm y)^p=x^p\pm y^p$ (semnele se corespund).

Demonstrație. (i). Avem px=p(1_Kx)=(p·1_K)x=0·x=0

(ii). Este evidentă deoarece xy=yx.

(iii). Cum p este prim p | C_p^k pentru orice 1≤k≤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 $(x-y)^2=x^2+y^2=x^2-y^2$. ■

Observația 1.8. Din propoziția precedentă deducem că funcția φ_p:K→K, $\varphi_p(x)=x^p$ este morfism de corpuri. Morfismul φ_p poartă numele de *morfismul lui Frobenius*.

§2.Construcția corpului ℂ al numerelor complexe

Scopul acestui paragraf este de a identifica corpul ℝ al numerelor reale cu un subcorp al unui corp comutativ ℂ în care ecuația $x^2 =-1$ are soluție.

Pentru aceasta vom considera ℂ=ℝ×ℝ iar pentru (x, y), (z, t)∈ℂ definim :

(x, y)+(z, t)=(x+z, y+t)

(x, y)·(z, t)=(xz-yt, xt+yz).

Teorema 2.1. (ℂ, +, ·) este corp comutativ în care ecuația $x^2=-1$ are soluție.

Demonstrație. Faptul că (ℂ, +) este grup abelian se probează imediat (elementul neutru este (0, 0), iar pentru (x, y)∈ℂ, -(x, y)= =(-x, -y)).

În mod evident înmulțirea este comutativă.

Pentru a proba că (ℂ*, ·) este grup, fie (x, y), (z, t), (r, s)∈ℂ. Deoarece (x, y)[(z, t)·(r, s)]=[(x, y)(z, t)]·(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)∈ℂ* (adică x≠0 sau y≠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)∈ℂ, (x, y)·[(z, t)+(r, s)]=(x, y)·(z, t)+(x, y)·(r, s)=(xz+xr-yt-ys, xt+xs+yz+yr) deducem că înmulțirea este distributivă față de adunare, adică (ℂ, +, ·) este corp comutativ.

Să notăm i=(0, 1). Cum i^2=(0, 1)(0, 1)=(-1, 0)=-(1, 0) deducem că ecuația x^2=-1 are soluție în $\mathbb{C}$. ■

Observația 2.2. 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 funcție injectivă). În felul acesta $\mathbb{R}$ poate fi privit ca subcorp al lui $\mathbb{C}$.

Deoarece pentru $z=(x, y)\in\mathbb{C}$ putem scrie z=(x, 0)+(y, 0)(0, 1), ținând cont de identificările anterioare deducem că z se poate scrie (formal) sub forma z=x+iy (cu i=(0, 1) iar i^2=-1).

Mulțimea $\mathbb{C}$ poartă numele de *mulțimea 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 părții 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).

Propoziția 2.3. Fie $z, z_1, z_2\in\mathbb{C}$. Atunci

(i) $z\in\mathbb{R} \Leftrightarrow z=\bar{z}$

(ii) $\bar{\bar{z}}=z$, $z\cdot\bar{z}=|z|^2$

(iii) $\overline{z_1\pm z_2}=\bar{z}_1\pm\bar{z}_2$, $\overline{z_1z_2}=\bar{z}_1\ \bar{z}_2$, $\overline{\left(\frac{z_1}{z_2}\right)}=\frac{\bar{z}_1}{\bar{z}_2}$ **(cu $z_2\neq0$)**

(iv) $|z|=|\bar{z}|$, $|z_1+z_2|\le|z_1|+|z_2|$, $|z_1\ z_2|=|z_1|\ |z_2|$, $\left|\frac{z_1}{z_2}\right|=\frac{|z_1|}{|z_2|}$ **(cu $z_2\neq0$).**

Demonstrație. (i). Fie z=a+ib. Dacă $z\in\mathbb{R}$, atunci b=0, deci $\bar{z}=a=z$ iar dacă $z=\bar{z}$ atunci b =-b adică b=0, deci $z\in\mathbb{R}$.

(ii). şi (iii). sunt evidente.

(iv). Să probăm doar inegalitatea $|z_1+z_2|\le|z_1|+|z_2|$ (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

$$|z_1+z_2|\le|z_1|+|z_2| \Leftrightarrow \sqrt{(x_1+x_2)^2+(y_1+y_2)^2} \le \sqrt{x_1^2+y_1^2}+\sqrt{x_2^2+y_2^2} \Leftrightarrow$$

$$x_1^2+x_2^2+2x_1x_2+y_1^2+y_2^2+2y_1y_2 \le x_1^2+y_1^2+x_2^2+y_2^2+$$

$$+2\sqrt{\left(x_1^2+y_1^2\right)\left(x_2^2+y_2^2\right)}$$

$$\Leftrightarrow (x_1x_2+y_1y_2)^2 \le \left(x_1^2+y_1^2\right)\left(x_2^2+y_2^2\right) \Leftrightarrow (x_1y_2-x_2y_1)^2 \ge 0$$ 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 2.4. 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 $M_2(\mathbb{R})$.

CURSUL nr. 11

§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, $c_0=a_0b_0$, $c_1=a_0b_1+a_1b_0$, ..., $c_n=a_0b_n+a_1b_{n-1}+...+a_{n-1}b_1+a_nb_0$, …

Propoziţia 1.1. $(A^{\mathbb{N}}, +,\cdot)$ este inel unitar comutativ.

Demonstraţie. 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 înmulţirii de pe $A^{\mathbb{N}}$ rezultă din comutativitatea înmulţirii de pe A. Pentru a proba asociativitatea înmulţirii 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 înmulţirea de pe $A^{\mathbb{N}}$. Deoarece înmulţirea de pe A este distributivă faţă 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 înmulţirea de pe $A^{\mathbb{N}}$ este distributivă faţă de adunarea de pe $A^{\mathbb{N}}$ şi cu aceasta propoziţia este demonstrată. ■

Observaţia 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:

$f= (a_0, a_1, ..., a_n, ...) = (a_0, 0, ...) + (0, a_1, 0, ...) + ... = (a_0, 0, ...) + +(a_1, 0, ...) (0, 1, 0,...) + (a_2, 0, ...) (0, 0, 1, 0, ...) +...+ (a_n, 0, ...) (\underbrace{0,0,...,0}_{nori}, 1, 0, ...) +... =(a_0, 0, ...) + (a_1, 0, ...) X + (a_2, 0, ...) X^2+...+ +(a_n, 0, ...) X^n+...= a_0+a_1X+...+a_nX^n+...$

Obținem astfel scrierea obişnuită a unei serii formale. Această observație ne permite să dăm următoarea definiție :

Definiția 1.3. Inelul $(A^{\mathbb{N}}, +, \cdot)$ se *numeşte inelul seriilor formale în nedeterminata X cu coeficienți 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 notație, fără sens de adunare).

Definiția 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 coeficienți în A.

Vom nota prin A[X] mulțimea polinoamelor cu coeficienți 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 $0\leq i\leq n$.

În particular, f=**0** dacă şi numai dacă $a_i=0$ pentru orice $0\leq i\leq n$ şi $f\neq 0$ dacă şi numai dacă există $0\leq i\leq n$ 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 $grad(f)=n\geq 1$, 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 $n\leq m$, 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) $grad (f+g)\leq max\{grad(f), grad(g)\}$
(ii) $grad (fg)\leq grad(f) + grad(g)$.

Demonstrație. Dacă f=g=**0** totul este clar. De asemenea, dacă de exemplu f=**0** şi g$\neq$ **0** (ținând cont de convențiile de calcul cu $\pm\infty$). Dacă f$\neq$**0** şi g$\neq$**0** inegalitățile de la (i) şi (ii) rezultă imediat din felul în care se efectuează f+g şi fg ■

Propoziția 1.10. Fie f=$a_0+a_1X+...+a_nX^n \in$A[X]. **Atunci**:

(i) f$\in$U(A[X]) $\Leftrightarrow$ $a_0\in$U(A) iar a_1, ..., $a_n\in$N(A) (reamintim că prin N(A) am notat mulțimea elementelor nilpotente din A)

(ii) f este divizor al lui zero în A[X] $\Leftrightarrow$ există a$\in A^*$ a.î. af=0.

Demonstrație. (i). "$\Rightarrow$". Dacă f$\in$**U**(A[X]), atunci există $g=b_0+b_1X+...+b_mX^m \in$A[X] a.î. fg=1 $\Leftrightarrow$

$$(*)\quad \begin{cases} a_0b_0 = 1 \\ a_0b_1 + a_1b_0 = 0 \\ a_0b_2 + a_1b_1 + a_2b_0 = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n-1}b_m + a_nb_{m-1} = 0 \\ a_nb_m = 0 \end{cases}$$

Din prima egalitate din (*) deducem că $a_0\in$**U**(A). Înmulțind ambii membrii ai penultimei egalități din (*) cu a_n şi ținând 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 $b_0\in$**U**(A)), adică $a_n\in$**N**(A). Atunci $a_nX^n \in$**N**(A[X]) şi cum f$\in$**U**(A[X]) deducem că $f_1=f-a_nX^n \in$**U**(A[X]). Cum $f_1=a_0+a_1X+...+a_{n-1}X^{n-1}$ deducem că $a_{n-1}\in$**N**(A). Raționând acum inductiv deducem că a_{n-2}, ..., a_2, $a_1 \in$**N**(A).

"$\Leftarrow$". Să presupunem că $a_0\in$**U**(A) (deci $a_0\in$U(A[X])) şi a_1, a_2, ..., $a_n\in$**N**(A). Atunci a_1, ..., $a_n\in$**N**(A[X]) şi cum **N**(A[X]) este ideal în A[X] deducem că a_1X, a_2X^2,…,$a_nX^n \in$**N**(A[X]) deci şi $a_1X+a_2X^2+...+a_nX^n\in$**N**(A[X]). Cum $a_0\in$**U**(A[X]) iar $f=a_0+(a_1X+...+a_nX^n)$ deducem că f$\in$**U**(A[X]) .

(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 minimalității lui m deducem că $g_1=$**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$\neq$ **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 $b_jf=$**0**. ■

Corola 1.11. Dacă A este domeniu de integritate atunci

(i) $f=a_0+a_1X+...+a_nX^n \in$U(A[X]) $\Leftrightarrow$ $a_1=a_2=...=a_n=0$ iar $a_0\in$U(A) (altfel zis, f$\in$U(A[X]) dacă şi numai dacă $f=a_0$, cu $a_0\in$U(A)).

(ii) A[X] este domeniu de integritate.

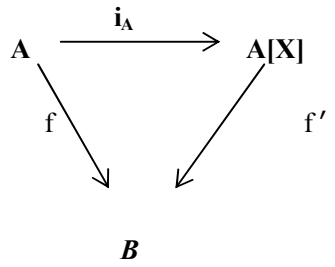
Demonstrație.(i). Rezultă imediat deoarece în cazul în care A este domeniu de integritate, **N**(A)={0}.

(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 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. ■

Aplicația i_A:A$\rightarrow$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 1.12. Pentru orice inel unitar, comutativ B, orice element b∈B şi orice morfism de inele f∈Hom(A, B), există un unic morfism de inele unitare f′∈Hom(A[X], B) a.î. f′(X)=b iar diagrama:



este comutativă (adică f′ ∘ i_A=f).

Demonstrație. 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 $m\le n$, 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 $c_i=\sum_{k=0}^{i}a_kb_{i-k}$ $(0\le i\le m+n)$ 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 $c_i=\sum_{k=0}^{i}a_kb_{i-k}$ 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∈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 1.13. 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∈A poartă numele de *funcția polinomială ataşată lui f.* Vom spune despre o funcție $g:A\to A$ că este *polinomială* dacă există f∈A[X] a.î. $g=\tilde{f}$.

Observația 1.14.

1. Dacă f, g ∈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≠ g.

3. Se probează imediat că dacă f, g ∈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 definește 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 $A[X_1]$ și 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 construiește 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 $A[X_1, ..., X_{n-2}]$, ș.a.m.d., deducem că f se scrie ca o sumă finită de forma

$$(*)\ f=\sum_{i_1,...,i_n=0}^{t_1,t_2,...,t_n} a_{i_1i_2...i_n} X_1^{i_1}...X_n^{i_n}$$ (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 și 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 numește *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 $A[X_1, ..., X_n]$.

$$f=\sum_{i_1,...,i_n=0}^{t_1,...,t_n} a_{i_1...i_n} X_1^{i_1}...X_n^{i_n}\ .$$

Monoamele nenule din scrierea lui f se numesc *termenii* lui f.

Gradul lui f se definește astfel:

$$grad(f) = \begin{cases} -\infty\ , \text{ dacă } f=\mathbf{0} \\ \text{maximul gradelor termenilor săi, dacă } f \neq \mathbf{0}. \end{cases}$$

Astfel, dacă $f=2X_1^2-3X_1X_2^2+4X_1X_2X_3 \in \mathbb{Z}[X_1, X_2, X_3]$, atunci

$grad(f)=\max\{2, 1+2, 1+1+1\} = \max\{2, 3, 3\}=3$.

Observăm deci că în cadrul unui polinom f de mai multe variabile pot să apară termeni diferiți (în cazul exemplului nostru fiind monoamele $-3X_1X_2^2$ și $4X_1X_2X_3$) care însă să aibă același 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 $n \geq 2$, $M_1=aX_1^{i_1}...X_n^{i_n}$,

$M_2=bX_1^{j_1}...X_n^{j_n} \in A[X_1, ..., X_n]$ cu a, $b \in A^*$, atunci definim $M_1 \le M_2 \Leftrightarrow \Leftrightarrow (i_1, ... ,i_n) \le (j_1, ..., j_n)$ (în ordonarea lexicografică de pe $\mathbb{N}^n$!).

Astfel, $M_1 \le M_2 \Leftrightarrow$ există $1 \le k \le n$ a.î. $i_1=i_2,...,i_k=j_k$ şi $i_{k+1}<j_{k+1}$.

De exemplu, în $\mathbb{Z}[X_1, X_2, X_3]$: $2X_1^2X_2^3X_3^4 \le -4X_1^2X_2^3X_3^5$, $X_1 \le X_1X_2X_3$.

În general, având un polinom nenul $f \in A[X_1, ..., X_n]$, cum acesta se poate scrie ca sumă finită de monoame nenule din $A[X_1, ..., X_n]$, cu ajutorul ordonării lexicografice de pe $A[X_1, ..., X_n]$ 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 $grad(fg)=grad(f)+grad(g)$.

Demonstraţie. Vom face inducţie matematică după n, pentru n=1 totul fiind clar dacă ţinem 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.

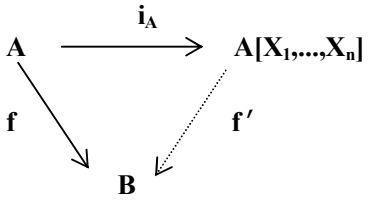
Fie acum f, g polinoame nenule din $A[X_1, ..., X_n]$ de grad m şi respectiv n. Atunci scriem pe f şi g sub forma $f=f_0+f_1+...+f_m$, $g=g_0+g_1+...+g_n$ cu $f_m \neq 0$, $g_n \neq 0$ iar f_i, g_i sunt sau nule sau polinoame omogene de grad i, respectiv j, $0 \le i \le m-1$, $0 \le j \le n-1$. Avem $fg=\sum_{k=0}^{m+n} h_k$ cu $h_k=\sum_{i+j=k} f_i g_j$ $(0 \le k \le m+n)$. Cum $A[X_1, ..., X_n]$ este domeniu de integritate avem $h_{m+n}=f_mg_n$, de unde relaţia $grad(fg)=grad(f)+grad(g)$. ■

Funcţia $i_A:A \to A[X_1, ..., X_n]$ 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 notaţia, 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.

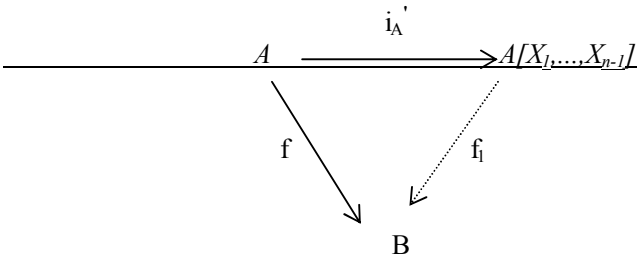
Teorema 2.9. Fie $n\in\mathbb{N}$, $n\geq 2$, B un inel unitar comutativ, $f:A\to B$ un morfism de inele unitare şi $b_1, ..., b_n\in B$. Atunci există un unic morfism de inele unitare $f' : A[X_1, ..., X_n] \to B$ a.î. $f'(X_i)=b_i$ pentru orice $1\leq i\leq n$ iar diagrama



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

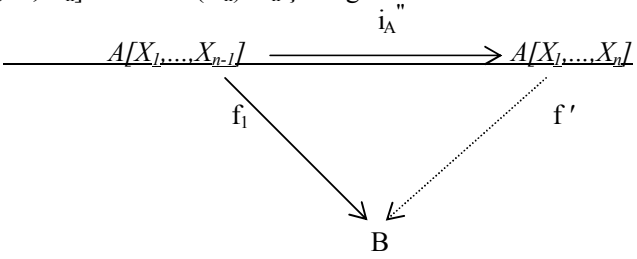
Demonstraţie. Facem inducţie matematică după n (pentru n=1 rezultatul fiind adevărat conform Teoremei 1).

Să presupunem acum afirmaţia din enunţ 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. $f_1(X_i)=b_i$, $1\leq i\leq n-1$ şi diagrama



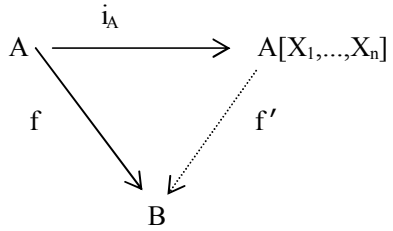
este comutativă, adică $f_1\circ i_A'=f$ (i_A' fiind morfismul canonic de la A la $A[X_1,...,X_{n-1}]$).

Cum $A[X_1,...,X_n]=A[X_1,...,X_{n-1}][X_n]$, conform Teoremei 1 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 obţinem din cele două diagrame comutative de mai înainte diagrama comutativă

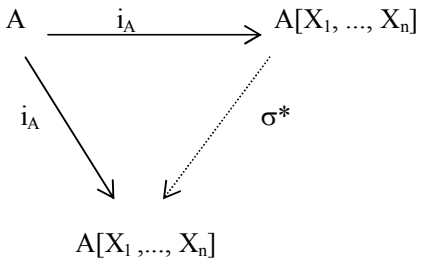


În mod evident $f'(X_i)=b_i$ pentru orice $1\le i\le n$. Unicitatea lui f' rezultă din unicitatea lui f_1 şi a faptului că $f'\circ i_A''=f_1$.

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 $f\in A[X_1, ..., X_n]$, $f=\sum_{i_1,i_2,...,i_n=0}^{t_1,t_2,...,t_n} a_{i_1i_2...i_n}X_1^{i_1}...X_n^{i_n}$, atunci

$$\sigma^*(f)=\sum_{i_1,i_2,...,i_n=0}^{t_1,t_2,...,t_n} a_{i_1i_2...i_n}X_{\sigma(1)}^{i_1}...X_{\sigma(n)}^{i_n}.$$

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 $\sigma^*(f)=X_3^2-2X_3X_1-X_1X_2^2$.

Observaţia 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 $e^*=1_{A[x_1,...,x_n]}$.

3. Dacă $\sigma\in S_n$, atunci $\sigma^*:A[X_1, ..., X_n]\to A[X_1, ..., X_n]$ este izomorfism de inele unitare (ţinând cont de prima parte a acestei observaţii deducem că inversul lui σ^* este $(\sigma^{-1})^*$).

Definiţia 3.2. Vom spune că un polinom $f\in A[X_1, ..., X_n]$ ($n\ge 2$) 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 transpoziţii, atunci un polinom din $A[X_1, ..., X_n]$ este simetric dacă şi numai dacă f rămâne invariant la orice transpoziţie din S_n. Vom nota prin $\mathbf{S}(A[X_1, ..., X_n])$ mulţimea polinoamelor simetrice din $A[X_1, ..., X_n]$.

Propoziţia 3.3. $\mathbf{S}(A[X_1, ..., X_n])$ este subinel unitar al inelului $A[X_1, ..., X_n]$.

Demonstraţie. În mod evident, polinoamele constante din $A[X_1, ..., X_n]$ (deci şi **1**) fac parte din $\mathbf{S}(A[X_1, ..., X_n])$ iar dacă $f, g\in\mathbf{S}(A[X_1, ..., X_n])$ 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 $f-g, fg\in\mathbf{S}(A[X_1, ..., X_n])$, adică $\mathbf{S}(A[X_1, ..., X_n])$ este subinel unitar al lui $A[X_1, ..., X_n]$.

Observaţia 3.4. După cum am văzut în paragraful precedent, orice polinom $f\in A[X_1, ..., X_n]$ se scrie în mod unic sub forma $f=f_0+f_1+...+f_k$ unde fiecare f_i este un polinom omogen de grad i ($0\le i\le k$)

din $A[X_1, ..., X_n]$. Astfel, dacă $\sigma \in S_n$, atunci $\sigma^*(f)=\sigma^*(f_0+f_1+...+f_k)=\sigma^*(f_0)+\sigma^*(f_1)+...+\sigma^*(f_k)$. 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 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 $\sigma^*(\mathbf{S_i})=\mathbf{S_i}$ pentru orice $1 \le i \le n$, adică $\mathbf{S_i} \in \mathbf{S}(A[X_1, ..., X_n])$ pentru orice $1 \le i \le n$. ■

Definiţia 3.6. Polinoamele $\mathbf{S_1, S_2, ..., S_n}$ poartă numele de *polinoamele simetrice fundamentale* din $\mathbf{A[X_1, ..., X_n]}$.

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).

Propoziţia 3.7. Fie $f \in \mathbf{S}(A[X_1, ... ,X_n])$ şi să presupunem că $t_p(f)=aX_1^{i_1}X_2^{i_2}...X_n^{i_n}$ cu $a \in \mathbf{A^*}$. Atunci cu necesitate $i_1 \ge i_2 \ge ... \ge i_n$.

Demonstraţie. 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. Contradicţia provine din aceea că, relativ la ordonarea lexicografică, $t_p(f) < M$ - absurd. ■

Observaţia 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} posibilităţi 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 de mai sus putem presupune că f este şi omogen; fie grad(f)=m. Dacă $t_p(f)=aX_1^{i_1}...X_n^{i_n}$, atunci avem că $i_1\geq i_2\geq ...\geq i_n$. Ținând cont de faptul că pentru orice $1\leq i\leq n$, $t_p(\mathbf{S_i})=X_1X_2...X_i$ 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

$g=aX_1^{i_1-i_2}X_2^{i_2-i_3}...X_{n-1}^{i_{n-1}-i_n}X_n^{i_n}+bX_1^{j_1-j_2}X_2^{j_2-j_3}...$

$....X_{n-1}^{j_{n-1}-j_n}X_n^{j_n}+\ldots\in A[X_1,...,X_n]$ 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 $grad(t_p)=\sum_{k=1}^{n}j_k=\sum_{k=1}^{n}ki_k$.

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 obţinem $1= -27+36+b$, de unde $b = -8$.

Deci $f = - \mathbf{S_1}^3+4\mathbf{S_1S_2}-8\mathbf{S_3}$, 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 aplicaţie la Teorema fundamentală a polinoamelor simetrice (Teorema 3.9.) vom arăta cum se exprimă în funcţie de polinoamele simetrice fundamentale $S_1, ..., S_n$, polinoamele $P_k= X_1^k +...+ X_n^k$ $(k\in\mathbb{N})$.

§4.Rădăcini ale polinoamelor cu coeficienţi într-un corp. Teorema fundamentală a algebrei. Polinoame ireductibile. Rezolvarea ecuaţiilor 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.

Definiţia 4.1. Fie k un corp, K o extindere a sa şi $M \subseteq K$ o submulţime oarecare. Intersecţia tuturor subcorpurilor lui K ce conţin $k\cup M$ se notează prin k(M) şi se spune că este corpul obţinut prin *adjuncţionarea* 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 submulţime 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 funcţia 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, aparţine lui k, vom spune despre k că este *algebric închis*.

Teorema 4.2. (*Teorema împărţirii 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 $grad(r)<grad(g)$.

Demonstraţie. 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 existenţa polinoamelor q şi r prin inducţie matematică după gradul lui f (adică după n).

Dacă $grad(g) > n$, putem alege $q=0$ şi $r=f$.

Dacă $grad(g) \leq n$, considerăm polinomul $f_1=f-b_m^{-1}a_nX^{n-m}g$. Cum $grad(f_1)<n$, conform ipotezei de inducţie există $q_1, r_1\in K[X]$ a.î. $f_1=gq_1+r_1$ cu $grad(r_1)<grad(g)$. Obţinem $f-b_m^{-1} a_n X^{n-m} g =gq_1+r_1$, 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 inducţiei matematice partea de existenţă 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 **g | f**.

Un polinom f∈A[X] care nu este ireductibil în A[X] se va zice *reductibil* în A[X].

Propoziția 4.4. (*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 $f=a_0+a_1X+...+a_nX^n \in A[X]$ şi să presupunem că $\widetilde{f}(a)=0 \Leftrightarrow a_0+a_1a+...+a_na^n=0$. 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 $k\in\mathbb{N}$, $X^k-a^k=(X-a)(X^{k-1}+aX^{k-2}+...+a^{k-2}X+a^{k-1})$ (adică $X-a \mid X^k-a^k$) 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

$\widetilde{f}=\widetilde{(x-a)}\,\widetilde{g}$ deducem că $\widetilde{f}(a)=(a-a)\,\widetilde{g}(a)=0\cdot\widetilde{g}(a)=0$. ■

Observația 4.5. 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 $f=(1+X^2)(1+X^4)\in\mathbb{Z}[X]$ care deşi este reductibil în $\mathbb{Z}[X]$ nu are nici o rădăcină în $\mathbb{Z}$. 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 4.6. Fie f∈A[X], f≠0 şi a∈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 4.7. Fie A un domeniu de integritate.

(i) Dacă a∈A este rădăcină multiplă pentru polinoamele nenule f, g∈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∈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∈A[X].

Demonstrație. (i). Putem scrie $f=(X-a)^if_1$ şi $g=(X-a)^jg_1$ cu $f_1, g_1\in A[X]$ iar $\widetilde{f_1}(a)\neq 0$, $\widetilde{g_1}(a)\neq 0$. Atunci $fg=(X-a)^if_1\,(X-a)^jg_1=(X-a)^{i+j}f_1g_1$

şi $\widetilde{f_1g_1}(a)=\widetilde{f_1}(a)\,\widetilde{g_1}(a)\neq 0$ (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 . 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 $f=(X-a_1)^{i_1}...(X-a_k)^{i_k} g$. ■

Propoziția 4.8. (*Relațiile lui Viète*) Fie A un domeniu de integritate şi $f\in A[X]$ un polinom de grad n, $f=a_0+a_1X+...+a_nX^n$ (deci $a_n\neq 0$). Dacă $x_1, ..., x_n$ sunt rădăcinile lui f în A, atunci

$$a_n(x_1+...+x_n)=-a_{n-1}$$
$$a_n(x_1x_2+x_1x_3+...+x_{n-1}x_n)=a_{n-2}$$
$$.....$$
$$a_n(x_1x_2...x_k+x_1x_2...x_{k-1}x_{k+1}+...+x_{n-k+1}x_{n-k+2}...x_n)=(-1)^k a_{n-k}$$
$$.....$$
$$a_n(x_1...x_n)=(-1)^n a_0.$$

Demonstrație. 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 $f=a_n(X-x_1)...(X-x_n)=$
$=a_nX^n-a_n(x_1+...+x_n)X^{n-1}+a_n(x_1x_2+x_1x_3+...+x_{n-1}x_n)X^{n-2}+...+(-1)^k a_n(x_1...x_k+$
$+x_1...x_{k-1}x_{k+1}+...+x_{n-k+1}x_{n-k+2}...x_n)X^{n-k}+...+(-1)^n a_n x_1...x_n.$
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 4.9. Dacă A este corp comutativ, atunci relațiile dintre rădăcinile şi coeficienții lui f devin:

$$\begin{cases} x_1+...+x_n=-a_{n-1}a_n^{-1} \\ x_1x_2+x_1x_3+...+x_{n-1}x_n=a_{n-2}a_n^{-1} \\ ..... \\ x_1x_2...x_k+x_1x_2...x_{k-1}x_{k+1}+...+x_{n-k+1}x_{n-k+2}...x_n=(-1)^k a_{n-k}a_n^{-1} \\ ..... \\ x_1x_2...x_n=(-1)^n a_0 a_n^{-1} \end{cases}$$

Corolar 4.10. (*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, avem că pentru orice $\hat{x}\in\mathbb{Z}_p^*$, $\hat{x}^{p-1}=\hat{1}$ şi rădăcinile lui f sunt $\hat{1}$, $\hat{2}$, ..., $\overset{\wedge}{p-1}$.

Conform ultimei relații a lui Viète avem $\hat{1}\,\hat{2}.....\overset{\wedge}{p-1}=(-1)^{p-1}(-\hat{1}) \Leftrightarrow \overset{\wedge}{(p-1)!}+1=\hat{0} \Leftrightarrow (p-1)!+1\equiv 0\ (p)$.
■

Suntem acum în măsură să prezentăm un rezultat deosebit de important în algebră cunoscut sub numele de *teorema fundamentală a algebrei* :

Teorema 4.11. (*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 $\bar{f} = \bar{a}_0 + \bar{a}_1 X+...+\bar{a}_n X^n$ (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.

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 $z_{ij}^{\,a} = x_ix_j+a(x_i+x_j)$, $1\leq i<j\leq m$.

Dacă vom considera polinomul

$g_a= \prod_{1\leq i<j\leq m} (X - z_{ij}^{\,a})$, atunci $grad(g_a)= C_m^2 = \frac{m(m-1)}{2}$ şi cum $m=grad(f)=2^k r$ (cu k, $r\in\mathbb{N}$, r impar)

avem că grad $(g_a)= \frac{2^k r(2^k r-1)}{2} = =2^{k-1} r\,(2^k r-1)=2^{k-1}\,r'$ unde $r'=r\,(2^k r-1)$ 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 $z_{ij}^{\,a}$, $1\leq i<j\leq m$ 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 $(1\leq i<j\leq m)$. 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 $1\leq i<j\leq m$ 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 $1\leq i<j\leq m$ 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. ■

Observație. 1. 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 $\widetilde{f}(\bar{\alpha})=0$, 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 observația de mai înainte deducem că problema ireductibilității 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:*

Propoziție 4.12. 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 $\mathbb{Z}[X]$.

Demonstrație. 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 coeficienții lui f deducem că

$$(*)\quad \begin{cases} a_0 = b_0c_0 \\ a_1 = b_0c_1 + b_1c_0 \\ a_2 = b_0c_2 + b_1c_1 + b_2c_0 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n-1} = b_{m-1}c_k + b_mc_{k-1} \\ a_n = b_mc_k \end{cases}$$

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 ținem cont de relațiile (*) deducem din aproape în aproape că $p \mid b_1$, $p \mid b_2$, ..., $p \mid b_{m-1}$ şi din ultima relație 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 relație din (*) am deduce că $p \mid a_n$ -absurd. ■

Observația 4.13. 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 ecuațiilor algebrice de grade 3 şi 4 cu coeficienți din $\mathbb{C}$ (adică a ecuațiilor de forma $\widetilde{f}(x)=0$ cu $f\in\mathbb{C}[X]$ iar $grad(f)=3$ sau 4).

1. Să considerăm la început ecuația algebrică de grad 3 cu coeficienți din $\mathbb{C}$ scrisă sub forma

(1) $x^3+ax^2+bx+c=0$ cu $a\in\mathbb{C}$.

Dacă în (1) înlocuim $y=x+\frac{a}{3}$ obținem o ecuație algebrică în y de forma:

(2) $y^3+py+q=0$ 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 ecuației

(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 ε_0, ε_1, ε_2 sunt rădăcinile ecuației $x^3-1=0$.

Cum rădăcinile ecuației $x^3-1=0$ sunt 1 şi ε, ε^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.

CURSUL nr. 12

DETERMINANȚI.SISTEME DE ECUAȚII LINIARE.

§1. Definiția unui determinant de ordin n. Proprietățile determinanților. Dezvoltarea unui determinant după elementele unei linii. Regula lui Laplace.

În cadrul acestui paragraf prin A vom desemna un inel comutativ şi unitar.

Definiția 1.1. Dacă $n\in\mathbb{N}$, $n\geq 1$ şi $M=(a_{ij})_{1\leq i,j\leq n}\in \mathbf{M_n(A)}$, atunci prin *determinantul matricei M* notat det(M) înțelegem elementul

$$\mathbf{det(M)}=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}\ldots a_{n\sigma(n)}\in\mathbf{A}$$

(unde prin S_n am notat mulțimea permutărilor asupra mulțimii {1, 2, …, n} iar pentru $\sigma\in S_n$, sgn(σ) reprezintă *signatura* permutării σ).

Convenim să notăm $\mathbf{det}(M)=\begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n}\\ a_{21} & a_{22} & \ldots & a_{2n}\\ \ldots & \ldots & \ldots & \ldots\\ a_{n1} & a_{n2} & \ldots & a_{nn}\end{vmatrix}$ (sau condensat, $\mathbf{det}(M)=|a_{ij}|_{1\leq i,j\leq n}$).

Asociind la fiecare $M\in\mathbf{M_n}(A)$ elementul $\mathbf{det}(M)\in A$, obținem o funcție $\mathbf{det}:\mathbf{M_n}(A)\to A$ numită *funcția determinant*.

De exemplu, dacă n=2 şi $M=\begin{pmatrix} a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}$, atunci $\mathbf{det}(M)=a_{11}a_{22}-a_{12}a_{21}$ iar dacă n=3 şi $M=\begin{pmatrix} a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{pmatrix}$, atunci:

$$\mathbf{det}(M)=a_{11}a_{22}a_{33}+a_{12}a_{23}a_{31}+a_{13}a_{21}a_{32}-a_{13}a_{22}a_{31}-a_{12}a_{21}a_{33}-a_{11}a_{23}a_{32}.$$

Produsul $a_{1\sigma(1)}a_{2\sigma(2)}\ldots a_{n\sigma(n)}$ poartă numele de *termen* al lui **det**(M). Astfel, **det**(M) este suma a n! termeni dintre care $\frac{n!}{2}$ apar în **det**(M) cu semnul (+) iar $\frac{n!}{2}$ cu semnul (-).

Dacă n=1, adică $M=(a_{11})$ convenim să definim $\mathbf{det}(M)=a_{11}$.

În cele ce urmează vom pune în evidență principalele proprietăți ale determinanților.

Propoziția 1.2. Pentru orice $M\in\mathbf{M_n}(A)$, $\mathbf{det}({}^tM)=\mathbf{det}(M)$ (unde prin ${}^tM$ am notat transpusa matricei M).

Demonstrație. Fie $M=(a_{ij})_{1\leq i,j\leq n}$ şi ${}^tM=({}^ta_{ij})_{1\leq i,j\leq n}$ unde prin ${}^ta_{ij}$ am notat elementul a_{ji}.

Avem $\mathbf{det}({}^tM)=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\,{}^ta_{1\sigma(1)}{}^ta_{2\sigma(2)}\ldots{}^ta_{n\sigma(n)}=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{\sigma(1)1}a_{\sigma(2)2}\ldots a_{\sigma(n)n}=$

$=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{\sigma(1)\sigma^{-1}(\sigma(1))}a_{\sigma(2)\sigma^{-1}(\sigma(2))}\ldots a_{\sigma(n)\sigma^{-1}(\sigma(n))}=\sum_{\sigma^{-1}\in S_n}\operatorname{sgn}(\sigma^{-1})a_{1\sigma^{-1}(1)}a_{2\sigma^{-1}(2)}\ldots a_{n\sigma^{-1}(n)}=\mathbf{det}(M)$ (deoarece atunci când σ parcurge S_n şi σ^{-1} parcurge bijectiv pe S_n iar $\operatorname{sgn}(\sigma^{-1})=\operatorname{sgn}(\sigma)$). ■

Observația 1.3. Egalitatea $\mathbf{det}({}^tM)=\mathbf{det}(M)$ ne arată că ori de cîte ori avem o proprietate adevărată referitoare la liniile unui determinant, aceeaşi proprietate este adevărată şi pentru coloanele determinantului. Din această cauză în continuare vom prezenta principalele proprietăți ale determinanților referitoare la linii, rezultând tacit că acestea sunt adevărate şi pentru coloane.

Propoziția 1.4. (i) Dacă toate elementele unei linii dintr-o matrice sunt nule, atunci determinantul matricei este nul

(ii) Dacă într-o matrice schimbăm două linii între ele, matricea astfel obținută are determinantul egal cu opusul determinantului matricei inițiale.

(iii) Dacă o matrice are două linii identice, atunci determinatul său este nul

(iv) Dacă toate elementele unei linii a unei matrice conțin factor comun un element $a\in A$, atunci acel element poate fi scos în fața determinantului matricei

(v) Dacă elementele a două linii ale unei matrice sunt proporționale, atunci determinantul său este nul.

Demonstrație. (i). Dacă de exemplu, toate elementele de pe linia i a matricei M sunt egale cu 0, atunci cum fiecare termen al determinantului conține ca factor şi un element al liniei i deducem că **det**(M)=0.

(ii). Fie M_{ij} matricea ce se obține din matricea $M=(a_{ij})_{1\le i,j\le n}$ schimbând între ele liniile i şi j.

Avem $\mathbf{det}(M_{ij})=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}...a_{j\sigma(i)}...a_{i\sigma(j)}...a_{n\sigma(n)}$

Dacă considerăm transpoziția ε=(i j) (ce duce pe i în j, pe j în i şi lasă pe loc restul elementelor din {1, 2, …, n}) atunci putem scrie $\mathbf{det}(M_{ij})=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{1(\sigma\circ\varepsilon)(1)}a_{2(\sigma\circ\varepsilon)(2)}...a_{n(\sigma\circ\varepsilon)(n)}=-\sum_{\tau\in S_n}\operatorname{sgn}(\tau)a_{1\tau(1)}a_{2\tau(2)}...a_{n\tau(n)}=-\mathbf{det}(M)$ (deoarece atunci când σ parcurge pe S_n, σ∘ε=τ parcurge bijectiv pe S_n iar sgn(τ)=sgn(σ)·sgn(ε)=-sgn(σ)).

(iii). Dacă matricea M are identice liniile i şi j, atunci schimbând între ele aceste linii trebuie după ii) ca **det**(M)=-**det**(M), de unde deducem că **det**(M)=0 (evident în ipoteza că inelul A nu este de caracteristică 2).

(iv). Fie $M=(a_{ij})_{1\le i,j\le n}$ iar M′ matricea ce diferă de M prin aceea că în locul liniei $(a_{i1}, a_{i2}, …, a_{in})$ are linia $(aa_{i1}, aa_{i2}, …, aa_{in})$. Atunci $\mathbf{det}(M')=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}...(aa_{i\sigma(i)})..a_{n\sigma(n)}=a\cdot\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}...a_{n\sigma(n)}==a\cdot\mathbf{det}(M)$.

(v). Rezultă imediat din (iv) şi (iii). ■

Fie acum $M=(a_{ij})_{1\le i,j\le n}\in\mathbf{M_n}(A)$ şi să presupunem că elementele liniei i se scriu sub forma $a_{ij}=a_{ij}'+a_{ij}''$ pentru fiecare $1\le j\le n$.

Dacă notăm cu M′ (respectiv M″) matricea care se obține din M înlocuind elementele de pe linia i cu elementele (a_{ij}') (respectiv (a_{ij}'')) $(1\le j\le n)$ atunci avem următorul rezultat:

Propoziția 1.5. det(M)=det(M′)+det(M″).

Demonstrație. Avem $\mathbf{det}(M)=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}...a_{i\sigma(i)}...a_{n\sigma(n)}=$

$=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}...(a'_{i\sigma(i)}+a''_{i\sigma(i)})..a_{n\sigma(n)}=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}...a'_{i\sigma(i)}...a_{n\sigma(n)}+$

$+\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}....a''_{i\sigma(i)}..a_{n\sigma(n)}=\mathbf{det}(M')+\mathbf{det}(M'')$. ■

Corolar 1.6. (i) Dacă o linie a unei matrice pătratice este o combinație liniară de celelalte linii, atunci determinantul matricei este nul.

(ii) Dacă la o linie a unei matrice pătratice adăugăm o combinație liniară de alte linii, determinantul matricei nu se schimbă.

Observația 1.7. Sintetizând proprietățile de mai sus ale determinanților avem următoarele proprietăți principale ale determinanților:

Proprietatea 1: Dacă într-un determinant schimbăm liniile cu coloanele, determinantul nu-şi modifică valoarea.

Proprietatea 2: Dacă toate elementele unei linii a unui determinant sunt nule, atunci şi determinantul este nul.

Proprietatea 3: Dacă într-un determinant schimbăm două linii între ele, determinantul îşi schimbă doar semnul.

Proprietatea 4: Într-un determinant factorii comuni se scot pe linii.

Proprietatea 5: Dacă într-un determinant două linii sunt proporționale, atunci determinantul este nul.

Proprietatea 6: Dacă toate elementele unei linii a unui determinant se scriu ca sumă de două elemente atunci şi determinantul se scrie ca sumă de doi determinanți.

Proprietatea 7: Dacă o linie a unui determinant este o combinație liniară de celelelte linii, atunci determinantul este nul.

Proprietatea 8: Dacă într-un determinant la o linie adăugăm o combinație liniară de alte linii, atunci determinantul nu-şi schimbă valoarea.

Observația 1.8. În cazul determinanților de ordinul 3 există două reguli simple de calcul a acestora cunoscute sub numele de *regula lui Sarrus* şi respectiv *regula triunghiului*.

Pentru *regula lui Sarrus* se procedează astfel:

Dacă $M=\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ atunci adăugând primele două linii la M obținem matricea de ordinul (5, 3):

$$M'=\begin{pmatrix} a_{11} & & a_{12} & & a_{13} \\ & \ddots & & & \\ a_{21} & & a_{22} & & a_{23} \\ & \ddots & & \ddots & \\ a_{31} & & a_{32} & & a_{33} \\ & \ddots & & \ddots & \\ a_{11} & & a_{12} & & a_{13} \\ & & & \ddots & \\ a_{21} & & a_{22} & & a_{23} \end{pmatrix}.$$

Termenii cu (+) din dezvoltarea lui **det**(M) sunt cei ce se obțin înmulțind elementele de pe diagonala principală a lui M şi cele ale „diagonalelor paralele" cu aceasta din M′ iar cei cu (-) se obțin înmulțind elementele de pe diagonala secundară lui M şi cele ale „diagonalelor paralele" cu aceasta din M′. De exemplu, dacă

$$M=\begin{pmatrix} 1 & 2 & -3 \\ -2 & 1 & 1 \\ 2 & -1 & 4 \end{pmatrix}$$ atunci

$$M'=\begin{pmatrix} 1 & & 2 & & -3 \\ & \ddots & & & \\ -2 & & 1 & & 1 \\ & \ddots & & \ddots & \\ 2 & & -1 & & 4 \\ & \ddots & & \ddots & \\ 1 & & 2 & & -3 \\ & \ddots & & \ddots & \\ -2 & & 1 & & 1 \end{pmatrix}$$ şi astfel

det(M)=1·1·4+(-2)·(-1)·(-3)+2·2·1-(-3)·1·2-1·(-1)·1-4·2·(-2)=4-6+4+ +6+1+16 = 25.

Pentru *regula triunghiului* se procedează astfel:

Se consideră $M=\begin{pmatrix} a_{11} & & a_{12} & & a_{13} \\ & \ddots & & \iddots & \\ a_{21} & & a_{22} & & a_{23} \\ & \iddots & & \ddots & \\ a_{31} & & a_{32} & & a_{33} \end{pmatrix}$ şi se observă că tripletele (a_{13}, a_{21}, a_{32}) şi (a_{31}, a_{12}, a_{23}) formează două „triunghiuri" cu vârfurile în a_{13} şi respectiv a_{31} şi cu bazele „paralele" cu diagonala principală, astfel că termenii din dezvoltarea lui det(M) ce apar cu semnul plus pot fi individualizați astfel: produsul elementelor de pe diagonala principală precum şi produsele celor două triplete ce formează două triunghiuri cu bazele paralele cu diagonala principală. Cele cu semnul minus vor fi:

produsul elementelor de pe diagonala secundară precum şi cele două produse ale tripletelor (a_{11}, a_{32}, a_{23}) şi (a_{33}, a_{21}, a_{12}) ce formează două triunghiuri cu vârfurile în a_{11} şi respectiv a_{33} şi cu bazele „paralele" cu diagonala secundară.

În continuare vom prezenta un procedeu recursiv de calcul al unui determinant de ordinul n prin care calculul acestuia se reduce la calculul a n determinanţi de ordinul n-1.

Fie deci $M=(a_{ij})_{1\le i,j\le n}\in\mathbf{M_n}(A)$ $(n\ge 2)$ şi $d=\mathbf{det}(M)=|a_{ij}|_{1\le i,j\le n}$.

Definiţia 1.9. Numim *minor complementar* al elementului a_{ij} în det(M) elementul notat d_{ij} ce se obţine calculând determinantul de ordinul n-1 obţinut prin eliminarea din det(M) a liniei i şi coloanei j $(1\le i, j\le n)$.

Elementul $\delta_{ij}=(-1)^{i+j}d_{ij}$ se numeşte *complementul algebric* al lui a_{ij} în det(M).

Teorema 1.10. Dacă $M=(a_{ij})_{1\le i,j\le n}\in\mathbf{M_n}(A)$, atunci pentru orice $1\le i\le n$ avem egalitatea:

$$\mathbf{det(M)= a_{i1}\delta_{i1}+a_{i2}\delta_{i2}+\ldots+a_{in}\delta_{in}.}$$

Demonstraţie. Avem $\mathbf{det}(M)=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\, a_{1\sigma(1)}a_{2\sigma(2)}\ldots a_{n\sigma(n)}$ şi să notăm pentru $1\le i\le n$, $s_i=a_{i1}\delta_{i1}+a_{i2}\delta_{i2}+\ldots+a_{in}\delta_{in}$.

Ideea de demonstraţie a egalităţii $\mathbf{det}(M)=s_i$ este următoarea: vom arăta că fiecare termen de forma $a_{ij}\delta_{ij}$ al sumei s_i este suma a (n-1)! termeni din dezvoltarea lui **det**(M) având acelaşi semn ca şi cei din dezvoltarea lui **det**(M) iar pentru două valori diferite ale indicelui j avem termeni diferiţi din dezvoltarea lui **det**(M). O dată stabilit lucrul acesta, egalitatea $\mathbf{det}(M)=s_i$ se probează astfel: suma s_i are $n\cdot(n-1)!=n!$ termeni identici şi cu acelaşi semn ca şi termenii ce ne dau dezvoltarea lui **det**(M), deci cu necesitate $\mathbf{det}(M)=s_i$.

Să ne ocupăm la început de termenul $a_{11}\delta_{11}$.

Avem $a_{11}\delta_{11}=a_{11}\sum_{\tau}\operatorname{sgn}(\tau)a_{2\tau(2)}a_{3\tau(3)}\ldots a_{n\tau(n)}=\sum_{\tau}\operatorname{sgn}(\tau)a_{11}a_{2\tau(2)}a_{3\tau(3)}\ldots a_{n\tau(n)}$

(sumarea făcându-se după toate permutările τ asupra mulţimii $\{2, 3, \ldots, n\}$). Se observă că cei (n-1)! termeni ce apar în dezvoltarea lui $a_{11}\delta_{11}$ sunt termeni ce apar şi în dezvoltarea lui **det**(M).

Să arătăm că aceştia apar cu acelaşi semn ca şi în dezvoltarea lui **det**(M). Pentru o permutare τ asupra mulţimii $\{2, 3, \ldots, n\}$ semnul termenului $a_{2\tau(2)}a_{3\tau(3)}\ldots a_{n\tau(n)}$ din dezvoltarea lui δ_{11} este $\operatorname{sgn}(\tau)$, deci semnul termenului $a_{11}a_{2\tau(2)}a_{3\tau(3)}\ldots a_{n\tau(n)}$ provenit din produsul $a_{11}\delta_{11}$ este egal cu $\operatorname{sgn}(\tau)$.

Pe de altă parte, semnul termenului $a_{11}a_{2\tau(2)}a_{3\tau(3)}\ldots a_{n\tau(n)}$ în dezvoltarea lui **det**(M) este egal cu $\operatorname{sgn}(\tau')$ unde $\tau'=\begin{pmatrix}1 & 2 & 3 & \ldots & n\\ 1 & \tau(2) & \tau(3) & \ldots & \tau(n)\end{pmatrix}$ şi avem în mod evident $\operatorname{sgn}(\tau)=\operatorname{sgn}(\tau')$.

Pentru cazul general al produsului $a_{ij}\delta_{ij}$ procedăm astfel: schimbăm liniile şi coloanele în aşa fel încît elementul a_{ij} să vină în locul elementului a_{11} şi minorul d_{ij} să rămînă neschimbat. În felul acesta linia i şi coloana j devin linia 1 şi respectiv coloana 1; linia 1 devine linia 2, linia 2 devine linia 3, …, linia i-1 devine linia i; coloana 1 devine coloana 2, coloana 2 devine coloana 3,…, coloana j-1 devine coloana j, astfel că dacă notăm prin d' determinantul obţinut prin astfel de schimbări avem $\mathbf{det}(M)=(-1)^{i+j}d'$ şi în plus $d'_{11}=d_{ij}$.

Dacă $a_{1k_1}a_{2k_2}\ldots a_{i-1\ k_{i-1}}a_{i+1\ k_{i+1}}\ldots a_{nk_n}$ este un termen oarecare din dezvoltarea determinantului d_{ij} din egalitatea $\mathbf{det}(M)=(-1)^{i+j}d'$ şi ţinând cont de prima parte a demonstraţiei deducem că semnul termenului $(-1)^{i+j}a_{1k_1}a_{2k_2}\ldots a_{i-1\ k_{i-1}}a_{ij}a_{i+1\ k_{i+1}}\ldots a_{nk_n}$ provenit din produsul $a_{ij}\delta_{ij}$ este acelaşi cu cel dat de dezvoltarea determinantului d. Astfel, demonstraţia teoremei este completă. ■

Corolar 1.11. Dacă $1\le i\ne j\le n$, atunci

$$\mathbf{a_{j1}\delta_{i1}+a_{j2}\delta_{i2}+\ldots+a_{jn}\delta_{in}=0.}$$

Demonstraţie. Conform Teoremei 1.10. avem

$(\star)$ **det**$(M)=a_{i1}\delta_{i1}+a_{i2}\delta_{i2}+\ldots+a_{in}\delta_{in}$.

Deoarece δ_{i1}, δ_{i2} ,…, δ_{in} nu conţin elementele a_{i1}, a_{i2},…, a_{in}, egalitatea $(\star)$ este de fapt o identitate în a_{i1}, a_{i2},…, a_{in} .

Astfel, $a_{j1}\delta_{i1}+a_{j2}\delta_{i2}+\ldots+a_{jn}\delta_{in}$ va fi un determinant ce are linia i formată din elementele a_{j1}, a_{j2},…,a_{jn} şi cum $j\neq i$ avem atunci două linii identice (linia j şi linia i ce coincide cu linia j), de unde deducem că $a_{j1}\delta_{i1}+a_{j2}\delta_{i2}+\ldots+a_{jn}\delta_{in}=0$ (conform Proprietăţii 5). ■

Sumând cele stabilite anterior, avem următorul rezultat important:

Teorema 1.12. Dacă $M=(a_{ij})_{1\le i,j\le n}\in M_n(A)$, atunci pentru orice $1\le i, j\le n$ avem

$$a_{j1}\delta_{i1}+a_{j2}\delta_{i2}+\ldots+a_{jn}\delta_{in}=\begin{cases}\det(M) & pentru\ \ j=i\\ 0 & pentru\ \ j\neq i\end{cases}.$$

În continuare vom prezenta o generalizare a celor stabilite în Teorema 1.10. ce ne dă dezvoltarea unui determinant după o linie. Mai precis vom prezenta o regulă de dezvoltare a unui determinant după mai multe linii (aşa zisa *regulă a lui Laplace*).

Înainte de a enunţa regula lui Laplace vom defini noţiunile de *minor de ordin k* ($k\le n-1$), *minor complementar* şi *complement algebric* pentru un minor complementar de ordin k (care generalizează de fapt noţiunile definite mai înainte).

Să alegem o matrice $M\in\mathbf{M_n}(A)$ ($n\ge 2$) şi să fixăm k linii $i_1, i_2,\ldots, i_k$ şi k coloane $j_1, j_2,\ldots, j_k$ ($k\le n-1$) distincte.

Elementele ce se află la intersecţia liniilor $i_1, i_2,\ldots, i_k$ şi coloanelor $j_1, j_2,\ldots, j_k$ fomează o matrice de ordinul k al cărei determinant îl vom nota prin $M_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}$ şi îl vom numi *minor de ordin k* pentru **det**(M).

Dacă eliminăm din matricea iniţială liniile $i_1, i_2,\ldots, i_k$ şi coloanele $j_1, j_2,\ldots, j_k$ obţinem o matrice pătratică de ordin n-k al cărei determinant îl vom nota prin $\overline{M}_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}$ şi îl vom numi *minorul complementar* al lui $M_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}$.

Convenim de asemenea să notăm $\begin{bmatrix} i_1 & i_2 & \ldots & i_k\\ j_1 & j_2 & \ldots & j_k\end{bmatrix}=\sum_{t=1}^{k}(i_t+j_t)$. Numărul $A_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}=(-1)^{\begin{bmatrix} i_1 & i_2 & \ldots & i_k\\ j_1 & j_2 & \ldots & j_k\end{bmatrix}}\cdot\overline{M}_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}$ se va numi *complementul algebric* al lui $M_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}$.

Observăm că pentru $k=1$ obţinem noţiunile prezentate în Definiţia 1.9..

Exemplu. Fie matricea $M=\begin{pmatrix}1 & 2 & 3 & -1\\ 0 & 1 & -1 & 2\\ -1 & 1 & 1 & -2\\ 0 & -1 & 3 & 1\end{pmatrix}\in M_4(\mathbb{Z})$.

Să alegem liniile $i_1=2$, $i_2=4$ şi coloanele $j_1=1$, $j_2=2$ (deci $k=2$).

Avem $M_{12}^{24}=\begin{vmatrix}0 & 1\\ 0 & -1\end{vmatrix}=0$, $\overline{M}_{12}^{24}=\begin{vmatrix}3 & -1\\ 1 & -2\end{vmatrix}=-5$, $\begin{bmatrix}2 & 4\\ 1 & 2\end{bmatrix}=9$, deci

$$A_{12}^{24}=(-1)^9\,\overline{M}_{12}^{24}=-(-5)=5.$$

Să observăm că dacă fixăm k linii, cu elementele acestora putem forma C_n^k minori de ordin k.

Suntem acum în măsură să prezentăm *regula lui Laplace:*

Teorema 1.13. (*Laplace*). Dacă $M=(a_{ij})_{1\le i,j\le n}\in M_n(A)$ şi fixăm liniile $1\le i_1<i_2<\ldots<i_k\le n$ ($k\le n-1$), atunci

$$\mathbf{det(M)}=\sum_{1\le j_1<j_2<\ldots<j_k\le n}M_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}\cdot A_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}\quad\textbf{(o sumă de } C_n^k \textbf{ termeni).}$$

Demonstrație. În esență, ideea de demonstrație este asemănătoare cu cea de la demonstrația Teoremei 1.10. cu deosebirea că este ceva mai elaborată.

Observăm că pentru $1\le j_1<j_2<\ldots<j_k\le n$, $M_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}$ este o sumă de k! termeni iar $A_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}$ este o sumă de (n-k)! termeni astfel că dacă notăm cu S suma din partea dreaptă a egalității din enunț atunci S va fi o sumă de $k!\cdot(n-k)!\cdot C_n^k=n!$ termeni.

Dacă vom arăta că cei n! termeni ce formează pe S sunt de fapt termeni distincți din dezvoltarea lui **det**(M) (şi cu acelaşi semn ca în **det**(M)) atunci în mod evident avem egalitatea din enunț **det**(M)=S.

Să considerăm la început cazul $i_1=j_1=1$, $i_2=j_2=2$, …, $i_k=j_k=k$.

Atunci $M_{12\ldots k}^{12\ldots k}=\sum_{\sigma\in S_k}\operatorname{sgn}(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}\ldots a_{k\sigma(k)}$,

$\begin{bmatrix}1&2&\ldots&k\\1&2&\ldots&k\end{bmatrix}=2(1+2+\ldots+k)=k(k+1)$, deci

$A_{12\ldots k}^{12\ldots k}=(-1)^{k(k+1)}\cdot\overline{M}_{12\ldots k}^{12\ldots k}=\overline{M}_{12\ldots k}^{12\ldots k}=\sum_{\tau\in S_k'}\operatorname{sgn}(\tau)a_{k+1\ \tau(k+1)}\ldots a_{n\tau(n)}$ (unde prin S'_k am notat mulțimea permutărilor asupra elementelor k+1, k+2, …, n) astfel că

$$M_{12\ldots k}^{12\ldots k}\cdot A_{12\ldots k}^{12\ldots k}=\sum_{\substack{\sigma\in S_k\\ \tau\in S_k'}}\operatorname{sgn}(\sigma)\cdot\operatorname{sgn}(\tau)\cdot a_{1\sigma(1)}a_{2\sigma(2)}\ldots a_{k\sigma(k)}a_{k+1\ \tau(k+1)}\ldots a_{n\tau(n)}.$$

Dacă notăm $\varepsilon=\begin{pmatrix}1&2&\ldots&k&k+1&\ldots&n\\ \sigma(1)&\sigma(2)&\ldots&\sigma(k)&\tau(k+1)&\ldots&\tau(n)\end{pmatrix}\in S_n$, atunci în mod evident $\operatorname{sgn}(\varepsilon)=\operatorname{sgn}(\sigma)\cdot\operatorname{sgn}(\tau)$, astfel că termenii sumei $M_{12\ldots k}^{12\ldots k}\cdot A_{12\ldots k}^{12\ldots k}$ fac parte din termenii lui **det**(M) şi apar cu acelaşi semn ca şi în dezvoltarea lui **det**(M).

Căutăm acum să probăm un rezultat similar pentru un produs general de forma $M_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}\cdot A_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}$. Permutând succesiv liniile şi coloanele vecine putem aduce minorul $M_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}$ în colțul din stânga sus al determinantului **det**(M); pentru aceasta sunt necesare $(i_1-1)+(i_2-2)+\ldots+(i_k-k)+(j_1-1)+(j_2-2)+\ldots+(j_k-k)=\begin{bmatrix}i_1&i_2&\ldots&i_k\\ j_1&j_2&\ldots&j_k\end{bmatrix}-k\cdot(k+1)$ permutări de linii şi coloane.

Dacă notăm prin N matricea astfel obținută avem că $\mathbf{det}(N)=(-1)^{\begin{bmatrix}i_1&i_2&\ldots&i_k\\ j_1&j_2&\ldots&j_k\end{bmatrix}}\cdot\mathbf{det}(M)$, $M_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}=N_{12\ldots k}^{12\ldots k}$ iar $\overline{M}_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}=\overline{N}_{12\ldots k}^{12\ldots k}$. Din cele demonstrate anterior, în **det**(N) suma tuturor termenilor ale căror prime k elemente intră în minorul $M_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}$ este egală cu produsul $M_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}\cdot\overline{M}_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}$. De aici rezultă că suma termenilor corespunzători ai lui **det**(M) este egală cu produsul:

$$(-1)^{\begin{bmatrix}i_1&i_2&\ldots&i_k\\ j_1&j_2&\ldots&j_k\end{bmatrix}}\cdot M_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}\cdot\overline{M}_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}=M_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}\cdot A_{j_1j_2\ldots j_k}^{i_1i_2\ldots i_k}.$$

Cu aceasta teorema este complet demonstrată. ■

Exemplu. Fie matricea $M=\begin{pmatrix}1&2&-1&0\\0&-1&1&1\\-1&2&3&-1\\1&2&3&0\end{pmatrix}\in M_4(\mathbb{Z})$.

Să calculăm **det**(M) dezvoltându-l cu ajutorul regulii lui Laplace după liniile 1 şi 2. Avem

$\mathbf{det}(M)=M_{12}^{12}A_{12}^{12}+M_{13}^{12}A_{13}^{12}+M_{14}^{12}A_{14}^{12}+M_{23}^{12}A_{23}^{12}+M_{24}^{12}A_{24}^{12}+M_{34}^{12}A_{34}^{12}=$

$=\begin{vmatrix}1&2\\0&-1\end{vmatrix}\cdot(-1)^{\begin{bmatrix}1&2\\1&2\end{bmatrix}}\cdot\begin{vmatrix}3&-1\\3&0\end{vmatrix}+\begin{vmatrix}1&-1\\0&1\end{vmatrix}\cdot(-1)^{\begin{bmatrix}1&2\\1&3\end{bmatrix}}\cdot\begin{vmatrix}2&-1\\2&0\end{vmatrix}+\begin{vmatrix}1&0\\0&1\end{vmatrix}\cdot(-1)^{\begin{bmatrix}1&2\\1&4\end{bmatrix}}\cdot\begin{vmatrix}2&3\\2&3\end{vmatrix}$

$+\begin{vmatrix}2&-1\\-1&1\end{vmatrix}\cdot(-1)^{\begin{bmatrix}1&2\\2&3\end{bmatrix}}\cdot\begin{vmatrix}-1&-1\\1&0\end{vmatrix}+\begin{vmatrix}2&0\\-1&1\end{vmatrix}\cdot(-1)^{\begin{bmatrix}1&2\\2&4\end{bmatrix}}\cdot\begin{vmatrix}-1&3\\1&3\end{vmatrix}+$

$+\begin{vmatrix}-1&0\\1&1\end{vmatrix}\cdot(-1)^{\begin{bmatrix}1&2\\3&4\end{bmatrix}}\cdot\begin{vmatrix}-1&2\\1&2\end{vmatrix}=\begin{aligned}&=(-1)\cdot(-1)^6\cdot3+1\cdot(-1)^7\cdot2+1\cdot(-1)^8\cdot0+1\cdot(-1)^8\cdot1+2\cdot(-1)^9\cdot(-6)=\\&=-3-2+1+12=8\end{aligned}$.

Corolar 1.14. Dacă M, N∈$\mathbf{M_n(A)}$, atunci det(M·N)=det(M)·det(N) (adică aplicația det:$\mathbf{M_n(A)}$→A este morfism de monoizi multiplicativi).

Demonstrație. Alegem M=$(a_{ij})_{1\le i,j\le n}$, N=$(b_{ij})_{1\le i,j\le n}$ şi considerăm matricea P∈$\mathbf{M_{2n}(A)}$, P=$\begin{pmatrix} M & O_n \\ -I_n & N \end{pmatrix}$ al cărui determinant îl calculăm în două moduri:

Pe de o parte, cu ajutorul regulei lui Laplace dezvoltăm pe **det**(P) după primele n linii şi obținem **det**(P)=**det**(M)·$(-1)^{\begin{bmatrix}1 & 2 & \dots & n\\ 1 & 2 & \dots & n\end{bmatrix}}$·**det**(N)=**det**(M)·**det**(N).

Pe de altă parte, pentru fiecare 1≤j≤n în **det**(P) facem următoarele operații: înmulțim coloana 1 cu b_{1j}, pe a doua cu b_{2j}, …, pe a n-a cu b_{nj} şi ce obținem adunăm la coloana n+j, obținând astfel pentru **det**(P) următoarea formă: **det**(P)=**det**(P′), unde P′ este matricea $\begin{pmatrix} M & M\cdot N \\ -I_n & O_n \end{pmatrix}$.

Dezvoltând acum pe **det**(P) după ultimele n coloane obținem:

det(P)=**det**(M·N)·$(-1)^{\begin{bmatrix}1 & 2 & \dots & n\\ n+1 & n+2 & \dots & 2n\end{bmatrix}}$·**det**($I_n$)=**det**(M·N)·$(-1)^{1+2+\dots+2n}\cdot(-1)^n$=**det**(M·N)·$(1)^{n(2n+1)+n}$=**det**(MN),

de unde deducem egalitatea **det**(M·N)=**det**(M)·**det**(N). ■

§2. Matrice inversabilă. Inversa unei matrice. Rangul unui sistem de vectori. Rangul unei matrice. Rangul unei aplicații liniare între spații vectoriale de dimensiuni finite.

În cadrul acestui paragraf prin A vom desemna un inel unitar şi comutativ (cu 0≠1). Reamintim că prin **U**(A) se notează de obicei unitățile monoidului (A, ·) (adică **U**(A)={a∈A | există b∈A a.î. ab=ba=1}). În mod evident (**U**(A), ·) este grup, numit *grupul unităților* lui A.

Grupul unităților inelului $\mathbf{M_n(A)}$ se notează cu $\mathbf{GL_n(A)}$ şi poartă numele de *grupul general liniar de grad n* al inelului A; în particular $\mathbf{GL_1(A)}$=**U**(A).

În continuare vom prezenta o caracterizare a unităților inelului $\mathbf{M_n(A)}$ cu ajutorul determinanților.

Teorema 2.1. Dacă A este un inel unitar şi comutativ, atunci M∈$\mathbf{M_n(A)}$ este inversabilă (adică M∈$\mathbf{GL_n(A)}$) dacă şi numai dacă det(M)∈U(A).

Demonstrație. „⇒". Dacă M∈$\mathbf{M_n(A)}$ este inversabilă, atunci există N∈$\mathbf{M_n(A)}$ a.î. M·N=I_n. Deducem imediat că **det**(M)·**det**(N)=1, adică **det**(M)∈U(A).

„⇐". Să presupunem că d=**det**(M)∈U(A). Vom nota prin M^* matricea din $\mathbf{M_n(A)}$ ce se obține din ${}^tM$ înlocuind fiecare element din ${}^tM$ prin complementul său algebric din ${}^tM$ şi să demonstrăm că $M^{-1}=d^{-1}\cdot M^*$. Pentru aceasta observăm că dacă $M^*=(a_{ij}^*)_{1\le i,\, j\le n}$, atunci $a_{ij}^*=(-1)^{i+j}\,d_{ji}=\Gamma_{ji}$ (vezi notațiile de la §1.).

Astfel, un element oarecare al matricei $M\cdot M^*$ va fi de forma $c_{ij}=a_{i1}\cdot a_{1j}^*+\dots+a_{in}\cdot a_{nj}^*=a_{i1}\cdot\Gamma_{j1}+\dots+a_{in}\cdot\Gamma_{jn}$.

Deoarece $c_{ij}=\begin{cases} d & pentru\ i=j \\ 0 & pentru\ i\ne j \end{cases}$ (vezi Teorema 1.12.) deducem că $M\cdot M^*=d\cdot I_n$ şi atunci $M\cdot(d^{-1}\cdot M^*)=I_n$. Analog deducem şi că $(d^{-1}\cdot M^*)\cdot M=I_n$, de unde concluzia că $M^{-1}=d^{-1}\cdot M^*$. ■

Observația 2.2. Matricea M^* construită mai sus poartă numele de *reciproca* lui M.

Corolar 2.3. Dacă K este un corp comutativ, atunci M∈$\mathbf{M_n(K)}$ este inversabilă dacă şi numai dacă det(M)≠0.

Exemplu. Fie $M=\begin{pmatrix} 1 & 2 & -1 \\ 0 & -1 & 0 \\ -1 & 1 & 0 \end{pmatrix} \in \mathbf{M_3(\mathbb{Z})}$. Deoarece $d=\mathbf{det}(M)=1\in U(\mathbb{Z})$ deducem că M este inversabilă în $\mathbf{M_3(\mathbb{Z})}$. Pentru calculul lui M^{-1} procedăm ca în cazul demonstrației Teoremei 3.1..

Pentru aceasta calculăm ${}^tM=\begin{pmatrix} 1 & 0 & -1 \\ 2 & -1 & 1 \\ -1 & 0 & 0 \end{pmatrix}$ iar $M^*=\begin{pmatrix} 0 & -1 & -1 \\ 0 & -1 & 0 \\ -1 & -3 & -1 \end{pmatrix}$ şi astfel $M^{-1}=M^*=\begin{pmatrix} 0 & -1 & -1 \\ 0 & -1 & 0 \\ -1 & -3 & -1 \end{pmatrix}$.

Într-adevăr, $M\cdot M^*=\begin{pmatrix} 1 & 2 & -1 \\ 0 & -1 & 0 \\ -1 & 1 & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & -1 & -1 \\ 0 & -1 & 0 \\ -1 & -3 & -1 \end{pmatrix}=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}=I_3$ şi analog $M^*\cdot M=I_3$.

Corolar 2.4. Fie K un corp comutativ şi $M\in\mathbf{M_n(K)}$. Atunci următoarele afirmații sunt echivalente :

(i) $M\in\mathbf{GL_n(K)}$

(ii) $\det(M)\neq 0$

(iii) $ind_K\{\widetilde{c}_1^M,...,\widetilde{c}_n^M\}$

(iv) $ind_K\{l_1^M,...,l_n^M\}$, **unde prin** $\widetilde{c}_1^M,...,\widetilde{c}_n^M$**, respectiv** $l_1^M,...,l_n^M$ **am notat transpusele coloanelor, respectiv liniile matricei M (**$\widetilde{c}_1^M,...,\widetilde{c}_n^M$ **sunt priviți ca vectori în** $K^m = M_{1,m}(K)$ **iar** $l_1^M,...,l_n^M$ **ca vectori în** $K^n = M_{1,n}(K)$**).**

În cazul în care numărul n este mai mare metoda de calcul a lui M^{-1} descrisă în demonstrația Teoremei 2.1. este inutilizabilă datorită numărului mare de calcule pe care le implică.

Pentru matricele cu coeficienți într-un corp comutativ K, lema substituției oferă o metodă eficientă de calcul a inversei acestora.

Într-adevăr, se pleacă de la tabelul :

Baza	c_1^M	c_2^M	…	c_n^M	$c_1^{I_n}$	$c_2^{I_n}$	…	$c_n^{I_n}$
e_1	a_{11}	a_{12}	…	a_{1n}	1	0	…	0
e_2	a_{21}	a_{22}	…	a_{2n}	0	1	…	0
…..	……	……			……			
e_n	a_{n1}	a_{n2}		a_{nn}	0	0	…	1

Cu ajutorul lemei substituției înlocuim pe c_1^M, c_2^M,…, c_n^M prin $c_1^{I_n}$, $c_2^{I_n}$, …, $c_n^{I_n}$ (lucru posibil datorită Corolarului 2.4., (iii)) obținând în final tabelul:

Baza	c_1^M	c_2^M	…	c_n^M	$c_1^{I_n}$	$c_2^{I_n}$	…	$c_n^{I_n}$
c_1^M	1	0	…	0	b_{11}	b_{12}	…	b_{1n}
c_2^M	0	1	…	0	b_{21}	b_{22}	…	b_{2n}
…..	……	……			……			
c_n^M	0	0	…	1	b_{n1}	b_{n2}	…	b_{nn}

Matricea $N=(b_{ij})_{1\le i,j\le n}$ ce apare în al doilea „compartiment” al ultimului tabel este chiar inversa lui M deoarece pentru orice $1\le i, j\le n$ avem $c_j^{I_n}=b_{1j}c_1^M+...+b_{nj}c_n^M$, lucru echivalent cu egalitatea $I_n=M\cdot N$.

Să calculăm de exemplu cu ajutorul lemei substituției inversa matricei $M=\begin{pmatrix} 3 & 2 \\ -1 & 1 \end{pmatrix} \in \mathbf{M_2(\mathbb{R})}$

(aceasta există deoarece **det**(M)=3+2=5≠0):

Baza	c_1^M	c_2^M	$c_1^{I_2}$	$c_2^{I_2}$
e_1	③	2	1	0
e_2	-1	1	0	1
c_1^M	1	2/3	1/3	0
e_2	0	5/3	1/3	1
c_1^M	1	0	1/5	-2/5
c_2^M	0	1	1/5	3/5

Deducem că $M^{-1}=\begin{pmatrix} 1/5 & -2/5 \\ 1/5 & 3/5 \end{pmatrix}$.

Într-adevăr, $\begin{pmatrix} 3 & 2 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1/5 & -2/5 \\ 1/5 & 3/5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$.

Observația 2.5. 1. Vectorii bazei canonice $e_1, \ldots, e_n$ din K^n nu pot fi întotdeauna înlocuiți cu $c_1^M, c_2^M, \ldots, c_n^M$ (în această ordine). În general $e_1, \ldots, e_n$ se înlocuiesc cu $c_{\sigma(1)}^M, c_{\sigma(2)}^M, \ldots, c_{\sigma(n)}^M$ unde $\sigma \in S_n$, astfel că M^{-1} apare în ultimul tabel din lema substituției „perturbată" de σ. În acest caz, M^{-1} poate fi obținută prin diferite permutări de linii care restabilesc ordinea $c_1^M, c_2^M, \ldots, c_n^M$ în baza $\{c_{\sigma(1)}^M, \ldots, c_{\sigma(n)}^M\}$.

2. Calculul lui M^{-1} cu ajutorul lemei substituției poate demara fără a ne asigura că **det**(M)≠0.

Dacă **det**(M)=0, atunci la un anumit pas al iterației din lema substituției, nu toți vectorii c_i^M, $1 \le i \le n$ pot să înlocuiască vectorii e_i, $1 \le i \le n$, ceea ce va avea ca efect blocarea algoritmului de calcul, de unde concluzia că **det**(M)=0, adică M^{-1} nu existăSă considerăm acum sistemul de n ecuații cu n necunoscute cu coeficienți în corpul comutativ K:

$$[S] \begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \ldots + a_{2n}x_n = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + \ldots + a_{nn}x_n = b_n \end{cases}$$

Notăm $M=(a_{ij})_{1 \le i,j \le n} \in \mathbf{M_n(K)}$, $b=(b_1, \ldots, b_n) \in K^n$ iar pentru $1 \le i \le n$ fie M_i matricea ce se obține din M înlocuindu-i coloana i prin coloana termenilor liberi $\widetilde{b}={}^t b$.

În aceste condiții avem următorul rezultat:

Teorema 2.6. (*Cramer*) Dacă d=det(M)≠0, atunci sistemul [S] admite soluția unică $\mathbf{x=(x_1, \ldots, x_n)}$ unde $\mathbf{x_i=d_i \cdot d^{-1}}$ cu $\mathbf{d_i=det(M_i)}$ pentru orice $\mathbf{1 \le i \le n}$.

Demonstrație. Scriem sistemul [S] sub forma matriceală $M \cdot \widetilde{x} = \widetilde{b}$, unde $x=(x_1, \ldots, x_n)$ iar $b=(b_1, \ldots, b_n)$. Deoarece d=**det**(M)≠0, conform Corolarului 2.3. există M^{-1}, astfel că $\widetilde{x} = M^{-1} \cdot \widetilde{b}$. În cadrul demonstrației Teoremei 2.1. am stabilit că

$$M^{-1} = \frac{1}{\det(M)} \cdot M^* = \frac{1}{d} \cdot \left(a_{ij}^*\right)_{1 \le i,j \le n},$$

unde $a_{ij}^* = \Gamma_{ji}$, $1 \le i, j \le n$.

Astfel:

$$\widetilde{x} = d^{-1} \cdot \left(a_{ij}^*\right)_{1\le i,j\le n} \quad \text{sau}$$

$$\widetilde{x} = d^{-1} \cdot \begin{pmatrix} a_{11}^* b_1 + \ldots + a_{1n}^* b_n \\ a_{21}^* b_1 + \ldots + a_{2n}^* b_n \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n1}^* b_1 + \ldots + a_{nn}^* b_n \end{pmatrix} = d^{-1} \cdot \begin{pmatrix} \Gamma_{11} b_1 + \ldots + \Gamma_{n1} b_n \\ \Gamma_{12} b_1 + \ldots + \Gamma_{n2} b_n \\ \ldots\ldots\ldots\ldots\ldots \\ \Gamma_{1n} b_1 + \ldots + \Gamma_{nn} b_n \end{pmatrix} = d^{-1} \cdot \begin{pmatrix} d_1 \\ d_2 \\ \ldots \\ d_n \end{pmatrix} = \begin{pmatrix} d^{-1} \cdot d_1 \\ d^{-1} \cdot d_2 \\ \ldots \\ d^{-1} \cdot d_n \end{pmatrix}$$

(ţinând cont de Teorema 1.12.), de unde $x_i = d^{-1} \cdot d_i$, $1 \le i \le n$. ■

Observaţia 2.7. În condiţiile Teoremei 2.6. spunem despre sistemul [S] că este *Cramerian.*

Definiţia 2.8. Fie V un spaţiu vectorial peste corpul K iar $S=\{v_1, \ldots, v_n\} \subseteq V$ un sistem finit de vectori.

Prin *rangul* lui S notat rang(S), înţelegem numărul maxim de vectori din S ce sunt liniar independenţi peste K.

În mod evident, **rang**(S)=$\mathbf{dim}_K$(S), unde reamintim că prin (S) am notat spaţiul vectorial generat de S (vezi §1. din Capitolul 6).

Să definim acum noţiunea de *rang* al unei matrice $M=\left(a_{ij}\right)_{\substack{1\le i\le m \\ 1\le j\le n}} \in \mathbf{M_{m,n}(K)}$ cu K corp comutativ.

Pentru $1 \le p \le m$ şi $1 \le q \le n$ prin *minor de tipul (p, q)* al lui M înţelegem determinantul matricei de tipul (p, q) ce are elementele situate la intersecţia a p linii şi q coloane ale lui M. Dacă p=q un minor de ordinul (p, p) al lui M se zice *minor de ordinul p al lui M* (în mod evident, matricea M are $C_m^p \cdot C_n^q$ minori de tipul (p, q) şi $C_m^p \cdot C_n^p$ minori de ordin p).

Definiţia 2.9. Fie K un corp (comutativ) şi $M \in \mathbf{M_{m,n}(K)}$. Spunem despre matricea M că are *rangul* r şi scriem rang(M)=r dacă M are un minor de ordinul r nenul şi toţi minorii de ordin mai mare ca r (dacă există!) egali cu zero. În mod evident, $0 \le \mathbf{rang}(M) \le \min\{m, n\}$ şi în definiţia lui rang(M) este suficient să cerem ca toţi minorii de rang r+1 (dacă există) să fie egali cu zero.

Dacă m=n, a spune că rang(M)=n revine în mod evident la a spune că det(M)≠0.

Din definiţia de mai sus deducem imediat următoarele proprietăţi elementare pentru rangul unei matrice $M \in \mathbf{M_{m,n}(K)}$:

R_1) **rang**(M)=**rang**(^{t}M)

R_2) Dacă notăm prin M′ matricea ce se obţine din M schimbând între ele două linii (sau coloane), atunci **rang**(M)=**rang**(M′)

R_3) Dacă $a \in K^*$ şi notăm prin M′ matricea obţinută din M prin înmulţirea tuturor elementelor unei linii (sau coloane) cu a, atunci **rang**(M)=**rang**(M′).

Corolar 2.10. Rangul unei matrice M nu se schimbă dacă la o linie (sau coloană) a sa adunăm o combinaţie liniară de alte linii (sau coloane).

Demonstraţie. Într-adevăr, dacă notăm prin M′ matricea ce se obţine din M adăugând la o linie (sau coloană) a sa o combinaţie liniară de linii (sau coloane) atunci subspaţiul vectorial generat de liniile lui M′ va fi în mod evident egal cu subspaţiul vectorial generat de liniile lui M. ■

Observaţia 2.11. Teorema 2.10. ne permite să calculăm iterativ rangul unei matrice nenule $M \in \mathbf{M_{m,n}(K)}$.

Deoarece M este nenulă, **rang**(M)≥1. Să presupunem că am găsit un minor de ordin r≥1 nenul. Pe acesta îl bordăm cu elementele corespunzătoare ale uneia din liniile şi uneia dintre coloanele ce nu fac parte din acel minor. Dacă toţi aceşti minori de ordin r+1 sunt nuli, atunci **rang**(M)=r. Dacă însă cel puţin unul este nenul, atunci continuăm procedeul cu acel minor.

Să observăm că în felul acesta numărul minorilor de ordin r+1 ce se calculează prin bordarea unui minor de ordin r este (m-r)(n-r) pe când dacă am fi calculat rangul lui M cu ajutorul Definiţiei

3.9. ar fi trebuit să calculăm $C_m^{r+1} \cdot C_n^{r+1}$ m minori de ordin r+1, reducând astfel anumite calcule (deoarece în general $C_m^{r+1} \cdot C_n^{r+1}$>(m-r)(n-r)).

Exemple. 1. Să determinăm rangul matricei $M=\begin{pmatrix} 2 & -1 & 1 & 0 \\ 3 & 1 & -1 & 2 \\ -1 & 1 & 0 & 1 \end{pmatrix} \in \mathbf{M_{3,4}(\mathbb{R})}$.

Se observă că $\begin{vmatrix} 2 & -1 \\ 3 & 1 \end{vmatrix} = 5 \neq 0$, deci **rang**(M)≥2. Pentru a vedea dacă **rang**(M) este 2 sau 3 este suficient să calculăm doar doi determinanți şi anume:

$$\begin{vmatrix} 2 & -1 & 1 \\ 3 & 1 & -1 \\ -1 & 1 & 0 \end{vmatrix} = 5 \quad \text{şi} \quad \begin{vmatrix} 2 & -1 & 0 \\ 3 & 1 & 2 \\ -1 & 1 & 1 \end{vmatrix} = 3 .$$

Deducem astfel că **rang**(M)=3.

2. Dacă considerăm acum matricea $M=\begin{pmatrix} 1 & 2 & -1 & 3 \\ 0 & -1 & 1 & -2 \\ 1 & 1 & 0 & 1 \end{pmatrix} \in \mathbf{M_{3,4}(\mathbb{R})}$.

Se observă că $\begin{vmatrix} 1 & 2 \\ 0 & -1 \end{vmatrix} = -1 \neq 0$, deci **rang**(M)≥2.

Calculând acum cei doi minori ai lui M ce bordează pe $\begin{vmatrix} 1 & 2 \\ 0 & -1 \end{vmatrix}$ obținem: $\begin{vmatrix} 1 & 2 & -1 \\ 0 & -1 & 1 \\ 1 & 1 & 0 \end{vmatrix} = 0$ şi $\begin{vmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \\ 1 & 1 & 1 \end{vmatrix} = 0$ (deoarece ultima linie este suma primelor două), astfel că **rang**(M)=2.

Observația 2.12. 1. Există şi alte procedee de a determina rangul unei matrice cu ajutorul anumitor transformări elementare de matrice. În cadrul acestei lucrări (mai ales pentru teoria sistemelor liniare pe care o vom prezenta în continuare) vom utiliza doar procedeul recursiv de mai înainte de a determina rangul unei matrice deoarece pe lîngă faptul că acest procedeu ne oferă cît este rangul matricei M ne permite şi punerea în evidență a unui minor de ordin cît este rangul lui M care este nenul.

2. Când m şi n sunt numere mari, o metodă mai rapidă de calcul a rangului unei matrice ne este oferită de lema substituției: dacă $M \in \mathbf{M_{m,n}(K)}$ şi $(e_1, \ldots, e_m)$ este baza canonică a lui K^m, atunci rangul lui M coincide cu numărul vectorilor coloană $\{c_1^M, c_2^M, \ldots, c_n^M\}$ ai lui M care prin aplicarea succesivă a lemei substituției înlocuiesc vectorii din baza canonică $\{e_1, \ldots, e_m\}$.

Spre exemplificare, să stabilim cu ajutorul lemei substituției cât este rangul matricei $M=\begin{pmatrix} 2 & -1 & 0 & 3 \\ 1 & 0 & -2 & 1 \\ 3 & -1 & -2 & 4 \end{pmatrix} \in \mathbf{M_{3,4}(\mathbb{R})}$:

Baza	c_1^M	c_2^M	c_3^M	c_4^M
e_1	②	-1	0	3
e_2	1	0	-2	1
e_3	3	-1	-2	4
c_1^M	1	-1/2	0	3/2
e_2	0	(1/2)	-2	-1/2
e_3	0	1/2	-2	-1/2
c_1^M	1	0	2	-2
c_2^M	0	1	-4	-1
e_3	0	0	0	0

Cum în locul lui e_3 nu poate fi adus nici c_3^M şi nici c_4^M deducem că **rang**(M)=2.

Fie V şi W două K-spaţii vectoriale de dimensiuni finite iar f:V→W o aplicaţie liniară ce are în raport cu bazele fixate din V şi W matricea M.

Definiţia 2.13. Prin definiţie, rang(f)=rang(M).

Ţinând cont că dacă considerăm în V şi W alte baze matricea lui f în raport cu aceste noi baze este de forma P·M·N cu P şi N matrice pătratice inversabile iar **rang**(P·M·N)=**rang**(M) deducem că definiţia pentru rangul lui f de mai înainte este corectă.

Observaţia 2.14. Ţinând cont de cele stabilite mai înainte deducem că dacă f:V→W este o aplicaţie liniară între două spaţii vectoriale de dimensiuni finite atunci:

(i) f este momomorfism dacă şi numai dacă **rang**(f)=$\mathbf{dim}_K$V

(ii) f este epimorfism dacă şi numai dacă **rang**(f)=$\mathbf{dim}_K$W

(iii) f este izomorfism dacă şi numai dacă **rang**(f)=$\mathbf{dim}_K$V=$\mathbf{dim}_K$W.

§3. Sisteme de ecuaţii liniare cu coeficienţi într-un corp comutativ. Sisteme omogene. Vectori şi valori proprii ai unui operator liniar. Teorema Cayley–Hamilton

În cadrul acestui paragraf prin K vom desemna un corp comutativ.

Prin *sistem de m ecuaţii liniare cu n necunoscute* (m, n∈$\mathbb{N}^*$) înţelegem un sistem de forma:

$$[S]\ \begin{cases} a_{11}x_1 + ... + a_{1n}x_n = b_1 \\ a_{21}x_1 + ... + a_{2n}x_n = b_2 \\ ..... \\ a_{m1}x_1 + ... + a_{mn}x_n = b_m \end{cases}$$, unde a_{ij}, b_j∈K, 1≤i≤m, 1≤j≤n.

A *rezolva* sistemul [S] revine la a găsi x=(x_1, …, x_n)∈K^n ce verifică [S]; un astfel de x∈K^n se va numi *soluţie* a lui [S].

Sistemul [S] se zice *compatibil* în K dacă are cel puţin o soluţie şi *incompatibil* în caz contrar. Dacă [S] are un număr finit de soluţii el se zice *compatibil determinat* iar în cazul în care are o infinitate de soluţii se zice *compatibil nedeterminat*. Dacă mai avem un alt sistem [S′] de ecuaţii liniare cu m linii şi n necunoscute, vom spune că [S] şi [S′] sunt *echivalente* dacă au aceleaşi soluţii; în acest caz vom scrie [S]~[S′].

Notând $M=(a_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}}\in\mathbf{M_{m,n}}(K)$, b=($b_1$, …, b_m)∈K^m şi x=(x_1, …, x_n)∈K^n, sistemul [S] admite scrierea matriceală $M\cdot\widetilde{x}=\widetilde{b}$ (unde $\widetilde{x}={}^t x$ şi $\widetilde{b}={}^t b$).

A rezolva sistemul [S] revine la a da răspuns (în această ordine) la următoarele probleme:

P_1: Dacă [S] este compatibil sau nu;

P_2: În caz de compatibilitate, cum se rezolvă [S].

Fie r=**rang**(M); din cele stabilite în §2. avem că 0≤r≤min{m, n}. Există atunci un minor de ordin r al lui M nenul şi toţi minorii de ordinul r+1 sunt nuli (evident, dacă există minori de ordinul r+1).

Ţinând cont de proprietăţile determinanţilor putem presupune că minorul de ordinul r nenul (pe care îl vom numi *minor principal*) este $\left|a_{ij}\right|_{1\le i,j\le r}\neq 0$.

Necunoscutele x_1, …, x_r se vor numi *necunoscute principale* iar restul se vor numi *necunoscute secundare*. Ecuaţiile 1, 2, …, r se vor numi *ecuaţii principale* iar restul *secundare.*

În cele ce urmează vom răspunde la P_1 şi P_2 în funcţie de valorile pe care le poate lua r.

Cazul 1: r=m=n. În acest caz d=**det**(M)≠0, sistemul [S] se zice Cramerian din cele stabilite în §2., (vezi Teorema 2.6.) deducem că sistemul [S] este compatibil determinat iar soluţia este dată de

$x=(x_1, \ldots, x_n)$ cu $x_i=d^{-1}d_i$, $1\le i\le n$, unde d_i este determinantul matricei ce se obține din M înlocuind coloana i prin coloana $\widetilde{b}$ a termenilor liberi, $1\le i\le n$.

Cazul 2: $r=m<n$. În acest caz toate ecuațiile sunt principale şi avem doar necunoscute secundare (şi anume pe $x_{r+1}, x_{r+2}, \ldots, x_n$).

Răspunsul la P_1 şi P_2 este dat de:

Teorema 3.1. Dacă r=m<n atunci:

P_1: Sistemul [S] este compatibil n-r nedeterminat

P_2: Pentru rezolvarea lui [S] procedăm astfel: trecem în membrul drept termenii ce conțin necunoscutele secundare, obținând astfel un sistem Cramerian în necunoscutele principale. Alegând $x_s=\alpha_s\in K$ pentru $r+1\le s\le n$ vom determina cu ajutorul formulelor lui Cramer pe $x_1, \ldots, x_r$ în funcție de $\alpha_{r+1}, \ldots, \alpha_n$.

Demonstrație. Într-adevăr, dacă notăm $M_r=\left(a_{ij}\right)_{1\le i,j\le r}$, $N_{n-r}=\left(a_{ij}\right)_{\substack{1\le i\le m\\ r+1\le j\le n}}$, $x'=(x_1, \ldots, x_r)\in K^r$ şi $x''=(x_{r+1}, \ldots, x_n)\in K^{n-r}$, atunci sistemul [S] se scrie sub forma echivalentă:

$$[S'] \qquad M_r\cdot\widetilde{x}'+N_{n-r}\cdot\widetilde{x}''=\widetilde{b}\ .$$

Deoarece **det**$(M_r)\neq 0$, există M_r^{-1} şi astfel [S′] este echivalent cu:

$$[S''] \qquad M_r\cdot\widetilde{x}'=-N_{n-r}\cdot\widetilde{x}''+\widetilde{b}$$

care este un sistem Cramerian în necunoscutele principale $x_1, \ldots, x_r$. Alegând $x_s=\alpha_s\in K$ cu $r+1\le s\le n$ din rezolvarea lui [S″] cu ajutorul formulelor lui Cramer găsim pe $x_1, \ldots, x_r$ în funcție de $\alpha_{r+1}, \ldots, \alpha_n$, astfel că soluția generală a lui [S] este dată de: $x_1=x_1(\alpha_{r+1}, \ldots, \alpha_n), \ldots, x_r=x_r(\alpha_{r+1}, \ldots, \alpha_n)$, $x_{r+1}=\alpha_{r+1}, \ldots, x_n=\alpha_n$, cu $\alpha_{r+1}, \ldots, \alpha_n$ din K, alese arbitrar. ■

Exemplu. Să considerăm în $\mathbb{R}$ sistemul:

$$[S] \quad \begin{cases} 2x_1-x_2+3x_3-x_4=2\\ x_1+x_2-x_3+2x_4=-1\end{cases}.$$

În acest caz m=2, n=4, $M=\begin{pmatrix}2 & -1 & 3 & -1\\ 1 & 1 & -1 & 2\end{pmatrix}$ şi deoarece $\begin{vmatrix}2 & -1\\ 1 & 1\end{vmatrix}=3\neq 0$, deducem că **rang**$(M)=2=m<n=4$, astfel că x_1 şi x_2 sunt necunoscute principale iar x_3 şi x_4 secundare.

Din cele prezentate mai sus deducem că sistemul [S] este compatibil 4-2=2 -nedeterminat. Pentru rezolvarea sa să alegem $x_3=\alpha_3$, $x_4=\alpha_4$ (cu $\alpha_3, \alpha_4\in\mathbb{R}$) şi astfel sistemul [S] este echivalent cu sistemul Cramerian:

$$[S'] \quad \begin{cases} 2x_1-x_2=-3\alpha_3+\alpha_4+2\\ x_1+x_2=\alpha_3-2\alpha_4-1\end{cases}.$$

Folosind formulele lui Cramer deducem imediat că $x_1=-\frac{2}{3}\alpha_3-\frac{1}{3}\alpha_4+\frac{1}{3}$ şi $x_2=\frac{5}{4}\alpha_3-\alpha_4-\frac{4}{3}$, astfel că soluția lui [S] este $x=(-\frac{2}{3}\alpha_3-\frac{1}{3}\alpha_4+\frac{1}{3}, \frac{5}{4}\alpha_3-\alpha_4-\frac{4}{3}, \alpha_3, \alpha_4)$ cu $\alpha_3, \alpha_4\in\mathbb{R}$ arbitrare.

Cazul 3: $r<m$. În acest caz sistemul [S] are şi ecuații secundare. Pentru a răspunde la la P_1 şi P_2 să stabilim anumite notații şi definiții specifice acestui caz.

Vom nota $\overline{M}=\left(M,\widetilde{b}\right)\in\mathbf{M_{m,n+1}}(K)$, matricea ce se obține din M adăugându-i acesteia coloana $\widetilde{b}$ a termenilor liberi. Matricea $\overline{M}$ astfel obținută poartă numele de *extinsa lui M*.

Următorul rezultat răspunde la P_1:

Teorema 3.2. (*Kronecker-Capelli*) Sistemul [S] este compatibil dacă şi numai dacă rang(M)=rang($\overline{M}$).

Demonstrație. Totul rezultă din scrierea lui [S] sub forma matriceală echivalentă următoare:

$$[S'] \qquad x_1\cdot\widetilde{c}_1+x_2\cdot\widetilde{c}_2+\ldots+x_n\cdot\widetilde{c}_n=\widetilde{b}$$

(unde $\widetilde{c}_1,\widetilde{c}_2,\ldots,\widetilde{c}_n$ sunt coloanele matricei M) şi privind pe $\widetilde{c}_1,\widetilde{c}_2,\ldots,\widetilde{c}_n$ ca vectori din K^m.

Astfel, dacă $(\alpha_1,\ldots,\alpha_n)\in K^n$ este o soluție a lui [S] atunci $\alpha_1\cdot\widetilde{c}_1+\alpha_2\cdot\widetilde{c}_2+\ldots+\alpha_n\cdot\widetilde{c}_n=\widetilde{b}$ şi deci $\widetilde{b}$ este o combinație liniară de $\widetilde{c}_1,\widetilde{c}_2,\ldots,\widetilde{c}_n$, de unde concluzia că **rang**(M)=**rang**($\overline{M}$) (ținând cont de Teorema 2.10. şi Corolarul 2.11.).

Reciproc, dacă **rang**(M)=**rang**($\overline{M}$) înseamnă că $\widetilde{b}$ este o combinație liniară de $\widetilde{c}_1,\widetilde{c}_2,\ldots,\widetilde{c}_n$, adică există $\alpha_1,\ldots,\alpha_n\in K$ a.î. $\alpha_1\cdot\widetilde{c}_1+\alpha_2\cdot\widetilde{c}_2+\ldots+\alpha_n\cdot\widetilde{c}_n=\widetilde{b}$ şi astfel $x=(\alpha_1,\ldots,\alpha_n)\in K^n$ este o soluție a lui [S]. ■

Pentru fiecare $r+1\le j\le m$ să notăm prin N_j matricea

$$N_j=\left(\begin{array}{ccc|c} a_{11} & \ldots & a_{1r} & b_1 \\ \ldots & \ldots & \ldots & \ldots \\ a_{r1} & \ldots & a_{rr} & b_r \\ \hline a_{j1} & \ldots & a_{jr} & b_j \end{array}\right) \text{ iar } \Delta_j=\mathbf{det}(N_j).$$

Cei m-r determinanți Δ_j ($r+1\le j\le m$) poartă numele de *determinanți caracteristici*.

Astfel, Teorema 3.2. are următoarea formă echivalentă datorată lui Rouché:

Teorema 3.3. (*Rouché*) Sistemul [S] este compatibil dacă şi numai dacă toți cei m-r determinanți caracteristici Δ_j ($r+1\le j\le m$) sunt egali cu zero.

Pentru a răspunde la P_2 avem nevoie de următorul rezultat:

Propoziția 3.4. Dacă sistemul [S] este compatibil, atunci [S] este echivalent cu sistemul $[S_r]$ format doar din ecuațiile principale.

Demonstrație. Avem de demonstrat doar că în caz de compatibilitate a lui [S], dacă $(\alpha_1,\ldots,\alpha_n)\in K^n$ este o soluție a lui $[S_r]$ atunci pentru orice $r+1\le j\le m$ avem:

$$a_{j1}\alpha_1+a_{j2}\alpha_2+\ldots+a_{jn}\alpha_n=b_j.$$

Pentru aceasta plecăm de la determinantul de ordin r+1:

$$D_{r,j}(x_1,\ldots,x_n)=\left|\begin{array}{ccc|c} a_{11} & \ldots & a_{1r} & a_{11}x_1+\ldots+a_{1n}x_n-b_1 \\ \ldots & \ldots & \ldots & \ldots \\ a_{r1} & \ldots & a_{rr} & a_{r1}x_1+\ldots+a_{rn}x_n-b_r \\ \hline a_{j1} & \ldots & a_{jr} & a_{j1}x_1+\ldots+a_{jn}x_n-b_j \end{array}\right|=\sum_{s=1}^{n}\left|\begin{array}{ccc|c} a_{11} & \ldots & a_{1r} & a_{1s} \\ \ldots & \ldots & \ldots & \ldots \\ a_{r1} & \ldots & a_{rr} & a_{rs} \\ \hline a_{j1} & \ldots & a_{jr} & a_{js} \end{array}\right|\cdot x_s-\Delta_j$$

(Δ_j fiind determinantul caracteristic).

Cum **rang**(M)=r deducem că

$$(\star)\ D_{r,j}(x_1,\ldots,x_n)=-\Delta_j.$$

Dacă $(\alpha_1,\ldots,\alpha_n)\in K^n$ este o soluție a lui $[S_r]$, atunci

$$D_{r,j}(\alpha_1,\ldots,\alpha_n)=\left|\begin{array}{ccc|c} a_{11} & \ldots & a_{1r} & 0 \\ \ldots & \ldots & \ldots & \ldots \\ a_{r1} & \ldots & a_{rr} & 0 \\ \hline a_{j1} & \ldots & a_{jr} & a_{j1}\alpha_1+\ldots+a_{jn}\alpha_n-b_j \end{array}\right|=$$

$=\mathbf{det}(M_r)(a_{j1}\alpha_1+a_{j2}\alpha_2+\ldots+a_{jn}\alpha_n-b_j)$ şi ținând cont de $(\star)$ deducem că

$$\mathbf{det}(M_r)(a_{j1}\alpha_1+a_{j2}\alpha_2+\ldots+a_{jn}\alpha_n-b_j)=-\Delta_j\ (\star\star).$$

Cum [S] este compatibil, deducem că $\Delta_j=0$ pentru orice $r+1\le j\le m$ (conform Teoremei 3.3.) şi astfel din $(\star\star)$ deducem că

$$a_{j1}\alpha_1+a_{j2}\alpha_2+\ldots+a_{jn}\alpha_n-b_j=0 \text{ pentru orice } r+1\le j\le m.\ ■$$

Observația 3.5. Din cele stabilite mai înainte, deducem că în cazul când **rang**(M)=r < m, pentru a răspunde la P_1 calculăm cei m-r determinanți caracteristici Δ_j ($r+1\le j\le m$). Dacă unul dintre aceştia este nenul, atunci sistemul [S] este incompatibil pe când dacă toți sunt nuli, atunci sistemul [S] este compatibil, n-r nedeterminat.

Pentru a răspunde la P_2 (în caz de compatibilitate) reținem sistemul format din ecuațiile principale și procedăm ca în *Cazul 2*.

Exemplu. Să se decidă dacă sistemul

$$[S]\quad \begin{cases} 2x_1 - 3x_2 + 4x_3 = -1 \\ x_1 + x_2 - x_3 = 2 \\ 3x_1 - 2x_2 + 3x_3 = 1 \end{cases}$$

este compatibil sau nu și în caz afirmativ să se rezolve în $\mathbb{R}$.

Avem $M = \begin{pmatrix} 2 & -3 & 4 \\ 1 & 1 & -1 \\ 3 & -2 & 3 \end{pmatrix} \in \mathbf{M_3}(\mathbb{R})$ și cum **det**(M)=0 iar $\begin{vmatrix} 2 & -3 \\ 1 & 1 \end{vmatrix} = 5 \neq 0$ deducem că **rang**(M)=2 < 3=m astfel că suntem în *Cazul 3*.

Avem un singur determinant caracteristic $\left|\begin{array}{cc|c} 2 & -3 & -1 \\ 1 & 1 & 2 \\ \hline 3 & -2 & 1 \end{array}\right| = 0$ și atunci conform Teoremei lui Rouché sistemul [S] este compatibil 1-nedeterminat. Primele două ecuații, ca și necunoscutele x_1, x_2 sunt principale. Pentru rezolvarea lui [S] reținem sistemul format din ecuațiile principale:

$$[S']\quad \begin{cases} 2x_1 - 3x_2 + 4x_3 = -1 \\ x_1 + x_2 - x_3 = 2 \end{cases}$$

și procedând ca în *Cazul 2* găsim soluția ($x_1 = -\frac{1}{5}\alpha + 1$, $x_2 = \frac{6}{5}\alpha + 1$, $x_3 = \alpha$) cu $\alpha \in \mathbb{R}$.

Dacă în sistemul inițial [S], $b_1=b_2=\ldots=b_m=0$, vom spune despre [S] că este *omogen*.

Observația 3.9. Sistemele liniare se pot rezolva și cu ajutorul lemei substituției.

Vom exemplifica pe un caz particular de sistem cramerian (cititorul putând intui ușor cum se procedează în general).

Pentru aceasta să considerăm sistemul:

$$[S]\quad \begin{cases} 2x_1 - 3x_2 = 4 \\ x_1 + x_2 = 2 \end{cases} \quad \Leftrightarrow \quad \begin{pmatrix} 2 \\ 1 \end{pmatrix} \cdot x_1 + \begin{pmatrix} -3 \\ 1 \end{pmatrix} \cdot x_2 = \begin{pmatrix} 4 \\ 2 \end{pmatrix}.$$

Deoarece $\begin{vmatrix} 2 & -3 \\ 1 & 1 \end{vmatrix} = 5 \neq 0$, deducem că sistemul [S] este Cramerian și deci coloanele $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$ și $\begin{pmatrix} -3 \\ 1 \end{pmatrix}$ formează o bază pentru $\mathbb{R}^2$ și a rezolva pe [S] revine la a găsi coordonatele lui $\begin{pmatrix} 4 \\ 2 \end{pmatrix}$ în această bază.

Din tabelul lemei substituției:

Baza	c_1	c_2	b
e_1	②	-3	4
e_2	1	1	2
c_1	1	-3/2	2
e_2	0	5/2	0
c_1	1	0	2
c_2	0	1	0

deducem că soluția lui [S] este (2, 0).

CURSUL nr. 13

SPAȚII VECTORIALE

În cadrul acestui capitol prin K vom desemna un corp comutativ .

Definiția 1.1. Vom spune despre un grup abelian (V,+) că este *K-spațiu vectorial* (la stinga) dacă este definită o operație algebrică externă pe M, φ:K×V→V, φ(a,x)=ax, pentru orice a∈K şi x∈V a.î. pentru oricare a, b∈K şi x, y∈V sunt verificate condițiile:

(i) a(x+y)=ax+ay
(ii) (a+b)x = ax+bx
(iii) a(bx)=(ab)x
(iv) 1·x=x

În acest caz, elementele lui K se numesc *scalari* iar φ se numeşte *înmulțire cu scalari*.

Exemple 1. Corpul K devine în mod canonic K- spațiu vectorial considerând înmulțirea de pe K drept înmulțirea cu scalari.

2. Considerând un număr natural $n\in\mathbb{N}^*$ şi grupul aditiv $K^n=K\times\ldots\times K$ (față de adunarea $x+y=(x_i+y_i)_{1\le i\le n}$, cu $x=(x_i)_{1\le i\le n}$ şi $y=(y_i)_{1\le i\le n}\in K^n$) atunci K^n devine în mod canonic un K-spațiu vectorial definind înmulțirea φ cu scalari pentru a∈K şi $x=(x_i)_{1\le i\le n}\in K^n$ prin $\varphi(a, x)=(a\cdot x_i)_{1\le i\le n}\in K^n$.

3. K[X] devine K- spațiu vectorial , definind pentru a∈K şi $P = a_0+a_1X+\ldots+a_nX^n\in K[X]$ înmulțirea cu scalari φ prin

$$\varphi(a, P) = (aa_0)+(aa_1)X+\ldots+(aa_n)X^n\in K[X].$$

4. Grupul aditiv $M_{m,n}(K)$ al matricelor de tipul (m, n) (m, n≥1) devine în mod canonic K-spațiu vectorial definind înmulțirea cu scalari pentru a∈K şi o matrice $(a_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}}$ prin $a(a_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}}=(a\cdot a_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}}\in M_{m,n}(K)$.

5. Dacă I este un interval de numere reale, atunci mulțimea

$$C(I, \mathbb{R})=\{f : I\to\mathbb{R} \mid f \text{ este continuă}\}$$

(care devine grup abelian față de adunarea canonică a funcțiilor continue) devine ℝ-spațiu vectorial definind înmulțirea φ cu scalari pentru a∈ℝ şi f:I→ℝ prin φ(a, f): I→ℝ, φ(a, f)(x)=af(x), oricare ar fi x∈I.

Propoziția 1.3. Dacă V este un K-spațiu vectorial, atunci pentru orice a, b, $a_1, \ldots, a_n\in K$ şi x, y, $x_1, \ldots, x_m\in V$ avem:

(i) a·0=0·a=0
(ii) (-a)x=a(-x)=-(ax) iar (–a)(-x)=ax
(iii) a(x-y)=ax-ay iar (a-b)x=ax-bx
(iv) $(a_1+\ldots+a_n)x=a_1x+\ldots+a_nx$ iar $a(x_1+\ldots+x_m)=ax_1+\ldots+ax_m$.

Demonstrație. (i). Din 0+0=0 deducem că a(0+0)=a·0 ⇔a·0+a·0=a·0⇔ a·0=0. Analog deducem şi că 0·a=0.

(ii). Scriind că a+(-a)=0 deducem că ax+(-a)x=0·x=0, de unde (–a)x=-(ax). Analog restul de afirmații.

(iii). Se ține cont de (ii).

(iv). Se face inducție matematică după m şi n.■

Definiția 1.4. Fiind dat un K-spațiu vectorial V, o submulțime nevidă V′ a lui V se zice *sub-spațiu vectorial* dacă V′ este subgrup al grupului aditiv (V,+) iar restricția înmulțirii cu scalari la V′ îi conferă lui V′ structură de K-spațiu vectorial.

Vom nota prin $\mathbf{L_K}(V)$ familia sub-spațiilor vectoriale ale lui V. În mod evident, {0} şi V fac parte din $\mathbf{L_K}(V)$. Oricare alt sub-spațiu vectorial al lui V diferit de {0} şi V se zice *propriu.* Dacă nu este pericol de confuzie, sub-spațiul vectorial {0} se mai notează şi prin **0** şi poartă numele de K-spațiu vectorial *nul*.

Următorul rezultat este imediat:

Propoziția 1.5. Dacă V este un K-spațiu vectorial, atunci pentru o submulțime nevidă N a lui V următoarele afirmații sunt echivalente:

(i) $\mathbf{N\in L_K(V)}$

(ii) Pentru orice x, y∈N şi a∈K, x-y∈N şi ax∈N

(iii) Pentru orice x, y∈N şi a, b∈K , ax+by∈N .

Propoziția 1.6. Dacă $(N_i)_{i\in I}$ **este o familie de sub-spații vectoriale ale unui K-spațiu vectorial V, atunci** $\bigcap_{i\in I} N_i \in \mathbf{L_K(V)}$.

Demonstrație. Fie $N=\bigcap_{i\in I} N_i$ şi x, y∈N (adică x, y∈N_i pentru orice i∈I) iar a, b∈K. Atunci ax+by∈N_i pentru orice i∈I, adică ax+by∈$\bigcap_{i\in I} N_i$ =N, deci $N\in\mathbf{L_K}(V)$.■

Propoziția 1.6. ne permite să introducem pentru un K-spațiu vectorial V şi o submulțime nevidă M a sa, noțiunea de *sub-spațiul vectorial generat de M* ca fiind cel mai mic K-spațiu vectorial al lui V (față de relația de incluziune), ce conține pe M. Dacă notăm prin (M) acest sub-spațiu vectorial avem în mod evident

$$(M)=\bigcap\{N\in L_K(V)\,|\,M\subseteq V\}.$$

Propoziția 1.7. Dacă V este un K-spațiu vectorial iar M⊆V o submulțime nevidă a sa, atunci (M)={$a_1x_1+\ldots+a_nx_n$ | $a_1, \ldots, a_n\in$K, $x_1, \ldots, x_n\in$M, n∈$\mathbb{N}^*$}.

Demonstrație. Să notăm prin M′ mulțimea combinațiilor finite cu elemente din M din partea dreaptă a egalității din enunț. Se arată imediat că M′ este sub-spațiu vectorial al lui V ce conține pe M, de unde incluziunea (M)⊆M′. Dacă alegem $N\in\mathbf{L_K}(V)$ a.î. M⊆N atunci M′⊆N şi cum N este oarecare deducem că M′⊆∩N=(M), de unde egalitatea (M)=M′. ■

Observația 1.8. 1. Dacă (M)=V, elementele lui M se zic *generatori* pentru M. Dacă M este finită, M se zice K-spațiu vectorial *finit generat* .

2. Dacă M={x} cu x∈V, atunci sub-spațiul vectorial al lui V generat de mulțimea {x} se zice *principal* şi conform propoziției precedente avem:

$$(\{x\})=\{ax\,|\,a\in K\}\overset{\text{def}}{=}Kx.$$

3. Mulțimea ordonată $(\mathbf{L_K}(V), \subseteq)$ devine în mod canonic latice completă, unde pentru o familie $(N_i)_{i\in I}$ de elemente din $\mathbf{L_K}(V)$ avem $\underset{i\in I}{\wedge} N_i=\bigcap_{i\in I} N_i$ iar $\underset{i\in I}{\vee} N_i=(\bigcup_{i\in I} N_i)$; în mod evident această latice este mărginită, unde **0**={0} iar **1**=V.

4. Dacă $N, P\in\mathbf{L_K}(V)$, atunci

$$N\vee P=(N\cup P)=\{x+y|x\in N \text{ şi } y\in P\}\overset{\text{def}}{=}N+P,$$

iar $(\{x_1, \ldots, x_n\})=Kx_1+\ldots+Kx_n$.

Propoziția 1.9. Pentru orice K-spațiu vectorial V, laticea $(\mathbf{L_K}(V), \subseteq)$ este modulară.

Demonstrație. Trebuie să arătăm că dacă P, Q, R∈$\mathbf{L}_K$(V) şi R⊆P, atunci P∧(Q∨R)=(P∧Q)∨R⇔P∩(Q+R)=(P∩Q)+R.

Cum incluziunea (P∩Q)+R⊆P∩(Q+R) este evidentă, fie x∈P∩(Q+R). Atunci x∈P şi x=y+z cu y∈Q şi z∈R. Cum R⊆P deducem că y=x-z∈P şi cum y∈Q avem că y∈P∩Q, adică x∈(P∩Q)+R, deci este adevărată şi incluziunea P∩(Q+R)⊆(P∩Q)+R, de unde egalitatea P∩(Q+R)=(P∩Q)+R. ■

Definiția 1.11. Fie V un K-spațiu vectorial. Vom spune despre elementele $x_1, \ldots, x_n \in V$ că sunt *liniar independente* peste K dacă având o combinație liniară nulă $a_1x_1+\ldots+a_nx_n= 0$ cu $a_1, \ldots, a_n \in K$, deducem că $a_1=a_2=\ldots=a_n=0$.

Dacă notăm $F=\{x_1, \ldots, x_n\}$ convenim să notăm fapul că elementele lui F sunt liniar independente peste K scriind $ind_K F$.

Dacă $V' \subseteq V$ este o submulțime oarecare a lui V, vom spune că elementele lui V' sunt *liniar independente* peste K dacă orice submulțime finită $F \subseteq V'$ este formată din elemente liniar independente peste K (vom nota lucrul acesta scriind $ind_K V'$).

În cazul în care elementele $x_1, \ldots, x_n \in V$ nu sunt liniar independente peste K vom spune despre ele că sunt *liniar dependente* peste K (acest lucru revenind la a spune că există $a_1, \ldots, a_n \in K$ nu toate nule a.î. $a_1x_1+\ldots+a_nx_n=0$) .

Exemple. 1. Dacă $n \in \mathbb{N}^*$ şi $V=K^n$ atunci notând cu e_i elementele lui V ce au 1 pe poziția i şi 0 în rest $(1 \le i \le n)$ se deduce imediat că elementele $e_1, e_2, .., e_n$ sunt liniar independente peste K.

2. Fie m, $n \in \mathbb{N}^*$ şi $M=\mathbf{M}_{m,n}(K)$ iar E_{ij} matricea de tip (m,n) ce are 1 pe poziția (i, j) şi 0 în rest $(1 \le i \le m, 1 \le j \le n)$. Se verifică imediat că elementele $(E_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ sunt liniar independente peste K.

3. Dacă V=K[X], atunci mulțimea infinită $\{1, X, X^2, \ldots.\}$ este formată din polinoame liniar independente peste K.

Definiția 1.12. Dacă V este un K-spațiu vectorial, o submulțime B a lui V se zice *bază* pentru V dacă (S)=V şi $ind_K B$.

În acest caz, spunem despre K-spațiu vectorial V că este *liber* (în mod evident V≠0).

Din cele prezentate anterior deducem că K-spațiile vectoriale K^n şi $M_{m,n}(K)$ (cu m, n≥2) sunt libere şi au baze finite iar K[X] este de asemenea liber, având însă o bază infinită.

Teorema 1.13. Fie K un corp arbitrar, V un K-spațiu vectorial nenul, $I, G \subseteq V$ a.î. $ind_K I$, (G)=V şi I⊆G. Atunci există o bază B⊆V pentru V a.î. I⊆B⊆G.

Demonstrație. Să remarcăm la început faptul că există submulțimi I şi G ale lui V cu proprietățile din enunț. Într-adevăr, putem considera în cel mai nefavorabil caz G=V iar I={x} cu x∈G, x≠0 (căci V≠**0**).

Fie $F=\{B \subseteq V \mid I \subseteq B \subseteq G$ şi $ind_K B\}$ (deoarece I∈F deducem că F≠∅). Se verifică imediat că dacă $(B_i)_{i \in I}$ este o familie total ordonată (față de incluziune) de elemente din F, atunci $\bigcup_{i \in I} B_i \in F$, de unde concluzia că (F, ⊆) este o mulțime inductivă. Conform Lemei lui Zorn există un element maximal $B_0 \in F$. Dacă vom demonstra că $(B_0)=V$, cum $ind_K B_0$, vom deduce că B_0 este bază pentru V şi teorema este demonstrată.

Pentru aceasta este suficient să demonstrăm că G⊆(B_0) (căci atunci am deduce că V=(G)⊆(B_0), de unde $(B_0)=V$).

Cum $B_0 \subseteq G$, fie $x_0 \in G \setminus B_0$. Atunci $I \subseteq B_0 \cup \{x_0\} \subseteq G$ iar datorită maximalității lui B_0 deducem că vectorii din $B_0 \cup \{x_0\}$ trebuie să fie liniar dependenți peste K. Există deci $\lambda_0, \lambda_1, \ldots, \lambda_n \in K$ nu toți nuli şi $x_1, \ldots, x_n \in B_0$ a.î. $\lambda_0x_0+ \lambda_1x_1+\ldots+\lambda_nx_n=0$.

Să observăm că $\lambda_0 \neq 0$ (căci în caz contrar, cum $\text{ind}_K B_0$ am deduce că $\lambda_1=\ldots=\lambda_n=0$, absurd), de unde deducem că $x_0 = (-\lambda_0^{-1}\lambda_1)x_1 + \ldots + (-\lambda_0^{-1}\lambda_n)x_n$ adică $x_0 \in (B_0)$. Deducem deci că $G \subseteq (B_0)$ şi astfel $(B_0)=V$, adică B_0 este o bază pentru V. ■

Ţinând cont de observaţia de la începutul demonstraţiei Teoremei 1.13., deducem imediat următorul rezultat:

Corolar 1.14. (i) Dacă K este un corp oarecare, atunci orice K-spaţiu vectorial nenul admite cel puţin o bază.

(ii) Orice parte I liniar independentă a unui sistem de generatori G al unui K-spaţiu vectorial V poate fi completată cu elemente din G pînă la o bază a lui V.

(iii) Orice sistem de vectori liniar independenţi ai unui spaţiu vectorial poate fi completat pînă la o bază a spaţiului.

Teorema 1.15. (*Teorema schimbului*). Fie K un corp oarecare iar V un K-spaţiu vectorial nenul. Dacă $x_1, \ldots, x_n \in V$ sunt liniar independenţi peste K iar $y_1, \ldots, y_m \in V$ un sistem de generatori pentru V, atunci $n \leq m$ şi există o reindexare a vectorilor $y_1, \ldots, y_m$ a.î. $(x_1, \ldots, x_n, y_{n+1}, \ldots, y_m)=V$.

Demonstraţie. Se face inducţie matematică după n. Dacă n=1 atunci în mod evident $1 \leq m$. Deoarece $(y_1,\ldots,y_m)=V$, există $a_1,\ldots,a_m \in K$ a.î. $x_1=a_1y_1+\ldots+a_my_m$; cum $x_1 \neq 0$, există un scalar a_i nenul (să zicem $a_1 \neq 0$). Atunci $y_1 = a_1^{-1}x_1 - (a_1^{-1}a_2)y_2 - \ldots - (a_1^{-1}a_m)y_m$, de unde concluzia că $(x_1, y_2,\ldots,y_m)=V$.

Să presupunem afirmaţia adevărată pentru n-1. Deoarece $x_1,\ldots,x_n$ sunt liniar independenţi peste K atunci şi $x_1,\ldots,x_{n-1}$ sunt liniar independenţi peste K şi conform ipotezei de inducţie $n-1 \leq m$ şi există o reindexare a vectorilor $y_1, \ldots, y_m$ a.î. $(x_1, \ldots, x_{n-1}, y_n , y_{n+1}, \ldots, y_m)=V$. Atunci există $b_1, \ldots, b_{n-1}, b_n , b_{n+1}, \ldots, b_m \in K$ a.î. $x_n=b_1x_1+\ldots+b_{n-1}x_{n-1}+ +b_ny_n+\ldots+b_my_m$. $(*)$

Dacă $n-1=m$ atunci $x_n=b_1x_1+\ldots+b_{n-1}x_{n-1}$ ceea ce contrazice faptul că vectorii $x_1, \ldots, x_{n-1}, x_n$ sunt liniar independenţi peste K. Atunci $n-1 \leq m-1$, de unde $n \leq m$.

Din $(*)$ deducem că există un indice i, $n \leq i \leq m$ a.î. $b_i \neq 0$ (să zicem i=n). Atunci din $(*)$ deducem că

$$y_n = b_n^{-1}x_n - (b_n^{-1}b_1)x_1 - \ldots - (b_n^{-1}b_{n-1})x_{n-1} - (b_n^{-1}b_{n+1})y_{n+1} - \ldots - (b_n^{-1}b_m)y_m$$

ceea ce ne arată că $(x_1, \ldots, x_n, y_{n+1}, \ldots, y_m)=V$ şi astfel, conform principiului inducţiei matematice teorema este complet demonstrată.■

Corolar 1.16. Fie K un corp oarecare iar V un K-spaţiu vectorial nenul. Atunci oricare două baze finite ale lui V au acelaşi număr de elemente.

Demonstraţie. Dacă $B_1=\{x_1, \ldots, x_n\}$ şi $B_2=\{y_1, \ldots, y_m\}$ sunt două baze ale lui V cu n respectiv m elemente, deoarece în particular $\text{ind}_K\{x_1, \ldots, x_n\}$ şi $(y_1, \ldots, y_m)=V$, conform teoremei schimbului avem $n \leq m$. Schimbând rolul lui B_1 cu B_2 deducem că şi $m \leq n$, de unde $m=n$.■

Definiţia 1.17. Dacă V este un K-spaţiu vectorial nenul vom nota cu $\dim_K V$ sau $[V:K]$ cardinalul unei baze arbitrare a lui V ce se va numi *dimensiunea lui V peste K.*

Dacă $\dim_K V$ este finită vom spune despre V că este de *dimensiune finită*.

Dacă $V=\{0\}$ convenim ca $\dim_K V=0$.

Din cele expuse mai înainte deducem că dacă K este un corp oarecare atunci $\dim_K K^n=n$, $\dim_K M_{m,n}(K)=mn$, $(m, n \geq 2)$ iar $\dim_K K[X]$ este infinită.

Dacă pentru $n \in \mathbb{N}$ notăm $K_n[X]=\{f \in K[X] \mid \text{grad}(f) \leq n\}$, atunci $\dim_K K_n[X]=n+1$ (căci $\{1, X,\ldots, X^n\}$ este o bază a lui $K_n[X]$ peste K).

2. Matricea de trecere de la o bază la alta. Formula de schimbare a coordonatelor unui element la schimbarea bazelor. Lema substituţiei.

Fie V un K- spaţiu vectorial de dimensiune n $(n \geq 1)$ iar $B=\{e_1, \ldots, e_n\}$ şi $B'=\{e_1',\ldots, e_n'\}$ două baze ale lui V.

Există atunci elementele a_{ij} $(1\le i, j\le n)$ din K a.î.

$$e_1'=a_{11}e_1+\ldots+a_{1n}e_n$$
$$e_2'=a_{21}e_1+\ldots+a_{2n}e_n$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$e_n'=a_{n1}e_1+\ldots+a_{nn}e_n\ .$$

Definiția 2.1. Matricea $\begin{pmatrix} a_{11} & a_{21} & \ldots & a_{n1} \\ a_{12} & a_{22} & \ldots & a_{n2} \\ \ldots & \ldots & \ldots. & \ldots \\ a_{1n} & a_{2n} & \ldots & a_{nn} \end{pmatrix}\in \mathbf{M_n(A)}$ **poartă numele de *matricea de trecere de la baza B la baza B′* şi se notează prin M(B, B′).**

Să fixăm acum anumite notații:

Dacă $x\in V$ atunci există şi sunt unice elementele $\alpha_1, \ldots,\alpha_n\in K$ a.î. $x=\alpha_1e_1+\ldots+\alpha_ne_n$. Elementele $\alpha_1, \ldots,\alpha_n\in K$ se vor numi *coordonatele lui x în baza B.* Convenim să desemnăm lucrul acesta scriind

$$x_B=\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}\in M_{n,1}(A).$$

Din raţiuni de tehnoredactare convenim de asemenea să scriem $\widetilde{x}_B={}^t x_B=(\alpha_1,\ldots,\alpha_n)$.

Teorema 2.2. Fie V un K- spaţiu vectorial de dimensiune n iar $B=\{e_1, \ldots, e_n\}$ şi $B'=\{e_1',\ldots, e_n'\}$ două baze ale sale. Atunci:

(i) Matricea M(B, B′) de trecere de la B la B′ este inversabilă, inversa sa fiind M(B′, B)

(ii) Dacă $x\in V$ atunci

$$\mathbf{x_{B'}=M(B, B')^{-1}\cdot x_B}$$

(iii) Dacă în V mai avem o a treia bază B″, atunci

$$\mathbf{M(B, B'')=M(B, B')\cdot M(B', B'').}$$

Demonstraţie. (i). Pentru orice $1\le i\le n$ avem:

$$(1)\qquad e_i'=\sum_{j=1}^{n}a_{ij}e_j \qquad \text{şi}$$

$$(2)\qquad e_i=\sum_{j=1}^{n}b_{ij}e_j'$$

Atunci $M(B, B')=\begin{pmatrix} a_{11} & a_{21} & \ldots & a_{n1} \\ a_{12} & a_{22} & \ldots & a_{n2} \\ \ldots & \ldots & \ldots. & \ldots \\ a_{1n} & a_{2n} & \ldots & a_{nn} \end{pmatrix}$ iar

$M(B', B)=\begin{pmatrix} b_{11} & b_{21} & \ldots & b_{n1} \\ b_{12} & b_{22} & \ldots & b_{n2} \\ \ldots & \ldots & \ldots. & \ldots \\ b_{1n} & b_{2n} & \ldots & b_{nn} \end{pmatrix}$.

Dacă în (1) înlocuim pentru fiecare $1\le j\le n$ pe e_j cu valorile date de (2) obținem pentru fiecare $1\le i\le n$ egalitățile:

$$e_i'=\sum_{j=1}^{n}a_{ij}\left(\sum_{k=1}^{n}b_{jk}e_k'\right)=\sum_{k=1}^{n}\left(\sum_{j=1}^{n}a_{ij}b_{jk}\right)e_k'$$

de unde cu necesitate:

$$(3)\quad \sum_{j=1}^{n}a_{ij}b_{jk}=\begin{cases}1 & pentru\quad k=i\\ 0 & pentru\quad k\ne i\end{cases}.$$

Egalitățile de la (3) ne arată că $M(B, B')\cdot M(B', B)=\mathbf{I_n}$ ($\mathbf{I_n}$ fiind maticea unitate ce are pe diagonala principală 1 şi 0 în rest), de unde deducem că $M(B, B')$ este inversabilă având inversa $M(B', B)$.

(ii). Dacă $x\in V$, atunci există $\alpha_1, \ldots, \alpha_n\in A$ a.î. $x=\alpha_1e_1+\ldots+\alpha_ne_n=\sum_{i=1}^{n}\alpha_ie_i$.

Ținând cont de (2) deducem că

$$x=\sum_{i=1}^{n}\alpha_i\left(\sum_{j=1}^{n}b_{ij}e'_j\right)=\sum_{j=1}^{n}\left(\sum_{i=1}^{n}\alpha_ib_{ij}\right)e_j' \text{ , adică}$$

$$x_{B'}=\begin{pmatrix}\sum_{i=1}^{n}\alpha_ib_{i1}\\ \vdots\\ \sum_{i=1}^{n}\alpha_ib_{in}\end{pmatrix}=\begin{pmatrix}b_{11} & b_{21} & \ldots & b_{n1}\\ b_{12} & b_{22} & \ldots & b_{n2}\\ \ldots & \ldots & \ldots & \ldots\\ b_{1n} & b_{2n} & \ldots & b_{nn}\end{pmatrix}\cdot\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}=M(B', B)\cdot x_B=M(B, B')^{-1}\cdot x_B.$$

(iii). Se verifică direct prin calcul (analog ca la (i)). ■

Vom considera acum K un corp comutativ, V un K-spațiu vectorial de dimensiune finită iar $B=\{e_1, \ldots, e_n\}\subset V$ o bază a lui V. Astfel, pentru orice vector $v\in V$ există şi sunt unice elementele (scalarii) $\alpha_1, \ldots, \alpha_n\in K$ a.î. $v=\alpha_1e_1+\ldots+\alpha_ne_n$. Reamintim că am notat $v_B=\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}$ iar prin $\widetilde{v}_B={}^tv_B=(\alpha_1, \ldots, \alpha_n)$.

Următoarea observație este imediată şi foarte utilă:

Observația 2.3. Dacă $v_1, v_2, \ldots, v_n\in V$ şi $v_i=\sum_{j=1}^{n}a_{ij}e_j$, $1\le i\le n$, atunci $\{v_1, \ldots, v_n\}$ formează o nouă bază pentru V dacă şi numai dacă

$$\begin{vmatrix}a_{11} & a_{12} & \ldots & a_{1n}\\ a_{21} & a_{22} & \ldots & a_{2n}\\ \ldots & \ldots & \ldots & \ldots\\ a_{n1} & a_{n2} & \ldots & a_{nn}\end{vmatrix}\neq 0.$$

În continuare vom prezenta un rezultat fundamental pentru metodele numerice ale algebrei liniare cunoscut sub numele de *lema substituției*.

Lema 2.4. (*Lema substituției*) Fie V un K-spațiu vectorial de dimensiune finită, $B=\{e_1, \ldots, e_n\}\subset V$ o bază a lui V, $v=\alpha_1e_1+\ldots+\alpha_ne_n\in V$ iar pentru $1\le i\le n$ notăm prin $B_i=\{e_1, \ldots, e_{i-1}, v, e_{i+1}, \ldots, e_n\}$. Atunci pentru $1\le i\le n$:

(i) B_i formează o nouă bază pentru V dacă şi numai dacă $\alpha_i\neq 0$

(ii) Dacă $\alpha_i\neq 0$ şi pentru $x\in V$, $\widetilde{x}_B=(\lambda_1, \ldots, \lambda_n)$, atunci $\widetilde{x}_{B_i}=(\lambda'_1, \ldots, \lambda'_n)$ unde $\lambda'_i=\lambda_i/\alpha_i$ iar $\lambda'_j=\lambda_j-\alpha_j\lambda_i/\alpha_i$ pentru $1\le j\le n$, $j\neq i$ (unde pentru a, $b\in K$, $b\neq 0$ prin a / b desemnăm elementul ab^{-1}).

Demonstrație. (i). Determinantul coordonatelor vectorilor din B_i în baza B este:

$$\begin{vmatrix}1 & 0 & \ldots & \ldots & \ldots & 0\\ 0 & 1 & \ldots & \ldots & \ldots & 0\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\ 0 & 0 & \ldots & \alpha_i & \ldots & 0\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\ 0 & 0 & \ldots & \ldots & \ldots & 1\end{vmatrix}=\alpha_i$$

şi acum totul rezultă din Observația 7.3..

(ii). Fie $x\in V$, $x=\lambda_1e_1+\ldots+\lambda_ie_i+\ldots+\lambda_ne_n$.

Din $v=\alpha_1e_1+\ldots+\alpha_ie_i+\ldots+\alpha_ne_n$ deducem imediat că

$\alpha_i e_i = v - \alpha_1 e_1 - \ldots - \alpha_{i-1} e_{i-1} - \alpha_{i+1} e_{i+1} - \ldots - \alpha_n e_n$,

deci $e_i = (1/\alpha_i)v - (\alpha_1/\alpha_i)e_1 - \ldots - (\alpha_{i-1}/\alpha_i)e_{i-1} - (\alpha_{i+1}/\alpha_i)e_{i+1} - \ldots - (\alpha_n/\alpha_i)e_n$ şi astfel $x=\lambda_1 e_1+\ldots+\lambda_i e_i+\ldots+\lambda_n e_n = \lambda_1 e_1+\ldots+\lambda_i [(1/\alpha_i)v - (\alpha_1/\alpha_i)e_1 - \ldots - -(\alpha_{i-1}/\alpha_i)e_{i-1} - (\alpha_{i+1}/\alpha_i)e_{i+1} - \ldots - (\alpha_n/\alpha_i)e_n]+\ldots+ \lambda_n e_n = [\lambda_1 - (\lambda_i\alpha_1)/\alpha_i]e_1 + \ldots + [\lambda_{i-1} - (\lambda_i\alpha_{i-1})/\alpha_i]e_{i-1} + (\lambda_i/\alpha_i)v + [\lambda_{i+1} - (\lambda_i\alpha_{i+1})/\alpha_i]e_{i+1} + \ldots + [\lambda_n - -(\lambda_i\alpha_n)/\alpha_i]\, e_n$, de unde deducem imediat formula din enunț. ■

În practică, lema substituției se aplică punând în evidență următorul tabel:

B	v	x
e_1	α_1	λ_1
…	…	…
e_i	α_i	λ_i
…	…	…
e_j	α_j	λ_j
…	…	…
e_n	α_n	λ_n
e_1	0	$\lambda'_1 = \lambda_1 - (\alpha_1\lambda_1) / \alpha_1$
…	…	……..
v	1	$\lambda'_i = \lambda_i / \alpha_i$
…	…	……..
e_j	0	$\lambda'_j = \lambda_j - (\alpha_j\lambda_i) / \alpha_i$
…	…	……..
e_n	0	$\lambda'_n = \lambda_n - (\alpha_n\lambda_i) / \alpha_i$

În cazul în care $\alpha_i \neq 0$, elementul α_i se va numi *pivot.*

Se observă deci că noile coordonate ale lui x în baza B_i se pun în evidență în tabelul de mai sus astfel:

1) Pe linia i a pivotului împărțim toate elemntele la pivotul α_i.

2) Pe oricare altă linie j cu $j\neq i$ coordonata de ordin j a lui x în noua bază B_i se obține după regula: „*vechea coordonată minus produsul proiecțiilor împărțit la pivot*" (interpretând pe α_j şi λ_i ca fiind „proiecțiile" pivotului α_i pe linia şi coloana pivotului). În anumite lucrări, această operație este cunoscută sub numele de „*regula dreptunghiului*" deoarece pentru $i\neq j$ putem scrie

$$\lambda'_j=\lambda_j-(\alpha_j\lambda_i)/\alpha_i=\left(\frac{1}{\alpha_i}\right)\det\begin{pmatrix}\alpha_i & \lambda_i\\ \alpha_j & \lambda_j\end{pmatrix}$$

şi astfel se obține „dreptunghiul" $\Delta_{ij}=\det\begin{pmatrix}\alpha_i & \lambda_i\\ \alpha_j & \lambda_j\end{pmatrix}$ şi regula de obținere a lui λ'_j se poate enunța astfel: „*produsul elementelor de pe diagonala principală a lui Δ_{ij} minus produsul elementelor de pe diagonala secundară a lui Δ_{ij} şi ceea ce se obține se împarte la pivot*".

Ca o primă aplicație a lemei substituției vom stabili dacă un anumit număr de vectori din V sunt sau nu liniar independenți.

Pentru aceasta vedem cîți dintre aceşti vectori pot înlocui vectorii din baza inițială (cu ajutorul lemei substituției) şi cîți vor verifica această condiție atîția vor fi liniar independenți. În mod evident, dacă numărul acestora coincide cu dimensiunea lui V, atunci ei vor forma o nouă bază pentru V.

De exemplu în $\mathbb{R}^3$ să considerăm baza canonică $e_1=(1, 0, 0)$, $e_2=(0, 1, 0)$, $e_3=(0, 0, 1)$ şi vectorii $v_1=(3, -2, 1)$, $v_2=(1, -1, 0)$, $v_3=(-1, 1, 1)$ şi $v=(1, 2, 3)$. Ne propunem să vedem dacă vectorii v_1, v_2, v_3 formează o nouă bază pentru $\mathbb{R}^3$ în care caz să deducem şi coordonatele lui v în această bază.

Ținând cont de cele stabilite mai înainte facem o serie de calcule puse sub forma următorului tabel:

B	v_1	v_2	v_3	v
e_1	③	1	-1	1
e_2	-2	-1	1	2
e_3	1	0	1	3
v_1	1	1/3	-1/3	1/3
e_2	0	-1/3	1/3	8/3
e_3	0	-1/3	4/3	8/3
v_1	1	0	0	3
v_2	0	1	-1	-8
e_3	0	0	①	0
v_1	1	0	0	3
v_2	0	1	0	-8
v_3	0	0	1	0

În concluzie, vectorii $\{v_1, v_2, v_3\}$ formează o nouă bază pentru $\mathbb{R}^3$ iar coordonatele lui v în această bază sunt 3, -8, 0.

Într-adevăr, $3\cdot v_1 + (-8)\cdot v_2 + 0\cdot v_3 = 3\cdot(3, -2, 1) - 8\cdot(1, -1, 0) =$ $=(9, -6, 3) + (-8, 8, 0) = (1, 2, 3) = v$.

Pe parcursul acestei lucrări vom mai prezenta şi alte aplicaţii ale lemei substituţiei.

CURSUL nr. 14

Aplicaţii liniare

Definiţia 1.1. Fie V şi W două K- spaţii vectoriale. O funcţie f:M→N se zice *aplicaţie liniară* dacă

(i) f(x+y)=f(x)+f(y)

(ii) f(ax)=af(x), oricare ar fi x, y∈V şi a∈K.

Observaţia 1.2. 1. Se verifică imediat că dacă M şi N sunt două K-spaţii vectoriale, atunci f:M→N este aplicaţie liniară dacă şi numai dacă f(ax+by)=af(x)+bf(y), oricare ar fi x, y∈M şi a, b∈K.

Deoarece în particular f este morfism de grupuri aditive deducem că f(0)=0 şi f(-x)=-f(x), oricare ar fi x∈M.

2. Un morfism de K-spaţii vectoriale f:M→M se zice *endomorfism* al lui M; în particular 1_M:M→M, 1_M(x)=x, oricare ar fi x∈M este endomorfism al lui M (numit *endomorfismul identic al lui M*).

3. Dacă M şi N sunt două K-spaţii vectoriale, atunci funcţia **0**:M→N, **0**(x)=0, oricare ar fi x∈M este morfism de module numit *morfismul nul*.

4. Dacă **0** este un K-spaţiu vectorial nul nul şi M un K-spaţiu vectorial, atunci morfismul nul este singura aplicaţe liniară de la **0** la M ca şi de la M la **0**.

Pentru două K-spaţii vectoriale M şi N vom nota

$\mathbf{Hom_K}(M, N)=\{f:M\to N \mid f$ este aplicaţie liniară$\}$

iar pentru f, g∈$\mathbf{Hom}_K(M, N)$ definim

f+g:M→N prin (f+g)(x)=f(x)+g(x), oricare ar fi x∈M.

Propoziția 1..3. ($\mathbf{Hom_K}(M, N), +$) este grup abelian.

Demonstrație. Se verifică imediat că adunarea morfismelor este asociativă, comutativă şi admite morfismul nul **0**:M→N ca element neutru. Pentru f∈$\mathbf{Hom_K}$(M, N), fie –f:M→N dată prin (–f)(x)=-f(x), oricare ar fi x∈M. Deoarece pentru orice x, y∈M şi a, b∈A avem (–f)(ax+by)=-f(ax+by)=-(af(x)+bf(y))=-af(x)-bf(y)=a(-f(x))+b(-f(y)) deducem că -f∈$\mathbf{Hom_K}$(M, N) şi cum f+(-f)=(-f)+f=**0** rezultă că –f este opusul lui f în $\mathbf{Hom_K}$(M, N). ■

Propoziția 1.4. Fie M, N, P trei K-spații vectoriale şi f∈$\mathbf{Hom_K}$(M, N), g∈$\mathbf{Hom_K}$(N, P). Atunci g∘f∈$\mathbf{Hom_K}$(M, P).

Demonstrație. Într-adevăr, dacă x, y∈M şi a, b∈A atunci (g∘f)(ax+by)=g(f(ax+by))=g(af(x)+bf(y))=ag(f(x))+bg(f(y))=a(g∘f)(x)++b(g∘f)(y), de unde concluzia că g∘f∈$\mathbf{Hom_K}$(M, P).■

Propoziția 1.5. Fie M, N două K-spații vectoriale f∈$\mathbf{Hom_K}$(M, N). Atunci:

(i) M′∈$\mathbf{L_K}$(M)⇒f (M′)∈$\mathbf{L_K}$(N)

(ii) N′∈$\mathbf{L_K}$(N)⇒$\mathbf{f^{-1}}$(N′)∈$\mathbf{L_K}$(M).

Demonstrație. (i). Ținem cont de Propoziția 1.5. iar pentru aceasta fie x′=f(x), y′=f(y) din f(M′) (cu x, y∈M′) şi a, b∈K. Deoarece ax′+ay′=af(x)+bf(y)=f(ax+by)∈f(M′) (căci ax+by∈M′) deducem că f(M′)∈$\mathbf{L_K}$(N).

(ii). se probează analog cu (i). ■

Propoziția 1.5. ne permite să dăm următoarea definiție:

Definiția 1.6. Fie M, N două A-module stângi iar f∈$\mathbf{Hom_K}$(M, N). Prin:

i) ***Imaginea lui f*** **(notată Im(f)) înțelegem Im(f)=f(M)**

ii) ***Nucleul lui f*** **(notat Ker(f)) înțelegem**

Ker(f)=$\mathbf{f^{-1}}$(0)={x∈M|f(x)=0}

Observația 1.8. Dacă f:M→N este un izomorfism de K-spații vectoriale ,vom spune despre M şi N că sunt *izomorfe* şi vom scrie M≈N.

Un endomorfism al lui M ce este izomorfism se zice *automorfism* al lui M. Notăm prin **End**(M) (respectiv **Aut**(M)) mulțimea endomorfismelor (automorfismelor) lui M. Se verifică imediat prin calcul că (**End**(M), +, ∘) este inel numit *inelul endomorfismelor* lui M (unde a doua lege de compoziție este compunerea endomorfismelor !).

Propoziția 1.9. (i) Dacă $\mathbf{ind_K}$X şi f este monomorfism, atunci $\mathbf{ind_A}$Y

(ii) Dacă $\mathbf{ind_A}$Y, atunci $\mathbf{ind_K}$X

(iii) Dacă M=(X) şi f este epimorfism, atunci N=(Y)

(iv) Dacă N=(Y), atunci f este epimorfism

(v) Dacă f este izomorfism, atunci X este bază a lui M dacă şi numai dacă Y este bază a lui N.

Demonstrație. (i). Fie I′⊆I finită a.î. $\sum_{i\in I'} a_i y_i = 0$ cu a_i∈K, pentru i∈I′. Atunci $f\left(\sum_{i\in I'} a_i x_i\right) = \sum_{i\in I'} a_i f(x_i) = \sum_{i\in I'} a_i y_i = 0$ şi cum f este ca funcție o injecție deducem că $\sum_{i\in I'} a_i x_i = 0$. Cum $\mathrm{ind_K}$X deducem că a_i=0 pentru orice i∈I′, adică $\mathrm{ind_K}$Y.

(ii). Analog ca la (i).

(iii). Fie y∈N. Cum f este epimorfism, există x∈M a.î. f(x)=y. Deoarece M=(X), există $I'\subseteq I$ finită a.î. $x=\sum_{i\in I'} a_i x_i$ cu $a_i\in K$, pentru $i\in I'$. Atunci $y=f(x)=\sum_{i\in I'} a_i f(x_i)=\sum_{i\in I'} a_i y_i$, de unde concluzia că N=(Y).

(iv). Dacă y∈N, atunci cum N=(Y) există $I'\subseteq I$ finită a.î. $y=\sum_{i\in I'} a_i y_i$ cu $a_i\in K$. Cum $y_i=f(x_i)$ obținem că $y=f\left(\sum_{i\in I'} a_i x_i\right)$, adică f este surjecție.

(v). Rezultă imediat din (i)-(iv). ■

Teorema 2.20. (*a defectului*) Fie V şi W două K-spații vectoriale de dimensiuni finite iar $f\in Hom_K(V, W)$. Atunci:

$$\dim_K Ker(f)+\dim_K Im(f)=\dim_K V.$$

Demonstrație. Fie $(v_i)_{1\le i\le n}$ bază pentru Ker(f) iar $(w_j)_{1\le j\le m}$ bază pentru Im(f). Alegem $(v_j')_{1\le i\le m}\subset V$ a.î. $f(v_j')=w_j$ pentru orice $1\le j\le m$.

Vom demonstra că $B=\{v_1,\dots,v_n, v_1', \dots,v_m'\}$ este o bază pentru V şi astfel teorema va fi demonstrată.

Să arătăm la început $ind_K B$ iar pentru aceasta fie $\alpha_1,\dots,\alpha_n, \beta_1,\dots,\beta_m\in K$ a.î. $\alpha_1v_1+\dots+\alpha_nv_n+\beta_1v_1'+\dots+\beta_mv_m'=0$. Deducem că $\alpha_1f(v_1)+\dots+\alpha_nf(v_n)+\beta_1f(v_1')+\dots+\beta_mf(v_m')=0$ sau $\beta_1w_1+\dots+\beta_mw_m=0$, de unde $\beta_1=\dots=\beta_m=0$.

Atunci $\alpha_1v_1+\dots+\alpha_nv_n=0$, de unde şi $\alpha_1=\dots=\alpha_n=0$.

Pentru a arăta că B este şi sistem de generatori pentru V (adică (B)=V), fie x∈V. Atunci f(x)∈Im(f) şi deci există $\beta_1,\dots,\beta_m\in K$ a.î. $f(x)=\beta_1w_1+\dots+\beta_mw_m=\beta_1f(v_1')+\dots+\beta_mf(v_m')=f(\beta_1v_1'+\dots+\beta_mv_m')$, de unde concluzia că $x-(\beta_1v_1'+\dots+\beta_mv_m')\in Ker(f)$, adică există $\alpha_1,\dots,\alpha_n\in K$ a.î. $x-(\beta_1v_1'+\dots+\beta_mv_m')=\alpha_1v_1+\dots+\alpha_nv_n\Leftrightarrow x=\alpha_1v_1+\dots+\alpha_nv_n+\beta_1v_1'+\dots+\beta_mv_m'$. ■

2.Matricea ataşată unei apicații liniare între două spații vectoriale de dimensiuni finite; formula de schimbare a acesteia la schimbarea bazelor.

Fie acum V şi V′ două K-spații vectoriale de dimensiuni finite, $B=\{e_1, \dots, e_m\}$ o bază a lui V iar $B'=\{e_1',\dots, e_n'\}$ o bază ale lui V′ iar $f:V\to V'$ o aplicație liniară.

Atunci, există elementele $a_{ij}\in K$ $(1\le i\le m, 1\le j\le n)$ a.î.:

$$\begin{aligned}
f(e_1)&=a_{11}e_1' + a_{12}e_2' + \dots + a_{1n}e_n'\\
f(e_2)&=a_{21}e_1' + a_{22}e_2' + \dots + a_{2n}e'_n\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
f(e_m)&=a_{m1}e_1' + a_{m2}e_2' + \dots + a_{mn}e_n' .
\end{aligned}$$

Definiția 2.1. Matricea

$$\mathbf{M_f(B, B')}=\begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1}\\ a_{12} & a_{22} & \dots & a_{m2}\\ \dots & \dots & \dots & \dots\\ a_{1n} & a_{2n} & \dots & a_{mn}\end{pmatrix}\in\mathbf{M_{n,m}(K)}$$

poartă numele de *matricea asociată lui f relativă la perechea de baze (B, B′)* .

Propoziția 2.2. Dacă V şi V′ sunt două K-spații vectoriale de dimensiuni finite, de baze B=$\{e_1, \ldots, e_m\}$ şi respectiv B′=$\{e_1', \ldots, e_n'\}$, atunci oricare ar fi f, g∈$\mathbf{Hom_K(V, V')}$ şi a∈K avem:

$$\mathbf{M_{f+g}(B, B')=M_f(B, B')+ M_g(B, B')} \quad \textbf{iar}$$

$$\mathbf{M_{a\,f}(B, B')=a\cdot M_f(B, B').}$$

Demonstrație. Dacă alegem $M_f(B, B')=(a_{ij})_{\substack{1\le i\le n\\ 1\le j\le m}}$ şi $M_g(B, B')=(b_{ij})_{\substack{1\le i\le n\\ 1\le j\le m}}$, atunci avem egalitățile

$f(e_j)=\sum_{i=1}^{n} a_{ij}e_i'$ şi $g(e_j)=\sum_{i=1}^{n} b_{ij}e_i'$, $1\le j\le m$.

Egalitățile din enunț rezultă imediat ținând cont că pentru orice $1\le j\le m$ avem egalitățile:

$$(f+g)(e_j)=f(e_j)+g(e_j)=\sum_{i=1}^{n} a_{ij}e_i' +\sum_{i=1}^{n} b_{ij}e_i' =\sum_{i=1}^{n}(a_{ij}+b_{ij})e_i' \text{ şi}$$

$$(af)(e_j)=a\cdot f(e_j)=a\cdot\sum_{i=1}^{n} a_{ij}e_i' =\sum_{i=1}^{n}(a\cdot a_{ij})e_i' . \blacksquare$$

Propoziția 2.3. FieV, V′, V′′ trei K-spații vectoriale de dimensiuni finite, de baze B, B′ şi B′′. Atunci oricare ar fi f∈$\mathbf{Hom_K(V, V')}$ şi g∈$\mathbf{Hom_K(V', V'')}$ avem

$$\mathbf{M_{g\circ f}(B, B'')=M_g(B', B'')\cdot M_f(B, B').}$$

Demonstrație. Alegem B=$\{e_1, \ldots, e_m\}$, B′=$\{e_1', \ldots e_n'\}$, B′′=$\{e_1'', \ldots e_p''\}$, $M_f(B, B')=(a_{ij})_{\substack{1\le i\le n\\ 1\le j\le m}}$ şi $M_g(B', B'')=(b_{ij})_{\substack{1\le i\le p\\ 1\le j\le n}}$.

Acum, egalitatea din enunț rezultă imediat deoarece pentru orice $1\le j\le m$ avem $(g\circ f)(e_j)=g(f(e_j))=$

$$=g\left(\sum_{k=1}^{n} a_{kj}e_k'\right)=\sum_{k=1}^{n} a_{kj}g\left(e_k'\right)=\sum_{k=1}^{n} a_{kj}\left(\sum_{i=1}^{p} b_{ik}e_i''\right)=\sum_{i=1}^{p}\left(\sum_{k=1}^{n} b_{ik}a_{kj}\right)e_i'' . \blacksquare$$

Fie acum V şi V′ sunt două K-spații vectoriale de dimensiuni finite de baze B=$\{e_1, \ldots, e_m\}$ şi respectiv B′=$\{e_1', \ldots, e_n'\}$. Dacă definim $\varphi:\mathbf{Hom_K}(V, V')\to M_{n,m}(K)$ prin $\varphi(f)=M_f(B, B')$ pentru orice f∈$\mathbf{Hom_K}(V, V')$, atunci din Propoziția 6.4. deducem că φ este aplicație liniară . Cum în mod evident φ este şi bijecție, deducem următorul rezultat:

Corolar 2.4. $\mathbf{Hom_K(L, L')\approx M_{n,m}(K)}$ (izomorfism de spații vectoriale).

Din Propoziția 2.2. şi Propoziția 2.3. deducem imediat că dacă V este un K-spațiu vectorial având baza B=$\{e_1, \ldots, e_n\}$, atunci definind $\psi:\mathbf{End_K}(V)\to M_n(V)$ prin $\psi(f)=M_f(B, B)$, ψ este morfism de inele. Deoarece ψ este în mod evident şi bijecție deducem un alt rezultat asemănător celui de mai înainte:

Corolar 2.5. (i) $\mathbf{End_K(L)\approx M_n(K)}$ (izomorfism de inele)

(ii) f∈$\mathbf{End_K(V)}$ este inversabil (adică este izomorfism de K-spații vectoriale) dacă şi numai dacă matricea $\mathbf{M_f(B, B)}$ este inversabilă în $\mathbf{M_n(K)}$.

Propoziția 2.6. Fie V şi V′ două K-spații vectoriale de dimensiuni finite de baze B=$\{e_1, \ldots, e_m\}$ şi respectiv B′=$\{e_1', \ldots, e_n'\}$ iar g∈$\mathbf{Hom_K(L, L')}$.

Dacă C=$\{f_1, \ldots, f_m\}$ şi C′=$\{f_1', \ldots, f_m'\}$ reprezintă o altă pereche de baze pentru L şi respectiv L′, atunci

$$\mathbf{M_g(C, C')=M(B', C')^{-1}\cdot M_g(B, B')\cdot M(B, C).}$$

Demonstrație. Dacă alegem $M(B, C)=(u_{ij})_{1\le i, j\le m}$,

$M(B', C')=(v_{ij})_{1\le i,j\le n}$, $M_g(B, B')=(a_{ij})_{\substack{1\le i\le n\\ 1\le j\le m}}$, $M_g(C, C')=\left(a_{ij}'\right)_{\substack{1\le i\le n\\ 1\le j\le m}}$, atunci avem egalitățile: $f_i=\sum_{j=1}^{n}u_{ji}e_j$ $(1\le i\le m)$, $f_i'=\sum_{j=1}^{n}v_{ji}e_j'$ $(1\le i\le n)$, $g(e_i)=\sum_{j=1}^{n}a_{ji}e_j'$ $(1\le i\le m)$ şi $g(f_i)=\sum_{j=1}^{n}a_{ji}'f_j'$ $(1\le i\le m)$.

Deducem imediat că pentru orice $1\le j\le m$ avem

$$g(f_j)=\sum_{k=1}^{n}a_{kj}'f_k'=\sum_{k=1}^{n}a_{kj}'\left(\sum_{i=1}^{n}v_{ik}e_i'\right)=\sum_{i=1}^{n}\left(\sum_{k=1}^{n}v_{ik}a_{kj}'\right)e_i'$$

iar pe de altă parte

$$g(f_i)=g\left(\sum_{k=1}^{n}u_{kj}e_k\right)=\sum_{k=1}^{m}u_{kj}g(e_k)=\sum_{k=1}^{m}u_{kj}\left(\sum_{i=1}^{n}a_{ik}e_i'\right)=\sum_{i=1}^{n}\left(\sum_{k=1}^{m}a_{ik}u_{kj}\right)e_i',$$

de unde egalitățile $\sum_{k=1}^{n}v_{ik}a_{kj}'=\sum_{k=1}^{m}a_{ik}u_{kj}$ oricare ar fi $1\le i\le n$ şi $1\le j\le m$. Aceste ultime egalități ne arată că avem egalitatea matriceală

$$M(B', C')\cdot M_g(C, C')=M_g(B, B')\cdot M(B, C)$$

echivalentă cu cea din enunț. ■

Corolar 2.7. Dacă L este un A-modul liber de rang finit având două baze B şi B′ atunci pentru orice $f\in End_A(L)$ avem:

$$\mathbf{M_g(B', B')=M(B, B')^{-1}\cdot M_g(B, B)\cdot M(B, B').}$$

∗∗∗