ALGEBRĂ

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

CUPRINS

Pentru specializările **Matematică** şi **Matematică informatică**:

Numai pentru specializarea **Matematică**:

1 Introducere

În realizarea părţii de algebră a acestei broşuri s-a încercat alcătuirea unui material care să poată fi utilizat independent de alte surse bibliografice. Totuşi, nu am reuşit pe deplin acest lucru, aşa că recomandăm studenţilor ca acolo unde au nevoie de completări să apeleze la titlurile din bibliografia de la finalul acestui material. În acest sens, precizăm că demonstraţia Teoremei 3.32 foloseşte instrumente care nu au fost predate în liceu şi nu sunt discutate aici, de aceea am menţionat alăturat, într-o paranteză, că este facultativă. De asemenea, discuţia despre sisteme de ecuaţii liniare se bazează pe câteva rezultate referitoare la determinanţi şi rangul unei matrice cu coeficienţi într-un corp comutativ K pe care din motive de spaţiu nu le putem prezenta aici în detaliu. Ele au fost prezentate în liceu în cazul $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ şi pot fi găsite în cazul general în capitolul VI din [5]. Din aceste motive am ales ca aici doar să le amintim. De altfel, Secţiunea 4.3 conţine destul de puţine 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 şi ilustrarea lor prin exerciţii 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 licenţă. Astfel, **tematica propusă pentru specializarea Matematică** este acoperită de **capitolele 2, 3, 4 şi 5**, iar **tematica propusă pentru specializarea Matematică informatică** este acoperită de **capitolele 2, 3 şi 4** din acest material. Bibliografia de la sfârşit este comună tematicii ambelor specializări.

Dacă numărul de pagini dedicat unor teme este mai mare, aceasta se datorează faptului că s-au adăugat unele explicaţii şi observaţii pe care le-am considerat importante şi 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 explicaţii şi 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 priveşte problemele propuse, studenţii pot găsi în bibliografia menţionată rezolvări sau indicaţii care să îi ajute în abordarea acestora.

Trebuie menţionat că finalizarea acestui material în timp util şi în bune condiţii nu ar fi fost posibilă fără fişierele sursă ale unor cursuri publicate sau în pregătire puse la dispoziţie de domnul profesor Ioan Purdea şi domnul conferenţiar Simion Breaz. Contribuţia subsemnatului a fost aceea de a da un caracter autonom şi un aspect unitar (pe cât a permis tematica abordată) părţii de algebră a acestei broşuri. Nu excludem posibilitatea ca în material să se fi strecurat erori de tehnoredactare (dintre care unele ar putea să-şi lase amprenta asupra corectitudinii unor afirmaţii). Încurajăm cititorii să ne atragă atenţia asupra acelor erori pe care le identifică şi apreciem pozitiv toate semnalele care ne vor veni în acest sens.

Cosmin Pelea

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

2.1 Grupuri

Definiţia 2.1. Fie A o mulţime. O funcţie $\varphi : A \times A \to A$ se numeşte **operaţie binară** sau **lege de compoziţie** pe A.

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

Exemplele 2.2. a) Adunarea $(+)$ şi înmulţirea $(\cdot)$ sunt operaţii în $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ şi $\mathbb{C}$, dar nu sunt operaţii în mulţimea numerelor iraţionale.
b) Scăderea este operaţie în $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ şi $\mathbb{C}$, dau nu este operaţie în $\mathbb{N}$.
c) Împărţirea este operaţie în $\mathbb{Q}^*, \mathbb{R}^*$ şi $\mathbb{C}^*$, dar nu e operaţie în $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{N}^*$ şi $\mathbb{Z}^*$.

Definiţiile 2.3. Fie $*$ o operaţie în A. Spunem că:
i) operaţia $*$ este **asociativă** dacă

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

ii) operaţia $*$ este **comutativă** dacă

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

Definiţiile 2.4. Un cuplu $(A, *)$, unde A este o mulţime şi $*$ este operaţie pe A, se numeşte **grupoid**. Un grupoid în care operaţia este **asociativă** se numeşte **semigrup**. Un grupoid în care operaţia este comutativă se numeşte **grupoid comutativ**.

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

Definiţiile 2.5. Fie $*$ o operaţie în A. Spunem că operaţia $*$ **admite element neutru** dacă există un element $e \in A$ astfel încât

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

Elementul $e \in A$ se numeşte **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 numeşte **simetricul lui** a.

Observaţiile 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 şi f ar fi elemente neutre, privindu-l succesiv pe fiecare dintre ele ca element neutru, avem

$$e * f = f \text{ şi } e * f = e.$$

Prin urmare, $e = f$.

b) Într-un semigrup $(A, *)$ care are element neutru, există elemente simetrizabile. De exemplu, elementul neutru este simetrizabil şi 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 şi a' şi a'' ar fi simetrice ale lui a, avem

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

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

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

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

Exemplele 2.8. a) $(\mathbb{N}, +)$ şi $(\mathbb{Z}, \cdot)$ sunt monoizi comutativi, dar nu sunt grupuri.
b) $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ sunt 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 mulţime şi $M^M = \{f \mid f : M \to M\}$. Perechea $(M^M, \circ)$, unde $\circ$ este compunerea funcţiilor, este un monoid. Elementul neutru în acest monoid este funcţia identică $1_M : M \to M$, $1_M(x) = x$.

Observaţiile 2.9. a) Din Observaţiile 2.6 a) şi 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) Definiţia grupului poate fi rescrisă astfel: Un grupoid $(A, *)$ se numeşte **grup** dacă au loc următoarele condiţii:
(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 atenţia asupra câtorva greşeli care apar frecvent în definiţia grupului:

1) Condiţia (iii) de mai sus nu vorbeşte depre ,,existenţa elementelor simetrizabile", ci despre faptul că toate elementele sunt simetrizabile. După cum arată Observaţia 2.6 b), elemente simetrizabile există şi în monoizi care nu sunt grupuri, dar acolo există şi elemente care nu sunt simetrizabile, iar în grupuri, nu.

2) Ordinea cuantificatorilor în scrierea formală a proprietăţilor (ii) şi (iii) este esenţială. În general, cuantificatorii $\exists$ şi $\forall$ nu comută, iar aici permutarea lor duce la condiţii mult diferite de cele din definiţia grupului.

3) Introducerea unicităţii elementului neutru şi a unicităţii simetricului fiecărui element în definiţia grupului nu sunt necesare. După cum am văzut la a), acestea sunt consecinţe imediate ale definiţiei grupului şi trebuie privite ca atare.

În continuarea acestei secţiuni, cu rare excepţii, operaţia dintr-un grup va fi notată multiplicativ. Dacă $(A, \cdot)$ este un semigrup, $a \in A$ şi $n \in \mathbb{N}^*$, atunci a^n se defineşte 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 şi $a \in A$ se defineşte

$$a^0 = 1,$$

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

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

Dacă operaţia din semigrup este notată cu $+$, atunci în locul notaţiei a^n se foloseşte notaţia na.

Propoziţia 2.10. (Reguli de calcul într-un grup)
Fie $(G, \cdot)$ un grup. Se verifică uşor următoarele proprietăţi:
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 $a, b \in G$ şi 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 ecuaţiile $ax = b$ şi $ya = b$ are soluţie unică în G (pe $x = a^{-1}b$, respectiv $y = ba^{-1}$).

Corolarul 2.11. Dacă $(G, \cdot)$ este grup, atunci pentru orice $a \in G$ funcţiile $t_a : G \to G$, $t_a(x) = ax$ şi $t'_a : G \to G$, $t'_a(x) = xa$ (numite **translaţia stângă**, respectiv **translaţia dreaptă** cu a) sunt bijecţii.

Definiţiile 2.12. Fie (A, φ) un grupoid şi $B \subseteq A$. Vom spune că B este un **subgrupoid** al lui (A, φ) sau că B este **parte stabilă** în raport cu φ sau în (A, φ) 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 φ, o operaţie pe B astfel:

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

Aceasta se numeşte **operaţia indusă** de φ în B şi se notează, de multe ori, tot cu φ.

Observaţiile 2.13. a) Fie (A, φ) un grupoid, $B \subseteq A$ o parte stabilă în (A, φ) şi φ' operaţia indusă de φ în B. Dacă φ este asociativă (comutativă), atunci φ' este asociativă (comutativă). Deci orice parte stabilă B a unui semigrup (A, φ) este semigrup în raport cu operaţia indusă de φ în B, de aceea un subgrupoid al unui semigrup se mai numeşte **subsemigrup**.
b) Fie φ_1 şi φ_2 două operaţii definite pe A şi $B \subseteq A$ stabilă în raport cu φ_1 şi φ_2, iar φ_1' şi φ_2' operaţiile induse de φ_1 şi φ_2 în B. Dacă φ_1 este distributivă în raport cu φ_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 φ_1' este distributivă în raport cu φ_2'.
c) Existenţa elementului neutru este o proprietate care, în general, nu „se moşteneşte" 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.

Definiţia 2.14. Fie $(G, \cdot)$ un grup. O submulţime $H \subseteq G$ se numeşte **subgrup** al lui $(G, \cdot)$ dacă verifică condiţiile:
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 operaţia indusă de operaţia 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 $(\mathbb{R}, +)$ şi $\mathbb{Z}$ este subgrup în $(\mathbb{Q}, +)$.
b) $\mathbb{Q}^*$, $\mathbb{R}^*$ sunt subgrupuri în $(\mathbb{C}^*, \cdot)$ şi $\mathbb{Q}^*$ este subgrup în $(\mathbb{R}^*, \cdot)$.
c) $\mathbb{N}$ este un subsemigrup al lui $(\mathbb{Z}, +)$ care nu este subgrup.

Observaţiile 2.16. a) Orice subgrup este nevid.

Această afirmaţie 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 şi $h \in H \subseteq G$, 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 $(G,\cdot)$ şi $h \in H$, 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 şi simplificând cu h, rezultă $h' = h^{-1}$.

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

Teorema 2.17. (Teorema de caracterizare a subgrupului)
Fie $(G,\cdot)$ un grup şi $H \subseteq G$. Următoarele afirmaţii sunt echivalente:
1) H este subgrup al lui $(G,\cdot)$.
2) H verifică condiţiile:
   α) $H \neq \emptyset$;
   β) $h_1, h_2 \in H \Rightarrow h_1h_2 \in H$;
   γ) $h \in H \Rightarrow h^{-1} \in H$.
3) H verifică condiţiile:
   α) $H \neq \emptyset$;
   δ) $h_1, h_2 \in H \Rightarrow h_1h_2^{-1} \in H$.

Demonstraţie. 1) $\Rightarrow$ 2). Din Observaţia 2.16 a) rezultă α), iar β) coincide cu i) şi γ) urmează din Observaţia 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 condiţia δ) este verificată şi α) este comună.
3) $\Rightarrow$ 1). Dacă în δ) luăm $h_1 = h_2$ atunci rezultă $1 \in H$, iar dacă $h \in H$ şi luăm $h_1 = 1$ şi $h_2 = h$ atunci $h^{-1} \in H$. Folosind acest rezultat şi pe δ) 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 operaţia din $(G,\cdot)$ induce operaţie în H, iar din asociativitatea operaţiei în $(G,\cdot)$ rezultă asociativitatea operaţiei induse. Acum, din cele de mai sus urmează că H este subgrup. □

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

Exemplele 2.18. a) Dacă $(G,\cdot)$ este grup, atunci G şi $\{1\}$ sunt subgrupuri. Un subgrup al lui G diferit de G şi $\{1\}$ se numeşte **subgrup propriu**.
b) Submulţimea $H = \{z \in \mathbb{C} \mid |z| = 1\}$ 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 α). Folosind următoarele proprietăţi ale modulului

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

avem:

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

şi

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

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

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

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

Demonstraţie. Fie $\rho_H \subseteq G \times G$, relaţia 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 ρ_H este relaţie de echivalenţă. Cum pentru orice $x \in G$, $x^{-1}x = 1 \in H$,

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

adică ρ_H este reflexivă. Dacă $x \rho_H y$ şi $y \rho_H z$ atunci $x^{-1}y \in H$ şi $y^{-1}z \in H$. Prin urmare, $(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$ şi rezultă că $x \rho_H z$. Aşadar, ρ_H este tranzitivă. Relaţia ρ_H este şi 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 obţinem $y \rho_H x$.

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 (şi numai unul) din fiecare dintre clasele diferite (şi implicit distincte) $H, xH, yH, \ldots$ obţinem o submulţime $X \subseteq G$. Mulţimea cât şi partiţia determinată de ρ_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 $xH \bigcap yH = \emptyset$. Mai mult, pentru orice $x \in X$, funcţia $t_x : H \to xH$, $t_x(h) = xh$ este bijectivă, deci $|H| = |xH|$. Atunci

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

şi teorema este demonstrată. □

Definiţia 2.20. Fie $(G,*)$, $(G',\perp)$ grupuri. O funcţie $f: G \to G'$ se numeşte **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 numeşte **izomorfism**. Un omomorfism al lui $(G,*)$ în el însuşi se numeşte **endomorfism** al lui $(G,*)$. Un izomorfism al lui $(G,*)$ pe el însuşi se numeşte **automorfism** al lui $(G,*)$. Dacă există un izomorfism $f: G \to G$, atunci vom spune că grupurile $(G,*)$ şi $(G',\perp)$ sunt izomorfe şi vom scrie $G \simeq G'$ sau $(G,*) \simeq (G',\perp)$.

Pentru simplificarea scrierii, revenim la notaţia multiplicativă a operaţiilor.

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

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

şi

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

Demonstraţie. 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 $(G,\cdot)$ şi $(G',\cdot)$ sunt grupuri, iar $f: G \to G'$ este un izomorfism, atunci f^{-1} este un izomorfism.

Demonstraţie. Întrucât inversa unei bijecţii este o bijecţie, mai trebuie arătat că:

$$f^{-1}(y_1y_2) = f^{-1}(y_1)f^{-1}(y_2),\ \forall\ y_1, y_2 \in G'. \tag{3}$$

Conform definiţiei funcţiei 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

$$f^{-1}(y_1)f^{-1}(y_2) = x_1x_2 \tag{4}$$

Din $f(x_1x_2) = f(x_1)f(x_2) = y_1y_2$ urmează

$$f^{-1}(y_1y_2) = x_1x_2. \tag{5}$$

Acum, din (4) şi (5) rezultă (3). □

Corolarul 2.23. a) Dacă $(G,\cdot) \simeq (G',\cdot)$ atunci $(G',\cdot) \simeq (G,\cdot)$, adică relaţia $\simeq$ între grupuri este simetrică.
b) Un omomorfism $f: G \to G'$ este izomorfism, dacă şi numai dacă există un omomorfism $g: G \to G'$ astfel încât $g \circ f = 1_G$ şi $f \circ g = 1_{G'}$.

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

Demonstraţie. Folosind definiţia compunerii funcţiilor şi ipoteza că f şi g sunt omomorfisme, pentru orice $x_1,x_2\in G$ avem:

$$(g\circ f)(x_1x_2)=g(f(x_1x_2))=g(f(x_1)f(x_2))=g(f(x_1))\cdot g(f(x_2))=(g\circ f)(x_1)\cdot(g\circ f)(x_2),$$

ceea ce ne arată că $g\circ f$ este omomorfism. Compusa a două bijecţii fiind o bijecţie rezultă că dacă f şi g sunt izomorfisme, atunci $g\circ f$ este izomorfism. □

Corolarul 2.25. a) Dacă $(G,\cdot)\simeq(G',\cdot)$ şi $(G',\cdot)\simeq(G'',\cdot)$ atunci $(G,\cdot)\simeq(G'',\cdot)$, adică relaţia $\simeq$ este tranzitivă.
b) Fie $(G,\cdot)$ un grup şi $End(G,\cdot)$, respectiv $Aut(G,\cdot)$ mulţimea endomorfismelor, respectiv automorfismelor lui $(G,\cdot)$. Mulţimea $End(G,\cdot)$ este parte stabilă în $(G^G,\circ)$ şi $(End(G,\cdot),\circ)$ este monoid. Mulţimea $Aut(G,\cdot)$ este o parte stabilă a lui $(End(G,\cdot),\circ)$ care conţine 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 $1_A:A\to A$, $1_A(x)=x$ este un automorfism numit **automorfismul identic** al lui $(G,\cdot)$. Acesta este elementul unitate din $(End(G,\cdot),\circ)$ şi $(Aut(G,\cdot),\circ)$. Din acest exemplu rezultă că relaţia $\simeq$ este reflexivă.
b) Dacă $(G,\cdot)$ şi $(G',\cdot)$ sunt grupuri, iar $1'$ este elementul neutru din $(G',\cdot)$, atunci funcţia $\theta:G\to G'$, $\theta(x)=1'$ este omomorfism numit **omomorfismul nul** sau **zero**.
c) Fie $a\in\mathbb{R}$, $a\neq 1$, $a>0$. Funcţia $f:\mathbb{R}_+^*\to\mathbb{R}$, $f(x)=\log_a x$ este un izomorfism al grupului $(\mathbb{R}_+^*,\cdot)$ pe grupul $(\mathbb{R},+)$ şi inversul acestuia este $f^{-1}:\mathbb{R}\to\mathbb{R}_+^*$, $f^{-1}(x)=a^x$. Proprietăţile $\log_a(xy)=\log_a x+\log_a y$ şi $a^{x+y}=a^xa^y$ exprimă faptul că f şi f^{-1} sunt omomorfisme.
d) Funcţia $f:\mathbb{C}^*\to\mathbb{R}^*$, $f(z)=|z|$ este un omomorfism al grupului $(\mathbb{C}^*,\cdot)$ în grupul $(\mathbb{R}^*,\cdot)$ pentru că $f(z_1z_2)=|z_1z_2|=|z_1|\cdot|z_2|=f(z_1)f(z_2)$.
e) Funcţia $f:\mathbb{C}\to\mathbb{C}$, $f(z)=\overline{z}$ (unde $\overline{z}$ este conjugatul lui z) este un automorfism al grupului $(\mathbb{C},+)$, iar $f^{-1}=f$. Restricţia lui f la $\mathbb{C}^*$ este automorfism al grupului $(\mathbb{C}^*,\cdot)$.
f) Pentru orice grup $(G,\cdot)$ funcţia $f:G\to G$, $f(x)=x^{-1}$ este bijectivă. Funcţia f este un automorfism al lui $(G,\cdot)$ dacă şi numai dacă grupul $(G,\cdot)$ este abelian.

Reamintim că pentru o funcţie $f:A\to B$, $X\subseteq A$ şi $Y\subseteq B$, notăm

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

Teorema 2.27. Fie $(G,\cdot)$ şi $(G',\cdot)$ grupuri şi $f:G\to G'$ 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 $\overset{-1}{f}(H')$ este un subgrup al lui $(G,\cdot)$.

Demonstraţie. 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:

$$y_1y_2^{-1}=f(x_1)\cdot f(x_2)^{-1}=f(x_1)\cdot f(x_2^{-1})=f(x_1x_2^{-1}),$$

iar $x_1, x_2 \in H$ implică $x_1 x_2^{-1} \in H$. Rezultă că $y_1 y_2^{-1} \in f(H)$. Deci $f(H)$ este un subgrup al lui $(G', \cdot)$.

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

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

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

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

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

Definiţia 2.29. Fie $(G, \cdot)$ şi $(G', \cdot)$ grupuri şi $f : G \to G'$ un omomorfism. Subgrupul $\mathrm{Ker} f = \{x \in G \mid f(x) = 1'\}$ al lui G se numeşte **nucleul omomorfismului** f.

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

Demonstraţie. Dacă omomorfismul f este injectiv, atunci

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

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

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

ceea ce ne arată că omomorfismul f este injectiv. □

2.2 Exerciţii rezolvate

1) Fie M o mulţime, $\mathcal{P}(M)$ mulţimea submulţimilor sale şi $\triangle$ **diferenţa simetrică**, adică pentru $X, Y \subseteq M$ avem $X \triangle Y = (X \setminus Y) \cup (Y \setminus X)$. Să se arate că $(\mathcal{P}(M), \triangle)$ este un grup.

Soluţie: Fie $C(X) = C_M X = M \setminus X$ complementara submulţimii $X \subseteq M$. Avem

$$X \triangle Y = [X \cap C(Y)] \cup [Y \cap C(X)]. \tag{1}$$

În stabilirea asociativităţii operaţiei $\triangle$ avem nevoie de egalitatea

$$C(X \triangle Y) = (X \cap Y) \cup [C(X) \cap C(Y)] \tag{2}$$

care se deduce din (1), din formulele lui de Morgan şi din distributivitatea intersecţiei faţă de reuniune astfel:

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

Folosind (1) şi (2) avem

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

La acelaşi rezultat se ajunge şi calculând pe $X\triangle(Y\triangle Z)$. Deci $\triangle$ este asociativă.

Din definiţia operaţiei $\triangle$ rezultă că $\triangle$ este comutativă, are element neutru submulţimea vidă şi $X\triangle X=\emptyset$, adică opusa lui X este X. Deci $(\mathcal{P}(M),\triangle)$ este grup abelian.

2) Fie $G=(-1,1)$, $x,y\in G$ şi

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

Să se arate că:
i) egalitatea $(*)$ defineşte o operaţie $*$ pe G şi $(G,*)$ este un grup abelian;
ii) între grupul multiplicativ al numerelor reale pozitive $(\mathbb{R}_+^*,\cdot)$ şi $(G,*)$ există un izomorfism $f:\mathbb{R}_+^*\to G$ de forma $f(x)=\dfrac{\alpha x-1}{x+1}$.
Soluţie: i) Dacă $x,y\in G$ atunci $x*y\in G$ deoarece

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

Aşadar, $*$ este o operaţie pe G. Din (1) rezultă că $*$ este comutativă. Asociativitatea sa se obţine 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 $\dfrac{x+e}{1+xe}=x$ 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 uşor 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

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

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 $(**)$ defineşte o funcţie $f : \mathbb{R}_+^* \to G$. Funcţia f este bijectivă deoarece ecuaţia $f(x) = y$ are o soluţie unică $x = \dfrac{1+y}{1-y} \in \mathbb{R}_+^*$. 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 şi $\emptyset \neq H \subseteq G$. Să se arate că H este un subgrup în G dacă şi numai dacă H este parte stabilă în $(G, \cdot)$.

Soluţie: 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 restricţiilor translaţiilor cu h la H sunt în H. Prin urmare, avem funcţiile

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

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

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, obţinem $1 = e \in H$. Aşadar, t_h fiind surjecţie, 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 $(\mathbb{Z}, +)$.

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

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

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

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

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

$$f(x) = f(\underbrace{1 + 1 + \cdots + 1}_{x \text{ termeni}}) = xf(1)$$

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

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

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

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

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

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

2.3 Inele şi corpuri

Definiţiile 2.31. Un sistem ordonat $(R, +, \cdot)$ în care R este o mulţime, iar $+$ şi $\cdot$ sunt operaţii pe R se numeşte **inel** dacă verifică următoarele axiome:
i) $(R, +)$ este grup abelian;
ii) $(R, \cdot)$ este semigrup;
iii) Operaţia $\cdot$ este distributivă faţă de $+$, adică

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

Inelul $(R, +, \cdot)$ se numeşte **comutativ**, respectiv **cu unitate** dacă operaţia $\cdot$ 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 numeşte **inversabil** dacă

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

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

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

Observaţiile 2.32. a) În liceu se foloseşte 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 $a \in R$ şi $n \in \mathbb{Z}$ se poate defini na ca înainte de Propoziţia 2.10. În semigrupul $(R, \cdot)$ se poate defini a^n pentru orice $a \in R$ şi orice $n \in \mathbb{N}^*$, iar dacă R este inel cu unitate putem defini a^n şi pentru $n \in \mathbb{Z}$ în condiţiile discutate pe larg în Secţiunea 2.1. Proprietăţile calculului cu multipli şi ale calculului cu puteri într-un inel rezultă imediat din Propoziţia 2.10.

Definiţia 2.33. Un inel cu unitate $(K, +, \cdot)$ se numeşte **corp** dacă:
i) K conţine cel puţin două elemente, adică $|K| \geq 2$.
ii) Orice $a \in K^*$ este inversabil.

Observaţia 2.34. Un triplet $(K, +, \cdot)$ este corp dacă şi numai dacă:
1) $(K, +)$ este grup abelian.
2) K^* este stabilă în $(K, \cdot)$ şi $(K^*, \cdot)$ este grup.
3) Operaţia $\cdot$ este distributivă în raport cu $+$.

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

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

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

Demonstraţie. 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. □

Corolarul 2.36. (Reguli de calcul într-un inel) Fie $(R, +, \cdot)$ un inel.
a) Pentru orice $a, b \in R$ au loc egalităţile:

$$a0 = 0 = 0a,\ a(-b) = -ab = (-a)b,\ (-a)(-b) = ab. \tag{1}$$

Primele două (şiruri de) egalităţi din (1) rezultă din teorema de mai sus şi din Teorema 2.21. Ultima egalitate se obţine astfel:

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

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

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

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

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

Cum implicaţiile din şirul

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

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 şi $R \neq \{0\}$, 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 afirmaţii nu este, în general, adevărată. Inelele în care această inversă este adevărată constituie o clasă specială de inele.

Definiţia 2.38. Fie R un inel. Un element $a \in R$, $a \neq 0$ se numeşte **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 şi care nu conţine divizori ai lui zero (diferiţi de zero) se numeşte **domeniu de integritate**.

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

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

Menţionăm că implicaţia 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 şi $a, b \in K$,

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

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 şdi 1.
b) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sunt corpuri comutative.
c) Pe o mulţime formată dintr-un singur element există o singură operaţie. Dacă luăm în calitate de $+$ şi de $\cdot$ această operaţie, atunci se obţine un inel asociativ, comutativ şi cu element unitate. Acesta se numeşte **inelul nul**. În acest inel avem $0 = 1$. Din Observaţia 2.37 a) rezultă că inelul nul este caracterizat de această egalitate.
d) Fie R o mulţime şi $m, n \in \mathbb{N}^*$. O funcţie

$$A : \{1, \ldots, m\} \times \{1, \ldots, n\} \to R$$

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

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

Pentru acest tabel vom folosi notaţia $A = (a_{ij})$. Mulţimea 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 operaţie $+$ în $M_{m,n}(R)$ definită astfel: dacă $A = (a_{ij})$ şi $B = (b_{ij})$ sunt două matrice de tipul (m, n) atunci

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

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

Denumirea de înmulţire a matricelor este întrebuinţată pentru operaţia parţială definită în mulţimea $\bigcup\{M_{m,n}(R) \mid (m,n) \in \mathbb{N}^* \times \mathbb{N}^*\}$ astfel: dacă avem $A = (a_{ij}) \in M_{m,n}(R)$ şi $B = (b_{ij}) \in M_{n,p}(R)$, atunci

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

Dacă lucrăm cu matrici pătratice de acelaşi ordin, operaţia parţială $\cdot$ de mai sus devine o operaţie în sensul Definiţiei 2.1, operaţie care este asociativă şi distributivă faţa 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 $n \geq 2$ şi $R \neq \{0\}$ atunci inelul $M_n(R)$ nu este comutativ şi 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 şi pentru a arăta că semigrupul $(M_n(R), \cdot)$ nu este comutativ.

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

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

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

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

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

e) Fie $n \in \mathbb{N}, \ n \geq 2$. Teorema împărţirii cu rest în $\mathbb{Z}$ (a se vedea Secţiunea 5.1) permite partiţionarea mulţimii $\mathbb{Z}$ în clase determinate de resturile ce pot fi obţinute prin împărţire 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 notaţii

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

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

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

Operaţiile

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

sunt bine definite, adică, dacă se consideră alţi reprezentanţi a' şi b' pentru două clase $\widehat{a}$, respectiv $\widehat{b}$ rezultatele operaţiilor rămân aceleaşi. Într-adevăr, din $a' \in \widehat{a}$ şi $b' \in \widehat{b}$ rezultă

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

şi

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

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

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

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

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

Definiţia 2.41. Fie $(R,+,\cdot)$ un inel. O submulţime $A\subseteq R$ se numeşte **subinel** al lui $(R,+,\cdot)$ dacă
i) A este stabilă în raport cu $+$ şi $\cdot$, adică

$$a_1,a_2\in A \Rightarrow a_1+a_2\in A \text{ şi } a_1a_2\in A.$$

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

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

Afirmaţia rezultă din definiţiile subinelului şi subgrupului şi din Observaţia 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 conţine elementul nul din R.
d) Un subinel A al unui inel cu unitate R, în general, nu conţine unitatea lui R. De exemplu, $(\mathbb{Z},+,\cdot)$ este inel cu unitate şi $2\mathbb{Z}$ este subinel al acestuia, dar $1\notin 2\mathbb{Z}$.

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

Teorema 2.43. (Teorema de caracterizare a subinelului)
Fie $(R,+,\cdot)$ un inel şi $A\subseteq R$. Sunt echivalente următoarele afirmaţii:
1) A este subinel al lui $(R,+,\cdot)$.
2) A verifică condiţiile:
α) $A\neq\emptyset$;
β) $\alpha_1,\alpha_2\in A \Rightarrow a_1-a_2\in A$;
γ) $\alpha_1,a_2\in A \Rightarrow a_1a_2\in A$.

3) A verifică condiţiile:
α) $A \neq \emptyset$;
β') $a_1, a_2 \in A \Rightarrow a_1 + a_2 \in A$;
β'') $a \in A \Rightarrow -a \in A$;
γ) $a_1, a_2 \in A \Rightarrow a_1 a_2 \in A$.

Demonstraţie. Rezultă din Observaţia 2.42 a) şi din faptul că atât condiţiile α) şi β) cât şi condiţiile α), β') şi β'') sunt echivalente cu afirmaţia că A este subgrup în $(R, +)$ (vezi Teorema 2.17). □

Exemplele 2.44. a) Dacă R este un inel, atunci $\{0\}$ şi R sunt subinele ale lui R. Un subinel al lui R diferit de $\{0\}$ şi R se numeşte **propriu**.
b) Fiecare din inelele $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ şi $\mathbb{C}$ 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 γ), ceea ce este imediat pentru că produsul a doi multipli de n este multiplu de n.

Definiţia 2.45. Fie $(K, +, \cdot)$ un corp. O submulţime $A \subseteq K$ se numeşte **subcorp** al lui $(K, +, \cdot)$ dacă
i) A este stabilă în raport cu $+$ şi $\cdot$, adică

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

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

Observaţiile 2.46. a) Din ii) rezultă că dacă A este subcorp, atunci avem $|A| \geq 2$.
b) Dacă $(K, +, \cdot)$ este corp şi $A \subseteq K$, atunci A este subcorp dacă şi numai dacă A este subgrup în $(K, +)$ şi 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 şi $A \subseteq K$, atunci A este subcorp dacă şi numai dacă A este subinel în $(K, +, \cdot)$, $|A| \geq 2$ şi pentru orice $a \in A^*$, $a^{-1} \in A$.

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

Teorema 2.47. (Teorema de caracterizare a subcorpului)
Fie $(K, +, \cdot)$ un corp şi $A \subseteq K$. Sunt echivalente următoarele afirmaţii:
1) A este subcorp al lui $(K, +, \cdot)$.
2) A verifică condiţiile:
α) $|A| \geq 2$;
β) $a_1, a_2 \in A \Rightarrow a_1 - a_2 \in A$;
γ) $a_1, a_2 \in A;\ a_2 \neq 0 \Rightarrow a_1 a_2^{-1} \in A$;
3) A verifică condiţiile:
α) $|A| \geq 2$;
β') $a_1, a_2 \in A \Rightarrow a_1 + a_2 \in A$;
β'') $a \in A \Rightarrow -a \in A$;
γ') $a_1, a_2 \in A \Rightarrow a_1 a_2 \in A$;
γ'') $a \in A;\ a \neq 0 \Rightarrow a^{-1} \in A$.

Demonstraţie. Rezultă din Observaţiile 2.46 a) şi b) şi din Teorema 2.17. □

Exemplele 2.48. a) $\mathbb{Q}$ este subcorp în $\mathbb{R}$ şi 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.

Definiţiile 2.49. Fie $(R,+,\cdot)$ şi $(R',+,\cdot)$ două inele. O funcţie $f : R \to R'$ se numeşte **omomorfism (de inele)** dacă pentru orice $x_1, x_2 \in R$,

$$f(x_1 + x_2) = f(x_1) + f(x_2) \text{ şi } f(x_1x_2) = f(x_1)f(x_2). \tag{2}$$

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

Fie $(R,+,\cdot)$ şi $(R',+,\cdot)$ inele cu unitate (1 şi $1'$ fiind, respectiv, unităţile lor). Un **omomorfism** $f : R \to R'$ se numeşte **unital** dacă

$$f(1) = 1' \tag{3}$$

Observaţia 2.50. Prima condiţie din (2) arată că dacă $f : R \to R'$ este un omomorfism între inelele $(R,+,\cdot)$ şi $(R',+,\cdot)$, atunci f este omomorfism al grupului $(R,+)$ în $(R',+)$.

Teorema 2.51. Fie $(R,+,\cdot)$, $(R',+,\cdot)$ inele şi $f : R \to R'$ un omomorfism. Atunci

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

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

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

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

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

şi din (3) urmează

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

ceea ce demonstrează pe (5). □

Exemplele 2.52. a) Dacă $(R,+,\cdot)$ şi $(R',+,\cdot)$ sunt inele, atunci funcţia $\theta : R \to R'$, $\theta(x) = 0$ este un omomorfism numit **omomorfismul nul** sau **zero**. Dacă R şi R' sunt cu unitate şi $|R'| \geq 2$, atunci omomorfismul θ nu este unital.
b) Fie $f : \mathbb{C} \to \mathbb{C}$, $f(z) = \overline{z}$ (unde $\overline{z}$ este conjugatul lui z). Din

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2},\ \overline{z_1 z_2} = \overline{z_1}\,\overline{z_2} \text{ şi } \overline{\overline{z}} = z$$

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

c) Fie R un inel, $n \in \mathbb{N}^*$ şi $M_n(R)$ inelul matricelor pătrate cu elemente din R. Funcţia $f : R \to M_n(R)$ 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.

Observaţia 2.53. Orice omomorfism nenul dintre două corpuri este unital.

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

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

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

2.4 Exerciţii rezolvate

1) Fie M o mulţime şi $\mathcal{P}(M)$ mulţimea submulţimilor lui M. Definim pe $\mathcal{P}(M)$ două operaţii $+$ şi $\cdot$ astfel:

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

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 şi numai dacă $|M| = 1$.

Soluţie: i) Observăm că $X + Y$ este diferenţa simetrică a mulţimilor X şi Y, iar din Exerciţiul rezolvat 1) de la secţiunea anterioară deducem că $(\mathcal{P}(M), +)$ este grup abelian. Din proprietăţile intersecţiei şi definiţia operaţiei $\cdot$ rezultă că $\cdot$ este asociativă, comutativă şi M este element neutru. Deci $(\mathcal{P}(M), \cdot)$ este monoid comutativ.

Stabilim distributivitatea operaţiei $\cdot$ faţă 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 şi numai dacă $P(M)=\{\emptyset,M\}$, adică $|M|\leq 1$. Dacă $|M|=0$ atunci $M=\emptyset$ şi $(\mathcal{P}(M),+,\cdot)$ 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 şi $a,b\in R$. 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

$$\begin{aligned}(a+b)^n=&C_n^0a^n+C_n^1a^{n-1}b+\cdots+C_n^{n-1}ab^{n-1}+C_n^nb^n;\\ a^n-b^n=&(a-b)\left(a^{n-1}+a^{n-2}b+\cdots+ab^{n-2}+b^{n-1}\right);\\ a^{2n+1}+b^{2n+1}=&(a+b)\left(a^{2n}-a^{2n-1}b+\cdots-ab^{2n-1}+b^{2n}\right).\end{aligned}$$

Soluţie: 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 egalităţi se verifică imediat.
b) Ţinem seama de faptul că orice puteri (cu exponent natural nenul) ale elementelor a, b comută şi procedăm prin inducţie după n. Pentru $n=1$ afirmaţia este, evident, adevărată, iar dacă egalitatea este adevărată pentru n atunci

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

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

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

ceea ce finalizează raţionamentul prin inducţie. Celelalte egalităţi se obţin efectuând calculul din membrul drept.

3) Fie $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$ şi $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$. Să se arate că:
i) $\mathbb{Z}[\sqrt{2}]$ este un subinel al lui $(\mathbb{R},+,\cdot)$ care conţine 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 $(\mathbb{R},+,\cdot)$.
Soluţie: 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:

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

şi $1=1+0\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$. Deci $\mathbb{Z}[\sqrt{2}]$ este subinel şi $1\in\mathbb{Z}[\sqrt{2}]$.
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 $a,b\in\mathbb{Q}$ şi $a^2-2b^2\neq 0$ şi 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 iraţional, urmează $ab = 2$ şi $a + b^2 = 0$. Acest sistem nu are soluţii în $\mathbb{Z}$. Deci S_1 nu este stabilă în raport cu $\cdot$ şi astfel S_1 nu este subinel în $(\mathbb{R}, +, \cdot)$.
iv) Se arată la fel ca şi în iii) că $u = \sqrt[3]{2} \in S_2$, dar $u^2 \notin S_2$.

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

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

Dacă $m, n \in \mathbb{N}^*$ atunci $f\left(\frac{m}{n}\right) = f\left(\underbrace{\frac{1}{n} + \cdots + \frac{1}{n}}_{m \text{ termeni}}\right) = mf\left(\frac{1}{n}\right)$. 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 $f\left(-\frac{m}{n}\right) = -f\left(\frac{m}{n}\right) = -\frac{m}{n}$. Aşadar, $f(x) = x$ pentru orice $x \in \mathbb{Q}$. De aici şi 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 $f_1(a + b\sqrt{2}) = a + b\sqrt{2}$ şi $f_2(a + b\sqrt{2}) = a - b\sqrt{2}$. 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 bijecţie şi $f_2^{-1} = f_2$. Se verifică uşor că f_2 este omomorfism. Deci şi f_2 este automorfism. În concluzie, automorfismele corpului $\mathbb{Q}(\sqrt{2})$ sunt f_1 şi f_2.

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

Soluţie: 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 $a \in \mathbb{R} \setminus \mathbb{Q}$ şirul $(a'_n)_{n \in \mathbb{N}}$ al aproximărilor sale raţionale prin lipsă şi şirul $(a''_n)_{n \in \mathbb{N}}$ al aproximărilor sale raţionale prin adaos, obţinem $a'_n \leq a \leq a''_n$ 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 obţinem $f(a) = a$. Deci $f = 1_{\mathbb{R}}$.

2.5 Exerciţii propuse

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

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

3) Demonstraţi Propoziţia 2.10.
4) Fie $(G, \cdot)$ un grup şi $f, g : G \to G$, $f(x) = x^{-1}$, $g(x) = x^2$. Să se arate că:
i) f este o bijecţie;
ii) f este automorfism dacă şi numai dacă $(G, \cdot)$ este abelian;
iii) g este omomorfism dacă şi numai dacă $(G, \cdot)$ este abelian.
5) Să se arate că $H \subseteq \mathbb{Z}$ este subgrup al lui $(\mathbb{Z}, +)$ dacă şi 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 $f : \mathbb{Q} \to \mathbb{Q}$ este un endomorfism al grupului $(\mathbb{Q}, +)$ atunci

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

adică f este o translaţie a lui $(\mathbb{Q}, \cdot)$ şi că orice translaţie 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 şi numai dacă $(a, n) = 1$. Să se deducă de aici că inelul $(\mathbb{Z}_n, +, \cdot)$ este corp dacă şi numai dacă n este număr prim.
9) a) Să se rezolve în $\mathbb{Z}_{12}$ ecuaţiile $\widehat{4}x + \widehat{5} = \widehat{9}$ şi $\widehat{5}x + \widehat{5} = \widehat{9}$ şi în $M_2(\mathbb{C})$ ecuaţia

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

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 numeşte **întreg liber de pătrate** dacă $d \neq 1$ şi 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) $a, b \in \mathbb{Q}$ şi $a + b\sqrt{d} = 0$ 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 conţine 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 $i : \mathbb{Q} \to \mathbb{C}$, $i(x) = x$.

3 Spaţii vectoriale (de Ioan Purdea şi Cosmin Pelea)

3.1 Spaţii, subspaţii, transformări liniare

Definiţia 3.1. Fie K un corp comutativ. O pereche ordonată formată dintr-un grup abelian $(V, +)$ şi o funcţie $\varphi : K \times V \to V$ se numeşte **K-spaţiu vectorial (liniar) stâng** sau **spaţiu 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 $\alpha,\beta\in K$ şi $x,y\in V$.

Elementele din K, respectiv V se numesc **scalari**, respectiv **vectori**. Funcţia φ se numeşte **operaţie externă** pe V cu domeniul de operatori K sau înmulţire cu scalari, iar $+$ din V **operaţie internă** sau adunare a vectorilor. De cele mai multe ori — şi aşa vom face şi noi în cele ce urmează — vom folosi $\cdot$ în loc de φ. Astfel, $\varphi(\alpha,x)$ se notează cu αx (sau cu $x\alpha$) şi se numeşte **produsul** dintre scalarul α şi vectorul x. Cu aceste notaţii 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) $1x=x$.

Observaţia 3.2. Atragem atenţia că $+$ şi $\cdot$ notează fiecare câte două operaţii. De exemplu, în axioma 1) primul $+$ este operaţia din corp, iar al doilea este operaţia din grup, iar în axioma 3), în membrul stâng, primul $\cdot$ este operaţia din corp, iar al doilea este operaţia externă, în timp ce în membrul drept ambii $\cdot$ simbolizează operaţia externă.

Teorema 3.3. Dacă V este un K-spaţiu vectorial, atunci:
i) Pentru orice $\alpha\in K$, funcţia $t_\alpha:V\to V$, $t_\alpha(x)=\alpha x$ este un endomorfism al grupului $(V,+)$. Dacă, în plus, $\alpha\neq 0$ atunci t_α este un automorfism al lui $(V,+)$ şi $t_\alpha^{-1}=t_{\alpha^{-1}}$.
ii) Pentru orice $x\in V$ funcţia $t'_x:K\to V$, $t'_x(\alpha)=\alpha x$ este un omomorfism al grupului $(K,+)$ în grupul $(V,+)$.

Demonstraţie. 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 $t_\alpha\in End(V,+)$. 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

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

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 spaţiu vectorial)
a) Pentru orice $\alpha\in K$ şi $x\in V$ avem:

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

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

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

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

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

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 poziţie al punctului M (relativ la originea O). Notăm cu V_2 mulţimea tuturor vectorilor $\overrightarrow{OM}$ când M parcurge punctele planului fixat. Mulţimea V_2 este $\mathbb{R}$ - spaţiu vectorial în raport cu adunarea vectorilor după regula paralelogramului şi înmulţirea cu scalari definită astfel: dacă $\alpha \in \mathbb{R}$ atunci $\alpha\overrightarrow{OM}$ este vectorul cu originea în O care are direcţia lui $\overrightarrow{OM}$, sensul lui $\overrightarrow{OM}$ dacă $\alpha > 0$ şi sens contrar lui $\overrightarrow{OM}$ dacă $\alpha < 0$, iar lungimea (modulul) este produsul dintre $|\alpha|$ şi 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 operaţiile de adunare a vectorilor şi de înmulţire a vectorilor cu scalari se exprimă astfel:

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

Coordonatele vectorului $\overrightarrow{OM}$ (adică ale lui M) depind de alegerea sistemului de coordonate. Analog se obţine spaţiul liniar V_3 al vectorilor din spaţiul 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 mulţime dintr-un singur element $\{0\}$ există o singură operaţie $+$ definită prin egalitatea $0 + 0 = 0$ şi $(\{0\}, +)$ este grup abelian. Pentru orice corp comutativ K există o singură operaţie externă

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

Cele două operaţii definesc pe $\{0\}$ o structură de K-spaţiu vectorial. Acest spaţiu vectorial se numeşte **spaţiul vectorial zero** sau **nul**.
c) Dacă K este un corp comutativ, atunci pentru orice $n \in \mathbb{N}^*$ mulţimea K^n este un K-spaţiu vectorial în raport cu operaţiile definite pe componente astfel:

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

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

unde $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in K^n$ şi $\alpha \in K$.
d) Grupul $(K, +)$ al unui corp $(K, +, \cdot)$ este un K-spaţiu vectorial în raport cu operaţia externă $K \times K \to K$, $(\alpha, x) \mapsto \alpha x$ unde αx este produsul perechii (α, x) în $(K, \cdot)$. Acest exemplu se obţine din c) luând $n = 1$.
e) Fie K' un corp şi K un un subcorp al lui K'. Dacă $(V, +)$ este un K'-spaţiu vectorial, atunci $(V, +)$ este un K-spaţiu vectorial în raport cu operaţia externă $K \times V \to V$, $(\alpha, x) \mapsto \alpha x$ unde αx este produsul dintre scalarul α şi vectorul x în V privit K'-spaţiu vectorial. Se spune că K-spaţiul vectorial V s-a obţinut din K'-spaţiul vectorial V prin

restricţia corpului de scalari de la K' la K. Astfel $\mathbb{R}$ este un $\mathbb{Q}$-spaţiu vectorial, iar $\mathbb{C}$ este un $\mathbb{Q}$-spaţiu vectorial şi un $\mathbb{R}$-spaţiu vectorial.
f) Fie K un corp comutativ şi

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

mulţimea polinoamelor cu coeficienţi 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 acelaşi număr de termeni, adăugând, dacă e cazul, monoame cu coeficientul 0 în scrierea unuia dintre ele). Egalitatea

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

defineşte o operaţie asociativă şi comutativă pe $K[X]$. Aceasta are element neutru pe $0 \in K[X]$ (polinomul nul) şi 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-spaţiu vectorial în raport cu înmulţirea cu scalari definită astfel: dacă $\alpha \in K$ şi $f = a_0 + a_1X + \cdots + a_nX^n \in K[X]$, 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-spaţiu vectorial în raport cu înmulţirea cu scalari definită astfel:

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

Să observăm că în cazul matricilor pătratice (de ordin n), pe lânga structura de K-spaţiu vectorial a lui $M_n(K)$ avem şi o structură de inel pe $M_n(K)$ (vezi Exemplul 2.40 d)). Mai mult, între cele două structuri avem o relaţie de legătură, şi anume:

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

h) Dacă V_1 şi V_2 sunt K-spaţii vectoriale, atunci produsul cartezian $V_1 \times V_2$ este K-spaţiu vectorial în raport cu operaţiile definite astfel:

$$(x_1, x_2) + (x_1', x_2') = (x_1 + x_1', x_2 + x_2'),\ \alpha(x_1, x_2) = (\alpha x_1, \alpha x_2)$$

unde $(x_1, x_2), (x_1', x_2') \in V_1 \times V_2$ şi $\alpha \in K$. Spaţiul vectorial astfel obţinut se numeşte **produsul direct** al spaţiilor V_1 şi V_2.

Definiţia 3.6. Fie V un K-spaţiu vectorial. O submulţime $A \subseteq V$ se numeşte **subspaţiu** 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 $(V, +)$ şi în raport cu înmulţirea cu scalari) şi A este K-spaţiu vectorial în raport cu operaţiile induse.

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

Observaţiile 3.7. a) Dacă V este un K-spaţiu vectorial şi $A \subseteq V$, atunci A este un subspaţiu dacă şi numai dacă A este subgrup al grupului $(V, +)$ şi A verifică condiţia ii).
b) Dacă A este un subspaţiu al K-spaţiului vectorial V, atunci $0 \in A$.

Practic, când arătăm că o submulţime a unui spaţiu vectorial este subspaţiu aplicăm următoarea teoremă.

Teorema 3.8. (Teorema de caracterizare a subspaţiului)
Fie V un K-spaţiu vectorial şi $A \subseteq V$. Sunt echivalente următoarele afirmaţii:
1) A este subspaţiu al lui V.
2) A verifică condiţiile:
   $\alpha)$ $A \neq \emptyset$;
   $\beta)$ $a_1, a_2 \in A \Rightarrow a_1 - a_2 \in A$;
   $\gamma)$ $\alpha \in K,\ a \in A \Rightarrow \alpha a \in A$.
3) A verifică condiţiile:
   $\alpha)$ $A \neq \emptyset$;
   $\beta')$ $a_1, a_2 \in A \Rightarrow a_1 + a_2 \in A$;
   $\gamma)$ $\alpha \in K,\ a \in A \Rightarrow \alpha a \in A$.
4) A verifică condiţiile:
   $\alpha)$ $A \neq \emptyset$;
   $\beta'')$ $\alpha_1, \alpha_2 \in K,\ a_1, a_2 \in A \Rightarrow \alpha_1 a_1 + \alpha_2 a_2 \in A$.

Demonstraţie. Echivalenţa 1) $\Leftrightarrow$ 2) rezultă din Observaţia 3.7 a) şi din faptul că $\alpha)$ şi $\beta)$ sunt condiţii necesare şi suficiente ca A să fie subgrup în $(V, +)$.

Din teorema de caracterizare a subgrupului rezultă implicaţia 2) $\Rightarrow$ 3). Din $\gamma)$ şi $\beta')$ 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) şi astfel am arătat că 2) $\Leftrightarrow$ 3).

Din $\gamma)$ şi $\beta')$ 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 $\beta')$ şi luând $\alpha_1 = \alpha$, $\alpha_2 = 0$, $a_1 = a$, rezultă $\gamma)$. Deci şi echivalenţa 3) $\Leftrightarrow$ 4) este demonstrată. □

Exemplele 3.9. a) Pentru orice spaţiu vectorial V submulţimile $\{0\}$ şi V sunt subspaţii ale lui V. Un subspaţiu al lui V diferit de $\{0\}$ şi V, se numeşte **subspaţiu propriu**.
b) Fie K un corp comutativ şi $K[X]$, K-spaţiul vectorial al polinoamelor, iar $n \in \mathbb{N}^*$. Se constată uşor că

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

verifică pe $\alpha)$, $\beta')$, $\gamma)$. Deci $P_n(K)$ este un subspaţiu al lui $K[X]$.
c) Fie V_3 spaţiul vectorial peste $\mathbb{R}$ al vectorilor (segmentelor orientate) din spaţiu cu originea într-un punct O. Subspaţiile lui V_3 sunt: $\{0\}$, V_3, dreptele care trec prin O (mai exact mulţimile de vectori de poziţie ai punctelor situate pe aceste drepte) şi planele care trec prin O (mulţimile de vectori de poziţie conţinuţi în aceste plane).

d) Fie $I \subseteq \mathbb{R}$ un interval. Mulţimea $\mathbb{R}^I = \{f \mid f : I \to \mathbb{R}\}$ este $\mathbb{R}$-spaţiu vectorial în raport cu operaţiile definite prin:

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

unde $f, g \in \mathbb{R}^I$ şi $\alpha \in \mathbb{R}$. Submulţimile

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

sunt subspaţii ale lui $\mathbb{R}^I$ pentru că sunt nevide şi

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

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

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

Demonstraţie. Din ipoteză avem $I \neq \emptyset$. Cum fiecare A_i este subspaţiu rezultă $0 \in A_i$ pentru toţi $i \in I$, de unde urmează că $\bigcap_{i\in I} A_i \neq \emptyset$. Folosind definiţia intersecţiei şi faptul că fiecare A_i este subspaţiu, 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 subspaţiu 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 subspaţiu al lui V notat cu $\langle X \rangle$ numit **subspaţiul generat** de X. Din (1) rezultă că $\langle X \rangle$ este cel mai mic subspaţiu 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 submulţime finită $X \subseteq V$ astfel încât $V = \langle X \rangle$, atunci spunem că spaţiul V este de **tip finit** sau **finit generat**. Dacă $X = \{x_1, \ldots, x_n\}$, vom nota $\langle X \rangle$ cu $\langle x_1, \ldots, x_n \rangle$.

Observaţia 3.11. Din definiţia subspaţiului 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) $X \subseteq V \Rightarrow \langle \langle X \rangle \rangle = \langle X \rangle$.

Definiţia 3.12. Fie V un K-spaţiu vectorial şi $X \subseteq V$, $X \neq \emptyset$. O sumă de forma

$$x = \alpha_1 x_1 + \cdots + \alpha_n x_n\ (\alpha_1, \ldots, \alpha_n \in K,\ x_1, \ldots, x_n \in X)$$

se numeşte **combinaţie liniară** de elemente din X.

Teorema 3.13. Dacă V este un K-spaţiu vectorial şi $\emptyset \neq X \subseteq V$, atunci

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

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

Demonstraţie. Notând cu A membrul doi din (2) avem:

i) $X \subseteq S$,

ii) $x, x' \in A$ şi $\alpha, \beta \in K \Rightarrow \alpha x + \beta x' \in A$,

iii) dacă $X \subseteq B$ şi $B \leq_K V$, atunci $A \subseteq B$.

Din i), ii) şi iii) rezultă că A este cel mai mic subspaţiu care include pe X ceea ce demonstrează pe (2). □

Corolarul 3.14. a) Dacă $x \in V$ atunci $\langle x \rangle = \{\alpha x \mid \alpha \in K\} = Kx$.
b) Dacă $x_1, \ldots, x_n \in V$ atunci $\langle x_1, \ldots, x_n \rangle = Kx_1 + \cdots + Kx_n$.

În general reuniunea a două subspaţii ale unui spaţiu vectorial nu este un subspaţiu.

Exemplul 3.15. Mulţimile $A = \{(a, 0) \mid a \in \mathbb{R}\}$ şi $B = \{(0, b) \mid b \in \mathbb{R}\}$ sunt subspaţii ale $\mathbb{R}$-spaţiului vectorial $\mathbb{R}^2$, dar $A \cup B$ nu este subspaţiu, 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 subspaţiu ce conţine două subspaţii date rezultă din următoarea teoremă.

Teorema 3.16. Fie $A_1, \ldots, A_n$ subspaţii ale K-spaţiului vectorial V. Cel mai mic subspaţiu al lui V ce conţine toate subspaţiile $A_1, \ldots, A_n$ este $A_1 + \cdots + A_n$, adică

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

Demonstraţie. Amintim că

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

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

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

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

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

Din definiţia subspaţiului generat urmează proprietatea din enunţ. □

Corolarul 3.17. a) Dacă A şi B sunt subspaţii ale lui V, atunci

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

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

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

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

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

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

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

Definiţia 3.18. Fie K un corp şi V, V' două K-spaţii vectoriale. O funcţie $f : V \to V'$ se numeşte **transformare liniară** sau **funcţie liniară** sau **aplicaţie liniară** dacă

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

O transformare liniară bijectivă se numeşte **izomorfism** de spaţii liniare. O transformare liniară a unui spaţiu vectorial V în V se numeşte **endomorfism** al lui V. Un izomorfism al lui V pe V se numeşte **automorfism** al lui V.

Observaţiile 3.19. a) O funcţie $f : V \to V'$ este liniară dacă şi numai dacă

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

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) $\alpha_1 = \alpha_2 = 1$ obţinem prima egalitate din (3), iar dacă $\alpha_1 = \alpha$, $x_1 = x$ şi $\alpha_2 = 0$, $x_2 = 0$ primim a doua egalitate din (3). Deci (4) $\Rightarrow$ (3) şi astfel s-a arătat că (3) $\Leftrightarrow$ (4).
b) Dacă $f : V \to V'$ este o transformare liniară, atunci

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

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

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

d) Dacă V, V' şi V'' sunt K-spaţii vectoriale şi $f : V \to V'$, $g : V' \to V''$ sunt transformări liniare, atunci $g \circ f$ este transformare liniară.

Într-adevăr,

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

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

pentru orice $x_1, x_2 \in V$ şi $\alpha_1, \alpha_2 \in K$, ceea ce ne arată că $g \circ f$ este liniară.
e) Dacă $f : V \to V'$ este izomorfism de spaţii vectoriale, atunci f^{-1} este izomorfism de spaţii vectoriale.

Într-adevăr trebuie arătat

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

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-spaţiu vectorial, $End(V,+)$ respectiv $End_K(V)$ mulţimea endomorfismelor grupului $(V,+)$ respectiv K-spaţiului vectorial V. Din Observaţia 3.19 d) rezultă că $End_K(V)$ este stabilă în $(End(V,+),\circ)$, iar $(End_K(V),\circ)$ este monoid.

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

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

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

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

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

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

Exemplele 3.20. a) Pentru orice K-spaţii vectoriale V şi V' funcţia $\theta : V \to V'$, $\theta(x) = 0$ 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 $x_1, x_2 \in V$ şi orice $\alpha_1, \alpha_2 \in K$, ceea ce ne arată că θ este liniară.

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

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

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

adică rotaţia planului de unghi φ, este o transformare liniară.

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

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

este o transformare liniară.

Într-adevăr, pentru orice $f, g \in C(I,\mathbb{R})$ şi $\alpha, \beta \in \mathbb{R}$ 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 şi V' K-spaţii vectoriale. Dacă $f, g : V \to V'$ şi $\alpha \in K$, atunci definim $f + g : V \to V'$ şi $\alpha f : V \to V'$ prin

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

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

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

2) Dacă f este transformare liniară, atunci αf este transformare liniară.

Demonstraţie. 1) Pentru orice $x_1, x_2 \in V$ şi $\alpha_1, \alpha_2 \in K$ avem:

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

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

adică $f+g$ este transformare liniară.
2) Pentru orice $x_1, x_2 \in V$ şi $\beta_1, \beta_2 \in K$ avem:

$$(\alpha f)(\beta_1 x_1+\beta_2 x_2) = \alpha f(\beta_1 x_1+\beta_2 x_2) = \alpha(\beta_1 f(x_1)+\beta_2 f(x_2)) = (\alpha\beta_1) f(x_1)+(\alpha\beta_2) f(x_2) =$$

$$= (\beta_1\alpha) f(x_1)+(\beta_2\alpha) f(x_2) = \beta_1(\alpha f(x_1))+\beta_2(\alpha f(x_2)) = \beta_1(\alpha f)(x_1)+\beta_2(\alpha f)(x_2),$$

adică αf este o transformare liniară. □

Corolarul 3.22. a) Mulţimea $Hom_K(V, V')$ a transformărilor liniare ale lui V în V' este stabilă în raport cu operaţia definită de (6) şi $(Hom_K(V, V'), +)$ este grup abelian.

Într-adevăr din asociativitatea şi comutativitatea operaţiei $+$ în V rezultă asociativitatea şi comutativitatea operaţiei definită în (6). Funcţia $\theta : V \to V'$, $\theta(x) = 0$ este liniară şi θ este element neutru în $Hom_K(V, V')$. Pentru orice $f \in Hom_K(V, V')$ funcţia $-f : V \to V'$, $(-f)(x) = -f(x)$ este liniară şi $-f$ este simetrica lui f în $(Hom_K(V, V'), +)$.
b) Mulţimea $Hom_K(V, V')$ este stabilă în raport cu operaţiile definite în (6) şi (7) şi $Hom_K(V, V')$ este K-spaţiu vectorial în raport cu operaţiile induse de acestea.
c) Grupul abelian $(End_K(V), +)$ este un K-spaţiu vectorial în raport cu operaţia externă definită de (7). Mai mult, compunerea $\circ$ a endomorfismelor K-spatiului vectorial V este distributivă faţă de $+$, prin urmare avem şi o structură de inel cu unitate pe $End_K(V)$, şi anume $(End_K(V), +, \circ)$.

Teorema 3.23. Dacă $f : V \to V'$ este o transformare liniară, atunci:
1) $\operatorname{Ker} f = \{x \in V \mid f(x) = 0\}$ este un subspaţiu al lui V numit **nucleul** lui f.
2) Transformarea liniară f este injectivă dacă şi numai dacă $\operatorname{Ker} f = \{0\}$.

Demonstraţie. 1) Din $f(0) = 0$ rezultă $0 \in \operatorname{Ker} f$, adică $\operatorname{Ker} f \neq \emptyset$. În plus, pentru orice $x_1, x_2 \in \operatorname{Ker} f$ şi $\alpha_1, \alpha_2 \in K$ avem

$$f(\alpha_1 x_1+\alpha_2 x_2) = \alpha_1 f(x_1)+\alpha_2 f(x_2) = \alpha_1 0+\alpha_2 0 = 0$$

de unde urmează $\alpha_1 x_1+\alpha_2 x_2 \in \operatorname{Ker} f$. Deci $\operatorname{Ker} f$ este subspaţiu al lui V.
2) Într-adevăr,

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

ceea ce ne arată că

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

dacă şi numai dacă $\operatorname{Ker} f = \{0\}$, adică dacă şi numai dacă $\operatorname{Ker} f = \{0\}$. □

3.2 Exerciţii rezolvate

1) Poate fi organizată o mulţime finită ca un spaţiu vectorial peste un corp infinit?

Soluţie: Fie V o mulţime finită şi K un corp infinit. Dacă V are un singur element, atunci există o singură structură de K-spaţiu vectorial pe V şi anume spaţiul vectorial nul. Dacă $|V| \geq 2$, presupunând că există o structură de K-spaţiu vectorial pe V şi luând $x \neq 0$, funcţia $t'_x : K \to V$, $t'_x(\alpha) = \alpha x$ este injectivă, deoarece

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

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

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

Soluţie: Din $x \in \langle S, y\rangle$ rezultă că există $s_1, \ldots, s_n \in S$ şi $\alpha_1, \ldots, \alpha_n, \alpha \in K$ astfel încât

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

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

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

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

Soluţie: Fie V_1, V_2, V_3, V_4 subspaţii ale unui K-spaţiu vectorial V cu proprietatea că $V = V_1 \oplus V_2$ şi $V_1 = V_3 \oplus V_4$. 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 $v_2 \in V_1 \cap V_2 = \{0\}$. Obţinem $v_2 = 0$ şi $v_3 = v_4 \in V_3 \cap V_4 = \{0\}$. Aşadar, $V_3 \cap (V_4 + V_2) = \{0\}$ şi 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 $\mathbb{R}$-spaţii vectoriale $f : \mathbb{R}^3 \to \mathbb{R}^2$ astfel încât

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

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

3.3 Baze. Dimensiune

Definiţiile 3.24. Fie V un K-spaţiu vectorial şi $x_1, \ldots, x_n \in V$. Elementele $x_1, \ldots, x_n$ se numesc **liniar independente** dacă

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

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

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

Observaţiile 3.25. a) Vectorii $x_1, \ldots, x_n \in V$ sunt liniar dependenţi dacă şi numai dacă există scalarii $\alpha_1, \ldots, \alpha_n \in K$ nu toţi zero astfel încât

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

b) Dacă unul dintre vectorii $x_1, \ldots, x_n \in V$ este zero, atunci ei sunt liniar dependenţi.
c) Dacă vectorii $x_1, \ldots, x_n \in V$ sunt liniar independenţi, atunci ei sunt doi câte doi diferiţi.
d) Dacă $x \in V$ atunci $\{x\}$ este liberă dacă şi numai dacă $x \neq 0$.
e) Submulţimea vidă $\emptyset \subseteq V$ este liberă.
f) Orice submulţime a unei mulţimi libere este liberă.
g) Dacă submulţimea $X \subseteq V$ are o submulţime legată atunci X este legată. În particular, orice submulţime a lui V care conţine vectorul zero este legată.

Teorema 3.26. Vectorii $x_1, \ldots, x_n \in V$ sunt liniar dependenţi dacă şi numai dacă unul dintre ei este o combinaţie liniară a celorlalţi.

Demonstraţie. Fie $x_1, \ldots, x_n \in V$ liniar dependenţi. Atunci există scalarii $\alpha_1, \ldots, \alpha_n$ din K, nu toţi nuli, de exemplu $\alpha_k \neq 0$, astfel încât

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

de unde rezultă

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

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

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

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

cu $\beta_i \in K$, de unde rezultă

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

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

Corolarul 3.27. a) Dacă $X \subseteq V$, atunci X este legată dacă şi 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 şi 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, $\mathbb{R}$-spaţiul vectorial al vectorilor din plan, respectiv spaţiu (vezi Exemplul 3.5 a)). Doi vectori din V_2 sau V_3 sunt liniar independenţi dacă şi numai dacă nu au aceeaşi direcţie. Orice trei vectori din V_2 sunt liniar dependenţi. Trei vectori din V_3 sunt liniar independenţi dacă şi numai dacă nu sunt coplanari. Orice patru vectori din V_3 sunt liniar dependenţi.

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

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

sunt liniar independenţi pentru că

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

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

Definiţiile 3.29. Fie V un K-spaţiu vectorial. O submulţime $X \subseteq V$ se numeşte **bază** a lui V dacă X este liberă şi X generează pe V, adică $V = \langle X \rangle$.

Teorema 3.30. Fie V un K-spaţiu vectorial. O submulţime X a lui V este bază a lui V dacă şi numai dacă orice vector din V se exprimă într-un singur mod ca şi combinaţie 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 $v = \sum_{x \in X} \alpha_x x$).

Demonstraţie. Condiţia $V = \langle X \rangle$ este echivalentă cu faptul că orice vector din V este o combinaţie liniară de elemente din V, iar faptul că X este liberă este echivalent cu unicitatea acestei reprezentări. □

Exemplele 3.31. a) Orice doi vectori din V_2 (plan) care nu au aceeaşi direcţie formează o bază a lui V_2. Orice trei vectori necoplanari din V_3 (spaţiu) formează o bază a lui V_3.
b) Vectorii $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1)$ formează o bază în K-spaţiul vectorial K^n numită **baza canonică**.
c) Fie K un corp comutativ. Mulţimea $\{X^n \mid n \in \mathbb{N}\}$ este o bază în K-spaţiul vectorial $K[X]$.

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

Demonstraţie. (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 lanţ nevid, în $(\mathcal{C}, \subseteq)$ şi

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

Arătăm că $X_0 \in \mathcal{C}$. Pentru orice $x_1, \ldots, x_n \in X_0$ există $X_1', \ldots, X_n'$ în $\mathcal{C}'$ astfel încât $x_i \in X_i'$ $(i = 1, \ldots, n)$, iar $\mathcal{C}'$ fiind lanţ rezultă că există $i_0 \in \{1, \ldots, n\}$ astfel încât $X_i' \subseteq X_{i_0}'$ $(i = 1, \ldots, n)$ ceea ce implică $x_i \in X_{i_0}'$ $(i = 1, \ldots, n)$. Prin urmare, din $X_{i_0}' \in \mathcal{C}$ deducem că elementele $x_1, \ldots, x_n$ sunt liniar independente. Deci X_0 este liberă şi $X_1 \subseteq X_0 \subseteq X$, adică $X_0 \in \mathcal{C}$ şi 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 $x \in X \setminus \langle X_2 \rangle$ şi 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 $x_i \in X_2$ şi $\alpha, \alpha_i \in K$ $(i = 1, \ldots, n)$ 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 $\alpha_i = 0$ $(i = 1, \ldots, n)$. Deci $X_2 \cup \{x\}$ este liberă. □

Corolarul 3.33. a) Orice spaţiu vectorial V are o bază.

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

b) Orice submulţime liberă a unui spaţiu vectorial V poate fi extinsă la o bază a lui V.

c) O submulţime Y a unui spaţiu vectorial V este o bază a lui V dacă şi numai dacă Y este o submulţime liberă maximală a lui V.

d) Din orice sistem de generatori al unui spaţiu vectorial V se poate extrage o bază a lui V.

e) O submulţime Y a unui spaţiu vectorial V este o bază a lui V dacă şi numai dacă Y este un sistem de generatori minimal al lui V.

f) Dacă X_1 este o submulţime liberă a lui V şi $V = \langle Y \rangle$ 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 spaţiilor vectoriale)

1) Dacă V este un K-spaţiu vectorial şi X o bază a sa, atunci pentru orice K-spaţiu vectorial V' şi orice funcţie $f : X \to V'$ există o singură transformare liniară $\overline{f} : V \to V'$ pentru care $\overline{f}|_X = f$ (cu alte cuvinte $f : X \to V'$ se poate prelungi în mod unic la o transformare liniară $\overline{f} : V \to V'$).

2) Transformarea liniară $\overline{f}$ este injectivă dacă şi numai dacă f este injectivă şi $f(X)$ este liberă.

3) Transformarea liniară $\overline{f}$ este surjectivă dacă şi numai dacă $V' = \langle f(X) \rangle$.

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

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

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

$$\overline{f}(x) = \alpha_1 \overline{f}(x_1) + \cdots + \alpha_n \overline{f}(x_n) = \alpha_1 f(x_1) + \cdots + \alpha_n f(x_n)$$

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

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

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

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

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

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

$$= (\alpha\alpha_1 + \beta\beta_1)f(x_1) + \cdots + (\alpha\alpha_n + \beta\beta_n)f(x_n) =$$

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

ceea ce ne arată că $\overline{f}$ este liniară.
2) Din (1) şi (2) rezultă

$$x \in \operatorname{Ker}\overline{f} \Leftrightarrow \alpha_1 f(x_1) + \cdots + \alpha_n f(x_n) = 0$$

ceea ce ne arată că $\operatorname{Ker}\overline{f} = \{0\}$ (adică $\overline{f}$ este injectivă) dacă şi numai dacă f este injectivă şi $f(X)$ este liberă.
3) Din Observaţia 3.19 h) rezultă $\langle\overline{f}(X)\rangle = \overline{f}(\langle X\rangle) = \overline{f}(V)$, adică $\overline{f}(V) = \langle f(X)\rangle$. Deci $\overline{f}$ este surjectivă dacă şi numai dacă $V' = \langle f(X)\rangle$. □

Corolarul 3.35. a) Dacă X este o bază a spaţiului vectorial V şi $\varphi, \varphi' : V \to V'$ sunt transformări liniare, atunci

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

adică o transformare liniară este determinată de restricţia sa la o bază.
b) Dacă $\varphi : V \to V'$ este o transformare liniară şi X o bază a lui V, atunci φ este izomorfism dacă şi numai dacă $\varphi|_X$ este injectivă şi $\varphi(X)$ este o bază a lui V'.

În Corolarul 3.33 a) am arătat că orice spaţiu vectorial are o bază. În cele ce urmează vom considera că spaţiile vectoriale cu care lucrăm sunt de tip finit. Vom arăta că toate bazele unui spaţiu vectorial V de tip finit au acelaşi cardinal (adică acelaşi număr de elemente). Acest cardinal se numeşte **dimensiunea** lui V. Chiar dacă în acest material nu este inclus cazul spaţiilor vectoriale care au un sistem infinit de generatori, menţionăm că şi în cazul lor toate bazele au acelaşi cardinal, cardinal care este dimensiunea spaţiului. De altfel, cititorul atent va observa că unele demonstraţii ce vor urma se potrivesc şi pentru spaţii vectoriale care nu sunt de dimensiune finită.

Teorema 3.36. (Teorema schimbului (Steinitz))
Fie V un K-spaţiu vectorial. Dacă $x_1, \ldots, x_m$ sunt elementele liniar independente din V şi $V = \langle y_1, \ldots, y_n\rangle$, atunci $m \leq n$ şi după o reindexare convenabilă avem

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

Demonstraţie. Vom utiliza inducţia după m. Pentru $m = 0$ concluzia teoremei este $0 \leq n$ care este adevărată.

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

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

$$x_m = \alpha_1 x_1 + \cdots + \alpha_{m-1}x_{m-1} + \alpha_m y_m + \cdots + \alpha_n y_n.$$

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

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

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

Corolarul 3.37. Toate bazele unui spaţiu vectorial V de tip finit (finit generat) sunt finite şi au acelaşi număr de vectori.

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

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

Observaţiile 3.38. a) Dacă spaţiul vectorial V are dimensiune finită, atunci $\dim V = n$ dacă şi numai dacă există n vectori liniar independenţi şi orice $n+1$ vectori din V sunt liniar dependenţi.

Această afirmaţie rezultă din definiţia $\dim V$ şi din faptul că bazele lui V coincid cu submulţimile independente maximale ale lui V.
b) Dacă spaţiul vectorial V are dimensiune finită şi $\dim V = n$, atunci orice n vectori liniar independenţi din V formează o bază a lui V.
c) Dacă V este un spaţiu vectorial de tip finit şi A este un subspaţiu al lui V, atunci $\dim A \leq \dim V$. Mai mult, $A \neq V$ dacă şi 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 şi numai dacă $X \neq Y$. Cum $\dim V$ este finită, Y este finită şi atunci $X \neq Y$ este echivalentă cu $|X| < |Y|$, adică $\dim A < \dim V$.

Exemplele 3.39. a) Dacă K este un corp comutativ şi $n \in \mathbb{N}^*$, atunci $\dim K^n = n$ pentru că $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1)$ formează o bază a lui K^n.
b) Dacă K este un corp comutativ, atunci $\dim P_n(K) = n+1$ pentru că $1, X, X^2, \ldots, X^n$ formează o bază a K-spaţiului $P_n(K) = \{f \in K[X] \mid \operatorname{grad} f \leq n\}$.
c) Dacă V_1 şi V_2 sunt K-spaţii vectoriale şi X, respectiv Y este o bază a lui V_1, respectiv V_2, atunci se verifică uşor 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 ţinând seama că $|X| = |\{(x, 0) \mid x \in X\}|$, $|Y| = |\{(0, y) \mid y \in Y\}|$ şi $\{(x, 0) \mid x \in X\} \cap \{(0, y) \mid y \in Y\} = \emptyset$ rezultă

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

Teorema 3.40. Două K-spaţii vectoriale V şi V' sunt izomorfe dacă şi numai dacă $\dim V = \dim V'$.

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

$$\alpha_1 y_1 + \cdots + \alpha_n y_n = 0 \Rightarrow \alpha_1 f(x_1) + \cdots + \alpha_n f(x_n) = 0 \Rightarrow f(\alpha_1 x_1 + \cdots + \alpha_n x_n) = f(0) \Rightarrow$$

$$\Rightarrow \alpha_1 x_1 + \cdots + \alpha_n x_n = 0 \Rightarrow \alpha_1 = \cdots = \alpha_n = 0$$

unde $\alpha_1, \ldots, \alpha_n \in K$. 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 $x_1, \ldots, x_n \in X$ şi $\alpha_1, \ldots, \alpha_n \in K$ astfel încât

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

de unde deducem

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

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 funcţia $f' : X \to f(X)$, $f'(x) = f(x)$ 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 şi Y este o bază a lui V', atunci există o bijecţie $g : X \to Y$. Din Teorema 3.34 urmează că g şi g^{-1} se pot prelungi în mod unic la transformările liniare $\overline{g} : V \to V'$ şi $\overline{g^{-1}} : V' \to V$. Rezultă că pentru orice $x \in X$ şi $y \in Y$ avem

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

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

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

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

$$f : K^n \to V,\ f(\alpha_1, \ldots, \alpha_n) = \alpha_1 x_1 + \cdots + \alpha_n x_n$$

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

Teorema 3.42. Dacă V şi V' sunt K-spaţii vectoriale şi $f : V \to V'$ este o transformare liniară, atunci

$$\dim V = \dim \operatorname{Ker} f + \dim f(V). \tag{4}$$

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

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

Deci $f|_{X'} : X' \to f(X')$ este bijecţie, 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 $x_1, \ldots, x_m \in X$, $x'_{m+1}, \ldots, x'_n \in X'$ astfel ca

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

de unde ţinând seama de $\alpha_1 x_1 + \cdots + \alpha_n x_n \in \operatorname{Ker} f$ deducem

$$y = f(x) = f(\alpha_1 x_1 + \cdots + \alpha_m x_m) + \alpha_{m+1} f(x'_{m+1}) + \cdots + \alpha_n f(x'_n) =$$

$$= \alpha_{m+1} f(x'_{m+1}) + \cdots + \alpha_n f(x'_n) \in \langle f(X') \rangle$$

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

$$f(\beta_1 x'_1 + \cdots + \beta_l x'_l) = 0 \Rightarrow \beta_1 x'_1 + \cdots + \beta_l x'_l \in \langle X' \rangle \cap \operatorname{Ker} f = \langle X' \rangle \cap \langle X \rangle = \{0\} \Rightarrow$$

$$\Rightarrow \beta_1 x'_1 + \cdots + \beta_1 x'_l = 0 \Rightarrow \beta_1 = \cdots = \beta_l = 0$$

ceea ce arată că $f(X')$ este liberă. Deci $f(X')$ este o bază a lui $f(V)$ şi $|X'| = |f(X')|$ 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 $\operatorname{Ker} f$ şi $X \cap X' = \emptyset$ implică pe (4). □

Cu notaţiile din teoremă, $\dim \operatorname{Ker} f$ se numeşte **defectul** lui f, iar $\dim f(V)$ se numeşte **rangul** lui f.

Corolarul 3.43. a) Fie V un K-spaţiu vectorial şi A, B subspaţii ale lui V. Atunci

$$\dim A + \dim B = \dim(A \cap B) + \dim(A + B). \tag{5}$$

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

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

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

$$\dim(\operatorname{Ker} f) = \dim(A \cap B), \tag{7}$$

iar din Exemplul 3.39 c) rezultă

$$\dim(A \times B) = \dim A + \dim B. \tag{8}$$

Acum din (6), (7) şi (8) se obţine (5).
b) Dacă V este un K-spaţiu vectorial de dimensiune finită, iar A şi B sunt subspaţii 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-spaţii vectoriale de dimensiune finită şi $\dim V = \dim V'$, iar $f : V \to V'$ este o transformare liniară, atunci sunt echivalente următoarele afirmaţii:
i) f este injectivă;

ii) f este surjectivă;

iii) f este izomorfism.

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

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

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

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

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

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

Aşadar, $\operatorname{Ker} f = \{0\}$, deci f e injectivă.

3.4 Exerciţii rezolvate

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

Soluţie: L este liberă dacă şi numai dacă pentru orice $n_1, \ldots, n_k \in \mathbb{N}$ distincţi, vectorii $f_{n_1}, \ldots, f_{n_k}$ sunt liniar independenţi. Fie $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$ astfel ca $\alpha_1 f_{n_1} + \cdots + \alpha_k f_{n_k} = \theta$ (unde cu θ am notat funcţia identic nulă). Rezultă că

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

de unde deducem că polinomul

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

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

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

Soluţie: V este un subspaţiul 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 $a, b, c \in \mathbb{Q}$ şi $a + b\sqrt[3]{p} + c\sqrt[3]{p^2} = 0$ atunci, prin înmulţire cu $\sqrt[3]{p}$ obţinem $a\sqrt[3]{p} + b\sqrt[3]{p^2} + cp = 0$. Eliminând pe $\sqrt[3]{p^2}$ între cele două egalităţi 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 $c = \dfrac{b^2}{a}$, prin urmare $ab - \dfrac{b^4}{a^2}\sqrt[3]{p} = 0$, adică $\sqrt[3]{p} = \dfrac{b^3}{a^3}$. Aceasta implică $\sqrt[3]{p} = \dfrac{b}{a} \in \mathbb{Q}$, contradicţie cu $\sqrt[3]{p} \notin \mathbb{Q}$. Deci $a = 0$, ceea ce implică şi $b = c = 0$.

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

Soluţie: Din $V_1 \neq V_2$ şi $\dim V_1 = \dim V_2$ rezultă $V_2 \not\subseteq V_1$. Prin urmare

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

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

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

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

4) Fie V un K-spaţiu vectorial de dimensiune $n \in \mathbb{N}^*$ şi V_1, V_2 subspaţii ale lui V. Să se arate că dacă $\dim V_1 = n - 1$ şi $V_2 \nsubseteq V_1$ atunci

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

Soluţie: Din $V_2 \nsubseteq V_1$ 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

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

Aşadar, $\dim(V_1 + V_2) = n = \dim V$, 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 Exerciţii propuse

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

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

şi că acest spaţiu vectorial este izomorf cu $\mathbb{R}$-spaţiul vectorial definit pe $\mathbb{R}$ de operaţiile uzuale de adunare şi înmulţire.
2) Fie V un K-spaţiu vectorial, $\alpha, \beta, \gamma \in K$ şi $x, y, z \in V$ astfel încât $\alpha\gamma \neq 0$ şi

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

Să se arate că $\langle x, y \rangle = \langle y, z \rangle$.
3) În $\mathbb{R}$-spaţiul vectorial $\mathbb{R}^{\mathbb{R}} = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$ considerăm

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

Să se arate că $(\mathbb{R}^{\mathbb{R}})_i$ şi $(\mathbb{R}^{\mathbb{R}})_p$ sunt subspaţii ale lui $\mathbb{R}^{\mathbb{R}}$ şi că $\mathbb{R}^{\mathbb{R}} = (\mathbb{R}^{\mathbb{R}})_i \oplus (\mathbb{R}^{\mathbb{R}})_p$.
4) Fie V un $\mathbb{R}$-spaţiu vectorial şi $v_1, v_2, v_3 \in V$. Să se arate că vectorii v_1, v_2, v_3 sunt liniar independenţi dacă şi numai dacă vectorii $v_2 + v_3, v_3 + v_1, v_1 + v_2$ sunt liniar independenţi.
5) Să se arate că în $\mathbb{R}$-spaţiul vectorial $M_2(\mathbb{R})$ matricele

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

formează o bază şi 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 $\mathbb{Q}$-spaţiul 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 $\mathbb{R}$-spaţiul vecorial $\mathbb{R}^4$ se consideră subspaţiile generate astfel:

a) $S = \langle u_1, u_2, u_3\rangle$, cu $u_1 = (1, 2, 1, -2)$, $u_2 = (2, 3, 1, 0)$, $u_3 = (1, 2, 2, -3)$,
$T = \langle v_1, v_2, v_3\rangle$, 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 $u_1 = (1, 2, 1, 0)$, $u_2 = (-1, 1, 1, 1)$,
$T = \langle v_1, v_2\rangle$, cu $v_1 = (2, -1, 0, 1)$, $v_2 = (1, -1, 3, 7)$;

c) $S = \langle u_1, u_2\rangle$, cu $u_1 = (1, 1, 0, 0)$, $u_2 = (1, 0, 1, 1)$,
$T = \langle v_1, v_2\rangle$, cu $v_1 = (0, 0, 1, 1)$, $v_2 = (0, 1, 1, 0)$;

d) $S = \langle u_1, u_2, u_3\rangle$, cu $u_1 = (1, 2, -1, -2)$, $u_2 = (3, 1, 1, 1)$, $u_3 = (-1, 0, 1, -1)$,
$T = \langle v_1, v_2\rangle$, cu $v_1 = (-1, 2, -7, -3)$, $v_2 = (2, 5, -6, -5)$.

Să se determine câte o bază şi dimensiunea subspaţiilor S, T, $S + T$ şi $S \cap T$.

4 Transformări liniare şi matrici, sisteme de ecuaţii liniare (de Ioan Purdea şi Cosmin Pelea)

4.1 Transformări liniare şi matrici

În acest paragraf vom arăta că studiul transformărilor liniare între două K-spaţii vectoriale V şi V' de tip finit se reduce la studiul matricelor de tipul (m, n) cu elemente din K, unde $m = \dim V'$ şi $n = \dim V$. Menţionăm că în această secţiune, bazele nu vor fi privite doar ca mulţimi ci ca mulţimi ordonate. Astfel, prin **bază** vom înţelege **bază ordonată**.

Fie K un corp comutativ, V şi V' K-spaţii vectoriale de dimansiune finită, $n = \dim V$, $m = \dim V'$ şi $u = (u_1, \ldots, u_n)$ respectiv $v = (v_1, \ldots, v_m)$ o bază a lui V respectiv V'. Fiecare vector $y \in V'$ are o reprezentare unică de forma

$$y = \beta_1 v_1 + \cdots + \beta_m v_m. \tag{1}$$

Scalarii $\beta_1, \ldots, \beta_m$ din (1) se numesc **coordonatele** lui y în baza v.

Dacă $f : V \to V'$ este o transformare liniară, atunci conform Corolarului 3.35 a) f este determinată de restricţia sa la u, adică de $f(u_1), \ldots, f(u_n)$, iar fiecare vector $f(u_j)$ $(j = 1, \ldots, n)$ este determinat de coordonatele sale în baza v.

Deci transformarea liniară f este determinată de scalarii α_{ij}, $1 \le i \le m$, $1 \le j \le n$ din relaţiile

$$\begin{aligned} f(u_1) &= \alpha_{11} v_1 + \alpha_{21} v_2 + \cdots + \alpha_{m1} v_m \\ f(u_2) &= \alpha_{12} v_1 + \alpha_{22} v_2 + \cdots + \alpha_{m2} v_m \\ &\vdots \\ f(u_n) &= \alpha_{1n} v_1 + \alpha_{2n} v_2 + \cdots + \alpha_{mn} v_m. \end{aligned} \tag{2}$$

Notăm cu $[f]_{u,v}$ matricea de tipul (m, n) care are **coloanele** formate din coordonatele

vectorilor $f(u_1), \ldots, f(u_n)$ în baza v, adică

$$[f]_{u,v} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{m1} & \alpha_{m2} & \ldots & \alpha_{mn} \end{pmatrix}.$$

Matricea $[f]_{u,v}$ se numeşte **matricea transformării liniare f în perechea de baze** (u, v). Folosind matrice linie cu elementele vectori, relaţiile (2) se pot scrie astfel:

$$(f(u_1), \ldots, f(u_n)) = (v_1, \ldots, v_m)[f]_{u,v}.$$

Dacă $x \in V$ şi x are coordonatele $\alpha_1, \ldots, \alpha_n$ în baza u, iar $f(x)$ are coordonatele $\beta_1, \ldots, \beta_m$ în baza v, adică

$$x = \alpha_1 u_1 + \cdots + \alpha_n u_n, \ f(x) = \beta_1 v_1 + \cdots + \beta_m v_m$$

atunci

$$\alpha_1 f(u_1) + \cdots + \alpha_n f(u_n) = \beta_1 v_1 + \cdots + \beta_m v_m$$

de unde, folosind pe (2) obţinem

$$\sum_{i=1}^{m} \left(\sum_{j=1}^{n} \alpha_{ij} \alpha_j \right) v_i = \sum_{i=1}^{m} \beta_i v_i. \tag{3}$$

Din (3) şi din unicitatea coordonatelor rezultă

$$\beta_i = \sum_{j=1}^{n} \alpha_{ij} \alpha_j \ (i = 1, \ldots, m) \tag{4}$$

ceea ce ne arată că coordonatele lui $f(x)$ sunt combinaţii liniare ale coordonatelor lui x cu coeficienţii din **liniile** matricei $[f]_{u,v}$. Relaţiile (4) se exprimă matriceal astfel

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_m \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{m1} & \alpha_{m2} & \ldots & \alpha_{mn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Menţionăm că matricea $[f]_{u,v}$ depinde de f, de bazele u, v şi de ordonările acestor baze, iar $\operatorname{rang} f = \operatorname{rang} [f]_{u,v}$.

Exemplele 4.1. a) Fie $P_n(\mathbb{R})$ $\mathbb{R}$ - spaţiul vectorial al polinoamelor de grad cel mult n cu coeficienţii din $\mathbb{R}$. Funcţia

$$\varphi : P_3(\mathbb{R}) \to P_2(\mathbb{R}), \ \varphi(a_0 + a_1 X + a_2 X^2 + a_3 X^3) = a_1 + 2a_2 X + 3a_3 X^2$$

(adică funcţia care asociază unui polinom f derivata formală f' a sa) este o transformare liniară. Vom scrie matricea lui φ în perechile de baze ordonate $u = (1, X, X^2, X^3)$,

$v = (1, X, X^2)$ şi $u = (1, X, X^2, X^3)$, $v' = (X^2, 1, X)$. Avem

$$\varphi(1) = 0 \cdot 1 + 0 \cdot X + 0 \cdot X^2 = 0 \cdot X^2 + 0 \cdot 1 + 0 \cdot X$$
$$\varphi(X) = 1 \cdot 1 + 0 \cdot X + 0 \cdot X^2 = 0 \cdot X^2 + 1 \cdot 1 + 0 \cdot X$$
$$\varphi(X^2) = 0 \cdot 1 + 2 \cdot X + 0 \cdot X^2 = 0 \cdot X^2 + 0 \cdot 1 + 2 \cdot X$$
$$\varphi(X^3) = 0 \cdot 1 + 0 \cdot X + 3 \cdot X^2 = 3 \cdot X^2 + 0 \cdot 1 + 0 \cdot X$$

de unde rezultă

$$[\varphi]_{u,v} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \text{ şi } [\varphi]_{u,v'} = \begin{pmatrix} 0 & 0 & 0 & 3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \end{pmatrix}.$$

b) Fie K un corp comutativ, $m, n \in \mathbb{N}^*$ şi $A \in M_{m,n}(K)$ iar e baza canonică a lui K^n şi e' baza canonică a lui K^m. Scriind vectorii din K^n şi K^m sub formă de matrice coloane se verifică uşor că

$$f_A : K^n \to K^m,\ f_A(x) = Ax$$

este o transformare liniară şi $[f_A]_{e,e'} = A$.

Teorema 4.2. Fie K un corp comutativ, V, V', V'' K-spaţii vectoriale, $f : V \to V'$, $f' : V \to V'$, $g : V' \to V''$ transformări liniare şi $\alpha \in K$.
1) Dacă $u = (u_1, \ldots, u_n)$ şi $v = (v_1, \ldots, v_m)$ sunt baze în V, respectiv V', atunci

$$[f + f']_{u,v} = [f]_{u,v} + [f']_{u,v} \text{ şi } [\alpha f]_{u,v} = \alpha [f]_{u,v}. \tag{5}$$

2) Dacă $w = (w_1, \ldots, w_p)$ este o bază a lui V'', atunci

$$[g \circ f]_{u,w} = [g]_{v,w} \cdot [f]_{u,v}. \tag{6}$$

Demonstraţie. 1) Dacă $[f]_{u,v} = (\alpha_{ij})$, $[f']_{u,v} = (\alpha'_{ij})$ atunci

$$(f + f')(u_j) = f(u_j) + f'(u_j) = \sum_{i=1}^{m} \alpha_{ij} v_i + \sum_{i=1}^{m} \alpha'_{ij} v_i = \sum_{i=1}^{m} (\alpha_{ij} + \alpha'_{ij}) v_i$$

şi

$$(\alpha f)(u_j) = \alpha f(u_j) = \alpha \sum_{i=1}^{m} \alpha_{ij} v_i = \sum_{i=1}^{m} (\alpha \alpha_{ij}) v_i$$

ceea ce demonstrează egalităţile (5).
2) Fie $[g]_{v,w} = (b_{ij})$. Folosind comutativitatea lui K avem

$$(g \circ f)(u_j) = g(f(u_j)) = g\left(\sum_{k=1}^{m} \alpha_{kj} v_k\right) = \sum_{k=1}^{m} \alpha_{kj} g(v_k) =$$

$$= \sum_{k=1}^{m} \alpha_{kj} \sum_{i=1}^{p} \beta_{ik} w_i = \sum_{i=1}^{p} \left(\sum_{k=1}^{m} \beta_{ik} \alpha_{kj}\right) w_i,$$

de unde rezultă (6). □

Corolarul 4.3. a) Aplicaţia

$$\varphi : Hom_K(V, V') \to M_{m,n}(K),\ \varphi(f) = [f]_{u,v}$$

este un izomorfism de K-spaţii vectoriale.

Într-adevăr din (5) urmează că φ este o transformare liniară, iar din Teorema 3.34 rezultă că φ este bijectivă. Deci φ este izomorfism.

b) Aplicaţia

$$\varphi : End_K(V) \to M_n(K),\ \varphi(f) = [f]_{u,u}$$

este un izomorfism de K-spaţii vectoriale şi de inele.

Într-adevăr, din a) urmează că φ este un izomorfism de K-spaţii vectoriale, iar din prima egalitate din (5) şi din (6) rezultă că φ este un izomorfism de inele.

c) Aplicaţia

$$\varphi' : Aut_K(V) \to GL_n(K),\ \varphi'(f) = [f]_{u,u}$$

este un izomorfism de grupuri. Matricea $[f]_{u,u}$ se notează cu $[f]_u$ şi se numeşte **matricea lui f în baza u.**

Această afirmaţie rezultă din b) şi din faptul că un izomorfism între două inele cu unitate păstrează elementele inversabile.

d) Dacă $u = (u_1, \ldots, u_n)$ este o bază a lui V şi $u'_1, \ldots, u'_n \in V$, atunci $u' = (u'_1, \ldots, u'_n)$ este o bază a lui V dacă şi 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

$$u'_j = \sum_{i=1}^{n} s_{ij} u_i \ (j = 1, \ldots, n) \tag{7}$$

adică

$$(u'_1, \ldots, u'_n) = (u_1, \ldots, u_n) \cdot S.$$

Într-adevăr, dacă $f : V \to V$ este endomorfismul definit pe baza u prin $f(u_j) = u'_j$ $(j = 1, \ldots, n)$, atunci din (7) rezultă $S = [f]_u$. Deci u' este o bază dacă şi numai dacă f este un izomorfism ceea ce este echivalent cu S inversabilă. Acum, unicitatea lui S rezultă din bijectivitatea lui φ.

e) Dacă S este matricea de trecere de la baza $u = (u_1, \ldots, u_n)$ la baza $u' = (u'_1, \ldots, u'_n)$, atunci S^{-1} este matricea de trecere de la baza u' la baza u.

f) Fie $u = (u_1, \ldots, u_n)$ şi $u' = (u'_1, \ldots, u'_n)$ baze ordonate ale K-spaţiului vectorial V şi $S = (s_{ij})$ matricea de trecere de la u la u'. Dacă $x \in V$ şi $\alpha_1, \ldots, \alpha_n$ respectiv $\alpha'_1, \ldots, \alpha'_n$ sunt coordonatele lui x în baza u respectiv u', atunci

$$\alpha_i = \sum_{j=1}^{n} s_{ij} \alpha'_j \ (i = 1, \ldots, n), \tag{8}$$

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 dependenţă a matricei $[f]_{u,v}$ de perechea de baze ordonate (u, v).

Teorema 4.4. Fie $u = (u_1, \ldots, u_n)$ şi $u' = (u'_1, \ldots, u'_n)$, respectiv $v = (v_1, \ldots, v_m)$ şi $v' = (v'_1, \ldots, v'_m)$ baze ale K-spaţiului vectorial V, respectiv V'. Dacă S este matricea de trecere de la u la u' şi T este matricea de trecere de la v la v', atunci

$$[f]_{u',v'} = T^{-1} \cdot [f]_{u,v} \cdot S. \tag{9}$$

Demonstraţie. Aşa cum am văzut (în demonstraţia 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 $f = 1_{V'} \circ f \circ 1_V$ şi din (6) deducem pe (9). □

Corolarul 4.5. Fie $u = (u_1, \ldots, u_n)$ şi $u' = (u'_1, \ldots, u'_n)$ baze ale K-spaţiului vectorial V, S este matricea de trecere de la u la u' şi $f : V \to V$ este un endomorfism. Atunci

$$[f]_{u'} = S^{-1} \cdot [f]_u \cdot S.$$

4.2 Exerciţii rezolvate

1) Fie $v = ((1, 2), (-2, 1))$ şi $v' = ((1, -1, 0), (-1, 0, 1), (1, 1, 1))$. Să se arate că v, respectiv v' este bază în $\mathbb{R}^2$, respectiv $\mathbb{R}^3$ şi să se scrie matricea tranformării liniare $f : \mathbb{R}^2 \to \mathbb{R}^3$, $f(x, y) = (x + y, 2x - y, 3x + 2y)$ în perechea de baze (v, v').

Soluţie: 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 $\mathbb{R}^2$ şi v' este bază în $\mathbb{R}^3$. Coloanele matricei $[f]_{v,v'} = (a_{ij}) \in M_{3,2}(\mathbb{R})$ rezultă din egalităţile

$$(3, 0, 7) = f(1, 2) = a_{11}(1, -1, 0) + a_{21}(-1, 0, 1) + a_{31}(1, 1, 1),$$
$$(-1, -5, -4) = f(-2, 1) = a_{12}(1, -1, 0) + a_{22}(-1, 0, 1) + a_{32}(1, 1, 1).$$

Cele două egalităţi conduc la sistemele

$$\begin{cases} a_{11} - a_{21} + a_{31} = 3 \\ -a_{11} \quad + a_{31} = 0 \\ a_{21} + a_{31} = 7 \end{cases} \text{ şi } \begin{cases} a_{12} - a_{22} + a_{32} = -1 \\ -a_{12} \quad + a_{32} = -5 \\ a_{22} + a_{32} = -4 \end{cases}$$

care au, respectiv, soluţiile $\left(\frac{10}{3}, \frac{11}{3}, \frac{10}{3}\right)$ şi $\left(\frac{5}{3}, -\frac{2}{3}, -\frac{10}{3}\right)$. 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 soluţie: 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 $f(1,2)$ şi $f(-2,1)$ 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 $f : \mathbb{R}^3 \to \mathbb{R}^4$ aplicaţia 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 $\operatorname{Im} f$ şi $\operatorname{Ker} f$.

Soluţie: 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 şi coloane pe $f(e_1)$, $f(e_2)$ şi $f(e_3)$, respectiv, adică

$$\begin{pmatrix} 1 & 4 & -2 \\ 2 & 3 & 1 \\ 3 & 2 & 4 \\ 4 & 1 & 1 \end{pmatrix}.$$

iii) $\operatorname{Im} f = f(\langle e_1, e_2, e_3\rangle) = \langle f(e_1), f(e_2), f(e_3)\rangle$, deci

$$\dim(\operatorname{Im} f) = \operatorname{rang} \begin{pmatrix} 1 & 4 & -2 \\ 2 & 3 & 1 \\ 3 & 2 & 4 \\ 4 & 1 & 1 \end{pmatrix} = 3,$$

prin urmare $f(e_1)$, $f(e_2)$ şi $f(e_3)$ formează o bază în $\operatorname{Im} f$. Atunci

$$\dim(\operatorname{Ker} f) = \dim \mathbb{R}^3 - \dim(\operatorname{Im} f) = 3 - 3 = 0,$$

deci $\operatorname{Ker} f = \{(0,0,0)\}$ şi $\emptyset$ este bază în $\operatorname{Ker} f$.

3) Fie V, V' $\mathbb{R}$-spaţii vectoriale, $v = (v_1, v_2, v_3)$ o bază în V, $v' = (v'_1, v'_2, v'_3)$ o bază în V' şi $f : V \to V'$ transformarea liniară cu

$$[f]_{v,v'} = \begin{pmatrix} 0 & -1 & 5 \\ 1 & 0 & 0 \\ 0 & 1 & -5 \end{pmatrix}.$$

Să se determine:
i) dimensiunea şi câte o bază pentru $\operatorname{Im} f$ şi $\operatorname{Ker} f$;
ii) $[f]_{v,e'}$ în cazul în care $V' = \mathbb{R}^3$, $v'_1 = (1,0,0)$, $v'_2 = (0,1,1)$, $v'_3 = (0,0,1)$ şi e' este baza canonică a lui $\mathbb{R}^3$;
iii) $f(x)$ pentru $x = 2v_1 - v_2 + 3v_3$, în condiţiile de la ii).

Soluţie: 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

$$f(v_1) = v_2',\ f(v_2) = -v_1' + v_3' \text{ şi } f(v_3) = 5v_1' - 5v_3'.$$

Atunci $\dim(\mathrm{Im}\, f) = \mathrm{rang}[f]_{v,v'} = 2$, iar un minor nenul de ordinul 2 al matricii $[f]_{v,v'}$ poate fi decupat din primele 2 coloane (şi primele 2 linii), prin urmare, $f(v_1)$ şi $f(v_2)$ formează o bază în $\mathrm{Im}\, f$. Deducem că

$$\dim(\mathrm{Ker} f) = \dim V - \dim(\mathrm{Im} f) = 3 - 2 = 1,$$

iar cum coloanele 2 şi 3 ale matricii $[f]_{v,v'}$ sunt proporţionale, avem

$$f(v_3) = -5f(v_2) \Leftrightarrow f(v_3 - 5v_2) = 0 \Leftrightarrow v_3 - 5v_2 \in \mathrm{Ker}\, f.$$

Prin urmare, $v_3 - 5v_2$ formează o bază în $\mathrm{Ker} f$.
ii) Matricea de trecere de la baza canonică e' la baza v' este matricea T care are ca şi 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 $f \in End_{\mathbb{Q}}(\mathbb{Q}^4)$ 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 $\mathrm{Ker}\, f$ şi $\mathrm{Im}\, f$.

Soluţie: 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 şi a dimensiunii lui $\mathrm{Im}\, f$ se calculează rangul matricei $[f]_e$, urmărind din ce coloane a fost „decupat" un minor nenul de ordin egal cu $\mathrm{rang}[f]_e$. Obţinem $\dim(\mathrm{Im}\, f) = 3$, în consecinţă, $\dim(\mathrm{Ker}\, f) = 1$. Pentru determinarea unei baze în $\mathrm{Ker}\, f$ 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 matricei date care este chiar $f(e_i)$), fie se procedează astfel:

$$(x_1, x_2, x_3, x_4) \in \mathrm{Ker} f \Leftrightarrow [f]_e \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{cases} x_1 + 2x_2 + x_3 + 2x_4 = 0 \\ 3x_1 + 2x_2 + 3x_3 + 2x_4 = 0 \\ -x_1 - 3x_2 + 4x_4 = 0 \\ +4x_2 - x_3 - 3x_4 = 0 \end{cases}.$$

Mulţimea soluţiilor acestui sistem de ecuaţii 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 $\mathrm{Ker}\, f$.

4.3 Sisteme de ecuaţii liniare

Pentru o bună înţelegere a acestei secţiuni, recomandăm cititorilor să îşi reamintească definiţiile şi proprietăţile determinanţilor, precum şi ale rangului unei matrice. Pentru a veni în sprijinul lor în acest sens, vom prezenta câteva astfel de proprietăţi care vor apărea în discuţiile 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} şi $\alpha_{ij} = (-1)^{i+j} d_{ij}$ complementul algebric al elementului a_{ij}. Au loc următoarele:
1) Determinantul matricei A este egal cu determinantul matricei transpuse ${}^tA$.
2) Dacă matricea B se obţine din A prin înmulţirea fiecărui element dintr-o linie (coloană) a lui A cu un scalar α atunci $\det(B) = \alpha \det(A)$.
3) Dacă A are două linii (coloane) egale, atunci $\det(A) = 0$.
4) Dacă matricea B se obţine 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 obţine din A prin adunarea la linia (coloana) i a liniei (coloanei) j, cu $i \neq j$, înmulţită cu un scalar, atunci $\det B = \det A$.
7) Dacă o linie (coloană) a lui A este o combinaţie 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**)**

$$\det(A) = a_{i1}\alpha_{i1} + a_{i2}\alpha_{i2} + \cdots + a_{in}\alpha_{in}, \ \forall i \in \{1, \ldots, n\}.$$

10) **(dezvoltarea determinantului** $\det(A)$ **după coloana** j**)**

$$\det A = a_{1j}\alpha_{1j} + a_{2j}\alpha_{2j} + \cdots + a_{nj}\alpha_{nj}, \ \forall j \in \{1, \ldots, n\}.$$

11) Dacă $i, k \in \{1, \ldots, n\}$, $i \neq k$, atunci

$$a_{i1}\alpha_{k1} + a_{i2}\alpha_{k2} + \cdots + a_{in}\alpha_{in} = 0.$$

12) Dacă $j, k \in \{1, \ldots, n\}$, $j \neq k$ 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 şi numai dacă $d = \det(A) \neq 0$. În acest caz

$$A^{-1} = d^{-1} \cdot A^*.$$

Demonstraţie. 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) şi 12) urmează

$$A^* \cdot A = d \cdot I_n = A \cdot A^*$$

de unde deducem că dacă $d \neq 0$, atunci A este inversabilă şi $A^{-1} = d^{-1} \cdot A^*$. □

De asemenea, proprietăţile de mai sus permit stabilirea următoarei legături între rangul unei matrici şi dimensiunea subspaţiului generat de liniile (coloanele) sale.

Teorema 4.7. Dacă $A \in M_{m,n}(K)$ şi $l_1^A, \ldots, l_m^A \in K^n$ respectiv $c_1^A, \ldots, c_n^A \in K^m$ sunt liniile respectiv coloanele lui A, atunci

$$\operatorname{rang} A = \dim\langle l_1^A, \ldots, l_m^A\rangle = \dim\langle c_1^A, \ldots, c_n^A\rangle.$$

unde $\langle l_1^A, \ldots, l_m^A\rangle$, respectiv $\langle c_1^A, \ldots, c_n^A\rangle$ este subspaţiul lui K^n, respectiv K^m generat de $l_1^A, \ldots, l_m^A$, respectiv $c_1^A, \ldots, c_n^A$.

Demonstraţie. Fie $r = \operatorname{rang} A$. Rezultă că A are un minor de ordinul r nenul, pentru a nu complica notaţiile, presupunem că

$$d = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1r} \\ a_{21} & a_{22} & \ldots & a_{2r} \\ \vdots & \vdots & & \vdots \\ a_{r1} & a_{r2} & \ldots & a_{rr} \end{vmatrix} \neq 0$$

şi orice minor de ordinul $r+1$ este zero. Prin urmare determinantul

$$D_{ij} = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1r} & a_{1j} \\ a_{21} & a_{22} & \ldots & a_{2r} & a_{2j} \\ \vdots & \vdots & & \vdots & \vdots \\ a_{r1} & a_{r2} & \ldots & a_{rr} & a_{rj} \\ a_{i1} & a_{i2} & \ldots & a_{ir} & a_{ij} \end{vmatrix}$$

de ordinul $r+1$, obţinut prin adăugarea la d a liniei i şi a coloanei j, cu $1 \leq i \leq m$ şi $r < j \leq n$, este zero, adică $D_{ij} = 0$. Dacă $r < i \leq m$ şi $r < j \leq n$, atunci spunem că D_{ij} se obţine din d prin **bordarea** lui d cu linia i şi coloana j. Dezvoltând determinantul D_{ij} după linia $r+1$ primim

$$a_{i1}d_1 + a_{i2}d_2 + \cdots + a_{ir}d_r + a_{ij}d = 0$$

unde complementii algebrici $d_1, d_2, \ldots, d_r$ nu depind de linia adăugată. Rezultă

$$a_{ij} = -d^{-1}d_1a_{i1} - d^{-1}d_2a_{i2} - \cdots - d^{-1}d_ra_{ir}$$

pentru $i = 1, 2, \ldots, m$ şi $j = r+1, \ldots, n$ ceea ce ne arată că

$$c_j^A = \alpha_1 c_1^A + \alpha_2 c_2^A + \cdots + \alpha_r c_r^A \text{ pentru } j = r+1, \ldots, n,$$

unde $\alpha_k = -d^{-1}d_k$, $1 \leq k \leq r$, adică c_j^A este combinaţie liniară de $c_1^A, c_2^A, \ldots, c_r^A$. Astfel am arătat că $\dim\langle c_1^A, \ldots, c_n^A\rangle \leq r$. Dacă am avea $\dim\langle c_1^A, \ldots, c_r^A\rangle < r$ ar rezulta că una dintre coloanele $c_1^A, \ldots, c_r^A$ ar fi o combinaţie liniară a celorlalte, ceea ce ar implica $d = 0$ ceea ce este fals. Astfel am arătat că $\dim\langle c_1^A, \ldots, c_1^A\rangle = r$. De aici şi din $\operatorname{rang} A = \operatorname{rang}\ {}^tA$ rezultă $\dim\langle l_1^A, \ldots, l_n^A\rangle = r$. □

Corolarul 4.8. a) Rangul lui A coincide cu numărul maxim de linii (coloane) liniar independente ale lui A.
b) Dacă un determinant d de ordinul r este nenul, iar un determinant D obţinut din d prin adăugarea unei linii şi unei coloane este nul atunci coloana (linia) adăugată este o combinaţie liniară a celorlalte coloane (linii) din D.

Fie K un corp comutativ. Un sistem de ecuaţii de forma

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{1}$$

unde $a_{ij} \in K$, $i = 1, \ldots, m$, $j = 1, \ldots, n$, $b_j \in K$, $j = 1, \ldots, n$ şi $x_1, \ldots, x_n$ sunt necunoscute se numeşte **sistem de ecuaţii liniare** cu m ecuaţii cu n necunoscute. Matricea

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

de tipul (m, n), formată din coeficienţii necunoscutelor, se numeşte **matricea sistemului**, iar matricea

$$\overline{A} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_m \end{pmatrix}$$

de tipul $(m, n+1)$ obţinută din A prin adăugarea coloanei

$$B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

formată din termenii liberi se numeşte **matricea extinsă a sistemului**. Rangul matricei A se numeşte **rangul sistemului**. Dacă toţi termenii liberi sunt zero, adică $b_1 = b_2 = \cdots = b_m = 0$, atunci sistemul (1) se numeşte **sistem liniar şi omogen**. Notând

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

sistemul (1) se scrie sub formă de ecuaţie matriceală, astfel:

$$AX = B \tag{2}$$

Sistemul de ecuaţii $AX = O_{m,1}$ se numeşte **sistemul omogen asociat** sistemului (2).

Un sistem ordonat $(\alpha_1, \ldots, \alpha_n) \in K^n$ se numeşte **soluţie a sistemului** (1) dacă înlocuind în (1) pe x_i cu α_i pentru $i = 1, \ldots, n$ ecuaţiile sistemului sunt verificate, adică au loc în K egalităţile:

$$\sum_{j=1}^{n} a_{ij}\alpha_j = b_j, \ \forall\, j \in \{1, \ldots, m\}.$$

Un sistem de ecuaţii care are cel puţin o soluţie se numeşte **compatibil**. Un sistem de ecuaţii care are o singură soluţie respectiv mai multe soluţii se numeşte **compatibil determinat** respectiv **compatibil nedeterminat**. Un sistem de ecuaţii care nu are soluţii se numeşte **incompatibil**.

Dacă sistemul (1) este omogen, atunci $(0, 0, \ldots, 0) \in K^n$ e soluţie a sistemului, numită **soluţia nulă** sau **soluţia banală**. Deci orice sistem liniar şi omogen este compatibil.

În cazul $m = n$ şi $\det(A) \neq 0$ vom vedea că sistemul (1) este compatibil determinat, adică are soluţie unică şi vom prezenta formule pentru determinarea acestora.

Teorema 4.9. (Regula lui Cramer). Fie sistemul de n ecuaţii cu n necunoscute

$$(S)\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_n \end{cases}$$

cu $A = (a_{ij}) \in M_n(K)$ şi $b_1, \ldots, b_n \in K$, $d = \det(A)$ şi d_j determinantul obţinut din d prin înlocuirea coloanei j cu coloana formată din $b_1, \ldots, b_n$. Dacă $d \neq 0$ atunci sistemul (S) are o soluţie unică, dată de formulele:

$$\begin{cases} x_1 = d_1 \cdot d^{-1} \\ x_2 = d_2 \cdot d^{-1} \\ \vdots \\ x_n = d_n \cdot d^{-1} \end{cases}$$

numite **formulele lui Cramer**.

Demonstraţie. Sistemul (S) este echivalent cu ecuaţia matriceală

$$A \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

de unde, întrucât $d \neq 0$, folosind Teorema 4.6 şi (10) avem

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = A^{-1} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = d^{-1} \cdot A^* \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = d^{-1} \cdot \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix}$$

de unde se deduc formulele din enunţ. □

Teorema următoare rezolvă problema compatibilităţii sau incompatibilităţii unui sistem de ecuaţii liniare.

Teorema 4.10. (Kronecker-Cappelli) Sistemul (1) este compatibil dacă şi numai dacă rangul matricei sistemului este egal cu rangul matricei extinse, adică $\operatorname{rang} A = \operatorname{rang} \overline{A}$.

Demonstraţie. Notând cu $c_1^A, \ldots, c_n^A$ coloanele matricei A şi cu $c_{n+1}^{\overline{A}}$ ultima coloană a lui $\overline{A}$, adică $c_{n+1}^{\overline{A}} = B$, atunci $A = (c_1^A, \ldots, c_n^A)$ şi $\overline{A} = (c_1^A, \ldots, c_n^A, c_{n+1}^{\overline{A}})$ iar sistemul (1) se poate scrie sub formă vectorială astfel:

$$x_1 c_1^A + \cdots + x_n c_n^A = c_{n+1}^{\overline{A}} \tag{3}$$

ceea ce ne arată că sistemul (1) este compatibil dacă şi numai dacă vectorul $c_{n+1}^{\overline{A}}$ este o combinaţie liniară a vectorilor $c_1^A, \ldots, c_n^A$. Egalitatea de vectori (3) este echivalentă cu egalitatea

$$\langle c_1^A, \ldots, c_n^A \rangle = \langle c_1^A, \ldots, c_n^A, c_{n+1}^{\overline{A}} \rangle$$

de subspaţii generate, care la rândul ei este echivalentă cu

$$\dim\langle c_1^A, \ldots, c_n^A \rangle = \dim\langle c_1^A, \ldots, c_n^A, c_{n+1}^{\overline{A}} \rangle.$$

De aici, folosind Teorema 4.7, rezultă că sistemul (1) este compatibil dacă şi numai dacă $\operatorname{rang} A = \operatorname{rang} \overline{A}$. □

Dacă $\operatorname{rang} A = r$ atunci există în A un minor de ordinul r nenul şi toţi minorii din A de ordin mai mare decât r sunt nuli. Un minor al lui A de ordinul r nenul se numeşte **minor principal**. Dacă d_p este un minor principal, atunci minorii de ordinul $r+1$ obţinuţi prin bordarea lui d_p cu coloana termenilor liberi şi 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 obţine $\overline{A}$ din A şi ştiind că rangul unei matrici este r dacă şi numai dacă are un minor de ordinul r nenul şi toţi minorii de ordinul $r+1$ care bordează acest minor sunt zero, rezultă că $\operatorname{rang} A = \operatorname{rang} \overline{A}$ dacă şi numai dacă toţi minorii caracteristici sunt nuli. Prin urmare, Teorema lui Kronecker-Cappelli este echivalentă cu:

Teorema 4.11. (Rouché) Sistemul (1) este compatibil dacă şi numai dacă toţi minorii caracteristici corespunzători unui minor principal sunt nuli.

Teorema 4.12. 1) Mulţimea soluţiilor unui sistem liniar şi omogen de m ecuaţii cu n necunoscute formează un subspaţiu al lui K^n de dimensiune $n - r$, unde r este rangul matricei sistemului.
2) Dacă S_0 este mulţimea soluţiilor sistemului liniar şi omogen asociat lui (1) şi S_B este mulţimea soluţiilor sistemului (1), atunci

$$S_B = s + S_0 \tag{4}$$

unde s este o soluţie a sistemului (1).

Demonstraţie. 1) Dacă $A \in M_{m,n}(K)$, atunci

$$f_A : K^n \to K^m,\ f_A(X) = AX$$

este o transformare liniară şi mulţimea S_0 a soluţiilor sistemului omogen $AX = O_{m,1}$ coincide cu $\operatorname{Ker} f_A$. Deci S_0 este subspaţiu a lui K^n. Din Teorema 3.42 rezultă

$$\dim K^n = \dim \operatorname{Ker} f_A + \dim f_A(K^n)$$

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 soluţie 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). □

Corolarul 4.13. a) Un sistem liniar şi omogen are numai soluţia nulă dacă şi numai dacă numărul necunoscutelor este egal cu rangul sistemului.
b) Un sistem liniar şi omogen de n ecuaţii cu n necunoscute are numai soluţia nulă dacă şi numai dacă determinantul matricei sistemului este diferit de zero.
c) Dacă sistemul (1) este compatibil, atunci acesta are soluţie unică dacă şi numai dacă $\operatorname{rang} A = n$, 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 şi procedeul se încheie. Dacă toţi minorii caracteristici sunt nuli, atunci sistemul este compatibil. Dacă d_p este un minor principal şi ordinul lui d_p este r atunci cele r ecuaţii care ne dau liniile lui d_p se numesc **ecuaţii principale**, iar necunoscutele ale căror coeficienţi intervin în d_p se numesc **necunoscute principale**. Celelalte $m - r$ ecuaţii şi $n - r$ necunoscute se numesc **secundare**. Din $\operatorname{rang} \overline{A} = \operatorname{rang} A = r$, rezultă, conform Corolarului 4.8 b), că ecuaţiile secundare sunt combinaţii liniare a ecuaţiilor principale. Prin urmare sistemul (1) are aceleaşi soluţii ca şi sistemul format numai din ecuaţiile principale, adică cele două sisteme sunt echivalente. Pentru simplificarea scrierii

presupunem că primele r ecuaţii şi r necunoscute sunt principale. Deci sistemul (1) este echivalent cu sistemul

$$\begin{cases} a_{11}x_1 + x_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + x_{22}x_2 + \cdots + a_{2n}x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{r1}x_1 + x_{r2}x_2 + \cdots + a_{rn}x_n = b_r \end{cases} \tag{5}$$

Dacă $n = r$, adică toate necunoscutele sunt principale, atunci sistemul (4) are numărul ecuaţiilor egal cu numărul necunoscutelor şi determinantul $d_p \neq 0$. În acest caz sistemul are o soluţie unică, care se poate determina cu formulele lui Cramer.

Dacă $n > r$, necunoscutele secundare $x_{r+1}, \ldots, x_n$ iau valori arbitrare $\alpha_{r+1}, \ldots, \alpha_n$ în K, iar necunoscutele principale se obţin, în funcţie de acestea, rezolvând sistemul de r ecuaţii cu r necunoscute

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1r}x_r = b_1 - a_{1,r+1}\alpha_{r+1} - \cdots - a_{1n}\alpha_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2r}x_r = b_2 - a_{2,r+1}\alpha_{r+1} - \cdots - a_{2n}\alpha_n \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{r1}x_1 + a_{r2}x_2 + \cdots + a_{rr}x_r = b_r - a_{r,r+1}\alpha_{r+1} - \cdots - a_{rn}\alpha_n \end{cases}$$

cu determinantul $d_p \neq 0$.

2. Metoda lui Gauss este o metodă de stabilire a compatibilităţii sau incompatibilităţii şi de rezolvare în caz de compatibilitate a unui sistem de ecuaţii liniare care se bazează pe observaţia că aplicând transformări elementare ecuaţiilor din sistemul (1) se obţin sisteme echivalente cu (1).

Vom numi **transformări elementare asupra** liniilor (coloanelor) **unei matrici** A următoarele:

I) permutarea a două linii (coloane) ale lui A;

II) înmulţirea unei linii (coloane) ale lui A cu un scalar nenul;

III) înmulţirea unei linii (coloane) ale lui A cu un scalar şi adunarea la alta.

Metoda constă în efectuarea de tranformări elementare succesive asupra liniilor matricei extinse $\overline{A}$ a sistemului (1) de ecuaţii liniare cu scopul de a aduce această matrice la o formă trapezoidală B, adică o formă în care numărul de zerouri de la începutul liniei k e este $k-1$ sau toate elementele dintr-o linie sunt 0 exceptând, eventual, pe cel din ultima coloană. Acest fapt corespunde eliminării parţiale a unor necunoscute din sistem prin efectuarea de transformări asupra ecuaţiilor din sistem cu scopul de a obţine un sistem echivalent mai uşor de rezolvat (în mod asemănător cu binecunoscuta metodă a reducerii de la sistemele de 2 ecuaţii cu 2 necunoscute). Fiecărei matrici obţinute prin astfel de tranformări îi corespunde un sistem echivalent cu sistemul dat.

Aplicând transformări elementare exclusiv asupra liniilor matricei extinse $\overline{A}$, aducem sistemul (1) la un sistem echivalent cu (1) care are matricea extinsă de forma numită **eşalon** cu $k \leq m$ linii nenule caracterizată de proprietăţile:

i) Dacă $k < m$, atunci liniile $k+1, \ldots, m$ sunt nule.

ii) Dacă $n_0(i)$ reprezintă numărul elementelor nule de la începutul liniei i, atunci

$$0 \leq n_0(1) < n_0(2) < \cdots < n_0(k).$$

Aşa cum se va observa în Exerciţiul rezolvat 2), sunt cazuri în care putem lucra foarte bine cu forma eşalon. Dacă, însă, dorim să ajungem la forma trapezoidală B, este necesar uneori să permutăm câte 2 coloane ale matricii obţinute din matricea sistemului, ceea ce corespunde permutării a câte doi termeni în fiecare din ecuaţiile sistemului echivalent corespunzător.

Dacă pe parcursul acestui procedeu, apare într-o linie a unei matrici 0 în toate poziţiile corespunzătoare matricii sistemului şi un element nenul a în ultima poziţie, adică în coloana corespunzătoare termenilor liberi atunci sistemul dat este incompatibil, ecuaţia corespunzătoare din sistemul echivalent corespunzător fiind $0 = a$.

Elementele nenule de pe diagonala lui B furnizează necunoscutele principale, iar sistemul obţinut prin parametrizarea necunoscutelor secundare se rezolvă începând cu ultima ecuaţie.

4.4 Exerciţii rezolvate

1) Să se rezolve în $\mathbb{R}^3$ sistemul de ecuaţii

$$\begin{cases} x_1 + x_2 + 2x_3 = -1 \\ 2x_1 - x_2 + 2x_3 = -4 \\ 4x_1 + x_2 + 4x_3 = -2. \end{cases}$$

Soluţie: **Metoda I** (cu metoda lui Gauss) Matricea extinsă a sistemului este

$$\overline{A} = \left(\begin{array}{ccc|c} 1 & 1 & 2 & -1 \\ 2 & -1 & 2 & -4 \\ 4 & 1 & 4 & -2 \end{array}\right)$$

Scăzând din linia 2 linia 1 înmulţită cu 2, ceea ce vom nota cu $l_2 - 2l_1$, iar din linia 3 linia 1 înmulţită cu 4 obţinem matricea

$$\overline{A}_1 = \left(\begin{array}{ccc|c} 1 & 1 & 2 & -1 \\ 0 & -3 & -2 & -2 \\ 0 & -3 & -4 & 2 \end{array}\right)$$

Continuând cu transformarea $l_3 - l_2$ ajungem la matricea eşalon:

$$\overline{A}_2 = \left(\begin{array}{ccc|c} 1 & 1 & 2 & -1 \\ 0 & -3 & -2 & -2 \\ 0 & 0 & -2 & 4 \end{array}\right)$$

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 soluţie unică, din ultima ecuaţie obţinem $x_3 = -2$, din a doua $x_2 = 2$, iar din prima $x_1 = 1$. Deci sistemul are soluţia $(1, 2, -2)$.

Dacă în $\overline{A}_2$ continuăm cu transformările

$$\overline{A}_2 \overset{\substack{l_2-l_3\\ l_1+l_3}}{\sim} \begin{pmatrix} 1 & 1 & 0 & 3 \\ 0 & -3 & 0 & -6 \\ 0 & 0 & -2 & 4 \end{pmatrix} \overset{l_1+\frac{1}{3}l_2}{\sim} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & -3 & 0 & -6 \\ 0 & 0 & -2 & 4 \end{pmatrix}$$

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 soluţia.

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 şi soluţia sa este dată de formulele lui Cramer. Lăsăm calculele în seama cititorului.

2) Să se rezolve în $\mathbb{R}^4$ sistemul de ecuaţii

$$\begin{cases} 3x_1 + 4x_2 + x_3 + 2x_4 = 3 \\ 6x_1 + 8x_2 + 2x_3 + 5x_4 = 7 \\ 9x_1 + 12x_2 + 3x_3 + 10x_4 = 13 \end{cases}$$

Soluţie: **Metoda I** (cu metoda lui Gauss)

Scriem matricea extinsă a sistemului şi efectuăm transformările elementare indicate

$$\overline{A} = \left(\begin{array}{cccc|c} 3 & 4 & 1 & 2 & 3 \\ 6 & 8 & 2 & 5 & 7 \\ 9 & 12 & 3 & 10 & 13 \end{array}\right) \overset{\substack{l_2-2l_1\\ l_3-3l_1}}{\sim} \left(\begin{array}{cccc|c} 3 & 4 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 4 & 4 \end{array}\right)$$

$$\overset{l_3-4l_2}{\sim} \left(\begin{array}{cccc|c} 3 & 4 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

ceea ce ne arată că sistemul este echivalent cu

$$\begin{cases} 3x_1 + 4x_2 + x_3 + 2x_4 = 3 \\ x_4 = 1 \end{cases}$$

şi x_1, x_4 sunt necunoscute principale. Rezultă că sistemul dat are soluţiile:

$$\left(\frac{1}{3}(1 - 4\alpha - \beta), \alpha, \beta, 1\right) \text{ cu } \alpha, \beta \in \mathbb{R}.$$

Metoda II (cu Teorema lui Rouché) Avem

$$\begin{vmatrix} 1 & 2 \\ 2 & 5 \end{vmatrix} = 1 \text{ şi } \begin{vmatrix} 3 & 1 & 2 \\ 6 & 2 & 5 \\ 9 & 3 & 10 \end{vmatrix} = \begin{vmatrix} 4 & 1 & 2 \\ 8 & 2 & 5 \\ 12 & 3 & 10 \end{vmatrix} = 0$$

(având primele 2 coloane proporţionale). 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 şi 2. Aşadar, 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 ecuaţii cu 2 necunoscute este un exerciţiu simplu, pe care îl lăsăm cititorului.

3) Să se rezolve, în $\mathbb{R}^3$, sistemul de ecuaţii

$$\begin{cases} x_1 + x_2 - 3x_3 = -1 \\ 2x_1 + x_2 - 2x_3 = 1 \\ x_1 + x_2 + x_3 = 3 \\ x_1 + 2x_2 - 3x_3 = 1 \end{cases}$$

Soluţie: **Metoda I** (cu metoda lui Gauss)

$$\overline{A} = \left(\begin{array}{ccc|c} 1 & 1 & -3 & -1 \\ 2 & 1 & -2 & 1 \\ 1 & 1 & 1 & 3 \\ 1 & 2 & -3 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & -3 & -1 \\ 0 & -1 & 4 & 3 \\ 0 & 0 & 4 & 4 \\ 0 & 1 & 0 & 2 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|c} 1 & 1 & -3 & -1 \\ 0 & -1 & 4 & 3 \\ 0 & 0 & 4 & 4 \\ 0 & 0 & 4 & 5 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & -3 & -1 \\ 0 & -1 & 4 & 3 \\ 0 & 0 & 4 & 4 \\ 0 & 0 & 0 & 1 \end{array}\right).$$

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)

Avem $\begin{vmatrix} 1 & 1 & -3 \\ 2 & 1 & -2 \\ 1 & 1 & 1 \end{vmatrix} = -4 \neq 0$, iar minorul caracteristic $\begin{vmatrix} 1 & 1 & -3 & -1 \\ 2 & 1 & -2 & 1 \\ 1 & 1 & 1 & 3 \\ 1 & 2 & -3 & 1 \end{vmatrix} = -4$ fiind nenul, sistemul este incompatibil.

4) Să se discute după parametrul real α compatibilitatea sistemului de mai jos, apoi să se rezolve în $\mathbb{R}^4$:

$$\begin{cases} 2x_1 - x_2 + 3x_3 + 4x_4 = 5 \\ 4x_1 - 2x_2 + 5x_3 + 6x_4 = 7 \\ 6x_1 - 3x_2 + 7x_3 + 8x_4 = 9 \\ \alpha x_1 - 4x_2 + 9x_3 + 10x_4 = 11 \end{cases}.$$

Soluţie: **Metoda I** (cu metoda lui Gauss)
Pornind de la matricea extinsă a sistemului obţinem 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 $\alpha \neq 8$, ţinând seama de permutările de coloane efectuate anterior obţinem sistemul de mai jos (care este echivalent cu sistemul dat):

$$\begin{cases} -x_2 + 2x_4 + 4x_1 + 3x_3 = 5 \\ -2x_4 - x_3 = -3 \\ (\alpha-8)x_1 = 0 \end{cases}.$$

Mulţimea soluţiilor 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 mulţimea soluţiilor 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)
Avem $\begin{vmatrix} -1 & 3 \\ -2 & 5 \end{vmatrix} = 1,$

$$\begin{vmatrix} 2 & -1 & 3 \\ 4 & -2 & 5 \\ 6 & -3 & 7 \end{vmatrix} = \begin{vmatrix} -1 & 3 & 4 \\ -2 & 5 & 6 \\ -3 & 7 & 8 \end{vmatrix} = \begin{vmatrix} -1 & 3 & 4 \\ -2 & 5 & 6 \\ -4 & 9 & 10 \end{vmatrix} = 0 \text{ şi } \begin{vmatrix} 2 & -1 & 3 \\ 4 & -2 & 5 \\ \alpha & -4 & 9 \end{vmatrix} = \alpha - 8.$$

1) Dacă $\alpha = 8$, atunci $\begin{vmatrix} -1 & 3 \\ -2 & 5 \end{vmatrix}$ este minor principal. Minorii caracteristici corespunzători 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 şi rezolvarea sa revine la rezolvarea unui sistem de 2 ecuaţii 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 situaţii de compatibilitate nedeterminată sunt diferite, într-un caz având 2 necunoscute principale, în celălalt 3.

5) Să se discute după parametrul real α compatibilitatea sistemului de mai jos, apoi să se rezolve în $\mathbb{R}^3$:

$$\begin{cases} \alpha x_1 + x_2 + x_3 = 1 \\ x_1 + \alpha x_2 + x_3 = 1 \\ x_1 + x_2 + \alpha x_3 = 1 \end{cases}.$$

Soluţie: **Metoda I** (cu metoda lui Gauss) Obţinem succesiv matricele echivalente:

$$\begin{pmatrix} \alpha & 1 & 1 & 1 \\ 1 & \alpha & 1 & 1 \\ 1 & 1 & \alpha & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & \alpha & 1 \\ 1 & \alpha & 1 & 1 \\ \alpha & 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & \alpha & 1 \\ 0 & \alpha - 1 & 1 - \alpha & 0 \\ 0 & 1 - \alpha & (1-\alpha)(1+\alpha) & 1 - \alpha \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 1 & \alpha & 1 \\ 0 & \alpha - 1 & 1 - \alpha & 0 \\ 0 & 0 & (1-\alpha)(2+\alpha) & 1 - \alpha \end{pmatrix} = B.$$

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 şi este echivalent cu ecuaţia $x_1 + x_2 + x_3 = 1$, iar mulţimea soluţiilor 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 soluţia 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 obţine o expresie polinomială de gradul 3. Întrucât, pentru a realiza discuţia, trebuie să rezolvăm ecuaţia algebrică rezultată din egalarea ei cu 0, acest polinom va trebui descompus în factori. Cu transformări elementare putem obţine 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 şi soluţia unică se obţine cu formulele lui Cramer.

2) Dacă $\alpha = 1$ atunci se observă că toate ecuaţiile sunt echivalente cu ecuaţia

$$x_1 + x_2 + x_3 = 1,$$

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 Exerciţii propuse

1) Fie $\varphi \in \mathbb{R}$. Să se arate că rotaţia în plan de unghi φ, adică funcţia

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

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 funcţiile $f : \mathbb{R}^2 \to \mathbb{R}^2$, $f(x, y) = (x, -y)$ (simetria în raport cu axa Ox) şi $g : \mathbb{R}^2 \to \mathbb{R}^2$, $f(x, y) = (-x, y)$ (simetria în raport cu axa Oy) sunt automorfisme ale lui $\mathbb{R}^2$. Să se scrie matricele lui f, g, $f - g$, $f + 2g$ şi $g \circ f$ în baza canonică.

3) Să se arate că fiecare dintre mulţimile de vectori $\{v_1, v_2, v_3\}$ şi $\{v_1', v_2', v_3'\}$ cu

$$v_1 = (1, 2, 1), v_2 = (2, 3, 3), v_3 = (3, 7, 1) \text{ şi } v_1' = (3, 1, 4), v_2' = (5, 2, 1), v_3' = (1, 1, -6)$$

formează câte o bază a lui $\mathbb{R}^3$ şi 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 $\mathbb{R}$-spaţiului vectorial $\mathbb{R}^4$, vectorii

$$u_1 = v_1,\ u_2 = v_1 + v_2,\ u_3 = v_1 + v_2 + v_3,\ u_4 = v_1 + v_2 + v_3 + v_4$$

şi $f \in End_{\mathbb{R}}(\mathbb{R}^4)$ 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 $\mathbb{R}^4$ şi să se scrie matricea $[f]_u$.
5) Fie V un spaţiu vectorial real, $v = (v_1, v_2, v_3)$ o bază a spaţiului V, vectorii

$$u_1 = v_1 + 2v_2 + v_3,\ u_2 = v_1 + v_2 + 2v_3,\ u_3 = v_1 + v_2$$

şi $f \in End_{\mathbb{R}}(V)$. Să se arate că $u = (u_1, u_2, u_3)$ este o bază a lui V şi să se scrie matricea lui $[f]_v$ ştiind că

$$[f]_u = \begin{pmatrix} 1 & 1 & 3 \\ 0 & 5 & -1 \\ 2 & 7 & -3 \end{pmatrix}.$$

6) Fie $f \in End_{\mathbb{Q}}(\mathbb{Q}^4)$ 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 $\operatorname{Ker} f$, $\operatorname{Im} f$, $\operatorname{Ker} f + \operatorname{Im} f$ şi $\operatorname{Ker} f \cap \operatorname{Im} f$.
7) Fie $K = \mathbb{R}$. Să se verifice egalitatea $S_B = s + S_0$ din Teorema 4.12 în cazul sistemului de ecuaţii:

$$\begin{cases} 2x_1 + x_2 - x_3 - x_4 + x_5 = 1 \\ x_1 - x_2 + x_3 + x_4 - 2x_5 = 0 \\ 3x_1 + 3x_2 - 3x_3 - 3x_4 + 4x_5 = 2 \end{cases}$$

şi să se determine o bază pentru spaţiul soluţiilor sistemului liniar omogen asociat.
8) Să se discute după parametrii reali $\alpha,\ \beta,\ \gamma,\ \lambda$ compatibilitatea sistemelor de mai jos, apoi să se rezolve:

$$a)\ \begin{cases} 5x_1 - 3x_2 + 2x_3 + 4x_4 = 3 \\ 4x_1 - 2x_2 + 3x_3 + 7x_4 = 1 \\ 8x_1 - 6x_2 - x_3 - 5x_4 = 9 \\ 7x_1 - 3x_2 + 7x_3 + 17x_4 = \alpha \end{cases} \text{(în } \mathbb{R}^4\text{)},\ b)\ \begin{cases} x_1 + x_2 + x_3 = 1 \\ \alpha x_1 + \beta x_2 + \gamma x_3 = \lambda \\ \alpha^2 x_1 + \beta^2 x_2 + \gamma^2 x_3 = \lambda^2 \end{cases} \text{(în } \mathbb{R}^3\text{)}.$$

5 Noţiuni de aritmetica numerelor întregi (de Simion Breaz şi Cosmin Pelea)

5.1 Teorema împărţirii cu rest în $\mathbb{Z}$

Teorema împărţirii cu rest reprezintă un instrument de bază în studiul numerelor întregi.

Teorema 5.1. (Teorema împărţirii cu rest în $\mathbb{N}$) Oricare ar fi numerele naturale a şi b, cu $b \neq 0$, există o singură pereche de numerele naturale $(q, r) \in \mathbb{N} \times \mathbb{N}$, astfel încât:

$$a = b \cdot q + r \text{ şi } r < b. \tag{1}$$

Demonstraţie. Fie $a,\, b \in \mathbb{N}$, cu $b \neq 0$.

Demonstrăm existenţa numerelor $q,\, r \in \mathbb{N}$, astfel încât $a = b \cdot q + r$ şi $r < b$. Fie

$$\mathcal{S} = \{x \in \mathbb{N} \mid \exists y \in \mathbb{N} : a = by + x\} \subseteq \mathbb{N}$$

şi 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 $r - b \in \mathbb{N}$ şi $a = b(q+1) + r - b$, deci $r - b \in \mathcal{S}$. Din ipoteza $b \neq 0$ deducem $r - b < r$, ceea ce contrazice alegerea lui r. Aşadar $r < b$ şi perechea (r, b) satisface condiţia (1).

Pentru demonstraţia unicităţii, să presupunem că ar exista două perechi (q_1, r_1), (q_2, r_2) care satisfac (1) pentru aceleaşi numere $a, b \in \mathbb{N}$, $b \neq 0$. Deci

$$a = b \cdot q_1 + r_1 = b \cdot q_2 + r_2 \text{ şi } r_1 < b,\, r_2 < b.$$

Presupunem că $q_1 < q_2$. Rezultă că există $x \in \mathbb{N}^*$, astfel încât $q_2 = q_1 + x$. Obţinem

$$bq_1 + r_1 = b(q_1 + x) + r_2 \Rightarrow bq_1 + r_1 = bq_1 + bx + r_2,$$

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 $b \leq bx \leq r_1$, contradicţie.

Analog se arată că nu putem avea $q_2 < q_1$. Rezultă că $q_1 = q_2$ şi mai departe

$$b \cdot q_1 + r_1 = b \cdot q_1 + r_2,$$

de unde, prin simplificare, $r_1 = r_2$ şi demonstraţia este încheiată. □

Corolarul 5.2. (Teorema împărţirii cu rest în $\mathbb{Z}$) Oricare ar fi numerele întregi a şi b, cu $b \neq 0$, există şi sunt unice numerele întregi q şi r, astfel încât

$$a = b \cdot q + r \text{ şi } 0 \leq r < |b|\,. \tag{2}$$

Demonstraţie. Fie $a, b \in \mathbb{Z}$, $b \neq 0$. Atunci $|a|,\, |b| \in \mathbb{N}$, cu $|b| \neq 0$ şi aplicăm teorema împărţirii 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. $a \geq 0$ şi $b > 0$. Atunci $a = b \cdot h + k$. Luăm $q = h$ şi $r = k$.

II. $a \geq 0$ şi $b < 0$. Atunci $a = b \cdot (-h) + k$. Luăm $q = -h$ şi $r = k$.

III. $a < 0$ şi $b > 0$. Considerăm aici subcazurile:

a) $k = 0$. Atunci $-a = b \cdot h$, adică $a = b \cdot (-h)$. Luăm $q = -h$ şi $r = 0$.

b) $k \neq 0$. Atunci

$$a = b \cdot (-h) + (-k) = -b - b \cdot h + b - k = -b \cdot (1 + h) + (b - k).$$

Luăm $q = -(1 + h)$ şi $r = b - k < b$, deci $0 \leq r < |b|$.

IV. $a < 0$ şi $b < 0$. Considerăm două subcazuri, ca în cazul anterior:

a) $k = 0$. Atunci $-a = -b \cdot h$, de unde $a = b \cdot h$. Luăm $q = h$ şi $r = 0$.

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 $q = h + 1$ şi $r = -b - k < -b$, deci $0 \leq r < |b|$.

Pentru demonstrarea unicităţii, să presupunem că ar exista două perechi (q_1, r_1), (q_2, r_2) care satisfac condiţiile (2) pentru aceleaşi numere $a, b \in \mathbb{Z}$, $b \neq 0$. Deci

$$a = b \cdot q_1 + r_1 = b \cdot q_2 + r_2 \text{ şi } 0 \leq r_1 < |b|,\ 0 \leq r_2 < |b|.$$

Rezultă că $|r_2 - r_1| < |b|$ şi $b(q_1 - q_2) = r_2 - r_1$.

Cum $|q_1 - q_2| \in \mathbb{N}$, $|q_1 - q_2| \geq 1$ ar implica

$$|b| \leq |b||q_1 - q_2| = |r_2 - r_1| < |b|,$$

contradicţie. 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, $r_1 = r_2$ şi demonstraţia este încheiată. □

Dacă a, b, q şi r sunt ca în Corolarul 5.2, vom spune că numărul q este **câtul împărţirii** lui a la b, iar r este **restul împărţirii** lui a la b. În acest context se mai foloseşte terminologia **deîmpărţit** pentru a, respectiv **împărţitor** pentru b.

Exemplul 5.3. Prezentăm câteva exemple concrete:
i) $a = 7$, $b = 3 \Rightarrow q = 2$ şi $r = 1$;
ii) $a = -7$, $b = 3 \Rightarrow q = -3$ şi $r = 2$;
iii) $a = 7$, $b = -3 \Rightarrow q = -2$ şi $r = 1$;
iv) $a = -7$, $b = -3 \Rightarrow q = 3$ şi $r = 2$;
v) $a = -6$, $b = 3 \Rightarrow q = -2$ şi $r = 0$.

Observaţia 5.4. În practică identitatea dată de teorema împărţirii cu rest este uneori înlocuită cu

$$a = bk + s,\ -|b|/2 < s \leq |b|/2.$$

De exemplu, dacă împărţim 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 împărţire 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 împărţire la 3, adică este un multiplu al lui 3).

5.2 Exerciţii rezolvate

1) Să se arate că restul împărţirii unui pătrat perfect impar la 8 este 1.

Soluţie: 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 împărţirii lui 5^{n^2} la 8.

Soluţie: Prezentăm două variante:
(I) Considerăm două cazuri: (a) n este par şi (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

$$5^{n^2} = 5^{4k^2+4k+1} = 5^{4k^2}5^{4k}5 = (\mathcal{M}_8 + 1)(\mathcal{M}_8 + 1)5 = \mathcal{M}_8 + 5.$$

Aşadar resturile posibile sunt 1 sau 5.
(II) Putem folosi exerciţiul 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 $\mathbb{Z}$

Definiţia 5.5. Fie $a, b \in \mathbb{Z}$. Spunem că a **divide pe** b şi notăm $a \mid b$ sau $b \vdots a$ dacă există un număr întreg q, astfel încât $b = a \cdot q$. Aceasta defineşte o relaţia binară omogenă pe $\mathbb{Z}$ care se numeşte **relaţia 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.

Observaţia 5.6. Dacă $a \neq 0$, următoarele afirmaţii sunt echivalente:
a) $a \mid b$;
b) b este multiplu pentru a, fapt notat prin $b = \mathcal{M}_a$;
c) restul împărţirii 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 proprietăţi elementare ale relaţiei de divizibilitate.

Teorema 5.8. (Proprietăţi ale relaţiei de divizibilitate)
Fie $a, b, c \in \mathbb{Z}$. Sunt adevărate afirmaţiile:
(i) $\pm 1 \mid a$, $\pm a \mid a$, $a \mid 0$;
(ii) dacă $a \mid b$ şi $b \mid c$, atunci $a \mid c$;
(iii) dacă $a \mid b$ şi $b \mid a$, atunci $a = \pm b$;
(iv) dacă $a \mid b$ şi $a \mid c$, atunci $a \mid (b + c)$;
(v) dacă $a \mid b$, atunci $a \mid bc$;
(vi) dacă $a \mid b + c$ şi $a \mid b$, atunci $a \mid c$;
(vii) dacă $a \mid b$ şi $b \neq 0$, atunci $|a| \leq |b|$.

Demonstraţie. (i) Fie $a \in \mathbb{Z}$. Atunci

$$a = 1 \cdot a, \text{ respectiv } a = (-1) \cdot (-a),\ a = a \cdot 1 \text{ şi } a = (-a) \cdot (-1),$$

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 obţinem

$$\begin{aligned} a \mid b &\Rightarrow \exists q_1 \in \mathbb{Z},\ b = a \cdot q_1; \\ b \mid c &\Rightarrow \exists q_2 \in \mathbb{Z},\ c = b \cdot q_2. \end{aligned}$$

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 obţinem

$$\begin{aligned} a \mid b &\Rightarrow \exists q_1 \in \mathbb{Z},\ b = a \cdot q_1; \\ b \mid a &\Rightarrow \exists q_2 \in \mathbb{Z},\ a = b \cdot q_2. \end{aligned}$$

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, aşadar $q_1 \in \{-1, 1\}$ şi $a = \pm b$.

Lăsăm cititorului demonstrarea celorlalte proprietăţi ca exerciţiu. □

Fie $a \in \mathbb{Z}$. Numim **divizori banali** (**divizori improprii**) ai lui a numerele ± 1 şi $\pm a$. Un divizor al lui a diferit de ± 1 şi de $\pm a$ se numeşte **divizor propriu** al lui a.

Observaţiile 5.9. a) Relaţia de divizibilitate pe $\mathbb{Z}$ este o relaţie de preordine pe $\mathbb{Z}$.
b) Relaţia de divizibilitate pe $\mathbb{Z}$ nu este o relaţie de ordine, deoarece ea nu este antisimetrică, după cum arată următorul exemplu:

$$2, -2 \in \mathbb{Z},\ 2|(-2) \text{ şi } (-2)|2, \text{ dar } 2 \neq -2.$$

c) Restricţia la $\mathbb{N}$ a relaţiei de divizibilitate din $\mathbb{Z}$ este o relaţie de ordine deoarece reflexivitatea şi tranzitivitatea se păstrează, iar dacă $a, b \in \mathbb{N}$ cu $a \mid b$ şi $b \mid a$, atunci $a = b$.

Fie $a, b \in \mathbb{Z}$. Spunem că un număr $d \in \mathbb{Z}$ este un **divizor comun** al numerelor a şi b dacă $d \mid a$ şi $d \mid b$.

Exemplele 5.10. 1) Numărul 1 este divizor comun al numerelor a şi b pentru orice $a, b \in \mathbb{Z}$.
2) Numărul 3 este divizor comun al numerelor 6 şi -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 mulţimea divizorilor comuni ai numerelor a şi b. Acest număr se numeşte **cel mai mare divizor comun al numerelor** a **şi** b şi se notează cu $d = (a, b)$ sau $d = \text{c.m.m.d.c.}(a, b)$.

Observaţiile 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 şi b este 0, atunci definiţia celui mai mare divizor comun poate fi extinsă pentru această situaţie.
3) Dacă $a = b = 0$, atunci nu există cel mai mare divizor comun al numerelor a şi b.
4) $(a, b) = d \Leftrightarrow \begin{cases} d \in \mathbb{N}^*, \\ d \mid a \text{ şi } d \mid b, \\ c \in \mathbb{N},\ c \mid a \text{ şi } c \mid b \Rightarrow c \leq d \end{cases}$

Următorul rezultat este foarte util în practică şi ne spune că cel mai mare divizor comun a două numere întregi poate fi obţinut ca o combinaţie liniară a acestora.

Teorema 5.12. (reprezentarea Bézout a c.m.m.d.c.)
Dacă $a, b \in \mathbb{Z}^*$ şi $d = (a, b)$, atunci există $u, v \in \mathbb{Z}$ astfel încât

$$d = au + bv.$$

Demonstraţie. Fie $S = \{ax + by \mid ax + by > 0,\ x, y \in \mathbb{Z}\} \subseteq \mathbb{N}^*$. Constatăm că $S \neq \emptyset$ pentru că $a = a \cdot 1 + b \cdot 0$ şi $-a = a \cdot (-1) + b \cdot 0$, 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 împărţirii cu rest şi 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 $r \leq 0$ şi rezultă $r = 0$. Aşadar $d \mid a$. Analog se arată că $d|b$.

Fie $c \in \mathbb{N}$ cu $c \mid a$ şi $c \mid b$. Rezultă că $c \mid au + bv = d$, şi de aici găsim $c \leq |d| = d$. Aşadar $d = (a, b)$. □

Dacă scriem $(a, b) = au + bv$, $u, v \in \mathbb{Z}$, atunci spunem că am ales o **reprezentare Bézout** pentru (a, b). Atragem atenţia 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 $a, b \in \mathbb{Z}^*$ şi $d \in \mathbb{N}^*$. Atunci

$$(a, b) = d \Leftrightarrow \begin{cases} d \mid a \text{ şi } d \mid b, \\ c \in \mathbb{Z},\ c \mid a \text{ şi } c \mid b \Rightarrow c \mid d \end{cases}$$

Observaţia 5.15. Această caracterizare este folosită ca definiţie pentru c.m.m.d.c. în diverse tipuri de inele unde nu avem definită o relaţie de ordine ,,naturală" (de exemplu in $\mathbb{Q}[X]$). În acest context, c.m.m.d.c. este de fapt o clasă de echivalenţă. Pentru cazul inelului $\mathbb{Z}$, c.m.m.d.c este de fapt mulţimea $\{-d, d\}$, unde $d = (a, b)$.

Un caz special în studiul divizibilităţii 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 şi b sunt relativ prime dacă şi numai dacă există $u, v \in \mathbb{Z}$ astfel încât $au + bv = 1$.

Demonstraţie. ($\Rightarrow$) Această implicaţie rezultă din Teorema 5.12.
($\Leftarrow$) Fie $d = (a, b)$. Din $d \mid a$ şi $d \mid b$ rezultă că $d \mid au + bv = 1$, deci $d = 1$. □

Corolarul 5.17. Dacă $a, b \in \mathbb{Z}^*$ şi $d = (a, b)$, atunci $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demonstraţie. 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 $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. □

Folosim consideraţiile făcute până acum ca să demonstrăm proprietăţi importante ale relaţiei de divizibilitate.

Teorema 5.18. Fie $a, b, c \in \mathbb{Z}$. Sunt adevărate afirmaţiile:
(i) dacă $a \mid b$, $b \mid c$ şi $(a, b) = 1$, atunci $ab \mid c$;
(ii) **(Lema lui Euclid)** dacă $a \mid bc$ şi $(a, b) = 1$, atunci $a \mid c$.

Demonstraţie. (i) Fie $r, s \in \mathbb{Z}$ astfel încât $c = ar = bs$ şi $u, v \in \mathbb{Z}$ 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 $au + bv = 1$ şi $bc = ka$. Calculăm

$$c = c \cdot 1 = c(au + bv) = acu + bcv = acu + kav = a(cu + bv),$$

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**, şi 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 $b \neq 0$ şi $b \leq a$. Considerăm identităţile următoarelor împărţiri:

$$\begin{aligned}
a &= b \cdot q_0 + r_0, && \text{unde } r_0 < b; \text{ fie } r_0 \neq 0; && (E_1)\\
b &= r_0 \cdot q_1 + r_1, && \text{unde } r_1 < r_0; \text{ fie } r_1 \neq 0; && (E_2)\\
r_0 &= r_1 \cdot q_2 + r_2, && \text{unde } r_2 < r_1; \text{ fie } r_2 \neq 0; && (E_3)\\
&\dots && \dots &&\\
r_{n-3} &= r_{n-2} \cdot q_{n-1} + r_{n-1}, && \text{unde } r_{n-1} < r_{n-2};\ \text{ fie } r_{n-1} \neq 0; && (E_n)\\
r_{n-2} &= r_{n-1} \cdot q_n + r_n, && \text{unde } r_n < r_{n+1};\ \text{ fie } r_n \neq 0; && (E_{n-1})\\
r_{n-1} &= r_n \cdot q_{n+1} + r_{n+1}, && \text{unde } r_{n+1} = 0. && (E_{n+2})
\end{aligned}$$

Atunci cel mai mare divizor comun al numerelor a şi b este ultimul rest diferit de zero al acestor împărţiri, adică:

$$(a, b) = r_n.$$

Demonstraţie. Observăm că şirul resturilor diferite de zero este un şir strict descrescător

$$r_0 > r_1 > r_2 > ...$$

de numere naturale, deci acest şir este finit, adică, după un număr finit de împărţiri obţinem restul zero.

Demonstrăm că $r_n \mid a$ şi $r_n \mid b$ folosind inducţia completă pentru propoziţia

$$P(i) : r_n \mid r_{n-i}, \text{ unde } 0 \leq i \leq n.$$

Propoziţia $P(0)$ 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 $1 \leq j \leq i$ şi demonstrăm că $r_n \mid r_{n-(i+1)}$.

Pentru aceasta folosim relaţia $r_{n-(i+1)} = r_{n-i} \cdot q_{n-(i-1)} + r_{n-(i-1)}$, de unde concluzia este evidentă.

Deci r_n divide pe r_0 şi pe r_1, iar din egalitatea găsită în pasul (E_2) dedicem $r_n \mid b$. Apoi folosim (E_1) ca să deducem şi $r_n \mid a$.

Fie $c \in \mathbb{N}$, astfel încât $c \mid a$ şi $c \mid b$. Vom arăta că $c \mid r_n$. Folosind din nou identităţile din enunţ, avem:

$$c \mid a = b \cdot q_0 + r_0 \text{ şi } c \mid (b \cdot q_0) \Rightarrow c \mid r_0.$$

Apoi obţinem:

$$c \mid b = r_0 \cdot q_1 + r_1 \text{ şi } c \mid (r_0 \cdot q_1) \Rightarrow c | r_1,$$

şi continuăm raţionamentul, parcurgând identităţile împărţirilor de la prima spre ultima. În final găsim

$$c \mid r_{n-2} = r_{n-1} \cdot q_n + r_n \text{ şi } c \mid (r_{n-1} \cdot q_n),$$

deci $c \mid r_n$.

În concluzie, $r_n = (a, b)$. □

Observaţia 5.20. Plecând de la identităţile (E_1)–(E_n) putem găsi o reprezentare Bézout astfel: înlocuim succesiv resturile, plecând de la (E_n) către (E_1)

$$r_n = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) = -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2} = \cdots,$$

iar în final obţinem pe r_n sub forma $r_n = au + bv$.

Procedeul dat de algoritmul lui Euclid poate fi folosit în demonstrarea unor proprietăţi ale c.m.m.d.c.

Corolarul 5.21. Pentru orice a, b, $k \in \mathbb{N}^*$, avem:

$$(a \cdot k, b \cdot k) = (a, b) \cdot k.$$

Demonstraţie. Scriem algoritmul lui Euclid pentru calculul lui $d = (a, b)$. Dacă înmulţim liniile (E_1)–(E_n) cu k se constată uşor că noile egalităţi reprezintă chiar algoritmul lui Euclid aplicat numerelor ka şi 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 şi b dacă $a \mid m$ şi $b \mid m$.

Exemplele 5.22. 1) Pentru orice $a, b \in \mathbb{Z}$, numărul $a \cdot b$ este multiplu comun al numerelor a şi b.
2) Numărul 6 este multiplu comun al numerelor 2 şi -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 mulţimea multiplilor comuni strict pozitivi ai numerelor a şi b. Acest număr se numeşte **cel mai mic multiplu comun al numerelor a şi b** şi se notează cu $m = [a, b] = \text{c.m.m.m.c.}(a, b)$.

Observaţia 5.23. Ca pentru cel mai mare divizor comun, observăm că

$$[a, b] = m \Leftrightarrow \begin{cases} m \in \mathbb{N}^*, \\ a \mid m \text{ şi } b \mid m, \\ c \in \mathbb{N}^*, a \mid c \text{ şi } b \mid c \Rightarrow m \leq c. \end{cases}$$

Teorema 5.24. Oricare ar fi $a, b \in \mathbb{N}^*$, are loc egalitatea:

$$ab = (a, b)[a, b].$$

Demonstraţie. Fie $d = (a, b)$. Atunci există $r, s \in \mathbb{N}^*$ astfel încât $a = dr$, $b = ds$ şi $(r, s) = 1$. Notăm $m = drs = as = br$, deci m este multiplu comun al numerelor a şi b.

Dacă $c \in \mathbb{N}^*$ este un multiplu comun pentru a şi 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 demonstraţia de mai sus se deduce imediat:

Corolarul 5.25. Fie $a, b \in \mathbb{Z}^*$ şi $m \in \mathbb{N}^*$. Atunci

$$m = [a, b] \Leftrightarrow \begin{cases} a \mid m \text{ şi } b \mid m, \\ c \in \mathbb{Z}, a \mid c \text{ şi } b \mid c \Rightarrow m \mid c. \end{cases}$$

Din formula dată în teoremă rezultă şi

Corolarul 5.26. Dacă $(a, b) = 1$, atunci $ab = [a, b]$.

Observaţia 5.27. Definiţiile celui mai mare divizor comun şi celui mai mic multiplu comun pot fi extinse la o mulţime finită de numere întregi. Fie $a_1, \ldots, a_n$ numere întregi nenule. Atunci $d \in \mathbb{N}^*$ este **cel mai mare divizor comun al acestor numere** dacă

$$\begin{cases} d \mid a_1, \ldots, d \mid a_n, \\ c \mid a_1, \ldots, c \mid a_n \Rightarrow c \leq d. \end{cases}$$

În aceste condiţii notăm $d = (a_1, \ldots, a_n) = \text{c.m.m.d.c.}(a_1, \ldots, a_n)$.

Numărul $m \in \mathbb{N}^*$ este **cel mai mic multiplu comun al acestor numere** dacă

$$\begin{cases} a_1 \mid m, \ldots, a_n \mid m, \\ a_1 \mid c, \ldots, a_n \mid c \Rightarrow m \leq c. \end{cases}$$

În aceste condiţii notăm $m = [a_1, \ldots, a_n] = \text{c.m.m.m.c.}(a_1, \ldots, a_n)$.

Se constată imediat că

$$(a_1, \ldots, a_n, a_{n+1}) = ((a_1, \ldots, a_n), a_{n+1}) \text{ şi } [a_1, \ldots, a_n, a_{n+1}] = [[a_1, \ldots, a_n], a_{n+1}].$$

5.4 Exerciţii rezolvate

1) Fie $a \in \mathbb{N}$, $a = \overline{a_n a_{n-1} \ldots a_2 a_1 a_0}$, $a_i \in \{0, \ldots, 9\}$, $i = 1, \ldots, n$, $a_n \neq 0$. Arătaţi că:
(i) $2 \mid a \Leftrightarrow 2 \mid a_0$;
(ii) pentru $k \in \mathbb{N}^*$ avem $2^k \mid a \Leftrightarrow 2 \mid \overline{a_{k-1} \ldots a_0}$;
(iii) $3 \mid a \Leftrightarrow 3 \mid a_n + \cdots + a_0$;
(iv) $27 \mid a \Leftrightarrow 27 \mid \overline{a_2 a_1 a_0} + \overline{a_5 a_4 a_3} + \cdots$.

Soluţie: (i) Scriem

$$a = 10 \cdot (a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + ... + a_2 \cdot 10 + a_1) + r_0 = \mathcal{M}_2 + a_0.$$

Deci

$$2|a \Leftrightarrow 2|\mathcal{M}_2 + a_0 \Leftrightarrow 2|a_0.$$

(ii) Analog, scriem numărul a sub forma:

$$a = 10^k \cdot (a_n \cdot 10^{n-k} + a_{n-1} \cdot 10^{n-k-1} + ... + a_k) + (a_{k-1} \cdot 10^{k-1} + ... + a_1 \cdot 10 + a_0),$$

adică

$$a = \mathcal{M}_{2^k} + \overline{a_{k-1} \dots a_1 a_0}.$$

Deci

$$2^k \mid a \Leftrightarrow 2^k \mid \mathcal{M}_{2^k} + \overline{a_{k-1} \dots a_1 a_0} \Leftrightarrow 2^k \mid \overline{a_{k-1} \dots a_1 a_0}.$$

(iii) Observăm că dacă $k \in \mathbb{N}^*$, atunci $10^k = (\mathcal{M}_3 + 1)^k = \mathcal{M}_3 + 1$. Obţinem

$$a = a_n \cdot (\mathcal{M}_3 + 1) + ... + a_2 \cdot (\mathcal{M}_3 + 1) + a_1 \cdot (\mathcal{M}_3 + 1) + a_0 = \mathcal{M}_3 + (a_n + ... + a_2 + a_1 + a_0).$$

Deci

$$3|a \Leftrightarrow 3|(a_n + a_{n-1} + ... + a_2 + a_1 + a_0).$$

(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 obţine

$$a = \mathcal{M}_{27} + \overline{a_2 a_1 a_0} + \overline{a_5 a_4 a_3} + \dots,$$

de unde se deduce criteriul enunţat.

2) Fie $a, b \in \mathbb{Z}$, $d = (a, b)$ şi $T = \{ax + by \mid x, y \in \mathbb{Z}\}$. Să se arate că $T = d\mathbb{Z}$.

Soluţie: Reamintim că $d\mathbb{Z} = \{dk \mid k \in \mathbb{Z}\}$ şi demonstrăm egalitatea prin dublă incluziune.

Fie $z \in T$. Atunci există $x, y \in \mathbb{Z}$ astfel încât $z = ax + by$. Din $d \mid a$ şi $d \mid b$ deducem $d \mid ax + by = z$, deci $z \in d\mathbb{Z}$. Aşadar $T \subseteq d\mathbb{Z}$ (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 $z = auk + bvk \in T$. Aşadar $d\mathbb{Z} \subseteq T$ şi soluţia 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 $M_b \mid M_a$ şi că

$$(M_m, M_n) = M_{(m,n)}, \ \forall m, n \in \mathbb{N}^*.$$

Soluţie: Pentru început să considerăm o identitate de tipul $a = bq + r$, unde $a, b, q, r \in \mathbb{N}$ cu a şi 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

$$x^k - y^k = (x-y)(x^{k-1} + x^{k-2}y + \cdots + y^{k-1}).$$

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 algoritmii pentru calculul numerelor (m, n) şi (M_m, M_n) în paralel:

$$\begin{aligned}
&m = n \cdot q_0 + r_0, && M_m = M_n \cdot Q_0 + M_{r_0} && (E_1)\\
&n = r_0 \cdot q_1 + r_1, && M_n = M_{r_0} \cdot Q_1 + M_{r_1} && (E_2)\\
&r_0 = r_1 \cdot q_2 + r_2, && M_{r_0} = M_{r_1} \cdot Q_2 + M_{r_2} && (E_3)\\
&\cdots\cdots && \cdots\cdots &&\\
&r_{k-2} = r_{k-1} \cdot q_k + r_k, && M_{r_{k-2}} = M_{r_{k-1}} \cdot Q_k + M_{r_k} && (E_{k+1})\\
&r_{k-1} = r_k \cdot q_{k+1} + r_{k+1}, && M_{r_{k-1}} = M_{r_k} \cdot Q_{k+1} + M_{r_{k+1}}, && (E_{k+2})
\end{aligned}$$

unde $0 = r_{k+1} < r_k < \ldots r_1 < n \leq m$ şi $0 = M_{r_{k+1}} < M_{r_k} < \ldots M_{r_1} < M_n \leq M_m$. 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 ± 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 ± 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 şi $a, b \in \mathbb{Z}$ astfel încât $p \mid ab$. Să observăm că nu restrângem generalitatea dacă presupunem $a \in \mathbb{N}$ şi $p \nmid a$ (putem să înmulţim 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 $p \mid ab$ şi Teorema 5.18 (ii) implică $p \mid b$. Dar $p \neq \pm 1$ pentru că este ireductibil, deci p este un număr prim. □

Observaţiile 5.31. a) Din definiţia numerelor prime rezultă imediat că un număr p este prim dacă şi numai dacă $-p$ este prim. Aşadar, din punctul de vedere al relaţiei de divizibilitate, este suficient să lucrăm cu numere prime pozitive.
b) Proprietatea din definiţia numerelor prime poate fi extinsă la produse cu un număr arbitrar de factori. Deci, dacă p este prim şi $p \mid a_1 \cdot \ldots \cdot a_n$, atunci există $i \in \{1, \ldots, n\}$ 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 divizibilităţii este evidenţiat 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, abstracţie făcând de ordinea factorilor. Mai precis, pentru orice $n \in \mathbb{N}$, $n \geq 2$ există $p_1, \ldots, p_k$ numere prime (nu neapărat diferite) astfel încât

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$$

şi din $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l$, cu $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_l$ numere prime, rezultă $k = l$ şi existenţa unei funcţii bijective $\sigma : \{1, \ldots, k\} \to \{1, \ldots, k\}$ astfel încât

$$p_i = q_{\sigma(i)}, \ \forall i \in \{1, \ldots, k\}.$$

Demonstraţie. Pentru existenţa descompunerii în factori primi vom folosi metoda inducţiei 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. *Demonstraţia*: Presupunem că orice $m \in \mathbb{N}$, $2 \leq m < n$ se descompune într-un produs cu toţi factorii numere prime şi arătăm că şi n are aceeaşi 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 $1 < a, b < n$ şi aplicând ipoteza inducţiei, obţinem:

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_j \text{ şi } b = p_{j+1} \cdot p_{j+2} \cdot \ldots \cdot p_k,$$

unde $p_i \in \mathbb{N}$, sunt numere prime pentru orice $i = 1, \ldots, k$. Atunci

$$n = a \cdot b = p_1 \cdot p_2 \cdot \ldots \cdot p_j \cdot p_{j+1} \cdot p_{j+2} \cdot \ldots \cdot p_k,$$

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

$$n = p_1 \cdot p_2 \cdot ... \cdot p_k = q_1 \cdot q_2 \cdot ... \cdot q_l,$$

unde $k, l \neq l$. Pentru că înmulţirea este comutativă, putem presupune

$$p_1 \leq p_2 \leq \ldots \leq p_k \text{ şi } q_1 \leq q_2 \leq \ldots \leq q_l.$$

Din $p_k \mid n = q_1 \cdot q_2 \cdot ... \cdot q_l$ rezultă că există $i \in \{1, \ldots, l\}$ astfel încât $p_k \mid q_i$, deci $p_k \leq q_l$. Analog se demonstrează şi inegalitatea $q_l \leq p_k$, deci $p_k = q_l$ şi

$$p_1 \cdot p_2 \cdot ... \cdot p_{k-1} = q_1 \cdot q_2 \cdot ... \cdot q_{l-1}.$$

Continuăm procedeul de mai sus şi obţinem $p_{k-1} = q_{l-1}$ şi mai departe $p_{k-i} = q_{k-i}$ pentru orice $0 \leq i \leq \min\{k, l\}$. Dacă am aveam $k \neq l$, atunci s-ar obţine că 1 este un produs de numere prime. Aşadar $k = l$ şi $p_i = q_i$ pentru orice $i \in \{1, \ldots, k\}$. □

Corolarul 5.34. Pentru orice $n \in \mathbb{N}$, $n \geq 2$, există numerele prime distincte $p_1, \ldots, p_k$ şi $\alpha_1, \ldots, \alpha_k \in \mathbb{N}^*$ astfel încât

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}.$$

Această descompunere este unică dacă facem abstracţie de ordinea factorilor.

Descompunerea din Corolarul 5.34 se numeşte **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 şir de numere. Spunem că numerele α_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 şirul crescător al numerelor prime

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5, \ldots\ .$$

Pentru orice $n \in \mathbb{N}^*$ există un singur şir $(\alpha_k)_{k>0}$ 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 toţi factorii, cu excepţia unui număr finit, sunt egali cu 1.

Exemplul 5.37. Pentru $n = 1$, avem $n = \prod_{k \geq 1} p_k^0$, i.e. şirul $(\alpha_k)_{k>0}$ este şirul constant nul. Pentru $n = 5$, şirul $(\alpha_k)_{k>0}$ are pe 1 pe poziţia a treia ($\alpha_3 = 1$) şi pe 0 pe celelalte poziţii. Numărul 360 este determinat de şirul $(3, 2, 1, 0, 0, \ldots, 0, \ldots)$.

Folsind această reformulare a teoremei fundamentale a aritmeticii, putem da o caracterizare a divizibilităţii şi formule de calcul pentru cel mai mare divizor comun şi cel mai mic multiplu comun.

Propoziţia 5.38. Fie $m = \prod_{k\geq 1} p_k^{\alpha_k}$ şi $n = \prod_{k\geq 1} p_k^{\beta_k}$ descompunerile numerelor naturale $m, n > 0$ date de Corolarul 5.36. Sunt adevărate afirmaţiile:
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 Exerciţii rezolvate

1) Să se arate că numărul $\sqrt{2}$ este iraţional.

Soluţie: 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 $d = (m, n)$ şi $m = du$, $n = dv$, atunci $\sqrt{2} = \frac{u}{v}$ şi $(u, v) = 1$. Rezultă că $2v^2 = u^2$, deci $2 \mid u^2$. Cum 2 este număr prim, rezutlă că $2 \mid u$. Aşadar $u = 2k$, deci $2v^2 = 4k^2$, de unde găsim $2 \mid v^2$. Folosim din nou faptul că 2 este prim şi obţinem $2 \mid v$, deci $2 \mid (u, v)$, o contradicţie. Aşadar $\sqrt{2} \notin \mathbb{Q}$.

2) Să se arate că există o infinitate de numere prime.

Soluţie: Pentru a arăta că există o infinitate de numere prime este suficient că oricare ar fi $S = \{p_1, \ldots, p_m\}$ o mulţime de numere prime există un număr prim $p \notin S$.

Fie $S = \{p_1, \ldots, p_m\}$ o mulţime nevidă de numere prime. Considerăm numărul $n = p_1 \cdot \ldots \cdot p_m + 1$. Observăm că $n \geq 2$, deci există un divizor prim p al lui n. Din $p \mid p_1 \cdot \ldots \cdot p_m + 1$ rezultă că există $u \in \mathbb{Z}$ astfel încât $pu - p_1 \cdot \ldots \cdot p_m = 1$. Deci oricare ar fi $i \in \{1, \ldots, m\}$ avem $(p, p_i) = 1$, şi rezultă $p \notin S$, ceea ce trebuia demonstrat.

3) Să se arate că există o infinitate de numere prime de forma $4k - 1$.

Soluţie: Fie $S = \{p_1, \ldots, p_m\}$ o mulţime nevidă de numere prime de forma $4k - 1$. Observăm că există astfel de mulţimi pentru că 3 are această formă.

Considerăm numărul $n = 4p_1 \cdot \ldots \cdot p_m - 1$. Observăm că $n \geq 2$, deci există un divizor prim p al lui n. Mai mult, dacă presupunem că toţi divizorii primi ai lui n sunt de forma $\mathcal{M}_4 + 1$, rezultă imediat că n are aceeaşi formă. Dar acest fapt este imposibil pentru că restul împărţirii lui n la 4 este 3.

Aşadar există un divizor prim p al lui n de forma $4k-1$. Din $p \mid 4p_1 \cdot \ldots \cdot p_m - 1$ rezultă că există $u \in \mathbb{Z}$ astfel încât $-pu + 4p_1 \cdot \ldots \cdot p_m = 1$. Deci oricare ar fi $i \in \{1, \ldots, m\}$ avem $(p, p_i) = 1$, şi rezultă $p \notin S$, ceea ce trebuia demonstrat.

4) Să se arate că dacă $p_1, p_2, \ldots, p_n, \ldots$ reprezintă şirul numerelor prime aranjate în ordine crescătoare, atunci $p_n \leq 2^{2^{n-1}}$.

Soluţie: Aplicăm metoda inducţiei matematice. Pentru $n = 1$ avem $p_1 = 2 \leq 2^{2^0}$. Presupunem enunţul adevărat pentru $p_1, \ldots, p_n$ şi vom demonstra că $p_{n+1} \leq 2^{2^n}$. Din soluţia Exerciţiului 2) rezultă că există un număr prim p diferit de $p_1, \ldots, p_n$ care este divizor pentru $p_1 \cdot \ldots \cdot p_n + 1$. Deci

$$p_{n+1} \leq p \leq p_1 \cdot \ldots \cdot p_n + 1 \leq 2^{2^0} \cdot 2^{2^1} \cdot \ldots \cdot 2^{2^{n-1}} + 1 = 2^{\sum_{i=0}^{n-1} 2^i} + 1 = 2^{2^n - 1} + 1 < 2^{2^n}$$

şi soluţia este încheiată.

5.7 Exerciţii propuse

1) Determinaţi restul împărţirii lui $19^{44} \cdot 23^{17}$ la 7.

2) Fie $n \in \mathbb{N}$ un număr natural care împărţit la 6, 8, 9, 12 şi 16 dă acelaşi rest 5.

i) Determinaţi cel mai mic n cu această proprietate.

ii) Determinaţi cel mai mic $n > 5$ cu această proprietate.

iii) Determinaţi 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. şi c.m.m.m.c. al numerelor 4148 şi 7684.

7) Determinaţi numerele prime care pot fi scise atât ca sumă, cât şi ca diferenţă de două numere prime.

8) Demonstraţi 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 $a, b \in \mathbb{N}^*$ şi $(a, b) = 1$ 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 şi $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$), 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. Coconeţ, C. Conţiu, *Lecţii de algebră*, Ed. Eikon, Cluj-Napoca, 2010.

[3] S. Breaz, R. Covaci, *Elemente de logică matematică, teoria mulţimilor şi 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 şi Pedagogică, Bucureşti, 1991.

[6] I. Purdea, I. Pop, *Algebră*, Ed. Gil, Zalău, 2003.

[7] I. Purdea, C. Pelea, *Probleme de algebră*, Ed. Eikon, Cluj-Napoca, 2008.