

# ALGEBRĂ

(Îndrumar pentru examenul licență valabil începând cu sesiunea de finalizare a studiilor iulie 2013)

## CUPRINS

Pentru specializările **Matematică** și **Matematică informatică**:

<b>1</b>	<b>Introducere</b>	<b>1</b>
<b>2</b>	<b>Grupuri, inele și corpuri (de Ioan Purdea și Cosmin Pelea)</b>	<b>2</b>
<b>2.1</b>	<b>Grupuri</b>	<b>2</b>
<b>2.2</b>	<b>Exerciții rezolvate</b>	<b>10</b>
<b>2.3</b>	<b>Inele și corpuri</b>	<b>13</b>
<b>2.4</b>	<b>Exerciții rezolvate</b>	<b>20</b>
<b>2.5</b>	<b>Exerciții propuse</b>	<b>23</b>
<b>3</b>	<b>Spații vectoriale (de Ioan Purdea și Cosmin Pelea)</b>	<b>23</b>
<b>3.1</b>	<b>Spații, subspații, transformări liniare</b>	<b>23</b>
<b>3.2</b>	<b>Exerciții rezolvate</b>	<b>33</b>
<b>3.3</b>	<b>Baze. Dimensiune</b>	<b>33</b>
<b>3.4</b>	<b>Exerciții rezolvate</b>	<b>41</b>
<b>3.5</b>	<b>Exerciții propuse</b>	<b>42</b>
<b>4</b>	<b>Transformări liniare și matrici, sisteme de ecuații liniare (de Ioan Purdea și Cosmin Pelea)</b>	<b>43</b>
<b>4.1</b>	<b>Transformări liniare și matrici</b>	<b>43</b>
<b>4.2</b>	<b>Exerciții rezolvate</b>	<b>47</b>
<b>4.3</b>	<b>Sisteme de ecuații liniare</b>	<b>50</b>
<b>4.4</b>	<b>Exerciții rezolvate</b>	<b>57</b>
<b>4.5</b>	<b>Exerciții propuse</b>	<b>62</b>

Numai pentru specializarea **Matematică**:

<b>5 Noțiuni de aritmetica numerelor întregi (de Simion Breaz și Cosmin Pelea)</b>	<b>63</b>
<b>5.1 Teorema împărțirii cu rest în <math>\mathbb{Z}</math></b>	<b>63</b>
<b>5.2 Exerciții rezolvate</b>	<b>65</b>
<b>5.3 Divizibilitatea în <math>\mathbb{Z}</math></b>	<b>66</b>
<b>5.4 Exerciții rezolvate</b>	<b>71</b>
<b>5.5 Numere prime. Teorema fundamentală a aritmeticii</b>	<b>73</b>
<b>5.6 Exerciții rezolvate</b>	<b>76</b>
<b>5.7 Exerciții propuse</b>	<b>77</b>
<b>Bibliografie (pentru ambele specializări)</b>	<b>77</b>

# 1 Introducere

În realizarea părții de algebră a acestei broșuri s-a încercat alcătuirea unui material care să poată fi utilizat independent de alte surse bibliografice. Totuși, nu am reușit pe deplin acest lucru, așa că recomandăm studenților ca acolo unde au nevoie de completări să apeleze la titlurile din bibliografia de la finalul acestui material. În acest sens, precizăm că demonstrația Teoremei 3.32 folosește instrumente care nu au fost predate în liceu și nu sunt discutate aici, de aceea am menționat alăturat, într-o paranteză, că este facultativă. De asemenea, discuția despre sisteme de ecuații liniare se bazează pe câteva rezultate referitoare la determinanți și rangul unei matrice cu coeficienți într-un corp comutativ  $K$  pe care din motive de spațiu nu le putem prezenta aici în detaliu. Ele au fost prezentate în liceu în cazul  $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$  și pot fi găsite în cazul general în capitolul VI din [5]. Din aceste motive am ales ca aici doar să le amintim. De altfel, Secțiunea 4.3 conține destul de puține rezultate teoretice. Am considerat că cititorului îi va fi mai folositoare o abordare în care insistăm mai mult pe descrierea metodelor prezentate de rezolvare a sistemelor și ilustrarea lor prin exerciții rezolvate.

Cele 4 capitole de după Introducere abordează câte o temă care ar putea fi (sau chiar a fost) predată pe durata unui curs de 2 ore. Fiecare dintre aceste capitole corespunde câte unui punct din tematica propusă pentru examenul de licență. Astfel, **tematica propusă pentru specializarea Matematică** este acoperită de **capitolele 2, 3, 4 și 5**, iar **tematica propusă pentru specializarea Matematică informatică** este acoperită de **capitolele 2, 3 și 4** din acest material. Bibliografia de la sfârșit este comună tematicii ambelor specializări.

Dacă numărul de pagini dedicat unor teme este mai mare, aceasta se datorează faptului că s-au adăugat unele explicații și observații pe care le-am considerat importante și care în timpul unui curs pot fi comunicate oral (iar aici nu). De asemenea, numărul de exemple din acest material este, poate, ceva mai mare decât al celor prezentate în sala de curs, acolo existând seminarul ca un ajutor în acest sens. Exceptând, poate, „suplimentul” de explicații și exemple, am căutat să organizăm prezentarea într-o formă cât mai apropiată de cea în care aceste teme au fost predate la cursurile aferente. În ce privește problemele propuse, studenții pot găsi în bibliografia menționată rezolvări sau indicații care să îi ajute în abordarea acestora.

Trebuie menționat că finalizarea acestui material în timp util și în bune condiții nu ar fi fost posibilă fără fișierele sursă ale unor cursuri publicate sau în pregătire puse la dispoziție de domnul profesor Ioan Purdea și domnul conferențiar Simion Breaz. Contribuția subsemnatului a fost aceea de a da un caracter autonom și un aspect unitar (pe cât a permis tematica abordată) părții de algebră a acestei broșuri. Nu excludem posibilitatea ca în material să se fi strecurat erori de tehnoredactare (dintre care unele ar putea să-și lase amprenta asupra corectitudinii unor afirmații). Încurajăm cititorii să ne atragă atenția asupra acelor erori pe care le identifică și apreciem pozitiv toate semnalele care ne vor veni în acest sens.

Cosmin Pelea

## 2 Grupuri, inele și corpuri (de Ioan Purdea și Cosmin Pelea)

### 2.1 Grupuri

**Definiția 2.1.** Fie  $A$  o mulțime. O funcție  $\varphi : A \times A \rightarrow A$  se numește **operație binară** sau **lege de compoziție** pe  $A$ .

Pentru că în acest capitol ne vom ocupa numai de operații binare, le vom numi simplu **operații**. Pentru notarea unei operații se pot folosi simboluri ca  $*$ ,  $\cdot$ ,  $+$  etc. Dacă operația  $\varphi$  este notată cu  $*$ , atunci  $\varphi(a_1, a_2)$  se notează cu  $a_1 * a_2$ . Cel mai des  $\varphi$  se notează **multiplicativ**, adică cu  $\cdot$ , caz în care  $\varphi(a_1, a_2)$  se notează cu  $a_1 \cdot a_2$  sau  $a_1 a_2$ , sau **aditiv**, adică cu  $+$ , caz în care  $\varphi(a_1, a_2)$  se notează cu  $a_1 + a_2$ .

**Exemplele 2.2.** a) Adunarea ( $+$ ) și înmulțirea ( $\cdot$ ) sunt operații în  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$  și  $\mathbb{C}$ , dar nu sunt operații în mulțimea numerelor iraționale.

b) Scăderea este operație în  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  și  $\mathbb{C}$ , dar nu este operație în  $\mathbb{N}$ .

c) Împărțirea este operație în  $\mathbb{Q}^*, \mathbb{R}^*$  și  $\mathbb{C}^*$ , dar nu e operație în  $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{N}, \mathbb{Z}, \mathbb{N}^*$  și  $\mathbb{Z}^*$ .

**Definițiile 2.3.** Fie  $*$  o operație în  $A$ . Spunem că:

i) operația  $*$  este **asociativă** dacă

$$(a_1 * a_2) * a_3 = a_1 * (a_2 * a_3), \quad \forall a_1, a_2, a_3 \in A;$$

ii) operația  $*$  este **comutativă** dacă

$$a_1 * a_2 = a_2 * a_1, \quad \forall a_1, a_2 \in A.$$

**Definițiile 2.4.** Un cuplu  $(A, *)$ , unde  $A$  este o mulțime și  $*$  este operație pe  $A$ , se numește **grupoid**. Un grupoid în care operația este **asociativă** se numește **semigrup**. Un grupoid în care operația este comutativă se numește **grupoid comutativ**.

Uneori, pentru simplificarea notațiilor, grupoidul  $(A, *)$  va fi notat cu  $A$ .

**Definițiile 2.5.** Fie  $*$  o operație în  $A$ . Spunem că operația  $*$  **admite element neutru** dacă există un element  $e \in A$  astfel încât

$$a * e = e * a = a, \quad \forall a \in A.$$

Elementul  $e \in A$  se numește **elementul neutru** al grupoidului  $(A, *)$ . Într-un grupoid care are un element neutru  $e$ , spunem că un **element**  $a \in A$  este **simetrizabil** dacă există un element  $a' \in A$  astfel încât

$$a * a' = a' * a = e.$$

Elementul  $a'$  se numește **simetricul lui**  $a$ .

**Observațiile 2.6.** a) Într-un grupoid  $(A, *)$  există cel mult un element neutru.

Într-adevăr, dacă nu există element neutru, proprietatea este, evident, adevărată, iar dacă  $e$  și  $f$  ar fi elemente neutre, privindu-l succesiv pe fiecare dintre ele ca element neutru, avem

$$e * f = f \text{ și } e * f = e.$$

Prin urmare,  $e = f$ .

b) Într-un semigrup  $(A, *)$  care are element neutru, există elemente simetrizabile. De exemplu, elementul neutru este simetrizabil și coincide cu simetricul său.

c) Într-un semigrup  $(A, *)$  care are element neutru, orice element simetrizabil  $a$  are un singur simetric.

Într-adevăr, dacă  $e$  este elementul neutru,  $a \in A$  este simetrizabil și  $a'$  și  $a''$  ar fi simetrice ale lui  $a$ , avem

$$a' * a * a'' = a' * (a * a'') = a' * e = a' \text{ și } a' * a * a'' = (a' * a) * a'' = e * a'' = a''.$$

Prin urmare,  $a' = a''$ .

În notație aditivă, elementul neutru este notat cu 0 și numit **element nul (sau zero)**, iar simetricul unui element  $a$  (dacă există) este notat cu  $-a$  și este numit **opusul lui  $a$** . În notație multiplicativă, elementul neutru este notat cu 1 și numit **element unitate**, iar simetricul unui element  $a$  (dacă există) este notat cu  $a^{-1}$  și e numit **inversul lui  $a$** .

**Definițiile 2.7.** Un semigrup  $(A, *)$  cu element neutru se numește **monoid**. Dacă, în plus, operația  $*$  este comutativă spunem că  $(A, *)$  este un **monoid comutativ**. Un monoid  $(A, *)$  se numește **grup** dacă toate elementele sale sunt simetrizabile. Dacă, în plus, operația  $*$  este comutativă spunem că  $(A, *)$  este **grup comutativ** sau **grup abelian**.

**Exemplele 2.8.** a)  $(\mathbb{N}, +)$  și  $(\mathbb{Z}, \cdot)$  sunt monoizi comutativi, dar nu sunt grupuri.

b)  $(\mathbb{Q}, \cdot)$ ,  $(\mathbb{R}, \cdot)$ ,  $(\mathbb{C}, \cdot)$  sunt monoizi comutativi care nu sunt grupuri deoarece 0 nu este element inversabil.

c)  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$ ,  $(\mathbb{Q}^*, \cdot)$ ,  $(\mathbb{R}^*, \cdot)$ ,  $(\mathbb{C}^*, \cdot)$  sunt grupuri abeliene.

d) Fie  $M$  o mulțime și  $M^M = \{f \mid f : M \rightarrow M\}$ . Perechea  $(M^M, \circ)$ , unde  $\circ$  este compunerea funcțiilor, este un monoid. Elementul neutru în acest monoid este funcția identică  $1_M : M \rightarrow M$ ,  $1_M(x) = x$ .

**Observațiile 2.9.** a) Din Observațiile 2.6 a) și c) se deduc imediat următoarele:

1) Într-un monoid există un singur element neutru.

2) Într-un grup, fiecare element are un singur invers.

b) Definiția grupului poate fi rescrisă astfel: Un grupoid  $(A, *)$  se numește **grup** dacă au loc următoarele condiții:

(i)  $(a_1 * a_2) * a_3 = a_1 * (a_2 * a_3)$ ,  $\forall a_1, a_2, a_3 \in A$  ( $*$  este asociativă);

(ii)  $\exists e \in A$ ,  $\forall a \in A : a * e = e * a = a$  ( $*$  admite element neutru);

(iii)  $\forall a \in A$ ,  $\exists a' \in A : a * a' = a' * a = e$  (toate elementele lui  $A$  sunt simetrizabile).

c) Atragem atenția asupra câtorva greșeli care apar frecvent în definiția grupului:

1) Condiția (iii) de mai sus nu vorbește despre „existența elementelor simetrizabile”, ci despre faptul că toate elementele sunt simetrizabile. După cum arată Observația 2.6 b), elemente simetrizabile există și în monoizi care nu sunt grupuri, dar acolo există și elemente care nu sunt simetrizabile, iar în grupuri, nu.

2) Ordinea cuantificatorilor în scrierea formală a proprietăților (ii) și (iii) este esențială. În general, cuantificatorii  $\exists$  și  $\forall$  nu comută, iar aici permutarea lor duce la condiții mult diferite de cele din definiția grupului.

3) Introducerea unicității elementului neutru și a unicității simetricului fiecărui element în definiția grupului nu sunt necesare. După cum am văzut la a), acestea sunt consecințe imediate ale definiției grupului și trebuie privite ca atare.

În continuarea acestei secțiuni, cu rare excepții, operația dintr-un grup va fi notată multiplicativ. Dacă  $(A, \cdot)$  este un semigrup,  $a \in A$  și  $n \in \mathbb{N}^*$ , atunci  $a^n$  se definește inductiv astfel:  $a^1 = a$ , iar dacă  $n > 1$ , atunci

$$a^n = a^{n-1} \cdot a = \underbrace{a \cdot \cdots \cdot a}_{n \text{ factori}}.$$

Dacă semigrupul  $(A, \cdot)$  este monoid și  $a \in A$  se definește

$$a^0 = 1,$$

iar dacă, în plus,  $a$  e inversabil (simetrizabil), atunci se extinde noțiunea de putere a lui  $a$  la cazul exponenților negativi. Mai exact, dacă  $a \in A$  este inversabil și  $n \in \mathbb{N}^*$ , atunci

$$a^{-n} = (a^{-1})^n.$$

Dacă operația din semigrup este notată cu  $+$ , atunci în locul notației  $a^n$  se folosește notația  $na$ .

**Propoziția 2.10. (Reguli de calcul într-un grup)**

Fie  $(G, \cdot)$  un grup. Se verifică ușor următoarele proprietăți:

1) Pentru orice  $a, b \in G$  avem

$$(a^{-1})^{-1} = a, (ab)^{-1} = b^{-1}a^{-1},$$

$$ab = ba \Leftrightarrow (ab)^{-1} = a^{-1}b^{-1}.$$

2) Pentru orice  $a, b \in G$  și orice  $m, n \in \mathbb{Z}$  avem:

$$a^m a^n = a^{m+n}, (a^m)^n = a^{mn},$$

$$ab = ba \Rightarrow (ab)^n = a^n b^n.$$

3) În  $G$  se poate simplifica cu orice element, adică pentru orice  $a, x, y \in G$ ,

$$ax = ay \Rightarrow x = y,$$

$$xa = ya \Rightarrow x = y.$$

4) Pentru orice  $a, b \in G$ , fiecare dintre ecuațiile  $ax = b$  și  $ya = b$  are soluție unică în  $G$  (pe  $x = a^{-1}b$ , respectiv  $y = ba^{-1}$ ).

**Corolarul 2.11.** Dacă  $(G, \cdot)$  este grup, atunci pentru orice  $a \in G$  funcțiile  $t_a : G \rightarrow G$ ,  $t_a(x) = ax$  și  $t'_a : G \rightarrow G$ ,  $t'_a(x) = xa$  (numite **translația stângă**, respectiv **translația dreaptă** cu  $a$ ) sunt bijecții.

**Definițiile 2.12.** Fie  $(A, \varphi)$  un grupoid și  $B \subseteq A$ . Vom spune că  $B$  este un **subgrupoid** al lui  $(A, \varphi)$  sau că  $B$  este **parte stabilă** în raport cu  $\varphi$  sau în  $(A, \varphi)$  dacă:

$$b_1, b_2 \in B \Rightarrow \varphi(b_1, b_2) \in B.$$

Dacă  $B$  este stabilă, atunci se poate defini cu ajutorul lui  $\varphi$ , o operație pe  $B$  astfel:

$$\varphi' : B^2 \rightarrow B, \varphi'(b_1, b_2) = \varphi(b_1, b_2).$$

Aceasta se numește **operația indusă** de  $\varphi$  în  $B$  și se notează, de multe ori, tot cu  $\varphi$ .

**Observațiile 2.13.** a) Fie  $(A, \varphi)$  un grupoid,  $B \subseteq A$  o parte stabilă în  $(A, \varphi)$  și  $\varphi'$  operația indusă de  $\varphi$  în  $B$ . Dacă  $\varphi$  este asociativă (comutativă), atunci  $\varphi'$  este asociativă (comutativă). Deci orice parte stabilă  $B$  a unui semigrup  $(A, \varphi)$  este semigrup în raport cu operația indusă de  $\varphi$  în  $B$ , de aceea un subgrupoid al unui semigrup se mai numește **subsemigrup**.

b) Fie  $\varphi_1$  și  $\varphi_2$  două operații definite pe  $A$  și  $B \subseteq A$  stabilă în raport cu  $\varphi_1$  și  $\varphi_2$ , iar  $\varphi'_1$  și  $\varphi'_2$  operațiile induse de  $\varphi_1$  și  $\varphi_2$  în  $B$ . Dacă  $\varphi_1$  este distributivă în raport cu  $\varphi_2$ , adică

$$\varphi_1(a_1, \varphi_2(a_2, a_3)) = \varphi_2(\varphi_1(a_1, a_2), \varphi_1(a_1, a_3))$$

pentru orice  $a_1, a_2, a_3 \in A$ , atunci  $\varphi'_1$  este distributivă în raport cu  $\varphi'_2$ .

c) Existența elementului neutru este o proprietate care, în general, nu „se moștenește” de la un grupoid la o parte stabilă a sa. De exemplu,  $\mathbb{N}^*$  este o parte stabilă în  $(\mathbb{N}, +)$ , dar  $(\mathbb{N}^*, +)$  nu are element neutru.

**Definiția 2.14.** Fie  $(G, \cdot)$  un grup. O submulțime  $H \subseteq G$  se numește **subgrup** al lui  $(G, \cdot)$  dacă verifică condițiile:

i)  $H$  este stabilă în  $(G, \cdot)$ , adică

$$h_1, h_2 \in H \Rightarrow h_1 h_2 \in H;$$

ii)  $H$  este grup în raport cu operația indusă de operația din  $(G, \cdot)$ .

Faptul că  $H$  este subgrup al lui  $(G, \cdot)$  se va nota cu  $H \leq G$ .

**Exemplele 2.15.** a)  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  sunt subgrupuri în  $(\mathbb{C}, +)$ ,  $\mathbb{Z}, \mathbb{Q}$  sunt subgrupuri în  $(\mathbb{R}, +)$  și  $\mathbb{Z}$  este subgrup în  $(\mathbb{Q}, +)$ .

b)  $\mathbb{Q}^*, \mathbb{R}^*$  sunt subgrupuri în  $(\mathbb{C}^*, \cdot)$  și  $\mathbb{Q}^*$  este subgrup în  $(\mathbb{R}^*, \cdot)$ .

c)  $\mathbb{N}$  este un subsemigrup al lui  $(\mathbb{Z}, +)$  care nu este subgrup.

**Observațiile 2.16.** a) Orice subgrup este nevid.

Această afirmație rezultă din ii).

b) Dacă  $H$  este un subgrup al grupului  $(G, \cdot)$ , atunci elementul neutru al lui  $(H, \cdot)$  coincide cu elementul neutru al lui  $(G, \cdot)$ .

Într-adevăr, dacă  $e$ , respectiv 1 este element neutru din  $H$ , respectiv  $G$  și  $h \in H \subseteq G$ , atunci în  $G$  are loc egalitatea

$$eh = h = 1h.$$

Simplificând în  $G$  cu  $h$ , rezultă  $e = 1$ .

c) Dacă  $H$  este un subgrup al grupului  $(G, \cdot)$  și  $h \in H$ , atunci simetricul lui  $h$  în  $(H, \cdot)$  coincide cu simetricul lui  $h$  în  $(G, \cdot)$ .

Într-adevăr, dacă  $h'$ , respectiv  $h^{-1}$  e simetricul lui  $h$  în  $H$ , respectiv  $G$ , din b) avem

$$h'h = e = 1 = h^{-1}h.$$

Privind această egalitate în  $G$  și simplificând cu  $h$ , rezultă  $h' = h^{-1}$ .

De cele mai multe ori e mai ușor să arătăm că o submulțime a unui grup este subgrup aplicând următoarea teoremă.

**Teorema 2.17. (Teorema de caracterizare a subgrupului)**

Fie  $(G, \cdot)$  un grup și  $H \subseteq G$ . Următoarele afirmații sunt echivalente:

- 1)  $H$  este subgrup al lui  $(G, \cdot)$ .
- 2)  $H$  verifică condițiile:
  - $\alpha$ )  $H \neq \emptyset$ ;
  - $\beta$ )  $h_1, h_2 \in H \Rightarrow h_1h_2 \in H$ ;
  - $\gamma$ )  $h \in H \Rightarrow h^{-1} \in H$ .
- 3)  $H$  verifică condițiile:
  - $\alpha$ )  $H \neq \emptyset$ ;
  - $\delta$ )  $h_1, h_2 \in H \Rightarrow h_1h_2^{-1} \in H$ .

*Demonstrație.* 1)  $\Rightarrow$  2). Din Observația 2.16 a) rezultă  $\alpha$ ), iar  $\beta$ ) coincide cu i) și  $\gamma$ ) urmează din Observația 2.16 c).

2)  $\Rightarrow$  3). Folosind pe 2) avem:

$$h_1, h_2 \in H \Rightarrow h_1, h_2^{-1} \in H \Rightarrow h_1h_2^{-1} \in H.$$

Deci condiția  $\delta$ ) este verificată și  $\alpha$ ) este comună.

3)  $\Rightarrow$  1). Dacă în  $\delta$ ) luăm  $h_1 = h_2$  atunci rezultă  $1 \in H$ , iar dacă  $h \in H$  și luăm  $h_1 = 1$  și  $h_2 = h$  atunci  $h^{-1} \in H$ . Folosind acest rezultat și pe  $\delta$ ) avem:

$$h_1, h_2 \in H \Rightarrow h_1, h_2^{-1} \in H \Rightarrow h_1(h_2^{-1})^{-1} = h_1h_2 \in H.$$

Deci operația din  $(G, \cdot)$  induce operație în  $H$ , iar din asociativitatea operației în  $(G, \cdot)$  rezultă asociativitatea operației induse. Acum, din cele de mai sus urmează că  $H$  este subgrup.  $\square$

Practic, când se arată că o submulțime a unui grup este subgrup se verifică 2) sau 3), iar condiția  $\alpha$ ) o înlocuim cu condiția  $1 \in H$ .

**Exemplele 2.18.** a) Dacă  $(G, \cdot)$  este grup, atunci  $G$  și  $\{1\}$  sunt subgrupuri. Un subgrup al lui  $G$  diferit de  $G$  și  $\{1\}$  se numește **subgrup propriu**.

b) Submulțimea  $H = \{z \in \mathbb{C} \mid |z| = 1\}$  a lui  $\mathbb{C}^*$  este un subgrup al lui  $(\mathbb{C}^*, \cdot)$ .

Într-adevăr,  $H \neq \emptyset$  pentru că  $1 \in H$ , adică  $H$  verifică pe  $\alpha$ ). Folosind următoarele proprietăți ale modulului

$$|z_1z_2| = |z_1| \cdot |z_2| \text{ și } |z^{-1}| = |z|^{-1}$$



avem:

$$z_1, z_2 \in H \Rightarrow |z_1| = 1, |z_2| = 1 \Rightarrow |z_1 z_2| = 1 \Rightarrow z_1 z_2 \in H$$

și

$$z \in H \Rightarrow |z| = 1 \Rightarrow |z^{-1}| = 1 \Rightarrow z^{-1} \in H.$$

Deci  $H$  verifică pe  $\alpha), \beta), \gamma)$ , adică  $H$  este subgrup.

c) Fie  $n \in \mathbb{N}$  fixat. Atunci mulțimea  $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$  a multiplilor lui  $n$ , este un subgrup al lui  $(\mathbb{Z}, +)$  deoarece  $n\mathbb{Z} \neq \emptyset$  și diferența a doi multipli de  $n$  este un multiplu de  $n$ . Deci  $n\mathbb{Z}$  verifică pe  $\alpha)$  și  $\delta)$ , adică  $n\mathbb{Z} \leq (\mathbb{Z}, +)$ .

Reamintim că pentru o mulțime finită  $X$ , se notează cu  $|X|$  numărul de elemente al mulțimii  $X$ .

**Teorema 2.19. (Teorema lui Lagrange)** Fie  $G$  un grup finit și  $H \leq G$ . Atunci  $|H|$  divide pe  $|G|$ .

*Demonstrație.* Fie  $\rho_H \subseteq G \times G$ , relația omogenă definită prin

$$x\rho_H y \Leftrightarrow y \in xH,$$

unde  $xH = \{xh \mid h \in H\} \subseteq G$ . Observăm că

$$x\rho_H y \Leftrightarrow x^{-1}y \in H.$$

Demonstrăm că  $\rho_H$  este relație de echivalență. Cum pentru orice  $x \in G$ ,  $x^{-1}x = 1 \in H$ ,

$$\forall x \in G, x\rho_H x,$$

adică  $\rho_H$  este reflexivă. Dacă  $x\rho_H y$  și  $y\rho_H z$  atunci  $x^{-1}y \in H$  și  $y^{-1}z \in H$ . Prin urmare,  $(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$  și rezultă că  $x\rho_H z$ . Așadar,  $\rho_H$  este tranzitivă. Relația  $\rho_H$  este și simetrică, deoarece dacă  $x\rho_H y$ , adică  $x^{-1}y \in H$ , cum  $H$  este subgrup,  $(x^{-1}y)^{-1} = y^{-1}x \in H$ , de unde obținem  $y\rho_H x$ .

Pentru  $x \in G$ , avem

$$\rho_H \langle x \rangle = \{y \in G \mid x\rho_H y\} = \{y \in G \mid x^{-1}y \in H\} = \{y \in G \mid y \in xH\} = xH.$$

Alegând câte un element (și numai unul) din fiecare dintre clasele diferite (și implicit distincte)  $H, xH, yH, \dots$  obținem o submulțime  $X \subseteq G$ . Mulțimea cât și partiția determinată de  $\rho_H$  este

$$G/\rho_H = \{\rho_H \langle x \rangle \mid x \in X\} = \{xH \mid x \in X\},$$

prin urmare

$$G = \bigcup_{x \in X} \rho_H \langle x \rangle = \bigcup_{x \in X} xH.$$

Pentru orice  $x, y \in X$ ,  $x \neq y$  avem  $xH \cap yH = \emptyset$ . Mai mult, pentru orice  $x \in X$ , funcția  $t_x : H \rightarrow xH$ ,  $t_x(h) = xh$  este bijectivă, deci  $|H| = |xH|$ . Atunci

$$|G| = \sum_{x \in X} |xH| = \underbrace{|H| + \dots + |H|}_{|X| \text{ termeni}} = |X||H|,$$

și teorema este demonstrată. □

**Definiția 2.20.** Fie  $(G, *)$ ,  $(G', \perp)$  grupuri. O funcție  $f : G \rightarrow G'$  se numește **omomorfism** dacă

$$f(x_1 * x_2) = f(x_1) \perp f(x_2), \forall x_1, x_2 \in G.$$

Un omomorfism bijectiv se numește **izomorfism**. Un omomorfism al lui  $(G, *)$  în el însuși se numește **endomorfism** al lui  $(G, *)$ . Un izomorfism al lui  $(G, *)$  pe el însuși se numește **automorfism** al lui  $(G, *)$ . Dacă există un izomorfism  $f : G \rightarrow G'$ , atunci vom spune că grupurile  $(G, *)$  și  $(G', \perp)$  sunt izomorfe și vom scrie  $G \simeq G'$  sau  $(G, *) \simeq (G', \perp)$ .

Pentru simplificarea scrierii, revenim la notația multiplicativă a operațiilor.

**Teorema 2.21.** Fie  $(G, \cdot)$  și  $(G', \cdot)$  grupuri, iar  $1$ , respectiv  $1'$  elementul neutru al lui  $(G, \cdot)$ , respectiv  $(G', \cdot)$ . Dacă  $f : G \rightarrow G'$  este omomorfism, atunci

$$f(1) = 1' \tag{1}$$

și

$$f(x^{-1}) = [f(x)]^{-1}, \forall x \in G. \tag{2}$$

*Demonstrație.* Pentru orice  $x \in G$  avem

$$f(1)f(x) = f(1 \cdot x) = f(x) = 1' \cdot f(x),$$

adică  $f(1)f(x) = 1' \cdot f(x)$ , de unde rezultă (1). Folosind pe (1) avem:

$$x^{-1}x = 1 \Rightarrow f(x^{-1})f(x) = 1',$$

de unde urmează (2). □

**Teorema 2.22.** Dacă  $(G, \cdot)$  și  $(G', \cdot)$  sunt grupuri, iar  $f : G \rightarrow G'$  este un izomorfism, atunci  $f^{-1}$  este un izomorfism.

*Demonstrație.* Întrucât inversa unei bijecții este o bijecție, mai trebuie arătat că:

$$f^{-1}(y_1 y_2) = f^{-1}(y_1) f^{-1}(y_2), \forall y_1, y_2 \in G'. \tag{3}$$

Conform definiției funcției  $f^{-1}$ ,  $f^{-1}(y_i)$  este acel element  $x_i \in G$  ( $i = 1, 2$ ) pentru care avem  $f(x_i) = y_i$ , adică

$$f^{-1}(y_i) = x_i \Leftrightarrow f(x_i) = y_i.$$

Deci

$$f^{-1}(y_1) f^{-1}(y_2) = x_1 x_2 \tag{4}$$

Din  $f(x_1 x_2) = f(x_1) f(x_2) = y_1 y_2$  urmează

$$f^{-1}(y_1 y_2) = x_1 x_2. \tag{5}$$

Acum, din (4) și (5) rezultă (3). □

**Corolarul 2.23.** a) Dacă  $(G, \cdot) \simeq (G', \cdot)$  atunci  $(G', \cdot) \simeq (G, \cdot)$ , adică relația  $\simeq$  între grupuri este simetrică.

b) Un omomorfism  $f : G \rightarrow G'$  este izomorfism, dacă și numai dacă există un omomorfism  $g : G' \rightarrow G$  astfel încât  $g \circ f = 1_G$  și  $f \circ g = 1_{G'}$ .

**Teorema 2.24.** Dacă  $(G, \cdot)$ ,  $(G', \cdot)$  și  $(G'', \cdot)$  sunt grupuri, iar  $f : G \rightarrow G'$  și  $g : G' \rightarrow G''$  sunt omomorfisme (izomorfisme), atunci  $g \circ f$  este omomorfism (izomorfism).

*Demonstrație.* Folosind definiția compunerii funcțiilor și ipoteza că  $f$  și  $g$  sunt omomorfisme, pentru orice  $x_1, x_2 \in G$  avem:

$$(g \circ f)(x_1 x_2) = g(f(x_1 x_2)) = g(f(x_1) f(x_2)) = g(f(x_1)) \cdot g(f(x_2)) = (g \circ f)(x_1) \cdot (g \circ f)(x_2),$$

ceea ce ne arată că  $g \circ f$  este omomorfism. Compusa a două bijecții fiind o bijecție rezultă că dacă  $f$  și  $g$  sunt izomorfisme, atunci  $g \circ f$  este izomorfism.  $\square$

**Corolarul 2.25.** a) Dacă  $(G, \cdot) \simeq (G', \cdot)$  și  $(G', \cdot) \simeq (G'', \cdot)$  atunci  $(G, \cdot) \simeq (G'', \cdot)$ , adică relația  $\simeq$  este tranzitivă.

b) Fie  $(G, \cdot)$  un grup și  $End(G, \cdot)$ , respectiv  $Aut(G, \cdot)$  mulțimea endomorfismelor, respectiv automorfismelor lui  $(G, \cdot)$ . Mulțimea  $End(G, \cdot)$  este parte stabilă în  $(G^G, \circ)$  și  $(End(G, \cdot), \circ)$  este monoid. Mulțimea  $Aut(G, \cdot)$  este o parte stabilă a lui  $(End(G, \cdot), \circ)$  care conține elementul unitate (a se vedea Exemplul 2.26 a)). Conform Corolarului 2.23, toate elementele din  $Aut(G, \cdot)$  sunt inversabile, deci  $(Aut(G, \cdot), \circ)$  este grup.

**Exemplele 2.26.** a) Dacă  $(G, \cdot)$  este un grupoid, atunci  $1_A : A \rightarrow A$ ,  $1_A(x) = x$  este un automorfism numit **automorfismul identic** al lui  $(G, \cdot)$ . Acesta este elementul unitate din  $(End(G, \cdot), \circ)$  și  $(Aut(G, \cdot), \circ)$ . Din acest exemplu rezultă că relația  $\simeq$  este reflexivă.

b) Dacă  $(G, \cdot)$  și  $(G', \cdot)$  sunt grupuri, iar  $1'$  este elementul neutru din  $(G', \cdot)$ , atunci funcția  $\theta : G \rightarrow G'$ ,  $\theta(x) = 1'$  este omomorfism numit **omomorfismul nul** sau **zero**.

c) Fie  $a \in \mathbb{R}$ ,  $a \neq 1$ ,  $a > 0$ . Funcția  $f : \mathbb{R}_+^* \rightarrow \mathbb{R}$ ,  $f(x) = \log_a x$  este un izomorfism al grupului  $(\mathbb{R}_+^*, \cdot)$  pe grupul  $(\mathbb{R}, +)$  și inversul acestuia este  $f^{-1} : \mathbb{R} \rightarrow \mathbb{R}_+^*$ ,  $f^{-1}(x) = a^x$ . Proprietățile  $\log_a(xy) = \log_a x + \log_a y$  și  $a^{x+y} = a^x a^y$  exprimă faptul că  $f$  și  $f^{-1}$  sunt omomorfisme.

d) Funcția  $f : \mathbb{C}^* \rightarrow \mathbb{R}^*$ ,  $f(z) = |z|$  este un omomorfism al grupului  $(\mathbb{C}^*, \cdot)$  în grupul  $(\mathbb{R}^*, \cdot)$  pentru că  $f(z_1 z_2) = |z_1 z_2| = |z_1| \cdot |z_2| = f(z_1) f(z_2)$ .

e) Funcția  $f : \mathbb{C} \rightarrow \mathbb{C}$ ,  $f(z) = \bar{z}$  (unde  $\bar{z}$  este conjugatul lui  $z$ ) este un automorfism al grupului  $(\mathbb{C}, +)$ , iar  $f^{-1} = f$ . Restricția lui  $f$  la  $\mathbb{C}^*$  este automorfism al grupului  $(\mathbb{C}^*, \cdot)$ .

f) Pentru orice grup  $(G, \cdot)$  funcția  $f : G \rightarrow G$ ,  $f(x) = x^{-1}$  este bijectivă. Funcția  $f$  este un automorfism al lui  $(G, \cdot)$  dacă și numai dacă grupul  $(G, \cdot)$  este abelian.

Reamintim că pentru o funcție  $f : A \rightarrow B$ ,  $X \subseteq A$  și  $Y \subseteq B$ , notăm

$$f(X) = \{f(x) \mid x \in X\} \text{ și } f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}.$$

**Teorema 2.27.** Fie  $(G, \cdot)$  și  $(G', \cdot)$  grupuri și  $f : G \rightarrow G'$  un omomorfism.

1) Dacă  $H$  este un subgrup al lui  $(G, \cdot)$ , atunci  $f(H)$  este un subgrup al lui  $(G', \cdot)$ .

2) Dacă  $H'$  este un subgrup al lui  $(G', \cdot)$ , atunci  $f^{-1}(H')$  este un subgrup al lui  $(G, \cdot)$ .

*Demonstrație.* 1) Dacă  $H$  este subgrup, atunci  $H \neq \emptyset$ , ceea ce implică  $f(H) \neq \emptyset$ . Dacă  $y_1, y_2 \in f(H)$ , atunci există  $x_1, x_2 \in H$  astfel încât  $y_1 = f(x_1)$ ,  $y_2 = f(x_2)$ . Acum,  $f$  fiind omomorfism, avem:

$$y_1 y_2^{-1} = f(x_1) \cdot f(x_2)^{-1} = f(x_1) \cdot f(x_2^{-1}) = f(x_1 x_2^{-1}),$$

iar  $x_1, x_2 \in H$  implică  $x_1x_2^{-1} \in H$ . Rezultă că  $y_1y_2^{-1} \in f(H)$ . Deci  $f(H)$  este un subgrup al lui  $(G', \cdot)$ .

2) Cum  $f(1) = 1' \in H'$ , deducem că  $1 \in f^{-1}(H')$ , adică  $f^{-1}(H') \neq \emptyset$ . În plus, avem

$$x_1, x_2 \in f^{-1}(H') \Rightarrow f(x_1), f(x_2) \in H' \Rightarrow f(x_1)[f(x_2)]^{-1} = f(x_1x_2^{-1}) \in H' \Rightarrow x_1x_2^{-1} \in f^{-1}(H').$$

Deci  $f^{-1}(H')$  este un subgrup al lui  $(G, \cdot)$ . □

Aplicând 2) din teorema de mai sus subgrupului  $\{1'\}$  al lui  $G'$ , rezultă:

**Corolarul 2.28.**  $\text{Ker}f = \{x \in G \mid f(x) = 1'\}$  este un subgrup al lui  $G$ .

**Definiția 2.29.** Fie  $(G, \cdot)$  și  $(G', \cdot)$  grupuri și  $f : G \rightarrow G'$  un omomorfism. Subgrupul  $\text{Ker}f = \{x \in G \mid f(x) = 1'\}$  al lui  $G$  se numește **nucleul omomorfismului**  $f$ .

**Teorema 2.30.** Fie  $(G, \cdot)$ ,  $(G', \cdot)$  grupuri și  $1$ , respectiv  $1'$  elementul neutru al lui  $G$ , respectiv  $G'$ . Omomorfismul  $f : G \rightarrow G'$  este injectiv dacă și numai dacă  $\text{Ker}f = \{1\}$ .

*Demonstrație.* Dacă omomorfismul  $f$  este injectiv, atunci

$$x \in \text{Ker}f \Rightarrow f(x) = 1' \Rightarrow f(x) = f(1) \Rightarrow x = 1$$

de unde urmează incluziunea  $\text{Ker}f \subseteq \{1\}$ , iar incluziunea inversă rezultă din  $f(1) = 1'$ . Deci  $\text{Ker}f = \{1\}$ . Invers, dacă  $\text{Ker}f = \{1\}$ , atunci

$$f(x_1) = f(x_2) \Rightarrow f(x_1)(f(x_2))^{-1} = 1' \Rightarrow f(x_1x_2^{-1}) = 1' \Rightarrow x_1x_2^{-1} = 1 \Rightarrow x_1 = x_2$$

ceea ce ne arată că omomorfismul  $f$  este injectiv. □

## 2.2 Exerciții rezolvate

1) Fie  $M$  o mulțime,  $\mathcal{P}(M)$  mulțimea submulțimilor sale și  $\Delta$  **diferența simetrică**, adică pentru  $X, Y \subseteq M$  avem  $X\Delta Y = (X \setminus Y) \cup (Y \setminus X)$ . Să se arate că  $(\mathcal{P}(M), \Delta)$  este un grup.

*Soluție:* Fie  $C(X) = C_M X = M \setminus X$  complementara submulțimii  $X \subseteq M$ . Avem

$$(1) \quad X\Delta Y = [X \cap C(Y)] \cup [Y \cap C(X)].$$

În stabilirea asociativității operației  $\Delta$  avem nevoie de egalitatea

$$(2) \quad C(X\Delta Y) = (X \cap Y) \cup [C(X) \cap C(Y)]$$

care se deduce din (1), din formulele lui de Morgan și din distributivitatea intersecției față de reuniune astfel:

$$\begin{aligned} C(X\Delta Y) &= C(X \cap C(Y)) \cap C(Y \cap C(X)) = [C(X) \cup Y] \cup [C(Y) \cup X] \\ &= \{[C(X) \cup Y] \cap C(Y)\} \cup \{[C(X) \cup Y] \cap X\} \\ &= [C(X) \cap C(Y)] \cup [Y \cap C(Y)] \cup [C(X) \cup X] \cup [Y \cap X] \\ &= [C(X) \cap C(Y)] \cup \emptyset \cup \emptyset \cup (X \cap Y) = (X \cap Y) \cup [C(X) \cap C(Y)]. \end{aligned}$$

Folosind (1) și (2) avem

$$\begin{aligned}
(X\Delta Y)\Delta Z &= [(X+Y) \cap C(Z)] \cup [C(X+Y) \cap Z] \\
&= \{[(X \cap C(Y)) \cup (Y \cap C(X))] \cap C(Z)\} \cup \{[(X \cap Y) \cup (C(X) \cap C(Y))] \cap Z\} \\
&= [X \cap C(Y) \cap C(Z)] \cup [Y \cap C(X) \cap C(Z)] \cup [X \cap Y \cap Z] \cup [C(X) \cap C(Y) \cap Z] \\
&= (X \cap Y \cap Z) \cup [X \cap C(Y) \cap C(Z)] \cup [C(X) \cap Y \cap C(Z)] \cup [C(X) \cap C(Y) \cap Z].
\end{aligned}$$

La același rezultat se ajunge și calculând pe  $X\Delta(Y\Delta Z)$ . Deci  $\Delta$  este asociativă.

Din definiția operației  $\Delta$  rezultă că  $\Delta$  este comutativă, are element neutru submulțimea vidă și  $X\Delta X = \emptyset$ , adică opusa lui  $X$  este  $X$ . Deci  $(\mathcal{P}(M), \Delta)$  este grup abelian.

2) Fie  $G = (-1, 1)$ ,  $x, y \in G$  și

$$(*) \quad x * y = \frac{x+y}{1+xy}.$$

Să se arate că:

- i) egalitatea (\*) definește o operație  $*$  pe  $G$  și  $(G, *)$  este un grup abelian;
- ii) între grupul multiplicativ al numerelor reale pozitive  $(\mathbb{R}_+^*, \cdot)$  și  $(G, *)$  există un izomorfism  $f: \mathbb{R}_+^* \rightarrow G$  de forma  $f(x) = \frac{\alpha x - 1}{x + 1}$ .

*Soluție:* i) Dacă  $x, y \in G$  atunci  $x * y \in G$  deoarece

$$x * y = -1 + \frac{(x+1)(y+1)}{1+xy} \quad \text{și} \quad x * y = 1 - \frac{(x-1)(y-1)}{1+xy}.$$

Așadar,  $*$  este o operație pe  $G$ . Din (1) rezultă că  $*$  este comutativă. Asociativitatea sa se obține astfel:

$$\begin{aligned}
(x * y) * z &= \frac{x+y}{1+xy} * z = \frac{x+y+z+xyz}{xy+xz+yz+1}, \\
x * (y * z) &= x * \frac{y+z}{1+yz} = \frac{x+y+z+xyz}{xy+xz+yz+1}.
\end{aligned}$$

Presupunem că  $e$  este elementul neutru. Atunci  $x * e = x$  pentru orice  $x \in G$ , adică  $\frac{x+e}{1+xe} = x$  pentru orice  $x \in G$ . Rezultă că  $e = 0$ . Prin urmare, dacă elementul neutru există, acesta este 0. Întrucât  $x * 0 = x$  pentru orice  $x \in G$ , rezultă că 0 este elementul neutru. Dacă  $x'$  este simetricul lui  $x \in G$  atunci  $x * x' = 0$  de unde deducem  $x' = -x \in G$ . Deci, dacă simetricul lui  $x$  există, acesta este  $-x$ . Se verifică ușor că  $-x$  este simetricul lui  $x$  pentru orice  $x \in G$ . Astfel am arătat că  $(G, *)$  este un grup abelian.

ii) Cum imaginea elementului neutru printr-un omomorfism de grupuri este elementul neutru, rezultă că  $f(1) = 0$ , ceea ce implică  $\alpha = 1$ . Deci

$$(**) \quad f(x) = \frac{x-1}{x+1}.$$

Întrucât,

$$\begin{aligned}
\frac{x-1}{x+1} > -1 &\Leftrightarrow \frac{2x}{x+1} > 0, \\
\frac{x-1}{x+1} < +1 &\Leftrightarrow \frac{-2}{x+1} < 0,
\end{aligned}$$

avem  $f(x) \in G$  pentru orice  $x \in \mathbb{R}_+^*$ , ceea ce arată că egalitatea (\*\*\*) definește o funcție  $f : \mathbb{R}_+^* \rightarrow G$ . Funcția  $f$  este bijectivă deoarece ecuația  $f(x) = y$  are o soluție unică  $x = \frac{1+y}{1-y} \in \mathbb{R}_+^*$ . Prin calcul se arată că  $f$  este un omomorfism, adică

$$f(x_1x_2) = \frac{x_1x_2 - 1}{x_1x_2 + 1} = f(x_1) * f(x_2).$$

Deci  $f$  este izomorfism.

3) Fie  $(G, \cdot)$  un grup finit și  $\emptyset \neq H \subseteq G$ . Să se arate că  $H$  este un subgrup în  $G$  dacă și numai dacă  $H$  este parte stabilă în  $(G, \cdot)$ .

*Soluție:* Dacă  $H \leq G$  atunci, evident,  $H$  este parte stabilă în  $(G, \cdot)$ .

Fie  $h \in H$  arbitrar. Dacă  $H$  este parte stabilă în  $(G, \cdot)$ , atunci imaginile restricțiilor translațiilor cu  $h$  la  $H$  sunt în  $H$ . Prin urmare, avem funcțiile

$$t_h, t'_h : H \rightarrow H, \quad t_h(x) = hx, \quad t'_h(x) = xh.$$

Dacă  $x_1, x_2 \in H$  și  $t_h(x_1) = t_h(x_2)$ , adică  $hx_1 = hx_2$ , privind această egalitate în  $G$ , putem simplifica cu  $h$  și obținem  $x_1 = x_2$ . Rezultă că  $t_h$  este injectivă, iar cum  $H$  e finită,  $t_h$  este o bijecție.

Din surjectivitatea lui  $t_h$  deducem că există  $e \in H$  astfel încât  $h = t_h(e) = he$ . Atunci avem, în  $G$ ,  $1h = eh$ , de unde, simplificând din nou cu  $h$ , obținem  $1 = e \in H$ . Așadar,  $t_h$  fiind surjecție, există  $h' \in H$  cu proprietatea că

$$1 = t_h(h') = hh' \Rightarrow hh^{-1} = 1 = hh' \Rightarrow h^{-1} = h' \in H.$$

Cum  $h \in H$  a fost arbitrar, din teorema de caracterizare a subgrupului urmează  $H \leq G$ .

4) Să se arate că există un singur omomorfism de la grupul  $(\mathbb{Q}, +)$  la grupul  $(\mathbb{Z}, +)$ .

*Soluție:* Fie  $f : \mathbb{Q} \rightarrow \mathbb{Z}$  un omomorfism,  $x \in \mathbb{Q}$  arbitrar și  $f(x) = a \in \mathbb{Z}$ . Pentru orice  $n \in \mathbb{N}^*$  avem

$$a = f(x) = f\left(n \cdot \frac{x}{n}\right) = f\left(\underbrace{\frac{x}{n} + \dots + \frac{x}{n}}_{n \text{ termeni}}\right) = \underbrace{f\left(\frac{x}{n}\right) + \dots + f\left(\frac{x}{n}\right)}_{n \text{ termeni}} = n \cdot f\left(\frac{x}{n}\right),$$

iar cum  $f\left(\frac{x}{n}\right) \in \mathbb{Z}$ , deducem că  $a = 0$  (fiind multiplu pentru orice  $n \in \mathbb{N}^*$ ), așadar  $f(x) = 0$  pentru orice  $x \in \mathbb{Q}$ .

5) Să se determine automorfismele grupului  $(\mathbb{Z}, +)$ .

*Soluție:* Fie  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  un endomorfism al grupului  $(\mathbb{Z}, +)$ . Dacă  $x \in \mathbb{N}^*$ , atunci

$$f(x) = f(\underbrace{1 + 1 + \dots + 1}_x) = xf(1)$$

și  $f(-x) = -f(x)$ . Evident  $f(0) = 0 = f(1) \cdot 0$ , prin urmare,

$$f(x) = f(1) \cdot x, \quad \forall x \in \mathbb{Z}.$$

Dacă  $f$  este un automorfism,  $f$  fiind surjectivă, există  $a \in \mathbb{Z}$  astfel încât  $1 = f(1) \cdot a$ . Rezultă că  $f(1)$  divide pe 1, adică  $f(1) \in \{-1, 1\}$ . Dacă  $f(1) = 1$ , atunci  $f = 1_{\mathbb{Z}}$  care este, evident, automorfism al lui  $(\mathbb{Z}, +)$ , iar dacă  $f(1) = -1$ , atunci  $f$  este

$$-1_{\mathbb{Z}} : \mathbb{Z} \rightarrow \mathbb{Z}, (-1_{\mathbb{Z}})(x) = -x$$

despre care se arată ușor că e automorfism al lui  $(\mathbb{Z}, +)$ .

Deci automorfismele lui  $(\mathbb{Z}, +)$  sunt  $1_{\mathbb{Z}}$  și  $-1_{\mathbb{Z}}$ .

## 2.3 Inele și corpuri

**Definițiile 2.31.** Un sistem ordonat  $(R, +, \cdot)$  în care  $R$  este o mulțime, iar  $+$  și  $\cdot$  sunt operații pe  $R$  se numește **inel** dacă verifică următoarele axiome:

- i)  $(R, +)$  este grup abelian;
- ii)  $(R, \cdot)$  este semigrup;
- iii) Operația  $\cdot$  este distributivă față de  $+$ , adică

$$a(b + c) = ab + ac \text{ și } (b + c)a = ba + ca, \forall a, b, c \in \mathbb{R}.$$

Inelul  $(R, +, \cdot)$  se numește **comutativ**, respectiv **cu unitate** dacă operația  $\cdot$  este comutativă, respectiv dacă are element unitate (notat cu 1). Dacă  $(R, +, \cdot)$  este un inel cu unitate, atunci un element  $a \in R$  se numește **inversabil** dacă

$$\exists a^{-1} \in R : a^{-1}a = 1 = aa^{-1}.$$

Uneori inelul  $(R, +, \cdot)$  va fi notat cu  $R$ . Menționăm că dacă  $(R, +, \cdot)$  este inel atunci, întrucât  $(R, +)$  este grup, rezultă că mulțimea  $R$  este nevidă. Conform convențiilor făcute în Secțiunea 2.1, elementul neutru al grupului  $(R, +)$  va fi notat cu 0 și îl vom numi zero. Vom nota pe  $R \setminus \{0\}$  cu  $R^*$ . Dacă  $a \in R$ , atunci opusul (simetricul față de  $+$ ) al lui  $a$  va fi notat cu  $-a$ . Întrucât  $(R, +)$  este grup abelian, avem

$$-(a + b) = -a - b, \forall a, b \in R.$$

**Observațiile 2.32.** a) În liceu se folosește denumirea de inel pentru ceea ce am numit mai sus inel cu unitate.

b) Fie  $(R, +, \cdot)$  un inel. Întrucât  $(R, +)$  este grup abelian, pentru orice  $a \in R$  și  $n \in \mathbb{Z}$  se poate defini  $na$  ca înainte de Propoziția 2.10. În semigrupul  $(R, \cdot)$  se poate defini  $a^n$  pentru orice  $a \in R$  și orice  $n \in \mathbb{N}^*$ , iar dacă  $R$  este inel cu unitate putem defini  $a^n$  și pentru  $n \in \mathbb{Z}$  în condițiile discutate pe larg în Secțiunea 2.1. Proprietățile calculului cu multipli și ale calculului cu puteri într-un inel rezultă imediat din Propoziția 2.10.

**Definiția 2.33.** Un inel cu unitate  $(K, +, \cdot)$  se numește **corp** dacă:

- i)  $K$  conține cel puțin două elemente, adică  $|K| \geq 2$ .
- ii) Orice  $a \in K^*$  este inversabil.

**Observația 2.34.** Un triplet  $(K, +, \cdot)$  este corp dacă și numai dacă:

- 1)  $(K, +)$  este grup abelian.
- 2)  $K^*$  este stabilă în  $(K, \cdot)$  și  $(K^*, \cdot)$  este grup.
- 3) Operația  $\cdot$  este distributivă în raport cu  $+$ .

**Teorema 2.35.** Dacă  $(R, +, \cdot)$  este un inel, atunci pentru orice  $a \in R$ , funcțiile

$$t_a, t'_a : R \rightarrow R, \quad t_a(x) = ax, \quad t'_a(x) = xa$$

sunt endomorfisme ale grupului  $(R, +)$ .

*Demonstrație.* Pentru orice  $x, y \in R$  avem:

$$t_a(x + y) = a(x + y) = ax + ay = t_a(x) + t_a(y),$$

adică  $t_a$  este endomorfism al grupului  $(R, +)$ . Analog se arată că  $t'_a$  este endomorfism.  $\square$

**Corolarul 2.36. (Reguli de calcul într-un inel)** Fie  $(R, +, \cdot)$  un inel.

a) Pentru orice  $a, b \in R$  au loc egalitățile:

$$a0 = 0 = 0a, \quad a(-b) = -ab = (-a)b, \quad (-a)(-b) = ab. \quad (1)$$

Primele două (șiruri de) egalități din (1) rezultă din teorema de mai sus și din Teorema 2.21. Ultima egalitate se obține astfel:

$$(-a)(-b) = -((-a)b) = -(-ab) = ab.$$

b) Dacă  $R$  este inel asociativ,  $a \in R$  și  $n \in \mathbb{N}^*$ , atunci

$$(-a)^n = \begin{cases} a^n & \text{dacă } n \text{ este par} \\ -a^n & \text{dacă } n \text{ este impar} \end{cases}$$

c) Dacă  $a, b, c \in R$  atunci

$$a(b - c) = ab - ac \text{ și } (b - c)a = ba - ca.$$

**Observațiile 2.37.** 1) Dacă  $(R, +, \cdot)$  este un inel cu unitate, atunci

$$R \neq \{0\} \Leftrightarrow |R| \geq 2 \Leftrightarrow 0 \neq 1.$$

Cum implicațiile din șirul

$$R \neq \{0\} \Leftarrow |R| \geq 2 \Leftarrow 0 \neq 1$$

sunt evidente, rămâne de demonstrat că  $|R| \neq \{0\}$  implică  $0 \neq 1$ , adică

$$0 = 1 \Rightarrow |R| = \{0\}.$$

Într-adevăr, dacă  $0 = 1$ , pentru orice  $a \in R$ ,

$$a = a \cdot 1 = a \cdot 0 = 0.$$

2) Dacă  $R$  este inel cu unitate și  $R \neq \{0\}$ , atunci  $0$  nu este inversabil.

Din (1) rezultă că (într-un inel) dacă într-un produs unul din factor este zero, atunci produsul este zero. Inversa acestei afirmații nu este, în general, adevărată. Inelele în care această inversă este adevărată constituie o clasă specială de inele.



**Definiția 2.38.** Fie  $R$  un inel. Un element  $a \in R$ ,  $a \neq 0$  se numește **divizor al lui zero** dacă există  $b \in R$ ,  $b \neq 0$  astfel încât  $ab = 0$  sau  $ba = 0$ . Un inel  $R \neq \{0\}$  comutativ, cu unitate și care nu conține divizori ai lui zero (diferiți de zero) se numește **domeniu de integritate**.

**Observația 2.39.** a) Un inel  $R$  nu are divizori ai lui zero dacă și numai dacă  $R^*$  este o parte stabilă în  $(R, \cdot)$ , adică

$$a, b \in R, a \neq 0 \text{ și } b \neq 0 \Rightarrow ab \neq 0.$$

Menționăm că implicația de mai sus este echivalentă cu

$$a, b \in R, ab = 0 \Rightarrow a = 0 \text{ sau } b = 0.$$

b) Corpurile nu au divizori ai lui zero, prin urmare corpurile comutative sunt domenii de integritate.

Într-adevăr, pentru un corp  $K$  și  $a, b \in K$ ,

$$ab = 0 \text{ și } a \neq 0 \Rightarrow b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0.$$

**Exemplele 2.40.** a)  $(\mathbb{Z}, +, \cdot)$  este domeniu de integritate, dar nu este corp, pentru că singurele elemente inversabile din  $(\mathbb{Z}, +, \cdot)$  sunt  $-1$  și  $1$ .

b)  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$  sunt corpuri comutative.

c) Pe o mulțime formată dintr-un singur element există o singură operație. Dacă luăm în calitate de  $+$  și de  $\cdot$  această operație, atunci se obține un inel asociativ, comutativ și cu element unitate. Acesta se numește **inelul nul**. În acest inel avem  $0 = 1$ . Din Observația 2.37 a) rezultă că inelul nul este caracterizat de această egalitate.

d) Fie  $R$  o mulțime și  $m, n \in \mathbb{N}^*$ . O funcție

$$A : \{1, \dots, m\} \times \{1, \dots, n\} \rightarrow R$$

se numește **matrice** de tipul  $(m, n)$  cu elemente din  $R$ . Când  $m = n$  matricea  $A$  se numește **matrice pătratică** de ordinul  $n$ . Notând pentru toți  $i = 1, \dots, m$  și  $j = 1, \dots, n$  pe  $A(i, j)$  cu  $a_{ij} (\in R)$ , putem scrie pe  $A$  sub formă de tabel dreptunghiular cu  $m$  linii și  $n$  coloane în care trecem imaginea fiecărei perechi  $(i, j)$  în linia  $i$  și coloana  $j$

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Pentru acest tabel vom folosi notația  $A = (a_{ij})$ . Mulțimea matricelor de tipul  $(m, n)$  cu elemente din  $R$  o vom nota cu  $M_{m,n}(R)$ , iar când  $m = n$  cu  $M_n(R)$ . Dacă  $(R, +, \cdot)$  este un inel, atunci  $+$  din  $R$  induce o operație  $+$  în  $M_{m,n}(R)$  definită astfel: dacă  $A = (a_{ij})$  și  $B = (b_{ij})$  sunt două matrice de tipul  $(m, n)$  atunci

$$A + B = (a_{ij} + b_{ij}).$$

Se verifică ușor că această operație este asociativă, comutativă, are ca element neutru (element nul) matricea  $O_{m,n}$  care are pe  $0$  în toate pozițiile și fiecare element  $A = (a_{ij})$  din  $M_{m,n}(R)$  are un opus (pe matricea  $-A = (-a_{ij})$ , numită opusa matricei  $A$ ).

Denumirea de înmulțire a matricelor este întrebuințată pentru operația parțială definită în mulțimea  $\bigcup\{M_{m,n}(R) \mid (m,n) \in \mathbb{N}^* \times \mathbb{N}^*\}$  astfel: dacă avem  $A = (a_{ij}) \in M_{m,n}(R)$  și  $B = (b_{ij}) \in M_{n,p}(R)$ , atunci

$$AB = (c_{ij}) \in M_{m,p}, \text{ cu } c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}, \quad (i,j) \in \{1,\dots,m\} \times \{1,\dots,p\}.$$

Dacă lucrăm cu matrici pătratice de același ordin, operația parțială  $\cdot$  de mai sus devine o operație în sensul Definiției 2.1, operație care este asociativă și distributivă față de  $+$ . Rezultă că  $(M_n(R), +, \cdot)$  este un inel numit **inelul matricelor pătrate de ordinul  $n$  cu elemente din  $R$** . Dacă inelul  $R$  este cu unitate, atunci inelul  $M_n(R)$  este cu unitate. Unitatea inelului  $M_n(R)$  este matricea

$$I_n = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

de tipul  $(n,n)$ , numită **matricea unitate** de ordinul  $n$ . Dacă  $n \geq 2$  și  $R \neq \{0\}$  atunci inelul  $M_n(R)$  nu este comutativ și are divizori ai lui zero. Dacă  $a, b \in R^*$ , atunci matricele nenule

$$\begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \dots & b \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

pot fi folosite atât pentru a demonstra că  $M_n(R)$  are divizori ai lui zero, cât și pentru a arăta că semigrupul  $(M_n(R), \cdot)$  nu este comutativ.

Dacă  $R$  e un inel cu unitate, mulțimea elementelor inversabile ale inelului  $M_n(R)$  este

$$GL_n(R) = \{A \in M_n(R) \mid \exists B \in M_n(R) : AB = BA = I_n\}.$$

Mulțimea  $GL_n(R)$  e stabilă în  $(M_n(R), \cdot)$  și  $(GL_n(R), \cdot)$  e un grup numit **grupul general liniar de gradul  $n$  peste  $R$** . Se știe că dacă  $R$  este unul dintre corpurile numerice ( $\mathbb{Q}$ ,  $\mathbb{R}$  sau  $\mathbb{C}$ ) atunci  $A \in M_n(R)$  este inversabilă dacă și numai dacă  $\det A \neq 0$ . Prin urmare,

$$GL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) \mid \det A \neq 0\},$$

și analog se pot redefini și  $GL_n(\mathbb{R})$  și  $GL_n(\mathbb{Q})$ .

e) Fie  $n \in \mathbb{N}$ ,  $n \geq 2$ . Teorema împărțirii cu rest în  $\mathbb{Z}$  (a se vedea Secțiunea 5.1) permite partiționarea mulțimii  $\mathbb{Z}$  în clase determinate de resturile ce pot fi obținute prin împărțire la  $n$ :  $\{n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}$ , unde  $r + n\mathbb{Z} = \{r + nk \mid k \in \mathbb{Z}\}$  ( $r \in \mathbb{Z}$ ). Folosim următoarele notații

$$\widehat{r} = r + n\mathbb{Z} \quad (r \in \mathbb{Z}) \quad \text{și} \quad \mathbb{Z}_n = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\} = \{\widehat{0}, \widehat{1}, \dots, \widehat{n-1}\}.$$

Să observăm că pentru  $a, r \in \mathbb{Z}$ ,

$$\widehat{a} = \widehat{r} \Leftrightarrow a + n\mathbb{Z} = r + n\mathbb{Z} \Leftrightarrow a - r \in n\mathbb{Z} \Leftrightarrow n \mid a - r.$$

Operațiile

$$\widehat{a} + \widehat{b} = \widehat{a + b}, \quad \widehat{a} \widehat{b} = \widehat{ab}$$

sunt bine definite, adică, dacă se consideră alți reprezentanți  $a'$  și  $b'$  pentru două clase  $\widehat{a}$ , respectiv  $\widehat{b}$  rezultatele operațiilor rămân aceleași. Într-adevăr, din  $a' \in \widehat{a}$  și  $b' \in \widehat{b}$  rezultă

$$n|a' - a, n|b' - b \Rightarrow n|a' - a + b' - b \Rightarrow n|(a' + b') - (a + b) \Rightarrow \widehat{a' + b'} = \widehat{a + b}$$

și

$$a' = a + nk, b' = b + nl \quad (k, l \in \mathbb{Z}) \Rightarrow a'b' = ab + n(al + bk + nkl) \in ab + n\mathbb{Z} \Rightarrow \widehat{a'b'} = \widehat{ab}.$$

Se verifică ușor că operațiile  $+$  și  $\cdot$  sunt asociative și comutative,  $+$  admite element neutru pe  $\widehat{0}$ , pentru orice clasă  $\widehat{a}$  există un element opus în  $(\mathbb{Z}_n, +)$ ,  $-\widehat{a} = \widehat{-a} = \widehat{n - a}$ , operația  $\cdot$  admite element neutru pe  $\widehat{1}$  și este distributivă față de  $+$ . Prin urmare,  $(\mathbb{Z}_n, +, \cdot)$  este un inel cu unitate.

Luând, de exemplu  $n = 4$ , inelul obținut  $(\mathbb{Z}_4, +, \cdot)$  are divizori ai lui zero:

$$\widehat{2} \in \mathbb{Z}_4 \setminus \{\widehat{0}\} = \{\widehat{1}, \widehat{2}, \widehat{3}\} \text{ și } \widehat{2} \cdot \widehat{2} = \widehat{0}.$$

Prin urmare, inelul  $(\mathbb{Z}_n, +, \cdot)$  nu este, în general, un corp. De fapt,  $\widehat{a} \in \mathbb{Z}_n$  este inversabil dacă și numai dacă  $(a, n) = 1$ . Rezultă că inelul  $(\mathbb{Z}_n, +, \cdot)$  este corp dacă și numai dacă  $n$  este număr prim.

**Definiția 2.41.** Fie  $(R, +, \cdot)$  un inel. O submulțime  $A \subseteq R$  se numește **subinel** al lui  $(R, +, \cdot)$  dacă

i)  $A$  este stabilă în raport cu  $+$  și  $\cdot$ , adică

$$a_1, a_2 \in A \Rightarrow a_1 + a_2 \in A \text{ și } a_1 a_2 \in A.$$

ii)  $A$  este un inel în raport cu operațiile induse de  $+$  și  $\cdot$  din  $R$ .

**Observațiile 2.42.** a) Dacă  $(R, +, \cdot)$  este inel și  $A \subseteq R$ , atunci  $A$  este subinel al lui  $R$  dacă și numai dacă  $A$  este subgrup al grupului  $(R, +)$  și  $A$  este stabilă în  $(R, \cdot)$ .

Afirmația rezultă din definițiile subinelului și subgrupului și din Observația 2.13 b).

b) Dacă  $A$  e un subinel al inelului  $R$ , atunci elementul nul din  $(A, +)$  coincide cu elementul nul din  $(R, +)$ , iar opusul unui element  $a \in A$  în  $(A, +)$  coincide cu opusul lui  $a$  în  $(R, +)$ .

c) Orice subinel al unui inel  $R$  conține elementul nul din  $R$ .

d) Un subinel  $A$  al unui inel cu unitate  $R$ , în general, nu conține unitatea lui  $R$ . De exemplu,  $(\mathbb{Z}, +, \cdot)$  este inel cu unitate și  $2\mathbb{Z}$  este subinel al acestuia, dar  $1 \notin 2\mathbb{Z}$ .

Practic, când arătăm că o submulțime a unui inel este subinel aplicăm:

**Teorema 2.43. (Teorema de caracterizare a subinelului)**

Fie  $(R, +, \cdot)$  un inel și  $A \subseteq R$ . Sunt echivalente următoarele afirmații:

1)  $A$  este subinel al lui  $(R, +, \cdot)$ .

2)  $A$  verifică condițiile:

$\alpha$ )  $A \neq \emptyset$ ;

$\beta$ )  $\alpha_1, \alpha_2 \in A \Rightarrow \alpha_1 - \alpha_2 \in A$ ;

$\gamma$ )  $\alpha_1, \alpha_2 \in A \Rightarrow \alpha_1 \alpha_2 \in A$ .

3)  $A$  verifică condițiile:

$$\alpha) A \neq \emptyset;$$

$$\beta') a_1, a_2 \in A \Rightarrow a_1 + a_2 \in A;$$

$$\beta'') a \in A \Rightarrow -a \in A;$$

$$\gamma) a_1, a_2 \in A \Rightarrow a_1 a_2 \in A.$$

*Demonstrație.* Rezultă din Observația 2.42 a) și din faptul că atât condițiile  $\alpha$ ) și  $\beta$ ) cât și condițiile  $\alpha$ ),  $\beta'$ ) și  $\beta''$ ) sunt echivalente cu afirmația că  $A$  este subgrup în  $(R, +)$  (vezi Teorema 2.17).  $\square$

**Exemplele 2.44.** a) Dacă  $R$  este un inel, atunci  $\{0\}$  și  $R$  sunt subinele ale lui  $R$ . Un subinel al lui  $R$  diferit de  $\{0\}$  și  $R$  se numește **propriu**.

b) Fiecare din inelele  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  și  $\mathbb{C}$  este subinel în următoarele.

c) Pentru orice  $n \in \mathbb{N}$ ,  $n\mathbb{Z}$  este un subinel al lui  $(\mathbb{Z}, +, \cdot)$ .

Într-adevăr, din Exemplul 2.18 c) rezultă că  $n\mathbb{Z}$  (cu  $n \in \mathbb{N}$ ) sunt subgrupuri ale lui  $(\mathbb{Z}, +)$ . Deci este suficient să arătăm că  $n\mathbb{Z}$  verifică pe  $\gamma$ ), ceea ce este imediat pentru că produsul a doi multipli de  $n$  este multiplu de  $n$ .

**Definiția 2.45.** Fie  $(K, +, \cdot)$  un corp. O submulțime  $A \subseteq K$  se numește **subcorp** al lui  $(K, +, \cdot)$  dacă

i)  $A$  este stabilă în raport cu  $+$  și  $\cdot$ , adică

$$a_1, a_2 \in A \Rightarrow a_1 + a_2 \in A \text{ și } a_1 a_2 \in A.$$

ii)  $A$  este corp în raport cu operațiile induse de  $+$  și  $\cdot$  din  $K$ .

**Observațiile 2.46.** a) Din ii) rezultă că dacă  $A$  este subcorp, atunci avem  $|A| \geq 2$ .

b) Dacă  $(K, +, \cdot)$  este corp și  $A \subseteq K$ , atunci  $A$  este subcorp dacă și numai dacă  $A$  este subgrup în  $(K, +)$  și  $A^*$  este subgrup în  $(K^*, \cdot)$ .

c) Dacă  $A$  este subcorp în  $(K, +, \cdot)$ , atunci  $0, 1 \in A$ .

d) Dacă  $(K, +, \cdot)$  este corp și  $A \subseteq K$ , atunci  $A$  este subcorp dacă și numai dacă  $A$  este subinel în  $(K, +, \cdot)$ ,  $|A| \geq 2$  și pentru orice  $a \in A^*$ ,  $a^{-1} \in A$ .

Practic când arătăm că o submulțime a unui corp este subcorp aplicăm următoarea teoremă.

**Teorema 2.47. (Teorema de caracterizare a subcorpului)**

Fie  $(K, +, \cdot)$  un corp și  $A \subseteq K$ . Sunt echivalente următoarele afirmații:

1)  $A$  este subcorp al lui  $(K, +, \cdot)$ .

2)  $A$  verifică condițiile:

$$\alpha) |A| \geq 2;$$

$$\beta) a_1, a_2 \in A \Rightarrow a_1 - a_2 \in A;$$

$$\gamma) a_1, a_2 \in A; a_2 \neq 0 \Rightarrow a_1 a_2^{-1} \in A;$$

3)  $A$  verifică condițiile:

$$\alpha) |A| \geq 2;$$

$$\beta') a_1, a_2 \in A \Rightarrow a_1 + a_2 \in A;$$

$$\beta'') a \in A \Rightarrow -a \in A;$$

$$\gamma') a_1, a_2 \in A \Rightarrow a_1 a_2 \in A;$$

$$\gamma'') a \in A; a \neq 0 \Rightarrow a^{-1} \in A.$$

*Demonstrație.* Rezultă din Observațiile 2.46 a) și b) și din Teorema 2.17. □

**Exemplele 2.48.** a)  $\mathbb{Q}$  este subcorp în  $\mathbb{R}$  și în  $\mathbb{C}$ , iar  $\mathbb{R}$  este subcorp în  $\mathbb{C}$ .

b)  $\mathbb{Z}$  nu e subcorp în  $\mathbb{Q}$ .

c) Dacă  $K$  este corp atunci  $\{0\}$  este subinel al lui  $K$ , dar nu este subcorp, iar  $K$  este un subcorp al lui  $K$ .

**Definițiile 2.49.** Fie  $(R, +, \cdot)$  și  $(R', +, \cdot)$  două inele. O funcție  $f : R \rightarrow R'$  se numește **omomorfism (de inele)** dacă pentru orice  $x_1, x_2 \in R$ ,

$$f(x_1 + x_2) = f(x_1) + f(x_2) \text{ și } f(x_1 x_2) = f(x_1) f(x_2). \quad (2)$$

Un omomorfism bijectiv de inele se numește **izomorfism (de inele)**. Un omomorfism al lui  $(R, +, \cdot)$  în el însuși se numește **endomorfism al inelului**  $(R, +, \cdot)$ . Un izomorfism al lui  $(R, +, \cdot)$  pe el însuși se numește **automorfism al inelului**  $(R, +, \cdot)$ . Dacă există un izomorfism  $f : R \rightarrow R'$ , atunci se spune că inelele  $(R, +, \cdot)$  și  $(R', +, \cdot)$  sunt **izomorfe** și vom scrie  $R \simeq R'$  sau  $(R, +, \cdot) \simeq (R', +, \cdot)$ .

Fie  $(R, +, \cdot)$  și  $(R', +, \cdot)$  inele cu unitate ( $1$  și  $1'$  fiind, respectiv, unitățile lor). Un **omomorfism**  $f : R \rightarrow R'$  se numește **unital** dacă

$$f(1) = 1' \quad (3)$$

**Observația 2.50.** Prima condiție din (2) arată că dacă  $f : R \rightarrow R'$  este un omomorfism între inelele  $(R, +, \cdot)$  și  $(R', +, \cdot)$ , atunci  $f$  este omomorfism al grupului  $(R, +)$  în  $(R', +)$ .

**Teorema 2.51.** Fie  $(R, +, \cdot)$ ,  $(R', +, \cdot)$  inele și  $f : R \rightarrow R'$  un omomorfism. Atunci

$$f(0) = 0 \text{ și } f(-x) = -f(x), \forall x \in R. \quad (4)$$

Dacă  $R$  și  $R'$  sunt inele cu unitate,  $f$  este omomorfism unital și  $x \in R$  e inversabil, atunci

$$f(x^{-1}) = [f(x)]^{-1}. \quad (5)$$

*Demonstrație.* Din (1) rezultă că  $f$  este un omomorfism al grupului  $(R, +)$  în  $(R', +)$  de unde, conform Teoremei 2.21, rezultă (4). Din

$$x x^{-1} = 1 = x^{-1} x$$

și din (3) urmează

$$f(x) f(x^{-1}) = 1' = f(x^{-1}) f(x)$$

ceea ce demonstrează pe (5). □

**Exemplele 2.52.** a) Dacă  $(R, +, \cdot)$  și  $(R', +, \cdot)$  sunt inele, atunci funcția  $\theta : R \rightarrow R'$ ,  $\theta(x) = 0$  este un omomorfism numit **omomorfismul nul** sau **zero**. Dacă  $R$  și  $R'$  sunt cu unitate și  $|R'| \geq 2$ , atunci omomorfismul  $\theta$  nu este unital.

b) Fie  $f : \mathbb{C} \rightarrow \mathbb{C}$ ,  $f(z) = \bar{z}$  (unde  $\bar{z}$  este conjugatul lui  $z$ ). Din

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2, \quad \overline{z_1 z_2} = \bar{z}_1 \bar{z}_2 \text{ și } \bar{\bar{z}} = z$$

rezultă că  $f$  este un automorfism al corpului  $(\mathbb{C}, +, \cdot)$  și  $f^{-1} = f$ .

c) Fie  $R$  un inel,  $n \in \mathbb{N}^*$  și  $M_n(R)$  inelul matricelor pătrate cu elemente din  $R$ . Funcția  $f : R \rightarrow M_n(R)$  definită astfel

$$f(a) = \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & a \end{pmatrix}$$

este un omomorfism injectiv de inele.

**Observația 2.53.** Orice omomorfism nenul dintre două corpuri este unital.

Într-adevăr, dacă  $(K, +, \cdot)$  și  $(K', +, \cdot)$  sunt corpuri, iar  $f : K \rightarrow K'$  este un omomorfism nenul, atunci există  $x_0 \in K$  astfel încât  $f(x_0) \neq 0$ . Cum

$$1 \cdot x_0 = x_0 \Rightarrow f(1)f(x_0) = f(x_0) = 1'f(x_0),$$

înmulțind la dreapta ambii membri cu inversul lui  $f(x_0)$ , obținem  $f(1) = 1'$ .

## 2.4 Exerciții rezolvate

1) Fie  $M$  o mulțime și  $\mathcal{P}(M)$  mulțimea submulțimilor lui  $M$ . Definim pe  $\mathcal{P}(M)$  două operații  $+$  și  $\cdot$  astfel:

$$X + Y = (X \setminus Y) \cup (Y \setminus X) \text{ și } X \cdot Y = X \cap Y.$$

Să se arate că:

- i)  $(\mathcal{P}(M), +, \cdot)$  este inel asociativ, comutativ, cu unitate;
- ii) dacă  $|M| \geq 2$  atunci orice  $X \in \mathcal{P}(M) \setminus \{\emptyset, M\}$  este divizor al lui zero;
- iii)  $(\mathcal{P}(M), +, \cdot)$  este corp dacă și numai dacă  $|M| = 1$ .

*Soluție:* i) Observăm că  $X + Y$  este diferența simetrică a mulțimilor  $X$  și  $Y$ , iar din Exercițiul rezolvat 1) de la secțiunea anterioară deducem că  $(\mathcal{P}(M), +)$  este grup abelian. Din proprietățile intersecției și definiția operației  $\cdot$  rezultă că  $\cdot$  este asociativă, comutativă și  $M$  este element neutru. Deci  $(\mathcal{P}(M), \cdot)$  este monoid comutativ.

Stabilim distributivitatea operației  $\cdot$  față de  $+$ . Într-adevăr,

$$\begin{aligned} X \cdot Y + X \cdot Z &= (X \cap Y) + (X \cap Z) \\ &= [(X \cap Y) \cap C(X \cap Z)] \cup [(X \cap Z) \cap C(X \cap Y)] \\ &= [X \cap Y \cap (C(X) \cup C(Z))] \cup [X \cap Z \cap (C(X) \cup C(Y))] \\ &= [X \cap Y \cap C(X)] \cup [X \cap Y \cap C(Z)] \cup [X \cap Z \cap C(X)] \cup [X \cap Z \cap C(Y)] \\ &= \emptyset \cup [X \cap Y \cap C(Z)] \cup \emptyset \cup [X \cap Z \cap C(Y)] \\ &= [X \cap Y \cap C(Z)] \cup [X \cap Z \cap C(Y)] = X \cap [(Y \cap C(Z)) \cup (Z \cap C(Y))] \\ &= X \cdot (Y + Z), \end{aligned}$$

ceea ce arată că  $\cdot$  este distributivă în raport cu  $+$ . Deci  $(\mathcal{P}(M), +, \cdot)$  este inel asociativ, comutativ, cu unitate. Elementul zero, respectiv elementul unitate este  $\emptyset$ , respectiv  $M$ .

ii) În acest inel avem, pentru orice  $X \subseteq M$ ,  $X^2 = X$ , adică  $X(X - 1) = 0$ , sau echivalent,  $X(X + M) = \emptyset$ , ceea ce arată că orice  $X \in \mathcal{P}(M) \setminus \{\emptyset, M\}$  este divizor al lui zero.

iii) Din ii) rezultă că inelul  $(\mathcal{P}(M), +, \cdot)$  este fără divizori ai lui zero dacă și numai dacă  $\mathcal{P}(M) = \{\emptyset, M\}$ , adică  $|M| \leq 1$ . Dacă  $|M| = 0$  atunci  $M = \emptyset$  și  $(\mathcal{P}(M), +, \cdot)$  este inelul nul, iar dacă  $|M| = 1$  atunci  $(\mathcal{P}(M), +, \cdot)$  este izomorf cu  $(\mathbb{Z}_2, +, \cdot)$ , de unde rezultă că  $(\mathcal{P}(M), +, \cdot)$  este corp.

2) Fie  $(R, +, \cdot)$  un inel asociativ și  $a, b \in R$ . Să se arate că:

a)  $(a + b)^2 = a^2 + 2ab + b^2 \Leftrightarrow ab = ba \Leftrightarrow a^2 - b^2 = (a - b)(a + b)$ ;

b) dacă  $ab = ba$  atunci pentru orice  $n \in \mathbb{N}^*$  avem

$$\begin{aligned} (a + b)^n &= C_n^0 a^n + C_n^1 a^{n-1} b + \dots + C_n^{n-1} a b^{n-1} + C_n^n b^n; \\ a^n - b^n &= (a - b) (a^{n-1} + a^{n-2} b + \dots + a b^{n-2} + b^{n-1}); \\ a^{2n+1} + b^{2n+1} &= (a + b) (a^{2n} - a^{2n-1} b + \dots - a b^{2n-1} + b^{2n}). \end{aligned}$$

*Soluție:* a) Dacă  $(a + b)^2 = a^2 + 2ab + b^2$  atunci  $a^2 + ab + ba + b^2 = a^2 + ab + ab + b^2$ , iar cum în grupul  $(R, +)$  se poate simplifica cu orice element, deducem că  $ab = ba$ . Din  $a^2 - b^2 = (a - b)(a + b)$  rezultă  $a^2 - b^2 = a^2 + ab - ba - b^2$ , de unde urmează că  $0 = ab - ba$ , adică  $ab = ba$ . Dacă  $ab = ba$  atunci cele două egalități se verifică imediat.

b) Ținem seama de faptul că orice puteri (cu exponent natural nenul) ale elementelor  $a, b$  comută și procedăm prin inducție după  $n$ . Pentru  $n = 1$  afirmația este, evident, adevărată, iar dacă egalitatea este adevărată pentru  $n$  atunci

$$\begin{aligned} (a + b)^{n+1} &= (a + b)^n (a + b) = (C_n^0 a^n + C_n^1 a^{n-1} b + \dots + C_n^{n-1} a b^{n-1} + C_n^n b^n) a \\ &\quad + (C_n^0 a^n + C_n^1 a^{n-1} b + \dots + C_n^{n-1} a b^{n-1} + C_n^n b^n) b \\ &= C_n^0 a^{n+1} + (C_n^1 + C_n^0) a^n b + \dots + (C_n^{n-1} + C_n^n) a b^n + C_n^n b^{n+1}. \end{aligned}$$

Cum  $C_n^0 = C_n^n = 1$  și  $C_n^k + C_n^{k-1} = C_{n+1}^k$  pentru orice  $n \in \mathbb{N}^*$  și  $1 \leq k \leq n$ , avem

$$(a + b)^{n+1} = C_{n+1}^0 a^{n+1} + C_{n+1}^1 a^n b + \dots + C_{n+1}^n a b^n + C_{n+1}^{n+1} b^{n+1},$$

ceea ce finalizează raționamentul prin inducție. Celelalte egalități se obțin efectuând calculul din membrul drept.

3) Fie  $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$  și  $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ . Să se arate că:

i)  $\mathbb{Z}[\sqrt{2}]$  este un subinel al lui  $(\mathbb{R}, +, \cdot)$  care conține pe 1;

ii)  $\mathbb{Q}(\sqrt{2})$  este un subcorp al lui  $(\mathbb{R}, +, \cdot)$ ;

iii)  $S_1 = \{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Z}\}$  nu este subinel al lui  $(\mathbb{R}, +, \cdot)$ ;

iv)  $S_2 = \{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\}$  nu este subcorp al lui  $(\mathbb{R}, +, \cdot)$ .

*Soluție:* i) Evident  $\mathbb{Z}[\sqrt{2}] \neq \emptyset$ . Pentru orice  $u = a + b\sqrt{2}$ ,  $u' = a' + b'\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$  ( $a, a', b, b' \in \mathbb{Z}$ ) avem:

$$u - u' = (a - a') + (b - b')\sqrt{2} \in \mathbb{Z}[\sqrt{2}], \quad uu' = (aa' + 2bb') + (ab' + a'b)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

și  $1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ . Deci  $\mathbb{Z}[\sqrt{2}]$  este subinel și  $1 \in \mathbb{Z}[\sqrt{2}]$ .

ii) Evident că  $|\mathbb{Q}(\sqrt{2})| \geq 2$ . Analog cu i) se arată că pentru orice  $u, u' \in \mathbb{Q}(\sqrt{2})$  avem  $u - u', uu' \in \mathbb{Q}(\sqrt{2})$ . Fie  $u = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ ,  $u \neq 0$ . Aceasta înseamnă că  $a, b \in \mathbb{Q}$  și  $a^2 - 2b^2 \neq 0$  și astfel,

$$u^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} \sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Deci  $\mathbb{Q}(\sqrt{2})$  este subcorp.

iii) Fie  $u = \sqrt[3]{2}$ . Evident că  $u \in S_1$ . Arătăm că  $u^2 \notin S_1$ . Dacă am avea  $u^2 \in S_1$  ar rezulta că  $u^2 = a + bu$  cu  $a, b \in \mathbb{Z}$ , ceea ce implică  $u^3 = au + bu^2$ , adică

$$2 = au + b(a + bu) = ab + (a + b^2)u,$$

dar  $u$  fiind irațional, urmează  $ab = 2$  și  $a + b^2 = 0$ . Acest sistem nu are soluții în  $\mathbb{Z}$ . Deci  $S_1$  nu este stabilă în raport cu  $\cdot$  și astfel  $S_1$  nu este subinel în  $(\mathbb{R}, +, \cdot)$ .

iv) Se arată la fel ca și în iii) că  $u = \sqrt[3]{2} \in S_2$ , dar  $u^2 \notin S_2$ .

4) Să se determine automorfismele corpului  $\mathbb{Q}(\sqrt{2})$ .

*Soluție:* Presupunem că  $f : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$  este un automorfism. Cum omomorfismele nenule de corpuri sunt unitale,  $f(1) = 1$ .

Dacă  $m, n \in \mathbb{N}^*$  atunci  $f\left(\frac{m}{n}\right) = f\left(\underbrace{\frac{1}{n} + \dots + \frac{1}{n}}_{m \text{ termeni}}\right) = mf\left(\frac{1}{n}\right)$ . Rezultă că

$$1 = f(1) = f\left(\frac{n}{n}\right) = nf\left(\frac{1}{n}\right),$$

deci  $f\left(\frac{1}{n}\right) = \frac{1}{n}f(1) = \frac{1}{n}$ ,  $f\left(\frac{m}{n}\right) = \frac{m}{n}f(1) = \frac{m}{n}$ , iar  $f\left(-\frac{m}{n}\right) = -f\left(\frac{m}{n}\right) = -\frac{m}{n}$ .

Așadar,  $f(x) = x$  pentru orice  $x \in \mathbb{Q}$ . De aici și din  $(\sqrt{2})^2 = 2$  rezultă  $[f(\sqrt{2})]^2 = 2$ , ceea ce implică  $f(\sqrt{2}) \in \{-\sqrt{2}, \sqrt{2}\}$ . Deci  $f \in \{f_1, f_2\}$ , unde  $f_1(a + b\sqrt{2}) = a + b\sqrt{2}$  și  $f_2(a + b\sqrt{2}) = a - b\sqrt{2}$ . Din  $f_1 = 1_{\mathbb{Q}(\sqrt{2})}$  rezultă că  $f_1$  este automorfism. Avem  $f_2 \circ f_2 = 1_{\mathbb{Q}(\sqrt{2})}$ , ceea ce implică  $f_2$  bijectiv și  $f_2^{-1} = f_2$ . Se verifică ușor că  $f_2$  este omomorfism. Deci și  $f_2$  este automorfism. În concluzie, automorfismele corpului  $\mathbb{Q}(\sqrt{2})$  sunt  $f_1$  și  $f_2$ .

5) Să se arate că singurul endomorfism nenul al corpului  $(\mathbb{R}, +, \cdot)$  este  $1_{\mathbb{R}}$ .

*Soluție:* Fie  $f$  un endomorfism al lui  $(\mathbb{R}, +, \cdot)$ . Avem  $(f(1))^2 = f(1)$ , deci  $f(1) = 1$  sau  $f(1) = 0$ , caz în care  $f$  este omomorfismul nul. Dacă  $f$  este nenul atunci  $f$  este injectiv. Ca în problema anterioară, se arată că  $f(x) = x$  pentru orice  $x \in \mathbb{Q}$ , iar dacă  $x \in \mathbb{R}$ ,  $x > 0$  atunci  $f(x) = f((\sqrt{x})^2) = (f(\sqrt{x}))^2 > 0$  (faptul că inegalitatea e strică provine din injectivitatea lui  $f$ ). Rezultă că pentru orice  $x, y \in \mathbb{R}$  cu  $x < y$  avem

$$f(y) - f(x) = f(y - x) > 0,$$

deci  $f$  este strict crescătoare. Considerând pentru un  $a \in \mathbb{R} \setminus \mathbb{Q}$  șirul  $(a'_n)_{n \in \mathbb{N}}$  al aproximărilor sale raționale prin lipsă și șirul  $(a''_n)_{n \in \mathbb{N}}$  al aproximărilor sale raționale prin adaos, obținem  $a'_n \leq a \leq a''_n$  pentru orice  $n \in \mathbb{N}$ , prin urmare

$$a'_n = f(a'_n) \leq f(a) \leq f(a''_n) = a''_n$$

pentru orice  $n \in \mathbb{N}$ . Trecând la limită obținem  $f(a) = a$ . Deci  $f = 1_{\mathbb{R}}$ .



## 2.5 Exerciții propuse

- 1) Fie  $x, y \in \mathbb{R}$  și  $x * y = xy - 5x - 5y + 30$ . Este  $(\mathbb{R}, *)$  grup? Dar  $(\mathbb{R} \setminus \{5\}, *)$ ?  
2) Fie  $(G, \cdot)$  un grup și  $a, b \in G$  astfel încât  $ab = ba$ . Arătați că

$$a^m b^n = b^n a^m, \quad \forall m, n \in \mathbb{Z}.$$

- 3) Demonstrați Propoziția 2.10.  
4) Fie  $(G, \cdot)$  un grup și  $f, g : G \rightarrow G$ ,  $f(x) = x^{-1}$ ,  $g(x) = x^2$ . Să se arate că:  
i)  $f$  este o bijecție;  
ii)  $f$  este automorfism dacă și numai dacă  $(G, \cdot)$  este abelian;  
iii)  $g$  este omomorfism dacă și numai dacă  $(G, \cdot)$  este abelian.  
5) Să se arate că  $H \subseteq \mathbb{Z}$  este subgrup al lui  $(\mathbb{Z}, +)$  dacă și numai dacă există un unic  $n \in \mathbb{N}$  astfel încât  $H = n\mathbb{Z}$ .  
6) Fie  $n \in \mathbb{N}$ ,  $n \geq 2$ . Să se arate că există un singur omomorfism de la grupul  $(\mathbb{Z}_n, +)$  la grupul  $(\mathbb{Z}, +)$ .  
7) Să se arate că dacă  $f : \mathbb{Q} \rightarrow \mathbb{Q}$  este un endomorfism al grupului  $(\mathbb{Q}, +)$  atunci

$$f(x) = f(1) \cdot x, \quad \forall x \in \mathbb{Q},$$

adică  $f$  este o translație a lui  $(\mathbb{Q}, \cdot)$  și că orice translație a lui  $(\mathbb{Q}, \cdot)$  este un endomorfism al lui  $(\mathbb{Q}, +)$ . Să se determine apoi automorfismele lui  $(\mathbb{Q}, +)$ .

- 8) Fie  $a \in \mathbb{Z}$ . Să se arate că  $\widehat{a} \in \mathbb{Z}_n$  este inversabil în  $\mathbb{Z}_n$  dacă și numai dacă  $(a, n) = 1$ . Să se deducă de aici că inelul  $(\mathbb{Z}_n, +, \cdot)$  este corp dacă și numai dacă  $n$  este număr prim.  
9) a) Să se rezolve în  $\mathbb{Z}_{12}$  ecuațiile  $\widehat{4}x + \widehat{5} = \widehat{9}$  și  $\widehat{5}x + \widehat{5} = \widehat{9}$  și în  $M_2(\mathbb{C})$  ecuația

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} X = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}.$$

- b) Să se rezolve în  $\mathbb{Z}_{12}$  sistemul:

$$\begin{cases} \widehat{3}x + \widehat{4}y = \widehat{11} \\ \widehat{4}x + \widehat{9}y = \widehat{10} \end{cases}.$$

10) Un număr  $d \in \mathbb{Z}$  se numește **întreg liber de pătrate** dacă  $d \neq 1$  și  $d$  nu se divide prin pătratul nici unui număr prim. Fie  $d$  un întreg liber de pătrate. Să se arate că:

- i)  $\sqrt{d} \notin \mathbb{Q}$ ;  
ii)  $a, b \in \mathbb{Q}$  și  $a + b\sqrt{d} = 0$  implică  $a = b = 0$ ;  
iii)  $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$  este un subinel în  $(\mathbb{C}, +, \cdot)$  care conține pe 1;  
iv)  $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$  este un subcorp al lui  $(\mathbb{R}, +, \cdot)$ .  
11) Să se arate că singurul omomorfism nenul de corpuri de la  $(\mathbb{Q}, +, \cdot)$  la  $(\mathbb{C}, +, \cdot)$  este omomorfismul de incluziune  $i : \mathbb{Q} \rightarrow \mathbb{C}$ ,  $i(x) = x$ .

## 3 Spații vectoriale (de Ioan Purdea și Cosmin Pelea)

### 3.1 Spații, subspații, transformări liniare

**Definiția 3.1.** Fie  $K$  un corp comutativ. O pereche ordonată formată dintr-un grup abelian  $(V, +)$  și o funcție  $\varphi : K \times V \rightarrow V$  se numește  **$K$ -spațiu vectorial (liniar) stâng** sau **spațiu vectorial (liniar) stâng peste  $K$**  dacă verifică următoarele axiome:

- 1)  $\varphi(\alpha + \beta, x) = \varphi(\alpha, x) + \varphi(\beta, x)$ ;
- 2)  $\varphi(\alpha, x + y) = \varphi(\alpha, x) + \varphi(\alpha, y)$ ;
- 3)  $\varphi(\alpha\beta, x) = \varphi(\alpha, \varphi(\beta, x))$ ;
- 4)  $\varphi(1, x) = x$

pentru orice  $\alpha, \beta \in K$  și  $x, y \in V$ .

Elementele din  $K$ , respectiv  $V$  se numesc **scalari**, respectiv **vectori**. Funcția  $\varphi$  se numește **operație externă** pe  $V$  cu domeniul de operatori  $K$  sau înmulțire cu scalari, iar  $+$  din  $V$  **operație internă** sau adunare a vectorilor. De cele mai multe ori — și așa vom face și noi în cele ce urmează — vom folosi  $\cdot$  în loc de  $\varphi$ . Astfel,  $\varphi(\alpha, x)$  se notează cu  $\alpha x$  (sau cu  $x\alpha$ ) și se numește **produsul** dintre scalarul  $\alpha$  și vectorul  $x$ . Cu aceste notații axiomele de mai sus se transcriu astfel:

- 1)  $(\alpha + \beta)x = \alpha x + \beta x$ ;
- 2)  $\alpha(x + y) = \alpha x + \alpha y$ ;
- 3)  $(\alpha\beta)x = \alpha(\beta x)$ ;
- 4)  $1x = x$ .

**Observația 3.2.** Atragem atenția că  $+$  și  $\cdot$  notează fiecare câte două operații. De exemplu, în axioma 1) primul  $+$  este operația din corp, iar al doilea este operația din grup, iar în axioma 3), în membrul stâng, primul  $\cdot$  este operația din corp, iar al doilea este operația externă, în timp ce în membrul drept ambii  $\cdot$  simbolizează operația externă.

**Teorema 3.3.** Dacă  $V$  este un  $K$ -spațiu vectorial, atunci:

- i) Pentru orice  $\alpha \in K$ , funcția  $t_\alpha : V \rightarrow V$ ,  $t_\alpha(x) = \alpha x$  este un endomorfism al grupului  $(V, +)$ . Dacă, în plus,  $\alpha \neq 0$  atunci  $t_\alpha$  este un automorfism al lui  $(V, +)$  și  $t_\alpha^{-1} = t_{\alpha^{-1}}$ .
- ii) Pentru orice  $x \in V$  funcția  $t'_x : K \rightarrow V$ ,  $t'_x(\alpha) = \alpha x$  este un omomorfism al grupului  $(K, +)$  în grupul  $(V, +)$ .

*Demonstrație.* i) Pentru orice  $x, y \in V$  avem,

$$t_\alpha(x + y) = \alpha(x + y) = \alpha x + \alpha y = t_\alpha(x) + t_\alpha(y)$$

ceea ce ne arată că  $t_\alpha \in \text{End}(V, +)$ . Dacă  $\alpha \neq 0$  atunci

$$(t_\alpha \circ t_{\alpha^{-1}})(x) = t_\alpha(t_{\alpha^{-1}}(x)) = \alpha(\alpha^{-1}x) = (\alpha\alpha^{-1})x = 1x = x = 1_V(x)$$

ceea ce ne arată că  $t_\alpha \circ t_{\alpha^{-1}} = 1_V$ . Analog se arată că  $t_{\alpha^{-1}} \circ t_\alpha = 1_V$ . Deci

$$t_\alpha \in \text{Aut}(V, +) \text{ și } t_\alpha^{-1} = t_{\alpha^{-1}}.$$

- ii) Pentru orice  $\alpha, \beta \in K$  are loc:

$$t'_x(\alpha + \beta) = (\alpha + \beta)x = \alpha x + \beta x = t'_x(\alpha) + t'_x(\beta).$$

Deci  $t'_x$  este un omomorfism al lui  $(K, +)$  în  $(V, +)$ . □

**Corolarul 3.4. (Reguli de calcul într-un spațiu vectorial)**

- a) Pentru orice  $\alpha \in K$  și  $x \in V$  avem:

$$\alpha x = 0 \Leftrightarrow \alpha = 0 \text{ sau } x = 0.$$

b) Pentru orice  $\alpha, \beta \in K$  și  $x, y \in V$  avem:

$$(\alpha - \beta)x = \alpha x - \beta x \text{ și } \alpha(x - y) = \alpha x - \alpha y.$$

c) Pentru orice  $\alpha, \alpha_1, \dots, \alpha_n \in K$  și  $x, x_1, \dots, x_n \in V$  avem:

$$(\alpha_1 + \dots + \alpha_n)x = \alpha_1 x + \dots + \alpha_n x \text{ și } \alpha(x_1 + \dots + x_n) = \alpha x_1 + \dots + \alpha x_n.$$

**Exemplele 3.5.** a) Fie  $O$  un punct fixat într-un plan fixat. Fiecărui punct  $M$  al planului  $i$  se asociază vectorul (segmentul orientat)  $\overrightarrow{OM}$  numit vectorul de poziție al punctului  $M$  (relativ la originea  $O$ ). Notăm cu  $V_2$  mulțimea tuturor vectorilor  $\overrightarrow{OM}$  când  $M$  parcurge punctele planului fixat. Mulțimea  $V_2$  este  $\mathbb{R}$  - spațiu vectorial în raport cu adunarea vectorilor după regula paralelogramului și înmulțirea cu scalari definită astfel: dacă  $\alpha \in \mathbb{R}$  atunci  $\alpha \overrightarrow{OM}$  este vectorul cu originea în  $O$  care are direcția lui  $\overrightarrow{OM}$ , sensul lui  $\overrightarrow{OM}$  dacă  $\alpha > 0$  și sens contrar lui  $\overrightarrow{OM}$  dacă  $\alpha < 0$ , iar lungimea (modulul) este produsul dintre  $|\alpha|$  și lungimea lui  $\overrightarrow{OM}$ . Dacă  $\alpha = 0$  sau  $\overrightarrow{OM}$  este vectorul nul atunci  $\alpha \overrightarrow{OM}$  este vectorul nul. Relativ la un sistem de coordonate cu originea în  $O$  un vector  $\overrightarrow{OM}$  este reprezentat de coordonatele  $(x, y)$  ale punctului  $M$ , iar operațiile de adunare a vectorilor și de înmulțire a vectorilor cu scalari se exprimă astfel:

$$(x, y) + (x', y') = (x + x', y + y'); \quad \alpha(x, y) = (\alpha x, \alpha y).$$

Coordonatele vectorului  $\overrightarrow{OM}$  (adică ale lui  $M$ ) depind de alegerea sistemului de coordonate. Analog se obține spațiul liniar  $V_3$  al vectorilor din spațiul cu originea într-un punct  $O$ . Un vector din  $V_3$  este determinat în raport cu un sistem de coordonate cu originea în  $O$  de un triplet  $(x, y, z)$  de numere reale.

b) Pe o mulțime dintr-un singur element  $\{0\}$  există o singură operație  $+$  definită prin egalitatea  $0 + 0 = 0$  și  $(\{0\}, +)$  este grup abelian. Pentru orice corp comutativ  $K$  există o singură operație externă

$$K \times \{0\} \rightarrow \{0\}, \quad (\alpha, 0) \mapsto 0.$$

Cele două operații definesc pe  $\{0\}$  o structură de  $K$ -spațiu vectorial. Acest spațiu vectorial se numește **spațiul vectorial zero** sau **nul**.

c) Dacă  $K$  este un corp comutativ, atunci pentru orice  $n \in \mathbb{N}^*$  mulțimea  $K^n$  este un  $K$ -spațiu vectorial în raport cu operațiile definite pe componente astfel:

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n);$$

$$\alpha(x_1, \dots, x_n) = (\alpha x_1, \dots, \alpha x_n),$$

unde  $(x_1, \dots, x_n), (y_1, \dots, y_n) \in K^n$  și  $\alpha \in K$ .

d) Grupul  $(K, +)$  al unui corp  $(K, +, \cdot)$  este un  $K$ -spațiu vectorial în raport cu operația externă  $K \times K \rightarrow K, (\alpha, x) \mapsto \alpha x$  unde  $\alpha x$  este produsul perechii  $(\alpha, x)$  în  $(K, \cdot)$ . Acest exemplu se obține din c) luând  $n = 1$ .

e) Fie  $K'$  un corp și  $K$  un subcorp al lui  $K'$ . Dacă  $(V, +)$  este un  $K'$ -spațiu vectorial, atunci  $(V, +)$  este un  $K$ -spațiu vectorial în raport cu operația externă  $K \times V \rightarrow V, (\alpha, x) \mapsto \alpha x$  unde  $\alpha x$  este produsul dintre scalarul  $\alpha$  și vectorul  $x$  în  $V$  privit  $K'$ -spațiu vectorial. Se spune că  $K$ -spațiul vectorial  $V$  s-a obținut din  $K'$ -spațiul vectorial  $V$  prin

**restricția corpului de scalari** de la  $K'$  la  $K$ . Astfel  $\mathbb{R}$  este un  $\mathbb{Q}$ -spațiu vectorial, iar  $\mathbb{C}$  este un  $\mathbb{Q}$ -spațiu vectorial și un  $\mathbb{R}$ -spațiu vectorial.

f) Fie  $K$  un corp comutativ și

$$K[X] = \{f = a_0 + a_1X + \cdots + a_nX^n \mid a_0, a_1, \dots, a_n \in K, n \in \mathbb{N}\}$$

mulțimea polinoamelor cu coeficienți în corpul  $K$  în nedeterminata  $X$ . Fie  $f, g \in K[X]$ ,  $f = a_0 + a_1X + \cdots + a_nX^n$ ,  $g = b_0 + b_1X + \cdots + b_nX^n$  (putem considera că ambele polinoame au același număr de termeni, adăugând, dacă e cazul, monoame cu coeficientul 0 în scrierea unuia dintre ele). Egalitatea

$$f + g = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_n + b_n)X^n$$

definește o operație asociativă și comutativă pe  $K[X]$ . Aceasta are element neutru pe  $0 \in K[X]$  (polinomul nul) și orice  $f = a_0 + a_1X + \cdots + a_nX^n \in K[X]$  are un opus, pe

$$-f = -a_0 + (-a_1)X + \cdots + (-a_n)X^n.$$

Grupul abelian  $(K[X], +)$  este un  $K$ -spațiu vectorial în raport cu înmulțirea cu scalari definită astfel: dacă  $\alpha \in K$  și  $f = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ , atunci

$$\alpha f = \alpha a_0 + \alpha a_1X + \cdots + \alpha a_nX^n.$$

g) Fie  $K$  un corp comutativ. Grupul  $(M_{m,n}(K), +)$  al matricelor de tipul  $(m, n)$  cu elemente din  $K$  e un  $K$ -spațiu vectorial în raport cu înmulțirea cu scalari definită astfel:

$$\alpha(a_{ij}) = (\alpha a_{ij}) \quad (\alpha \in K, (a_{ij}) \in M_{m,n}(K)).$$

Să observăm că în cazul matricilor pătratice (de ordin  $n$ ), pe lângă structura de  $K$ -spațiu vectorial a lui  $M_n(K)$  avem și o structură de inel pe  $M_n(K)$  (vezi Exemplitul 2.40 d)). Mai mult, între cele două structuri avem o relație de legătură, și anume:

$$\alpha(AB) = (\alpha A)B = A(\alpha B), \quad \forall \alpha \in K, \forall A, B \in M_n(K).$$

h) Dacă  $V_1$  și  $V_2$  sunt  $K$ -spații vectoriale, atunci produsul cartezian  $V_1 \times V_2$  este  $K$ -spațiu vectorial în raport cu operațiile definite astfel:

$$(x_1, x_2) + (x'_1, x'_2) = (x_1 + x'_1, x_2 + x'_2), \quad \alpha(x_1, x_2) = (\alpha x_1, \alpha x_2)$$

unde  $(x_1, x_2), (x'_1, x'_2) \in V_1 \times V_2$  și  $\alpha \in K$ . Spațiul vectorial astfel obținut se numește **produsul direct** al spațiilor  $V_1$  și  $V_2$ .

**Definiția 3.6.** Fie  $V$  un  $K$ -spațiu vectorial. O submulțime  $A \subseteq V$  se numește **subspațiu** al lui  $V$  dacă

i)  $a_1, a_2 \in A \Rightarrow a_1 + a_2 \in A$ ,

ii)  $\alpha \in K, a \in A \Rightarrow \alpha a \in A$

(adică  $A$  este stabilă în  $(V, +)$  și în raport cu înmulțirea cu scalari) și  $A$  este  $K$ -spațiu vectorial în raport cu operațiile induse.

Faptul că  $A$  este un subspațiu al  $K$ -spațiului vectorial  $V$  îl notăm prin  $A \leq_K V$ .

**Observațiile 3.7.** a) Dacă  $V$  este un  $K$ -spațiu vectorial și  $A \subseteq V$ , atunci  $A$  este un subspațiu dacă și numai dacă  $A$  este subgrup al grupului  $(V, +)$  și  $A$  verifică condiția ii).  
b) Dacă  $A$  este un subspațiu al  $K$ -spațiului vectorial  $V$ , atunci  $0 \in A$ .

Practic, când arătăm că o submulțime a unui spațiu vectorial este subspațiu aplicăm următoarea teoremă.

**Teorema 3.8. (Teorema de caracterizare a subspațiului)**

Fie  $V$  un  $K$ -spațiu vectorial și  $A \subseteq V$ . Sunt echivalente următoarele afirmații:

- 1)  $A$  este subspațiu al lui  $V$ .
- 2)  $A$  verifică condițiile:
  - $\alpha$ )  $A \neq \emptyset$ ;
  - $\beta$ )  $a_1, a_2 \in A \Rightarrow a_1 - a_2 \in A$ ;
  - $\gamma$ )  $\alpha \in K, a \in A \Rightarrow \alpha a \in A$ .
- 3)  $A$  verifică condițiile:
  - $\alpha$ )  $A \neq \emptyset$ ;
  - $\beta'$ )  $a_1, a_2 \in A \Rightarrow a_1 + a_2 \in A$ ;
  - $\gamma$ )  $\alpha \in K, a \in A \Rightarrow \alpha a \in A$ .
- 4)  $A$  verifică condițiile:
  - $\alpha$ )  $A \neq \emptyset$ ;
  - $\beta''$ )  $\alpha_1, \alpha_2 \in K, a_1, a_2 \in A \Rightarrow \alpha_1 a_1 + \alpha_2 a_2 \in A$ .

*Demonstrație.* Echivalența 1)  $\Leftrightarrow$  2) rezultă din Observația 3.7 a) și din faptul că  $\alpha$ ) și  $\beta$ ) sunt condiții necesare și suficiente ca  $A$  să fie subgrup în  $(V, +)$ .

Din teorema de caracterizare a subgrupului rezultă implicația 2)  $\Rightarrow$  3). Din  $\gamma$ ) și  $\beta'$ ) deducem pe  $\beta$ ) astfel:

$$a_1, a_2 \in A \Rightarrow a_1, (-1) \cdot a_2 \in A \Rightarrow a_1, -a_2 \in A \Rightarrow a_1 - a_2 \in A.$$

Deci 3)  $\Rightarrow$  2) și astfel am arătat că 2)  $\Leftrightarrow$  3).

Din  $\gamma$ ) și  $\beta'$ ) deducem pe  $\beta''$ ):

$$\alpha_1, \alpha_2 \in K; a_1, a_2 \in A \Rightarrow \alpha_1 a_1, \alpha_2 a_2 \in A \Rightarrow \alpha_1 a_1 + \alpha_2 a_2 \in A,$$

iar din  $\beta''$ ) luând  $\alpha_1 = \alpha_2 = 1$  rezultă  $\beta'$ ) și luând  $\alpha_1 = \alpha, \alpha_2 = 0, a_1 = a$ , rezultă  $\gamma$ ).  
Deci și echivalența 3)  $\Leftrightarrow$  4) este demonstrată.  $\square$

**Exemplele 3.9.** a) Pentru orice spațiu vectorial  $V$  submulțimile  $\{0\}$  și  $V$  sunt subspații ale lui  $V$ . Un subspațiu al lui  $V$  diferit de  $\{0\}$  și  $V$ , se numește **subspațiu propriu**.

b) Fie  $K$  un corp comutativ și  $K[X]$ ,  $K$ -spațiul vectorial al polinoamelor, iar  $n \in \mathbb{N}^*$ . Se constată ușor că

$$P_n(K) = \{f \in K[X] \mid \text{grad } f \leq n\}$$

verifică pe  $\alpha$ ),  $\beta'$ ),  $\gamma$ ). Deci  $P_n(K)$  este un subspațiu al lui  $K[X]$ .

c) Fie  $V_3$  spațiul vectorial peste  $\mathbb{R}$  al vectorilor (segmentelor orientate) din spațiu cu originea într-un punct  $O$ . Subspațiile lui  $V_3$  sunt:  $\{0\}$ ,  $V_3$ , dreptele care trec prin  $O$  (mai exact mulțimile de vectori de poziție ai punctelor situate pe aceste drepte) și planele care trec prin  $O$  (mulțimile de vectori de poziție conținuți în aceste plane).

d) Fie  $I \subseteq \mathbb{R}$  un interval. Mulțimea  $\mathbb{R}^I = \{f \mid f : I \rightarrow \mathbb{R}\}$  este  $\mathbb{R}$ -spațiu vectorial în raport cu operațiile definite prin:

$$(f + g)(x) = f(x) + g(x), (\alpha f)(x) = \alpha f(x)$$

unde  $f, g \in \mathbb{R}^I$  și  $\alpha \in \mathbb{R}$ . Submulțimile

$$C(I, \mathbb{R}) = \{f \in \mathbb{R}^I \mid f \text{ continuă pe } I\}, D(I, \mathbb{R}) = \{f \in \mathbb{R}^I \mid f \text{ derivabilă pe } I\}$$

sunt subspații ale lui  $\mathbb{R}^I$  pentru că sunt nevide și

$$\alpha, \beta \in \mathbb{R}, f, g \in C(I, \mathbb{R}) \Rightarrow \alpha f + \beta g \in C(I, \mathbb{R});$$

$$\alpha, \beta \in \mathbb{R}, f, g \in D(I, \mathbb{R}) \Rightarrow \alpha f + \beta g \in D(I, \mathbb{R}).$$

**Teorema 3.10.** Dacă  $(A_i)_{i \in I}$  este o familie nevidă de subspații ale  $K$ -spațiului vectorial  $V$ , atunci  $\bigcap_{i \in I} A_i$  este un subspațiu al lui  $V$ .

*Demonstrație.* Din ipoteză avem  $I \neq \emptyset$ . Cum fiecare  $A_i$  este subspațiu rezultă  $0 \in A_i$  pentru toți  $i \in I$ , de unde urmează că  $\bigcap_{i \in I} A_i \neq \emptyset$ . Folosind definiția intersecției și faptul că fiecare  $A_i$  este subspațiu, dacă  $a_1, a_2 \in \bigcap_{i \in I} A_i$  avem:

$$\forall i \in I, a_1, a_2 \in A_i \Rightarrow \forall i \in I, \forall \alpha, \beta \in K, \alpha a_1 + \beta a_2 \in A_i \Rightarrow \forall \alpha, \beta \in K, \alpha a_1 + \beta a_2 \in \bigcap_{i \in I} A_i.$$

Deci  $\bigcap_{i \in I} A_i$  este subspațiu al lui  $V$ . □

Din Teorema 3.10 rezultă că dacă  $X \subseteq V$  atunci

$$\bigcap \{A \leq_K V \mid X \subseteq A\} \tag{1}$$

este un subspațiu al lui  $V$  notat cu  $\langle X \rangle$  numit **subspațiul generat** de  $X$ . Din (1) rezultă că  $\langle X \rangle$  este cel mai mic subspațiu al lui  $V$  care include pe  $X$ . Dacă  $V = \langle X \rangle$  atunci vom spune că  $X$  este un **sistem de generatori** al lui  $V$  sau că  $X$  generează pe  $V$ . Dacă există o submulțime finită  $X \subseteq V$  astfel încât  $V = \langle X \rangle$ , atunci spunem că spațiul  $V$  este de **tip finit** sau **finit generat**. Dacă  $X = \{x_1, \dots, x_n\}$ , vom nota  $\langle X \rangle$  cu  $\langle x_1, \dots, x_n \rangle$ .

**Observația 3.11.** Din definiția subspațiului generat rezultă:

- a)  $\langle \emptyset \rangle = \{0\}$ ;
- b)  $X, Y \subseteq V, X \subseteq Y \Rightarrow \langle X \rangle \subseteq \langle Y \rangle$ ;
- c)  $A \leq_K V \Rightarrow \langle A \rangle = A$ ;
- d)  $X \subseteq V \Rightarrow \langle \langle X \rangle \rangle = \langle X \rangle$ .

**Definiția 3.12.** Fie  $V$  un  $K$ -spațiu vectorial și  $X \subseteq V, X \neq \emptyset$ . O sumă de forma

$$x = \alpha_1 x_1 + \dots + \alpha_n x_n \quad (\alpha_1, \dots, \alpha_n \in K, x_1, \dots, x_n \in X)$$

se numește **combinație liniară** de elemente din  $X$ .

**Teorema 3.13.** Dacă  $V$  este un  $K$ -spațiu vectorial și  $\emptyset \neq X \subseteq V$ , atunci

$$\langle X \rangle = \{\alpha_1 x_1 + \dots + \alpha_n x_n \mid \alpha_k \in K, x_k \in X, k = 1, \dots, n, n \in \mathbb{N}^*\} \tag{2}$$

adică  $\langle X \rangle$  este format din toate combinațiile liniare de elemente din  $X$ .

*Demonstrație.* Notând cu  $A$  membrul doi din (2) avem:

- i)  $X \subseteq S$ ,
- ii)  $x, x' \in A$  și  $\alpha, \beta \in K \Rightarrow \alpha x + \beta x' \in A$ ,
- iii) dacă  $X \subseteq B$  și  $B \leq_K V$ , atunci  $A \subseteq B$ .

Din i), ii) și iii) rezultă că  $A$  este cel mai mic subspațiu care include pe  $X$  ceea ce demonstrează pe (2).  $\square$

**Corolarul 3.14.** a) Dacă  $x \in V$  atunci  $\langle x \rangle = \{\alpha x \mid \alpha \in K\} = Kx$ .

b) Dacă  $x_1, \dots, x_n \in V$  atunci  $\langle x_1, \dots, x_n \rangle = Kx_1 + \dots + Kx_n$ .

În general reuniunea a două subspații ale unui spațiu vectorial nu este un subspațiu.

**Exemplul 3.15.** Mulțimile  $A = \{(a, 0) \mid a \in \mathbb{R}\}$  și  $B = \{(0, b) \mid b \in \mathbb{R}\}$  sunt subspații ale  $\mathbb{R}$ -spațiului vectorial  $\mathbb{R}^2$ , dar  $A \cup B$  nu este subspațiu, nefiind stabilă în raport cu  $+$  ( $(1, 0) \in A \subseteq A \cup B$ ,  $(0, 1) \in B \subseteq A \cup B$ , dar  $(1, 0) + (0, 1) = (1, 1) \notin A \cup B$ ).

Cel mai mic subspațiu ce conține două subspații date rezultă din următoarea teoremă.

**Teorema 3.16.** Fie  $A_1, \dots, A_n$  subspații ale  $K$ -spațiului vectorial  $V$ . Cel mai mic subspațiu al lui  $V$  ce conține toate subspațiile  $A_1, \dots, A_n$  este  $A_1 + \dots + A_n$ , adică

$$A_1 + \dots + A_n = \langle A_1 \cup \dots \cup A_n \rangle.$$

*Demonstrație.* Amintim că

$$A_1 + \dots + A_n = \{a_1 + \dots + a_n \mid a_1 \in A_1, \dots, a_n \in A_n\}.$$

Evident,  $0 \in A_1 + \dots + A_n$ . Din asociativitatea și comutativitatea lui  $+$  din  $V$  rezultă că suma oricăror două elemente din  $A_1 + \dots + A_n$  este în  $A_1 + \dots + A_n$ , iar din Corolarul 3.4 c) rezultă că produsul oricărui element din  $A_1 + \dots + A_n$  cu orice scalar din  $K$  rămâne în  $A_1 + \dots + A_n$ . Așadar,  $A_1 + \dots + A_n$  este subspațiu în  $V$ .

Cum pentru orice  $i \in \{1, \dots, n\}$  și orice  $a_i \in A_i$ , pe  $a_i$  îl regăsim în  $A_1 + \dots + A_n$  ca pe o sumă cu  $n$  termeni, termenul al  $i$ -lea fiind  $a_i$  și ceilalți fiind 0, deducem că

$$A_1 \cup \dots \cup A_n \subseteq A_1 + \dots + A_n,$$

iar dacă  $B$  este un subspațiu al lui  $V$  cu  $A_1 \subseteq B, \dots, A_n \subseteq B$  atunci  $A_1 + \dots + A_n \subseteq B$ , deoarece toate sumele  $a_1 + \dots + a_n$  ( $a_1 \in A_1 \subseteq B, \dots, a_n \in A_n \subseteq B$ ) sunt în  $B$ .

Din definiția subspațiului generat urmează proprietatea din enunț.  $\square$

**Corolarul 3.17.** a) Dacă  $A$  și  $B$  sunt subspații ale lui  $V$ , atunci

$$A + B = \langle A \cup B \rangle.$$

b) Dacă  $X_i \subseteq V$  ( $i = 1, \dots, n$ ), atunci  $\langle X_1 \cup \dots \cup X_n \rangle = \langle X_1 \rangle + \dots + \langle X_n \rangle$ .

Într-adevăr,  $X_i \subseteq X_1 \cup \dots \cup X_n$  implică  $\langle X_i \rangle \subseteq \langle X_1 \cup \dots \cup X_n \rangle$  ( $i = 1, \dots, n$ ) și avem

$$\langle X_1 \cup \dots \cup X_n \rangle \supseteq \langle X_1 \rangle + \dots + \langle X_n \rangle.$$

Cum  $X_i \subseteq \langle X_i \rangle \subseteq \langle X_1 \rangle + \dots + \langle X_n \rangle$  ( $i = 1, \dots, n$ ), avem  $X_1 \cup \dots \cup X_n \subseteq \langle X_1 \rangle + \dots + \langle X_n \rangle$ , prin urmare

$$\langle X_1 \cup \dots \cup X_n \rangle \subseteq \langle \langle X_1 \rangle + \dots + \langle X_n \rangle \rangle = \langle X_1 \rangle + \dots + \langle X_n \rangle.$$

Din Corolarul 3.17 a) rezultă că suma a două subspații este un subspațiu. Dacă  $A$  și  $B$  sunt subspații ale lui  $V$  și  $A \cap B = \{0\}$ , subspațiul  $A + B$  se notează cu  $A \oplus B$  și se numește **suma directă** a lui  $A$  și  $B$ . Se verifică ușor că  $A + B = A \oplus B$  dacă și numai dacă orice  $x \in A + B$  se scrie în mod unic sub forma  $x = a + b$  unde  $a \in A$  și  $b \in B$ .

**Definiția 3.18.** Fie  $K$  un corp și  $V, V'$  două  $K$ -spații vectoriale. O funcție  $f : V \rightarrow V'$  se numește **transformare liniară** sau **funcție liniară** sau **aplicație liniară** dacă

$$f(x_1 + x_2) = f(x_1) + f(x_2) \text{ și } f(\alpha x) = \alpha f(x), \forall x, x_1, x_2 \in V, \forall \alpha \in K. \quad (3)$$

O transformare liniară bijectivă se numește **izomorfism** de spații liniare. O transformare liniară a unui spațiu vectorial  $V$  în  $V$  se numește **endomorfism** al lui  $V$ . Un izomorfism al lui  $V$  pe  $V$  se numește **automorfism** al lui  $V$ .

**Observațiile 3.19.** a) O funcție  $f : V \rightarrow V'$  este liniară dacă și numai dacă

$$f(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1 f(x_1) + \alpha_2 f(x_2), \forall x_1, x_2 \in V, \forall \alpha_1, \alpha_2 \in K. \quad (4)$$

Într-adevăr din (3) rezultă

$$f(\alpha_1 x_1 + \alpha_2 x_2) = f(\alpha_1 x_1) + f(\alpha_2 x_2) = \alpha_1 f(x_1) + \alpha_2 f(x_2)$$

adică (3)  $\Rightarrow$  (4). Invers, luând în (4)  $\alpha_1 = \alpha_2 = 1$  obținem prima egalitate din (3), iar dacă  $\alpha_1 = \alpha, x_1 = x$  și  $\alpha_2 = 0, x_2 = 0$  primim a doua egalitate din (3). Deci (4)  $\Rightarrow$  (3) și astfel s-a arătat că (3)  $\Leftrightarrow$  (4).

b) Dacă  $f : V \rightarrow V'$  este o transformare liniară, atunci

$$f(\alpha_1 x_1 + \dots + \alpha_n x_n) = \alpha_1 f(x_1) + \dots + \alpha_n f(x_n), \forall x_1, \dots, x_n \in V, \forall \alpha_1, \dots, \alpha_n \in K.$$

c) Dacă  $f : V \rightarrow V'$  este o transformare liniară, atunci  $f$  este un omomorfism între grupurile  $(V, +)$  și  $(V', +)$  de unde rezultă

$$f(0) = 0 \text{ și } f(-x) = -f(x), \forall x \in V.$$

d) Dacă  $V, V'$  și  $V''$  sunt  $K$ -spații vectoriale și  $f : V \rightarrow V', g : V' \rightarrow V''$  sunt transformări liniare, atunci  $g \circ f$  este transformare liniară.

Într-adevăr,

$$\begin{aligned} (g \circ f)(\alpha_1 x_1 + \alpha_2 x_2) &= g(f(\alpha_1 x_1 + \alpha_2 x_2)) = g(\alpha_1 f(x_1) + \alpha_2 f(x_2)) = \\ &= \alpha_1 g(f(x_1)) + \alpha_2 g(f(x_2)) = \alpha_1 (g \circ f)(x_1) + \alpha_2 (g \circ f)(x_2) \end{aligned}$$

pentru orice  $x_1, x_2 \in V$  și  $\alpha_1, \alpha_2 \in K$ , ceea ce ne arată că  $g \circ f$  este liniară.

e) Dacă  $f : V \rightarrow V'$  este izomorfism de spații vectoriale, atunci  $f^{-1}$  este izomorfism de spații vectoriale.

Într-adevăr trebuie arătat

$$f^{-1}(\alpha_1 y_1 + \alpha_2 y_2) = \alpha_1 f^{-1}(y_1) + \alpha_2 f^{-1}(y_2), \forall y_1, y_2 \in V', \forall \alpha_1, \alpha_2 \in K. \quad (5)$$

Notând  $f^{-1}(y_i) = x_i, i = 1, 2$  avem  $f(x_1) = y_1, f(x_2) = y_2$ , prin urmare,

$$\alpha_1 y_1 + \alpha_2 y_2 = \alpha_1 f(x_1) + \alpha_2 f(x_2) = f(\alpha_1 x_1 + \alpha_2 x_2).$$



Deci,

$$f^{-1}(\alpha_1 y_1 + \alpha_2 y_2) = \alpha_1 x_1 + \alpha_2 x_2 = \alpha_1 f^{-1}(y_1) + \alpha_2 f^{-1}(y_2),$$

ceea ce demonstrează pe (5).

f) Fie  $V$  un  $K$ -spațiu vectorial,  $End(V, +)$  respectiv  $End_K(V)$  mulțimea endomorfismelor grupului  $(V, +)$  respectiv  $K$ -spațiului vectorial  $V$ . Din Observația 3.19 d) rezultă că  $End_K(V)$  este stabilă în  $(End(V, +), \circ)$ , iar  $(End_K(V), \circ)$  este monoid.

g) Mulțimea  $Aut_K(V)$  a automorfismelor spațiului vectorial  $V$  este un subgrup al grupului  $(Aut(V, +), \circ)$  al automorfismelor grupului  $(V, +)$ .

h) Dacă  $f : V \rightarrow V'$  este transformare liniară și  $X \subseteq V$ , atunci

$$f(\langle X \rangle) = \langle f(X) \rangle.$$

Într-adevăr, dacă  $X = \emptyset$ , egalitatea de mai sus devine  $f(\{0\}) = \{0\}$  și este, evident, adevărată. Dacă  $X \neq \emptyset$ ,  $y \in \langle f(X) \rangle$  dacă și numai dacă

$$\exists n \in \mathbb{N}^*, \exists \alpha_1, \dots, \alpha_n \in K, \exists x_1, \dots, x_n \in X : y = \sum_{i=1}^n \alpha_i f(x_i) = f\left(\sum_{i=1}^n \alpha_i x_i\right),$$

ceea ce este echivalent cu  $y \in f(\langle X \rangle)$ .

**Exemplele 3.20.** a) Pentru orice  $K$ -spații vectoriale  $V$  și  $V'$  funcția  $\theta : V \rightarrow V'$ ,  $\theta(x) = 0$  este o transformare liniară numită transformarea liniară **nulă** sau **zero**.

Într-adevăr  $\theta(\alpha_1 x_1 + \alpha_2 x_2) = 0 = 0 + 0 = \alpha_1 0 + \alpha_2 0 = \alpha_1 \theta(x_1) + \alpha_2 \theta(x_2)$  pentru orice  $x_1, x_2 \in V$  și orice  $\alpha_1, \alpha_2 \in K$ , ceea ce ne arată că  $\theta$  este liniară.

b) Pentru orice  $K$ -spațiu vectorial  $V$  aplicația identică  $1_V : V \rightarrow V$ ,  $1_V(x) = x$  este automorfism al lui  $V$ . Acest automorfism este element neutru în  $(End_K(V), \circ)$ .

c) Fie  $\varphi \in \mathbb{R}$  fixat. Funcția

$$f : \mathbb{R}^2 \rightarrow \mathbb{R}^2, f(x, y) = (x \cos \varphi - y \sin \varphi, x \sin \varphi + y \cos \varphi),$$

adică rotația planului de unghi  $\varphi$ , este o transformare liniară.

d) Fie  $a, b \in \mathbb{R}$ ,  $a < b$ ,  $I = [a, b]$ ,  $C(I, \mathbb{R}) = \{f : I \rightarrow \mathbb{R} \mid f \text{ continuă pe } I\}$ . Funcția

$$F : C(I, \mathbb{R}) \rightarrow \mathbb{R}, F(f) = \int_a^b f(x) dx$$

este o transformare liniară.

Într-adevăr, pentru orice  $f, g \in C(I, \mathbb{R})$  și  $\alpha, \beta \in \mathbb{R}$  avem

$$F(\alpha f + \beta g) = \int_a^b (\alpha f(x) + \beta g(x)) dx = \alpha \int_a^b f(x) dx + \beta \int_a^b g(x) dx = \alpha F(f) + \beta F(g)$$

**Teorema 3.21.** Fie  $V$  și  $V'$   $K$ -spații vectoriale. Dacă  $f, g : V \rightarrow V'$  și  $\alpha \in K$ , atunci definim  $f + g : V \rightarrow V'$  și  $\alpha f : V \rightarrow V'$  prin

$$(f + g)(x) = f(x) + g(x) \tag{6}$$

$$(\alpha f)(x) = \alpha f(x). \tag{7}$$

1) Dacă  $f$  și  $g$  sunt transformări liniare, atunci  $f + g$  este o transformare liniară.

2) Dacă  $f$  este transformare liniară, atunci  $\alpha f$  este transformare liniară.

*Demonstrație.* 1) Pentru orice  $x_1, x_2 \in V$  și  $\alpha_1, \alpha_2 \in K$  avem:

$$\begin{aligned}(f+g)(\alpha_1x_1+\alpha_2x_2) &= f(\alpha_1x_1+\alpha_2x_2)+g(\alpha_1x_1+\alpha_2x_2) = \alpha_1f(x_1)+\alpha_2f(x_2)+\alpha_1g(x_1)+\alpha_2g(x_2) = \\ &= \alpha_1(f(x_1)+g(x_1))+\alpha_2(f(x_2)+g(x_2)) = \alpha_1(f+g)(x_1)+\alpha_2(f+g)(x_2),\end{aligned}$$

adică  $f+g$  este transformare liniară.

2) Pentru orice  $x_1, x_2 \in V$  și  $\beta_1, \beta_2 \in K$  avem:

$$\begin{aligned}(\alpha f)(\beta_1x_1+\beta_2x_2) &= \alpha f(\beta_1x_1+\beta_2x_2) = \alpha(\beta_1f(x_1)+\beta_2f(x_2)) = (\alpha\beta_1)f(x_1)+(\alpha\beta_2)f(x_2) = \\ &= (\beta_1\alpha)f(x_1)+(\beta_2\alpha)f(x_2) = \beta_1(\alpha f(x_1))+\beta_2(\alpha f(x_2)) = \beta_1(\alpha f)(x_1)+\beta_2(\alpha f)(x_2),\end{aligned}$$

adică  $\alpha f$  este o transformare liniară.  $\square$

**Corolarul 3.22.** a) Mulțimea  $Hom_K(V, V')$  a transformărilor liniare ale lui  $V$  în  $V'$  este stabilă în raport cu operația definită de (6) și  $(Hom_K(V, V'), +)$  este grup abelian.

Într-adevăr din asociativitatea și comutativitatea operației  $+$  în  $V$  rezultă asociativitatea și comutativitatea operației definită în (6). Funcția  $\theta : V \rightarrow V'$ ,  $\theta(x) = 0$  este liniară și  $\theta$  este element neutru în  $Hom_K(V, V')$ . Pentru orice  $f \in Hom_K(V, V')$  funcția  $-f : V \rightarrow V'$ ,  $(-f)(x) = -f(x)$  este liniară și  $-f$  este simetrica lui  $f$  în  $(Hom_K(V, V'), +)$ .

b) Mulțimea  $Hom_K(V, V')$  este stabilă în raport cu operațiile definite în (6) și (7) și  $Hom_K(V, V')$  este  $K$ -spațiu vectorial în raport cu operațiile induse de acestea.

c) Grupul abelian  $(End_K(V), +)$  este un  $K$ -spațiu vectorial în raport cu operația externă definită de (7). Mai mult, compunerea  $\circ$  a endomorfismelor  $K$ -spațiului vectorial  $V$  este distributivă față de  $+$ , prin urmare avem și o structură de inel cu unitate pe  $End_K(V)$ , și anume  $(End_K(V), +, \circ)$ .

**Teorema 3.23.** Dacă  $f : V \rightarrow V'$  este o transformare liniară, atunci:

- 1)  $Ker f = \{x \in V \mid f(x) = 0\}$  este un subspațiu al lui  $V$  numit **nucleul** lui  $f$ .
- 2) Transformarea liniară  $f$  este injectivă dacă și numai dacă  $Ker f = \{0\}$ .

*Demonstrație.* 1) Din  $f(0) = 0$  rezultă  $0 \in Ker f$ , adică  $Ker f \neq \emptyset$ . În plus, pentru orice  $x_1, x_2 \in Ker f$  și  $\alpha_1, \alpha_2 \in K$  avem

$$f(\alpha_1x_1 + \alpha_2x_2) = \alpha_1f(x_1) + \alpha_2f(x_2) = \alpha_10 + \alpha_20 = 0$$

de unde urmează  $\alpha_1x_1 + \alpha_2x_2 \in Ker f$ . Deci  $Ker f$  este subspațiu al lui  $V$ .

2) Într-adevăr,

$$f(x_1) = f(x_2) \Leftrightarrow f(x_1 - x_2) = 0 \Leftrightarrow x_1 - x_2 \in Ker f$$

ceea ce ne arată că

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

dacă și numai dacă  $Ker f = \{0\}$ , adică dacă și numai dacă  $Ker f = \{0\}$ .  $\square$

### 3.2 Exerciții rezolvate

1) Poate fi organizată o mulțime finită ca un spațiu vectorial peste un corp infinit?

*Soluție:* Fie  $V$  o mulțime finită și  $K$  un corp infinit. Dacă  $V$  are un singur element, atunci există o singură structură de  $K$ -spațiu vectorial pe  $V$  și anume spațiul vectorial nul. Dacă  $|V| \geq 2$ , presupunând că există o structură de  $K$ -spațiu vectorial pe  $V$  și luând  $x \neq 0$ , funcția  $t'_x : K \rightarrow V$ ,  $t'_x(\alpha) = \alpha x$  este injectivă, deoarece

$$\alpha_1, \alpha_2 \in K, t'_x(\alpha_1) = t'_x(\alpha_2) \Rightarrow \alpha_1 x = \alpha_2 x \Rightarrow (\alpha_1 - \alpha_2)x = 0 \stackrel{x \neq 0}{\Rightarrow} \alpha_1 - \alpha_2 = 0 \Rightarrow \alpha_1 = \alpha_2.$$

Deducem că  $|K| \leq |V|$ , contradicție cu  $V$  finită.

2) Fie  $V$  un  $K$ -spațiu vectorial,  $S \leq_K V$  și  $x, y \in V$ . Notăm  $\langle S, x \rangle = \langle S \cup \{x\} \rangle$ . Să se arate că dacă  $x \in V \setminus S$  și  $x \in \langle S, y \rangle$  atunci  $y \in \langle S, x \rangle$ .

*Soluție:* Din  $x \in \langle S, y \rangle$  rezultă că există  $s_1, \dots, s_n \in S$  și  $\alpha_1, \dots, \alpha_n, \alpha \in K$  astfel încât

$$x = \alpha_1 s_1 + \dots + \alpha_n s_n + \alpha y.$$

Presupunerea  $\alpha = 0$  ne-ar conduce la  $x = \alpha_1 s_1 + \dots + \alpha_n s_n \in S$ , ceea ce contrazice ipoteza, prin urmare,  $\alpha \neq 0$  este inversabil în  $K$ . Deducem

$$y = -\alpha^{-1} \alpha_1 s_1 - \dots - \alpha^{-1} \alpha_n s_n + \alpha^{-1} x \in \langle S, x \rangle.$$

3) Dacă  $V$  este un  $K$ -spațiu, vectorial,  $V_1, V_2 \leq_K V$  și  $V = V_1 \oplus V_2$ , spunem că  $V_i$  ( $i = 1, 2$ ) este **sumand direct** în  $V$ . Să se arate că proprietatea unui subspațiu de a fi sumand direct este tranzitivă.

*Soluție:* Fie  $V_1, V_2, V_3, V_4$  subspații ale unui  $K$ -spațiu vectorial  $V$  cu proprietatea că  $V = V_1 \oplus V_2$  și  $V_1 = V_3 \oplus V_4$ . Rezultă că  $V = V_1 + V_2 = V_3 + V_4 + V_2$ . Mai mult, dacă  $v_3 \in V_3 \cap (V_4 + V_2)$  atunci există  $v_4 \in V_4, v_2 \in V_2$  astfel încât  $v_3 = v_4 + v_2$ . Deducem că  $v_2 = v_3 - v_4 \in V_3 + V_4 = V_1$ , prin urmare  $v_2 \in V_1 \cap V_2 = \{0\}$ . Obținem  $v_2 = 0$  și  $v_3 = v_4 \in V_3 \cap V_4 = \{0\}$ . Așadar,  $V_3 \cap (V_4 + V_2) = \{0\}$  și astfel,  $V = V_3 \oplus (V_4 + V_2)$ , ceea ce înseamnă că  $V_3$  este sumand direct în  $V$ .

4) Există o transformare liniară de  $\mathbb{R}$ -spații vectoriale  $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$  astfel încât

$$f(1, 0, 3) = (1, 1) \text{ și } f(-2, 0, -6) = (2, 1)?$$

*Soluție:* Nu, pentru că  $f(-2, 0, -6) \neq (-2)f(1, 0, 3)$  deoarece  $f(-2, 0, -6) = (2, 1)$  și  $(-2)f(1, 0, 3) = (-2)(1, 1) = (-2, -2)$ .

### 3.3 Baze. Dimensiune

**Definițiile 3.24.** Fie  $V$  un  $K$ -spațiu vectorial și  $x_1, \dots, x_n \in V$ . Elementele  $x_1, \dots, x_n$  se numesc **liniar independente** dacă

$$\alpha_1 x_1 + \dots + \alpha_n x_n = 0 \Rightarrow \alpha_1 = \dots = \alpha_n = 0,$$

unde  $\alpha_1, \dots, \alpha_n \in K$ . În caz contrar elementele  $x_1, \dots, x_n$  se numesc **liniar dependente**. O submulțime finită a lui  $V$  se numește **liberă** dacă elementele sale sunt liniar

independente, iar în caz contrar se numește **legată**. O submulțime oarecare  $X \subseteq V$  se numește **liberă** dacă orice submulțime finită a lui  $X$  este liberă, iar în caz contrar se numește **legată**.

**Observațiile 3.25.** a) Vectorii  $x_1, \dots, x_n \in V$  sunt liniar dependenți dacă și numai dacă există scalarii  $\alpha_1, \dots, \alpha_n \in K$  nu toți zero astfel încât

$$\alpha_1 x_1 + \dots + \alpha_n x_n = 0.$$

- b) Dacă unul dintre vectorii  $x_1, \dots, x_n \in V$  este zero, atunci ei sunt liniar dependenți.  
c) Dacă vectorii  $x_1, \dots, x_n \in V$  sunt liniar independenți, atunci ei sunt doi câte doi diferiți.  
d) Dacă  $x \in V$  atunci  $\{x\}$  este liberă dacă și numai dacă  $x \neq 0$ .  
e) Submulțimea vidă  $\emptyset \subseteq V$  este liberă.  
f) Orice submulțime a unei mulțimi libere este liberă.  
g) Dacă submulțimea  $X \subseteq V$  are o submulțime legată atunci  $X$  este legată. În particular, orice submulțime a lui  $V$  care conține vectorul zero este legată.

**Teorema 3.26.** Vectorii  $x_1, \dots, x_n \in V$  sunt liniar dependenți dacă și numai dacă unul dintre ei este o combinație liniară a celorlalți.

*Demonstrație.* Fie  $x_1, \dots, x_n \in V$  liniar dependenți. Atunci există scalarii  $\alpha_1, \dots, \alpha_n$  din  $K$ , nu toți nuli, de exemplu  $\alpha_k \neq 0$ , astfel încât

$$\alpha_1 x_1 + \dots + \alpha_{k-1} x_{k-1} + \alpha_k x_k + \alpha_{k+1} x_{k+1} + \dots + \alpha_n x_n = 0$$

de unde rezultă

$$x_k = -(\alpha_k^{-1} \alpha_1) x_1 - \dots - (\alpha_k^{-1} \alpha_{k-1}) x_{k-1} - (\alpha_k^{-1} \alpha_{k+1}) x_{k+1} - \dots - (\alpha_k^{-1} \alpha_n) x_n,$$

adică  $x_k$  este o combinație liniară a vectorilor  $x_1, \dots, x_{k-1}, x_{k+1}, \dots, x_n$ .

Invers, dacă un vector  $x_k$  e combinație liniară a vectorilor  $x_1, \dots, x_{k-1}, x_{k+1}, \dots, x_n$  atunci

$$x_k = \beta_1 x_1 + \dots + \beta_{k-1} x_{k-1} + \beta_{k+1} x_{k+1} + \dots + \beta_n x_n$$

cu  $\beta_i \in K$ , de unde rezultă

$$\beta_1 x_1 + \dots + \beta_{k-1} x_{k-1} - 1 \cdot x_k + \beta_{k+1} x_{k+1} + \dots + \beta_n x_n = 0$$

ceea ce ne arată că  $x_1, \dots, x_n \in V$  sunt liniar dependenți. □

**Corolarul 3.27.** a) Dacă  $X \subseteq V$ , atunci  $X$  este legată dacă și numai dacă există  $x \in X$  astfel încât  $x \in \langle X \setminus \{x\} \rangle$ .

b) Dacă  $X \subseteq V$ , atunci  $X$  este liberă dacă și numai dacă pentru orice  $x \in X$  avem  $x \notin \langle X \setminus \{x\} \rangle$ .

**Exemplele 3.28.** a) Fie  $V_2$ , respectiv  $V_3$ ,  $\mathbb{R}$ -spațiul vectorial al vectorilor din plan, respectiv spațiu (vezi Exemplul 3.5 a)). Doi vectori din  $V_2$  sau  $V_3$  sunt liniar independenți dacă și numai dacă nu au aceeași direcție. Orice trei vectori din  $V_2$  sunt liniar dependenți. Trei vectori din  $V_3$  sunt liniar independenți dacă și numai dacă nu sunt coplanari. Orice patru vectori din  $V_3$  sunt liniar dependenți.

b) Fie  $K$  un corp comutativ și  $n \in \mathbb{N}^*$ . În  $K$ -spațiul vectorial  $K^n$  vectorii

$$e_1 = (1, 0, \dots, 0), e_2 = (0, 1, \dots, 0), \dots, e_n = (0, 0, \dots, 1)$$

sunt liniar independenți pentru că

$$\alpha_1 e_1 + \dots + \alpha_n e_n = (0, \dots, 0) \Rightarrow (\alpha_1, \dots, \alpha_n) = (0, \dots, 0) \Rightarrow \alpha_1 = \dots = \alpha_n = 0.$$

c) Fie  $K$  un corp comutativ. În  $K$ -spațiul vectorial  $K[X]$  mulțimea  $\{X^n \mid n \in \mathbb{N}\}$  este liberă.

**Definițiile 3.29.** Fie  $V$  un  $K$ -spațiu vectorial. O submulțime  $X \subseteq V$  se numește **bază** a lui  $V$  dacă  $X$  este liberă și  $X$  generează pe  $V$ , adică  $V = \langle X \rangle$ .

**Teorema 3.30.** Fie  $V$  un  $K$ -spațiu vectorial. O submulțime  $X$  a lui  $V$  este bază a lui  $V$  dacă și numai dacă orice vector din  $V$  se exprimă într-un singur mod ca și combinație liniară de elemente din  $X$  (mai exact, pentru orice  $v \in V$  există o singură familie de scalari  $(\alpha_x)_{x \in X}$  cu un număr finit de componente nenule astfel încât  $v = \sum_{x \in X} \alpha_x x$ ).

*Demonstrație.* Condiția  $V = \langle X \rangle$  este echivalentă cu faptul că orice vector din  $V$  este o combinație liniară de elemente din  $X$ , iar faptul că  $X$  este liberă este echivalent cu unicitatea acestei reprezentări.  $\square$

**Exemplele 3.31.** a) Orice doi vectori din  $V_2$  (plan) care nu au aceeași direcție formează o bază a lui  $V_2$ . Orice trei vectori necoplanari din  $V_3$  (spațiu) formează o bază a lui  $V_3$ .

b) Vectorii  $e_1 = (1, 0, \dots, 0), e_2 = (0, 1, \dots, 0), \dots, e_n = (0, 0, \dots, 1)$  formează o bază în  $K$ -spațiul vectorial  $K^n$  numită  **baza canonică**.

c) Fie  $K$  un corp comutativ. Mulțimea  $\{X^n \mid n \in \mathbb{N}\}$  este o bază în  $K$ -spațiul vectorial  $K[X]$ .

**Teorema 3.32.** Fie  $V$  un  $K$ -spațiu vectorial și  $X \subseteq V$ . Dacă  $X$  generează pe  $V$  și submulțimea  $X_1 \subseteq X$  e liberă, atunci există o bază  $X_2$  a lui  $V$  astfel încât  $X_1 \subseteq X_2 \subseteq X$ .

*Demonstrație.* (facultativă)

Fie  $\mathcal{C} = \{X' \mid X_1 \subseteq X' \subseteq X, X' \text{ liberă}\}$ , din  $X_1 \in \mathcal{C}$  rezultă  $\mathcal{C} \neq \emptyset$ . Fie  $\mathcal{C}' \subseteq \mathcal{C}$  un lanț nevid, în  $(\mathcal{C}, \subseteq)$  și

$$X_0 = \bigcup \{X' \mid X' \in \mathcal{C}'\}.$$

Arătăm că  $X_0 \in \mathcal{C}$ . Pentru orice  $x_1, \dots, x_n \in X_0$  există  $X'_1, \dots, X'_n$  în  $\mathcal{C}'$  astfel încât  $x_i \in X'_i$  ( $i = 1, \dots, n$ ), iar  $\mathcal{C}'$  fiind lanț rezultă că există  $i_0 \in \{1, \dots, n\}$  astfel încât  $X'_i \subseteq X'_{i_0}$  ( $i = 1, \dots, n$ ) ceea ce implică  $x_i \in X'_{i_0}$  ( $i = 1, \dots, n$ ). Prin urmare, din  $X'_{i_0} \in \mathcal{C}$  deducem că elementele  $x_1, \dots, x_n$  sunt liniar independente. Deci  $X_0$  este liberă și  $X_1 \subseteq X_0 \subseteq X$ , adică  $X_0 \in \mathcal{C}$  și  $X_0$  este majorantă a lui  $\mathcal{C}'$ . Din lema lui Zorn rezultă că există, în  $\mathcal{C}$ , un element maximal  $X_2$ . Din  $X_2 \in \mathcal{C}$  urmează că  $X_2$  este liberă.

Pentru a arăta că  $X_2$  este o bază a lui  $V$  mai trebuie arătat că  $V = \langle X_2 \rangle$ . Dacă  $V \neq \langle X_2 \rangle$  urmează că  $X$  nu este inclusă în  $\langle X_2 \rangle$ , adică există  $x \in X \setminus \langle X_2 \rangle$  și vom deduce că  $X_2 \cup \{x\}$  este liberă ceea ce contrazice maximalitatea lui  $X_2$ .

Într-adevăr, dacă

$$\sum_{i=1}^n \alpha_i x_i + \alpha x = 0,$$

unde  $x_i \in X_2$  și  $\alpha, \alpha_i \in K$  ( $i = 1, \dots, n$ ) atunci  $\alpha = 0$  deoarece în caz contrar

$$x = - \sum_{i=1}^n \alpha^{-1} \alpha_i x_i \in \langle X_2 \rangle$$

ceea ce contrazice alegerea lui  $x$ . Întrucât  $X_2$  este liberă rezultă  $\alpha_i = 0$  ( $i = 1, \dots, n$ ). Deci  $X_2 \cup \{x\}$  este liberă.  $\square$

**Corolarul 3.33.** a) Orice spațiu vectorial  $V$  are o bază.

Rezultă din teoremă luând  $X_1 = \emptyset$  și  $X = V$ .

- b) Orice submulțime liberă a unui spațiu vectorial  $V$  poate fi extinsă la o bază a lui  $V$ .  
c) O submulțime  $Y$  a unui spațiu vectorial  $V$  este o bază a lui  $V$  dacă și numai dacă  $Y$  este o submulțime liberă maximală a lui  $V$ .  
d) Din orice sistem de generatori al unui spațiu vectorial  $V$  se poate extrage o bază a lui  $V$ .  
e) O submulțime  $Y$  a unui spațiu vectorial  $V$  este o bază a lui  $V$  dacă și numai dacă  $Y$  este un sistem de generatori minimal al lui  $V$ .  
f) Dacă  $X_1$  este o submulțime liberă a lui  $V$  și  $V = \langle Y \rangle$  atunci  $X_1$  poate fi completată cu vectori din  $Y$  până la o bază a lui  $V$ .

Rezultă din teoremă luând  $X = X_1 \cup Y$ .

**Teorema 3.34. (Proprietatea de universalitate a spațiilor vectoriale)**

- 1) Dacă  $V$  este un  $K$ -spațiu vectorial și  $X$  o bază a sa, atunci pentru orice  $K$ -spațiu vectorial  $V'$  și orice funcție  $f : X \rightarrow V'$  există o singură transformare liniară  $\bar{f} : V \rightarrow V'$  pentru care  $\bar{f}|_X = f$  (cu alte cuvinte  $f : X \rightarrow V'$  se poate prelunge în mod unic la o transformare liniară  $\bar{f} : V \rightarrow V'$ ).  
2) Transformarea liniară  $\bar{f}$  este injectivă dacă și numai dacă  $f$  este injectivă și  $f(X)$  este liberă.  
3) Transformarea liniară  $\bar{f}$  este surjectivă dacă și numai dacă  $V' = \langle f(X) \rangle$ .

*Demonstrație.* 1) Demonstrăm mai întâi unicitatea lui  $\bar{f}$ . Presupunem că există o transformare liniară  $\bar{f} : V \rightarrow V'$  astfel încât  $\bar{f}|_X = f$ . Orice  $x \in V$  are o reprezentare unică de forma

$$x = \alpha_1 x_1 + \dots + \alpha_n x_n \tag{1}$$

unde  $\alpha_i \in K$ ,  $x_i \in X$  ( $i = 1, \dots, n$ ). Deci

$$\bar{f}(x) = \alpha_1 \bar{f}(x_1) + \dots + \alpha_n \bar{f}(x_n) = \alpha_1 f(x_1) + \dots + \alpha_n f(x_n)$$

ceea ce demonstrează unicitatea lui  $\bar{f}$ . Unicitatea reprezentării (1) ne permite să definim funcția  $\bar{f} : V \rightarrow V'$  prin

$$\bar{f}(x) = \alpha_1 f(x_1) + \dots + \alpha_n f(x_n). \tag{2}$$

Din (2) rezultă că  $\bar{f}|_X = f$ . Dacă  $y \in V$ , atunci adăugând eventual termeni de forma  $0 \cdot z$  cu  $z \in X$ ,  $y$  se scrie

$$y = \beta_1 x_1 + \dots + \beta_n x_n \tag{3}$$

unde  $\beta_i \in K$  ( $i = 1, \dots, n$ ). Pentru orice  $\alpha, \beta \in K$  folosind (1), (2) și (3) avem

$$\bar{f}(\alpha x + \beta y) = \bar{f}((\alpha \alpha_1 + \beta \beta_1) x_1 + \dots + (\alpha \alpha_n + \beta \beta_n) x_n) =$$

$$\begin{aligned}
&= (\alpha\alpha_1 + \beta\beta_1)f(x_1) + \cdots + (\alpha\alpha_n + \beta\beta_n)f(x_n) = \\
&= \alpha(\alpha_1f(x_1) + \cdots + \alpha_nf(x_n)) + \beta(\beta_1f(x_1) + \cdots + \beta_nf(x_n)) = \alpha\bar{f}(x) + \beta\bar{f}(y)
\end{aligned}$$

ceea ce ne arată că  $\bar{f}$  este liniară.

2) Din (1) și (2) rezultă

$$x \in \text{Ker } \bar{f} \Leftrightarrow \alpha_1f(x_1) + \cdots + \alpha_nf(x_n) = 0$$

ceea ce ne arată că  $\text{Ker } \bar{f} = \{0\}$  (adică  $\bar{f}$  este injectivă) dacă și numai dacă  $f$  este injectivă și  $f(X)$  este liberă.

3) Din Observația 3.19 h) rezultă  $\langle \bar{f}(X) \rangle = \bar{f}(\langle X \rangle) = \bar{f}(V)$ , adică  $\bar{f}(V) = \langle f(X) \rangle$ . Deci  $\bar{f}$  este surjectivă dacă și numai dacă  $V' = \langle f(X) \rangle$ .  $\square$

**Corolarul 3.35.** a) Dacă  $X$  este o bază a spațiului vectorial  $V$  și  $\varphi, \varphi' : V \rightarrow V'$  sunt transformări liniare, atunci

$$\varphi|_X = \varphi'|_X \Rightarrow \varphi = \varphi',$$

adică o transformare liniară este determinată de restricția sa la o bază.

b) Dacă  $\varphi : V \rightarrow V'$  este o transformare liniară și  $X$  o bază a lui  $V$ , atunci  $\varphi$  este izomorfism dacă și numai dacă  $\varphi|_X$  este injectivă și  $\varphi(X)$  este o bază a lui  $V'$ .

În Corolarul 3.33 a) am arătat că orice spațiu vectorial are o bază. În cele ce urmează vom considera că spațiile vectoriale cu care lucrăm sunt de tip finit. Vom arăta că toate bazele unui spațiu vectorial  $V$  de tip finit au același cardinal (adică același număr de elemente). Acest cardinal se numește **dimensiunea** lui  $V$ . Chiar dacă în acest material nu este inclus cazul spațiilor vectoriale care au un sistem infinit de generatori, menționăm că și în cazul lor toate bazele au același cardinal, cardinal care este dimensiunea spațiului. De altfel, cititorul atent va observa că unele demonstrații ce vor urma se potrivesc și pentru spații vectoriale care nu sunt de dimensiune finită.

**Teorema 3.36. (Teorema schimbului (Steinitz))**

Fie  $V$  un  $K$ -spațiu vectorial. Dacă  $x_1, \dots, x_m$  sunt elementele liniar independente din  $V$  și  $V = \langle y_1, \dots, y_n \rangle$ , atunci  $m \leq n$  și după o reindexare convenabilă avem

$$V = \langle x_1, \dots, x_m, y_{m+1}, \dots, y_n \rangle.$$

*Demonstrație.* Vom utiliza inducția după  $m$ . Pentru  $m = 0$  concluzia teoremei este  $0 \leq n$  care este adevărată.

Presupunem  $m > 0$  și teorema adevărată pentru  $m - 1$  elemente liniar independente. Dacă elementele  $x_1, \dots, x_m$  sunt liniar independente, atunci  $x_1, \dots, x_{m-1}$  sunt liniar independente, de unde (conform ipotezei inducției) rezultă  $m - 1 \leq n$  și după o reindexare convenabilă,  $V = \langle x_1, \dots, x_{m-1}, y_m, \dots, y_n \rangle$ . Nu putem avea  $m - 1 = n$  pentru că ar rezulta  $x_m \in V = \langle x_1, \dots, x_{m-1} \rangle$  ceea ce contrazice liniar independența elementelor  $x_1, \dots, x_m$ . Deci  $m - 1 < n$ , adică  $m \leq n$ .

Din  $V = \langle x_1, \dots, x_{m-1}, y_m, \dots, y_n \rangle$  rezultă că există  $\alpha_1, \dots, \alpha_n \in K$  astfel încât

$$x_m = \alpha_1x_1 + \cdots + \alpha_{m-1}x_{m-1} + \alpha_my_m + \cdots + \alpha_ny_n.$$

Din liniar independența elementelor  $x_1, \dots, x_m$  urmează că unul din scalarii  $\alpha_m, \dots, \alpha_n$  este nenul, făcând eventual o reindexare avem  $\alpha_m \neq 0$ . Deci

$$y_m = -\alpha_m^{-1}(\alpha_1 x_1 + \dots + \alpha_{m-1} x_{m-1} - x_m + \alpha_{m+1} y_{m+1} + \dots + \alpha_n y_n)$$

de unde deducem  $V = \langle x_1, \dots, x_m, y_{m+1}, \dots, y_n \rangle$ .  $\square$

**Corolarul 3.37.** Toate bazele unui spațiu vectorial  $V$  de tip finit (finit generat) sunt finite și au același număr de vectori.

Într-adevăr, dacă  $V$  este de tip finit, există  $y_1, \dots, y_n \in V$  astfel încât  $V = \langle y_1, \dots, y_n \rangle$ . Din teoremă urmează că orice  $n + 1$  vectori din  $V$  sunt liniar dependenți. Rezultă că orice bază a lui  $V$  conține cel mult  $n$  vectori, adică este finită. Dacă  $\{x_1, \dots, x_m\}$  și  $\{y_1, \dots, y_n\}$  sunt baze ale lui  $V$ , atunci din teoremă rezultă  $m \leq n$  și  $n \leq m$  ceea ce implică  $m = n$ . Deci toate bazele lui  $V$  au același număr de vectori.

Din Corolarul 3.37 rezultă că pentru orice  $K$ -spațiu vectorial  $V$  de tip finit toate bazele lui  $V$  au același număr de elemente. Acest număr se numește **dimensiunea** lui  $V$  și se notează cu  $\dim V$  sau  $\dim_K V$ . Deci  $\dim V$  este cardinalul unei baze a lui  $V$ .

**Observațiile 3.38.** a) Dacă spațiul vectorial  $V$  are dimensiune finită, atunci  $\dim V = n$  dacă și numai dacă există  $n$  vectori liniar independenți și orice  $n + 1$  vectori din  $V$  sunt liniar dependenți.

Această afirmație rezultă din definiția  $\dim V$  și din faptul că bazele lui  $V$  coincid cu submulțimile independente maximale ale lui  $V$ .

b) Dacă spațiul vectorial  $V$  are dimensiune finită și  $\dim V = n$ , atunci orice  $n$  vectori liniar independenți din  $V$  formează o bază a lui  $V$ .

c) Dacă  $V$  este un spațiu vectorial de tip finit și  $A$  este un subspațiu al lui  $V$ , atunci  $\dim A \leq \dim V$ . Mai mult,  $A \neq V$  dacă și numai dacă  $\dim A < \dim V$ .

Într-adevăr, dacă  $X$  este o bază a lui  $A$ , atunci  $X$  se poate completa la o bază  $Y$  a lui  $V$ . Din  $X \subseteq Y$  rezultă  $\dim A = |X| \leq |Y| = \dim V$ . Avem  $A \neq V$  dacă și numai dacă  $X \neq Y$ . Cum  $\dim V$  este finită,  $Y$  este finită și atunci  $X \neq Y$  este echivalentă cu  $|X| < |Y|$ , adică  $\dim A < \dim V$ .

**Exemplele 3.39.** a) Dacă  $K$  este un corp comutativ și  $n \in \mathbb{N}^*$ , atunci  $\dim K^n = n$  pentru că  $e_1 = (1, 0, \dots, 0)$ ,  $e_2 = (0, 1, \dots, 0), \dots, e_n = (0, 0, \dots, 1)$  formează o bază a lui  $K^n$ .

b) Dacă  $K$  este un corp comutativ, atunci  $\dim P_n(K) = n + 1$  pentru că  $1, X, X^2, \dots, X^n$  formează o bază a  $K$ -spațiului  $P_n(K) = \{f \in K[X] \mid \text{grad } f \leq n\}$ .

c) Dacă  $V_1$  și  $V_2$  sunt  $K$ -spații vectoriale și  $X$ , respectiv  $Y$  este o bază a lui  $V_1$ , respectiv  $V_2$ , atunci se verifică ușor că  $\{(x, 0) \mid x \in X\} \cup \{(0, y) \mid y \in Y\}$  este o bază a produsului direct  $V_1 \times V_2$ , de unde ținând seama că  $|X| = |\{(x, 0) \mid x \in X\}|$ ,  $|Y| = |\{(0, y) \mid y \in Y\}|$  și  $\{(x, 0) \mid x \in X\} \cap \{(0, y) \mid y \in Y\} = \emptyset$  rezultă

$$\dim(V_1 \times V_2) = \dim V_1 + \dim V_2.$$

**Teorema 3.40.** Două  $K$ -spații vectoriale  $V$  și  $V'$  sunt izomorfe dacă și numai dacă  $\dim V = \dim V'$ .



*Demonstrație.* Presupunem că  $V$  și  $V'$  sunt izomorfe și  $f : V \rightarrow V'$  este un izomorfism, iar  $X$  este o bază a lui  $V$ . Arătăm că  $f(X)$  este o bază a lui  $V'$ . Dacă  $y_1, \dots, y_n \in f(X)$  atunci există  $x_i \in X$  astfel încât  $y_i = f(x_i)$  ( $i = 1, \dots, n$ ). Folosind liniaritatea lui  $f$ , injectivitatea lui  $f$  și libertatea lui  $X$  avem:

$$\begin{aligned} \alpha_1 y_1 + \dots + \alpha_n y_n = 0 &\Rightarrow \alpha_1 f(x_1) + \dots + \alpha_n f(x_n) = 0 \Rightarrow f(\alpha_1 x_1 + \dots + \alpha_n x_n) = f(0) \Rightarrow \\ &\Rightarrow \alpha_1 x_1 + \dots + \alpha_n x_n = 0 \Rightarrow \alpha_1 = \dots = \alpha_n = 0 \end{aligned}$$

unde  $\alpha_1, \dots, \alpha_n \in K$ . Deci  $f(X)$  este liberă. Din surjectivitatea lui  $f$  rezultă că pentru  $\forall y \in V'$  există  $x \in V$  astfel încât  $y = f(x)$ , iar din  $V = \langle X \rangle$  urmează că există  $x_1, \dots, x_n \in X$  și  $\alpha_1, \dots, \alpha_n \in K$  astfel încât

$$x = \alpha_1 x_1 + \dots + \alpha_n x_n$$

de unde deducem

$$y = f(x) = \alpha_1 f(x_1) + \dots + \alpha_n f(x_n)$$

ceea ce ne arată că  $y \in \langle f(X) \rangle$ . Deci  $V' = \langle f(X) \rangle$ . Astfel am arătat că  $f(X)$  este o bază a lui  $V'$ . Din bijectivitatea lui  $f$  rezultă că funcția  $f' : X \rightarrow f(X)$ ,  $f'(x) = f(x)$  este bijectivă, de unde urmează  $\dim V = |X| = |f(X)| = \dim V'$ .

Acum, presupunem că  $\dim V = \dim V'$ . Rezultă că dacă  $X$  este o bază a lui  $V$  și  $Y$  este o bază a lui  $V'$ , atunci există o bijecție  $g : X \rightarrow Y$ . Din Teorema 3.34 urmează că  $g$  și  $g^{-1}$  se pot prelungi în mod unic la transformările liniare  $\bar{g} : V \rightarrow V'$  și  $\bar{g}^{-1} : V' \rightarrow V$ . Rezultă că pentru orice  $x \in X$  și  $y \in Y$  avem

$$(\bar{g}^{-1} \circ \bar{g})(x) = \bar{g}^{-1}(\bar{g}(x)) = \bar{g}^{-1}(g(x)) = g^{-1}(g(x)) = (g^{-1} \circ g)(x) = 1_V(x),$$

$$(\bar{g} \circ \bar{g}^{-1})(y) = \bar{g}(\bar{g}^{-1}(y)) = \bar{g}(g^{-1}(y)) = g(g^{-1}(y)) = (g \circ g^{-1})(y) = 1_{V'}(y)$$

ceea ce arată că  $\bar{g}^{-1} \circ \bar{g} = 1_V$  și  $\bar{g} \circ \bar{g}^{-1} = 1_{V'}$ . Deci transformarea liniară  $\bar{g}$  este bijectivă, adică  $\bar{g}$  este un izomorfism. Prin urmare  $V$  și  $V'$  sunt izomorfe.  $\square$

**Corolarul 3.41.** Dacă  $V$  este un  $K$ -spațiu vectorial de dimensiune finită și  $\dim V = n$ , atunci  $V$  este izomorf cu  $K^n$ . Dacă  $\{x_1, \dots, x_n\}$  este o bază a lui  $V$ , atunci

$$f : K^n \rightarrow V, f(\alpha_1, \dots, \alpha_n) = \alpha_1 x_1 + \dots + \alpha_n x_n$$

este un izomorfism ce aplică baza canonică a lui  $K^n$  pe baza  $\{x_1, \dots, x_n\}$ .

**Teorema 3.42.** Dacă  $V$  și  $V'$  sunt  $K$ -spații vectoriale și  $f : V \rightarrow V'$  este o transformare liniară, atunci

$$\dim V = \dim \text{Ker } f + \dim f(V). \quad (4)$$

*Demonstrație.* Fie  $X$  o bază în  $\text{Ker } f$  și  $X \cup X'$  cu  $X \cap X' = \emptyset$  o completare a lui  $X$  la o bază a lui  $V$ . Din  $X \cap X' = \emptyset$  și unicitatea scrierii unui vector ca și combinație liniară de vectori dintr-o bază rezultă  $\langle X \rangle \cap \langle X' \rangle = \{0\}$ . Dacă  $x'_1, x'_2 \in X'$  și  $f(x'_1) = f(x'_2)$  atunci

$$f(x'_1 - x'_2) = 0 \Rightarrow x'_1 - x'_2 \in \langle X' \rangle \cap \text{Ker } f = \langle X' \rangle \cap \langle X \rangle = \{0\} \Rightarrow x'_1 - x'_2 = 0 \Rightarrow x'_1 = x'_2.$$

Deci  $f|_{X'} : X' \rightarrow f(X')$  este bijectie, ceea ce ne arată că  $|X'| = |f(X')|$ . Demonstrăm că  $f(X')$  este o bază a lui  $f(V)$ . Pentru orice  $y \in f(V)$  există  $x \in V$  astfel ca  $y = f(x)$ , dar  $X \cup X'$  fiind o bază a lui  $V$ , există  $x_1, \dots, x_m \in X$ ,  $x'_{m+1}, \dots, x'_n \in X'$  astfel ca

$$x = \alpha_1 x_1 + \dots + \alpha_m x_m + \alpha_{m+1} x'_{m+1} + \dots + \alpha_n x'_n,$$

de unde ținând seama de  $\alpha_1 x_1 + \dots + \alpha_n x_n \in \text{Ker } f$  deducem

$$\begin{aligned} y = f(x) &= f(\alpha_1 x_1 + \dots + \alpha_m x_m) + \alpha_{m+1} f(x'_{m+1}) + \dots + \alpha_n f(x'_n) = \\ &= \alpha_{m+1} f(x'_{m+1}) + \dots + \alpha_n f(x'_n) \in \langle f(X') \rangle \end{aligned}$$

ceea ce ne arată că  $f(V) = \langle f(X') \rangle$ . Dacă  $y_1, \dots, y_l \in f(X')$  atunci există  $x'_i \in X'$  astfel încât  $y_i = f(x'_i)$  ( $i = 1, \dots, l$ ). Pentru  $\beta_1, \dots, \beta_l \in K$  cu  $\beta_1 y_1 + \dots + \beta_l y_l = 0$  avem

$$\begin{aligned} f(\beta_1 x'_1 + \dots + \beta_l x'_l) = 0 &\Rightarrow \beta_1 x'_1 + \dots + \beta_l x'_l \in \langle X' \rangle \cap \text{Ker } f = \langle X' \rangle \cap \langle X \rangle = \{0\} \Rightarrow \\ &\Rightarrow \beta_1 x'_1 + \dots + \beta_l x'_l = 0 \Rightarrow \beta_1 = \dots = \beta_l = 0 \end{aligned}$$

ceea ce arată că  $f(X')$  este liberă. Deci  $f(X')$  este o bază a lui  $f(V)$  și  $|X'| = |f(X')|$  de unde rezultă că  $\dim f(V) = |X'|$  ceea ce împreună cu faptul că  $X \cup X'$  este bază pentru  $V$ , iar  $X$  este bază pentru  $\text{Ker } f$  și  $X \cap X' = \emptyset$  implică pe (4).  $\square$

Cu notațiile din teoremă,  $\dim \text{Ker } f$  se numește **defectul** lui  $f$ , iar  $\dim f(V)$  se numește **rangul** lui  $f$ .

**Corolarul 3.43.** a) Fie  $V$  un  $K$ -spațiu vectorial și  $A, B$  subspații ale lui  $V$ . Atunci

$$\dim A + \dim B = \dim(A \cap B) + \dim(A + B). \quad (5)$$

Într-adevăr, funcția  $f : A \times B \rightarrow A + B$ ,  $f(a, b) = a - b$  este o transformare liniară surjectivă și  $\text{Ker } f = \{(x, x) \mid x \in A \cap B\}$ . Din (4) rezultă

$$\dim(A \times B) = \dim(\text{Ker } f) + \dim(A + B). \quad (6)$$

Pe de altă parte  $g : A \cap B \rightarrow \text{Ker } f$ ,  $g(x) = (x, x)$  este un izomorfism de spații vectoriale, de unde urmează

$$\dim(\text{Ker } f) = \dim(A \cap B), \quad (7)$$

iar din Exemplul 3.39 c) rezultă

$$\dim(A \times B) = \dim A + \dim B. \quad (8)$$

Acum din (6), (7) și (8) se obține (5).

b) Dacă  $V$  este un  $K$ -spațiu vectorial de dimensiune finită, iar  $A$  și  $B$  sunt subspații ale lui  $V$ , atunci

$$\dim(A + B) = \dim A + \dim B \Leftrightarrow A + B = A \oplus B.$$

c) **(Teorema alternativei)** Dacă  $V, V'$  sunt  $K$ -spații vectoriale de dimensiune finită și  $\dim V = \dim V'$ , iar  $f : V \rightarrow V'$  este o transformare liniară, atunci sunt echivalente următoarele afirmații:

i)  $f$  este injectivă;

- ii)  $f$  este surjectivă;  
 iii)  $f$  este izomorfism.

Cum implicațiile iii)  $\Rightarrow$  i) și iii)  $\Rightarrow$  ii) sunt evidente, rămâne de demonstrat i)  $\Leftrightarrow$  ii).

Din i) rezultă  $\text{Ker } f = \{0\}$ , prin urmare,

$$\dim V' = \dim V = \dim \text{Ker } f + \dim f(V) = \dim f(V).$$

Aplicând Observația 3.38 c), deducem că  $f(V) = V'$ , deci  $f$  este surjectivă.

Reciproc, din ii) rezultă că  $\dim f(V) = \dim V'$ , prin urmare

$$\dim \text{Ker } f = \dim V - \dim f(V) = \dim V' - \dim f(V) = 0.$$

Așadar,  $\text{Ker } f = \{0\}$ , deci  $f$  e injectivă.

### 3.4 Exerciții rezolvate

1) Fie  $n \in \mathbb{N}$  și  $f_n : \mathbb{R} \rightarrow \mathbb{R}$ ,  $f_n(x) = \sin^n x$ . Să se arate că  $L = \{f_n \mid n \in \mathbb{N}\}$  este o submulțime liberă a  $\mathbb{R}$ -spațiului vectorial  $\mathbb{R}^{\mathbb{R}}$ .

*Soluție:*  $L$  este liberă dacă și numai dacă pentru orice  $n_1, \dots, n_k \in \mathbb{N}$  distincți, vectorii  $f_{n_1}, \dots, f_{n_k}$  sunt liniar independenți. Fie  $\alpha_1, \dots, \alpha_k \in \mathbb{R}$  astfel ca  $\alpha_1 f_{n_1} + \dots + \alpha_k f_{n_k} = \theta$  (unde cu  $\theta$  am notat funcția identic nulă). Rezultă că

$$\forall x \in \mathbb{R}, \alpha_1 \sin^{n_1} x + \dots + \alpha_k \sin^{n_k} x = 0,$$

de unde deducem că polinomul

$$p = \alpha_1 X^{n_1} + \dots + \alpha_k X^{n_k} \in \mathbb{R}[X]$$

are ca rădăcină orice număr  $t (= \sin x) \in [-1, 1]$ , adică are o infinitate de rădăcini. Aceasta implică  $p = 0$ , așadar  $\alpha_1 = \dots = \alpha_k = 0$ .

2) Fie  $p \in \mathbb{N}$  un număr prim. Să se arate că operațiile uzuale de adunare și înmulțire înzestreaază pe  $V = \{a + b\sqrt[3]{p} + c\sqrt[3]{p^2} \mid a, b, c \in \mathbb{Q}\}$  cu o structură de  $\mathbb{Q}$ -spațiu vectorial și să se determine o bază și dimensiunea acestui spațiu vectorial.

*Soluție:*  $V$  este un subspațiu al lui  ${}_{\mathbb{Q}}\mathbb{R}$  generat de  $\{1, \sqrt[3]{p}, \sqrt[3]{p^2}\}$ . Arătăm că  $1, \sqrt[3]{p}, \sqrt[3]{p^2}$  sunt liniar independente. Dacă  $a, b, c \in \mathbb{Q}$  și  $a + b\sqrt[3]{p} + c\sqrt[3]{p^2} = 0$  atunci, prin înmulțire cu  $\sqrt[3]{p}$  obținem  $a\sqrt[3]{p} + b\sqrt[3]{p^2} + cp = 0$ . Eliminând pe  $\sqrt[3]{p^2}$  între cele două egalități rezultă  $(ab - c^2p) + (b^2 - ac)\sqrt[3]{p} = 0$ , care, în baza faptului că  $\sqrt[3]{p} \notin \mathbb{Q}$ , conduce la  $ab - c^2p = 0 = b^2 - ac$ . Presupunând că  $a \neq 0$  avem  $c = \frac{b^2}{a}$ , prin urmare  $ab - \frac{b^4}{a^2}\sqrt[3]{p} = 0$ , adică  $\sqrt[3]{p} = \frac{b^3}{a^3}$ . Aceasta implică  $\sqrt[3]{p} = \frac{b}{a} \in \mathbb{Q}$ , contradicție cu  $\sqrt[3]{p} \notin \mathbb{Q}$ . Deci  $a = 0$ , ceea ce implică și  $b = c = 0$ .

3) Fie  $V$  un  $K$ -spațiu vectorial de dimensiune 3 și  $V_1, V_2$  două subspații diferite de dimensiune 2. Să se arate că  $V_1 \cap V_2$  are dimensiunea 1. Care este semnificația geometrică în cazul  $K = \mathbb{R}$ ,  $V = \mathbb{R}^3$ ?

*Soluție:* Din  $V_1 \neq V_2$  și  $\dim V_1 = \dim V_2$  rezultă  $V_2 \not\subseteq V_1$ . Prin urmare

$$V_1 \subsetneq V_1 + V_2 \subseteq V,$$

ceea ce implică  $\dim(V_1 + V_2) = 3$  și

$$\dim(V_1 \cap V_2) = \dim V_1 + \dim V_2 - \dim(V_1 + V_2) = 1.$$

În  $\mathbb{R}^3$  aceasta se interpretează geometric prin faptul că intersecția a două plane diferite care trec prin origine este o dreaptă care trece prin origine.

4) Fie  $V$  un  $K$ -spațiu vectorial de dimensiune  $n \in \mathbb{N}^*$  și  $V_1, V_2$  subspații ale lui  $V$ . Să se arate că dacă  $\dim V_1 = n - 1$  și  $V_2 \not\subseteq V_1$  atunci

$$\dim(V_1 \cap V_2) = \dim V_2 - 1 \text{ și } V_1 + V_2 = V.$$

*Soluție:* Din  $V_2 \not\subseteq V_1$  rezultă că  $V_1 \cap V_2 \subsetneq V_2$ , prin urmare  $\dim(V_1 \cap V_2) < \dim V_2$ , adică  $\dim V_2 - \dim(V_1 \cap V_2) \geq 1$ . Atunci

$$n = \dim V \geq \dim(V_1 + V_2) = \dim V_1 + \dim V_2 - \dim(V_1 \cap V_2) \geq n - 1 + 1 = n.$$

Așadar,  $\dim(V_1 + V_2) = n = \dim V$ , ceea ce implică  $V = V_1 + V_2$ . De aici rezultă

$$\dim(V_1 \cap V_2) = \dim V_1 + \dim V_2 - \dim(V_1 + V_2) = n - 1 + \dim V_2 - n = \dim V_2 - 1.$$

### 3.5 Exerciții propuse

1) Arătați că grupul abelian  $(\mathbb{R}_+^*, \cdot)$  este  $\mathbb{R}$ -spațiu vectorial în raport cu operația externă  $*$  definită prin

$$\alpha * x = x^\alpha, \quad \alpha \in \mathbb{R}, \quad x \in \mathbb{R}_+^*$$

și că acest spațiu vectorial este izomorf cu  $\mathbb{R}$ -spațiul vectorial definit pe  $\mathbb{R}$  de operațiile uzuale de adunare și înmulțire.

2) Fie  $V$  un  $K$ -spațiu vectorial,  $\alpha, \beta, \gamma \in K$  și  $x, y, z \in V$  astfel încât  $\alpha\gamma \neq 0$  și

$$\alpha x + \beta y + \gamma z = 0.$$

Să se arate că  $\langle x, y \rangle = \langle y, z \rangle$ .

3) În  $\mathbb{R}$ -spațiul vectorial  $\mathbb{R}^{\mathbb{R}} = \{f \mid f : \mathbb{R} \rightarrow \mathbb{R}\}$  considerăm

$$(\mathbb{R}^{\mathbb{R}})_i = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ este impară}\}, \quad (\mathbb{R}^{\mathbb{R}})_p = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ este pară}\}.$$

Să se arate că  $(\mathbb{R}^{\mathbb{R}})_i$  și  $(\mathbb{R}^{\mathbb{R}})_p$  sunt subspații ale lui  $\mathbb{R}^{\mathbb{R}}$  și că  $\mathbb{R}^{\mathbb{R}} = (\mathbb{R}^{\mathbb{R}})_i \oplus (\mathbb{R}^{\mathbb{R}})_p$ .

4) Fie  $V$  un  $\mathbb{R}$ -spațiu vectorial și  $v_1, v_2, v_3 \in V$ . Să se arate că vectorii  $v_1, v_2, v_3$  sunt liniar independenți dacă și numai dacă vectorii  $v_2 + v_3, v_3 + v_1, v_1 + v_2$  sunt liniar independenți.

5) Să se arate că în  $\mathbb{R}$ -spațiul vectorial  $M_2(\mathbb{R})$  matricele

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad E_3 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad E_4 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

formează o bază și să se determine coordonatele matricei  $A = \begin{pmatrix} -2 & 3 \\ 4 & -2 \end{pmatrix}$  în această bază.

6) Să se determine  $a \in \mathbb{R}$  astfel încât vectorii  $v_1 = (a, 1, 1)$ ,  $v_2 = (1, a, 1)$ ,  $v_3 = (1, 1, a)$  să formeze o bază a lui  $\mathbb{R}^3$ .

7) În  $\mathbb{Q}$ -spațiul vectorial  $\mathbb{Q}^3$  considerăm vectorii

$$a = (-2, 1, 3), b = (3, -2, -1), c = (1, -1, 2), d = (-5, 3, 4), e = (-9, 5, 10).$$

Să se arate că  $\langle a, b \rangle = \langle c, d, e \rangle$ .

8) În  $\mathbb{R}$ -spațiul vectorial  $\mathbb{R}^4$  se consideră subspațiile generate astfel:

a)  $S = \langle u_1, u_2, u_3 \rangle$ , cu  $u_1 = (1, 2, 1, -2)$ ,  $u_2 = (2, 3, 1, 0)$ ,  $u_3 = (1, 2, 2, -3)$ ,

$$T = \langle v_1, v_2, v_3 \rangle, \text{ cu } v_1 = (1, 1, 1, 1), v_2 = (1, 0, 1, -1), v_3 = (1, 3, 0, -3);$$

b)  $S = \langle u_1, u_2 \rangle$ , cu  $u_1 = (1, 2, 1, 0)$ ,  $u_2 = (-1, 1, 1, 1)$ ,

$$T = \langle v_1, v_2 \rangle, \text{ cu } v_1 = (2, -1, 0, 1), v_2 = (1, -1, 3, 7);$$

c)  $S = \langle u_1, u_2 \rangle$ , cu  $u_1 = (1, 1, 0, 0)$ ,  $u_2 = (1, 0, 1, 1)$ ,

$$T = \langle v_1, v_2 \rangle, \text{ cu } v_1 = (0, 0, 1, 1), v_2 = (0, 1, 1, 0);$$

d)  $S = \langle u_1, u_2, u_3 \rangle$ , cu  $u_1 = (1, 2, -1, -2)$ ,  $u_2 = (3, 1, 1, 1)$ ,  $u_3 = (-1, 0, 1, -1)$ ,

$$T = \langle v_1, v_2 \rangle, \text{ cu } v_1 = (-1, 2, -7, -3), v_2 = (2, 5, -6, -5).$$

Să se determine câte o bază și dimensiunea subspațiilor  $S$ ,  $T$ ,  $S + T$  și  $S \cap T$ .

## 4 Transformări liniare și matrici, sisteme de ecuații liniare (de Ioan Purdea și Cosmin Pelea)

### 4.1 Transformări liniare și matrici

În acest paragraf vom arăta că studiul transformărilor liniare între două  $K$ -spații vectoriale  $V$  și  $V'$  de tip finit se reduce la studiul matricelor de tipul  $(m, n)$  cu elemente din  $K$ , unde  $m = \dim V'$  și  $n = \dim V$ . Menționăm că în această secțiune, bazele nu vor fi privite doar ca mulțimi ci ca mulțimi ordonate. Astfel, prin **bază** vom înțelege **bază ordonată**.

Fie  $K$  un corp comutativ,  $V$  și  $V'$   $K$ -spații vectoriale de dimensiune finită,  $n = \dim V$ ,  $m = \dim V'$  și  $u = (u_1, \dots, u_n)$  respectiv  $v = (v_1, \dots, v_m)$  o bază a lui  $V$  respectiv  $V'$ . Fiecare vector  $y \in V'$  are o reprezentare unică de forma

$$y = \beta_1 v_1 + \dots + \beta_m v_m. \quad (1)$$

Scalarii  $\beta_1, \dots, \beta_m$  din (1) se numesc **coordonatele** lui  $y$  în baza  $v$ .

Dacă  $f : V \rightarrow V'$  este o transformare liniară, atunci conform Corolarului 3.35 a)  $f$  este determinată de restricția sa la  $u$ , adică de  $f(u_1), \dots, f(u_n)$ , iar fiecare vector  $f(u_j)$  ( $j = 1, \dots, n$ ) este determinat de coordonatele sale în baza  $v$ .

Deci transformarea liniară  $f$  este determinată de scalarii  $\alpha_{ij}$ ,  $1 \leq i \leq m$ ,  $1 \leq j \leq n$  din relațiile

$$\begin{aligned} f(u_1) &= \alpha_{11}v_1 + \alpha_{21}v_2 + \dots + \alpha_{m1}v_m \\ f(u_2) &= \alpha_{12}v_1 + \alpha_{22}v_2 + \dots + \alpha_{m2}v_m \\ &\vdots \\ f(u_n) &= \alpha_{1n}v_1 + \alpha_{2n}v_2 + \dots + \alpha_{mn}v_m. \end{aligned} \quad (2)$$

Notăm cu  $[f]_{u,v}$  matricea de tipul  $(m, n)$  care are **coloanele** formate din coordonatele

vectorilor  $f(u_1), \dots, f(u_n)$  în baza  $v$ , adică

$$[f]_{u,v} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} \end{pmatrix}.$$

Matricea  $[f]_{u,v}$  se numește **matricea transformării liniare  $f$  în perechea de baze  $(u, v)$** . Folosind matrice linie cu elementele vectori, relațiile (2) se pot scrie astfel:

$$(f(u_1), \dots, f(u_n)) = (v_1, \dots, v_m)[f]_{u,v}.$$

Dacă  $x \in V$  și  $x$  are coordonatele  $\alpha_1, \dots, \alpha_n$  în baza  $u$ , iar  $f(x)$  are coordonatele  $\beta_1, \dots, \beta_m$  în baza  $v$ , adică

$$x = \alpha_1 u_1 + \dots + \alpha_n u_n, \quad f(x) = \beta_1 v_1 + \dots + \beta_m v_m$$

atunci

$$\alpha_1 f(u_1) + \dots + \alpha_n f(u_n) = \beta_1 v_1 + \dots + \beta_m v_m$$

de unde, folosind pe (2) obținem

$$\sum_{i=1}^m \left( \sum_{j=1}^n \alpha_{ij} \alpha_j \right) v_i = \sum_{i=1}^m \beta_i v_i. \quad (3)$$

Din (3) și din unicitatea coordonatelor rezultă

$$\beta_i = \sum_{j=1}^n \alpha_{ij} \alpha_j \quad (i = 1, \dots, m) \quad (4)$$

ceea ce ne arată că coordonatele lui  $f(x)$  sunt combinații liniare ale coordonatelor lui  $x$  cu coeficienții din **liniile** matricei  $[f]_{u,v}$ . Relațiile (4) se exprimă matriceal astfel

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_m \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Menționăm că matricea  $[f]_{u,v}$  depinde de  $f$ , de bazele  $u, v$  și de ordonările acestor baze, iar  $\text{rang } f = \text{rang } [f]_{u,v}$ .

**Exemplele 4.1.** a) Fie  $P_n(\mathbb{R})$   $\mathbb{R}$  - spațiul vectorial al polinoamelor de grad cel mult  $n$  cu coeficienții din  $\mathbb{R}$ . Funcția

$$\varphi : P_3(\mathbb{R}) \rightarrow P_2(\mathbb{R}), \quad \varphi(a_0 + a_1 X + a_2 X^2 + a_3 X^3) = a_1 + 2a_2 X + 3a_3 X^2$$

(adică funcția care asociază unui polinom  $f$  derivata formală  $f'$  a sa) este o transformare liniară. Vom scrie matricea lui  $\varphi$  în perechile de baze ordonate  $u = (1, X, X^2, X^3)$ ,

$v = (1, X, X^2)$  și  $u = (1, X, X^2, X^3)$ ,  $v' = (X^2, 1, X)$ . Avem

$$\begin{aligned}\varphi(1) &= 0 \cdot 1 + 0 \cdot X + 0 \cdot X^2 = 0 \cdot X^2 + 0 \cdot 1 + 0 \cdot X \\ \varphi(X) &= 1 \cdot 1 + 0 \cdot X + 0 \cdot X^2 = 0 \cdot X^2 + 1 \cdot 1 + 0 \cdot X \\ \varphi(X^2) &= 0 \cdot 1 + 2 \cdot X + 0 \cdot X^2 = 0 \cdot X^2 + 0 \cdot 1 + 2 \cdot X \\ \varphi(X^3) &= 0 \cdot 1 + 0 \cdot X + 3 \cdot X^2 = 3 \cdot X^2 + 0 \cdot 1 + 0 \cdot X\end{aligned}$$

de unde rezultă

$$[\varphi]_{u,v} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \text{ și } [\varphi]_{u,v'} = \begin{pmatrix} 0 & 0 & 0 & 3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \end{pmatrix}.$$

b) Fie  $K$  un corp comutativ,  $m, n \in \mathbb{N}^*$  și  $A \in M_{m,n}(K)$  iar  $e$  baza canonică a lui  $K^n$  și  $e'$  baza canonică a lui  $K^m$ . Scriind vectorii din  $K^n$  și  $K^m$  sub formă de matrice coloane se verifică ușor că

$$f_A : K^n \rightarrow K^m, f_A(x) = Ax$$

este o transformare liniară și  $[f_A]_{e,e'} = A$ .

**Teorema 4.2.** Fie  $K$  un corp comutativ,  $V, V', V''$   $K$ -spații vectoriale,  $f : V \rightarrow V'$ ,  $f' : V \rightarrow V'$ ,  $g : V' \rightarrow V''$  transformări liniare și  $\alpha \in K$ .

1) Dacă  $u = (u_1, \dots, u_n)$  și  $v = (v_1, \dots, v_m)$  sunt baze în  $V$ , respectiv  $V'$ , atunci

$$[f + f']_{u,v} = [f]_{u,v} + [f']_{u,v} \text{ și } [\alpha f]_{u,v} = \alpha [f]_{u,v}. \quad (5)$$

2) Dacă  $w = (w_1, \dots, w_p)$  este o bază a lui  $V''$ , atunci

$$[g \circ f]_{u,w} = [g]_{v,w} \cdot [f]_{u,v}. \quad (6)$$

*Demonstrație.* 1) Dacă  $[f]_{u,v} = (\alpha_{ij})$ ,  $[f']_{u,v} = (\alpha'_{ij})$  atunci

$$(f + f')(u_j) = f(u_j) + f'(u_j) = \sum_{i=1}^m \alpha_{ij} v_i + \sum_{i=1}^m \alpha'_{ij} v_i = \sum_{i=1}^m (\alpha_{ij} + \alpha'_{ij}) v_i$$

și

$$(\alpha f)(u_j) = \alpha f(u_j) = \alpha \sum_{i=1}^m \alpha_{ij} v_i = \sum_{i=1}^m (\alpha \alpha_{ij}) v_i$$

ceea ce demonstrează egalitățile (5).

2) Fie  $[g]_{v,w} = (b_{ij})$ . Folosind comutativitatea lui  $K$  avem

$$\begin{aligned}(g \circ f)(u_j) &= g(f(u_j)) = g\left(\sum_{k=1}^m \alpha_{kj} v_k\right) = \sum_{k=1}^m \alpha_{kj} g(v_k) = \\ &= \sum_{k=1}^m \alpha_{kj} \sum_{i=1}^p \beta_{ik} w_i = \sum_{i=1}^p \left(\sum_{k=1}^m \beta_{ik} \alpha_{kj}\right) w_i,\end{aligned}$$

de unde rezultă (6). □

**Corolarul 4.3.** a) Aplicația

$$\varphi : \text{Hom}_K(V, V') \rightarrow M_{m,n}(K), \quad \varphi(f) = [f]_{u,v}$$

este un izomorfism de  $K$ -spații vectoriale.

Într-adevăr din (5) urmează că  $\varphi$  este o transformare liniară, iar din Teorema 3.34 rezultă că  $\varphi$  este bijectivă. Deci  $\varphi$  este izomorfism.

b) Aplicația

$$\varphi : \text{End}_K(V) \rightarrow M_n(K), \quad \varphi(f) = [f]_{u,u}$$

este un izomorfism de  $K$ -spații vectoriale și de inele.

Într-adevăr, din a) urmează că  $\varphi$  este un izomorfism de  $K$ -spații vectoriale, iar din prima egalitate din (5) și din (6) rezultă că  $\varphi$  este un izomorfism de inele.

c) Aplicația

$$\varphi' : \text{Aut}_K(V) \rightarrow GL_n(K), \quad \varphi'(f) = [f]_{u,u}$$

este un izomorfism de grupuri. Matricea  $[f]_{u,u}$  se notează cu  $[f]_u$  și se numește **matricea lui  $f$  în baza  $u$** .

Această afirmație rezultă din b) și din faptul că un izomorfism între două inele cu unitate păstrează elementele inversabile.

d) Dacă  $u = (u_1, \dots, u_n)$  este o bază a lui  $V$  și  $u'_1, \dots, u'_n \in V$ , atunci  $u' = (u'_1, \dots, u'_n)$  este o bază a lui  $V$  dacă și numai dacă există o matrice inversabilă  $S = (s_{ij}) \in M_n(K)$  unic determinată (numită matricea de trecere de la baza  $u$  la baza  $u'$ ) astfel încât

$$u'_j = \sum_{i=1}^n s_{ij} u_i \quad (j = 1, \dots, n) \quad (7)$$

adică

$$(u'_1, \dots, u'_n) = (u_1, \dots, u_n) \cdot S.$$

Într-adevăr, dacă  $f : V \rightarrow V$  este endomorfismul definit pe baza  $u$  prin  $f(u_j) = u'_j$  ( $j = 1, \dots, n$ ), atunci din (7) rezultă  $S = [f]_u$ . Deci  $u'$  este o bază dacă și numai dacă  $f$  este un izomorfism ceea ce este echivalent cu  $S$  inversabilă. Acum, unicitatea lui  $S$  rezultă din bijectivitatea lui  $\varphi$ .

e) Dacă  $S$  este matricea de trecere de la baza  $u = (u_1, \dots, u_n)$  la baza  $u' = (u'_1, \dots, u'_n)$ , atunci  $S^{-1}$  este matricea de trecere de la baza  $u'$  la baza  $u$ .

f) Fie  $u = (u_1, \dots, u_n)$  și  $u' = (u'_1, \dots, u'_n)$  baze ordonate ale  $K$ -spațiului vectorial  $V$  și  $S = (s_{ij})$  matricea de trecere de la  $u$  la  $u'$ . Dacă  $x \in V$  și  $\alpha_1, \dots, \alpha_n$  respectiv  $\alpha'_1, \dots, \alpha'_n$  sunt coordonatele lui  $x$  în baza  $u$  respectiv  $u'$ , atunci

$$\alpha_i = \sum_{j=1}^n s_{ij} \alpha'_j \quad (i = 1, \dots, n), \quad (8)$$

Într-adevăr din (7) rezultă că  $S$  este matricea lui  $1_V$  în perechea de baze  $(u', u)$  ceea ce conform lui (4) implică (8).

Teorema următoare ne dă legea de dependență a matricei  $[f]_{u,v}$  de perechea de baze ordonate  $(u, v)$ .



**Teorema 4.4.** Fie  $u = (u_1, \dots, u_n)$  și  $u' = (u'_1, \dots, u'_n)$ , respectiv  $v = (v_1, \dots, v_m)$  și  $v' = (v'_1, \dots, v'_m)$  baze ale  $K$ -spațiului vectorial  $V$ , respectiv  $V'$ . Dacă  $S$  este matricea de trecere de la  $u$  la  $u'$  și  $T$  este matricea de trecere de la  $v$  la  $v'$ , atunci

$$[f]_{u',v'} = T^{-1} \cdot [f]_{u,v} \cdot S. \quad (9)$$

*Demonstrație.* Așa cum am văzut (în demonstrația Corolarului 4.3 f))  $S$  coincide cu matricea lui  $1_V$  în perechea de baze  $(u', u)$ . Întrucât  $T$  este matricea de trecere de la  $v$  la  $v'$  rezultă că  $T^{-1}$  coincide cu matricea lui  $1_{V'}$  în  $(v, v')$ . Acum din  $f = 1_{V'} \circ f \circ 1_V$  și din (6) deducem pe (9).  $\square$

**Corolarul 4.5.** Fie  $u = (u_1, \dots, u_n)$  și  $u' = (u'_1, \dots, u'_n)$  baze ale  $K$ -spațiului vectorial  $V$ ,  $S$  este matricea de trecere de la  $u$  la  $u'$  și  $f : V \rightarrow V$  este un endomorfism. Atunci

$$[f]_{u'} = S^{-1} \cdot [f]_u \cdot S.$$

## 4.2 Exerciții rezolvate

1) Fie  $v = ((1, 2), (-2, 1))$  și  $v' = ((1, -1, 0), (-1, 0, 1), (1, 1, 1))$ . Să se arate că  $v$ , respectiv  $v'$  este bază în  $\mathbb{R}^2$ , respectiv  $\mathbb{R}^3$  și să se scrie matricea transformării liniare  $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ ,  $f(x, y) = (x + y, 2x - y, 3x + 2y)$  în perechea de baze  $(v, v')$ .

*Soluție:* Cum rangul matricei formate cu vectorii din  $v$  este 2, iar rangul matricei formate cu vectorii din  $v'$  este 3, rezultă că  $v$  este bază în  $\mathbb{R}^2$  și  $v'$  este bază în  $\mathbb{R}^3$ . Coloanele matricei  $[f]_{v,v'} = (a_{ij}) \in M_{3,2}(\mathbb{R})$  rezultă din egalitățile

$$\begin{aligned} (3, 0, 7) &= f(1, 2) = a_{11}(1, -1, 0) + a_{21}(-1, 0, 1) + a_{31}(1, 1, 1), \\ (-1, -5, -4) &= f(-2, 1) = a_{12}(1, -1, 0) + a_{22}(-1, 0, 1) + a_{32}(1, 1, 1). \end{aligned}$$

Cele două egalități conduc la sistemele

$$\begin{cases} a_{11} - a_{21} + a_{31} = 3 \\ -a_{11} + a_{31} = 0 \\ a_{21} + a_{31} = 7 \end{cases} \quad \text{și} \quad \begin{cases} a_{12} - a_{22} + a_{32} = -1 \\ -a_{12} + a_{32} = -5 \\ a_{22} + a_{32} = -4 \end{cases}$$

care au, respectiv, soluțiile  $\left(\frac{10}{3}, \frac{11}{3}, \frac{10}{3}\right)$  și  $\left(\frac{5}{3}, -\frac{2}{3}, -\frac{10}{3}\right)$ . prin urmare,

$$[f]_{v,v'} = \begin{pmatrix} \frac{10}{3} & \frac{5}{3} \\ \frac{11}{3} & -\frac{2}{3} \\ \frac{10}{3} & -\frac{10}{3} \end{pmatrix}.$$

**Altă soluție:** Matricea de trecere de la baza canonică  $e'$  a lui  $\mathbb{R}^3$  la baza  $v'$  a lui  $\mathbb{R}^3$

este  $T = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ , iar matricea lui  $f$  în perechea de baze  $v, e'$  este

$$[f]_{v,e'} = \begin{pmatrix} 3 & -1 \\ 0 & -5 \\ 7 & -4 \end{pmatrix},$$

(colanele sale fiind coordonatele lui  $f(1, 2)$  și  $f(-2, 1)$  în baza  $e'$ ) prin urmare,

$$[f]_{v,v'} = T^{-1}[f]_{v,e'} = \begin{pmatrix} \frac{10}{3} & \frac{5}{3} \\ \frac{11}{3} & -\frac{2}{3} \\ \frac{10}{3} & -\frac{10}{3} \end{pmatrix}.$$

2) Fie  $f : \mathbb{R}^3 \rightarrow \mathbb{R}^4$  aplicația liniară definită pe baza canonică astfel:

$$f(e_1) = (1, 2, 3, 4), f(e_2) = (4, 3, 2, 1), f(e_3) = (-2, 1, 4, 1).$$

Să se determine:

- i)  $f(v)$  pentru orice  $v \in \mathbb{R}^3$ ;
- ii) matricea lui  $f$  în bazele canonice;
- iii) câte o bază în  $\text{Im } f$  și  $\text{Ker } f$ .

*Soluție:* i)  $f(x_1, x_2, x_3) = x_1 f(e_1) + x_2 f(e_2) + x_3 f(e_3)$ .

ii) Matricea lui  $f$  în bazele canonice este matricea care are ca și coloane pe  $f(e_1)$ ,  $f(e_2)$  și  $f(e_3)$ , respectiv, adică

$$\begin{pmatrix} 1 & 4 & -2 \\ 2 & 3 & 1 \\ 3 & 2 & 4 \\ 4 & 1 & 1 \end{pmatrix}.$$

iii)  $\text{Im } f = f(\langle e_1, e_2, e_3 \rangle) = \langle f(e_1), f(e_2), f(e_3) \rangle$ , deci

$$\dim(\text{Im } f) = \text{rang} \begin{pmatrix} 1 & 4 & -2 \\ 2 & 3 & 1 \\ 3 & 2 & 4 \\ 4 & 1 & 1 \end{pmatrix} = 3,$$

prin urmare  $f(e_1)$ ,  $f(e_2)$  și  $f(e_3)$  formează o bază în  $\text{Im } f$ . Atunci

$$\dim(\text{Ker } f) = \dim \mathbb{R}^3 - \dim(\text{Im } f) = 3 - 3 = 0,$$

deci  $\text{Ker } f = \{(0, 0, 0)\}$  și  $\emptyset$  este bază în  $\text{Ker } f$ .

3) Fie  $V, V'$   $\mathbb{R}$ -spații vectoriale,  $v = (v_1, v_2, v_3)$  o bază în  $V$ ,  $v' = (v'_1, v'_2, v'_3)$  o bază în  $V'$  și  $f : V \rightarrow V'$  transformarea liniară cu

$$[f]_{v,v'} = \begin{pmatrix} 0 & -1 & 5 \\ 1 & 0 & 0 \\ 0 & 1 & -5 \end{pmatrix}.$$

Să se determine:

- i) dimensiunea și câte o bază pentru  $\text{Im } f$  și  $\text{Ker } f$ ;
- ii)  $[f]_{v,e'}$  în cazul în care  $V' = \mathbb{R}^3$ ,  $v'_1 = (1, 0, 0)$ ,  $v'_2 = (0, 1, 1)$ ,  $v'_3 = (0, 0, 1)$  și  $e'$  este baza canonică a lui  $\mathbb{R}^3$ ;
- iii)  $f(x)$  pentru  $x = 2v_1 - v_2 + 3v_3$ , în condițiile de la ii).

*Soluție:* i) Reamintim că coloanele matricii  $[f]_{v,v'}$  reprezintă coordonatele vectorilor  $f(v_1)$ ,  $f(v_2)$ , respectiv  $f(v_3)$  în baza  $v'$ , adică

$$f(v_1) = v'_2, \quad f(v_2) = -v'_1 + v'_3 \quad \text{și} \quad f(v_3) = 5v'_1 - 5v'_3.$$

Atunci  $\dim(\text{Im } f) = \text{rang}[f]_{v,v'} = 2$ , iar un minor nenul de ordinul 2 al matricii  $[f]_{v,v'}$  poate fi decupat din primele 2 coloane (și primele 2 linii), prin urmare,  $f(v_1)$  și  $f(v_2)$  formează o bază în  $\text{Im } f$ . Deducem că

$$\dim(\text{Ker } f) = \dim V - \dim(\text{Im } f) = 3 - 2 = 1,$$

iar cum coloanele 2 și 3 ale matricii  $[f]_{v,v'}$  sunt proporționale, avem

$$f(v_3) = -5f(v_2) \Leftrightarrow f(v_3 - 5v_2) = 0 \Leftrightarrow v_3 - 5v_2 \in \text{Ker } f.$$

Prin urmare,  $v_3 - 5v_2$  formează o bază în  $\text{Ker } f$ .

ii) Matricea de trecere de la baza canonică  $e'$  la baza  $v'$  este matricea  $T$  care are ca și coloane vectorii  $v'_1$ ,  $v'_2$ ,  $v'_3$ , iar

$$[f]_{v,v'} = T^{-1}[f]_{v,e'} \Leftrightarrow [f]_{v,e'} = T[f]_{v,v'}.$$

iii) Cum coloanele matricii  $[f]_{v,e'}$  reprezintă coordonatele vectorilor  $f(v_1)$ ,  $f(v_2)$ , respectiv  $f(v_3)$  în baza canonică  $e'$ , ele vor fi chiar vectorii  $f(v_1)$ ,  $f(v_2)$ ,  $f(v_3)$  din  $\mathbb{R}^3$ , iar

$$f(x) = f(2v_1 - v_2 + 3v_3) = 2f(v_1) - f(v_2) + 3f(v_3).$$

Lăsăm calculele în seama cititorului.

4) Fie  $f \in \text{End}_{\mathbb{Q}}(\mathbb{Q}^4)$  pentru care matricea în baza canonică este

$$\begin{pmatrix} 1 & 2 & 1 & 2 \\ 3 & 2 & 3 & 2 \\ -1 & -3 & 0 & 4 \\ 0 & 4 & -1 & -3 \end{pmatrix}.$$

Să se determine câte o bază în  $\text{Ker } f$  și  $\text{Im } f$ .

*Soluție:* Fie  $e = (e_1, e_2, e_3, e_4)$  baza canonică a lui  ${}_{\mathbb{Q}}\mathbb{Q}^4$ . Matricea dată este  $[f]_e$ , iar coloanele sale sunt vectorii  $f(e_1)$ ,  $f(e_2)$ ,  $f(e_3)$ , respectiv  $f(e_4)$ . Pentru determinarea unei baze și a dimensiunii lui  $\text{Im } f$  se calculează rangul matricii  $[f]_e$ , urmărind din ce coloane a fost „decupat” un minor nenul de ordin egal cu  $\text{rang}[f]_e$ . Obținem  $\dim(\text{Im } f) = 3$ , în consecință,  $\dim(\text{Ker } f) = 1$ . Pentru determinarea unei baze în  $\text{Ker } f$  fie procedăm ca la punctul i) al problemei anterioare, observând că  $7(c_1 - c_3) = c_2 - c_4$  (unde cu  $c_i$  am notat coloana  $i$  a matricii date care este chiar  $f(e_i)$ ), fie se procedează astfel:

$$(x_1, x_2, x_3, x_4) \in \text{Ker } f \Leftrightarrow [f]_e \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{cases} x_1 + 2x_2 + x_3 + 2x_4 = 0 \\ 3x_1 + 2x_2 + 3x_3 + 2x_4 = 0 \\ -x_1 - 3x_2 + 4x_4 = 0 \\ +4x_2 - x_3 - 3x_4 = 0 \end{cases}.$$

Mulțimea soluțiilor acestui sistem de ecuații liniare este

$$\{(7\alpha, -\alpha, -7\alpha, \alpha) \in \mathbb{Q}^4 \mid \alpha \in \mathbb{Q}\} = \{\alpha(7, -1, -7, 1) \mid \alpha \in \mathbb{Q}\} = \langle (7, -1, -7, 1) \rangle,$$

prin urmare vectorul  $(7, -1, -7, 1)$  este un generator liber, adică o bază, în  $\text{Ker } f$ .

### 4.3 Sisteme de ecuații liniare

Pentru o bună înțelegere a acestei secțiuni, recomandăm cititorilor să își reamintească definițiile și proprietățile determinantilor, precum și ale rangului unei matrice. Pentru a veni în sprijinul lor în acest sens, vom prezenta câteva astfel de proprietăți care vor apărea în discuțiile noastre ulterioare.

Fie  $K$  un corp comutativ,  $A = (a_{ij}) \in M_n(K)$ ,  $n \geq 2$ ,  $d = \det A$ ,  $d_{ij}$  minorul lui  $a_{ij}$  și  $\alpha_{ij} = (-1)^{i+j} d_{ij}$  complementul algebric al elementului  $a_{ij}$ . Au loc următoarele:

- 1) Determinantul matricei  $A$  este egal cu determinantul matricei transpuse  ${}^t A$ .
- 2) Dacă matricea  $B$  se obține din  $A$  prin înmulțirea fiecărui element dintr-o linie (coloană) a lui  $A$  cu un scalar  $\alpha$  atunci  $\det(B) = \alpha \det(A)$ .
- 3) Dacă  $A$  are două linii (coloane) egale, atunci  $\det(A) = 0$ .
- 4) Dacă matricea  $B$  se obține din  $A$  prin permutarea a două linii (coloane) ale lui  $A$  atunci  $\det(B) = -\det(A)$ .
- 5) Dacă o linie (coloană) a matricei  $A$  este formată numai din zerouri atunci  $\det(A) = 0$ .
- 6) Dacă matricea  $B$  se obține din  $A$  prin adunarea la linia (coloana)  $i$  a liniei (coloanei)  $j$ , cu  $i \neq j$ , înmulțită cu un scalar, atunci  $\det B = \det A$ .
- 7) Dacă o linie (coloană) a lui  $A$  este o combinație liniară a celorlalte linii (coloane), atunci  $\det A = 0$ .
- 8) Dacă  $A, B \in M_n(K)$  atunci  $\det(AB) = \det(A) \cdot \det(B)$ .
- 9) **(dezvoltarea determinantului  $\det(A)$  după linia  $i$ )**

$$\det(A) = a_{i1}\alpha_{i1} + a_{i2}\alpha_{i2} + \cdots + a_{in}\alpha_{in}, \quad \forall i \in \{1, \dots, n\}.$$

- 10) **(dezvoltarea determinantului  $\det(A)$  după coloana  $j$ )**

$$\det A = a_{1j}\alpha_{1j} + a_{2j}\alpha_{2j} + \cdots + a_{nj}\alpha_{nj}, \quad \forall j \in \{1, \dots, n\}.$$

- 11) Dacă  $i, k \in \{1, \dots, n\}$ ,  $i \neq k$ , atunci

$$a_{i1}\alpha_{k1} + a_{i2}\alpha_{k2} + \cdots + a_{in}\alpha_{kn} = 0.$$

- 12) Dacă  $j, k \in \{1, \dots, n\}$ ,  $j \neq k$  atunci

$$a_{1j}\alpha_{1k} + a_{2j}\alpha_{2k} + \cdots + a_{nj}\alpha_{nk} = 0.$$

Din cele de mai sus rezultă imediat următoarea:

**Teorema 4.6.** O matrice  $A = (a_{ij}) \in M_n(K)$  este inversabilă dacă și numai dacă  $d = \det(A) \neq 0$ . În acest caz

$$A^{-1} = d^{-1} \cdot A^*.$$

*Demonstrație.* Dacă  $A$  este inversabilă, adică există  $A^{-1} \in M_n(K)$  astfel încât

$$A^{-1} \cdot A = I_n = A \cdot A^{-1}$$

de unde, conform 8), rezultă

$$\det(A^{-1}) \cdot \det(A) = 1$$

ceea ce implică  $d \neq 0$ .

Invers, presupunem că  $d \neq 0$ . Din 9), 10), 11) și 12) urmează

$$A^* \cdot A = d \cdot I_n = A \cdot A^*$$

de unde deducem că dacă  $d \neq 0$ , atunci  $A$  este inversabilă și  $A^{-1} = d^{-1} \cdot A^*$ .  $\square$

De asemenea, proprietățile de mai sus permit stabilirea următoarei legături între rangul unei matrici și dimensiunea subspațiului generat de liniile (coloanele) sale.

**Teorema 4.7.** Dacă  $A \in M_{m,n}(K)$  și  $l_1^A, \dots, l_m^A \in K^n$  respectiv  $c_1^A, \dots, c_n^A \in K^m$  sunt liniile respectiv coloanele lui  $A$ , atunci

$$\text{rang } A = \dim \langle l_1^A, \dots, l_m^A \rangle = \dim \langle c_1^A, \dots, c_n^A \rangle.$$

unde  $\langle l_1^A, \dots, l_m^A \rangle$ , respectiv  $\langle c_1^A, \dots, c_n^A \rangle$  este subspațiul lui  $K^n$ , respectiv  $K^m$  generat de  $l_1^A, \dots, l_m^A$ , respectiv  $c_1^A, \dots, c_n^A$ .

*Demonstrație.* Fie  $r = \text{rang } A$ . Rezultă că  $A$  are un minor de ordinul  $r$  nenul, pentru a nu complica notațiile, presupunem că

$$d = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ \vdots & \vdots & & \vdots \\ a_{r1} & a_{r2} & \dots & a_{rr} \end{vmatrix} \neq 0$$

și orice minor de ordinul  $r + 1$  este zero. Prin urmare determinantul

$$D_{ij} = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1r} & a_{1j} \\ a_{21} & a_{22} & \dots & a_{2r} & a_{2j} \\ \vdots & \vdots & & \vdots & \vdots \\ a_{r1} & a_{r2} & \dots & a_{rr} & a_{rj} \\ a_{i1} & a_{i2} & \dots & a_{ir} & a_{ij} \end{vmatrix}$$

de ordinul  $r + 1$ , obținut prin adăugarea la  $d$  a liniei  $i$  și a coloanei  $j$ , cu  $1 \leq i \leq m$  și  $r < j \leq n$ , este zero, adică  $D_{ij} = 0$ . Dacă  $r < i \leq m$  și  $r < j \leq n$ , atunci spunem că  $D_{ij}$  se obține din  $d$  prin **bordarea** lui  $d$  cu linia  $i$  și coloana  $j$ . Dezvoltând determinantul  $D_{ij}$  după linia  $r + 1$  primim

$$a_{i1}d_1 + a_{i2}d_2 + \dots + a_{ir}d_r + a_{ij}d = 0$$

unde complementii algebrici  $d_1, d_2, \dots, d_r$  nu depind de linia adăugată. Rezultă

$$a_{ij} = -d^{-1}d_1a_{i1} - d^{-1}d_2a_{i2} - \dots - d^{-1}d_r a_{ir}$$

pentru  $i = 1, 2, \dots, m$  și  $j = r + 1, \dots, n$  ceea ce ne arată că

$$c_j^A = \alpha_1 c_1^A + \alpha_2 c_2^A + \dots + \alpha_r c_r^A \text{ pentru } j = r + 1, \dots, n,$$

unde  $\alpha_k = -d^{-1}d_k$ ,  $1 \leq k \leq r$ , adică  $c_j^A$  este combinație liniară de  $c_1^A, c_2^A, \dots, c_r^A$ . Astfel am arătat că  $\dim \langle c_1^A, \dots, c_n^A \rangle \leq r$ . Dacă am avea  $\dim \langle c_1^A, \dots, c_r^A \rangle < r$  ar rezulta că una dintre coloanele  $c_1^A, \dots, c_r^A$  ar fi o combinație liniară a celorlalte, ceea ce ar implica  $d = 0$  ceea ce este fals. Astfel am arătat că  $\dim \langle c_1^A, \dots, c_r^A \rangle = r$ . De aici și din  $\text{rang } A = \text{rang } {}^t A$  rezultă  $\dim \langle l_1^A, \dots, l_n^A \rangle = r$ .  $\square$





Teorema următoare rezolvă problema compatibilității sau incompatibilității unui sistem de ecuații liniare.

**Teorema 4.10. (Kronecker-Cappelli)** Sistemul (1) este compatibil dacă și numai dacă rangul matricei sistemului este egal cu rangul matricei extinse, adică  $\text{rang } A = \text{rang } \bar{A}$ .

*Demonstrație.* Notând cu  $c_1^A, \dots, c_n^A$  coloanele matricei  $A$  și cu  $c_{n+1}^{\bar{A}}$  ultima coloană a lui  $\bar{A}$ , adică  $c_{n+1}^{\bar{A}} = B$ , atunci  $A = (c_1^A, \dots, c_n^A)$  și  $\bar{A} = (c_1^A, \dots, c_n^A, c_{n+1}^{\bar{A}})$  iar sistemul (1) se poate scrie sub formă vectorială astfel:

$$x_1 c_1^A + \dots + x_n c_n^A = c_{n+1}^{\bar{A}} \quad (3)$$

ceea ce ne arată că sistemul (1) este compatibil dacă și numai dacă vectorul  $c_{n+1}^{\bar{A}}$  este o combinație liniară a vectorilor  $c_1^A, \dots, c_n^A$ . Egalitatea de vectori (3) este echivalentă cu egalitatea

$$\langle c_1^A, \dots, c_n^A \rangle = \langle c_1^A, \dots, c_n^A, c_{n+1}^{\bar{A}} \rangle$$

de subspații generate, care la rândul ei este echivalentă cu

$$\dim \langle c_1^A, \dots, c_n^A \rangle = \dim \langle c_1^A, \dots, c_n^A, c_{n+1}^{\bar{A}} \rangle.$$

De aici, folosind Teorema 4.7, rezultă că sistemul (1) este compatibil dacă și numai dacă  $\text{rang } A = \text{rang } \bar{A}$ .  $\square$

Dacă  $\text{rang } A = r$  atunci există în  $A$  un minor de ordinul  $r$  nenul și toți minorii din  $A$  de ordin mai mare decât  $r$  sunt nuli. Un minor al lui  $A$  de ordinul  $r$  nenul se numește **minor principal**. Dacă  $d_p$  este un minor principal, atunci minorii de ordinul  $r+1$  obținuți prin bordarea lui  $d_p$  cu coloana termenilor liberi și cu câte o linie care nu intervine în  $d_p$ , se numesc **minori caracteristici**. Numărul minorilor caracteristici este  $m-r$ .

Având în vedere modul cum se obține  $\bar{A}$  din  $A$  și știind că rangul unei matrice este  $r$  dacă și numai dacă are un minor de ordinul  $r$  nenul și toți minorii de ordinul  $r+1$  care bordează acest minor sunt zero, rezultă că  $\text{rang } A = \text{rang } \bar{A}$  dacă și numai dacă toți minorii caracteristici sunt nuli. Prin urmare, Teorema lui Kronecker-Cappelli este echivalentă cu:

**Teorema 4.11. (Rouché)** Sistemul (1) este compatibil dacă și numai dacă toți minorii caracteristici corespunzători unui minor principal sunt nuli.

**Teorema 4.12.** 1) Mulțimea soluțiilor unui sistem liniar și omogen de  $m$  ecuații cu  $n$  necunoscute formează un subspațiu al lui  $K^n$  de dimensiune  $n-r$ , unde  $r$  este rangul matricei sistemului.

2) Dacă  $S_0$  este mulțimea soluțiilor sistemului liniar și omogen asociat lui (1) și  $S_B$  este mulțimea soluțiilor sistemului (1), atunci

$$S_B = s + S_0 \quad (4)$$

unde  $s$  este o soluție a sistemului (1).



*Demonstrație.* 1) Dacă  $A \in M_{m,n}(K)$ , atunci

$$f_A : K^n \rightarrow K^m, f_A(X) = AX$$

este o transformare liniară și mulțimea  $S_0$  a soluțiilor sistemului omogen  $AX = O_{m,1}$  coincide cu  $\text{Ker } f_A$ . Deci  $S_0$  este subspațiu a lui  $K^n$ . Din Teorema 3.42 rezultă

$$\dim K^n = \dim \text{Ker } f_A + \dim f_A(K^n)$$

de unde urmează  $n = \dim S_0 + r$ , adică  $\dim S_0 = n - r$ .

2) Scriind sistemul (1) sub forma (2), avem

$$f_A(s + S_0) = f(s) = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

ceea ce ne arată că orice vector din  $s + S_0$  este soluție a sistemului (1), adică  $s + S_0 \subseteq S_B$ . Pentru orice  $s' \in S_B$  avem

$$f_A(s' - s) = f_A(s') - f(s) = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} - \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

de unde rezultă  $s' - s \in S_0$ , adică  $s' \in s + S_0$ . Astfel am arătat că  $S_B \subseteq s + S_0$ . Din cele două incluziuni stabilite rezultă egalitatea (4).  $\square$

**Corolarul 4.13.** a) Un sistem liniar și omogen are numai soluția nulă dacă și numai dacă numărul necunoscutelor este egal cu rangul sistemului.

b) Un sistem liniar și omogen de  $n$  ecuații cu  $n$  necunoscute are numai soluția nulă dacă și numai dacă determinantul matricei sistemului este diferit de zero.

c) Dacă sistemul (1) este compatibil, atunci acesta are soluție unică dacă și numai dacă  $\text{rang } A = n$ , adică rangul sistemului coincide cu numărul necunoscutelor.

În continuare vom prezenta două abordări a problemei rezolvării unui sistem liniar de forma (1).

**1. Cu ajutorul teoremei Rouché** studiem compatibilitatea sau incompatibilitatea sistemului (1). Dacă există un minor caracteristic nenul, atunci sistemul este incompatibil și procedeul se încheie. Dacă toți minorii caracteristici sunt nuli, atunci sistemul este compatibil. Dacă  $d_p$  este un minor principal și ordinul lui  $d_p$  este  $r$  atunci cele  $r$  ecuații care ne dau liniile lui  $d_p$  se numesc **ecuații principale**, iar necunoscutele ale căror coeficienți intervin în  $d_p$  se numesc **necunoscute principale**. Celelalte  $m - r$  ecuații și  $n - r$  necunoscute se numesc **secundare**. Din  $\text{rang } \bar{A} = \text{rang } A = r$ , rezultă, conform Corolarului 4.8 b), că ecuațiile secundare sunt combinații liniare a ecuațiilor principale. Prin urmare sistemul (1) are aceleași soluții ca și sistemul format numai din ecuațiile principale, adică cele două sisteme sunt echivalente. Pentru simplificarea scrierii



Așa cum se va observa în Exercițiul rezolvat 2), sunt cazuri în care putem lucra foarte bine cu forma eșalon. Dacă, însă, dorim să ajungem la forma trapezoidală  $B$ , este necesar uneori să permutăm câte 2 coloane ale matricii obținute din matricea sistemului, ceea ce corespunde permutării a câte doi termeni în fiecare din ecuațiile sistemului echivalent corespunzător.

Dacă pe parcursul acestui procedeu, apare într-o linie a unei matrici 0 în toate pozițiile corespunzătoare matricii sistemului și un element nenul  $a$  în ultima poziție, adică în coloana corespunzătoare termenilor liberi atunci sistemul dat este incompatibil, ecuația corespunzătoare din sistemul echivalent corespunzător fiind  $0 = a$ .

Elementele nenule de pe diagonala lui  $B$  furnizează necunoscutele principale, iar sistemul obținut prin parametrizarea necunoscutelor secundare se rezolvă începând cu ultima ecuație.

#### 4.4 Exerciții rezolvate

1) Să se rezolve în  $\mathbb{R}^3$  sistemul de ecuații

$$\begin{cases} x_1 + x_2 + 2x_3 = -1 \\ 2x_1 - x_2 + 2x_3 = -4 \\ 4x_1 + x_2 + 4x_3 = -2. \end{cases}$$

*Soluție: Metoda I* (cu metoda lui Gauss) Matricea extinsă a sistemului este

$$\bar{A} = \left( \begin{array}{ccc|c} 1 & 1 & 2 & -1 \\ 2 & -1 & 2 & -4 \\ 4 & 1 & 4 & -2 \end{array} \right)$$

Scăzând din linia 2 linia 1 înmulțită cu 2, ceea ce vom nota cu  $l_2 - 2l_1$ , iar din linia 3 linia 1 înmulțită cu 4 obținem matricea

$$\bar{A}_1 = \left( \begin{array}{ccc|c} 1 & 1 & 2 & -1 \\ 0 & -3 & -2 & -2 \\ 0 & -3 & -4 & 2 \end{array} \right)$$

Continuând cu transformarea  $l_3 - l_2$  ajungem la matricea eșalon:

$$\bar{A}_2 = \left( \begin{array}{ccc|c} 1 & 1 & 2 & -1 \\ 0 & -3 & -2 & -2 \\ 0 & 0 & -2 & 4 \end{array} \right)$$

Deci sistemul dat este echivalent cu sistemul

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

Rezultă că sistemul dat are soluție unică, din ultima ecuație obținem  $x_3 = -2$ , din a doua  $x_2 = 2$ , iar din prima  $x_1 = 1$ . Deci sistemul are soluția  $(1, 2, -2)$ .

Dacă în  $\bar{A}_2$  continuăm cu transformările

$$\bar{A}_2 \begin{matrix} l_2 \sim l_3 \\ l_1 + l_3 \end{matrix} \begin{pmatrix} 1 & 1 & 0 & 3 \\ 0 & -3 & 0 & -6 \\ 0 & 0 & -2 & 4 \end{pmatrix} \begin{matrix} l_1 + \frac{1}{3}l_2 \end{matrix} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & -3 & 0 & -6 \\ 0 & 0 & -2 & 4 \end{pmatrix}$$

spunem că am aplicat **metoda lui Gauss-Jordan** care reduce sistemul la forma:

$$\begin{cases} x_1 = 1 \\ -3x_2 = -6 \\ -2x_3 = 4 \end{cases}$$

de unde se deduce imediat soluția.

**Metoda II** (cu Teorema lui Rouché)

Determinantul matricei sistemului este

$$\begin{vmatrix} 1 & 1 & 2 \\ 2 & -1 & 2 \\ 4 & 1 & 4 \end{vmatrix} = 6.$$

Deci sistemul dat este ca cel din Teorema 4.9. Prin urmare, este compatibil determinat și soluția sa este dată de formulele lui Cramer. Lăsăm calculele în seama cititorului.

2) Să se rezolve în  $\mathbb{R}^4$  sistemul de ecuații

$$\begin{cases} 3x_1 + 4x_2 + x_3 + 2x_4 = 3 \\ 6x_1 + 8x_2 + 2x_3 + 5x_4 = 7 \\ 9x_1 + 12x_2 + 3x_3 + 10x_4 = 13 \end{cases}$$

*Soluție: Metoda I* (cu metoda lui Gauss)

Scriem matricea extinsă a sistemului și efectuăm transformările elementare indicate

$$\bar{A} = \left( \begin{array}{cccc|c} 3 & 4 & 1 & 2 & 3 \\ 6 & 8 & 2 & 5 & 7 \\ 9 & 12 & 3 & 10 & 13 \end{array} \right) \begin{matrix} l_2 \sim 2l_1 \\ l_3 \sim 3l_1 \end{matrix} \left( \begin{array}{cccc|c} 3 & 4 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 4 & 4 \end{array} \right) \\ \begin{matrix} l_3 \sim 4l_2 \end{matrix} \left( \begin{array}{cccc|c} 3 & 4 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

ceea ce ne arată că sistemul este echivalent cu

$$\begin{cases} 3x_1 + 4x_2 + x_3 + 2x_4 = 3 \\ x_4 = 1 \end{cases}$$

și  $x_1, x_4$  sunt necunoscute principale. Rezultă că sistemul dat are soluțiile:

$$\left( \frac{1}{3}(1 - 4\alpha - \beta), \alpha, \beta, 1 \right) \text{ cu } \alpha, \beta \in \mathbb{R}.$$

**Metoda II** (cu Teorema lui Rouché) Avem

$$\begin{vmatrix} 1 & 2 \\ 2 & 5 \end{vmatrix} = 1 \text{ și } \begin{vmatrix} 3 & 1 & 2 \\ 6 & 2 & 5 \\ 9 & 3 & 10 \end{vmatrix} = \begin{vmatrix} 4 & 1 & 2 \\ 8 & 2 & 5 \\ 12 & 3 & 10 \end{vmatrix} = 0$$

(având primele 2 coloane proporționale). Prin urmare,  $\begin{vmatrix} 1 & 2 \\ 2 & 5 \end{vmatrix}$  este un minor principal.

Există un singur minor caracteristic  $\begin{vmatrix} 1 & 2 & 3 \\ 2 & 5 & 7 \\ 3 & 10 & 13 \end{vmatrix}$  care este 0 deoarece coloana 3 este suma coloanelor 1 și 2. Așadar, sistemul dat este compatibil nedeterminat, echivalent cu sistemul

$$\begin{cases} x_3 + 2x_4 = 3 - 3x_1 - 4x_2 \\ 2x_3 + 5x_4 = 7 - 6x_1 - 8x_2 \end{cases}$$

în care necunoscutele secundare  $x_1, x_2$  sunt considerate parametri reali. Rezolvarea acestui sistem de 2 ecuații cu 2 necunoscute este un exercițiu simplu, pe care îl lăsăm cititorului.

3) Să se rezolve, în  $\mathbb{R}^3$ , sistemul de ecuații

$$\begin{cases} x_1 + x_2 - 3x_3 = -1 \\ 2x_1 + x_2 - 2x_3 = 1 \\ x_1 + x_2 + x_3 = 3 \\ x_1 + 2x_2 - 3x_3 = 1 \end{cases}$$

*Soluție: Metoda I* (cu metoda lui Gauss)

$$\begin{aligned} \bar{A} &= \left( \begin{array}{ccc|c} 1 & 1 & -3 & -1 \\ 2 & 1 & -2 & 1 \\ 1 & 1 & 1 & 3 \\ 1 & 2 & -3 & 1 \end{array} \right) \sim \left( \begin{array}{ccc|c} 1 & 1 & -3 & -1 \\ 0 & -1 & 4 & 3 \\ 0 & 0 & 4 & 4 \\ 0 & 1 & 0 & 2 \end{array} \right) \sim \\ &\sim \left( \begin{array}{ccc|c} 1 & 1 & -3 & -1 \\ 0 & -1 & 4 & 3 \\ 0 & 0 & 4 & 4 \\ 0 & 0 & 4 & 5 \end{array} \right) \sim \left( \begin{array}{ccc|c} 1 & 1 & -3 & -1 \\ 0 & -1 & 4 & 3 \\ 0 & 0 & 4 & 4 \\ 0 & 0 & 0 & 1 \end{array} \right). \end{aligned}$$

Ultima linie ne conduce la  $0 \cdot x_4 = 1$ , ceea ce este fals. Rezultă că sistemul dat este incompatibil.

**Metoda II** (cu Teorema lui Rouché)

$$\text{Avem } \begin{vmatrix} 1 & 1 & -3 \\ 2 & 1 & -2 \\ 1 & 1 & 1 \end{vmatrix} = -4 \neq 0, \text{ iar minorul caracteristic } \begin{vmatrix} 1 & 1 & -3 & -1 \\ 2 & 1 & -2 & 1 \\ 1 & 1 & 1 & 3 \\ 1 & 2 & -3 & 1 \end{vmatrix} = -4 \text{ fiind}$$

nenul, sistemul este incompatibil.

4) Să se discute după parametrul real  $\alpha$  compatibilitatea sistemului de mai jos, apoi să se rezolve în  $\mathbb{R}^4$ :

$$\begin{cases} 2x_1 - x_2 + 3x_3 + 4x_4 = 5 \\ 4x_1 - 2x_2 + 5x_3 + 6x_4 = 7 \\ 6x_1 - 3x_2 + 7x_3 + 8x_4 = 9 \\ \alpha x_1 - 4x_2 + 9x_3 + 10x_4 = 11 \end{cases}.$$

*Soluție: Metoda I* (cu metoda lui Gauss)

Pornind de la matricea extinsă a sistemului obținem succesiv matricele:

$$\begin{pmatrix} 2 & -1 & 3 & 4 & 5 \\ 4 & -2 & 5 & 6 & 7 \\ 6 & -3 & 7 & 8 & 9 \\ \alpha & -4 & 9 & 10 & 11 \end{pmatrix} \sim \begin{pmatrix} -1 & 2 & 3 & 4 & 5 \\ -2 & 4 & 5 & 6 & 7 \\ -3 & 6 & 7 & 8 & 9 \\ -4 & \alpha & 9 & 10 & 11 \end{pmatrix} \sim \begin{pmatrix} -1 & 2 & 3 & 4 & 5 \\ 0 & 0 & -1 & -2 & -3 \\ 0 & 0 & -2 & -4 & -6 \\ 0 & \alpha - 8 & -3 & -6 & -9 \end{pmatrix}$$

$$\sim \begin{pmatrix} -1 & 2 & 3 & 4 & 5 \\ 0 & -2 & -1 & 0 & -3 \\ 0 & -4 & -2 & 0 & -6 \\ 0 & -6 & -3 & \alpha - 8 & -9 \end{pmatrix} \sim \begin{pmatrix} -1 & 2 & 3 & 4 & 5 \\ 0 & -2 & -1 & 0 & -3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha - 8 & 0 \end{pmatrix}$$

$$\sim \begin{pmatrix} -1 & 2 & 3 & 4 & 5 \\ 0 & -2 & -1 & 0 & -3 \\ 0 & 0 & 0 & \alpha - 8 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} -1 & 2 & 4 & 3 & 5 \\ 0 & -2 & 0 & -1 & -3 \\ 0 & 0 & \alpha - 8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Rezultă că sistemul dat este compatibil nedeterminat.

1) Dacă  $\alpha \neq 8$ , ținând seama de permutările de coloane efectuate anterior obținem sistemul de mai jos (care este echivalent cu sistemul dat):

$$\begin{cases} -x_2 + 2x_4 + 4x_1 + 3x_3 = 5 \\ -2x_4 - x_3 = -3 \\ (\alpha - 8)x_1 = 0 \end{cases}.$$

Mulțimea soluțiilor sale este

$$S = \left\{ \left( 0, -2 + 2x_3, x_3, \frac{3}{2} - \frac{x_3}{2} \right) \mid x_3 \in \mathbb{R} \right\}.$$

2) Dacă  $\alpha = 8$ , sistemul dat este echivalent cu sistemul

$$\begin{cases} -x_2 + 2x_4 + 4x_1 + 3x_3 = 5 \\ -2x_4 - x_3 = -3 \end{cases},$$

pentru care mulțimea soluțiilor este

$$S = \left\{ \left( x_1, -2 + 4x_1 + 2x_3, x_3, \frac{3}{2} - \frac{x_3}{2} \right) \mid x_1, x_3 \in \mathbb{R} \right\}.$$

**Metoda II** (cu Teorema lui Rouché)

$$\text{Avem } \begin{vmatrix} -1 & 3 \\ -2 & 5 \end{vmatrix} = 1,$$

$$\begin{vmatrix} 2 & -1 & 3 \\ 4 & -2 & 5 \\ 6 & -3 & 7 \end{vmatrix} = \begin{vmatrix} -1 & 3 & 4 \\ -2 & 5 & 6 \\ -3 & 7 & 8 \end{vmatrix} = \begin{vmatrix} -1 & 3 & 4 \\ -2 & 5 & 6 \\ -4 & 9 & 10 \end{vmatrix} = 0 \text{ și } \begin{vmatrix} 2 & -1 & 3 \\ 4 & -2 & 5 \\ \alpha & -4 & 9 \end{vmatrix} = \alpha - 8.$$

1) Dacă  $\alpha = 8$ , atunci  $\begin{vmatrix} -1 & 3 \\ -2 & 5 \end{vmatrix}$  este minor principal. Minoriile caracteristici corespunzătoare sunt

$$\begin{vmatrix} -1 & 3 & 5 \\ -2 & 5 & 7 \\ -3 & 7 & 9 \end{vmatrix} = \begin{vmatrix} -1 & 3 & 5 \\ -2 & 5 & 7 \\ -4 & 9 & 11 \end{vmatrix} = 0,$$

sistemul compatibil nedeterminat și rezolvarea sa revine la rezolvarea unui sistem de 2 ecuații cu 2 necunoscute.

2) Dacă  $\alpha \neq 8$ , atunci  $\begin{vmatrix} 2 & -1 & 3 \\ 4 & -2 & 5 \\ \alpha & -4 & 9 \end{vmatrix}$  este minor principal. Singurul minor caracteristic corespunzător este nul, sistemul este compatibil, echivalent cu

$$\begin{cases} 2x_1 - x_2 + 3x_3 = 5 - 4x_4 \\ 4x_1 - 2x_2 + 5x_3 = 7 - 6x_4 \\ \alpha x_1 - 4x_2 + 9x_3 = 11 - 10x_4 \end{cases},$$

sistem care se rezolvă cu regula lui Cramer.

Să observăm că cele două situații de compatibilitate nedeterminată sunt diferite, într-un caz având 2 necunoscute principale, în celălalt 3.

5) Să se discute după parametrul real  $\alpha$  compatibilitatea sistemului de mai jos, apoi să se rezolve în  $\mathbb{R}^3$ :

$$\begin{cases} \alpha x_1 + x_2 + x_3 = 1 \\ x_1 + \alpha x_2 + x_3 = 1 \\ x_1 + x_2 + \alpha x_3 = 1 \end{cases}.$$

*Soluție: Metoda I* (cu metoda lui Gauss) Obținem succesiv matricele echivalente:

$$\begin{aligned} \begin{pmatrix} \alpha & 1 & 1 & 1 \\ 1 & \alpha & 1 & 1 \\ 1 & 1 & \alpha & 1 \end{pmatrix} &\sim \begin{pmatrix} 1 & 1 & \alpha & 1 \\ 1 & \alpha & 1 & 1 \\ \alpha & 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & \alpha & 1 \\ 0 & \alpha - 1 & 1 - \alpha & 0 \\ 0 & 1 - \alpha & (1 - \alpha)(1 + \alpha) & 1 - \alpha \end{pmatrix} \\ &\sim \begin{pmatrix} 1 & 1 & \alpha & 1 \\ 0 & \alpha - 1 & 1 - \alpha & 0 \\ 0 & 0 & (1 - \alpha)(2 + \alpha) & 1 - \alpha \end{pmatrix} = B. \end{aligned}$$

1) Dacă  $\alpha = -2$  atunci

$$B = \begin{pmatrix} 1 & 1 & -2 & 1 \\ 0 & -3 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix},$$

prin urmare sistemul este incompatibil.

2) Dacă  $\alpha \neq -2$  atunci sistemul este compatibil.

2.1) Dacă  $\alpha = 1$  atunci

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

sistemul este compatibil nedeterminat și este echivalent cu ecuația  $x_1 + x_2 + x_3 = 1$ , iar mulțimea soluțiilor sale este  $S = \{(1 - x_2 - x_3, x_2, x_3) \mid x_2, x_3 \in \mathbb{R}\}$ .

2.2) Dacă  $\alpha \in \mathbb{R} \setminus \{-2, 1\}$  atunci sistemul este compatibil determinat, echivalent cu sistemul

$$\begin{cases} x_1 + x_2 + \alpha x_3 = 1 \\ (\alpha - 1)x_2 + (1 - \alpha)x_3 = 0 \\ (1 - \alpha)(2 + \alpha)x_3 = 1 - \alpha \end{cases},$$

iar soluția sa este  $\left(\frac{1}{2+\alpha}, \frac{1}{2+\alpha}, \frac{1}{2+\alpha}\right)$ .

**Metoda II** (cu Teorema lui Rouché)

Determinantul matricii sistemului este  $\begin{vmatrix} \alpha & 1 & 1 \\ 1 & \alpha & 1 \\ 1 & 1 & \alpha \end{vmatrix}$ . Precizăm că dacă se calculează

acest determinant cu regula triunghiului sau cu regula lui Sarrus, se obține o expresie polinomială de gradul 3. Întrucât, pentru a realiza discuția, trebuie să rezolvăm ecuația algebrică rezultată din egalarea ei cu 0, acest polinom va trebui descompus în factori. Cu transformări elementare putem obține direct descompunerea acestui determinant

$$\begin{vmatrix} \alpha & 1 & 1 \\ 1 & \alpha & 1 \\ 1 & 1 & \alpha \end{vmatrix} = (\alpha + 2)(\alpha - 1)^2.$$

1) Dacă  $\alpha \in \mathbb{R} \setminus \{-2, 1\}$ , sistemul este compatibil determinat și soluția unică se obține cu formulele lui Cramer.

2) Dacă  $\alpha = 1$  atunci se observă că toate ecuațiile sunt echivalente cu ecuația

$$x_1 + x_2 + x_3 = 1,$$

care se rezolvă ca în metoda anterior prezentată.

3) Dacă  $\alpha = -2$ , minorul  $\begin{vmatrix} -2 & 1 \\ 1 & -2 \end{vmatrix}$  este principal, există un singur minor caracteristic

corespunzător  $\begin{vmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & 1 \end{vmatrix}$  care este nenul, deci sistemul e incompatibil.

## 4.5 Exerciții propuse

1) Fie  $\varphi \in \mathbb{R}$ . Să se arate că rotația în plan de unghi  $\varphi$ , adică funcția

$$f: \mathbb{R}^2 \rightarrow \mathbb{R}^2, f(x, y) = (x \cos \varphi - y \sin \varphi, x \sin \varphi + y \cos \varphi),$$

este automorfism al lui  $\mathbb{R}^2$ . Să se scrie matricea lui  $f$  în baza canonică a lui  $\mathbb{R}^2$  (adică în baza  $(e_1, e_2)$ , cu  $e_1 = (1, 0)$ ,  $e_2 = (0, 1)$ ).

2) Să se arate că funcțiile  $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2, f(x, y) = (x, -y)$  (simetria în raport cu axa  $Ox$ ) și  $g: \mathbb{R}^2 \rightarrow \mathbb{R}^2, f(x, y) = (-x, y)$  (simetria în raport cu axa  $Oy$ ) sunt automorfisme ale lui  $\mathbb{R}^2$ . Să se scrie matricele lui  $f, g, f - g, f + 2g$  și  $g \circ f$  în baza canonică.

3) Să se arate că fiecare dintre mulțimile de vectori  $\{v_1, v_2, v_3\}$  și  $\{v'_1, v'_2, v'_3\}$  cu

$$v_1 = (1, 2, 1), v_2 = (2, 3, 3), v_3 = (3, 7, 1) \text{ și } v'_1 = (3, 1, 4), v'_2 = (5, 2, 1), v'_3 = (1, 1, -6)$$

formează câte o bază a lui  $\mathbb{R}^3$  și să se găsească legătura dintre coordonatele unui vector scris în cele două baze.

4) Fie  $v = (v_1, v_2, v_3, v_4)$  o bază a  $\mathbb{R}$ -spațiului vectorial  $\mathbb{R}^4$ , vectorii

$$u_1 = v_1, u_2 = v_1 + v_2, u_3 = v_1 + v_2 + v_3, u_4 = v_1 + v_2 + v_3 + v_4$$



și  $f \in \text{End}_{\mathbb{R}}(\mathbb{R}^4)$  cu

$$[f]_v = \begin{pmatrix} 1 & 2 & 0 & 1 \\ 3 & 0 & -1 & 2 \\ 2 & 5 & 3 & 1 \\ 1 & 2 & 1 & 3 \end{pmatrix}.$$

Să se arate că  $u = (u_1, u_2, u_3, u_4)$  este o bază a lui  $\mathbb{R}^4$  și să se scrie matricea  $[f]_u$ .

5) Fie  $V$  un spațiu vectorial real,  $v = (v_1, v_2, v_3)$  o bază a spațiului  $V$ , vectorii

$$u_1 = v_1 + 2v_2 + v_3, \quad u_2 = v_1 + v_2 + 2v_3, \quad u_3 = v_1 + v_2$$

și  $f \in \text{End}_{\mathbb{R}}(V)$ . Să se arate că  $u = (u_1, u_2, u_3)$  este o bază a lui  $V$  și să se scrie matricea lui  $[f]_v$  știind că

$$[f]_u = \begin{pmatrix} 1 & 1 & 3 \\ 0 & 5 & -1 \\ 2 & 7 & -3 \end{pmatrix}.$$

6) Fie  $f \in \text{End}_{\mathbb{Q}}(\mathbb{Q}^4)$  pentru care matricea în baza canonică este

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ -1 & 2 & 1 & 0 \\ 3 & 0 & -1 & -2 \\ 5 & -3 & -1 & 1 \end{pmatrix}.$$

Să se determine câte o bază în  $\text{Ker } f$ ,  $\text{Im } f$ ,  $\text{Ker } f + \text{Im } f$  și  $\text{Ker } f \cap \text{Im } f$ .

7) Fie  $K = \mathbb{R}$ . Să se verifice egalitatea  $S_B = s + S_0$  din Teorema 4.12 în cazul sistemului de ecuații:

$$\begin{cases} 2x_1 + x_2 - x_3 - x_4 + x_5 = 1 \\ x_1 - x_2 + x_3 + x_4 - 2x_5 = 0 \\ 3x_1 + 3x_2 - 3x_3 - 3x_4 + 4x_5 = 2 \end{cases}$$

și să se determine o bază pentru spațiul soluțiilor sistemului liniar omogen asociat.

8) Să se discute după parametrii reali  $\alpha, \beta, \gamma, \lambda$  compatibilitatea sistemelor de mai jos, apoi să se rezolve:

$$a) \begin{cases} 5x_1 - 3x_2 + 2x_3 + 4x_4 = 3 \\ 4x_1 - 2x_2 + 3x_3 + 7x_4 = 1 \\ 8x_1 - 6x_2 - x_3 - 5x_4 = 9 \\ 7x_1 - 3x_2 + 7x_3 + 17x_4 = \alpha \end{cases} \quad (\text{în } \mathbb{R}^4), \quad b) \begin{cases} x_1 + x_2 + x_3 = 1 \\ \alpha x_1 + \beta x_2 + \gamma x_3 = \lambda \\ \alpha^2 x_1 + \beta^2 x_2 + \gamma^2 x_3 = \lambda^2 \end{cases} \quad (\text{în } \mathbb{R}^3).$$

## 5 Noțiuni de aritmetica numerelor întregi (de Simion Breaz și Cosmin Pelea)

### 5.1 Teorema împărțirii cu rest în $\mathbb{Z}$

Teorema împărțirii cu rest reprezintă un instrument de bază în studiul numerelor întregi.

**Teorema 5.1. (Teorema împărțirii cu rest în  $\mathbb{N}$ )** Oricare ar fi numerele naturale  $a$  și  $b$ , cu  $b \neq 0$ , există o singură pereche de numerele naturale  $(q, r) \in \mathbb{N} \times \mathbb{N}$ , astfel încât:

$$a = b \cdot q + r \quad \text{și} \quad r < b. \quad (1)$$

*Demonstrație.* Fie  $a, b \in \mathbb{N}$ , cu  $b \neq 0$ .

Demonstrăm existența numerelor  $q, r \in \mathbb{N}$ , astfel încât  $a = b \cdot q + r$  și  $r < b$ . Fie

$$\mathcal{S} = \{x \in \mathbb{N} \mid \exists y \in \mathbb{N} : a = by + x\} \subseteq \mathbb{N}$$

și observăm că  $\mathcal{S} \neq \emptyset$  pentru că  $a \in \mathcal{S}$  ( $a = b \cdot 0 + a$ ). Rezultă că există  $r \in \mathcal{S}$  cel mai mic element din  $\mathcal{S}$ . Cum  $r \in \mathcal{S}$ , deducem că există  $q \in \mathbb{N}$  cu proprietatea  $a = bq + r$ .

Presupunem că  $r \geq b$ . Atunci  $r - b \in \mathbb{N}$  și  $a = b(q + 1) + r - b$ , deci  $r - b \in \mathcal{S}$ . Din ipoteza  $b \neq 0$  deducem  $r - b < r$ , ceea ce contrazice alegerea lui  $r$ . Așadar  $r < b$  și perechea  $(r, b)$  satisface condiția (1).

Pentru demonstrația unicității, să presupunem că ar exista două perechi  $(q_1, r_1)$ ,  $(q_2, r_2)$  care satisfac (1) pentru aceleași numere  $a, b \in \mathbb{N}$ ,  $b \neq 0$ . Deci

$$a = b \cdot q_1 + r_1 = b \cdot q_2 + r_2 \text{ și } r_1 < b, r_2 < b.$$

Presupunem că  $q_1 < q_2$ . Rezultă că există  $x \in \mathbb{N}^*$ , astfel încât  $q_2 = q_1 + x$ . Obținem

$$bq_1 + r_1 = b(q_1 + x) + r_2 \Rightarrow bq_1 + r_1 = bq_1 + bx + r_2,$$

de unde, prin simplificare,  $r_1 = b \cdot x + r_2$ , ceea ce implică  $b \cdot x \leq r_1$ .

Dar din  $x \in \mathbb{N}^*$  deducem că  $1 \leq x$ , deci  $b \leq bx \leq r_1$ , contradicție.

Analog se arată că nu putem avea  $q_2 < q_1$ . Rezultă că  $q_1 = q_2$  și mai departe

$$b \cdot q_1 + r_1 = b \cdot q_1 + r_2,$$

de unde, prin simplificare,  $r_1 = r_2$  și demonstrația este încheiată.  $\square$

**Corolarul 5.2. (Teorema împărțirii cu rest în  $\mathbb{Z}$ )** Oricare ar fi numerele întregi  $a$  și  $b$ , cu  $b \neq 0$ , există și sunt unice numerele întregi  $q$  și  $r$ , astfel încât

$$a = b \cdot q + r \text{ și } 0 \leq r < |b|. \quad (2)$$

*Demonstrație.* Fie  $a, b \in \mathbb{Z}$ ,  $b \neq 0$ . Atunci  $|a|, |b| \in \mathbb{N}$ , cu  $|b| \neq 0$  și aplicăm teorema împărțirii cu rest în  $\mathbb{N}$ . Deducem că există numerele  $h, k \in \mathbb{N}$ , astfel încât

$$|a| = |b| \cdot h + k, \text{ unde } 0 \leq k < |b|.$$

Considerăm cazurile:

I.  $a \geq 0$  și  $b > 0$ . Atunci  $a = b \cdot h + k$ . Luăm  $q = h$  și  $r = k$ .

II.  $a \geq 0$  și  $b < 0$ . Atunci  $a = b \cdot (-h) + k$ . Luăm  $q = -h$  și  $r = k$ .

III.  $a < 0$  și  $b > 0$ . Considerăm aici subcazurile:

a)  $k = 0$ . Atunci  $-a = b \cdot h$ , adică  $a = b \cdot (-h)$ . Luăm  $q = -h$  și  $r = 0$ .

b)  $k \neq 0$ . Atunci

$$a = b \cdot (-h) + (-k) = -b - b \cdot h + b - k = -b \cdot (1 + h) + (b - k).$$

Luăm  $q = -(1 + h)$  și  $r = b - k < b$ , deci  $0 \leq r < |b|$ .

IV.  $a < 0$  și  $b < 0$ . Considerăm două subcazuri, ca în cazul anterior:

a)  $k = 0$ . Atunci  $-a = -b \cdot h$ , de unde  $a = b \cdot h$ . Luăm  $q = h$  și  $r = 0$ .

b)  $k \neq 0$ . Atunci  $-a = -b \cdot h + k$ , de unde

$$a = b \cdot h - k = b \cdot h + b - b - k = b \cdot (h + 1) + (-b - k).$$

Luăm  $q = h + 1$  și  $r = -b - k < -b$ , deci  $0 \leq r < |b|$ .

Pentru demonstrarea unicității, să presupunem că ar exista două perechi  $(q_1, r_1)$ ,  $(q_2, r_2)$  care satisfac condițiile (2) pentru aceleași numere  $a, b \in \mathbb{Z}$ ,  $b \neq 0$ . Deci

$$a = b \cdot q_1 + r_1 = b \cdot q_2 + r_2 \text{ și } 0 \leq r_1 < |b|, 0 \leq r_2 < |b|.$$

Rezultă că  $|r_2 - r_1| < |b|$  și  $b(q_1 - q_2) = r_2 - r_1$ .

Cum  $|q_1 - q_2| \in \mathbb{N}$ ,  $|q_1 - q_2| \geq 1$  ar implica

$$|b| \leq |b||q_1 - q_2| = |r_2 - r_1| < |b|,$$

contradicție. Deducem că  $|q_1 - q_2| = 0$ , deci  $q_1 = q_2$ . Atunci

$$b \cdot q_1 + r_1 = b \cdot q_1 + r_2,$$

de unde, prin simplificare,  $r_1 = r_2$  și demonstrația este încheiată. □

Dacă  $a$ ,  $b$ ,  $q$  și  $r$  sunt ca în Corolarul 5.2, vom spune că numărul  $q$  este **câtul împărțirii** lui  $a$  la  $b$ , iar  $r$  este **restul împărțirii** lui  $a$  la  $b$ . În acest context se mai folosește terminologia **deîmpărțit** pentru  $a$ , respectiv **împărțitor** pentru  $b$ .

**Exemplul 5.3.** Prezentăm câteva exemple concrete:

- i)  $a = 7$ ,  $b = 3 \Rightarrow q = 2$  și  $r = 1$ ;
- ii)  $a = -7$ ,  $b = 3 \Rightarrow q = -3$  și  $r = 2$ ;
- iii)  $a = 7$ ,  $b = -3 \Rightarrow q = -2$  și  $r = 1$ ;
- iv)  $a = -7$ ,  $b = -3 \Rightarrow q = 3$  și  $r = 2$ ;
- v)  $a = -6$ ,  $b = 3 \Rightarrow q = -2$  și  $r = 0$ .

**Observația 5.4.** În practică identitatea dată de teorema împărțirii cu rest este uneori înlocuită cu

$$a = bk + s, \quad -|b|/2 < s \leq |b|/2.$$

De exemplu, dacă împărțim la 3, putem scrie  $a = 3q + r$ ,  $r \in \{0, 1, 2\}$  sau  $a = 3k + s$  cu  $s \in \{0, \pm 1\}$ . A doua variantă este utilă dacă trebuie să-l ridicăm pe  $a$  la o putere pară, pentru că deducem imediat  $a^{2m} = \mathcal{M}_3 + t$ ,  $t \in \{0, 1\}$ , i.e. orice pătrat perfect dă prin împărțire la 3 restul 0 sau 1 ( $\mathcal{M}_3$  notează faptul că numărul pe care l-am înlocuit cu acest simbol dă restul 0 prin împărțire la 3, adică este un multiplu al lui 3).

## 5.2 Exerciții rezolvate

1) Să se arate că restul împărțirii unui pătrat perfect impar la 8 este 1.

*Soluție:* Fie  $a = b^2$  cu  $b$  impar. Atunci  $b = 4k + s$  cu  $s = \pm 1$ , deci

$$a = 16k^2 \pm 8k + 1 = \mathcal{M}_8 + 1.$$

2) Să se găsească resturile împărțirii lui  $5^{n^2}$  la 8.

*Soluție:* Prezentăm două variante:

(I) Considerăm două cazuri: (a)  $n$  este par și (b)  $n$  este impar.

(a) Dacă  $n = 2k$ , atunci  $5^{n^2} = 5^{4k^2} = 25^{2k^2} = (\mathcal{M}_8 + 1)^{2k^2} = \mathcal{M}_8 + 1$ .

(b) Dacă  $n = 2k + 1$ , atunci

$$5^{n^2} = 5^{4k^2+4k+1} = 5^{4k^2}5^{4k}5 = (\mathcal{M}_8 + 1)(\mathcal{M}_8 + 1)5 = \mathcal{M}_8 + 5.$$

Așadar resturile posibile sunt 1 sau 5.

(II) Putem folosi exercițiul precedent pentru a trata cazurile de mai sus astfel:

(a) Dacă  $n^2 = 2k$ , atunci  $5^{n^2} = 5^{2k} = (\mathcal{M}_8 + 1)^k = \mathcal{M}_8 + 1$ .

(b) Dacă  $n^2 = 2k + 1$ , atunci  $5^{n^2} = 5^{2k+1} = (\mathcal{M}_8 + 1)^k \cdot 5 = \mathcal{M}_8 + 5$ .

### 5.3 Divizibilitatea în $\mathbb{Z}$

**Definiția 5.5.** Fie  $a, b \in \mathbb{Z}$ . Spunem că  $a$  **divide pe**  $b$  și notăm  $a \mid b$  sau  $b : a$  dacă există un număr întreg  $q$ , astfel încât  $b = a \cdot q$ . Aceasta definește o relația binară omogenă pe  $\mathbb{Z}$  care se numește **relația de divizibilitate** pe  $\mathbb{Z}$ . Dacă  $a \mid b$ , mai spunem că  $a$  **este divizor pentru**  $b$  sau  $a$  **este factor al lui**  $b$  sau  $b$  **este multiplu pentru**  $a$  sau  $b$  **factorizează prin**  $a$ .

**Observația 5.6.** Dacă  $a \neq 0$ , următoarele afirmații sunt echivalente:

a)  $a \mid b$ ;

b)  $b$  este multiplu pentru  $a$ , fapt notat prin  $b = \mathcal{M}_a$ ;

c) restul împărțirii lui  $b$  la  $a$  este 0.

**Exemplul 5.7.** Din  $6 = 2 \cdot 3$  rezultă că  $2 \mid 6$ , iar din  $7 = 2 \cdot 3 + 1$  rezultă că  $2 \nmid 7$ .

Următoarea teoremă prezintă câteva proprietăți elementare ale relației de divizibilitate.

#### **Teorema 5.8. (Proprietăți ale relației de divizibilitate)**

Fie  $a, b, c \in \mathbb{Z}$ . Sunt adevărate afirmațiile:

(i)  $\pm 1 \mid a$ ,  $\pm a \mid a$ ,  $a \mid 0$ ;

(ii) dacă  $a \mid b$  și  $b \mid c$ , atunci  $a \mid c$ ;

(iii) dacă  $a \mid b$  și  $b \mid a$ , atunci  $a = \pm b$ ;

(iv) dacă  $a \mid b$  și  $a \mid c$ , atunci  $a \mid (b + c)$ ;

(v) dacă  $a \mid b$ , atunci  $a \mid bc$ ;

(vi) dacă  $a \mid b + c$  și  $a \mid b$ , atunci  $a \mid c$ ;

(vii) dacă  $a \mid b$  și  $b \neq 0$ , atunci  $|a| \leq |b|$ .

*Demonstrație.* (i) Fie  $a \in \mathbb{Z}$ . Atunci

$$a = 1 \cdot a, \text{ respectiv } a = (-1) \cdot (-a), a = a \cdot 1 \text{ și } a = (-a) \cdot (-1),$$

unde  $a, -a, 1, -1 \in \mathbb{Z}$ , iar  $a \mid 0$  deoarece  $0 = a \cdot 0$ , unde  $0 \in \mathbb{Z}$ .

(ii) Din ipoteze obținem

$$a \mid b \Rightarrow \exists q_1 \in \mathbb{Z}, b = a \cdot q_1;$$

$$b \mid c \Rightarrow \exists q_2 \in \mathbb{Z}, c = b \cdot q_2.$$

Atunci,

$$c = b \cdot q_2 = (a \cdot q_1) \cdot q_2 = a \cdot (q_1 \cdot q_2), \text{ cu } q_1 \cdot q_2 \in \mathbb{Z}.$$

Deci,  $a \mid c$ .

(iii) Din ipoteze obținem

$$a \mid b \Rightarrow \exists q_1 \in \mathbb{Z}, b = a \cdot q_1;$$

$$b \mid a \Rightarrow \exists q_2 \in \mathbb{Z}, a = b \cdot q_2.$$

Atunci,

$$a = b \cdot q_2 = (a \cdot q_1) \cdot q_2 = a \cdot (q_1 \cdot q_2) \Rightarrow q_1 \cdot q_2 = 1.$$

Prin urmare,  $q_1, q_2 \in \mathbb{Z}$  sunt inversabile, așadar  $q_1 \in \{-1, 1\}$  și  $a = \pm b$ .

Lăsăm cititorului demonstrarea celorlalte proprietăți ca exercițiu.  $\square$

Fie  $a \in \mathbb{Z}$ . Numim **divizori banali** (**divizori improprii**) ai lui  $a$  numerele  $\pm 1$  și  $\pm a$ . Un divizor al lui  $a$  diferit de  $\pm 1$  și de  $\pm a$  se numește **divizor propriu** al lui  $a$ .

**Observațiile 5.9.** a) Relația de divizibilitate pe  $\mathbb{Z}$  este o relație de preordine pe  $\mathbb{Z}$ .  
b) Relația de divizibilitate pe  $\mathbb{Z}$  nu este o relație de ordine, deoarece ea nu este antisimetrică, după cum arată următorul exemplu:

$$2, -2 \in \mathbb{Z}, 2 \mid (-2) \text{ și } (-2) \mid 2, \text{ dar } 2 \neq -2.$$

c) Restricția la  $\mathbb{N}$  a relației de divizibilitate din  $\mathbb{Z}$  este o relație de ordine deoarece reflexivitatea și tranzitivitatea se păstrează, iar dacă  $a, b \in \mathbb{N}$  cu  $a \mid b$  și  $b \mid a$ , atunci  $a = b$ .

Fie  $a, b \in \mathbb{Z}$ . Spunem că un număr  $d \in \mathbb{Z}$  este un **divizor comun** al numerelor  $a$  și  $b$  dacă  $d \mid a$  și  $d \mid b$ .

**Exemplele 5.10.** 1) Numărul 1 este divizor comun al numerelor  $a$  și  $b$  pentru orice  $a, b \in \mathbb{Z}$ .

2) Numărul 3 este divizor comun al numerelor 6 și  $-9$ .

Dacă  $d$  este divizor comun pentru numerele  $a, b \in \mathbb{Z}^*$ , atunci  $|d| \leq \min\{|a|, |b|\}$ .  
Rezultă că există un cel mai mare element în mulțimea divizorilor comuni ai numerelor  $a$  și  $b$ . Acest număr se numește **cel mai mare divizor comun al numerelor  $a$  și  $b$**  și se notează cu  $d = (a, b)$  sau  $d = \text{c.m.m.d.c.}(a, b)$ .

**Observațiile 5.11.** 1) Cum 1 este întotdeauna divizor comun, deducem că  $(a, b) \in \mathbb{N}^*$  pentru orice  $a, b \in \mathbb{Z}$ .

2) Dacă exact unul din numerele  $a$  și  $b$  este 0, atunci definiția celui mai mare divizor comun poate fi extinsă pentru această situație.

3) Dacă  $a = b = 0$ , atunci nu există cel mai mare divizor comun al numerelor  $a$  și  $b$ .

$$4) (a, b) = d \Leftrightarrow \begin{cases} d \in \mathbb{N}^*, \\ d \mid a \text{ și } d \mid b, \\ c \in \mathbb{N}, c \mid a \text{ și } c \mid b \Rightarrow c \leq d \end{cases}$$

Următorul rezultat este foarte util în practică și ne spune că cel mai mare divizor comun a două numere întregi poate fi obținut ca o combinație liniară a acestora.

**Teorema 5.12. (reprezentarea Bézout a c.m.m.d.c.)**

Dacă  $a, b \in \mathbb{Z}^*$  și  $d = (a, b)$ , atunci există  $u, v \in \mathbb{Z}$  astfel încât

$$d = au + bv.$$

*Demonstrație.* Fie  $S = \{ax + by \mid ax + by > 0, x, y \in \mathbb{Z}\} \subseteq \mathbb{N}^*$ . Constatăm că  $S \neq \emptyset$  pentru că  $a = a \cdot 1 + b \cdot 0$  și  $-a = a \cdot (-1) + b \cdot 0$ , prin urmare sau  $a \in S$  sau  $-a \in S$ . Deci există  $d$  cel mai mic element din  $S$ . Fie  $u, v \in \mathbb{Z}$  astfel încât  $d = au + bv$ .

Vom demonstra că  $d \mid a$ . Pentru aceasta aplicăm teorema împărțirii cu rest și scriem  $a = dq + r$ ,  $0 \leq r < d$ . Rezultă că

$$r = a - dq = a - (au + bv)q = a(1 - uq) + b(-vq).$$

Din  $r < d$  rezultă  $r \notin S$ . Dar  $1 - uq, -vq \in \mathbb{Z}$ , deci  $r \leq 0$  și rezultă  $r = 0$ . Așadar  $d \mid a$ . Analog se arată că  $d \mid b$ .

Fie  $c \in \mathbb{N}$  cu  $c \mid a$  și  $c \mid b$ . Rezultă că  $c \mid au + bv = d$ , și de aici găsim  $c \leq |d| = d$ . Așadar  $d = (a, b)$ .  $\square$

Dacă scriem  $(a, b) = au + bv$ ,  $u, v \in \mathbb{Z}$ , atunci spunem că am ales o **reprezentare Bézout** pentru  $(a, b)$ . Atragem atenția că această reprezentare nu este unică.

**Exemplul 5.13.** De exemplu,  $(2, 3) = 1 = 2 \cdot 2 + 3 \cdot (-1) = 2 \cdot (-4) + 3 \cdot 3$ .

**Corolarul 5.14.** Fie  $a, b \in \mathbb{Z}^*$  și  $d \in \mathbb{N}^*$ . Atunci

$$(a, b) = d \Leftrightarrow \begin{cases} d \mid a \text{ și } d \mid b, \\ c \in \mathbb{Z}, c \mid a \text{ și } c \mid b \Rightarrow c \mid d \end{cases}$$

**Observația 5.15.** Această caracterizare este folosită ca definiție pentru c.m.m.d.c. în diverse tipuri de inele unde nu avem definită o relație de ordine „naturală” (de exemplu în  $\mathbb{Q}[X]$ ). În acest context, c.m.m.d.c. este de fapt o clasă de echivalență. Pentru cazul inelului  $\mathbb{Z}$ , c.m.m.d.c este de fapt mulțimea  $\{-d, d\}$ , unde  $d = (a, b)$ .

Un caz special în studiul divizibilității îl ocupă perechile de numere care nu au divizori comuni proprii. Spunem că  $a, b \in \mathbb{Z}$  sunt **relativ prime** (sau **prime între ele**) dacă  $(a, b) = 1$ . Aceste perechi pot fi caracterizate cu ajutorul reprezentărilor Bézout.

**Corolarul 5.16.** Numerele întregi  $a$  și  $b$  sunt relativ prime dacă și numai dacă există  $u, v \in \mathbb{Z}$  astfel încât  $au + bv = 1$ .

*Demonstrație.* ( $\Rightarrow$ ) Această implicație rezultă din Teorema 5.12.

( $\Leftarrow$ ) Fie  $d = (a, b)$ . Din  $d \mid a$  și  $d \mid b$  rezultă că  $d \mid au + bv = 1$ , deci  $d = 1$ .  $\square$

**Corolarul 5.17.** Dacă  $a, b \in \mathbb{Z}^*$  și  $d = (a, b)$ , atunci  $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ .

*Demonstrație.* Din  $d = (a, b)$  rezultă că există  $u, v \in \mathbb{Z}$  astfel încât  $d = au + bv$ . Atunci  $1 = \frac{a}{d}u + \frac{b}{d}v$ , deci  $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ .  $\square$

Folosim considerațiile făcute până acum ca să demonstrăm proprietăți importante ale relației de divizibilitate.

**Teorema 5.18.** Fie  $a, b, c \in \mathbb{Z}$ . Sunt adevărate afirmațiile:

- (i) dacă  $a \mid b$ ,  $b \mid c$  și  $(a, b) = 1$ , atunci  $ab \mid c$ ;
- (ii) (**Lema lui Euclid**) dacă  $a \mid bc$  și  $(a, b) = 1$ , atunci  $a \mid c$ .

*Demonstrație.* (i) Fie  $r, s \in \mathbb{Z}$  astfel încât  $c = ar = bs$  și  $u, v \in \mathbb{Z}$  cu  $au + bv = 1$ . Atunci

$$c = c \cdot 1 = c(au + bv) = bsau + arbv = ab(su + rv).$$

Cum  $su + rv \in \mathbb{Z}$ , deducem că  $ab \mid c$ .

(ii) Fie  $u, v, k \in \mathbb{Z}$  astfel încât  $au + bv = 1$  și  $bc = ka$ . Calculăm

$$c = c \cdot 1 = c(au + bv) = acu + bcv = acu + kav = a(cu + kv),$$

deci  $a \mid c$ . □

În continuare, vom demonstra o teoremă care furnizează un procedeu de aflare a celui mai mare divizor comun, numit **algoritmul lui Euclid**, și o metodă de a determina o reprezentare Bézout. Observăm că  $(a, b) = (-a, b) = (-a, -b)$ , deci este suficient să considerăm cazul numerelor naturale.

**Teorema 5.19. (Algoritmul lui Euclid)**

Fie  $a, b \in \mathbb{N}^*$ , cu  $b \neq 0$  și  $b \leq a$ . Considerăm identitățile următoarelor împărțiri:

$$\begin{array}{lll} a = b \cdot q_0 + r_0, & \text{unde } r_0 < b; \text{ fie } r_0 \neq 0; & (E_1) \\ b = r_0 \cdot q_1 + r_1, & \text{unde } r_1 < r_0; \text{ fie } r_1 \neq 0; & (E_2) \\ r_0 = r_1 \cdot q_2 + r_2, & \text{unde } r_2 < r_1; \text{ fie } r_2 \neq 0; & (E_3) \\ & \dots & \dots \\ r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1}, & \text{unde } r_{n-1} < r_{n-2}; \text{ fie } r_{n-1} \neq 0; & (E_n) \\ r_{n-2} = r_{n-1} \cdot q_n + r_n, & \text{unde } r_n < r_{n-1}; \text{ fie } r_n \neq 0; & (E_{n-1}) \\ r_{n-1} = r_n \cdot q_{n+1} + r_{n+1}, & \text{unde } r_{n+1} = 0. & (E_{n+2}) \end{array}$$

Atunci cel mai mare divizor comun al numerelor  $a$  și  $b$  este ultimul rest diferit de zero al acestor împărțiri, adică:

$$(a, b) = r_n.$$

*Demonstrație.* Observăm că șirul resturilor diferite de zero este un șir strict descrescător

$$r_0 > r_1 > r_2 > \dots$$

de numere naturale, deci acest șir este finit, adică, după un număr finit de împărțiri obținem restul zero.

Demonstrăm că  $r_n \mid a$  și  $r_n \mid b$  folosind inducția completă pentru propoziția

$$P(i) : r_n \mid r_{n-i}, \text{ unde } 0 \leq i \leq n.$$

Propoziția  $P(0)$  este, evident, adevărată. Din pasul  $(E_{n+2})$  deducem că  $r_n \mid r_{n-1}$ . Presupunem că  $r_n \mid r_{n-j}$  pentru orice  $1 \leq j \leq i$  și demonstrăm că  $r_n \mid r_{n-(i+1)}$ .

Pentru aceasta folosim relația  $r_{n-(i+1)} = r_{n-i} \cdot q_{n-(i-1)} + r_{n-(i-1)}$ , de unde concluzia este evidentă.

Deci  $r_n$  divide pe  $r_0$  și pe  $r_1$ , iar din egalitatea găsită în pasul  $(E_2)$  deducem  $r_n \mid b$ . Apoi folosim  $(E_1)$  ca să deducem și  $r_n \mid a$ .

Fie  $c \in \mathbb{N}$ , astfel încât  $c \mid a$  și  $c \mid b$ . Vom arăta că  $c \mid r_n$ . Folosind din nou identitățile din enunț, avem:

$$c \mid a = b \cdot q_0 + r_0 \text{ și } c \mid (b \cdot q_0) \Rightarrow c \mid r_0.$$

Apoi obținem:

$$c \mid b = r_0 \cdot q_1 + r_1 \text{ și } c \mid (r_0 \cdot q_1) \Rightarrow c \mid r_1,$$

și continuăm raționamentul, parcurgând identitățile împărțirilor de la prima spre ultima.

În final găsim

$$c \mid r_{n-2} = r_{n-1} \cdot q_n + r_n \text{ și } c \mid (r_{n-1} \cdot q_n),$$

deci  $c \mid r_n$ .

În concluzie,  $r_n = (a, b)$ . □

**Observația 5.20.** Plecând de la identitățile  $(E_1)$ – $(E_n)$  putem găsi o reprezentare Bézout astfel: înlocuim succesiv resturile, plecând de la  $(E_n)$  către  $(E_1)$

$$r_n = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) = -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2} = \dots,$$

iar în final obținem pe  $r_n$  sub forma  $r_n = au + bv$ .

Procedeu dat de algoritmul lui Euclid poate fi folosit în demonstrarea unor proprietăți ale c.m.m.d.c.

**Corolarul 5.21.** Pentru orice  $a, b, k \in \mathbb{N}^*$ , avem:

$$(a \cdot k, b \cdot k) = (a, b) \cdot k.$$

*Demonstrație.* Scriem algoritmul lui Euclid pentru calculul lui  $d = (a, b)$ . Dacă înmulțim liniile  $(E_1)$ – $(E_n)$  cu  $k$  se constată ușor că noile egalități reprezintă chiar algoritmul lui Euclid aplicat numerelor  $ka$  și  $kb$ . Deci  $kr_n = (ka, kb)$ . □

Fie  $a, b \in \mathbb{Z}$ . Spunem că un număr  $m \in \mathbb{Z}$  este un **multiplu comun** al numerelor  $a$  și  $b$  dacă  $a \mid m$  și  $b \mid m$ .

**Exemplele 5.22.** 1) Pentru orice  $a, b \in \mathbb{Z}$ , numărul  $a \cdot b$  este multiplu comun al numerelor  $a$  și  $b$ .

2) Numărul 6 este multiplu comun al numerelor 2 și  $-3$ .

Dacă  $m$  este multiplu comun pentru numerele  $a, b \in \mathbb{Z}^*$ , atunci  $|m| \geq \max\{|a|, |b|\}$ . Rezultă că există un cel mai mic element în mulțimea multiplilor comuni strict pozitivi ai numerelor  $a$  și  $b$ . Acest număr se numește **cel mai mic multiplu comun al numerelor  $a$  și  $b$**  și se notează cu  $m = [a, b] = \text{c.m.m.m.c.}(a, b)$ .

**Observația 5.23.** Ca pentru cel mai mare divizor comun, observăm că

$$[a, b] = m \Leftrightarrow \begin{cases} m \in \mathbb{N}^*, \\ a \mid m \text{ și } b \mid m, \\ c \in \mathbb{N}^*, a \mid c \text{ și } b \mid c \Rightarrow m \leq c. \end{cases}$$



**Teorema 5.24.** Oricare ar fi  $a, b \in \mathbb{N}^*$ , are loc egalitatea:

$$ab = (a, b)[a, b].$$

*Demonstrație.* Fie  $d = (a, b)$ . Atunci există  $r, s \in \mathbb{N}^*$  astfel încât  $a = dr$ ,  $b = ds$  și  $(r, s) = 1$ . Notăm  $m = drs = as = br$ , deci  $m$  este multiplu comun al numerelor  $a$  și  $b$ .

Dacă  $c \in \mathbb{N}^*$  este un multiplu comun pentru  $a$  și  $b$ , atunci există  $x, y \in \mathbb{N}^*$  cu  $c = ax = by$ . Alegem o reprezentare Bézout  $1 = ru + sv$  a lui 1 ( $u, v \in \mathbb{Z}$ ). Calculăm

$$c = c \cdot 1 = c(ru + sv) = byru + axsv = m(yu + xv),$$

deci  $m \mid c$ . Din  $m, c \in \mathbb{N}^*$  rezultă că  $m \leq c$ . □

Din demonstrația de mai sus se deduce imediat:

**Corolarul 5.25.** Fie  $a, b \in \mathbb{Z}^*$  și  $m \in \mathbb{N}^*$ . Atunci

$$m = [a, b] \Leftrightarrow \begin{cases} a \mid m \text{ și } b \mid m, \\ c \in \mathbb{Z}, a \mid c \text{ și } b \mid c \Rightarrow m \mid c. \end{cases}$$

Din formula dată în teoremă rezultă și

**Corolarul 5.26.** Dacă  $(a, b) = 1$ , atunci  $ab = [a, b]$ .

**Observația 5.27.** Definițiile celui mai mare divizor comun și celui mai mic multiplu comun pot fi extinse la o mulțime finită de numere întregi. Fie  $a_1, \dots, a_n$  numere întregi nenule. Atunci  $d \in \mathbb{N}^*$  este **cel mai mare divizor comun al acestor numere** dacă

$$\begin{cases} d \mid a_1, \dots, d \mid a_n, \\ c \mid a_1, \dots, c \mid a_n \Rightarrow c \leq d. \end{cases}$$

În aceste condiții notăm  $d = (a_1, \dots, a_n) = \text{c.m.m.d.c.}(a_1, \dots, a_n)$ .

Numărul  $m \in \mathbb{N}^*$  este **cel mai mic multiplu comun al acestor numere** dacă

$$\begin{cases} a_1 \mid m, \dots, a_n \mid m, \\ a_1 \mid c, \dots, a_n \mid c \Rightarrow m \leq c. \end{cases}$$

În aceste condiții notăm  $m = [a_1, \dots, a_n] = \text{c.m.m.m.c.}(a_1, \dots, a_n)$ .

Se constată imediat că

$$(a_1, \dots, a_n, a_{n+1}) = ((a_1, \dots, a_n), a_{n+1}) \text{ și } [a_1, \dots, a_n, a_{n+1}] = [[a_1, \dots, a_n], a_{n+1}].$$

## 5.4 Exerciții rezolvate

- 1) Fie  $a \in \mathbb{N}$ ,  $a = \overline{a_n a_{n-1} \dots a_2 a_1 a_0}$ ,  $a_i \in \{0, \dots, 9\}$ ,  $i = 1, \dots, n$ ,  $a_n \neq 0$ . Arătați că:
  - (i)  $2 \mid a \Leftrightarrow 2 \mid a_0$ ;
  - (ii) pentru  $k \in \mathbb{N}^*$  avem  $2^k \mid a \Leftrightarrow 2 \mid \overline{a_{k-1} \dots a_0}$ ;
  - (iii)  $3 \mid a \Leftrightarrow 3 \mid a_n + \dots + a_0$ ;
  - (iv)  $27 \mid a \Leftrightarrow 27 \mid \overline{a_2 a_1 a_0} + \overline{a_5 a_4 a_3} + \dots$ .

*Soluție:* (i) Scriem

$$a = 10 \cdot (a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \dots + a_2 \cdot 10 + a_1) + r_0 = \mathcal{M}_2 + a_0.$$

Deci

$$2|a \Leftrightarrow 2|\mathcal{M}_2 + a_0 \Leftrightarrow 2|a_0.$$

(ii) Analog, scriem numărul  $a$  sub forma:

$$a = 10^k \cdot (a_n \cdot 10^{n-k} + a_{n-1} \cdot 10^{n-k-1} + \dots + a_k) + (a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0),$$

adică

$$a = \mathcal{M}_{2^k} + \overline{a_{k-1} \dots a_1 a_0}.$$

Deci

$$2^k | a \Leftrightarrow 2^k | \mathcal{M}_{2^k} + \overline{a_{k-1} \dots a_1 a_0} \Leftrightarrow 2^k | \overline{a_{k-1} \dots a_1 a_0}.$$

(iii) Observăm că dacă  $k \in \mathbb{N}^*$ , atunci  $10^k = (\mathcal{M}_3 + 1)^k = \mathcal{M}_3 + 1$ . Obținem

$$a = a_n \cdot (\mathcal{M}_3 + 1) + \dots + a_2 \cdot (\mathcal{M}_3 + 1) + a_1 \cdot (\mathcal{M}_3 + 1) + a_0 = \mathcal{M}_3 + (a_n + \dots + a_2 + a_1 + a_0).$$

Deci

$$3|a \Leftrightarrow 3|(a_n + a_{n-1} + \dots + a_2 + a_1 + a_0).$$

(iv) Constatăm că  $27 \cdot 37 = 999 = 1000 - 1$ . Scriem pe  $a$  astfel

$$10^3 \overline{a_n \dots a_4 a_3} + \overline{a_2 a_1 a_0} = (\mathcal{M}_{27} + 1) \overline{a_n \dots a_4 a_3} + \overline{a_2 a_1 a_0} = \mathcal{M}_{27} + \overline{a_n \dots a_4 a_3} + \overline{a_2 a_1 a_0}.$$

Repetând procedeul se obține

$$a = \mathcal{M}_{27} + \overline{a_2 a_1 a_0} + \overline{a_5 a_4 a_3} + \dots,$$

de unde se deduce criteriul enunțat.

2) Fie  $a, b \in \mathbb{Z}$ ,  $d = (a, b)$  și  $T = \{ax + by \mid x, y \in \mathbb{Z}\}$ . Să se arate că  $T = d\mathbb{Z}$ .

*Soluție:* Reamintim că  $d\mathbb{Z} = \{dk \mid k \in \mathbb{Z}\}$  și demonstrăm egalitatea prin dublă incluziune.

Fie  $z \in T$ . Atunci există  $x, y \in \mathbb{Z}$  astfel încât  $z = ax + by$ . Din  $d \mid a$  și  $d \mid b$  deducem  $d \mid ax + by = z$ , deci  $z \in d\mathbb{Z}$ . Așadar  $T \subseteq d\mathbb{Z}$  (elementul  $z$  a fost ales arbitrar).

Reciproc, dacă  $z \in d\mathbb{Z}$ , atunci există  $k \in \mathbb{Z}$  cu  $z = dk$ . Fie  $u, v \in \mathbb{Z}$  cu  $d = au + bv$ . Atunci  $z = auk + bvk \in T$ . Așadar  $d\mathbb{Z} \subseteq T$  și soluția este încheiată.

3) Pentru  $n \in \mathbb{N}^*$ , numerele  $M_n = 2^n - 1$  se numesc **numere Mersenne**. Să se arate că dacă  $b \mid a$ , atunci  $M_b \mid M_a$  și că

$$(M_m, M_n) = M_{(m,n)}, \quad \forall m, n \in \mathbb{N}^*.$$

*Soluție:* Pentru început să considerăm o identitate de tipul  $a = bq + r$ , unde  $a, b, q, r \in \mathbb{N}$  cu  $a$  și  $b$  nenule. Atunci

$$M_a = 2^{bq+r} - 1 = 2^{bq}2^r - 2^r + 2^r - 1 = 2^r((2^b)^q - 1) + M_r = M_b Q + M_r,$$

unde pentru ultima egalitate am folosit identitatea

$$x^k - y^k = (x - y)(x^{k-1} + x^{k-2}y + \dots + y^{k-1}).$$

Mai mult, dacă  $0 \leq r < b$ , atunci  $M_r = 2^r - 1 < 2^b - 1 = M_b$ , aşadar  $M_r$  este restul împărţirii lui  $M_a$  la  $M_b$ . De aici rezultă imediat că

$$b \mid a \Rightarrow M_b \mid M_a.$$

Să scriem algoritmi pentru calculul numerelor  $(m, n)$  şi  $(M_m, M_n)$  în paralel:

$$m = n \cdot q_0 + r_0, \quad M_m = M_n \cdot Q_0 + M_{r_0} \quad (E_1)$$

$$n = r_0 \cdot q_1 + r_1, \quad M_n = M_{r_0} \cdot Q_1 + M_{r_1} \quad (E_2)$$

$$r_0 = r_1 \cdot q_2 + r_2, \quad M_{r_0} = M_{r_1} \cdot Q_2 + M_{r_2} \quad (E_3)$$

$$\dots\dots \quad \dots\dots$$

$$r_{k-2} = r_{k-1} \cdot q_k + r_k, \quad M_{r_{k-2}} = M_{r_{k-1}} \cdot Q_k + M_{r_k} \quad (E_{k+1})$$

$$r_{k-1} = r_k \cdot q_{k+1} + r_{k+1}, \quad M_{r_{k-1}} = M_{r_k} \cdot Q_{k+1} + M_{r_{k+1}}, \quad (E_{k+2})$$

unde  $0 = r_{k+1} < r_k < \dots r_1 < n \leq m$  şi  $0 = M_{r_{k+1}} < M_{r_k} < \dots M_{r_1} < M_n \leq M_m$ . Se deduce că  $r_k = (m, n)$  şi  $M_{r_k} = (M_m, M_n)$ .

## 5.5 Numere prime. Teorema fundamentală a aritmeticii

Dacă  $n \in \mathbb{Z}$ , atunci spunem că divizorii  $\pm 1$  şi  $\pm n$  ai lui  $n$  sunt **divizori improprii** (sau **banali**). Spunem că  $n \neq 0$  este un **număr compus** dacă el are şi alţi divizori în afară de cei banali. Un număr  $p$  este **ireductibil** dacă  $p \neq \pm 1$  şi el nu este compus.

**Exemplul 5.28.** Numărul  $6 = 2 \cdot 3$  este compus, iar numerele  $\pm 1$  nu sunt compuse.

Spunem că  $p \in \mathbb{Z}$  este un **număr prim** dacă sunt îndeplinite condiţiile:

$$\begin{cases} p \neq \pm 1, \\ p \mid ab \Rightarrow p \mid a \text{ sau } p \mid b. \end{cases}$$

**Observaţia 5.29.** Să observăm că în limbajul obişnuit legat de studiul numerelor naturale în loc de „număr ireductibil” de foloseşte „număr prim”. Aceasta se bazează pe faptul că cele două noţiuni sunt echivalente în  $\mathbb{Z}$ , conform Teoremei 5.30. Totuşi există inele (care sunt folosite în studiul numerelor întregi) unde cele două noţiuni nu sunt identice. De exemplu se poate demonstra că dacă lucrăm în inelul  $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$  cu operaţiile obişnuite, atunci 2 este ireductibil, dar  $2 \mid 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$  şi  $2 \nmid 1 \pm i\sqrt{5}$ .

**Teorema 5.30.** Un număr întreg este prim dacă şi numai dacă el este ireductibil.

*Demonstraţie.* Presupunem că există un număr prim  $p$  care nu este ireductibil. Rezultă că există  $a, b \in \mathbb{Z} \setminus \{\pm 1, \pm p\}$  astfel încât  $p = ab$ .

Din faptul că  $p$  este prim şi  $p \mid ab$  deducem  $p \mid a$  sau  $p \mid b$ . Dacă  $p \mid a$ , din  $p = ab$  rezultă şi  $a \mid p$ , deci  $a = \pm p$ , contradicţie. Analog se obţine o contradicţie dacă  $p \mid b$ . Aşadar presupunerea iniţială este falsă, deci **orice număr prim este ireductibil**.

Reciproc, fie  $p$  un număr ireductibil și  $a, b \in \mathbb{Z}$  astfel încât  $p \mid ab$ . Să observăm că nu restrângem generalitatea dacă presupunem  $a \in \mathbb{N}$  și  $p \nmid a$  (putem să înmulțim ambii factori cu  $-1$ ).

Dacă  $d = (a, p)$ , atunci  $d \in \{1, p\}$ . Din  $p \nmid a$  rezultă  $d \neq p$ , deci  $(a, p) = 1$ . Aceasta împreună cu  $p \mid ab$  și Teorema 5.18 (ii) implică  $p \mid b$ . Dar  $p \neq \pm 1$  pentru că este ireductibil, deci  $p$  este un număr prim.  $\square$

**Observațiile 5.31.** a) Din definiția numerelor prime rezultă imediat că un număr  $p$  este prim dacă și numai dacă  $-p$  este prim. Așadar, din punctul de vedere al relației de divizibilitate, este suficient să lucrăm cu numere prime pozitive.

b) Proprietatea din definiția numerelor prime poate fi extinsă la produse cu un număr arbitrar de factori. Deci, dacă  $p$  este prim și  $p \mid a_1 \cdot \dots \cdot a_n$ , atunci există  $i \in \{1, \dots, n\}$  astfel încât  $p \mid a_i$ .

**Exemplul 5.32.** Numerele 2, 3, 5, 7, 11, 13, 17 sunt prime.

Rolul fundamental al numerelor prime în studiul divizibilității este evidențiat de următoarea teoremă.

**Teorema 5.33. (Teorema fundamentală a aritmeticii)**

Orice număr natural  $n \geq 2$  se descompune într-un produs de factori primi. Această descompunere este unică, abstracție făcând de ordinea factorilor. Mai precis, pentru orice  $n \in \mathbb{N}$ ,  $n \geq 2$  există  $p_1, \dots, p_k$  numere prime (nu neapărat diferite) astfel încât

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k$$

și din  $n = p_1 \cdot p_2 \cdot \dots \cdot p_k = q_1 \cdot q_2 \cdot \dots \cdot q_l$ , cu  $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_l$  numere prime, rezultă  $k = l$  și existența unei funcții bijective  $\sigma : \{1, \dots, k\} \rightarrow \{1, \dots, k\}$  astfel încât

$$p_i = q_{\sigma(i)}, \quad \forall i \in \{1, \dots, k\}.$$

*Demonstrație.* Pentru existența descompunerii în factori primi vom folosi metoda inducției complete în raport cu  $n \in \mathbb{N}$ ,  $n \geq 2$ .

I. *Verificare:* Pentru că 2 este număr prim, e clar că proprietatea e valabilă pentru  $n = 2$  ( $k = 1$ ,  $p_1 = 2$ ).

II. *Demonstrația:* Presupunem că orice  $m \in \mathbb{N}$ ,  $2 \leq m < n$  se descompune într-un produs cu toți factorii numere prime și arătăm că și  $n$  are aceeași proprietate. Avem două cazuri:

i) Dacă  $n$  este prim, proprietatea este evidentă ( $k = 1$ ,  $p_1 = n$ ).

ii) Dacă  $n$  nu este prim, atunci există  $a, b \in \mathbb{N}$  cu  $n = ab$ ,  $a \notin \{1, n\}$ . Deci  $1 < a, b < n$  și aplicând ipoteza inducției, obținem:

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_j \text{ și } b = p_{j+1} \cdot p_{j+2} \cdot \dots \cdot p_k,$$

unde  $p_i \in \mathbb{N}$ , sunt numere prime pentru orice  $i = 1, \dots, k$ . Atunci

$$n = a \cdot b = p_1 \cdot p_2 \cdot \dots \cdot p_j \cdot p_{j+1} \cdot p_{j+2} \cdot \dots \cdot p_k,$$

adică  $n$  admite o descompunere în factori primi.

Ca să demonstrăm unicitatea descompunerii în factori primi, considerăm două descompuneri ale lui  $n$  în produse de factori primi

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k = q_1 \cdot q_2 \cdot \dots \cdot q_l,$$

unde  $k, l \neq l$ . Pentru că înmulțirea este comutativă, putem presupune

$$p_1 \leq p_2 \leq \dots \leq p_k \text{ și } q_1 \leq q_2 \leq \dots \leq q_l.$$

Din  $p_k \mid n = q_1 \cdot q_2 \cdot \dots \cdot q_l$  rezultă că există  $i \in \{1, \dots, l\}$  astfel încât  $p_k \mid q_i$ , deci  $p_k \leq q_i$ . Analog se demonstrează și inegalitatea  $q_l \leq p_k$ , deci  $p_k = q_l$  și

$$p_1 \cdot p_2 \cdot \dots \cdot p_{k-1} = q_1 \cdot q_2 \cdot \dots \cdot q_{l-1}.$$

Continuăm procedeul de mai sus și obținem  $p_{k-1} = q_{l-1}$  și mai departe  $p_{k-i} = q_{l-i}$  pentru orice  $0 \leq i \leq \min\{k, l\}$ . Dacă am avea  $k \neq l$ , atunci s-ar obține că 1 este un produs de numere prime. Așadar  $k = l$  și  $p_i = q_i$  pentru orice  $i \in \{1, \dots, k\}$ .  $\square$

**Corolarul 5.34.** Pentru orice  $n \in \mathbb{N}$ ,  $n \geq 2$ , există numerele prime distincte  $p_1, \dots, p_k$  și  $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$  astfel încât

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}.$$

Această descompunere este unică dacă facem abstracție de ordinea factorilor.

Descompunerea din Corolarul 5.34 se numește **descompunerea canonică** a lui  $n$  (în produs de puteri de numere prime).

**Exemplul 5.35.** De exemplu  $360 = 2^3 \cdot 3^2 \cdot 5$ .

Fie  $(\alpha_k)_{k>0}$  un șir de numere. Spunem că numerele  $\alpha_k$ ,  $k \in \mathbb{N}^*$ , sunt **aproape toate nule** dacă există  $k_0 \in \mathbb{N}^*$  astfel încât  $\alpha_k = 0$  pentru orice  $k > k_0$ . Folosind această terminologie putem reformula Corolarul 5.34 astfel:

**Corolarul 5.36.** Considerăm șirul crescător al numerelor prime

$$p_1 = 2, p_2 = 3, p_3 = 5, \dots$$

Pentru orice  $n \in \mathbb{N}^*$  există un singur șir  $(\alpha_k)_{k>0}$  de numere naturale aproape toate nule astfel încât

$$n = \prod_{k \geq 1} p_k^{\alpha_k}.$$

Scrierea  $\prod_{k \geq 1} p_k^{\alpha_k}$  din acest corolar are sens pentru că toți factorii, cu excepția unui număr finit, sunt egali cu 1.

**Exemplul 5.37.** Pentru  $n = 1$ , avem  $n = \prod_{k \geq 1} p_k^0$ , i.e. șirul  $(\alpha_k)_{k>0}$  este șirul constant nul. Pentru  $n = 5$ , șirul  $(\alpha_k)_{k>0}$  are pe 1 pe poziția a treia ( $\alpha_3 = 1$ ) și pe 0 pe celelalte poziții. Numărul 360 este determinat de șirul  $(3, 2, 1, 0, 0, \dots, 0, \dots)$ .

Folosind această reformulare a teoremei fundamentale a aritmeticii, putem da o caracterizare a divizibilității și formule de calcul pentru cel mai mare divizor comun și cel mai mic multiplu comun.

**Propoziția 5.38.** Fie  $m = \prod_{k \geq 1} p_k^{\alpha_k}$  și  $n = \prod_{k \geq 1} p_k^{\beta_k}$  descompunerile numerelor naturale  $m, n > 0$  date de Corolarul 5.36. Sunt adevărate afirmațiile:

- a)  $m \mid n \Leftrightarrow \alpha_k \leq \beta_k, \forall k > 0$ ;  
 b)  $(m, n) = \prod_{k \geq 1} p_k^{\min\{\alpha_k, \beta_k\}}$ ;  
 c)  $[m, n] = \prod_{k \geq 1} p_k^{\max\{\alpha_k, \beta_k\}}$ .

## 5.6 Exerciții rezolvate

1) Să se arate că numărul  $\sqrt{2}$  este irațional.

*Soluție:* Prin reducere la absurd, presupunem că  $\sqrt{2} \in \mathbb{Q}$ . Atunci există  $m, n \in \mathbb{N}^*$  astfel încât  $\frac{m}{n} = \sqrt{2}$ . Dacă  $d = (m, n)$  și  $m = du, n = dv$ , atunci  $\sqrt{2} = \frac{u}{v}$  și  $(u, v) = 1$ . Rezultă că  $2v^2 = u^2$ , deci  $2 \mid u^2$ . Cum 2 este număr prim, rezultă că  $2 \mid u$ . Așadar  $u = 2k$ , deci  $2v^2 = 4k^2$ , de unde găsim  $2 \mid v^2$ . Folosim din nou faptul că 2 este prim și obținem  $2 \mid v$ , deci  $2 \mid (u, v)$ , o contradicție. Așadar  $\sqrt{2} \notin \mathbb{Q}$ .

2) Să se arate că există o infinitate de numere prime.

*Soluție:* Pentru a arăta că există o infinitate de numere prime este suficientă să arătăm că oricare ar fi  $S = \{p_1, \dots, p_m\}$  o mulțime de numere prime există un număr prim  $p \notin S$ .

Fie  $S = \{p_1, \dots, p_m\}$  o mulțime nevidă de numere prime. Considerăm numărul  $n = p_1 \cdot \dots \cdot p_m + 1$ . Observăm că  $n \geq 2$ , deci există un divizor prim  $p$  al lui  $n$ . Din  $p \mid p_1 \cdot \dots \cdot p_m + 1$  rezultă că există  $u \in \mathbb{Z}$  astfel încât  $pu - p_1 \cdot \dots \cdot p_m = 1$ . Deci oricare ar fi  $i \in \{1, \dots, m\}$  avem  $(p, p_i) = 1$ , și rezultă  $p \notin S$ , ceea ce trebuia demonstrat.

3) Să se arate că există o infinitate de numere prime de forma  $4k - 1$ .

*Soluție:* Fie  $S = \{p_1, \dots, p_m\}$  o mulțime nevidă de numere prime de forma  $4k - 1$ . Observăm că există astfel de mulțimi pentru că 3 are această formă.

Considerăm numărul  $n = 4p_1 \cdot \dots \cdot p_m - 1$ . Observăm că  $n \geq 2$ , deci există un divizor prim  $p$  al lui  $n$ . Mai mult, dacă presupunem că toți divizorii primi ai lui  $n$  sunt de forma  $4k + 1$ , rezultă imediat că  $n$  are aceeași formă. Dar acest fapt este imposibil pentru că restul împărțirii lui  $n$  la 4 este 3.

Așadar există un divizor prim  $p$  al lui  $n$  de forma  $4k - 1$ . Din  $p \mid 4p_1 \cdot \dots \cdot p_m - 1$  rezultă că există  $u \in \mathbb{Z}$  astfel încât  $-pu + 4p_1 \cdot \dots \cdot p_m = 1$ . Deci oricare ar fi  $i \in \{1, \dots, m\}$  avem  $(p, p_i) = 1$ , și rezultă  $p \notin S$ , ceea ce trebuia demonstrat.

4) Să se arate că dacă  $p_1, p_2, \dots, p_n, \dots$  reprezintă șirul numerelor prime aranjate în ordine crescătoare, atunci  $p_n \leq 2^{2^{n-1}}$ .

*Soluție:* Aplicăm metoda inducției matematice. Pentru  $n = 1$  avem  $p_1 = 2 \leq 2^{2^0}$ . Presupunem enunțul adevărat pentru  $p_1, \dots, p_n$  și vom demonstra că  $p_{n+1} \leq 2^{2^n}$ . Din soluția Exercițiului 2) rezultă că există un număr prim  $p$  diferit de  $p_1, \dots, p_n$  care este divizor pentru  $p_1 \cdot \dots \cdot p_n + 1$ . Deci

$$p_{n+1} \leq p \leq p_1 \cdot \dots \cdot p_n + 1 \leq 2^{2^0} \cdot 2^{2^1} \cdot \dots \cdot 2^{2^{n-1}} + 1 = 2^{\sum_{i=0}^{n-1} 2^i} + 1 = 2^{2^n - 1} + 1 < 2^{2^n}$$

și soluția este încheiată.

## 5.7 Exerciții propuse

- 1) Determinați restul împărțirii lui  $19^{44} \cdot 23^{17}$  la 7.
- 2) Fie  $n \in \mathbb{N}$  un număr natural care împărțit la 6, 8, 9, 12 și 16 dă același rest 5.
  - i) Determinați cel mai mic  $n$  cu această proprietate.
  - ii) Determinați cel mai mic  $n > 5$  cu această proprietate.
  - iii) Determinați cel mai mic multiplu de 7 cu această proprietate.
- 3) Fie  $a = \overline{a_n a_{n-1} \dots a_2 a_1 a_0} \in \mathbb{N}$ ,  $a_i \in \{0, \dots, 9\}$ ,  $i = 1, \dots, n$ ,  $a_n \neq 0$ . Să se arate că:
  - (i)  $5 \mid a \Leftrightarrow 5 \mid a_0$ ;
  - (ii)  $k \in \mathbb{N}^*$  avem  $5^k \mid a \Leftrightarrow 5 \mid \overline{a_{k-1} \dots a_0}$ ;
  - (iii)  $9 \mid a \Leftrightarrow 9 \mid a_n + \dots + a_0$ ;
  - (iv)  $7 \mid a \Leftrightarrow 7 \mid \overline{a_n \dots a_3 a_n} - \dots - \overline{a_2 a_1 a_0}$ ;
  - (v)  $11 \mid a \Leftrightarrow 11 \mid (a_0 + a_2 + a_4 + \dots) - (a_1 + a_3 + \dots)$ .
- 4) Să se arate că  $24 \mid (5n^2 + 3)(n^4 + 8)$  pentru orice număr natural  $n$ .
- 5) Să se arate că  $7 \mid 2222^{5555} + 5555^{2222}$ .
- 6) Să se determine c.m.m.d.c. și c.m.m.m.c. al numerelor 4148 și 7684.
- 7) Determinați numerele prime care pot fi scise atât ca sumă, cât și ca diferență de două numere prime.
- 8) Demonstrați că dacă  $2^n - 1$  este un număr prim, atunci  $n$  este un număr prim.
- 9) Dacă  $n \in \mathbb{N}^*$ , notăm cu  $\tau(n)$  numărul divizorilor naturali ai lui  $n$ . Să se arate că:
  - a) dacă  $a, b \in \mathbb{N}^*$  și  $(a, b) = 1$  atunci  $\tau(ab) = \tau(a)\tau(b)$ ;
  - b) dacă  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$  ( $p_1, \dots, p_k$  numere prime distincte și  $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$ ), atunci  $\tau(n) = (\alpha_1 + 1) \dots (\alpha_k + 1)$ .
- 10) Să se arate că dacă un număr natural are 133 de divizori naturali atunci el este un cub perfect.

## Bibliografie

- [1] S. Breaz, *Elemente de teoria numerelor*, note de curs.
- [2] S. Breaz, T. Coconet, C. Conțiu, *Lecții de algebră*, Ed. Eikon, Cluj-Napoca, 2010.
- [3] S. Breaz, R. Covaci, *Elemente de logică matematică, teoria mulțimilor și aritmetică*, Ed. EFES, Cluj-Napoca, 2006.
- [4] D. Burton, *Elementary number theory. Sixth edition*, McGraw-Hill, 2007.
- [5] I. D. Ion, N. Radu, *Algebră*, Editura Didactică și Pedagogică, București, 1991.
- [6] I. Purdea, I. Pop, *Algebră*, Ed. Gil, Zalău, 2003.
- [7] I. Purdea, C. Pelea, *Probleme de algebră*, Ed. Eikon, Cluj-Napoca, 2008.