Ministerul Educației, Cercetării și Tineretului

MIRCEA GANGA

MATEMATICĂ

MANUAL PENTRU CLASA a XII-a

PROFIL M1

ELEMENTE DE ALGEBRĂ

$$
\begin{aligned}
* : M \times M &\longrightarrow M \\
(x, y) &\longrightarrow x * y
\end{aligned}
$$

$$(G, *) \xrightarrow{\ f\ } (G', \circ)$$

$$
\begin{array}{c|ccccc}
* & a_1 & \dots & a_j & \dots & a_n \\
\hline
a_1 & & & \vdots & & \\
\vdots & & & \vdots & & \\
a_i & \dots & \dots & a_i * a_j & & \\
\vdots & & & & & \\
a_n & & & & &
\end{array}
\quad \xrightarrow{\ f\ } \quad
\begin{array}{c|ccccc}
\circ & b_1 & \dots & b_j & \dots & b_n \\
\hline
b_1 & & & \vdots & & \\
\vdots & & & \vdots & & \\
b_i & \dots & \dots & b_i \circ b_j & & \\
\vdots & & & & & \\
b_n & & & & &
\end{array}
$$

EDITURA MATHPRESS

CUPRINS

ELEMENTE
DE
ALGEBRĂ

1. GRUPURI

Acest capitol conține informații despre noțiunea de lege de compoziție (notată generic „$*$“) pe o mulțime nevidă (M) şi principalele proprietăți ale acesteia. Acest concept este ilustrat prin exemple întâlnite în anii precedenți. Cuplul $(M,*)$ este o structură algebrică: monoid, grup.

Noțiunea de grup este una fundamentală în matematică, având aplicații în diverse domenii: teoria ecuațiilor algebrice şi a ecuațiilor diferențiale, teoria relativității, cristalografiei, teoria informației, etc.

Ca grupuri remarcabile figurează: grupurile de matrice, grupurile de transformări (care sunt grupuri infinite), grupuri de permutări, grupul claselor de resturi, grupul rădăcinilor de ordin n ale unității (care sunt grupuri finite) etc.

Se defineşte conceptul de izomorfism de grupuri. Două astfel de grupuri se bucură de aceleaşi proprietăți algebrice. Pentru grupurile finite izomorfe tablele lor sunt la fel organizate.

Fiecare concept introdus beneficiază de probleme rezolvate diverse precum şi de un set consistent de probleme propuse (cele mai multe fiind date la bacalaureat sau admitere în facultăți în ultimii ani).

Istoric. Noțiunea de grup a fost utilizată pentru prima dată de matematicianul francez Evariste Galois (1811-1832) (mort în duel la vârsta de 21 ani), care este adevăratul creator al teoriei grupurilor. Ideile teoriei grupurilor „erau în aer“ (cum se întâmplă adesea cu ideile matematice fundamentale) înainte de Galois, şi anumite teoreme ale teoriei grupurilor au fost demonstrate sub o formă naivă de Lagrange (1736-1813). Contemporanii lui Galois n-au înțeles şi deci nici apreciat lucrările sale geniale. Ei nu s-au interesat decât după apariția în 1870 a cărții lui Jordan „Traité des substitutions et des équations algébriques“. De abia la sfârşitul secolului al XIX-lea în teoria grupurilor, „fantezia a fost definitiv abandonată pentru a face loc unei pregătiri atente a scheletului logic“ (F. Klein „Conferințe asupra dezvoltării matematicilor secolului al XIX-lea“).

PIONIER AL MATEMATICII

Evariste GALOIS (1811 – 1832)
Matematician francez

Matematicianul englez Arthur Cayley (1821-1895), unul dintre cei mai prolifici matematicieni (cu studii la celebrul Trinity College of Cambridge University, a scris peste 200 de articole) a fost printre primii care a descris grupurile abstracte.

1.1. LEGE DE COMPOZIȚIE INTERNĂ

Conceptul care urmează a fi prezentat l-am întâlnit încă din gimnaziu, fără a-l defini în termenii folosiți în acest paragraf, iar mai târziu, în anii de liceu precedenți, l-am

extins pentru alte categorii de mulțimi. Acum vom interpreta lucrurile învățate în ceilalți ani dintr-un punct de vedere mai abstract.
Reamintim că dată fiind o mulțime nevidă M prin produsul cartezian $M \times M$ înțelegem mulțimea tuturor perechilor de elemente (x, y) (prima componentă este x, iar cea de-a doua este y) când $x, y \in M$, adică $M \times M = \{(x, y) | x, y \in M\}$.

> **Definiție.** Fie M o mulțime nevidă. Se numește **operație algebrică binară** (sau **lege de compoziție internă** sau simplu **lege de compoziție**) definită pe M o aplicație $f : M \times M \to M$, care asociază fiecărei perechi $(x, y) \in M \times M$ un unic element $f(x, y) \in M$.
>
> Elementul $f(x, y)$ se numește **compusul lui** x **cu** y.

Aşadar, la orice pereche (cuplu) $(x, y) \in M \times M = M^2$, această operație face să corespundă în mod unic elementul $f(x, y)$ **din aceeaşi mulțime** M. Uneori în loc de $f(x, y)$ se scrie xfy, dar cel mai des se desemnează operația binară pe M printr-un simbol special:

$$*, \circ, \perp, \top, \cup, \cap, \oplus, \bullet, \ldots .$$

Urmând această cale vom numi $x \cdot y$ (sau simplu xy, fără nici un semn între x şi y) **produsul şi** $x + y$ **suma** elementelor $x, y \in M$.
În primul caz vom spune că legea este dată **multiplicativ**, iar în al doilea **aditiv**.
Se înțelege că, în majoritatea cazurilor, aceste denumiri sunt convenționale.
În general, pe o mulțime M se pot defini mai multe operații diferite. Când dorim să punem în evidență una dintre ele vom utiliza parantezele $(M, *)$ şi vom spune că operația $*$ conferă mulțimii M o **structură algebrică** sau că $(M, *)$ este un **sistem algebric**.
De exemplu, pe mulțimea $\mathbb{Z}$ pe lângă operațiile $+, \cdot$ (adunarea şi înmulțirea numerelor întregi) putem defini şi alte operații „derivate":
$x \circ y = x + y - 2xy$, $x * y = -x + y$, $x \perp y = -x - y + xy$ etc. care se obțin cu ajutorul operațiilor $+$ (sau $-$) şi $\cdot$. Rezultă astfel structuri algebrice diferite: $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}, \circ)$, $(\mathbb{Z}, *)$, $(\mathbb{Z}, \perp)$.
Aşa cum vom vedea în capitolele care urmează, vom clasifica structurile algebrice după:

- **numărul de legi de compoziție;**
- **proprietățile acestor operații.**

Exemple cunoscute de legi de compoziție

1. Adunarea pe $\mathbb{N}$ (mulțimea numerelor naturale) este aplicația $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ care asociază cuplului (x, y) elementul $x + y$ (suma dintre x şi y). Vom marca această corespondență prin $(x, y) \to x + y$.

2. Înmulțirea pe $\mathbb{N}$ este aplicația $\cdot : \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ dată de corespondența $(x,y)\to x\cdot y$.

3. Adunarea pe $\mathcal{M}_n(\mathbb{C})$ (mulțimea matricelor pătratice de ordin n cu elemente numere complexe) este definită prin $+ : \mathcal{M}_n(\mathbb{C})\times\mathcal{M}_n(\mathbb{C})\to\mathcal{M}_n(\mathbb{C})$, $(A,B)\to A+B$.

4. Înmulțirea pe $\mathcal{M}_n(\mathbb{C})$ este aplicația definită prin $\cdot : \mathcal{M}_n(\mathbb{C})\times\mathcal{M}_n(\mathbb{C})\to\mathcal{M}_n(\mathbb{C})$, $(A,B)\to AB$.

5. Reuniunea pe $\mathcal{P}(M)$ (mulțimea părților lui M; reprezintă toate submulțimile lui M) este definită prin: $\cup : \mathcal{P}(M)\times\mathcal{P}(M)\to\mathcal{P}(M)$, $(A,B)\to A\cup B$.

6. Intersecția pe $\mathcal{P}(M)$ este definită prin $\bigcap : \mathcal{P}(M)\times\mathcal{P}(M)\to\mathcal{P}(M)$, $(A,B)\to A\bigcap B$.

7. Compunerea pe $\mathcal{F}(M)$ (mulțimea funcțiilor definite pe M cu valori în M) este aplicația $\circ : \mathcal{F}(M)\times\mathcal{F}(M)\to F(M)$, $(f,g)\to f\circ g$.

Desigur că exemplele pot continua cu alte legi de compoziție întâlnite în anii precedenți.

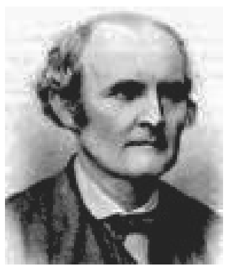
Tabla operației (legii)

Dacă mulțimea M este **finită**, atunci operația algebrică $*$ pe M poate fi dată prin așa numita **tablă a operației** (sau **tabla lui Cayley**). Într-adevăr, dacă $M=\{a_1, a_2, ..., a_n\}$, atunci tabla operației arată astfel:

$*$	a_1	a_2	$\cdots$	a_j	$\cdots$	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	$\cdots$	$a_1 * a_j$	$\cdots$	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	$\cdots$	$a_2 * a_j$	$\cdots$	$a_2 * a_n$
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
a_i	$a_i * a_1$	$a_i * a_2$	$\cdots$	$a_i * a_i$	$\cdots$	$a_i * a_n$
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
a_n	$a_n * a_1$	$a_n * a_2$	$\cdots$	$a_n * a_j$	$\cdots$	$a_n * a_n$

UN PIONIER AL MATEMATICII

Arthur CAYLEY (1821 – 1895)
Matematician englez



CONTRIBUȚII

- ***teoria matricelor***
- ***teoria grupurilor***

În acest tabel elementul $a_i * a_j$ este situat pe linia i și coloana j. Dacă notăm $a_{ij} = a_i * a_j$, atunci putem gândi tabla operației ca o matrice $A=\left(a_{ij}\right)_{ij=\overline{1,n}}$.

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Dacă luăm $M=\{1,-1,i,-i\}$ cu operația de înmulțire, atunci avem tabla legii prezentată alăturat. Alcătuiți tabla legii pe mulțimea M în cazurile:

1) $M=\{1, 2, 3, 4, 5, 6\}$, $x * y = \min\{x, y\}$;

2) $M=\{1, 2, 3, 4, 5, 6\}$, $x\circ y = \text{c.m.m.d.c.}\{x, y\}$.

1.2. PARTE STABILĂ

Dacă $(M,*)$ este o structură algebrică, iar *H* este o submulţime nevidă a lui *M*, atunci pentru $x.y \in H$ elementul $x * y$ poate să fie în mulţimea *H* sau să fie în afara ei, adică în $M - H$.

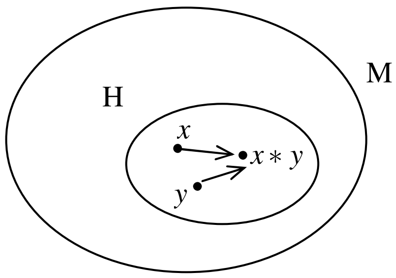
Definiţie. Dacă pentru orice $x, y \in H$, compusul $x * y$ aparţine tot lui *H*, atunci spunem că *H* este **parte stabilă a lui *M* în raport cu operaţia** $*$ **.**

Deci, $\varnothing \neq H \subset M$ este parte stabilă a lui *M* în raport cu $* \Leftrightarrow [\forall x, y \in H \Rightarrow$ $\Rightarrow x * y \in H]$ (fig. 1)

În raport cu adunarea, $\mathbb{N}$ este parte stabilă a lui $\mathbb{Z}$, $\mathbb{Z}$ este parte stabilă a lui $\mathbb{Q}$ etc.

Analog, în raport cu adunarea matricelor $\mathcal{M}_{m,n}(\mathbb{Z})$ este parte stabilă a lui $\mathcal{M}_{m,n}(\mathbb{Q})$, $\mathcal{M}_{m,n}(\mathbb{Q})$ este parte stabilă a lui $\mathcal{M}_{m,n}(\mathbb{R})$ etc.

Dacă $\mathcal{I}(M), \mathcal{S}(M)$ sunt mulţimea funcţiilor injective definite pe *M* cu valori în *M* şi respectiv mulţimea funcţiilor surjective de la *M* la *M*, atunci acestea sunt părţi stabile ale lui $\mathcal{F}(M)$ în raport cu operaţia de compunere a funcţiilor.



$x, y \in H \Rightarrow x * y \in H$

Fig. 1

Observaţii. **1)** Adjectivul „stabilă“ din noţiunea de „parte stabilă“ pentru o submulţime *H* a lui *M* în raport cu $*$ vine să precizeze că dacă $x, y \in H$ (sunt două elemente arbitrare din *H*), atunci şi compusul lor $x * y$ rămâne în *H*.

2) Dacă $H \subset M$ şi se consideră o aplicaţie $*$ pentru *H*, atunci aceasta nu este neapărat o lege de compoziţie. Acest lucru trebuie dovedit. Deci enunţul nu poate fi de forma:

„Fie *H* o mulţime şi legea de compoziţie pe *H*, $x * y = \ldots$“.

Exemplificăm acest lucru prin următoarea problemă:

Fie $H = [0,2]$ şi aplicaţia $x * y = xy - x - y + 2,\ (\forall)x, y, \in H$.

Arătaţi că $*$ este o lege de compoziţie pe *H*.

Deci trebuie să arătăm că $(\forall)x, y \in H \Rightarrow x * y \in H$. Ori avem $x * y = (x-1)(y-1)+1$.

Cum $x, y \in H \Rightarrow |x-1| \leq 1, |y-1| \leq 1$.

Prin urmare faptul că $x \in H \Leftrightarrow |x-1| \leq 1$. Deci $x * y \in H \Leftrightarrow |x * y - 1| \leq 1 \Leftrightarrow |(x-1)(y-1)| \leq 1 \Leftrightarrow$ $|x-1||y-1| \leq 1$, ceea ce este adevărat pentru că $|x-1| \leq 1, |y-1| \leq 1$.

3) Dacă *H este parte stabilă* a lui M în raport cu $*$, atunci $H \times H \subset M \times M$ şi deci putem vorbi de restricţia legii $*$ la $H \times H$, care este tot o lege de compoziţie. Pentru comoditate vom nota şi restricţia tot cu $*$.
Deci, dacă H este parte stabilă a lui M în raport cu $*$, atunci legea de compoziţie $*: H \times H \to H$ se spune că este indusă de legea de compoziţie de pe M. Se mai spune că legea de pe M induce pe H o lege de compoziţie.

Probleme rezolvate

1. Fie $M = \mathbb{Z}$, iar $H = 2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ (mulţimea numerelor întregi pare) şi $H' = 2\mathbb{Z}+1 = \{2k+1 \mid k \in \mathbb{Z}\}$ (mulţimea numerelor întregi impare) avem $H, H' \subset \mathbb{Z}$.

R. Pe $\mathbb{Z}$ considerăm legea de compoziţie adunarea numerelor întregi. Se constată uşor că H este parte stabilă a lui $\mathbb{Z}$ în raport cu adunarea deoarece din $x, y \in H$, $x = 2k, y = 2l$, $k, l \in \mathbb{Z}$ avem $x + y = 2(k + l) \in 2\mathbb{Z}$ în timp ce H' nu este parte stabilă a lui $\mathbb{Z}$ în raport cu adunarea pentru că dacă $x, y \in 2\mathbb{Z}+1$, $x = 2k+1$, $y = 2l+1$, $k, l \in \mathbb{Z}$, atunci $x + y = 2(k + l + 1) \notin 2\mathbb{Z}+1$.

2. Pentru $M = \mathbb{Z}$ considerăm legea de compoziţie $x * y = \max(x, y)$. Fie $H = \{0, 1, 2, 3, 4\}$. Atunci H este o parte stabilă a lui $\mathbb{Z}$ în raport cu $*$.

R. Într-adevăr, acest lucru va reieşi din tabla legii pentru H.
Observăm că toate elementele (rezultate din compunere) ce figurează în tablă aparţin lui H. Prin urmare H este parte stabilă a lui $\mathbb{Z}$ în raport cu legea $*$.

$*$	0	1	2	3	4
0	0	1	2	3	4
1	1	1	2	3	4
2	2	2	2	3	4
3	3	3	3	3	4
4	4	4	4	4	4

3. Fie $M = \mathbb{R}$ şi legea de compoziţie $x * y = xy - x - y + 2$. Considerăm intervalele H = (1, 2), H' = (2, 3) submulţimi ale lui $\mathbb{R}$. Să probăm că H este parte stabilă a lui $\mathbb{R}$ în raport cu $*$, în timp ce H' nu are această proprietate.

R. Într-adevăr, fie $x, y \in H$. Atunci trebuie probat că $x * y \in H \Leftrightarrow 1 < xy - x - y + 2 < 2 \Leftrightarrow$ $\Leftrightarrow 1 < (x-1)(y-1) + 1 < 2 \Leftrightarrow 0 < (x-1)(y-1) < 1$ ceea ce este evident, deoarece $x, y \in H \Leftrightarrow$ $\Leftrightarrow 1 < x, y < 2 \Leftrightarrow 0 < x-1, y-1 < 1$, iar de aici $0 < (x-1)(y-1) < 1$.

Pentru afirmaţia relativă la H' este de observat că luând $x = \frac{5}{2}, y = \frac{5}{2}$ din H', rezultă $x * y = \frac{5}{2} \cdot \frac{5}{2} - \frac{5}{2} - \frac{5}{2} + 2 = \frac{13}{4} \notin H'$. Deci nu pentru orice $x, y \in H' \Rightarrow x * y \in H'$.

4. Fie $M = \mathbb{C}$ împreună cu operaţia de înmulţire a numerelor complexe şi $H = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Să arătăm că H este parte stabilă a lui $\mathbb{C}$ în raport cu înmulţirea.

R. Fie $x = a + bi$ şi $y = c + di$, $a, b, c, d \in \mathbb{Z}$. Atunci $xy = (a + bi)(c + di) = ac - bd + i(ad + bc) \in \mathbb{Z}[i]$, deoarece $ac - bd$, $ad + bc \in \mathbb{Z}$ (operaţii cu numere întregi).

5. Fie $M = \mathbb{R}$ şi legea de compoziţie $x \top y = 7xy - 7(x + y) + 8$. Arătaţi că $H = (1, \infty)$ este parte stabilă a lui $\mathbb{R}$ în raport cu $\top$.

R. Trebuie să arătăm că dacă $x, y > 1$, atunci $x \top y > 1$.
Avem $x \top y = 7(x-1)(y-1) + 1 > 1 \Leftrightarrow (x-1)(y-1) > 0$, evident.
Altfel. Se pot lua $x, y > 1$ sub forma $x = 1 + \alpha$, $y = 1 + \beta$, $\alpha, \beta > 0$ când $x \top y = 7\alpha\beta + 1 > 1$.

6. Considerăm $M = \mathcal{M}_3(\mathbb{R})$ împreună cu operaţia de înmulţire a matricelor, iar $H = \left\{A(a) = \begin{pmatrix} a & 0 & a \\ 0 & 0 & 0 \\ a & 0 & a \end{pmatrix} \middle| a \in \mathbb{R}\right\}$. Să probăm că H este o parte stabilă a lui M în raport cu înmulţirea.

R. Într-adevăr, fie $A(a)=\begin{pmatrix} a & 0 & a \\ 0 & 0 & 0 \\ a & 0 & a \end{pmatrix}$ şi $A(b)=\begin{pmatrix} b & 0 & b \\ 0 & 0 & 0 \\ b & 0 & b \end{pmatrix}$ din *H*.

Avem $A(a)A(b)=\begin{pmatrix} 2ab & 0 & 2ab \\ 0 & 0 & 0 \\ 2ab & 0 & 2ab \end{pmatrix}=A(2ab)\in H$, deoarece $2ab\in\mathbb{R}$ şi matricea obţinută are forma matricelor din *H*.

7. Fie $M=\mathcal{F}(\mathbb{R})=\{f:\mathbb{R}\to\mathbb{R}\}$ împreună cu operaţia de compunere a funcţiilor şi $H=\{f_{a,b}:\mathbb{R}\to\mathbb{R},\ f_{a,b}(x)=ax+b \mid a,b\in\mathbb{R}, a\neq 0\}$ (transformările afine ale dreptei reale).

R. Din $f_{a,b}\circ f_{c,d}=f_{ac,ad+b}$, $ac\neq 0$ rezultă că *H* este parte stabilă a lui *M* în raport cu $\circ$.

8. Pe $\mathbb{R}$ se consideră legea de compoziţie „$*$" definită astfel: $x*y=xy+8(x+y)+\alpha$, $\alpha\in\mathbb{R}$. Să se determine α astfel încât $H=(-8,\infty)$ să fie parte stabilă a lui $\mathbb{R}$ în raport cu „$*$".

R. Fie $\alpha\in\mathbb{R}$ pentru care *H* este parte stabilă a lui $\mathbb{R}$. Fie $y_0>-8$ fixat din *H*. Atunci, pentru orice $x\in H$ rezultă $x*y_0\in H$. De aici $\lim\limits_{x\searrow -8}(xy_0+8x+8y_0+\alpha)\geq -8$, adică $\alpha\geq 56$. Reciproc, dacă $\alpha\geq 56$, atunci $x*y=(x+8)(y+8)-64+\alpha>-64+56=-8, \forall x,y\in H$, ceea ce arată că *H* este parte stabilă a lui $\mathbb{R}$ în raport cu legea $*$.

9. Se consideră $H=\left\{\begin{pmatrix} 1 & x & ax^2+bx \\ 0 & 1 & cx \\ 0 & 0 & 1 \end{pmatrix} \middle| x\in\mathbb{R}, a,b,c\in\mathbb{R}\right\}$. Să se determine *a*, *b*, *c*, astfel încât *H* să fie parte stabilă a lui $\mathcal{M}_3(\mathbb{R})$ în raport cu înmulţirea matricelor.

R. Fie $A(x), A(y)\in H$. Atunci:

$$A(x)A(y)=\begin{pmatrix} 1 & x+y & ax^2+cxy+ay^2+bx+by \\ 0 & 1 & c(x+y) \\ 0 & 0 & 1 \end{pmatrix}=A(x+y)\in H$$

dacă $ax^2+cxy+ay^2+bx+by=a(x+y)^2+b(x+y)$. De aici $c=2a$, $a,b\in\mathbb{R}$.

Probleme propuse

1. Pe $\mathbb{N}^*$ se consideră legea de compoziţie $x*y=\text{c.m.m.d.c.}(x,y)$. Fie $H=\{x\in\mathbb{N}^* \mid x \text{ divide } 10\}$.

Arătaţi că *H* este parte stabilă a lui $\mathbb{N}^*$ în raport cu $*$, construind tabla legii.

2. Pe mulţimea $\mathbb{Z}$ definim legile de compoziţie:

$x\oplus y=$ restul împărţirii lui $x+y$ prin 5,

$x\otimes y=$ restul împărţirii lui $x\cdot y$ prin 5.

Arătaţi că $H=\{0,1,2,3,4\}$ este parte stabilă a lui $\mathbb{Z}$ în raport cu fiecare din cele două legi, alcătuind tablele legilor.

3. Fie $H=\{-3,-1,0,1\}\subset\mathbb{Z}$ şi $x*y=\min(x,y)$ o lege de compoziţie pe $\mathbb{Z}$. Probaţi că *H* este parte stabilă a lui $\mathbb{Z}$ în raport cu $*$, alcătuind tabla legii.

4. Arătați că $\mathbb{Z}\left[\sqrt{p}\right]=\{a+b\sqrt{p}|a,b\in\mathbb{Z},\ p\in\mathbb{N}^*\ \text{prim}\}$,

$$\mathbb{Q}\left[\sqrt{p}\right]=\{a+b\sqrt{p}|a,b\in\mathbb{Q},\ p\in\mathbb{N}^*\ \text{prim}\}$$

sunt părți stabile ale lui $\mathbb{R}$ în raport cu adunarea și înmulțirea.

5. Să se arate că $H=\{z\in\mathbb{C}\mid |z|=1\}$ este parte stabilă a lui $\mathbb{C}$ în raport cu operația de înmulțire. Este finită mulțimea H ?

6. Pe $\mathbb{R}$ se consideră legea de compoziție $x*y=xy-2(x+y)+6$. Să se arate că $H=(1,3)$ este parte stabilă a lui $\mathbb{R}$ în raport cu legea $*$.

7. Pe $\mathbb{R}$ se consideră legea $x\perp y=5xy-20(x+y)+84$. Să se arate că $H=[4,\infty)$ este parte stabilă a lui $\mathbb{R}$ în raport cu legea $*$.

8. Pe $\mathbb{R}$ considerăm legea de compoziție $x*y=\sqrt{x^2+y^2-9}$. Arătați că $H=[3,\infty)$ este o parte stabilă a lui $\mathbb{R}$ în raport cu $*$.

9. Arătați că următoarele submulțimi ale lui $\mathbb{C}$ sunt părți stabile în raport cu înmulțirea numerelor complexe:

a) $\left\{2^n|n\in\mathbb{Z}\right\}$; b) $\left\{a+b\sqrt{3}|a,b\in\mathbb{Z},\ a^2+b^2\neq 0\right\}$; c) $\left\{z\,|\,|z|\leq 1\right\}$;

d) $\left\{z\,|\,|z|>1\right\}$; e) $\left\{z\,|\,|z|\geq 2\right\}$; f) $\left\{z\,|\,|z|<\frac{1}{2}\right\}$

10. Pe $\mathcal{F}(\mathbb{R}-\{0,1\})$ considerăm operația de compunere a funcțiilor. Fie $H=\{f_1,f_2,f_3\}$, $f_i:\mathbb{R}-\{0,1\}\to\mathbb{R}-\{0,1\},\ i=1,2,3,\ f_1(x)=x,\ f_2(x)=\frac{x-1}{x},\ f_3(x)=\frac{1}{1-x},x\in\mathbb{R}-\{0,1\}$.
Probați că H este parte stabilă a lui $\mathcal{F}(\mathbb{R}-\{0,1\})$ în raport cu operația de compunere, alcătuind tabla legii.

11. Pe $\mathcal{F}(\mathbb{R}-\{0\})$ se consideră operația de compunere a funcțiilor.
Fie $H=\{f_1,f_2,f_3,f_4\}\subset\mathcal{F}(\mathbb{R}-\{0\})$, unde $f_1(x)=x,\ f_2(x)=-x,\ f_3(x)=\frac{1}{x},f_4(x)=-\frac{1}{x}$.
Arătați că H este parte stabilă a lui $\mathcal{F}(\mathbb{R}-\{0\})$ în raport cu $\circ$, alcătuind tabla legii.

12. Determinați părțile finite ale lui $\mathbb{R}$ stabile în raport cu adunarea din $\mathbb{R}$ și părțile finite ale lui $\mathbb{R}$ stabile în raport cu înmulțirea din $\mathbb{R}$.

13. Fie $H=\left\{A(a)=\begin{pmatrix}1 & \ln a & 0\\ 0 & 1 & 0\\ 0 & 0 & a\end{pmatrix}\middle|\,a>0\right\}\subset\mathcal{M}_3(\mathbb{R})$.

Arătați că H este parte stabilă a lui $\mathcal{M}_3(\mathbb{R})$ în raport cu operația de înmulțire.

14. Fie $H=\left\{A_\alpha=\begin{pmatrix}\cos\alpha & \sin\alpha\\ -\sin\alpha & \cos\alpha\end{pmatrix}\middle|\,\alpha\in\mathbb{R}\right\}\subset\mathcal{M}_2(\mathbb{R})$

Să se arate că H este o parte stabilă a lui $\mathcal{M}_2(\mathbb{R})$ în raport cu operația de înmulțire.

15. Fie $H=\{A, B, C, D, E, F, G, H\}$ unde $A=\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$, $B=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$, $C=\begin{pmatrix}0 & -i\\ -i & 0\end{pmatrix}$, $D=\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}$,

$E=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, $F=\begin{pmatrix}-i & 0\\ 0 & -i\end{pmatrix}$, $G=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$, $H=\begin{pmatrix}i & 0\\ 0 & i\end{pmatrix}$.

Arătați că H este o parte stabilă a lui $\mathcal{M}_2(\mathbb{C})$ în raport cu înmulțirea matricelor şi alcătuiți tabla operației induse pe H.

16. **Fie** $H=\left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix} \middle| a,b,c,d\in\mathbb{Z}, a+b=c+d\right\}\subset\mathcal{M}_2(\mathbb{Z})$. **Arătați că H este parte stabilă a lui $\mathcal{M}_2(\mathbb{Z})$ în raport cu operația de înmulțire a matricelor.**

17. **Fie** $H=\left\{A\in\mathcal{M}_2(\mathbb{Q}) \middle| A=\begin{pmatrix} 2x & 3y \\ y & 2x\end{pmatrix}, 4x^2-3y^2=1, x,y\in\mathbb{Q}\right\}$. **Să se arate că H este parte stabilă a lui $\mathcal{M}_2(\mathbb{Q})$ în raport cu înmulțirea matricelor şi** $\operatorname{card}(H)=\infty$.

18. **Se consideră matricea** $A=\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0\end{pmatrix}$ **şi mulțimea** $H=\left\{A^n \middle| n\in N^*\right\}\subset\mathcal{M}_3(\mathbb{R})$. **Arătați că H este parte stabilă a lui $\mathcal{M}_3(\mathbb{R})$ în raport cu înmulțirea matricelor. Alcătuiți tabla operației pentru H.**

19. **Pe $\mathbb{R}$ se defineşte legea de compoziție $*$ prin $x*y=x+y+xy$. Să se determine $a\in\mathbb{R}$ astfel încât mulțimea $H=[a,\infty)$ să fie parte stabilă a lui $\mathbb{R}$ în raport cu legea $*$.**

20. **Pentru ce valori ale parametrului real a, intervalul I este parte stabilă a lui $\mathbb{R}$ în raport cu „$*$" în cazurile:**

1) $x*y=xy-2x-2y+a, I=(2,\infty)$; **2)** $x*y=x+y+axy, I=[-1,\infty)$

21.* **Pe $\mathbb{R}$ se defineşte legea de compoziție $x*y=xy-a(x+y)+b, a,b\in\mathbb{R}$. Să se arate că (a,∞) este parte stabilă a lui $\mathbb{R}$ în raport cu $*$ dacă şi numai dacă $b-a^2-a\geq 0$.**

22.* **Arătați că părțile finite ale lui $\mathbb{C}$ stabile față de înmulțire sunt:**
$\{0\}, U_n, \{0\}\cup U_n, n\in\mathbb{N}^*, U_n=\left\{x \middle| x^n=1\right\}$.

1.3. PROPRIETĂȚI GENERALE ALE LEGILOR DE COMPOZIȚIE

În cele ce urmează vom considera structura algebrică $(M,*)$. Pentru legea notată $*$ vom folosi denumirea de legea star (sau stea).

P1. Asociativitatea

> **Definiție.** Legea $*$ se numeşte **asociativă** dacă:
> $$(x*y)*z=x*(y*z),\ (\forall)x,y,z\in M.$$

În membrul stâng, $(x*y)*z$, se efectuează mai întâi calculul din paranteză, $x*y$ şi apoi rezultatul acestuia se „compune" cu z. În membrul drept efectuăm operaţia din paranteză, $y*z$ şi apoi calculăm $x*(y*z)$.

Definiţia spune că indiferent cum am efectua calculele algebrice în cei doi membri obţinem acelaşi rezultat.

Din acest motiv dacă legea $*$ este asociativă, atunci se omit în scriere parantezele şi se scrie simplu $x*y*z$.

Vom da acelaşi nume structurii algebrice $(M,*)$ definită prin $*$, adică vom spune că este o structură algebrică asociativă, sau spunem simplu că legea $*$ este asociativă pe M.

Dacă H **este o parte stabilă** a lui M în raport cu legea $*$ şi dacă $*$ **este asociativă** pe M, atunci $*$ rămâne asociativă şi pe H.

Altfel spus $(H,*)$ devine o structură algebrică asociativă.

Spre exemplu adunarea şi înmulţirea matricelor din $\mathcal{M}_n(\mathbb{C})$ sunt operaţii asociative. Dacă H este o parte stabilă a lui $\mathcal{M}_n(\mathbb{C})$ în raport cu cele două operaţii, atunci $(H, +)$, $(H,\cdot)$ sunt structuri algebrice asociative.

Pentru $H=\{-1,1\}\subset\mathbb{R}$, înmulţirea este asociativă pe H, deoarece este asociativă pe $\mathbb{R}$.

Observaţii. 1) O lege $*$ **nu este asociativă** dacă **există** $x,y,z\in M$ pentru care $(x*y)*z\neq x*(y*z)$.

2) Dacă $x_1, x_2, ..., x_n\in M$ şi pe M legea $*$ este asociativă, atunci prin compunerea elementelor date (în acea ordine) înţelegem $x_1*x_2*...*x_n$ element din M obţinut prin recurenţă. Pentru $n = 1$ el este x_1.

Dacă am obţinut elementul $x_1*x_2*...*x_{n-1}$, atunci $x_1*x_2*...*x_n=(x_1*x_2*...*x_{n-1})*x_n$.

Dacă legea de compoziţie pe M este multiplicativă, atunci $\prod_{i=1}^{n} x_i = x_1x_2...x_n = (x_1x_2...x_{n-1})x_n$, iar în notaţia aditivă în loc de produsul elementelor $x_1,x_2,...,x_n$ avem suma lor $x_1+x_2+...+x_n=\sum_{i=1}^{n} x_i$.

Exemple cunoscute de legi asociative

1. Adunarea şi înmulţirea pe $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sunt legi asociative.

2. Reuniunea, intersecţia pe $\mathcal{P}(M)$ sunt legi asociative.

3. Adunarea şi compunerea funcţiilor pe $\mathcal{F}(M)$ sunt legi asociative.

4. Adunarea şi înmulţirea matricelor pe $\mathcal{M}_n(\mathbb{C})$ sunt legi asociative.

Exemple de legi neasociative

1. Scăderea pe $\mathbb{R}$. Arătăm că există $x, y, z \in \mathbb{R}$ pentru care $(x-y)-z \neq x-(y-z)$. Fie $x = 5, y = 1$, $z = -3$. Atunci $(x-y)-z=(5-1)-(-3)=4+3=7$ şi $x-(y-z)=5-(1+3)=1$. Cum $7 \neq 1$, deducem că scăderea pe $\mathbb{R}$ nu este asociativă.

2. Diferenţa de mulţimi pe $\mathcal{P}(\mathbb{R})$.

Fie $A = \mathbb{R}$, $B=(0,\infty)$, $C=(-\infty,0)$. Atunci $(A-B)-C=(-\infty,0]-(-\infty,0)=\{0\}$ şi $A-(B-C)=\mathbb{R}-(0,\infty)=(-\infty,0]$.

Deci $(A-B)-C \neq A-(B-C)$.

Probleme rezolvate

1. Fie $H = \{0, 1, 2, 3, 4\}$ şi aplicaţia $x * y = |x-y|$, $x, y \in H$. Arătaţi că $*$ este lege de compoziţie şi stabiliţi dacă este asociativă.

$*$	0	1	2	3	4
0	0	1	2	3	4
1	1	0	1	2	3
2	2	1	0	1	2
3	3	2	1	0	1
4	4	3	2	1	0

R. Tabla aplicaţiei este dată alăturat şi se constată că $x * y \in H$, $(\forall) x, y \in H$. Prin urmare aplicaţia este o lege de compoziţie pe *H*. Legea nu este asociativă deoarece există $x=1,\ y=2,\ z=4$ pentru care $(x*y)*z=3 \neq x*(y*z)=1$.

2. Pe mulţimea numerelor reale $\mathbb{R}$ definim legea de compoziţie $x * y = \sqrt[3]{xy}$. Arătaţi că această lege nu este asociativă.

R. Va trebui să găsim trei numere $x, y, z \in \mathbb{R}$ pentru care $(x*y)*z \neq x*(y*z)$. Alegem $x=1, y=-2, z=3$ pentru care $(x*y)*z=\sqrt[3]{-2}*3=\sqrt[3]{3\sqrt[3]{-2}}$ şi $x*(y*z)=1*\sqrt[3]{-6}=\sqrt[3]{\sqrt[3]{-6}}=\sqrt[9]{-6}$.

Evident $\sqrt[3]{3\sqrt[3]{-2}}=\sqrt[9]{-54} \neq \sqrt[9]{-6}$.

3. Definim pe $\mathbb{R}$ legea de compoziţie $x * y = xy - x - y + 2$.

Arătaţi că legea $*$ induce pe (1,2) o lege de compoziţie asociativă.

R. Am văzut la problema rezolvată 3 din paragraful de la parte stabilă că (1,2) este parte stabilă a lui $\mathbb{R}$ în raport cu legea $*$.

Pentru a proba asociativitatea legii trebuie să demonstrăm că

$$(x*y)*z=x*(y*z),\ (\forall)x,y,z\in(1,3). \tag{1}$$

Calculăm membrul stâng al egalităţii şi avem:

$$\begin{aligned}(x*y)*z&=(xy-x-y+2)*z=(xy-x-y+2)\cdot z-(xy-x-y+2)-z+2=\\&=xyz-(xy+yz+xz)+x+y+z.\end{aligned} \tag{2}$$

Membrul drept al egalităţii (1) se scrie:

$$\begin{aligned}x*(y*z)&=x*(yz-y-z+2)=x(yz-y-z+2)-x-(yz-y-z+2)+2=\\&=xyz-(xy+xz+yz)+x+y+z.\end{aligned} \tag{3}$$

Din (2) şi (3) se deduce (1). Prin urmare legea este asociativă.

4. Fie $H=\left\{f_k:\mathbb{R}\to\mathbb{R},\ f_k(x)=x^k \,\middle|\, k\in\mathbb{N}^*\right\}\subset\mathcal{F}(\mathbb{R})$.

Arătaţi că *H* este o parte stabilă a lui $\mathcal{F}(\mathbb{R})$ în raport cu operaţia de compunere a funcţiilor şi această operaţie induce pe *H* o lege asociativă.

R. Pentru a arăta că H este parte stabilă a lui $\mathcal{F}(\mathbb{R})$ în raport cu operația de compunere trebuie verificat că: $(\forall) f_k, f_n \in H \Rightarrow f_k \circ f_n \in H$. Ori avem $f_k \circ f_n : \mathbb{R} \to \mathbb{R}$ și $f_k \circ f_n(x) = f_k(f_n(x)) = f_k\left(x^n\right) = \left(x^n\right)^k =$
$= x^{nk} = f_{nk}(x), (\forall) x \in \mathbb{R}$.

Așadar $f_k \circ f_n = f_{nk} \in H$ deoarece din $n,k \in \mathbb{N}^* \Rightarrow nk \in \mathbb{N}^*$.
Se știe că întotdeauna compunerea funcțiilor pe $\mathcal{F}(\mathbb{R})$ este asociativă. Atunci ea rămâne la fel și pe submulțimea *H.*

5. Pe $\mathbb{R} - (-1,1)$ definim legea $x * y = \sqrt{x^2y^2 - x^2 - y^2 + 2}$. Arătați că această lege induce pe $(1,\infty)$ o lege asociativă.

R. Arătăm mai întâi că $(1,\infty)$ este parte stabilă a $\mathbb{R} - (-1,1)$ în raport cu $*$. Fie $x, y > 1$ și să arătăm că:
$x * y > 1 \Leftrightarrow \sqrt{x^2y^2 - x^2 - y^2 + 2} > 1 \Leftrightarrow x^2y^2 - x^2 - y^2 + 2 > 1 \Leftrightarrow \left(x^2 - 1\right)\left(y^2 - 1\right) > 0$, evident deoarece $x, y > 1$.

Așadar $((1,\infty), *)$ este structură algebrică.
Să probăm acum că $*$ este o lege asociativă, adică să demonstrăm că

$$(x * y) * z = x * (y * z),\ (\forall) x, y, z \in (1,\infty) \tag{1}$$

Avem: $(x * y) * z = \sqrt{x^2y^2 - x^2 - y^2 + 2} * z =$

$$= \sqrt{\left(x^2y^2 - x^2 - y^2 + 2\right)z^2 - \left(x^2y^2 - x^2 - y^2 + 2\right) - z^2 + 2} =$$

$$= \sqrt{(xyz)^2 - \left(x^2y^2 + x^2z^2 + y^2z^2\right) + x^2 + y^2 + z^2} \tag{2}$$

și $\quad x * (y * z) = x * \sqrt{y^2z^2 - y^2 - z^2 + 2} =$

$$= \sqrt{x^2\left(y^2z^2 - y^2 - z^2 + 2\right) - x^2 - \left(y^2z^2 - y^2 - z^2 + 2\right) + 2} =$$

$$= \sqrt{(xyz)^2 - \left(x^2y^2 + x^2z^2 + y^2z^2\right) + x^2 + y^2 + z^2}\ . \tag{3}$$

Din (2) și (3) rezultă (1) .

6. Pe $\mathbb{R}$ definim legea de compoziție $x * y = ax + by, a,b \in \mathbb{R}^*$. Determinați pe *a, b* astfel încât legea să fie asociativă.

R. Condiția pentru asociativitatea legii este: $(x * y) * z = x * (y * z),\ (\forall) x, y, z \in \mathbb{R}$ sau
$(ax + by) * z = x * (ay + bz), (\forall) x, y, z \in \mathbb{R}$ sau încă
$a(ax + by) + bz = ax + b(ay + bz), (\forall x, y, z \in \mathbb{R})$ sau în fine

$$a^2x + aby + bz = ax + aby + b^2z, (\forall) x, y, z \in \mathbb{R}, \tag{1}$$

Cum (1) are loc pentru orice valori reale ale lui *x, y, z,* atunci are loc evident și pentru $x = 1$, $y = z = 0$ când obținem $a^2 = a$, (2).
De asemenea (1) are loc și pentru $x = z = 0$, $y = 1$ când $ab = ab$, evident. În fine punând în (1) $x = y = 0$, $z = 1$ rezultă $b = b^2$, (3).

Din (2) şi (3), ţinând cont că $a,b \neq 0$ deducem $a = b = 1$, care verifică (1). Aşadar legea $x * y = x + y$ este asociativă.

7*. Arătaţi că legea $*$ definită prin: $x * y = xy - \sqrt{x^2y^2 - x^2 - y^2 + 1}$, $x, y \in [-1,1]$, determină pe [-1, 1] o lege neasociativă.

R. Mai întâi arătăm că $([-1,1],*)$ este o structură algebrică, altfel spus $(\forall)\, x, y \in [-1,1] \Rightarrow$ $\Rightarrow x * y \in [-1,1]$. Pentru numerele $x, y \in [-1,1]$, există $\alpha, \beta \in [0,\pi]$ pentru care $x = \cos\alpha$, $y = \cos\beta$. Cu aceste scrieri legea $*$ are forma $x * y = \cos\alpha\cos\beta - |\sin\alpha\sin\beta| = \cos\alpha\cos\beta - \sin\alpha\sin\beta =$ $= \cos(\alpha+\beta) \in [-1,1]$.

Demonstrăm acum că legea nu este asociativă deoarece există $x = \frac{1}{2}$, $y = -\frac{1}{2}$, $z = 0$ pentru care (după unele calcule) $(x * y) * z = 0$, iar $x * (y * z) = -\frac{\sqrt{3}}{2}$. Aşadar nu pentru orice $x, y, z \in [-1,1]$ avem $(x * y) * z = x * (y * z)$.

8. Pe mulţimea $\mathbb{R}$ se consideră legea de compoziţie definită prin:

$$x * y = axy - b(x + y) + c, a, b, c \in \mathbb{R}$$

Ce relaţie trebuie să existe între *a, b, c,* pentru ca legea să fie asociativă?

R. Legea $*$ este asociativă dacă are loc egalitatea $(x * y) * z = x * (y * z)$, $(\forall) x, y, z \in \mathbb{R}$. Calculând fiecare membru se ajunge la egalitatea

$a^2xyz - ab(xy + xz + yz) + (ac - b)z + b^2(x + y) - bc + c = a^2xyz - ab(xy + xz + yz) +$ $+(ac-b)x + b^2(y+z) - bc + c, (\forall) x, y, z \in \mathbb{R}$, sau după unele calcule, $(ac - b - b^2)(x - z) = 0, (\forall) x, y, z \in \mathbb{R}$.

Această ultimă egalitate are loc dacă şi numai dacă $ac - b - b^2 = 0$.

Probleme propuse

1. Stabiliţi care din următoarele aplicaţii sunt operaţii algebrice asociative pe submulţimea $(0,\infty)$ a lui $\mathbb{R}$:

a) $a * b = \frac{a+b}{2}$; b) $a \circ b = a + b - 1$; c) $a \top b = ab^2$; d) $a \perp b = a^b$; e) $a * b = \sqrt{ab}$;

f) $a \circ b = \log_b a$; g) $a \top b = \max\{a,b\}$; h) $a \top b = |a - b|$.

2. Pe $\mathbb{R}$ se definesc următoarele legi de compoziţie:

a) $x * y = x + y + 2$; b) $x \circ y = 4xy$; c) $x \top y = x + y - 7xy$; d) $x \perp y = xy - 4x - 4y + 20$;

e) $x * y = x + y - \frac{xy}{2}$; f) $x \circ y = \sqrt[3]{x^3 + y^3}$. Care din aceste legi este asociativă?

3. Fie $H = \{f_a : (2,\infty) \to (2,\infty), f_a(x) = 2 + (x-2)^a, a > 0\}$. Arătaţi că $(H,\circ)$ este structură algebrică asociativă, unde $\circ$ este compunerea funcţiilor.

4. Fie $H = \left\{A = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{R}, \det(A) = 1\right\} \subset \mathcal{M}_2(\mathbb{R})$. Arătaţi că:

1) H este parte stabilă infinită a lui $\mathcal{M}_2(\mathbb{R})$ în raport cu înmulţirea matricelor.

2) $(H,\cdot)$ este structură algebrică asociativă.

5. Fie $H=\left\{f_a:\mathbb{R}\to\mathbb{R} \middle| f_a(x)=\begin{cases}0, & x<0\\ ax, & x\geq 0\end{cases}, a>0\right\}\subset\mathcal{F}(\mathbb{R})$. **Arătați că:**

1) H **este parte stabilă a lui** $\mathcal{F}(\mathbb{R})$ **în raport cu operația de compunere a funcțiilor; 2) legea** $\circ$ **pe** H **este asociativă.**

6. **Pe** $\mathbb{R}$ **se consideră legea de compoziție** $x*y=mx+y, m\in\mathbb{R}$. **Să se determine** m **astfel încât legea să fie asociativă.**

7. **Pe** $\mathbb{R}$ **se definește legea de compoziție** $x*y=xy+2a(x+y), a\in\mathbb{R}$. **Determinați** a **astfel încât legea să fie asociativă.**

8. **Pe** $\mathbb{R}$ **definim legile de compoziție**

$$x*y=ax+by-1,\quad x\circ y=2xy-2x-2y+c,\ x,\quad y=axy+y+b, a,b,c\in\mathbb{R}.$$

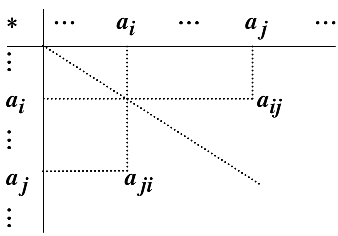
Determinați ***a, b, c*** **astfel încât operațiile să fie asociative.**

P2. Comutativitatea

Definiție. Legea $*$ se numește **comutativă** dacă:

$$x*y=y*x, (\forall)x,y\in M.$$

Din această definiție deducem că pentru o lege comutativă nu contează ordinea în care compunem. În membrul stâng primul element în compunere este *x*, al doilea fiind *y*, în timp ce în membrul drept primul element din compunere este *y*, iar al doilea este *x*. Rezultatul este același. Dacă mulțimea *M* este finită, $M=\{a_1, a_2, \ldots, a_n\}$, atunci comutativitatea legii se traduce prin $a_{ij}=a_{ji}$, $(\forall)i,j=\overline{1,n}$, unde $a_{ij}=a_i*a_j$. Gândită tabla legii ca o matrice pătratică înseamnă că elementul a_{ij} este simetricul lui a_{ji}, în raport cu diagonala principală (vezi tabla de mai jos). Pentru $n=4$, tabla legii comutative este următoarea:



$*$	a_1	a_2	a_3	a_4
a_1	a_{11}	a_{12}	a_{13}	a_{14}
a_2	a_{12}	a_{22}	a_{23}	a_{24}
a_3	a_{13}	a_{23}	a_{33}	a_{34}
a_4	a_{14}	a_{24}	a_{34}	a_{44}

Ca și în cazul terminologiei folosite pentru legea asociativă și aici vom da același nume structurii algebrice $(M,*)$ definită prin $*$ spunând că dacă $*$ este comutativă, atunci structura algebrică este comutativă sau mai simplu spunem că $*$ este comutativă pe *M*.

Un alt element important utilizat în aplicații este următorul:

> Dacă H **este o parte stabilă** a lui M în raport cu legea $*$ şi dacă $*$ **este comutativă** pe M, atunci $*$ rămâne comutativă şi pe H.

Altfel spus $(H,*)$ devine la rândul ei o structură algebrică comutativă. De exemplu adunarea şi înmulțirea pe $\mathbb{R}$ sunt operații comutative întotdeauna. Atunci aceste operații rămân la fel de exemplu pe $\mathbb{Q}\left[\sqrt{2}\right]=\left\{a+b\sqrt{2}\,|\,a,b\in\mathbb{Q}\right\}$ dacă am arătat în prealabil că $\mathbb{Q}\left[\sqrt{2}\right]$ este parte stabilă a lui $\mathbb{R}$ în raport cu cele două operații.

Observație. O lege $*$ **nu este comutativă** dacă există $x, y \in M$ astfel încât $x*y \neq y*x$.

Exemple cunoscute de legi comutative

1. Adunarea şi înmulțirea pe $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sunt legi de compoziție comutative.

2. Reuniunea, intersecția pe $\mathcal{P}(M)$ sunt legi comutative.

3. Adunarea şi înmulțirea funcțiilor pe $\mathcal{F}(\mathbb{R})$ sunt legi comutative.

4. Adunarea matricelor pe $\mathcal{M}_{m,n}(\mathbb{C})$ este o lege comutativă.

Exemple de legi necomutative

1. Scăderea pe $\mathbb{R}$ nu este comutativă.

Luăm $x = 3$, $y = 5$ şi avem $x - y = -2$, iar $y - x = 2$. Avem $2 \neq -2$.

2. Compunerea funcțiilor pe $\mathcal{F}(\mathbb{R})$ nu este comutativă. Luăm $f(x)=x^2, g(x)=x-1$. Avem $(f\circ g)(x)=(x-1)^2$ pe când $(g\circ f)(x)=x^2-1$. Evident nu pentru orice $x\in\mathbb{R}, (x-1)^2=x^2-1$.

Observație. Totuşi dacă se dă o submulțime finită $H\subset\mathcal{F}(\mathbb{R})$ şi ni se cere să arătăm că $(H,\circ)$ este structură algebrică comutativă, atunci se face tabla legii care trebuie să fie simetrică în raport cu diagonala principală.

3. Înmulțirea matricelor pe $\mathcal{M}_n(\mathbb{C})$ nu este comutativă. Pentru $n = 2$, de exemplu, luăm $A,B\in\mathcal{M}_2(\mathbb{C})$, $A=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $B=\begin{pmatrix}1&1\\0&1\end{pmatrix}$ pentru care $AB=\begin{pmatrix}0&1\\1&1\end{pmatrix}$ şi $BA=\begin{pmatrix}1&1\\1&0\end{pmatrix}$ şi deci $AB\neq BA$.

Probleme rezolvate

1. Pe mulțimea $H=\{1,2,3,4,5,6\}$ definim aplicația $x\top y=$c.m.m.d.c.(x,y).

Arătați că structura algebrică $(H,\top)$ este comutativă.

R. Arătăm că aplicația $\top$ este o lege de compoziție pe H construind tabla legii. Avem alăturat tabla legii.

$\top$	1	2	3	4	5	6
1	1	1	1	1	1	1
2	1	2	1	2	1	2
3	1	1	3	1	1	3
4	1	2	1	4	1	2
5	1	1	1	1	5	1
6	1	2	3	2	1	6

Cum tabla legii este simetrică în raport cu diagonala principală se deduce că legea de compoziție este comutativă.

Este clar că c.m.m.d.c.$(x,y)=$ c.m.m.d.c.(y,x).

2. **Fie $H = \{1, 2,3,4\}$ şi pe $\mathbb{R}$ legea de compoziţie: $x * y = \begin{cases} y - x, & \text{dacă } x \le 2 \text{ şi } y > 2 \\ 5 - y, & \text{în rest} \end{cases}$.**

Arătaţi că $(H,*)$ este structură necomutativă.

$*$	1	2	3	4
1	4	3	2	3
2	4	3	1	2
3	4	3	2	1
4	4	3	2	1

R. Mulţimea *H* fiind finită vom face tabla legii. Obţinem alăturat tabla.
Se vede că pentru orice $x, y \in H \Rightarrow x * y \in H$, ceea ce arată că aplicaţia $*$ este lege de compoziţie pe *H*.
Legea este necomutativă deoarece tabla legii nu este simetrică în raport cu diagonala principală. De exemplu pentru $x = 1$, $y = 4$ avem $1 * 4 = 3 \ne 4 * 1 = 4$.

3. **Pe $\mathbb{R}$ se consideră legea de compoziţie $x \circ y = xy - 4(x + y) + 20$. Fie $H = (3,5)$. Arătaţi că $(H,\circ)$ este o structură algebrică comutativă.**

R. Arătăm mai întâi că $(H,\circ)$ este structură algebrică, adică $(\forall)x, y \in (3,5) \Rightarrow x \circ y \in (3,5)$

Dacă $x \in (3,5)$ atunci $3 < x < 5 \Leftrightarrow -1 < x - 4 < 1 \Leftrightarrow |x - 4| < 1$.

Deci $x \circ y \in (3,5) \Leftrightarrow |x \circ y - 4| < 1 \Leftrightarrow |(x-4)(y-4)| < 1 \Leftrightarrow |x-1||y-1| < 1$, adevărat deoarece $|x-1| < 1, |y-1| < 1$.

Avem: $x \circ y = xy - 4(x + y) + 20 = yx - 4(y + x) + 20 = y \circ x, (\forall)x, y \in \mathbb{R}$.

4. **Fie $H = \left\{ A_a \in \mathcal{M}_2(\mathbb{R}) \middle| A_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \mathbb{R} \right\}$. Arătaţi că $(H,\cdot)$ este structură algebrică comutativă, unde $\cdot$ este înmulţirea obişnuită a matricelor.**

R. Arătăm mai întâi că $\cdot$ este lege de compoziţie pe *H*.

Fie $A_a, A_b \in H$. Atunci $A_a \cdot A_b = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} = A_{a+b} \in H$.

Înmulţirea pe *H* este comutativă deoarece $A_a \cdot A_b = A_{a+b} = A_{b+a} = A_b \cdot A_a, (\forall) A_a, A_b \in H$.

(În a doua egalitate am folosit comutativitatea adunării numerelor reale $a + b = b + a$).

5. **Pe mulţimea $\mathbb{R} \times \mathbb{R}$ definim operaţia algebrică $(x, y) * (x', y') = (xx' + yy', xx' - yy')$. Arătaţi că legea $*$ este comutativă.**

R. Într-adevăr avem (pentru $(x, y), (x', y') \in \mathbb{R} \times \mathbb{R}$)

$$(x, y) * (x', y') = (xx' + yy', xx' - yy') \text{ şi } (x', y') * (x, y) = (x'x + y'y, x'x - y'y)$$

Cum $xx' + yy' = x'x + y'y$ şi $xx' - yy' = x'x - y'y$ (înmulţirea pe $\mathbb{R}$ este comutativă) se deduce $(x, y) * (x', y') = (x', y') * (x, y)$ adică $*$ este comutativă.

6. **Fie $H = (1,\infty) - \{2\}$ şi aplicaţia $x * y = 1 + (x - 1)^{\ln\sqrt{y-1}}$.**

Să se arate că $(H,*)$ este o structură algebrică comutativă.

R. Probăm mai întâi că $*$ este lege de compoziţie pe *H*. Fie $x, y \in H$. Să arătăm că $x * y \in H \Leftrightarrow$ $\Leftrightarrow x * y > 1, x * y \ne 2$. Avem:

$1 + (x-1)^{\ln\sqrt{y-1}} > 1 \Leftrightarrow (x-1)^{\ln\sqrt{y-1}} > 0$ adevărat pentru că *x*, *y* > 1.

De asemenea $x * y \ne 2 \Leftrightarrow 1 + (x-1)^{\ln\sqrt{y-1}} \ne 2 \Leftrightarrow (x-1)^{\ln\sqrt{y-1}} \ne 1$ adevărat deoarece $x - 1 > 0, x - 1 \ne 1$, $y - 1 > 0, y - 1 \ne 1$.

Legea $*$ este comutativă dacă $x*y=y*x, (\forall)x,y\in H \Leftrightarrow 1+(x-1)^{\ln\sqrt{y-1}}=1+(y-1)^{\ln\sqrt{x-1}}$, $(\forall)x,y\in H \Leftrightarrow (x-1)^{\ln\sqrt{y-1}}=(y-1)^{\ln\sqrt{x-1}}, (\forall)x,y\in H \Leftrightarrow \ln\sqrt{y-1}\cdot\ln(x-1)=$ $=\ln\sqrt{x-1}\ln(y-1),(\forall)x,y\in H \Leftrightarrow \frac{1}{2}\ln(y-1)\cdot\ln(x-1)=\frac{1}{2}\ln(x-y)\ln(y-1),(\forall)x,y\in H$, evident.

7. Fie funcțiile $f_i:\{1,2,3,4\}\to\{1,2,3,4\}, i=1,2,3,4$ definite astfel:

$$f_1(x)=\begin{cases}1, x=1\\2, x=2\\3, x=3\\4, x=4\end{cases} \text{(funcția identică)},\ f_2(x)=\begin{cases}2, x=1\\1, x=2\\3, x=3\\4, x=4\end{cases},\ f_3(x)=\begin{cases}1, x=1\\2, x=2\\4, x=3\\3, x=4\end{cases},\ f_4(x)=\begin{cases}2, x=1\\1, x=2\\4, x=3\\3, x=4.\end{cases}$$

Considerăm $H=\{f_1,f_2,f_3,f_4\}\subset\mathcal{F}(\{1,2,3,4\})$ și operația $\circ$ de compunere a funcțiilor. Arătați că $(H,\circ)$ este structură algebrică comutativă.

R. Aceste funcții se mai pot reprezenta sub forma unui tabel cu două linii

$$f_1=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\ f_2=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}, f_3=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}, f_3=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}.$$

În prima linie se trec elementele domeniului de definiție, iar în a doua linie valorile funcțiilor calculate în punctele domeniului de definiție. Aceste funcții particulare se numesc permutări de gradul patru. Tabla legii este dată alăturat. De aici se vede că legea $\circ$ este o lege de compoziție pe H și în plus este comutativă dată fiind simetria tablei în raport cu diagonala principală.

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

8. Fie $M=\{a,b,c\}$. Câte legi de compoziție se pot defini pe M și câte dintre acestea sunt comutative?

R. Cum o lege de compoziție este o aplicație $f:M\times M\to M$, atunci se știe că numărul acestor aplicații este egal cu $(\text{card}(M))^{\text{card}(M\times M)}$ unde $\text{card}(M\times M)=\text{card}(M)\cdot\text{card}(M)$ ($\text{card}(M)=$ numărul de elemente din *M*).

În cazul nostru card(*M*) = 3, iar $\text{card}(M\times M)=9$. Deci numărul de legi de compoziție pe *M* este egal cu 3^9.

Altfel. Pentru că *M* este o mulțime finită se poate raționa utilizând tabla legii. Pentru fiecare lege de compoziție avem o singură tablă și reciproc.

	a	b	c
a	$*$	$*$	$*$
b	$*$	$*$	$*$
c	$*$	$*$	$*$

Am marcat prin steluțe posibilele elemente rezultate compunând elementele mulțimii M. Este limpede că fiecare loc marcat cu $*$ poate fi ocupat de oricare din elementele mulțimii *M*. Deci fiecare astfel de loc poate fi completat în trei moduri. Numărul total de moduri în care se pot completa toate locurile marcate cu $*$ este egal cu $\underbrace{3\times3\times...\times3}_{9\text{ori}}=3^9$, și acest număr reprezintă toate legile de compoziție pe *M*.

	a	b	c
a	$*$	$*$	$*$
b	$\circ$	$*$	$*$
c	$\circ$	$\circ$	$*$

O lege de compoziție definită pe o mulțime finită *M* este comutativă dacă tabla legii este simetrică în raport cu diagonala principală.
Deci este suficient să completăm locurile marcate cu $*$ din tabla prezentată alăturat, pentru că celelalte locuri marcate prin $\circ$ se completează prin simetrie în raport cu diagonala principală. Ori locurile marcate prin $*$ se pot completa în $3\times3\times3\times3\times3\times3=3^6$. Acesta este numărul legilor de compoziție comutative.

Probleme propuse

1. Pe mulțimea H = {1, 2, 3, 4, 5} definim aplicația $x \perp y$ = restul împărțirii lui xy prin 6. Arătați că $(H,\perp)$ este o structură algebrică comutativă.

2. Pe mulțimea $H=\{1,2,3,4\}$ se consideră aplicația $x * y$ = restul împărțirii lui x^y prin 5. Demonstrați că $(H,*)$ este structură algebrică necomutativă.

3. Pe $\mathbb{R}$ se defineşte legea de compoziție $x \circ y = 3x + y$. Arătați că „$\circ$" este o lege necomutativă.

4. Pe mulțimea $H=(2,\infty)$ se consideră aplicația $x * y = xy - 2x - 2y + 6$.

Arătați că *(H, *)* este structură algebrică comutativă.

5. Pe mulțimea $H=(-\infty,1)$ se defineşte aplicația $x * y = \dfrac{xy-2}{x+y-3}$.

Demonstrați că $(H,*)$ este o structură algebrică comutativă.

6. Pe mulțimea $\mathbb{R}\times\mathbb{R}$ se defineşte operația algebrică $(x,y)\circ(x',y')=(xy'+x'y,yy')$. Arătați că „$\circ$" este lege comutativă.

7. Fie $H=\{A_1,A_2,A_3,A_4\}\subset\mathcal{M}_2(\mathbb{R})$, unde $A_1=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $A_2=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $A_3=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$, $A_4=\begin{pmatrix}0&-1\\-1&0\end{pmatrix}$.

Arătați că $(H,\cdot)$ este o structură algebrică comutativă, unde „$\cdot$" este operația de înmulțire a matricelor.

8. Se consideră $H=\left\{A_a=\begin{pmatrix}2-a&a-1\\2(1-a)&2a-1\end{pmatrix}\middle| a\in\mathbb{R}^*\right\}\subset\mathcal{M}_2(\mathbb{R})$. Demonstrați că structura algebrică $(H,\cdot)$ este comutativă, unde „$\cdot$" este operația de înmulțire a matricelor.

9. Fie $H=\left\{\begin{pmatrix}x+4y&2y\\-7y&x-4y\end{pmatrix}\middle| x,\in\mathbb{R},x^2-2y^2=1\right\}\subset\mathcal{M}_2(\mathbb{R})$. Arătați că $(H,\cdot)$ este structură algebrică comutativă.

10. Fie $H=\{f_1,f_2,f_3\}\subset\mathcal{F}(\mathbb{R}-\{0,1\})$, $f_1(x)=x$, $f_2(x)=1-\dfrac{1}{x}$, $f_3(x)=\dfrac{1}{1-x}$. Demonstrați că $(H,\circ)$ este o structură algebrică comutativă, unde „$\circ$" este compunerea funcțiilor.

11. Se consideră $H=(0,\infty)-\{1\}$ şi aplicația $x*y=x^{\ln\sqrt[3]{y}}$. Arătați că $(H,*)$ este o structură algebrică comutativă.

12. Pe $\mathbb{R}$ se defineşte legea de compoziție definită prin $x*y=xy+2ax+by, a,b\in\mathbb{R}$. Determinați *a, b* pentru care legea este asociativă şi comutativă.

13. Fie $a,b\in\mathbb{R}^*$. Pe mulțimea $(0,\infty)$ definim operația: $xy=e^{a\ln x-b\ln y}, x,y>0$. Să se determine *a, b* astfel încât legea să fie comutativă şi asociativă.

14. Pe $\mathbb{R}$ se consideră legea de compoziție $x*y=(1-a)x+ay-a, x,y\in\mathbb{R}$. Legea este comutativă dacă: a) $a=1$; b) $a=-1$; c) $a=\dfrac{1}{2}$; d) $a=-\dfrac{1}{2}$; e) $a=0$.

15. Pe $\mathbb{R}$ se consideră legea de compoziție $*$ definită prin:

a) $x*y=xy+ax+15y+3, \forall x,y\in\mathbb{R}$; b) $x*y=(2a+1)x+(3a+1)y-2, \forall x,y\in\mathbb{R}$.

Să se determine $a\in\mathbb{R}$, astfel încât legea $*$ să fie comutativă în fiecare caz.

16. **Pe $\mathbb{R}$ se defineşte legea de compoziţie $*$ astfel:**
1) $x*y=ax+by+c$; 2) $x*y=xy+2x+2y+a$; 3) $x*y=xy+ax+by+6$;
4) $x*y=xy-3(x+y)+a$; 5) $x*y=3xy+a(x+y)+14$; 6) $x*y=2xy+ax+by+3$.
Să se determine $a,b,c\in\mathbb{R}$, astfel încât, în fiecare caz, legea să fie comutativă şi asociativă.

P3. Element neutru

Definiţie. Un element $e\in M$ se numeşte **element neutru** pentru legea $*$ dacă **pentru orice** $x\in M$ **avem**

$$x*e=e*x=x.$$

Uneori se mai spune că legea $*$ admite pe $e\in M$ ca element neutru dacă

$$x*e=e*x=x, (\forall)x\in M.$$

Faptul că o structură algebrică $(M,*)$ are elementul neutru e se notează uneori prin $(M,*,e)$.

Dacă în plus legea $*$ este comutativă, atunci condiţia ca $e\in M$ să fie element neutru pentru legea $*$ se reduce la $x*e=x, (\forall)x\in M$ (sau $e*x=x, (\forall)x\in M$).

Atragem atenţia că elementul neutru e al unei legi $*$ pe M **trebuie să aparţină mulţimii** M. Deci $e\in M$. Nu orice lege de compoziţie pe o mulţime admite element neutru.

Teoremă. Dacă o lege de compoziţie admite element neutru, atunci acesta este unic.

Demonstraţie. Vom arăta că dacă ar exista două elemente neutre $e_1,e_2\in M$ pentru legea $*$ atunci acestea coincid. Avem:

$x*e_1=e_1*x=x, (\forall)x\in M$, (1)

$x*e_2=e_2*x=x, (\forall)x\in M$, (2).

În (1) punem $x=e_2$ şi rezultă $e_2*e_1=e_1*e_2=e_2$, (3)

iar în (2) facem $x=e_1$ şi obţinem $e_1*e_2=e_2*e_1=e_1$, (4).

Din (3) şi (4) rezultă $e_1=e_2$. ■

Observaţie. Dacă H este o parte stabilă a lui M în raport cu legea $*$ şi dacă $e\in M$ este element neutru pentru $*$, atunci dacă $e\in H$, acesta este element neutru al legii induse de $*$ pe mulţimea H.

Astfel numărul 0 este element neutru pentru adunarea pe $\mathbb{R}$ Cum $0\in\mathbb{Z}$, acesta va fi element neutru şi pentru adunarea pe $\mathbb{Z}$ (A se vedea problema rezolvată 4).

Definiție. Un element $e_s \in M$ se numeşte **element neutru la stânga** pentru legea $*$ dacă $e_s * x = x, (\forall) x \in M$.
Un element $e_d \in M$ se numeşte **element neutru la dreapta** pentru legea $*$ dacă $x * e_d = x, (\forall) x \in M$.

Aşadar un element $e \in M$ este element neutru pentru legea $*$ dacă şi numai dacă e este element neutru atât la stânga cât şi la dreapta.
Dacă o lege de compoziție este notată multiplicativ, elementul neutru, dacă există, se numeşte **element unitate** şi se notează de obicei cu **simbolul** 1. Dacă legea este notată aditiv, elementul neutru, dacă există, se numeşte **element nul** şi se notează de obicei cu **simbolul** 0.

Fie M o mulțime pe care am definit o lege de compoziție asociativă şi cu element neutru $e \in M$. Pe o astfel de mulțime am definit compusul a n elemente, $n \geq 1$. Operația dată, având şi element neutru, definim acest compus şi pentru $n = 0$ ca fiind e.
Dacă operația algebrică pe M este scrisă multiplicativ atunci definim puterea a n-a a lui $x \in M$ prin $x^n = \begin{cases} x \cdot x \cdot \ldots \cdot x (n \text{ factori}), & \text{dacă } n > 0 \\ e, & \text{dacă } n = 0. \end{cases}$
Avem evident pentru orice $x \in M$ şi orice $m, n \in \mathbb{N}$

$$x^m \cdot x^n = x^{m+n}, \left(x^m\right)^n = x^{mn}.$$

Dacă M este înzestrată cu o lege de compoziție scrisă aditiv, asociativă şi cu element neutru $0 \in M$, atunci pentru orice $x \in M$ şi orice $n \in \mathbb{N}$, definim nx prin:

$$nx = \begin{cases} x + x + \ldots + x (n \text{ termeni}), & \text{dacă } n > 0 \\ 0, & \text{dacă } n = 0. \end{cases}$$

Au loc egalitățile:
$mx + nx = (m+n)x,\ n(mx) = (mn)x, (\forall) x \in M, (\forall) m, n \in \mathbb{N}$.

Exemple cunoscute de legi cu element neutru

1. Adunarea pe $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are ca element neutru numărul zero, când avem:

$$x + 0 = 0 + x = x, (\forall) x.$$

2. Înmulțirea pe $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are ca element neutru numărul unu, când avem:

$$1 \cdot x = x \cdot 1 = x, (\forall) x.$$

3. Compunerea pe $\mathcal{F}(M)$ admite ca element neutru funcția identică de la M la M, $1_M : M \to M$, $1_M(x) = x, x \in M$.

4. Adunarea matricelor pe $\mathcal{M}_n(\mathbb{C})$ are ca element neutru matricea nulă (cu toate elementele egale cu zero) notată simplu O_n.

5. **Matricea unitate $I_n \in \mathcal{M}_n(\mathbb{C})$ reprezintă elementul neutru pentru operația de înmulțire a matricelor din $\mathcal{M}_n(\mathbb{C})$.**

6. **Pe mulțimea $\mathcal{P}(M)$ a părților unei mulțimi M elementul neutru față de reuniune este mulțimea vidă, $X \cup \varnothing = \varnothing \cup X = X, (\forall) X \in \mathcal{P}(M)$, iar elementul neutru față de intersecție este mulțimea totală M, $M \cap X = X \cap M = X, (\forall) X \in \mathcal{P}(M)$**

Probleme rezolvate

1. **Pe mulțimea $M = \{e, a, b, c\}$ se consideră legea de compoziție $\top$ dată prin tabla legii (alăturat).**

$\top$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Să se arate că legea $\top$ admite element neutru.

R. Din egalitățile: $e \top e = e$, $a \top e = e \top a = a$, $b \top e = e \top b = b$, $c \top e = e \top c = c$ se deduce că $e \in M$ este elementul neutru pentru $\top$.

2. **Pe mulțimea $M = (-\infty, 1) \cup (3, \infty)$ se consideră aplicația $x * y = xy - 2(x+y) + 6$. Arătați că $(M, *)$ este o structură algebrică fără element neutru.**

R. Faptul că $x \in M \Leftrightarrow |x-2| > 1$. Probăm că $(M,*)$ este structură algebrică, adică $*$ este o lege de compoziție pe M, ceea ce revine la a arăta că $(\forall) x, y \in M \Rightarrow x * y \in M$. Avem $x * y \in M \Leftrightarrow$ $\Leftrightarrow |x * y - 2| > 1 \Leftrightarrow |(x-2)(y-2)| > 1 \Leftrightarrow |x-2||y-2| > 1$, evident.

Presupunem acum că $e \in M$ este elementul neutru. Trebuie să avem:

$$x * e = e * x = x, (\forall) x \in M$$

Se vede ușor că legea este comutativă și deci prima egalitate de mai sus se verifică. Deci trebuie ca $x * e = x, (\forall) x \in M \Leftrightarrow xe - 3(x+e) + 6 = x, (\forall) x \in M \Leftrightarrow (x-2)(e-3) = 0, (\forall) x \in M \Leftrightarrow e = 3$.

Observăm că $3 \notin M$ și prin urmare legea $*$ nu admite element neutru.

3. **Pe mulțimea $H = [-2, \infty)$ definim aplicația $x * y = 3xy + 6(x+y) + 10$.**

Să se arate că $*$ este o lege de compoziție pe H, cu element neutru.

R. Arătăm că $*$ este o lege de compoziție pe H.

Fie $x, y \in H$. Atunci $x = -2 + \alpha$, $y = -2 + \beta$, $\alpha, \beta \geq 0$, și deci

$x * y = 3(-2+\alpha)(-2+\beta) + 6(-4+\alpha+\beta) + 10 = -2 + 3\alpha\beta \geq -2$.

Aceasta arată că din $x, y \in H \Rightarrow x * y \in H$, adică $*$ este o lege de compoziție pe H.

Fie $e \in H$ elementul neutru. Legea fiind comutativă trebuie să avem

$x * e = x, (\forall) x \in H \Leftrightarrow 3xe + 6(x+e) + 10 = x, (\forall) x \in H \Leftrightarrow (x+2)(3e+5) = 0, (\forall) x \in H$.

Dacă $x \neq -2$, atunci din ultima egalitate $3e + 5 = 0$, adică $e = -\frac{5}{3} \in H$.

Acesta este element neutru pentru $*$ dacă verificăm egalitatea $x * e = x$ și pentru $x = -2$. Ori avem:

$(-2) * \left(-\frac{5}{3}\right) = 3(-2)\left(-\frac{5}{3}\right) + 6\left(-2 - \frac{5}{3}\right) + 10 = 10 - 22 + 10 = -2$.

Acum pentru orice $x \in H$ avem egalitatea $x * \left(-\frac{5}{3}\right) = x$.

Deci $e = -\frac{5}{3}$ reprezintă element neutru.

4. Se consideră mulțimea de matrice $H=\left\{\begin{pmatrix}1&1&a\\0&0&1\\0&0&1\end{pmatrix}\middle| a\in 2\mathbb{Z}+1\right\}\subset \mathcal{M}_3(\mathbb{Z})$. Arătați că $(H,\cdot)$ este o structură algebrică cu element unitate.

R. Mai întâi arătăm că înmulțirea matricelor din $\mathcal{M}_3(\mathbb{Z})$ induce pe H o lege de compoziție. Într-adevăr fie:

$A_a=\begin{pmatrix}1&1&a\\0&0&1\\0&0&1\end{pmatrix}$, $A_b=\begin{pmatrix}1&1&b\\0&0&1\\0&0&1\end{pmatrix}\in H$. Atunci: $A_aA_b=\begin{pmatrix}1&1&a+b+1\\0&0&1\\0&0&1\end{pmatrix}=A_{a+b+1}\in H$, deoarece $a+b+1\in 2\mathbb{Z}+1$.

Mai mult înmulțirea pe H este comutativă deoarece $A_a\cdot A_b=A_{a+b+1}=A_{b+a+1}=A_b\cdot A_a$.

Fie $A_e\in H$ elementul unitate pentru înmulțire. Trebuie să avem $A_e\cdot A_a=A_a, (\forall)A_a\in H$ sau $A_{a+e+1}=A_a, (\forall)A_a\in H$.

Este clar că $A_a=A_b \Leftrightarrow a=b$. Deci din $A_{a+e+1}=A_a$ rezultă $a+e+1=a$ sau $e=-1\in 2\mathbb{Z}+1$.

Elementul neutru este $A_{-1}=\begin{pmatrix}1&1&-1\\0&0&1\\0&0&1\end{pmatrix}$. Este oare vreo contradicție între faptul că I_3 este element neutru pentru înmulțirea din $\mathcal{M}_3(\mathbb{Z})$ (în cazul acesta) și faptul că A_{-1} este element neutru pentru $H\subset \mathcal{M}_3(\mathbb{Z})$? Nu, pentru că I_3 nu aparține mulțimii *H*.

Probleme propuse

1. Pe mulțimea H = {0, 1, 2, 3, 4} definim aplicația „$\circ$“ astfel $x\circ y=\begin{cases}x+y, & x<y\le 2\\ x-y, & x\ge y\\ y-x, & x\le 3 \text{ și } y>2.\end{cases}$

Arătați că $(H,\circ)$ este o structură algebrică neasociativă, necomutativă, dar cu element neutru.

2. Pe mulțimea H = [5, 7] definim aplicația $x*y=xy-6x-6y+42$.
Arătați că $(H,*)$ este o structură algebrică având elementul neutru e = 7.

3. Fie $H=\mathbb{C}-\{-i\}$ o submulțime a lui $\mathbb{C}$. Definim pe $\mathbb{C}$ legea de compoziție $x\top y=xy+i(x+y)-(1+i)$.
Arătați că $(H,\top)$ este o structură algebrică asociativă, comutativă cu element neutru $e=1-i$.

4. Considerăm $H=\left\{\begin{pmatrix}a_1&a_2\\a_3&a_4\end{pmatrix}\middle| a_i\in\mathbb{R}, a_1a_4\neq 0\right\}\subset \mathcal{M}_2(\mathbb{R})$ și legea de compoziție pe $\mathcal{M}_2(\mathbb{R})$

$\begin{pmatrix}a_1&a_2\\a_3&a_4\end{pmatrix}*\begin{pmatrix}b_1&b_2\\b_3&b_4\end{pmatrix}=\begin{pmatrix}a_1b_1&a_2+a_1b_2\\a_3+a_4b_3&a_4b_4\end{pmatrix}$. Demonstrați că $(H,*)$ este o structură algebrică asociativă, cu element neutru.

5. Fie $H=\left\{\begin{pmatrix}0&0\\a&b\end{pmatrix}\middle| a,b\in\mathbb{Z}\right\}\subset \mathcal{M}_2(\mathbb{Z})$ .Să se arate că $(H,\cdot)$ este structură algebrică asociativă cu elemente neutre la stânga.

6. **Pe $\mathbb{R}$ se defineşte legea de compoziție $x \circ y = xy - 2x - 2y + m$, $m \in \mathbb{R}$. Să se determine valorile lui m pentru care $H = [2,\infty)$ este o parte stabilă a lui $\mathbb{R}$ în raport cu „ $*$ “. Determinați apoi elementul neutru al legii „ $*$ “ pe *H*.**

7. **Fie $H = \left\{ A(x) = \begin{pmatrix} 1-x & 0 & x \\ 0 & 0 & 0 \\ x & 0 & 1-x \end{pmatrix} \middle| x \in R, x \neq \frac{1}{2} \right\} \subset \mathcal{M}_3(\mathbb{R})$. Arătați că $(H,\cdot)$ este structură algebrică asociativă, comutativă, cu element neutru.**

8. **Să se determine valorile parametrului real *a*, astfel încât legea de compoziție pe $\mathbb{R}$ definită prin $x * y = a(x+y) - xy$ să fie asociativă şi comutativă. Determinați elementul neutru.**

9. **Pe $\mathbb{R}$ se defineşte legea de compoziție $x * y = 2xy - 2x - 2y + c$, $x \in \mathbb{R}$. Fie $H = \mathbb{R} - \{1\}$. Determinați pe *c* pentru care $(H,*)$ este o structură algebrică asociativă şi apoi precizați elementul neutru.**

10. **Pe mulțimea $\mathbb{R}$ se consideră legea de compoziție $x * y = xy + ax + by + c$. Să se arate că legea„ $*$ “ este asociativă dacă şi numai dacă admite element neutru.**

11. **Pe $\mathbb{R}$ se defineşte legea „ $*$ “ prin: $x * y = xy - (x+y)\sqrt{2} + 2 + \sqrt{2}$, $x, y \in \mathbb{R}$.**

1) Arătați că legea „ $*$ “ este comutativă, iar $[\sqrt{2},\infty)$ este parte stabilă a lui $\mathbb{R}$ în raport cu „ $*$ “.

2) Să se determine $y \in [\sqrt{2},\infty)$ astfel încât $x * y = x$, $\forall x \in [\sqrt{2},\infty)$.

3) Determinați elementul neutru al legii „ $*$ “ pe $[\sqrt{2},\infty)$.

4) Pentru $a \in (\sqrt{2},\infty)$ fixat, să se determine $y \in (\sqrt{2},\infty)$ care verifică relația $a * y = 1 + \sqrt{2}$.

12. **Pe $\mathbb{R}$ se consideră legea de compoziție $*$ definită prin $x * y = xy + 5x + ay + b$. Să se determine $a, b \in \mathbb{R}$, astfel încât legea să admită element neutru.**

P4. Element simetric

> **Definiție.** Fie $(M,*)$ o structură algebrică **cu element neutru** $e \in M$ şi $x \in M$. Spunem că un element $x' \in M$ este **un simetric** al lui *x* în raport cu legea $*$ dacă $x * x' = x' * x = e$.

Dacă există *x'* cu această proprietate, spunem că *x* este **element simetrizabil**, în raport cu legea $*$.

Să observăm că *x'* este simetricul lui *x,* adică (*x'*)' = *x.*

Facem precizarea şi în acest caz că simetricul lui *x,* elementul *x'* **trebuie să aparțină mulțimii** *M*. Deci odată găsit *x',* **acesta trebuie să fie în** *M*. Dacă legea $*$ este comutativă, atunci $x' \in M$ este simetricul lui *x* dacă $x * x' = e$ (sau $x' * x = e$).

Când legea este notată **multiplicativ**, vom spune element **inversabil** în loc de simetrizabil şi element **invers** în loc de simetric; inversul lui *x* se va nota cu x^{-1} sau $\frac{1}{x}$.

Dacă legea de compoziție este notată **aditiv**, vom spune **opusul** lui *x* în loc de simetricul lui *x*; opusul lui *x* se va nota cu –*x.*

Exemple cunoscute de legi cu elemente simetrice

1. **Elementul neutru e este element simetrizabil, un simetric al său este el însuşi, $e' = e$.**
2. **Față de adunarea numerelor naturale, singurul element simetrizabil este 0 (zero), când –0 = 0.**
3. **Față de adunare pe $\mathbb{Z}$ (elementul neutru este 0), orice element este simetrizabil (orice element $x \in \mathbb{Z}$ are un opus $-x$) deoarece $x + (-x) = (-x) + x = 0$.**
4. **Față de înmulțirea pe $\mathbb{Z}$ (elementul neutru este 1), singurele elemente inversabile sunt 1 (având simetricul 1) şi –1 (având simetricul –1) când $1^{-1} = 1$ şi $(-1)^{-1} = -1$.**
5. **Față de înmulțirea pe $\mathcal{M}_n(\mathbb{C})$ (elementul neutru este I_n) elementele simetrizabile sunt matricele A cu $\det(A) \neq 0$, simetricul matricei A fiind matricea inversă A^{-1}, când $A \cdot A^{-1} = A^{-1} \cdot A = I_n$.**
6. **Față de compunerea pe $\mathcal{F}(M)$ (elementul neutru este 1_M) elementele simetrizabile sunt funcțiile bijective, deoarece o aplicație f este inversabilă dacă şi numai dacă este bijectivă când $f \circ f^{-1} = f^{-1} \circ f = 1_M$.**

Teoremă. Fie $(M, *)$ o structură algebrică **asociativă** şi **cu element neutru** e.
Dacă $x \in M$ are un element simetric, atunci acesta este unic.

Demonstrație. Fie x', x'' două elemente simetrice pentru x. Avem
$x * x' = x' * x = e$, (1) şi
$x * x'' = x'' * x = e$, (2).

Atunci $x' = x' * e \overset{(2)}{=} x' * (x * x'') = (x' * x) * x'' \overset{(1)}{=} e * x'' = x''$ şi teorema este demonstrată. ■

Notație. Dacă $(M, *)$ este structură algebrică **asociativă** şi cu **element neutru**, atunci notăm $U(M)$ submulțimea elementelor din M simetrizabile în raport cu $*$. Aşadar $U(M) = \{x \in M \mid (\exists) x' \in M,\ x * x' = x' * x = e\}$.

Pentru o lege de compoziție pe M, notată **multiplicativ** şi pentru un element inversabil $x \in M$, definim puterea negativă x^{-n}, $n \geq 1$, prin $\boxed{x^{-n} = \left(x^{-1}\right)^n,\ n \in \mathbb{N}^*}$.

Este clar că x^{-n} este invers pentru x^n, $\left(x^n\right)^{-1} = x^{-n}$.

Analog, dacă legea de compoziție pe M, este **aditivă** şi $x \in M$ are un opus $-x$, atunci definim $(-n)x, n \geq 1$, prin $\boxed{(-n)x = n(-x),\ n \in \mathbb{N}^*}$.

Este clar că $n(-x)$ este un opus al lui nx, $-(nx) = n(-x)$.

Teoremă. Fie $(M,*)$ o structură algebrică **asociativă** şi cu **element neutru**. Atunci:

1) Dacă elementele $x, y \in M$ sunt simetrizabile, atunci compusul lui x cu y este simetrizabil şi mai mult $(x*y)' = y' * x'$.

2) Dacă elementul $x \in M$ este simetrizabil, simetricul său, x', este, de asemenea, simetrizabil şi $(x')' = x$.

3) Dacă $x \in M$ este simetrizabil, iar $y \in M$ nu este simetrizabil, atunci $x*y,\ y*x \in M$ nu sunt simetrizabile.

Demonstrație. 1) Trebuie să probăm că $(x*y)*(y'*x') = (y'*x')*(x*y) = e$. Avem (folosind asociativitatea legii $*$):
$(x*y)*(y'*x') = x*(y*y')*x' = x*e*x' = x*x' = e$ şi analog
$(y'*x')*(x*y) = y'*(x'*x)*y = y'*e*y = y'*y = e$.
Deci $x*y$ este simetrizabil şi $y'*x'$ este unicul său simetric (vezi teorema precedentă).
2) Rezultă din definiția elementului simetric (observând că x şi x' au rol simetric în această definiție) şi din unicitatea sa.
3) Presupunem prin reducere la absurd, că elementul $z = x*y$ este simetrizabil. Atunci şi elementul $x'*z$ (de la punctul 1)) este simetrizabil.
Dar avem $x'*z = x'*(x*y) = (x'*x)*y = e*y = y$, ceea ce înseamnă că y ar fi simetrizabil. Contradicție.
Prin urmare $x*y$ nu este simetrizabil. Analog se arată că $y*x$ nu este simetrizabil. ■

Observații. 1) Afirmația **1)** din teoremă spune că $(U(M),*)$ este o structură algebrică, adică $*$ este lege de compoziție indusă pe $U(M)$ de legea de compoziție de pe M.
2) Dacă legea este notată multiplicativ, atunci această afirmație se transcrie $(xy)^{-1} = y^{-1}x^{-1}$.
Dacă legea este notată aditiv, atunci $-(x+y) = (-y)+(-x)$.

Definiție. Fie $(M,*)$ o operație algebrică având $e_s \in M$ element neutru la stânga ($e_d \in M$ element neutru la dreapta) şi $x \in M$.
Spunem că $x'_s \in M$ ($x'_d \in M$) este un simetric al lui x la stânga (la dreapta) în raport cu legea $*$ dacă

$$x'_s * x = e_s \quad (x * x'_d = e_d).$$

Se mai spune că $x \in M$ este **simetrizabil la stânga (la dreapta) în raport cu** $*$ dacă există $x'_s \in M$ ($x'_d \in M$) pentru care $x'_s * x = e_s$ ($x * x'_d = e_d$).

Probleme rezolvate

1. Pe mulțimea $\mathbb{Z}$ se definește legea de compoziție $x \oplus y =$ restul împărțirii lui $x + y$ la 6. Fie $H = \{0, 1, 2, 3, 4, 5\} \subset \mathbb{Z}$. Arătați că $(H, \oplus)$ este o structură algebrică. Determinați elementele simetrizabile din H în raport cu $\oplus$.

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

R. Tabla legii este dată alăturat.
Se observă că elementul neutru al legii este $e = 0$.
Pentru a determina simetricul unui element x utilizând tabla se procedează astfel: se urmărește pe orizontala lui x elementul neutru $e = 0$. Elementul corespunzător coloanei pe care se găsește $e = 0$ reprezintă simetricul lui x.
Având notația aditivă pentru lege în loc de simetricul elementului x vom utiliza denumirea de opusul lui x și scriem $-x$.
Deci $-0 = 0, -1 = 5, -2 = 4, -3 = 3, -4 = 2, -5 = 1$.

2. Pe mulțimea numerelor reale $\mathbb{R}$ definim legea de compoziție $x \top y = xy - 3(x + y) + 12$. Arătați că legea $\top$ este asociativă, comutativă, admite element neutru. Stabiliți elementele simetrizabile din $\mathbb{R}$ în raport cu $\top$.

R. Se verifică prin calcul asociativitatea și comutativitatea legii. Pentru determinarea elementului neutru $e \in \mathbb{R}$ utilizăm definiția acestuia $x * e = x, (\forall) x \in \mathbb{R} \Leftrightarrow xe - 3(x + e) + 12 = x, \ (\forall) x \in \mathbb{R} \Leftrightarrow$
$\Leftrightarrow e(x-3) = 4(x-3), (\forall) x \in \mathbb{R}$.
Dacă $x \neq 3$ rezultă $e = 4$. Pentru $x = 3$ se verifică imediat egalitatea $3 * 4 = 3$. Așadar $e = 4$ reprezintă elementul neutru pentru legea $\top$.
Să determinăm acum elementele simetrizabile. Fie $x \in \mathbb{R}$ și $x' \in \mathbb{R}$ simetricul lui x în raport cu $\top$. Avem: $x * x' = 4 \Leftrightarrow xx' - 3(x + x') + 12 = 4 \Leftrightarrow x'(x-3) = 3x + 8$. Dacă $x \neq 3$, atunci $x' = \dfrac{3x-8}{x-3} \in \mathbb{R}$

Deci orice $x \in \mathbb{R}, x \neq 3$ admite un simetric $x' = \dfrac{3x-8}{x-3}$.

3. Pe $\mathbb{R}$ se consideră legea de compoziție $x \circ y = xy - 6(x + y) + 42$. Fie $H = [5, 7]$. Arătați că $(H, \circ)$ este o structură algebrică asociativă, comutativă, cu element neutru. Determinați elementele simetrizabile din H în raport cu legea „$\circ$“.

R. Să observăm că $x \in H \Leftrightarrow 5 \leq x \leq 7 \Leftrightarrow -1 \leq x - 6 \leq 1 \Leftrightarrow |x - 6| \leq 1$.
Acum se arată ușor că dacă $x, y \in H$, atunci $x * y \in H$.
Prin calcul se verifică asociativitatea și comutativitatea legii.
Elementul $e \in H$ reprezintă elementul neutru în raport cu legea „$\circ$“ dacă $x \circ e = x, (\forall) x \in H \Leftrightarrow$
$\Leftrightarrow xe - 6(x + e) + 42 = x, (\forall) x \in H \Leftrightarrow e(x-6) = 7(x-6), (\forall) x \in H$.
Dacă $x \neq 6$, atunci $e = 7 \in H$, iar pentru $x = 6$ se verifică egalitatea $\mathbf{6 \circ 7 = 6}$. Deci $e = 7$ este elementul neutru în raport cu legea „$\circ$“.
Determinăm elementele simetrizabile. Fie $x \in H$ și $x' \in H$ elementul său simetric. Trebuie să avem egalitatea $x * x' = 7 \Leftrightarrow xx' - 6(x + x') + 42 = 7 \Leftrightarrow x'(x-6) = 6x - 35$.

Dacă $x \neq 6$, atunci $x' = \dfrac{6x-35}{x-6}$. Elementul obținut x' trebuie să aparțină lui H, adică $5 \leq \dfrac{6x-35}{x-6} \leq 7$, cea ce dă $x \in \{5, 7\}$.
Deci singurele elemente simetrizabile sunt $x = 5$ când $x' = 5$ și $x = 7$ când $x' = 7$.

4. Fie $M = (0, \infty) - \{1\}$ și aplicația $x * y = e^{\ln x \cdot \ln y}$. Arătați că $*$ este o lege de compoziție pe M, asociativă, comutativă, cu element neutru. Determinați elementele simetrizabile din M în raport cu „$*$“.

R. Dacă $x>0,\ x\neq 1,\ y>0,\ y\neq 1 \Rightarrow x*y>0,\ x*y\neq 1$, ceea ce înseamnă că „$*$“ este lege de compoziție pe M.

Prin calcul se verifică asociativitatea şi comutativitatea legii. Elementul neutru $u\in M$ are proprietatea

$x*u=x,(\forall)x\in M \Leftrightarrow e^{\ln x\cdot \ln u}=x,(\forall)x\in M \Leftrightarrow \ln x\cdot \ln u,=\ln x,\ (\forall)x\in M \Leftrightarrow$

$\Leftrightarrow \ln u=1 \Leftrightarrow u=e\in M$.

Observație. Când în structura legii figurează ln este indicat să notăm elementul neutru cu altă literă (aici am pus *u).*

Să determinăm acum elementele simetrice. Fie $x\in M$ şi $x'\in M$ simetricul său. Trebuie să avem egalitatea:

$$x*x'=e \Leftrightarrow e^{\ln x\cdot \ln x'}=e \Leftrightarrow \ln x \ln x'=1 \Leftrightarrow \ln x'=\frac{1}{\ln x} \Leftrightarrow x'=e^{\frac{1}{\ln x}}.$$

Avem de verificat că $x'\in M$. Evident $x'>0$ şi $x'\neq 1$ (deoarece dacă $x'=1 \Leftrightarrow e^{\frac{1}{\ln x}}=1 \Leftrightarrow \frac{1}{\ln x}=0$, fals).

Deci $(\forall)x\in M$ este simetrizabil.

5. Fie mulțimea $M=\left\{a+b\sqrt{5}\,\middle|\,a,b\in\mathbb{Q},\ a^2-5b^2=1\right\}\subset\mathbb{R}$ şi operația de înmulțire pe $\mathbb{R}$. Arătați că $(M,\cdot)$ este o structură algebrică, asociativă, comutativă, cu element neutru. Determinați elementele simetrizabile din *M* în raport cu înmulțirea.

R. Să arătăm că înmulțirea pe M este o lege de compoziție.

Fie $x=a+b\sqrt{5},\ y=c+d\sqrt{5},\ a,b,c,d\in\mathbb{Q},\ a^2-5b^2=1,\ c^2-5d^2=1.$

Avem $xy=ac+5bd+(ad+bc)\sqrt{5}$, unde $ac+5bd,\ ad+bc\in\mathbb{Q}$ şi $(ac+5bd)-5(ad+bc)^2=$ $=\left(a^2-5b^2\right)\left(c^2-5d^2\right)=1$ şi deci $xy\in M$.

Cum $M\subset\mathbb{R}$, iar înmulțirea pe $\mathbb{R}$ este asociativă şi comutativă se deduce că rămâne cu aceleaşi proprietăți şi pe submulțimea M.

Fie $e=\alpha+\beta\sqrt{5}\in M,\ \alpha,\beta\in\mathbb{Q},\ \alpha^2-5\beta^2=1$ elementul neutru. Trebuie să avem:

$xe=x,(\forall)x\in M \Leftrightarrow a\alpha+5b\beta+(a\beta+b\alpha)\sqrt{5}=a+b\sqrt{5},\ (\forall)a,b\in\mathbb{Q}$.

De aici rezultă sistemul: $\begin{cases} a\alpha+5b\beta=a \\ a\beta+b\alpha=b \end{cases},\ (\forall)a,b\in\mathbb{Q},\ a^2-5b^2=1$.

Punând $a=1$, $b=0$ în prima ecuație rezultă $\alpha=1$.

Din a doua ecuație rezultă acum $a\beta=0$, când $\beta=0$.

Deci $e=1+0\sqrt{5}\in M,\ \left(1^2-5\cdot 0^2=1\right)$.

Observație. Cum 1 este element neutru pentru înmulțirea din $\mathbb{R}$, iar $1=1+0\cdot\sqrt{5}\in M$, atunci (am văzut la partea teoretică pentru element neutru) că 1 este de asemenea element neutru şi pe mulțimea M în raport cu înmulțirea.

Să determinăm elementele simetrizabile. Fie $x=a+b\sqrt{5},\ a,b\in\mathbb{Q},\ a^2-5b^2=1$. Să găsim $x'\in M$ pentru care $xx'=1 \Leftrightarrow x'=\frac{1}{x} \Leftrightarrow x'=\frac{1}{a+b\sqrt{5}}=\frac{a-b\sqrt{5}}{a^2-5b^2}=a-b\sqrt{5}$. Deci $x'=a+(-b)\sqrt{5}\in M$, deoarece $a, -b \in \mathbb{Q}$ şi $a^2 - 5(-b)^2 = 1$. În final orice element din M este simetrizabil (inversabil) în raport cu înmulţirea. Din $x \in M \Rightarrow x^2, x^3, ..., x^n, ... \in M, (\forall) n$ şi deci M este infinită.

6. Fie $H = \{f_1, f_2, f_3, f_4\} \subset \mathcal{F}(\mathbb{R} - \{0\})$ cu operaţia de compunere a funcţiilor, unde $f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = -x$, $f_4(x) = -\frac{1}{x}$.

Arătaţi că $(H, \circ)$ este structură algebrică asociativă, comutativă, cu element neutru. Stabiliţi elementele simetrizabile din H în raport cu operaţia de compunere.

R. Tabla legii pe H este dată alăturat.

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Întotdeauna compunerea funcţiilor este asociativă. Deci şi pe H rămâne la fel. Comutativitatea legii rezultă din tablă, aceasta fiind simetrică în raport cu diagonala principală. Elementul neutru este f_1.

Observăm că pe fiecare linie a tablei apare elementul neutru. Deci toate elementele sunt simetrizabile (funcţiile sunt inversabile) şi avem:

$$f_1^{-1} = f_1,\ f_2^{-1} = f_2,\ f_3^{-1} = f_3,\ f_4^{-1} = f_4.$$

7. Fie $H = \left\{ A_a \in \mathcal{M}_2(\mathbb{R}) \,\middle|\, A_a = \begin{pmatrix} a & a-1 \\ 0 & 1 \end{pmatrix}, a \in \mathbb{R}, a \neq 0 \right\}$. Să se arate că înmulţirea matricelor de pe $\mathcal{M}_2(\mathbb{R})$ induce o lege de compoziţie asociativă, comutativă şi cu element neutru pe H. Care sunt elementele simetrizabile din H ?

R. Să arătăm că înmulţirea este lege de compoziţie pe *H*. Fie $A_a, A_b \in H$ şi să probăm că $A_a \cdot A_b \in H$.

Avem: $A_a A_b = \begin{pmatrix} a & a-1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} b & b-1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ab & ab-1 \\ 0 & 1 \end{pmatrix} = A_{ab} \in H$ pentru că $a, b \neq 0 \Rightarrow ab \neq 0$.

Înmulţirea matricelor este întotdeauna asociativă. Deci rămâne la fel şi pe *H*. Cum înmulţirea matricelor, în general, nu-i comutativă trebuie să arătăm că $A_a . A_b = A_b \cdot A_a, (\forall) A_a, A_b \in H$.

Ori avem: $A_a \cdot A_b = A_{ab} = A_{ba} = A_b \cdot A_a$ (pentru a doua egalitate am utilizat comutativitatea înmulţirii pe $\mathbb{R}, ab = ba$).

Găsim în continuare elementul neutru al legii. Fie acesta $A_e \in H$.

Trebuie să avem $A_a \cdot A_e = A_a, (\forall) A_a \in H \Leftrightarrow A_{ae} = A_a, (\forall) A_a \in H$.

Cum $A_a = A_b \Leftrightarrow a = b$, de mai sus avem $ae = a$ şi deci $e = 1$ $(a \neq 0)$.

Aşadar elementul neutru este $A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Acest lucru se putea obţine remarcând că pentru $a = 1$ rezultă $A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ matricea unitate care este element neutru în raport cu înmulţirea matricelor pe $\mathcal{M}_2(\mathbb{R})$. Deci rămâne element neutru şi pentru înmulţire pe *H*.

Elementul $A_a \in H$ este simetrizabil dacă există $A_{a'} \in H$ pentru care $A_a \cdot A_{a'} = A_1 \Leftrightarrow A_{aa'} = A_1$.

De aici $aa' = 1 \Rightarrow a' = \frac{1}{a} (a \neq 0)$.

Aşadar orice $A_a \in H$ are simetric matricea $A_{\frac{1}{a}} \in H$.

În acest caz, din $A_a \cdot A_{a'} = I_2$ rezultă că $A_{a'}$ este chiar inversa matricei A_a.

8. **Se consideră** $H = \left\{ \begin{pmatrix} a & 0 & a \\ 0 & 1 & 0 \\ a & 0 & a \end{pmatrix} \middle| a > 0 \right\}$**. Arătați că înmulțirea matricelor din** $\mathcal{M}_3(\mathbb{R})$ **induce pe** H **o lege de compoziție asociativă, comutativă, cu element neutru.**
Determinați elementele simetrizabile din H **în raport cu înmulțirea.**

R. Se verifică imediat că $(\forall) A_a, A_b \in H \Rightarrow A_a \cdot A_b = A_{2ab} \in H$ $(a,b > 0 \Rightarrow ab > 0)$. Înmulțirea matricelor este întotdeauna asociativă, deci la fel rămâne și pe *H*.

Pentru comutativitate avem: $A_a \cdot A_b = A_{2ab} = A_b \cdot A_a, (\forall) A_a, A_b \in H$.

Elementul neutru $A_e \in H$ are calitatea că $A_a \cdot A_e = A_a, (\forall) A_a \in H \Leftrightarrow A_{2ae} = A_a, (\forall) A_a \in H$. Cum $A_a = A_b \Leftrightarrow a = b$, de mai sus rezultă $2ae = a$ și deci $e = \frac{1}{2}$. Așadar elementul neutru pentru înmulțirea pe *H* este matricea $A_{\frac{1}{2}} = \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 1 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix}$.

Observăm că I_3 care este element neutru în raport cu înmulțirea de pe $\mathcal{M}_3(\mathbb{R})$ nu aparține lui H ! Deci nu poate fi vorba ca I_3 să fie element neutru pentru înmulțirea pe *H*.

Să determinăm acum elementele simetrizabile (și nu inversabile, care le numim așa dacă I_3 este element neutru față de înmulțirea matricelor din $\mathcal{M}_3(\mathbb{C})$) din H în raport cu înmulțirea. Fie $A_a \in H$ și $A_{a'} \in H$ simetricul său. Atunci trebuie să avem: $A_a \cdot A_{a'} = A_{\frac{1}{2}} \Leftrightarrow A_{2aa'} = A_{\frac{1}{2}}$. De aici $2aa' = \frac{1}{2}$ și deci $a' = \frac{1}{4a} > 0$ dacă $a > 0$. Deci pentru $A_a \in H$, simetricul său este $A_{\frac{1}{4a}}$.

9. **Fie** $n \in \mathbb{N}, n \geq 2$, **dat și** $H = \left\{ A = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \middle| x, y \in \mathbb{C}, A^n = I_2 \right\}$**. Arătați că** $(H, \cdot)$ **este o structură algebrică, comutativă, cu element neutru. Care sunt elementele simetrizabile din** H **în raport cu înmulțirea ?**

R. Înmulțirea pe H este o lege de compoziție deoarece $(\forall) A, B \in H \Rightarrow AB = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \begin{pmatrix} x' & 0 \\ 0 & y' \end{pmatrix} = \begin{pmatrix} xx' & 0 \\ 0 & yy' \end{pmatrix}$. Avem imediat că: $A^n = \begin{pmatrix} x^n & 0 \\ 0 & y^n \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, iar de aici $x^n = 1, \ y^n = 1$.

Aceasta înseamnă că pentru matricea $A = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$, elementele *x*, *y* sunt soluțiile ecuației $z^n = 1$. Deci mulțimea *H* are în total n^2 elemente.

Înmulțirea matricelor este întotdeauna asociativă.

Înmulțirea este și comutativă în acest caz (cum se vede ușor).

Elementul neutru este I_2 (îl obținem punând $x = y = 1$ rădăcină pentru $z^n = 1$).

Inversa lui *A* este A^{n-1} pentru că $A \cdot A^{n-1} = I_2$. Inversa lui A^2 este A^{n-2} etc. Toate elementele lui *H* sunt inversabile.

Probleme propuse

1. Pe mulțimea $\mathbb{Z}$ se definește legea de compoziție $x \otimes y =$ restul împărțirii lui xy la 6. Fie $H = \{0, 1, 2, 3, 4, 5\} \subset \mathbb{Z}$. Arătați că $(H, \otimes)$ este o structură algebrică comutativă, cu element unitate. Determinați elementele din H simetrizabile în raport cu „ $\otimes$ “.

2. Pe mulțimea numerelor complexe $\mathbb{C}$ se definește legea „ $*$ “ prin $z_1 * z_2 = z_1 + z_2 - z_1 z_2$. Fie $H = \mathbb{C} - \{1\}$. Arătați că „ $*$ “ induce pe H o lege de compoziție asociativă, comutativă, cu element neutru. Determinați elementele din H simetrizabile în raport cu legea dată.

3. Pe $\mathbb{R}$ definim legea de compoziție $x \top y = 3xy + 6(x+y) + 10$. Fie $H = (-2, \infty)$. Arătați că $(H, \top)$ este o structură algebrică comutativă, cu element neutru și că orice element din H este simetrizabil în raport cu legea „ $\top$ “.

4. Fie $H = \left\{ x \in \mathbb{R} \middle| x = a - b\sqrt{10},\ a, b \in \mathbb{Q},\ a^2 - 10b^2 = 1 \right\}$ și operația de înmulțire pe $\mathbb{R}$. Demonstrați că $(H, \cdot)$ este o structură algebrică asociativă, comutativă, cu element neutru și orice element din H admite un simetric (invers) în raport cu operația de înmulțire.

5. Fie $H = (-1, 1) \subset \mathbb{R}$ și aplicația $x * y = \dfrac{x+y}{1+xy}$. Arătați că $(H, *)$ este o structură algebrică asociativă, comutativă, cu element neutru și orice element din H este simetrizabil în raport cu „ $*$ “.

6. Se consideră $H = (0, \infty) - \{1\}$ și aplicația $x * y = x^{5 \ln y}$. Arătați că $(H, *)$ este o structură algebrică asociativă, comutativă, cu element neutru și că orice element din H este simetrizabil în raport cu legea dată.

7. Considerăm mulțimea de matrice $H = \left\{ X^n \middle| n \in \mathbb{N}, n \geq 1, X = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \right\}$ împreună cu operația de înmulțire. Demonstrați că $(H, \cdot)$ este o structură algebrică asociativă, comutativă, cu element neutru și orice element din H este simetrizabil în raport cu înmulțirea.

8. Fie $H = (0, 1)$ și aplicația $x \circ y = \dfrac{xy}{2xy + 1 - (x+y)}$. Arătați că $(H, \circ)$ este o structură algebrică asociativă, comutativă, cu element neutru și orice element din H este simetrizabil în raport cu „ $\circ$ “.

9. Fie $\left\{ A_\alpha = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \middle| \alpha \in \mathbb{R} \right\} \subset \mathcal{M}_2(\mathbb{R})$. Arătați că înmulțirea matricelor de pe $\mathcal{M}_2(\mathbb{R})$ induce pe H o lege de compoziție asociativă, comutativă, cu element neutru și orice element din H este simetrizabil în raport cu această lege.

10. Fie $A = \begin{pmatrix} -1 & 1 \\ -2 & 2 \end{pmatrix}$; $B = \begin{pmatrix} 2 & -1 \\ 2 & -1 \end{pmatrix}$ și mulțimea $H = \{aA + B \mid a \in \mathbb{R}^*\}$.
Arătați că H este parte stabilă a lui $\mathcal{M}_2(\mathbb{R})$ în raport cu înmulțirea matricelor și $U(H) = H$.

1.4. STRUCTURI ALGEBRICE

Am văzut că dacă pe mulțimea nevidă M definim o lege de compoziție $*$, atunci cuplul $(M,*)$ l-am numit sistem algebric.

În general, dacă $M \neq \varnothing$, atunci numim **structură algebrică pe mulțimea** M, orice structură determinată pe M de una sau mai multe legi de compoziție, aceste legi fiind supuse unor condiții (asociativitate, comutativitate, ...), sau fiind legate una de alta prin anumite relații (distributivitatea unei legi de compoziție față de alta).

Condițiile la care sunt supuse legile ce definesc o structură algebrică şi relațiile de legătură ce există între aceste legi constituie axiomele structurii respective. Numărul legilor de compoziție şi axiomele caracterizează specia de structură considerată.

Teoriile axiomatizate (numite şi sisteme axiomatice) sunt teorii ipotetico-deductive în care termenii nedefiniți (primitivi) şi propozițiile primitive (axiomele) sunt expuse explicit şi complet de la început.

Dezideratele ce se au în vedere despre ansamblul de axiome rezidă din pretențiile asupra unei teorii axiomatice, şi anume: **non contradicția axiomelor** (atunci când în sistem nu pot deriva simultan o propoziție şi negația sa), **independența axiomelor** (nici una din axiomele sistemului să nu poată fi dedusă în interiorul sistemului, utilizându-le doar pe celelalte) şi **completitudinea axiomelor** (pretinde ca întreaga teorie să se poată deduce în cadrul sistemului).

În toate structurile algebrice pe care le vom studia vom avea situația de mai jos: dată fiind o mulțime $M \neq \varnothing$ înzestrată cu o structură algebrică şi $M' \neq \varnothing, M' \subset M$, atunci numim **structură indusă** pe M' de structura lui M, structura algebrică determinată de legile induse pe M' de către legile care definesc structura pe M.

Se spunea adesea că structura dată pe M prelungeşte structura ce o induce pe o parte a lui M.

PIONIERI AI MATEMATICII	
EUCLID (330? – 375 î.C.) **Matematician grec**	**David HILBERT (1862-1943)** **Matematician german**
	
CONTRIBUȚII	**CONTRIBUȚII**
• ***„Părintele“ geometriei***	• ***algebră*** • ***analiză*** • ***geometrie***

Notă istorică. Istoric, problema axiomatizării începe cu lucrările lui Euclid în domeniul geometriei. Matematicienilor secolului al XIX-lea le revine meritul de a elucida această problemă plecând de la

dezvoltarea geometriei elementare. Marele matematician german David Hilbert (1862-1943) a reuşit să rezolve (1899) de o manieră satisfăcătoare dificila problemă a axiomatizării geometriei (20 axiome). Axiomatizarea aritmeticii (1889) a fost realizată de matematicianul italian Giuseppe Peano (1858-1932) (5 axiome). Teoria mulţimilor a fost axiomatizată de matematicianul german Zermelo (1871-1953) (7 axiome), reluată şi precizată de matematicianul german Fraenkel (1891-1965).
Ca număr de exemplare tipărite pe plan mondial, *Elementele* lui Euclid se situează pe locul doi după Biblie.

1.4.1. Monoizi

Definiţie. Cuplul $(M,*)$, unde $M \neq \varnothing$ şi $*$ este o lege de compoziţie pe *M,* se numeşte monoid dacă legea $*$ satisface următoarele două axiome:

M_1) Legea $*$ este **asociativă**.

M_2) Legea $*$ **are element neutru**.

Dacă , în plus, legea $*$ verifică şi axioma:

M_3) Legea $*$ este **comutativă**,

atunci cuplul $(M,*)$ se numeşte **monoid comutativ**.

Dacă $(M,*)$ este monoid, atunci $M' \subset M$, $M' \neq \varnothing$ pentru care $(M',*)$ este monoid îl numim **submonoidul** monoidului $(M,*)$.

Exemple cunoscute de monoizi

1. Mulţimea numerelor naturale $\mathbb{N}$ cu operaţia de adunare (respectiv de înmulţire este monoid comutativ cu elementul neutru 0 (zero) (respectiv 1 (unu)).
2. Mulţimea numerelor întregi $\mathbb{Z}$ cu operaţia de adunare (respectiv de înmulţire) este monoid comutativ cu elementul neutru zero (respectiv 1 (unu)).
Submulţimea lui $\mathbb{Z}$ formată din numerele întregi impare (notată $2\mathbb{Z}+1$) cu operaţia de înmulţire este un submonoid al lui $(\mathbb{Z},\cdot)$

3. Fie $X \neq \varnothing$. Atunci $(\mathcal{P}(X),\cup),(\mathcal{P}(X),\cap)$ sunt monoizi comutativi, cu element neutru $\varnothing$ şi respectiv *X*.

4. Fie $X \neq \varnothing$ şi $\mathcal{B}(X)=\{f: X \to X,\ f \text{ bijectivă}\} \subset \mathcal{F}(X)$. Cuplul $(\mathcal{B}(X),\circ)$ este monoid necomutativ cu element neutru aplicaţia identică a mulţimii $X, 1_X : X \to X, 1_X(a)=a, (\forall) a \in X$.

5. Mulţimea matricelor de ordin *n* cu elemente din $\mathbb{C}$, $\mathcal{M}_n(\mathbb{C}), n \geq 2$, împreună cu operaţia de înmulţire este un monoid necomutativ. Elementul neutru este matricea unitate I_n.

6. Dacă $(M,\cdot)$ este monoid multiplicativ şi $x \in M$, fixat, atunci $H_x=\{e=x^0, x^1, x^2,...,x^n,...\}$ cu înmulţirea este submonoid al lui *M,* numit submonoidul ciclic generat de *x*.

Elementele $x \in M$ simetrizabile în raport cu legea $*$ le numim **elemente simetrizabile ale monoidului**. Notăm mulţimea aceasta cu *U*(*M*). Deci:

$$\boxed{U(M)=\{x \mid x \in M,\ x \text{ simetrizabil}\}}$$

Evident $U(M) \neq \varnothing$, deoarece elementul neutru $e \in M$ aparţine lui *U*(*M*).

Exemple

1. Pentru monoidul $(\mathbb{N},+)$, avem $U(\mathbb{N})=\{0\}$, iar pentru $(\mathbb{N},\cdot)$ avem $U(\mathbb{N})=\{1\}$.

2. Pentru $(\mathbb{Z},+)$ avem $U(\mathbb{Z})=\mathbb{Z}$, iar pentru $(\mathbb{Z},\cdot)$ avem $U(\mathbb{Z})=\{-1,1\}$.

3. Pentru $(\mathcal{F}(X),\circ)$ avem $U(\mathcal{F}(x))=\mathcal{B}(X)$.

Am văzut în paragrafele precedente (la element neutru şi la elemente simetrice), pentru o lege multiplicativă pe M ce înseamnă x^n şi $x^{-n}=\left(x^{-1}\right)^n$, $n\in\mathbb{N}$.

Analog în cazul legii aditive am precizat ce înseamnă nx şi respectiv $(-nx)$.

Pentru monoid are loc

Teorema. Fie $(M,\cdot)$ monoid şi $x\in M$. Atunci:

1) $x^n\cdot x^m=x^{n+m},(\forall)n,m\in\mathbb{N}$.

2) $(x^n)^m=x^{nm},(\forall)n,m\in\mathbb{N}$.

Dacă $x\in U(M)$, atunci egalitățile 1), 2) au loc $(\forall)n,m\in\mathbb{Z}$.

Demonstrație. 1) Avem $x^n\cdot x^m=\underbrace{(x\cdot x\cdot\ldots\cdot x)}_{n}\cdot\underbrace{(x\cdot x\cdot\ldots\cdot x)}_{m}=\underbrace{(x\cdot x\cdot\ldots\cdot x)}_{n+m}=x^{n+m}$.

Dacă $x\in U(M)$, atunci se face discuția în cazurile: $n,m<0$; $n\geq 0, m<0$; $n<0, m\geq 0$. Să luăm spre exemplu cazul $n,m<0$. Atunci există $m',n'>0$ pentru care $m=-m'$, $n=-n'$. Avem:

$$x^n\cdot x^m=x^{n'}\cdot x^{-m'}=\left(x^{-1}\right)^{n'}\left(x^{-1}\right)^{m'}=\left(x^{-1}\right)^{n'+m'}=x^{(-n')+(-m')}=x^{n+m}.$$

Analog se tratează şi celelalte cazuri.

2) $(x^n)^m=\underbrace{x^n\cdot x^n\cdot\ldots\cdot x^n}_{m}=x^{n+n+\ldots+n}=x^{nm}$, dacă $n,m\in\mathbb{N}$.

Asemănător cu **1)** se tratează celelalte cazuri pentru $m,n\in\mathbb{Z}$. ■

Probleme propuse

1. Fie $M=\{(n,f)\mid f\in\mathbb{C}[X],\ \mathrm{grad}(f)=n\in\mathbb{N}\}$. Pe mulțimea M se defineşte legea de compoziție: $(n,f)*(m,g)=(n+m,f\cdot g)$, $(\forall)(n,f),(m,g)\in M$. Arătați că $(M,*)$ este monoid comutativ.

2. Fie $M=\left\{A=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathcal{M}_2(\mathbb{Z})\,\middle|\,a+c=b+d\right\}$.

1) Arătați că $(M,\cdot)$ este monoid, unde „$\cdot$" este înmulțirea uzuală a matricelor.

2) Arătați că elementele $A_k=\begin{pmatrix}k&k-1\\1-k&2-k\end{pmatrix}\in M$, $k\in\mathbb{Z}$, sunt simetrizabile.

3. Se defineşte pe $\mathbb{R}$ legea de compoziție $x*y=xy-ax+by$, $a,b\in\mathbb{R}$. Să se determine $(a,b)\in\mathbb{R}^2$ astfel încât, $(\mathbb{R},*)$ să fie monoid.

4. **În monoidul multiplicativ $(M,\cdot)$, $M=\left\{\begin{pmatrix} a & 0 & b \\ 0 & 0 & 0 \\ b & 0 & a \end{pmatrix} \middle| a,b\in\mathbb{R}\right\}$ să se determine simetricul elementului $\begin{pmatrix} 2 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 2 \end{pmatrix}$.**

5. **Se consideră $M=\left\{\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \middle| a+b+c=0,\ a,b,c\in\mathbb{R}\right\}$.**

1) Dacă $E=\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, atunci un element din M se scrie $aI_3+bE+cE^2$.

2) Să se arate că M este parte stabilă a lui $\mathcal{M}_3(\mathbb{R})$ în raport cu înmulțirea matricelor.

3) Să se arate că $(M,\cdot)$ este monoid comutativ.

6. **Fie șirul $(F_k)_{k\geq 0}$ definit prin $F_0=1$, $F_1=0$, $F_{k+1}=F_k+F_{k-1}$, $k\in\mathbb{N}^*$, iar $M=\left\{\begin{pmatrix} F_k & 0 & F_{k+1} \\ 0 & 1 & 0 \\ F_{k+1} & 0 & F_{k+2} \end{pmatrix} \middle| k\in\mathbb{N}\right\}$.**

Să se arate că $M=\left\{A^k \middle| k\in\mathbb{N}\right\}$, unde $A=\begin{pmatrix} F_1 & 0 & F_2 \\ 0 & 1 & 0 \\ F_2 & 0 & F_3 \end{pmatrix}$ și apoi că $(M,\cdot)$ este monoid.

1.4.2. Grupuri

Prin intermediul noțiunii de grup se pot aplica aceleași teoreme la mulțimi diferite înzestrate cu legi de compoziție diferite.
Marele matematician francez Henri Poincaré (1854-1912) spunea în legătură cu acest subiect: „La mathématique est l'art de donner le même nom à des choses différentes“.
Acest aforism subliniază un aspect esențial al matematicii secolului nostru.

Definiție. Fie $G\neq\varnothing$ și $*$ o lege de compoziție pe G. Cuplul $(G,*)$ se numește **grup** dacă au loc următoarele axiome:

G_1) Legea $*$ este **asociativă**, adică

$$(x*y)*z=x*(y*z),\ (\forall)x,y,z\in G.$$

G_2) Legea $*$ are **element neutru**, adică $(\exists)e\in G$ astfel încât $(\forall)x\in G$ să avem $x*e=e*x=x$.

G_3) Orice element din G este simetrizabil în raport cu $*$, adică pentru fiecare $x\in G$, există $x'\in G$ astfel încât

$$x*x'=x'*x=e.$$

Dacă, în plus, legea $*$ verifică și axioma

G_4) Legea $*$ este **comutativă**, adică

$$x*y=y*x,\ (\forall)x,y\in G$$

atunci cuplul $(G,*)$ se numește **grup comutativ (abelian)**.

UN PIONIER AL MATEMATICII

Niels ABEL (1802 – 1829)

Matematician norvegian

CONTRIBUȚII

- ***algebră abstractă***
- ***analiză***

Ştim că elementul neutru dacă există este unic. De asemenea simetricul unui element este unic.
Ansamblul de condiții G_1, G_2, G_3 poartă numele de **axiomele grupului**. Cât priveşte adjectivul abelian el derivă de la numele celebrului matematician norvegian Niels Abel (1802-1829).
Teoria grupurilor constă în a degaja din această definiție toate consecințele posibile. Se stabilesc astfel teoremele la care se poate face referire de fiecare dată când în cursul studiului se întâlneşte o structură de grup. Ilustrăm rolul teoriei grupurilor în matematică prin comparația următoare: boala M se manifestă sub forma unei mulțimi de fenomene $F=\{F_1, F_2, ..., F_n\}$. Printre acestea sunt unele care sunt determinante, adică acelea care sunt suficiente pentru a asigura existența bolii M; fie $F'=\{F'_1, F'_2, ..., F'_k\}$ mulțimea acestor simptome, care este o submulțime a lui F. Atunci când medicul a constatat prezența lor, el este în măsură să afirme că celelalte manifestări ale bolii (care aparțin complementarei lui F' în F) vor apare şi în consecință să stabilească o medicamentație adecvată.
Din definiție se deduce că un grup este un monoid în care orice element este simetrizabil, altfel spus $U(G) = G$. Reciproca nu este adevărată ($(\mathbb{N},+)$ când $U(\mathbb{N})=\{0\}$). Pentru uşurința prezentării părții teoretice considerăm că legea $*$ este înlocuită cu cea dată de înmulțire (când vorbim de **grup multiplicativ**) sau de adunare (când grupul îl **numim aditiv**).

Exemple cunoscute de grupuri

1. Grupuri numerice. Exemple de grupuri abeliene:

- **grupul aditiv al numerelor întregi** $(\mathbb{Z},+)$;
- **grupul aditiv al numerelor raționale** $(\mathbb{Q},+)$;
- **grupul aditiv al numerelor reale** $(\mathbb{R},+)$);
- **grupul aditiv al numerelor complexe** $(\mathbb{C},+)$;
- **grupul multiplicativ al numerelor raționale nenule** $(\mathbb{Q}^*,\cdot)$;
- **grupul multiplicativ al numerelor reale nenule** $(\mathbb{R}^*,\cdot)$;
- **grupul multiplicativ al numerelor complexe nenule** $(\mathbb{C}^*,\cdot)$.
- **grupuri multiplicative cu un element** $(\{1\},\cdot)$, $(\{0\},\cdot)$;
- **grupul multiplicativ cu două elemente** $(\{-1,1\},\cdot)$;

• **grupul multiplicativ cu trei elemente** $\left(\{1,\varepsilon,\varepsilon^2\},\cdot\right)$ **unde** $\varepsilon=\dfrac{-1+i\sqrt{3}}{2}$.

2. Grupul aditiv comutativ al matricelor de tip (m,n), $\left(\mathcal{M}_{m,n}(\mathbb{C}),+\right)$.

3. Exemple de grupuri necomutative:

• **grupul aplicațiilor bijective în raport cu operația de compunere,** $\left(\mathcal{B}(M),\circ\right)$.

Grupul $\left(\mathcal{B}(M),\circ\right)$ **el însuşi şi mai ales diversele sale subgrupuri numite grupuri de transformări constituie un punct de plecare pentru toate aplicațiile practice posibile ale teoriei grupurilor. Este suficient de a menționa „Programul de la Erlangen“, devenit celebru, de Felix Klein (1872), care a adoptat noțiunea de grup de transformări ca bază pentru clasificarea diferitelor tipuri de geometrii.**

• **grupul matricelor pătratice de ordin** n **cu coeficienți reali şi cu determinantul nenul, notat** $\left(GL(n,\mathbb{R}),\cdot\right)$. **Acest grup se numeşte grupul liniar complet de ordin** n **pe R.**

• **grupul cuaternionilor. Mulțimea** $G=\{1,i,j,k,-1,-i,-j,-k\}$ **cu operația de înmulțire necomutativă dată de** $(-1)^2=1, i^2=j^2=k^2=-1, ij=-ji=k, jk=-kj=i, ki=-ik=j$, $-x=(-1)x=x(-1), (\forall)x\in G$ **şi având elementul neutru pe 1.**

Definiție. Un grup G se numeşte **grup finit** dacă mulțimea G este **finită** şi **grup infinit**, în caz contrar.

Se numeşte **ordinul grupului** G, notat $|G|$, cardinalul lui G (numărul de elemente din G).

Grupurile de la exemplul 1 de mai sus sunt infinite (cu excepția ultimelor trei).
Dacă M este finită, atunci grupurile de la exemplul 2 de mai sus sunt finite.

Probleme rezolvate

1. Pe mulțimea numerelor întregi $\mathbb{Z}$ **se defineşte aplicația** $x*y=x+y-2$. **Să se arate că** $(\mathbb{Z},*)$ **este un grup comutativ.**

R. Dacă $x,y\in\mathbb{Z}$, evident că $x*y=x+y-2\in\mathbb{Z}$, ceea ce arată că $*$ este o lege de compoziție pe $\mathbb{Z}$. Verificăm axiomele grupului comutativ.

G_1) Asociativitatea legii $*$. Trebuie probat că $(x*y)*z=x*(y*z), (\forall)x,y,z\in\mathbb{Z}$.

Avem:

$(x*y)*z=(x+y-2)*z=(x+y-2)+z-2=x+y+z-4$, (1)

şi

$x*(y*z)=x*(y+z-2)=x+(y+z-2)-2=x+y+z-4$, (2).

Din (1) şi (2) rezultă că legea $*$ este asociativă.

G_2) Elementul neutru. Să arătăm că există $e\in\mathbb{Z}$ astfel încât $x*e=e*x=x, (\forall)x\in\mathbb{Z}$.

Din $x*e=x, (\forall)x\in\mathbb{Z}$ rezultă $x+e-2=x$ sau $e=2\in\mathbb{Z}$.

G_3) Elemente simetrizabile. Fie $x\in\mathbb{Z}$. Să arătăm că există $x'\in\mathbb{Z}$ pentru care $x*x'=x'*x=e$. Din $x*x'=e\Rightarrow x+x'-2=2$ sau $x'=4-x\in\mathbb{Z}$. Deci $x'=4-x$ este simetricul lui x în raport cu $*$.

G_4) Comutativitatea legii $*$. Avem de demonstrat că $x * y = y * x, (\forall) x, y \in \mathbb{Z}$. Relația de demonstrat se rescrie $x + y - 2 = y + x - 2, (\forall) x, y \in \mathbb{Z}$, ceea ce este adevărat deoarece adunarea pe $\mathbb{Z}$ este comutativă $(x + y = y + x)$. Aşadar $(\mathbb{Z}, *)$ este grup abelian.

Observație. Atunci când ni se cere să arătăm că un grup este comutativ, după asociativitate se demonstrează comutativitatea legii deoarece pentru celelalte axiome scriem relațiile mai simplu

- pentru element neutru $x * e = x, (\forall) x \in \mathbb{Z}$ (sau $e * x = x, (\forall) x \in \mathbb{Z}$).
- pentru element simetric $x * x' = e$ (sau $x' * x = e$).

2. Pe mulțimea numerelor reale $\mathbb{R}$ se consideră aplicația $x \top y = xy - 5x - 5y + 30$. Determină această lege pe $\mathbb{R}$ o structură de grup? Dar pe $\mathbb{R} - \{5\}$?

R. Evident aplicația este o lege de compoziție pe $\mathbb{R}$. Să vedem dacă se verifică axiomele grupului.

G_1) Asociativitatea legii $\top$. Avem de verificat că $(x \top y) \top z = x \top (y \top z), (\forall) x, y, z \in \mathbb{R}$.

Se calculează cei doi membri şi găsim expresia $xyz - 5(xy + xz + yz) + 25(x + y + z) - 120$.

G_2) Comutativitatea legii $\top$. Trebuie să avem: $x \top y = y \top x, (\forall) x, y \in \mathbb{R}$. Egalitatea se scrie $xy - 5(x + y) + 30 = yx - 5(y + x) + 30, (\forall) x, y \in \mathbb{R}$, care este adevărată dacă ținem seama de comutativitatea produsului şi sumei pe $\mathbb{R}$ $(xy = yx, x + y = y + x)$.

G_3) Element neutru. Să determinăm $e \in \mathbb{R}$ pentru care $x \top e = x, (\forall) x \in \mathbb{R}$. Egalitatea se mai scrie $xe - 5(x + e) + 30 = x, (\forall) x \in \mathbb{R}$ sau $e(x - 5) = 6(x - 5), (\forall) x \in \mathbb{R}$. Dacă $x \neq 5$, atunci $e = 6$. Mai rămâne să verificăm şi pentru x = 5 egalitatea $x \top e = x$, adică $5 \top 6 = 5$, ceea ce este imediat.

G_4) Elemente simetrizabile. Să vedem dacă orice $x \in \mathbb{R}$ are un simetric $x' \in \mathbb{R}$, pentru care $x \top x' = 6$. Rescriem egalitatea sub forma $xx' - 5(x + x') + 30 = 6$ sau $x'(x - 5) = 5x - 24$. De aici $x' = \dfrac{5x - 24}{x - 5}$ dacă $x \neq 5$. Aşadar nu orice $x \in \mathbb{R}$ $(x = 5)$ are simetric. Prin urmare legea $\top$ nu determină pe $\mathbb{R}$ o structură de grup. Dar pe $\mathbb{R} - \{5\}$ legea $\top$ determină o structură de grup dacă mai arătăm că $x, y \neq 5 \Rightarrow x \top y \neq 5 (\Leftrightarrow xy - 5x - 5y + 30 \neq 5 \Leftrightarrow (x - 5)(y - 5) \neq 0$, evident) şi $x' = \dfrac{5x - 24}{x - 5} \neq 5 (\Leftrightarrow 5x - 24 \neq 5x - 25$, evident). Aşadar $(\mathbb{R} - \{5\}, \top)$ este grup abelian.

3. Se consideră $G = (-1,1)$ şi pe G aplicația $x * y = \dfrac{x + y}{1 + xy}$. Arătați $(G, *)$ este un grup abelian.

R. Verificăm axiomele grupului abelian. Probăm mai întâi că $*$ este o lege de compoziție pe G.

Fie $x, y \in G$ şi să arătăm că $x * y \in G$. Avem $x \in G \Leftrightarrow -1 < x < 1 \Leftrightarrow |x| < 1$. Din $x, y \in G$ rezultă $|x|, |y| < 1$ şi deci $|xy| < 1 \Leftrightarrow -1 < xy < 1$, adică de aici $1 + xy > 0$. Acum $x * y \in G \Leftrightarrow$ $\Leftrightarrow -1 < x * y < 1$. Pentru prima inegalitate:

$$-1 < x * y \Leftrightarrow -1 < \frac{x + y}{1 + xy} \Leftrightarrow 0 < xy + x + y + 1 \Leftrightarrow 0 < (x + 1)(y + 1), \text{ evident deoarece } -1 < x, y.$$

Pentru a doua inegalitate avem echivalențele:

$$x * y < 1 \Leftrightarrow \frac{x + y}{1 + xy} < 1 \Leftrightarrow x + y - 1 - xy < 0 \Leftrightarrow (x - 1)(1 - y) < 0, \text{ adevărat deoarece } x, y < 1.$$

G_1) Asociativitatea legii $*$. Trebuie să verificăm că $(x * y) * z = x * (y * z), (\forall) x, y, z \in G$.

Efectuând calculele în cei doi membri găsim aceeaşi expresie: $\dfrac{x + y + z + xyz}{1 + xy + xz + yz}$.

Deci legea $*$ este asociativă pe G.

G$_2$) Comutativitatea legii $*$. Pentru orice $x, y \in G$ avem: $x * y = y * x \Leftrightarrow \frac{x+y}{1+xy} = \frac{y+x}{1+yx}$, adevărat deoarece adunarea şi înmulţirea numerelor reale sunt operaţii comutative.

G$_3$) Element neutru pentru $*$. Să arătăm că există $e \in G$, pentru care $x * e = x, (\forall) x \in G$.

Avem: $\frac{x+e}{1+xe} = x, (\forall) x \in G \Leftrightarrow x + e = x + x^2 e \Leftrightarrow e(1-x^2) = 0, (\forall) x \in (-1,1) \Leftrightarrow e = 0$. Este clar că $e = 0 \in G$ şi reprezintă elementul neutru în raport cu legea $*$.

G$_4$) Elemente simetrizabile. Să arătăm că orice $x \in G$ are un simetric $x' \in G$ astfel încât $x * x' = 0$. De aici $\frac{x+x'}{1+xx'} = 0$ dă $x + x' = 0$, adică $x' = -x$. Mai trebuie să arătăm că $x' \in (-1,1) \Leftrightarrow -1 < -x < 1 \Leftrightarrow 1 > x > -1$ evident deoarece $x \in (-1,1)$.

Aşadar $(G,*)$ este grup abelian.

4. Pe mulţimea $R_1 = \mathbb{R} - \{1\}$ se consideră aplicaţia: $x * y = 2xy - 2x - 2y + c, c \in \mathbb{R}$

Pentru ce valori ale lui c, cuplul $(R_1,*)$ este grup abelian?

R. Cerând ca legea $*$ să fie asociativă avem: $(x * y) * z = x * (y * z), (\forall) x, y, z \in R_1$ sau $4xyz - 4(xy + xz + yz) + 4x + 4y + 2(c-1)z - c = 4xyz - 4(xy + xz + yz) + 2(c-1)x + 4y + 4z - c$, $(\forall) x, y, z \in R_1$ sau după identificare c – 1 = 2, adică c = 3.

Aşadar legea $*$ devine $x * y = 2xy - 2x - 2y + 3$.

Să verificăm faptul că $*$ este lege de compoziţie pe R_1, adică să arătăm că dacă $x, y \in R_1$ atunci $x * y \in R_1$, mai precis să verificăm că pentru $x \neq 1,\ y \neq 1 \Rightarrow x * y \neq 1$ adică $2xy - 2x - 2y + 3 \neq 1 \Leftrightarrow$ $\Leftrightarrow (x-1)(y-1) \neq 0$, evident.

Comutativitatea legii este imediată. Elementul neutru e se determină din $x * e = x, (\forall) x \in R_1 \Leftrightarrow$ $\Leftrightarrow 2e(x-1) = 3(x-1) \Leftrightarrow e = \frac{3}{2} \in R_1$.

Se arată uşor că orice $x \in R_1$ are un simetric $x' \in R_1$ astfel încât $x * x' = \frac{3}{2} \Leftrightarrow 2x'(x-1) = 2x - \frac{3}{2}$ şi deci $x' = \frac{4x-3}{4(x-1)} \in R_1$ (deoarece dacă x' = 1, atunci ar rezulta $4x - 3 = 4(x-1)$ imposibil).

Aşadar $(R_1,*)$ este grup abelian.

5. Se consideră funcţiile $f_i : \mathbb{R} - \{0,1\} \to \mathbb{R} - \{0,1\}, i = \overline{1,6}$ definite prin $f_1(x) = x, f_2(x) = \frac{1}{x}$, $f_3(x) = 1 - x$, $f_4(x) = \frac{x-1}{x}$, $f_5(x) = \frac{x}{x-1}$, $f_6(x) = \frac{1}{1-x}$. Să se arate că pe mulţimea $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ compunerea funcţiilor determină o structură de grup necomutativ.

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_5	f_6	f_2	f_1
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_5	f_2	f_1	f_3	f_4

R. Tabla legii este dată alăturat.
Se constată că legea $\circ$ este lege de compoziţie pe G.
Întotdeauna compunerea funcţiilor este asociativă şi deci această proprietate se păstrează şi pe G. Elementul neutru este f_1. Orice element din G este inversabil,

$f_1^{-1} = f_1,\ f_2^{-1} = f_2,\ f_3^{-1} = f_3,\ f_4^{-1} = f_6,\ f_5^{-1} = f_5,\ f_6^{-1} = f_4$.

Compunerea nu este comutativă pe G deoarece $f_3 \circ f_2 = f_4 \neq f_2 \circ f_3 = f_6$.

6. Se consideră mulțimea de matrice: $G=\left\{\begin{pmatrix}1-x & x\\ x & 1-x\end{pmatrix}\middle| x\in\mathbb{R}-\left\{\frac{1}{2}\right\}\right\}$. Arătați că $(G,\cdot)$ este grup abelian.

R. Arătăm mai întâi că înmulțirea pe G este lege de compoziție.

Notăm $A_x=\begin{pmatrix}1-x & x\\ x & 1-x\end{pmatrix}, x\neq\frac{1}{2}$. Dacă $A_x, A_y\in G,\ x,y\neq\frac{1}{2}$, atunci

$A_x\cdot A_y=\begin{pmatrix}1-(x+y-2xy) & x+y-2xy\\ x+y-2xy & 1-(x+y-2xy)\end{pmatrix}=A_{x+y-2xy}\in G$ dacă $x+y-2xy\neq\frac{1}{2}$ adevărat, deoarece:

$x+y-2xy=\frac{1}{2}-2\left(x-\frac{1}{2}\right)\left(y-\frac{1}{2}\right)$.

Cum $x\neq\frac{1}{2},\ y\neq\frac{1}{2}$ rezultă $\left(x-\frac{1}{2}\right)\left(y-\frac{1}{2}\right)\neq 0$ și deci $x+y-2xy\neq\frac{1}{2}$. Verificăm axiomele grupului.

G_1) Asociativitatea înmulțirii. Înmulțirea matricelor în $\mathcal{M}_2(\mathbb{R})$ este asociativă și deci rămâne la fel pe o submulțime G a sa.

G_2) Comutativitatea înmulțirii. Fie $A_x, A_y\in G$. Atunci $A_x\cdot A_y=A_{x+y-2xy}=A_{y+x-2yx}=A_y\cdot A_x$, ceea ce arată că înmulțirea matricelor este comutativă pe G.

G_3) Element neutru. Există $A_e\in G$ astfel încât $A_x\cdot A_e=A_x, (\forall)A_x\in G$ sau $A_{x+e-2xe}=A_x$, $(\forall)A_x\in G$. Se vede că două matrice $A_x,\ A_y$ sunt egale $A_x=A_y \Leftrightarrow x=y$ (deci dacă indicii matricelor coincid). Din relația de mai sus deducem $x+e-2xe=x$, iar de aici $e=0$. Așadar elementul neutru este $A_0=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=I_2$.

G_4) Elemente simetrizabile. Fie $A_x\in G$. Să arătăm că există simetricul $A_{x'}\in G$ pentru care $A_x\cdot A_{x'}=A_0 \Leftrightarrow A_{x+x'-2xx'}=A_0$. De aici: $x+x'-2xx'=0$ și deci $x'=\frac{x}{2x-1}\neq\frac{1}{2},\ x\neq\frac{1}{2}$. Deci orice element $A_x\in G$ este inversabil (pentru că $A_0=I_2$) în raport cu operația de înmulțire obișnuită a matricelor. În final, $(G,\cdot)$ este grup abelian.

7. Fie matricea $A=\begin{pmatrix}0 & 1 & 0\\ 0 & 0 & -1\\ -1 & 0 & 0\end{pmatrix}$ și mulțimea $G=\{A^n \mid n\in\mathbb{N}^*\}$. Arătați că $(G,\cdot)$ este grup abelian.

R. Calculăm puterile lui A și găsim: $A^2=\begin{pmatrix}0 & 0 & -1\\ 1 & 0 & 0\\ 0 & -1 & 0\end{pmatrix}$ și $\boldsymbol{A^3=I_3}$.

Deci mulțimea G are doar trei elemente distincte $G=\{I_3, A, A^2\}$.

Tabla legii pe G, dată alăturat, arată că înmulțirea pe G este lege de compoziție. Întotdeauna înmulțirea matricelor pe $\mathcal{M}_3(\mathbb{R})$) este asociativă. Deci rămâne la fel și pe mulțimea $G\subset\mathcal{M}_3(\mathbb{R})$.

Elementul neutru este I_3. Orice element din G este inversabil în raport cu

$\cdot$	I_3	A	A^2
I_3	I_3	A	A^2
A	A	A^2	I_3
A^2	A^2	I_3	A

înmulțirea: $I_3^{-1} = I_3$, $A^{-1} = A^2, \left(A^2\right)^{-1} = A$. Tabla fiind simetrică în raport cu diagonala principală, grupul este abelian.

8. Se consideră sistemul de ecuații liniare $(S): \begin{cases} 2x - y + 3z = 0 \\ 3x + 4y - z = 0 \end{cases}$ şi $S = \{(a_1, a_2, a_3) | a_i \in \mathbb{Z}\}$ mulțimea soluțiilor întregi ale sistemului (S). Pe mulțimea S definim operația de adunare $(a_1, a_2, a_3) + (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3 + b_3)$. Arătați că $(S, +)$ este grup abelian.

R. Se rezolvă sistemul şi găsim soluțiile $S = \{(-\lambda, \lambda, \lambda) | \lambda \in \mathbb{Z}\}$.Mai întâi să observăm că adunarea pe S este lege de compoziție. Dacă $s_1 = (a_1, a_2, a_3)$, $s_2 = (b_1, b_2, b_3) \in S$, atunci $s_1 + s_2 \in S$. Se arată că $s_1 + s_2$ verifică fiecare ecuație. Pentru prima ecuație această verificare are loc $2(a_1 + b_1) - (a_2 + b_2) + 3(a_3 + b_3) = 0$ sau $(2a_1 - a_2 + 3a_3) + (2b_1 - b_2 + 3b_3) = 0$, adică 0 + 0 = 0. Asociativitatea adunării pe S se reduce în final la asociativitatea adunării pe $\mathbb{Z}$.

Elementul neutru este dat de soluția banală (0, 0, 0) cum uşor se verifică. Dacă $s = (a_1, a_2, a_3) \in S$, atunci $-s = (-a_1, -a_2, -a_3) \in S$, cum uşor se verifică.

Adunarea pe S fiind comutativă, grupul $(S, +)$ este abelian.

Grupuri remarcabile

1) Grupuri de matrice

Anul trecut am văzut că mulțimea matricelor de tip (m, n) cu elemente din $\mathbb{R}$, $\mathcal{M}_{m,n}(\mathbb{R})$, **cu operația de adunare formează grup abelian** $\left(A, B \in \mathcal{M}_{m,n}(\mathbb{R}) \Rightarrow A + B \in \mathcal{M}_{m,n}(\mathbb{R});\right.$ elementul neutru este $O_{m,n}$ – matricea nulă; $-A = \left(-a_{ij}\right)$ este opusul lui $\left.A = \left(a_{i,j}\right)\right)$.

Pentru $m = n$ are sens produsul oricăror matrice $A, B \in \mathcal{M}_n(\mathbb{R})$.

Fie mulțimea de matrice pătratice de ordin n cu elemente reale şi cu determinant nenul.

Vom nota această mulțime prin $GL(n, \mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) | \det(A) \neq 0\}$ şi considerăm **operația de înmulțire** pe $\mathcal{M}_n(\mathbb{R})$.

Are loc următoarea:

> **Teoremă**. Cuplul $(GL(n, \mathbb{R}), \cdot)$ este un grup infinit, numit **grupul liniar complet de ordin n pe $\mathbb{R}$**.

Demonstrație. Să observăm mai întâi că înmulțirea determină pe $GL(n, \mathbb{R})$ **o lege de compoziție**. Într-adevăr, din $A, B \in GL(n, \mathbb{R})$ să arătăm că $AB \in GL(n, \mathbb{R})$, adică să arătăm că $\det(AB) \neq 0$, ceea ce este adevărat deoarece $\det(AB) = \det(A) \cdot \det(B)$.

Verificăm axiomele grupului.

G_1) **Asociativitatea înmulțirii** are loc pe $GL(n,\mathbb{R})$, deoarece are loc întotdeauna pe $\mathcal{M}_n(\mathbb{R})$.

G_2) **Elementul neutru** este matricea unitate $I_n \in GL(n,\mathbb{R})$ (are $\det(I_n)=1\neq 0$).

G_3) **Orice matrice** $A\in GL(n,\mathbb{R})$ **are o inversă** (simetric) notată $A^{-1}\in GL(n,\mathbb{R})$ pentru care $AA^{-1}=A^{-1}A=I_n$.

Aici A^{-1} este chiar inversa matricei *A*. Ştim că *A* are inversă dacă $\det(A)\neq 0$ *(A* este o matrice nesingulară). Evident $A^{-1}\in GL(n,\mathbb{R})$ deoarece din $A\cdot A^{-1}=I_n$ şi $\det\left(A\cdot A^{-1}\right)=\det(A)\cdot\det\left(A^{-1}\right)=1$ rezultă $\det\left(A^{-1}\right)\neq 0$.

În final $\left(GL(n,\mathbb{R}),\cdot\right)$ este grup infinit.■

2) Grupuri de permutări de ordin *n*

Fie *M* mulțime finită cu *n* elemente. Natura acestor elemente fiind pentru noi fără importanță, este comod să luăm *M* = {1, 2, ... , *n*}.

Am văzut că $\mathcal{F}(M)=\{f:M\to M\}$ împreună cu operația de compunere a funcțiilor este un monoid. Considerăm o submulțime a lui $\mathcal{F}(M)$, $\mathcal{B}(M)$ formată din **aplicații bijective** (de fapt este destul să cerem ca *f* să fie injectivă (surjectivă) căci atunci *f* este bijectivă !).

Un element din $\mathcal{B}(M)$ îl numim **permutare de gradul** *n.*

Elementele lui $\mathcal{B}(M)$ le desemnăm prin litere mici ale alfabetului grec α, β, γ, δ,.... .

În loc de $\mathcal{B}(M)$ vom folosi notația S_n.

Sub o formă dezvoltată şi sugestivă permutarea $\sigma: M\to M$ o reprezentăm prin simbolul $\sigma=\begin{pmatrix}1 & 2 & \dots & n\\ \sigma(1) & \sigma(2) & \dots & \sigma(n)\end{pmatrix}\begin{matrix}\to \text{ domeniul de definiție}\\ \to \text{ mulțimea de valori.}\end{matrix}$

unde se indică **in extenso** toate imaginile:

$$\begin{matrix} & 1 & 2 & \dots & n\\ \sigma: & \downarrow & \downarrow & & \downarrow\\ & \sigma(1) & \sigma(2) & \dots & \sigma(n)\end{matrix}$$

$\sigma(k),\ k=\overline{1,n}$ sunt simbolurile 1,2, ... , *n,* eventual în altă ordine.

Pe mulțimea S_n a permutărilor de grad *n* am definit, anul precedent, operația de **compunere** (sau **produs**) a permutărilor.

Fie $\sigma,\tau\in S_n$, atunci $\sigma\circ\tau\in S_n$ se defineşte (compunerea obişnuită a funcțiilor) prin: $\sigma\circ\tau(k)=\sigma\left(\tau(k)\right),\ k=\overline{1,n}$

Vom scrie în loc de $\sigma \circ \tau$ simplu $\sigma\tau$. Are loc următoarea:

Teoremă. Cuplul $(S_n, \circ)$ este un grup finit de ordin $n!$, numit **grupul simetric de grad** n.

Demonstrație. Verificăm axiomele grupului.
Este clar că dacă $\sigma, \tau \in S_n$, atunci $\sigma\tau \in S_n$, adică **legea de compunere a permutărilor este o lege de compoziție pe** S_n.
Trebuie observat astfel **că se pot compune permutări de acelaşi grad**.
G₁) **Asociativitatea compunerii** pe S_n rezultă din faptul că această lege este asociativă pe mulțimea funcțiilor $\mathcal{F}(M)$.
G₂) **Elementul neutru** este aplicația identică a mulțimii M, pe care o notam cu e şi are forma: $e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$.

G₃) **Orice element** $\sigma \in S_n$, are un **invers** (simetric) notat $\sigma^{-1} \in S_n$ (σ^{-1} este aplicația inversă a lui σ) pentru care $\sigma\sigma^{-1} = \sigma^{-1}\sigma = e$.
De exemplu, dacă $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$, atunci $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$ (σ^{-1} este funcția care „acționează“ invers decât σ; prin σ, 1 este dus în 3; invers, prin σ^{-1} elementul 3 este dus în 1 etc.). Dacă $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, atunci $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ şi $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Deci $\sigma\tau \neq \tau\sigma$.
Aşadar $(S_n, \circ)$, $n \geq 3$, este grup necomutativ.
Să determinăm ordinul grupului. Fie $\sigma \in S_n$ un element oarecare din grup. Prin σ elementul 1 este dus în $\sigma(1)$ care poate fi oricare din elementele 1,2, ... , n. Deci poziția $\sigma(1)$ se poate completa în n moduri. Elementul $\sigma(2)$ se poate completa în (n – 1) moduri cu cele n – 1 elemente rămase după completarea lui $\sigma(1)$. În fine ultima poziție se poate completa într-un singur mod cu ultimul element rămas după completarea pozițiilor $\sigma(1), \sigma(2), \dots, \sigma(n-1)$. Aşadar numărul de astfel de permutări σ este egal cu $n \cdot (n-1) \dots 2 \cdot 1 = n!$ (regula produsului de la combinatorică) şi acesta este ordinul grupului S_n. ■
Grupurile de permutări joacă un rol fundamental în studiul grupurilor (vezi *Excursie matematică* de la sfârşitul acestui capitol).

3) Grupul claselor de resturi modulo *n*, $\mathbb{Z}_n$

Fie $\mathbb{Z}$ mulțimea numerelor întregi şi $n \in \mathbb{N}^*$ un număr fixat. Pe mulțimea $\mathbb{Z}$ definim următoarea relație: pentru $x, y \in \mathbb{Z}$ spunem că *x* **este congruent cu** *y* **modulo** *n* dacă şi numai dacă $x - y$ se divide prin *n.*
Această relație se notează prin: $x \equiv y \pmod{n} \Leftrightarrow x - y \,\vdots\, n$. (citim: $x - y$ se divide prin *n*).
Faptul că $x - y \,\vdots\, n$ este echivalent cu *x, y* dau acelaşi rest la împărțirea prin *n* (demonstrați !).
Relația de congruență pe $\mathbb{Z}$ are următoarele proprietăți:
1) $\equiv$ este **reflexivă**, adică $x \equiv x \pmod{n}$, $(\forall) x \in \mathbb{Z}$, deoarece $x - x = 0 \,\vdots\, n$.
2) $\equiv$ este **simetrică**, adică dacă $x \equiv y \pmod{n} \Rightarrow y \equiv x \pmod{n}$, ceea ce este imediat deoarece dacă $x - y \,\vdots\, n$, atunci şi $y - x = -(x - y) \,\vdots\, n$.
3) $\equiv$ este **tranzitivă**, adică dacă $x \equiv y \pmod{n}$ şi $y \equiv z \pmod{n}$, atunci $x \equiv z \pmod{n}$, ceea ce se verifică uşor deoarece din $x - y \,\vdots\, n$ şi $y - z \,\vdots\, n$ rezultă $x - z = (x - y) + (y - z) \,\vdots\, n$.
Relația $\equiv$ (de congruență modulo *n)* cu proprietățile 1), 2), 3) este o **relație de echivalență.**
Două numere întregi *x, y* pentru care $x \equiv y \pmod{n}$ spunem că sunt **echivalente** în raport cu relația $\equiv$.

Clase de echivalență şi mulțime cât

Pentru un număr întreg $x \in \mathbb{Z}$ definim **clasa sa de echivalență** în raport cu $\equiv$ mulțimea notată *C*(*x*) (sau $\hat{x}$) a tuturor numerelor întregi echivalente cu *x* față de relația $\equiv$. Aşadar $C(x) = \hat{x} = \left\{ y \in \mathbb{Z} \,\middle|\, y \equiv x \pmod{n} \right\}$.

Proprietăți ale claselor de echivalență

1) Dacă $x, y \in C(a)$, atunci $x \equiv y \pmod{n}$ (**două elemente aparținând aceleiaşi clase de echivalență sunt echivalente între ele**). Într-adevăr dacă $x \in C(a) \Rightarrow x \equiv a \pmod{n}$ şi dacă $y \in C(a) \Rightarrow y \equiv a \pmod{n}$.
Din $x \equiv a \pmod{n}$ şi $a \equiv y \pmod{n} \Rightarrow x \equiv y \pmod{n}$ (am aplicat tranzitivitatea relației $\equiv$).
2) Dacă $x \equiv y \pmod{n} \Rightarrow \hat{x} = \hat{y}$ (sau *C*(*x*) = *C*(*y*), adică **clasele de echivalență a două elemente echivalente coincid** – pentru demonstrație utilizați dubla incluziune $\hat{x} \subset \hat{y}$, $\hat{y} \subset \hat{x}$).
3) $\hat{x} \cap \hat{y} \neq \varnothing \Rightarrow \hat{x} = \hat{y}$ (**Două clase de echivalență, care au cel puțin un element în comun sunt egale**).

Într-adevăr dacă $a \in \hat{x} \cap \hat{y}$, atunci $a \in \hat{x}$ şi $a \in \hat{y}$. De aici $a \equiv x \pmod{n}$ şi $a \equiv y \pmod{n}$, adică $x \equiv y \pmod{n}$. Conform cu 2) $\Rightarrow \hat{x} = \hat{y}$.

Această relaţie de echivalenţă pe $\mathbb{Z}$, determină o partiţie a sa în sensul care urmează: **$\mathbb{Z}$ se scrie ca o reuniune de submulţimi nevide ale sale, disjuncte de două câte două.**

Mai precis, mulţimea claselor de echivalenţă determinate de relaţia de congruenţă modulo n pe $\mathbb{Z}$ se numeşte **mulţime cât** a lui $\mathbb{Z}$ în raport cu $\equiv$, şi se notează cu $\mathbb{Z}/\equiv$ sau încă $\mathbb{Z}_n$.

Dacă $x \in \mathbb{Z}$, atunci din teorema împărţirii pe $\mathbb{Z}$, $(\exists) k, r \in \mathbb{Z}, 0 \le r < n$ astfel încât $x = nk + r$, relaţie pe care o mai scriem sub forma $x - r = nk$. Deci $x - r \,\vdots\, n$ adică $x \equiv r \pmod{n}$ şi deci $\hat{x} = \hat{r}$, unde $r \in \{0, 1, ..., n-1\}$.

Să reţinem deci: clasa oricărui $x \in \mathbb{Z}$ este de fapt una din clasele $\hat{r}$, $r = 0, 1, .., n-1$.

Prin urmare relaţia de congruenţă modulo n pe $\mathbb{Z}$ determină mulţimea cât $\mathbb{Z}_n = \{\hat{0}, \hat{1}, ..., \widehat{n-1}\}$ numită **mulţimea claselor de resturi modulo** n (denumire justificată de faptul că numerele 0, 1, …, n – 1 reprezintă resturile la împărţire prin n a numerelor întregi). Scrise explicit acestea sunt:

$$\hat{0} = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{n}\} = \{nh \mid h \in \mathbb{Z}\} \overset{\text{notaţie}}{=} n\mathbb{Z}$$

$$\hat{1} = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{n}\} = \{nh + 1 \mid h \in \mathbb{Z}\} = n\mathbb{Z} + 1,$$

…………………………………………………

$$\widehat{n-1} = \{x \in \mathbb{Z} \mid x \equiv n-1 \pmod{n}\} = \{nh + n - 1 \mid h \in \mathbb{Z}\} = n\mathbb{Z} + n - 1.$$

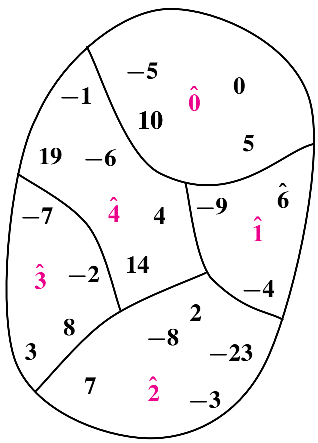
Numerele 0, 1, ..., n – 1 prin care am definit clasele $\hat{0}, \hat{1}, ..., \widehat{n-1}$ se vor numi **reprezentanţii canonici** ai acestor clase.

Pentru $\mathbb{Z}$ avem partiţia dată de $\mathbb{Z}_n$.

$\mathbb{Z} = \hat{0} \cup \hat{1} \cup ... \cup \widehat{n-1}$ şi evident (de mai sus) $\hat{i} \cap \hat{j} = \varnothing$ dacă $i \neq j$.

Pentru n = 5, $\mathbb{Z} = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}\}$, dacă dorim să vedem cărei clase îi aparţine un număr întreg $x \in \mathbb{Z}$ se efectuează împărţirea lui x prin 5 şi se ia restul acestei împărţiri r. Atunci $x \in \hat{r}$. În Fig. 2 pentru fiecare clasă sunt date câteva elemente.

De exemplu x = 19 pentru care avem: $19 = 5 \cdot 3 + 4$ şi deci r = 4. Prin urmare $19 \in \hat{4}$. Analog dacă x = –23, atunci $-23 = 5(-5) + 2$ şi deci $-23 \in \hat{2}$.



$n = 5, \mathbb{Z} = \hat{0} \cup \hat{1} \cup \hat{2} \cup \hat{3} \cup \hat{4}$

Fig. 2

Observație. Să fim atenți la scrierea claselor modulo n. De exemplu, $\hat{0}\in\mathbb{Z}_3$, $\hat{0}\in\mathbb{Z}_5$ **nu reprezintă aceeaşi mulțime** (descrieți-le). Pentru a ne feri de confuzii se poate scrie $\hat{0}_3\in\mathbb{Z}_3$ şi $\hat{0}_5\in\mathbb{Z}_5$, sau $\mathbb{Z}_3=\{\hat{0},\hat{1},\hat{2}\}$, iar $\mathbb{Z}_5=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\}$. O scriere superficială poate conduce **greşit** la $\mathbb{Z}_3\subset\mathbb{Z}_5$!

Pe mulțimea $\mathbb{Z}_n$ a claselor de resturi modulo n definim două operații:

$+:\mathbb{Z}_n\times\mathbb{Z}_n\to\mathbb{Z}_n$

$\left(\hat{a},\hat{b}\right)\to\hat{a}+\hat{b}=\widehat{a+b}$, numită **adunarea claselor** (suma claselor este clasa sumei). Clasa $\widehat{a+b}$ se obține adunând a cu b şi luând apoi clasa restului de la împărțirea lui $a+b$ prin n.

şi

$\cdot:\mathbb{Z}_n\times\mathbb{Z}_n\to\mathbb{Z}_n$

$\left(\hat{a},\hat{b}\right)\to\hat{a}\cdot\hat{b}=\widehat{a\cdot b}$, numită **produsul claselor** (produsul claselor este prin definiție clasa produsului).

Clasa $\widehat{a\cdot b}$ se obține înmulțind a cu b şi luând apoi clasa restului de la împărțirea lui $a\cdot b$ prin n.

Trebuie să arătăm că aplicațiile „+“ şi „·“ sunt corect definite, în sensul că fiecărui cuplu $\left(\hat{a},\hat{b}\right)\in\mathbb{Z}_n\times\mathbb{Z}_n$ îi corespunde un unic element $\widehat{a+b}\in\mathbb{Z}_n$, şi respectiv $\widehat{a\cdot b}\in\mathbb{Z}_n$.

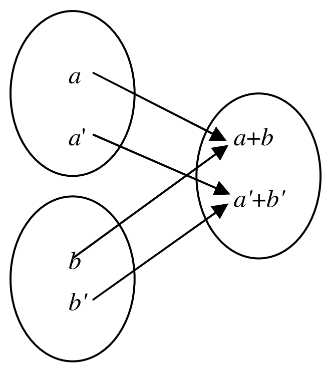
Fie: $\hat{a}=\hat{a}'$ şi $\hat{b}=\hat{b}'$ (Fig. 3). Atunci $\hat{a}+\hat{b}=\hat{a}'+\hat{b}'$, deoarece

din $\hat{a}=\hat{a}'\Rightarrow a\equiv a'(\bmod n)\Rightarrow\ a-a'\,\vdots\,n$, (1)

şi din $\hat{b}=\hat{b}'\Rightarrow b\equiv b'(\bmod n)\Rightarrow b-b'\,\vdots\,n$, (2).

Acum, adunând (1) cu (2) rezultă $a+b-(a'+b')\,\vdots\,n$, adică $\widehat{a+b}=\widehat{a'+b'}$.

Analog se arată că înmulțirea claselor este bine definită.



Contururile închise=clase de resturi

Fig. 3

Pentru $n = 6$ tablele operațiilor de adunare şi înmulțire sunt

$+$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{0}$	$\hat{1}$
$\hat{3}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{4}$	$\hat{4}$	$\hat{5}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{5}$	$\hat{5}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$

$\cdot$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{2}$	$\hat{0}$	$\hat{2}$	$\hat{4}$	$\hat{0}$	$\hat{2}$	$\hat{4}$
$\hat{3}$	$\hat{0}$	$\hat{3}$	$\hat{0}$	$\hat{3}$	$\hat{0}$	$\hat{3}$
$\hat{4}$	$\hat{0}$	$\hat{4}$	$\hat{2}$	$\hat{0}$	$\hat{4}$	$\hat{2}$
$\hat{5}$	$\hat{0}$	$\hat{5}$	$\hat{4}$	$\hat{3}$	$\hat{2}$	$\hat{1}$

Are loc următoarea:

Teoremă. a) $(\mathbb{Z}_n, +)$ este un grup abelian, numit **grupul aditiv al claselor de resturi modulo** *n*.
b) $(\mathbb{Z}_n, \cdot)$ este un monoid comutativ, în care grupul elementelor inversabile este $U(\mathbb{Z}_n) = \{\hat{k} \in \mathbb{Z}_n \mid (k,n) = 1\}$.

Demonstrație. a) Se verifică axiomele grupului abelian.

G$_1$) **Asociativitatea adunării**. Avem: $\hat{x} + (\hat{y} + \hat{z}) = \hat{x} + \widehat{y+z} = \widehat{x+(y+z)} = \widehat{(x+y)+z} =$
$= \widehat{x+y} + \hat{z} = (\hat{x} + \hat{y}) + \hat{z},\ (\forall)\hat{x}, \hat{y}, z \in \mathbb{Z}_n$.
(am ținut seama în a treia egalitate de asociativitatea adunării pe $\mathbb{Z}$).

G$_2$) **Elementul neutru**. Clasa $\hat{0} \in \mathbb{Z}_n$ este elementul neutru în raport cu adunarea deoarece $\hat{x} + \hat{0} = \hat{0} + \hat{x} = \hat{x},\ (\forall)\hat{x} \in \mathbb{Z}_n$.

G$_3$) **Elemente opuse**. Orice clasă $\hat{x} \in \mathbb{Z}_n$ are ca element simetric (opus) clasa notată $-\hat{x} = \widehat{-x}$ deoarece $x + \left(\widehat{-x}\right) = \widehat{-x} + \hat{x} = \widehat{x+(-x)} = \hat{0}$.

Mai precis avem: $-\hat{0} = \hat{0}$

$$-\hat{1} = \widehat{n-1} \quad (\widehat{n-1} + \hat{1} = \widehat{n-1+1} = \hat{0})$$
$$-\hat{2} = \widehat{n-2}$$
$$\vdots$$
$$-\hat{k} = \widehat{n-k}$$
$$\vdots$$
$$-(\widehat{n-1}) = \hat{1}.$$

G_4) **Comutativitatea adunării**. Adunarea claselor este comutativă deoarece $(\forall)\hat{x},\hat{y}\in\mathbb{Z}_n$ avem: $\hat{x}+\hat{y}=\widehat{x+y}=\widehat{y+x}=\hat{y}+\hat{x}$ (am folosit în a doua egalitate comutativitatea adunării pe Z).
Cu acestea am arătat că $(\mathbb{Z}_n,+)$ este grup abelian.

b) Asemănător se verifică asociativitatea, comutativitatea înmulțirii claselor. Clasa $\hat{1}\in\mathbb{Z}_n$ este elementul neutru.

Se arată uşor că $\left(U(\mathbb{Z}_n),\cdot\right)$ este un grup abelian.

Să găsim acum elementele inversabile din acest monoid. Mai precis arătăm că avem: $\hat{k}\in U(\mathbb{Z}_n)\Leftrightarrow(k,n)=1$.

Pentru n = 1 avem $\mathbb{Z}_1=\{\hat{0}\}=U(\mathbb{Z}_1)$, când (0,1) = 1 şi echivalența are loc.
Fie acum $n\geq 2$.

Demonstrăm implicația „$\Rightarrow$“. Presupunem $\hat{k}\in U(\mathbb{Z}_n)$ şi să arătăm că avem $(k, n) = 1$.

Din $\hat{k}\in U(\mathbb{Z}_n)\Rightarrow(\exists)\hat{p}\in\mathbb{Z}_n$ astfel încât $\hat{k}\cdot\hat{p}=\hat{1}\Leftrightarrow\widehat{kp}=\hat{1}\Leftrightarrow kp\equiv 1(\operatorname{mod} n)\Leftrightarrow$
$\Leftrightarrow kp-1\,\vdots\, n\Leftrightarrow kp-1=nq,\ q\in\mathbb{Z}$. Fie acum $d=(k,n)\in N^*$. Deci $d\,|\,kp-nq$, adică $d\,|\,1\Rightarrow d=1$. Aşadar $(k, n) = 1$.

Demonstrăm acum că dacă $(k, n) = 1$, atunci $\hat{k}\in U(\mathbb{Z}_n)$.
Se ştie că dacă $(k, n) = 1$, atunci există $p,q\in\mathbb{Z}$ astfel încât $kp+nq=1$ sau $kp-1=nq\Rightarrow kp-1\,\vdots\, n$, adică $kp\equiv 1(\operatorname{mod} n)$ sau în final $\widehat{kp}=\hat{k}\cdot\hat{p}=\hat{1}$, arată că avem $\hat{k}\in U(\mathbb{Z}_n)$.■

Observații. 1) Grupul $U(\mathbb{Z}_n)$ are ordinul $\varphi(n)$ = numărul numerelor naturale cel mult egale cu *n,* relativ prime cu *n.*

Funcția $\varphi:\mathbb{N}^*\to\mathbb{N}^*,\ n\to\varphi(n)$ se numeşte **indicatorul lui Euler**.

Dacă $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$, atunci

$$\varphi(n)=p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\cdot\ldots\cdot p_k^{\alpha_k-1}(p_k-1)$$

Dacă $n=p, p$ prim, atunci $\varphi(p)=p-1$. Se arată că $\sum\limits_{d|n}\varphi(d)=n$.

Pentru n = 6, avem $\varphi(6)=2$ când $U(\mathbb{Z}_6)=\{\hat{1},\hat{5}\}$.

2) Din tablele celor două legi, în cazul n = 6, se constată că acestea sunt simetrice în raport cu diagonala principală. Deci legile sunt comutative.
Din tabla înmulțirii se vede că doar pe liniile claselor $\hat{1}$ şi $\hat{5}$ apare elementul $\hat{1}$, ceea ce înseamnă că doar aceste clase au inverse.

Citind pe coloanele care-l conțin pe $\hat{1}$ găsim inversele: $\hat{1}^{-1} = \hat{1}, \hat{5}^{-1} = \hat{5}$.

3) Pe $\mathbb{Z}_n$ nu există relație de ordine similară relației $\leq$ de pe $\mathbb{Z}$.

Am identificat elementele lui $\mathbb{Z}$ cu punctele întregi de pe dreapta reală care se extind infinit la stânga şi la dreapta (Fig. 4).

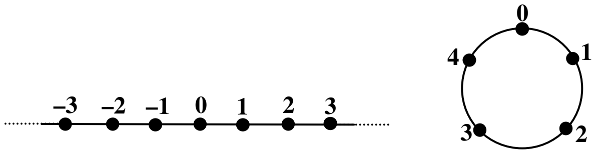


Fig. 4

Pe $\mathbb{Z}_n$ avem în schimb un fel de **ordine ciclică**, reprezentată printr-o mulțime de puncte de pe cerc cu o anumită regularitate. Din acest motiv aritmetică pe $\mathbb{Z}_n$ se mai numeşte **aritmetică modulară** sau **aritmetica cercului.**

Excursie matematică (facultativ)

* * * * *

1. Scurtă prezentare a teoriei codurilor

În manualele de clasa a XI-a am prezentat două aplicații legate de acest subiect:
1) codul de bare aplicat pe diferite produse şi 2) codul ISBN asociat unei cărți (din 2006 s-a trecut de la codul de 10 cifre la cel de 13 cifre – ca urmare a unificării celor două asociații UCC (din Canada şi S.U.A.) şi A.E.N. (din restul țărilor)).
S-a văzut că în ambele aplicații intervine noțiunea de congruență.
Orice informație transmisă prin diferite canale (sateliți etc.) şi stocată în calculator (pe CD etc.) este exprimată într-un anume cod. Ca urmare a unor factori diferiți (umani, echipamente etc.) mesajele recepționate pot conține erori la recepție. Detectarea şi corectarea erorilor reprezintă scopurile fundamentale ale teoriei codurilor.
*În teoria codurilor binare, elementele sunt din $\mathbb{Z}_2$, pe care le notăm simplu 0, 1. Mulțimea {0, 1} o numim **alfabet binar**. Un **bit** este un element al alfabetului binar, iar un **cuvânt** (sau **bloc**) este un şir de biți, unde toate cuvintele din mesaj au **aceeaşi lungime** (= numărul de biți).*
Un cuvânt de 2 biți este un element din $\mathbb{Z}_2 \times \mathbb{Z}_2$ pe care îl reprezentăm sub forma ab şi nu (a,b), cu $a,b \in \{0,1\}$. Analog, pentru cuvinte de 3 biți,4 biți etc.

Cuvintele din trei biți sunt $(2^3 = 8)$.

000 010 001 011

100 110 101 111.

Aşa cum am spus, în timpul transmiterii unui mesaj conținând cuvinte de k biți, unul sau mai mulți biți se pot recepționa incorect. Este important ca erorile să fie detectate şi pe cât posibil corijate.

Schema generală de transmitere a unui mesaj codificat este:

mesaj $\xrightarrow{\text{codificare}}$ **mesaj codificat** $\xrightarrow[\text{mesaj}]{\text{transmitere}}$ **mesaj recepționat** $\xrightarrow{\text{decodificare}}$ **mesaj final**

Cele mai multe coduri necesită adăugarea unor biți la fiecare cuvânt din k biți obținându-se cuvinte de n biți.

***Exemplu** (**controlul parității**). Fie un cuvânt din 3 biți, abc. Schema de codificare duce cuvântul abc în abcd, unde* $d \equiv a + b + c \pmod 2$.

Dacă d = 0, cuvântul abc este par, iar dacă d =1, cuvântul abc este impar.

cuvânt	*codificare* $d \equiv a+b+c \pmod 2$	*cuvânt codificat*
000	*0*	*0000*
010	*1*	*0101*
001	*1*	*0011*
011	*0*	*0110*
100	*1*	*1001*
110	*0*	*1100*
101	*0*	*1010*
111	*1*	*1111*

Evident, fiecare cuvânt de 4 biți este par. În felul acesta verificarea parității pe cuvântul codificat detectează numai eroare de un bit.

De exemplu dacă s-a primit mesajul:

1011 1010 1101

atunci primul şi ultimul cuvânt conțin cel puțin o eroare, dar nu ştim unde. Pentru clarificare se solicită retransmiterea masajului.

Erorile multiple pot fi detectate, dar nu corectate utilizând schema:

$a_1 a_2 \ldots a_k \xrightarrow{\text{codificare}} a_1 a_2 \ldots a_k a_1 a_2 \ldots a_k$ *în care un cuvânt de k biți este aplicat în unul de 2k biți.*

De exemplu, dacă pentru k = 3, se obține mesajul:

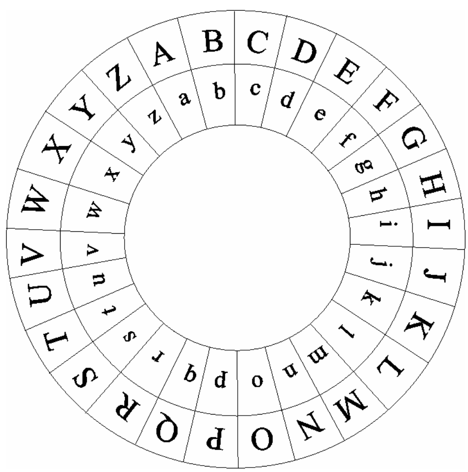
101101 100101 110111 001001,

Atunci în cuvintele al doilea şi al treilea avem erori.

Dacă la o nouă retransmitere avem mesajul:

101 101 100 100 110 110 001 001,

atunci după decodificare se obține:
101 100 110 001.
Acest ultim exemplu ne sugerează întrebarea: care este probabilitatea ca o eroare să se producă în unul sau mai mulți biți al unui cuvânt de n biți?
Se admite că: 1) probabilitatea ca un singur bit să fie transmis incorect este p şi 2) probabilitatea ca un singur bit să fie transmis incorect sau corect este independentă de probabilitatea ca un alt bit să fie transmis incorect sau corect.
Cu aceste observații suntem în cazul schemei lui Bernoulli. Deci probabilitatea ca un singur bit să fie transmis incorect este $C_n^1 p(1-p)^{n-1}$.
În cele de mai jos vom considera şi alte congruențe diferite de 2 (cu elemente din $\mathbb{Z}_n$, $n \neq 2$ *).*
Multe companii utilizează ***cifra de control*** *pentru securitatea informațiilor sau detectarea erorilor. De exemplu, a şasea cifră se adaugă la numărul de identificare format din cinci cifre şi se obține un număr de şase cifre de forma:*
$a_1a_2a_3a_4a_5c$ *unde c se calculează după formula:* $a_1a_2a_3a_4a_5 \equiv c \pmod{n}$.
Dacă utilizăm congruența modulo 7, atunci pentru numărul de identificare 21346, cifra de control este 3, deoarece $21346 \equiv 3 \pmod{7}$. *Deci numărul complet este 213463. Dacă în loc de numărul 21346 s-ar fi transmis 22346, atunci apare detectată o eroare de transmitere, deoarece* $22346 \not\equiv 3 \pmod{7}$ *(* $22346 \equiv 2 \pmod{7}$ *).*
Pentru determinarea cifrei de control se utilizează scheme mai complicate (aşa cum am văzut, anul trecut, la codul de bare al produselor, numărul paşaportului, codul de identificare de pe cartea de identitate a unei persoane).
Astfel, numărul asociat unui articol $x_1x_2...x_n$ *se scrie sub formă de vector* $(x_1, x_2, ..., x_n)$ *şi se înmulțeşte scalar cu un vector,* ***numit vector de ponderi*** $(y_1, y_2, ..., y_n)$, *iar rezultatul se ia modulo un număr p dat. Aceasta este cifra de control, care se adaugă articolului. Deci,* $x_1y_1 + x_2y_2 + ... + x_ny_n \equiv c \pmod{p}$.
De exemplu, numerele de identificare pentru anumite bănci au opt cifre $x_1, x_2, ..., x_8$, *iar a noua cifră* x_9 *(cifra de control) este definită prin*
$(x_1, x_2, ..., x_8) \cdot (7,3,9,7,3,9,7,3) \equiv x_9 \pmod{10}$.
În acest caz, vectorul de ponderi este: (7, 3, 9, 7, 3 ,9, 7, 3).



2. Congruența şi criptografia

Am prezentat, anul trecut, o scurtă introducere în criptografie (se ocupă cu studiul tehnicilor utilizate pentru a codifica un text inteligibil). Am prezentat atunci două tehnici de codificare a mesajelor: cifrul lui Iuliu Caesar (care *consta într-o decalare a alfabetului cu trei poziții) şi pătratul lui Polybe (fiecărei litere i se asocia un număr de două cifre). Vom aborda aceste probleme într-un cadru mai general, utilizând congruența modulo n. Criptografia este diferită de teoria codurilor. Ultima se ocupă de detectarea şi corectarea erorilor din mesaje, în timp ce prima studiază proiectarea codurilor secrete (de ascundere a mesajelor față de persoanele neautorizate). Cifrul lui Caesar este reprezentat prin două inele concentrice, fiecare din ele conținând întreg alfabetul (figura alăturată). Inelul interior, reprezintă textul inteligibil (clar), este fixat. Cel exterior, reprezintă, textul cifrat, este mobil. Cele două inele formează* ***roata cifrului***. *O pereche de litere (text clar/text cifrat) determina toată schema de decriptare. Aceasta este cheia de decodificare a oricărui mesaj. De exemplu (a, D)*

Descrierea matematică a cifrului traducere. *Asociem celor n litere ale alfabetului întregii 0, 1, …, n – 1. Notăm cu* $A = \{0,1,...,n-1\}$ *şi considerăm funcția* $f : A \to A,\ f(x) = x + k\left(\bmod n\right)$, *unde k este* ***cheia*** *numărului de poziție de la alfabetul clar la alfabetul cifrat. Pe lângă literele alfabetului de la a la z se adaugă şi blankul (=spațiul liber). Deci:*

Alfabetul:	*a*	*b*	*c*	*d*	*…*	*x*	*y*	*z*	*„blank“*
A:	*0*	*1*	*2*	*3*	*…*	*23*	*24*	*25*	*26*

Pentru k = 5, text clar „atac în zori“ se transformă în text cifrat: FYFHENSEDTWN astfel:

atac în zori $\xrightarrow[\text{în A}]{\text{Se traduce}}$ *0 19 0 2 26 8 13 26 25 14 17 8*

$\xrightarrow{f(x) = x + 5 (\bmod 27)}$ *5 24 5 7 4 13 18 4 3 19 22 13*

$\xrightarrow[\text{din A}]{\text{Se traduce}}$ *F Y F H E N S E D T W N*

Aplicația $f : A \to A,\ f(x) = x + k\left(\bmod n\right)$ *este bijectivă şi inversa ei este* $f^{-1} : A \to A,\ \ f^{-1}(x) = x - k\left(\bmod n\right)$. *Aplicația inversă se utilizează pentru a descifra textul cifrat.*

FYFHENSEDTWN													
	$\xrightarrow[\text{în A}]{\text{se traduce}}$	*5*	*24*	*5*	*7*	*4*	*13*	*18*	*4*	*3*	*19*	*22*	*13*
	$f(x) = x - 5(\bmod 27)$	*0*	*19*	*0*	*2*	*26*	*8*	*13*	*26*	*25*	*14*	*17*	*8*
	$\xrightarrow[\text{din A}]{\text{se traduce}}$	*a*	*t*	*a*	*c*		*i*	*n*		*z*	*o*	*r*	*i*

Mai general se poate considera funcția $f : A \to A,\ f(x) = ax + b\left(\bmod n\right)$, *unde a,b sunt întregi fixați (funcția afină). Perechea ordonată (a,b) este* ***cheia acestui cifru.***

*Dacă a = 1, avem **cifru translație**, iar dacă b = 0 se obține **cifru multiplicativ.** Funcția f are inversa* $f^{-1}: A \to A$, *dacă* $(a,n)=1$, *când* $f^{-1}(x) = a'x + b' (\operatorname{mod} n)$, *unde* $aa' \equiv 1 (\operatorname{mod} n)$ *cu* $0 < a' < n$ *şi* $b' \equiv -a'b (\operatorname{mod} n)$.

3. Pătratele latine şi congruența

*Prin **pătrat latin de ordin** n se înțelege un tabel pătratic* $n \times n$, *în care fiecare din cele n simboluri apare o dată în fiecare linie şi odată în fiecare coloană.*
De exemplu, în agricultură se testează 5 tipuri de îngrăşăminte pe un teren în formă pătratică. Se împarte acest pătrat în 25 pătrățele mai mici (un pătrat cu 5 linii şi 5 coloane). Se doreşte, pentru a evidenția mai bine eficiența îngrăşămintelor, ca pe fiecare coloană şi pe fiecare linie un îngrăşământ să apară o singură dată după schema (A, B, C, D, E sunt tipurile de îngrăşământ).
Observăm că acesta este un pătrat latin de ordin 5.

A	*B*	*C*	*D*	*E*
B	*C*	*A*	*E*	*D*
C	*D*	*E*	*A*	*B*
D	*E*	*B*	*C*	*A*
E	*A*	*D*	*B*	*C*

Fie L pătratul latin. Atunci $L(i,j)$ *reprezintă elementul de pe linia i şi coloana j. În cele ce urmează,* $i, j, L(i,j) \in \mathbb{Z}_n$.
Se stabileşte uşor că $\forall n \geq 2$ *pătratul* $n \times n$, *definit prin* $L(i,j) = i + j,\ i, j \in \mathbb{Z}_n$, *este un pătrat latin. Altfel spus, tabla operației de adunare pentru* $\mathbb{Z}_n$ *este un pătrat latin. Rezultatul arată că există întotdeauna cel puțin un pătrat latin de orice ordin. Se pot obține pătrate latine prin încercări.*
O problemă mai dificilă este de a găsi perechi de pătrate latine de acelaşi ordin, care sunt, într-un anume sens, cât mai diferite posibil.
Spunem că două pătrate latine L_1, L_2 ***de acelaşi ordin sunt ortogonale** dacă pentru orice pereche ordonată de simboluri* (k, k') *există o singură poziție* (i,j) *pentru care* $L_1(i,j) = k$ *şi* $L_2(i,j) = k'$.
De exemplu, pătratele de mai jos:

A	*B*	*C*	*D*
B	*A*	*D*	*C*
C	*D*	*A*	*B*
D	*C*	*B*	*A*

A	*B*	*C*	*D*
C	*D*	*A*	*B*
D	*C*	*B*	*A*
B	*A*	*D*	*C*

sunt ortogonale deoarece fiecare din cele 16 perechi $(A,A), (A,B), \ldots (D,D)$ *se realizează în una din cele 16 poziții.*

* * * * *

Probleme rezolvate

1. Să se rezolve în $\mathbb{Z}_7$ sistemele

a) $\begin{cases} \hat{4}x + \hat{6}y = \hat{5} \\ \hat{3}x + \hat{2}y = \hat{4} \end{cases}$ b) $\begin{cases} \hat{3}x + y = \hat{1} \\ \hat{2}x + \hat{3}y = \hat{6} \end{cases}$

şi în $\mathbb{Z}_5$ sistemele:

c) $\begin{cases} x + y + z = \hat{1} \\ \hat{2}x + \hat{3}y + z = \hat{1} \\ \hat{4}x + \hat{4}y + \hat{3}z = \hat{1} \end{cases}$ d) $\begin{cases} x + y + z = \hat{0} \\ x^2 + y^2 + z^2 = \hat{1} \\ x^3 + y^3 + z^3 = \hat{1}. \end{cases}$

R. Rezolvarea sistemelor în clase de resturi $\mathbb{Z}_n$ de regulă, utilizează aceleaşi metode de rezolvare cunoscute de pe $\mathbb{C}$ (reducerii, substituției, Cramer etc.) dar ținând seamă de operațiile permise pe $\mathbb{Z}_n$ (de pildă regula lui Cramer se scrie $x = \Delta_x \cdot \Delta^{-1}$, $y = \Delta_y \cdot \Delta^{-1}$,... unde $\Delta =$ determinantul sistemului trebuie să fie element invers abil în $\mathbb{Z}_n$ în raport cu înmulțirea).

a) Dacă adunăm ecuațiile, membru cu membru, rezultă $y = \hat{2}$ (s-a redus *x*). Din prima ecuație $x = \hat{0}$. Deci soluția este $(\hat{0}, \hat{2})$.

b) Se poate utiliza metoda substituției scriind sistemul succesiv

$$\begin{cases} y = \hat{1} + \hat{4}x \\ \hat{2}x + \hat{3}(1 + \hat{4}x) = \hat{6} \end{cases} \text{ sau } \begin{cases} y = \hat{1} + \hat{4}x \\ \hat{0} \cdot x = \hat{3} \end{cases}$$

Ori ultima ecuație este imposibilă. Prin urmare sistemul dat este imposibil.

Altfel. Se înmulţeşte prima ecuație cu $\hat{3}$ şi din membrii drepți ai celor două ecuații rezultă $\hat{3} = \hat{6}$, fals.

c) Determinantul sistemului este $\Delta = \begin{vmatrix} \hat{1} & \hat{1} & \hat{1} \\ \hat{2} & \hat{3} & \hat{1} \\ \hat{4} & \hat{4} & \hat{3} \end{vmatrix} = \hat{4}$ (se pot aplica proprietățile determinanților, dar ținând seama de operațiile pe $\mathbb{Z}_5$). Să observăm că $\Delta = \hat{4}$ este inversabil în $\mathbb{Z}_5$ $((4,5) = 1)$ şi $\hat{4}^{-1} = \hat{4}$. Deci se poate aplica regula lui Cramer în rezolvare. Găsim $\Delta_x = \hat{4}, \Delta_y = \hat{3}, \Delta_z = \hat{2}$, când $x = \Delta_x \cdot \Delta^{-1} = \hat{4} \cdot \hat{4} = \hat{1}$, $y = \Delta_y \cdot \Delta^{-1} = \hat{3} \cdot \hat{4} = \hat{2}$, $z = \Delta_z \cdot \Delta^{-1} = \hat{2} \cdot \hat{4} = \hat{3}$. Aşadar $(\hat{1}, \hat{2}, \hat{3})$ este soluția sistemului.

d) Observăm că sistemul este simetric în *x, y, z.*

Vom rezolva sistemul utilizând ecuația de gradul trei.

Notăm $S_1 = x + y + z = \hat{0}$, $S_2 = xy + xz + yz$, $S_3 = xyz$. Se ridică prima ecuație la pătrat şi rezultă $x^2 + y^2 + z^2 + \hat{2}(xy + yz + xz) = \hat{0}$. Aici ținând seama de ecuația a doua găsim $\hat{2}(xy + yz + xz) = \hat{4}$ şi deci $xy + yz + zx = \hat{2}$. Aşadar $S_2 = \hat{2}$. Scriem ecuația de gradul al treilea care are ca rădăcini pe *x, y, z,* cunoscând sumele simetrice fundamentale S_1, S_2, S_3. Aceasta este: $t^3 - S_1 t^2 + S_2 t - S_3 = 0$ sau $t^3 + \hat{2}t - S_3 = \hat{0}$.

Dar x, y, z verifică această ecuație. Atunci avem:

$x^3+\hat{2}x-S_3=\hat{0}, y^3+\hat{2}y-S_3=\hat{0}, z^3+\hat{2}z-S_3=\hat{0}$, care adunate dau $x^3+y^3+z^3+\hat{2}(x+y+z)-\hat{3}S_3=\hat{0}$, adică, via a treia ecuație a sistemului, $\hat{3}S_3=\hat{1}$ și deci $S_3=\hat{2}$. Ecuația $t^3+\hat{2}t-\hat{2}=\hat{0}$ are soluțiile $t_1=\hat{2}, t_2=\hat{4}, t_3=\hat{4}$.

Soluțiile sistemului sunt: $(\hat{2},\hat{4},\hat{4}),\ (\hat{4},\hat{2},\hat{4}),\ (\hat{4},\hat{4},\hat{2})$.

2. Să se rezolve în $\mathbb{Z}_{12}$ sistemele:

$$\text{a) } \begin{cases} x+\hat{2}y+\hat{3}z=\hat{4} & (1)\\ \hat{4}x+\hat{5}y+z=\hat{7} & (2)\\ \hat{4}x+\hat{2}y+z=\hat{1} & (3)\end{cases} \qquad \text{b) } \begin{cases} \hat{6}x+\hat{3}y+\hat{2}z=\hat{3}\\ x+\hat{2}y+z=\hat{6}\\ \hat{8}x+\hat{9}z+\hat{2}z=\widehat{11}.\end{cases}$$

R. a) Determinantul sistemului $\Delta=\begin{vmatrix}\hat{1} & \hat{2} & \hat{3}\\ \hat{4} & \hat{5} & \hat{1}\\ \hat{4} & \hat{2} & \hat{1}\end{vmatrix}=\hat{3}$, care, însă, nu este inversabil în raport cu înmulțirea în $\mathbb{Z}_{12}$ și deci nu se mai pot aplica formulele lui Cramer în rezolvarea sistemului.

Aplicăm alte metode (metoda substituției sau metoda reducerii) în rezolvarea sistemului. Scăzând din (2) ecuația (3) se obține $\hat{3}y=\hat{6}$. Această ecuație are în $\mathbb{Z}_{12}$ soluțiile $y_1=\hat{2}, y_2=\hat{6}, y_3=\widehat{10}$. Analizăm aceste cazuri.

Dacă $y=\hat{2}$, ecuațiile (1) și (2) dau sistemul:

$$\begin{cases} x+\hat{3}z=\hat{0}\\ \hat{4}x+z=\hat{9}\end{cases} \text{ sau } \begin{cases} x=-\hat{3}z\\ \hat{4}(-\hat{3}z)+z=\hat{9}\end{cases} \text{ sau } \begin{cases} x=\hat{9}\\ z=\hat{9}\end{cases}$$

Deci o soluție a sistemului dat este $x=\hat{9},\ y=\hat{2},\ z=\hat{9}$.

Dacă $\boldsymbol{y=\hat{6}}$, scriem sistemul format din ecuațiile (1) și (2):

$$\begin{cases} x+\hat{3}z=\hat{4}\\ \hat{4}x+z=\hat{1}\end{cases} \text{ sau } \begin{cases} x=\hat{4}-\hat{3}z\\ \hat{4}(\hat{4}-\hat{3}z)+z=\hat{1}\end{cases} \text{ sau } \begin{cases} x=\hat{1}\\ z=\hat{9}\end{cases}$$

Deci $x=\hat{1},\ y=\hat{6},\ z=\hat{9}$, este de asemenea o soluție a sistemului.

În fine, dacă $y=\widehat{10}$ se obține sistemul (din (1) și (2)):

$$\begin{cases} x+\hat{3}z=\hat{8}\\ \hat{4}x+z=\hat{5}\end{cases} \text{ cu soluția } x=\hat{5},\ z=\hat{9}.$$

Deci, în concluzie, sistemul dat are soluțiile: $(\hat{9},\hat{2},\hat{9}),\ (\hat{1},\hat{6},\hat{9}), (\hat{5},\widehat{10},\hat{9})$.

b) Aplicăm metoda substituției în rezolvarea acestui sistem. Din ecuația a doua se exprimă x și apoi se înlocuiește în ecuațiile unu și trei. Se obține sistemul:

$$\begin{cases} x=\hat{6}+\widehat{10}y+\widehat{11}z\\ \hat{6}z+\hat{3}y+\hat{2}z=\hat{3}\\ \hat{8}y+\hat{4}z+\hat{9}y+\hat{2}z=\widehat{11}\end{cases} \text{ sau } \begin{cases} x=\hat{6}+\widehat{10}y+\widehat{11}z\\ \hat{3}y+\hat{8}z=\hat{3}\\ \hat{5}y+\hat{6}z=\widehat{11}\end{cases} \quad (*)$$

Se ia sistemul format din ultimele două ecuații din (*) şi se rezolvă prin metoda reducerii înmulțind ecuația a doua cu $\hat{5}$, obținând sistemul:

$$\begin{cases} \hat{3}y+\hat{8}z=\hat{3} \\ y=\hat{7}+\hat{6}z \end{cases} \text{ sau } \begin{cases} \hat{2}z=\hat{6} \\ y=\hat{7}+\hat{6}z \end{cases}$$

Ecuația $\hat{2}z=\hat{6}$ are în $\mathbb{Z}_{12}$ soluțiile $z_1=\hat{3}, z_2=\hat{9}$, când $y_1=\hat{1}$ şi $y_2=\hat{1}$. Soluțiile sistemului dat sunt: $(\hat{1},\hat{1},\hat{3}), (\hat{7},\hat{1},\hat{9})$.

3. **Să se rezolve sistemul matriceal:** $\begin{cases} X+\begin{pmatrix} \hat{0} & \hat{3} \\ \hat{2} & \hat{4} \end{pmatrix}Y=\begin{pmatrix} \hat{1} & \hat{1} \\ \hat{3} & \hat{2} \end{pmatrix} \\ X\begin{pmatrix} \hat{1} & \hat{4} \\ \hat{2} & \hat{3} \end{pmatrix}+Y=\begin{pmatrix} \hat{0} & \hat{1} \\ \hat{2} & \hat{0} \end{pmatrix} \end{cases}$ **în** $\mathbb{Z}_5$.

R. Luăm $X=\begin{pmatrix} a & b \\ c & d \end{pmatrix}, Y=\begin{pmatrix} x & y \\ z & u \end{pmatrix}$ şi se rescrie sistemul sub forma:

$$\begin{cases} \begin{pmatrix} a & b \\ c & d \end{pmatrix}+\begin{pmatrix} \hat{3}z & \hat{3}u \\ \hat{2}x+\hat{4}z & \hat{2}y+\hat{4}u \end{pmatrix}=\begin{pmatrix} \hat{1} & \hat{1} \\ \hat{3} & \hat{2} \end{pmatrix} \\ \begin{pmatrix} a+\hat{2}b & \hat{4}a+\hat{3}b \\ c+\hat{2}d & \hat{4}x+\hat{3}d \end{pmatrix}+\begin{pmatrix} x & y \\ z & u \end{pmatrix}=\begin{pmatrix} \hat{0} & \hat{1} \\ \hat{2} & \hat{0} \end{pmatrix} \end{cases} \text{ sau } \begin{cases} \begin{pmatrix} a+\hat{3}z & b+\hat{3}u \\ c+\hat{2}x+\hat{4}z & d+\hat{2}y+\hat{4}u \end{pmatrix}=\begin{pmatrix} \hat{1} & \hat{1} \\ \hat{3} & \hat{2} \end{pmatrix} \\ \begin{pmatrix} a+\hat{2}b+x & \hat{4}a+\hat{3}b+y \\ x+\hat{2}d+z & \hat{4}c+\hat{3}d+u \end{pmatrix}=\begin{pmatrix} \hat{0} & \hat{1} \\ \hat{2} & \hat{0} \end{pmatrix} \end{cases},$$

iar de aici se obține sistemul : $\begin{cases} a+\hat{3}z=\hat{1} \\ b+\hat{3}u=1 \\ c+\hat{2}x+\hat{4}z=\hat{3} \\ d+\hat{2}y+\hat{4}u=\hat{2} \\ a+\hat{2}b+x=\hat{0} \\ \hat{4}a+\hat{3}b+y=\hat{1} \\ c+\hat{2}d+z=\hat{2} \\ \hat{4}c+\hat{3}d+u=\hat{0} \end{cases}$

cu soluția $x=\hat{0},\ y=\hat{1}, z=\hat{3},\ u=\hat{4}, a=\hat{2}, b=\hat{4}, c=\hat{1}, d=\hat{4}$.

Soluția sistemului este: $X=\begin{pmatrix} \hat{2} & \hat{4} \\ \hat{1} & \hat{4} \end{pmatrix},\ Y=\begin{pmatrix} \hat{0} & \hat{1} \\ \hat{3} & \hat{4} \end{pmatrix}$.

4)* Grupuri de transformări geometrice

Reamintim că $\mathcal{P}$ este mulțimea punctelor din plan, atunci o funcție $f:\mathcal{P}\to\mathcal{P}$ sau o restricție a unei asemenea funcții se numeşte transformare geometrică. Printre transformările geometrice studiate în anii precedenți au fost: translația, rotația şi omotetia. Vom vedea că aceste transformări împreună cu operația de compunere pot fi organizate ca grupuri.

Am văzut că dacă $\vec{v}$ este un vector dat, atunci **translația de vector** $\vec{v}$ este funcția $t_{\vec{v}}: \mathcal{P} \to \mathcal{P}, t_{\vec{v}}(M) = M', M, M' \in \mathcal{P}$ astfel încât $\overrightarrow{MM'} \sim \vec{v}$.

Punctul M' se numeşte **translatul lui** M de vector $\vec{v}$.
Am notat cu $\mathcal{T}$ **mulțimea translațiilor planului** $\mathcal{P}$. Atunci are loc următoarea:

> **Teoremă.** Cuplul $(\mathcal{T}, \circ)$ este un grup abelian, numit **grup al translațiilor** planului $\mathcal{P}$.

Dacă O este un punct fix al planului $\mathcal{P}$, iar α are un unghi orientat din acelaşi plan, atunci am numit **rotație de centru** O şi **unghi** α**,** aplicația $r_O^{\alpha}: \mathcal{P} \to \mathcal{P}$ definită prin $r_O^{\alpha}(A) = A', \ OA = OA', \ \widehat{AOA'} = \alpha$. Am numit punctul O **centrul rotației,** α **unghiul de rotație**, iar A' este **imaginea lui** A prin rotație. Am notat cu $\mathcal{R}_O$ **mulțimea rotațiilor de centru** O din planul $\mathcal{P}$. Are loc următorul rezultat:

> **Teoremă.** Cuplul $(\mathcal{R}_O, \circ)$ este un grup abelian, numit **grupul abelian al rotațiilor de centru** O **din planul** $\mathcal{P}$.

În fine, o ultimă transformare geometrică importantă în plan a fost **omotetia de centru** O (punct fix) **şi raport** $k \in \mathbb{R}^*, \ h_O^k: \mathcal{P} \to \mathcal{P}, \ h_O^k(A) = A', \ A, A' \in \mathcal{P}, \ O, A, A'$ coliniare şi $OA' = |k| OA$ (sau în limbaj vectorial, $\overrightarrow{OA'} = k \cdot \overrightarrow{OA}$). Punctul O se numeşte **centru de omotetie**, iar k este **raportul de omotetie;** punctul A' este **omoteticul lui** A. Am notat prin $\mathcal{H}_O$ mulțimea omotetiilor de centru O din planul $\mathcal{P}$. Are loc următoarea:

> **Teoremă.** Cuplul $(\mathcal{H}_O, \circ)$ este grup abelian, numit **grupul omotetiilor de centru** O **ale planului** $\mathcal{P}$.

O aplicație **bijectivă** $\varphi: \mathcal{P} \to \mathcal{P}$ se numeşte **izometrie** dacă $d(\varphi(A), \varphi(B)) = d(A, B)$, unde $d(A, B)$ înseamnă distanța dintre A şi B. Mai simplu scris $\varphi(A)\varphi(B) = AB$.
Dacă notăm cu Izom($\mathcal{P}$) mulțimea izometriilor planului, atunci are loc următoarea:

> **Teoremă.** Cuplul $(\text{Izom}(\mathcal{P}), \circ)$ este grup, numit **grupul izometriilor planului** $\mathcal{P}$**.**

Probleme propuse

1. 1) Arătați că fiecare din următoarele mulțimi cu legea de compoziție dată de tablele de mai jos este grup:

1) $\{e,a\}$

$\circ$	e	a
e	e	a
a	a	e

2) $\{e,a,b\}$

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

3) $\{1,\omega,\omega^2\}$, $\omega^2+\omega+1=0$

$\circ$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

2) Dacă $(M,\cdot)$ este un grup, $M = \{a, b, c, d\}$, atunci există un singur mod de a completa tabelul:

a)

$\cdot$	a	b	c	d
a		d		
b				
c			c	
d				c

;

b)

$\cdot$	a	b	c	d
a				
b	b	c		
c				
d				

;

c)

$\cdot$	a	b	c	d
a				
b		a		
c	a			
d				

.

2. Pe $\mathbb{Z}$ se definește aplicația $x * y = x + y - 1$. Arătați că $(\mathbb{Z},*)$ este grup abelian.

3. Fie $G = (-1,\infty)$ și aplicația pe G, $x \circ y = x + y + xy$. Să se arate că $(G,\circ)$ este grup abelian.

4. Pe $\mathbb{R}$ definim legea de compoziție $x * y = x + y - xy$. Să se arate că $R_1 = \mathbb{R} - \{1\}$ este o parte stabilă a lui $\mathbb{R}$ în raport cu legea $*$ și $(R_1,*)$ este grup abelian.

5. Pe mulțimea numerelor raționale $\mathbb{Q}$ se definește legea de compoziție $x \top y = x + y - \dfrac{xy}{2}$. Să se arate că $Q_2 = \mathbb{Q} - \{2\}$ este parte stabilă a lui $\mathbb{Q}$ în raport cu $\top$ și $(Q_2,\top)$ este grup comutativ.

6. Să se demonstreze că pe mulțimea $(0,\infty)-\{1\}$ aplicația $x \top y = x^{3\ln y}$ determină o structură de grup abelian.

7. Să se arate că pe mulțimea $G = (1,\infty)-\{2\}$ aplicația $x * y = (x-1)^{\frac{1}{2}\ln(y-1)} + 1$ determină o structură algebrică de grup comutativ.

8. Să se determine $a \in \mathbb{Z}$ astfel încât $\mathbb{Z}$ împreună cu aplicația $x \circ y = x + y - axy$ să fie un grup abelian.

9. a) Să se determine cea mai mică valoare a lui $\lambda \in \mathbb{R}$ pentru care intervalul $(1,\infty)$ este parte stabilă a lui $\mathbb{R}$ în raport cu legea de compoziție de pe $\mathbb{R}$, $x * y = xy - x - y + \lambda$.

b) Pentru λ de la punctul a), calculați $x^n = \underbrace{x * x * ... * x}_{n}$ și arătați că $(G,*)$ este grup abelian, unde $G = (1,\infty)$.

10. Pe intervalul (m,∞) se consideră aplicația $x * y = xy - m(x+y) + m^2 + m$. Arătați că $((m,\infty),*)$ este grup comutativ.

11. Fie mulțimea $G=(-1,\infty)$ pe care se consideră aplicația $x \top y = a\left(x^2+y^2\right) + 2xy + 2\left(m^2-3\right) + 2y + m - 1$, $a,m \in \mathbb{R}$ Determinați a, m pentru care $(G,\top)$ este grup abelian.

12. Se consideră $G=(-1,1)$ pe care definim aplicația $x*y=\dfrac{ax+by}{1+xy}$. Arătați că $(G,*)$ este grup $\Leftrightarrow a=b=1$.

13. Pe mulțimea $\mathbb{R}$ se definește operația $x*y=ax+by, a,b\in\mathbb{R}$. Determinați *a, b* pentru care $(\mathbb{R},*)$ este grup.

14*. Fie $G=(1,\infty)$ şi pe $\mathbb{R}$ legea de compoziție $x\circ y=xy+ax+by+c, a,b,c\in\mathbb{R}$. Determinați $a,b,c\in\mathbb{R}$ dacă $(G,\circ)$ este grup.

15. Arătați că următoarea mulțime de funcții: $G=\{g_1,g_2,g_3,g_4\}$, unde $g_i:\mathbb{R}-\{0,\pm1\}\to\mathbb{R}-\{0,\pm1\}$, $g_1(x)=x$, $g_2(x)=\dfrac{x-1}{x+1}$, $g_3(x)=-\dfrac{1}{x}$, $g_4(x)=\dfrac{x+1}{1-x}$, împreună cu operația de compunere formează grup comutativ.

16. Arătați că următoarele mulțimi de matrice pătratice de ordin doi sunt grupuri împreună cu operația de înmulțire:

1) $\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a,b\in\mathbb{R}, a^2+b^2>0\right\}$;

2) $\left\{\begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \middle| a,b\in\mathbb{Q}, a^2+b^2>0\right\}$;

3) $\left\{\begin{pmatrix} a & -3b \\ b & a \end{pmatrix} \middle| a,b\in\mathbb{Q}, a^2+b^2>0\right\}$;

4) $\left\{\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \middle| \alpha\in[0,2\pi)\right\}$;

5) $\left\{\begin{pmatrix} \cos\dfrac{2k\pi}{n} & -\sin\dfrac{2k\pi}{n} \\ \sin\dfrac{2k\pi}{n} & \cos\dfrac{2k\pi}{n} \end{pmatrix} \middle| k=\overline{0,n-1}\right\}$;

6) $\left\{\begin{pmatrix} 2-a & a-1 \\ 2(1-a) & 2a-1 \end{pmatrix} \middle| a\in\mathbb{R}^*\right\}$;

7) $\left\{\begin{pmatrix} a & 0 \\ c & b \end{pmatrix} \middle| a,b,c\in\mathbb{R}, a,b\neq 0\right\}$;

8) $\left\{\begin{pmatrix} a & 2b \\ \dfrac{7b}{2} & a \end{pmatrix} \middle| a,b\in\mathbb{Q}, a^2-7b^2=1\right\}$;

9) $\left\{A\in M_2(\mathbb{R}) \middle| {}^tA\cdot A=E\right\}$;

10) $\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}\right\}$.

17. Să se arate că mulțimea matricelor $G=\left\{A=\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a,b,c\in\mathbb{Z}\right\}$ este grup în raport cu înmulțirea matricelor.

18. Fie $G=\left\{M_{a,b}=\begin{pmatrix} a & b & b \\ b & a & b \\ b & b & a \end{pmatrix} \middle| M_{a,b}\in M_3(\mathbb{R}), \det(M_{a,b})=1\right\}$. Să se arate că *G* este grup în raport cu înmulțirea matricelor.

19. Fie ecuația $x^4+ax^3+bx^2+cx+d=0$. Determinați numerele reale *a, b, c, d* astfel încât mulțimea formată din soluțiile complexe ale ecuației să fie: 1) grup în raport cu adunarea uzuală; 2) grup în raport cu înmulțirea uzuală.

20. Fie $G=\left\{M(a)=\begin{pmatrix}1 & 0 & a\\ -a & 1 & -\frac{a^2}{2}\\ 0 & 0 & 1\end{pmatrix}\middle| a\in\mathbb{R}\right\}$. Să se arate că G este grup abelian în raport cu înmulțirea matricelor. Calculați $M^3(a)$.

21. 1) Se consideră mulțimea: $G=\left\{A(x)=\begin{pmatrix}1-x & 0 & x\\ 0 & 0 & 0\\ x & 0 & 1-x\end{pmatrix}\middle| x\in\mathbb{R}-\left\{\frac{1}{2}\right\}\right\}$. Arătați că G formează grup relativ la operația de înmulțire a matricelor și calculați $A^n(x)$.

2) Fie G mulțimea matricelor de forma: $M(a)=\frac{1}{\sqrt{1-a^2}}\begin{pmatrix}1 & -a & 0\\ -a & 1 & 0\\ 0 & 0 & \sqrt{1-a^2}\end{pmatrix}, a\in(-1,1)$. Să se arate că:

a) $(G,\cdot)$ este grup abelian;

b) dacă $a\in(-1,1)$, atunci pentru orice $n\in\mathbb{N}^*$ există un unic element $a_n\in(-1,1)$ cu proprietatea $M(a_n)=(M(a))^n$;

c) $\lim\limits_{n\to\infty} a_n=\frac{a}{|a|}, \forall a\in(-1,1)-\{0\}$.

3) Fie $\mathcal{M}=\left\{A(x)=\begin{pmatrix}1 & x & x+x^2\\ 0 & 1 & 2x\\ 0 & 0 & 1\end{pmatrix}; x\in\mathbb{R}\right\}$. Să se arate că:

a) $A(x)=A(y)\Leftrightarrow x=y$; b) $A(x)\cdot A(y)=A(x+y)$; c) $(\mathcal{M},\cdot)$ este grup abelian; d) Calculați $A(1)A(2)...A(n)$.

22. Fie matricea $A=\begin{pmatrix}0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{pmatrix}$ și $G=\{A^n \mid n\in\mathbb{N}^*\}$. Arătați că $(G,\cdot)$ este grup abelian. Câte elemente are G ?

23. Să se demonstreze că pe mulțimea $G=(1,\infty)\times(2,\infty)$ aplicația:

$$(x,y)\top(x',y')=(xx'-x-x'+2,\ yy'-2y-2y'+6)$$

determină o structură de grup comutativ.

24. 1) Fie mulțimea de matrice de ordinul doi:

$$G=\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix},\begin{pmatrix}0 & i\\ i & 0\end{pmatrix},\begin{pmatrix}0 & -i\\ -i & 0\end{pmatrix},\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\begin{pmatrix}-i & 0\\ 0 & i\end{pmatrix},\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}\right\}.$$

Să se arate că G împreună cu înmulțirea matricelor formează un grup necomutativ.

2) (Matrice permutare) O astfel de matrice se obține din matricea unitate I_n prin interschimbarea liniilor odată sau de mai multe ori (permutări de linii). Pentru $n=3$ avem matricele:

$$P_1=\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix},\ P_2=\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix},\ P_3=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix},\ P_4=\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix},\ P_5=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}.$$

Arătați că $G=\{I_3,P_1,P_2,...,P_5\}$ este grup cu înmulțirea matricelor.

3) Fie $A=\begin{pmatrix}0&-1\\1&0\end{pmatrix},\ B=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\ C=\begin{pmatrix}-1&0\\0&1\end{pmatrix},\ D=\begin{pmatrix}0&1\\1&0\end{pmatrix},\ E=\begin{pmatrix}0&-1\\-1&0\end{pmatrix}.$

Arătați $G=\left\{I_2,\ A,\ A^2,\ A^3,\ B,\ C,\ D,\ E\right\}$ este grup cu operația de înmulțire a matricelor. Scrieți tabla legii.

25. **Să se arate că mulțimea** $G=\left\{\begin{pmatrix}\hat{1}&a&b\\0&\hat{1}&c\\0&0&\hat{1}\end{pmatrix}\middle|\, a,b,c\in\mathbb{Z}_3\right\}$ **împreună cu înmulțirea obişnuită a matricelor este grup. Câte elemente are acest grup?**

26. **Arătați că mulțimea** $G=\left\{\begin{pmatrix}\hat{1}&\hat{4}a\\\hat{6}a&\hat{1}\end{pmatrix}\middle|\, a\in\mathbb{Z}_{12}\right\}$ **împreună cu operația de înmulțire obişnuită a matricelor este grup abelian.**

27. **Fie matricele** $A=\begin{pmatrix}\hat{0}&\hat{2}\\\hat{0}&\hat{0}\end{pmatrix},\ B=\begin{pmatrix}\hat{0}&\hat{4}\\\hat{0}&\hat{0}\end{pmatrix},\ C=\begin{pmatrix}\hat{0}&\hat{0}\\\hat{6}&\hat{0}\end{pmatrix}$ **din $\mathcal{M}_2(\mathbb{Z}_{12})$ şi mulțimea :**

$G=\{I_2+xA+yB+zC \mid x,y,z\in\mathbb{Z}_{12}\}$.

Arătați că $(G,\cdot)$ este grup abelian.

28. **Fie** $A=\begin{pmatrix}\hat{1}&\hat{2}\\\hat{5}&\hat{1}\end{pmatrix}\in\mathcal{M}_2(\mathbb{Z}_{10})$ **şi mulțimea** $G=\{A^n \mid n\in\mathbb{N}^*\}$.

1) Arătați că $(G,\cdot)$ este grup abelian.

2) Arătați că dacă $AX=AY$, atunci $X=Y$.

3) Rezolvați ecuația $XA=AX$.

29. **Să se rezolve sistemele:**

1) $\begin{cases}\hat{3}x+y+\hat{2}z=\hat{3}\\x+\hat{2}y+\hat{3}z=\hat{1}\\\hat{2}x+\hat{3}y+z=\hat{2}\end{cases}$ în $\mathbb{Z}_5$; 2) $\begin{cases}x+y+\hat{3}z=\hat{1}\\\hat{2}x+y+z=\hat{2}\\\hat{3}x+\hat{4}y=\hat{4}\end{cases}$ în $\mathbb{Z}_5$; 3) $\begin{cases}x+\hat{2}y+\hat{3}z=\hat{1}\\\hat{4}x+y+\hat{2}z=\hat{2}\\\hat{2}x+\hat{4}y+\hat{3}z=3\end{cases}$ în $\mathbb{Z}_5$;

4) $\begin{cases}\hat{3}x+\hat{3}y+z=\hat{2}\\x+\hat{2}y+\hat{3}z=\hat{3}\\\hat{2}x+y+\hat{3}z=\hat{5}\end{cases}$ în $\mathbb{Z}_7$; 5) $\begin{cases}\hat{2}x+\widehat{10}y+z=\hat{4}\\x+\hat{3}z=\hat{2}\\\widehat{10}x+\hat{2}y+\hat{2}z=\hat{1}\end{cases}$ în $\mathbb{Z}_{11}$; 6) $\begin{cases}x+y+z=\hat{0}\\\hat{3}x+\hat{2}y+z=\hat{1}\\\hat{5}x+\hat{3}y+\hat{2}z=\hat{4}\end{cases}$ în $\mathbb{Z}_{11}$;

7) $\begin{cases}\hat{2}x+y+\hat{2}z=\hat{2}\\ x+\hat{3}y+\hat{3}z=\hat{3}\\ \hat{4}x+\hat{5}y+\hat{4}z=\hat{4}\end{cases}$ în $\mathbb{Z}_6$; 8) $\begin{cases}x+\hat{2}y+\hat{3}z=\hat{0}\\ \hat{2}x+y+z=\hat{2}\\ x+\hat{3}y+\hat{3}z=\hat{3}\end{cases}$ în $\mathbb{Z}_6$; 9) $\begin{cases}\hat{2}x+\hat{4}y+\hat{3}z=\hat{5}\\ \hat{2}x+\hat{2}y+\hat{3}z=\hat{3}\\ x+\hat{3}y+\hat{4}z=\hat{1}\end{cases}$ în $\mathbb{Z}_6$;

10) $\begin{cases}\hat{2}x+\hat{3}y+z=\hat{3}\\ \hat{4}x+\hat{2}y+\hat{3}z=\hat{1}\\ \hat{6}x+\hat{3}y+\hat{2}z=\hat{2}\end{cases}$ în $\mathbb{Z}_8$; 11) $\begin{cases}\hat{2}x+\hat{5}y+\hat{9}z=\hat{7}\\ x+\hat{5}y+\hat{9}z=\hat{2}\\ \hat{3}x+\hat{4}y+\hat{2}z=\hat{1}\end{cases}$ în $\mathbb{Z}_{10}$; 12) $\begin{cases}x+\hat{5}y+\hat{7}z=\widehat{10}\\ \hat{3}y+\hat{2}z=\hat{9}\\ x+\hat{7}y+\hat{3}z=\hat{4}\end{cases}$ în $\mathbb{Z}_{12}$;

13) $\begin{cases}x+y+z=\hat{2}\\ xy+yz+zx=\hat{4}\\ xyz=\hat{3}\end{cases}$ în $\mathbb{Z}_5$; 14) $\begin{cases}x+y+z=\hat{1}\\ x^2+y^2+z^2=\hat{4}\\ x^3+y^3+z^3=\hat{1}\end{cases}$ în $\mathbb{Z}_5$;

15) $\begin{cases}x+y+z=\hat{2}\\ xy+xz+yz=\hat{4}\\ x^2yz+xy^2z+xyz^2=\hat{1}\end{cases}$ în $\mathbb{Z}_5$; 16) $\begin{cases}X+\hat{2}Y=\begin{pmatrix}\hat{0}&\hat{1}\\ \hat{1}&\hat{2}\end{pmatrix}\\ \hat{3}X+Y=\begin{pmatrix}\hat{1}&\hat{2}\\ \hat{3}&\hat{4}\end{pmatrix}\end{cases}$ în $\mathbb{Z}_5$.

30. Arătați că matricele (X,Y) sunt o soluție pentru fiecare din sistemele:

a) $\begin{cases}X\begin{pmatrix}\hat{1}&\hat{2}\\ \hat{1}&\hat{3}\end{pmatrix}+Y=\begin{pmatrix}\hat{3}&\hat{4}\\ \hat{2}&\hat{1}\end{pmatrix},\\ \begin{pmatrix}\hat{2}&\hat{1}\\ \hat{1}&\hat{0}\end{pmatrix}X+Y\begin{pmatrix}\hat{1}&\hat{2}\\ \hat{0}&\hat{1}\end{pmatrix}=\begin{pmatrix}\hat{4}&\hat{3}\\ \hat{3}&\hat{4}\end{pmatrix}\end{cases}$ în $\mathbb{Z}_5$; $X=\begin{pmatrix}\hat{1}&\hat{2}\\ \hat{2}&\hat{3}\end{pmatrix}$, $Y=\begin{pmatrix}\hat{0}&\hat{1}\\ \hat{2}&\hat{3}\end{pmatrix}$

b) $\begin{cases}X\begin{pmatrix}\hat{0}&\hat{2}\\ \hat{3}&\hat{3}\end{pmatrix}+\begin{pmatrix}\hat{1}&\hat{0}\\ \hat{2}&\hat{4}\end{pmatrix}Y=\begin{pmatrix}\hat{6}&\hat{5}\\ \hat{1}&\hat{1}\end{pmatrix}\\ X\begin{pmatrix}\hat{1}&\hat{3}\\ \hat{2}&\hat{0}\end{pmatrix}-Y\begin{pmatrix}\hat{0}&\hat{3}\\ \hat{2}&\hat{1}\end{pmatrix}=\begin{pmatrix}\hat{1}&\hat{4}\\ \hat{5}&\hat{1}\end{pmatrix}\end{cases}$ în $\mathbb{Z}_7$; $X=\begin{pmatrix}\hat{0}&\hat{4}\\ \hat{3}&\hat{2}\end{pmatrix}$, $Y=\begin{pmatrix}\hat{1}&\hat{0}\\ \hat{0}&\hat{1}\end{pmatrix}$

c) $\begin{cases}X\begin{pmatrix}\hat{0}&\hat{1}\\ \hat{0}&\hat{1}\end{pmatrix}+Y\begin{pmatrix}\hat{1}&\hat{0}\\ \hat{2}&\hat{1}\end{pmatrix}=\begin{pmatrix}\hat{1}&\hat{4}\\ \hat{3}&\hat{2}\end{pmatrix}\\ X\begin{pmatrix}\hat{2}&\hat{0}\\ \hat{1}&\hat{3}\end{pmatrix}-Y\begin{pmatrix}\hat{1}&\hat{1}\\ \hat{0}&\hat{3}\end{pmatrix}=\begin{pmatrix}\hat{3}&\hat{4}\\ \hat{6}&\hat{6}\end{pmatrix}\end{cases}$ în $\mathbb{Z}_7$; $X=\begin{pmatrix}\hat{0}&\hat{4}\\ \hat{3}&\hat{2}\end{pmatrix}$, $Y=\begin{pmatrix}\hat{1}&\hat{0}\\ \hat{2}&\hat{4}\end{pmatrix}$.

31. Alcătuiți tabla legii de compunere a permutărilor pe S_3 .

32. Arătați că mulțimea de permutări $S=\{e,\sigma_1,\sigma_2,\sigma_3\}$, unde:

$$e=\begin{pmatrix}1&2&3&4&5&6\\ 1&2&3&4&5&6\end{pmatrix},\ \sigma_1=\begin{pmatrix}1&2&3&4&5&6\\ 6&4&2&5&3&1\end{pmatrix},\ \sigma_2=\begin{pmatrix}1&2&3&4&5&6\\ 1&5&4&3&2&6\end{pmatrix},\ \sigma_3=\begin{pmatrix}1&2&3&4&5&6\\ 6&3&5&2&4&1\end{pmatrix},$$

împreună cu operația de compunere a permutărilor formează un grup.

33. **Să se rezolve ecuațiile:**

a) $x^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$; **b)** $x^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$.

34. **Să se rezolve ecuația** $\sigma x = x\sigma$ **, unde** $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

Reguli de calcul într-un grup

Am văzut pentru monoizi anumite posibilități de efectuare a unor calcule algebrice. Cum orice grup este monoid, se înțelege că toate regulile de calcul valabile pentru monoizi se păstrează şi pentru grupuri. În plus pentru grupuri există reguli care le sunt specifice (şi țin de existența pentru fiecare element a inversului).

Teoremă. (**Reguli de simplificare**) Fie $(G,\cdot)$ un grup şi $x, y \in G$ arbitrare. Au loc echivalențele:

1) $zx = zy \Leftrightarrow x = y$ („simplificare“ la stânga), $z \in G$.

2) $xz = yz \Leftrightarrow x = y$ („simplificare“ la dreapta), $z \in G$.

Demonstrație. **1)** „$\Rightarrow$“ Fie $zx = zy$. Prin înmulțire la stânga cu z^{-1} rezultă $z^{-1}(zx) = z^{-1}zy \Leftrightarrow (z^{-1}z)y \Leftrightarrow ex = ey \Leftrightarrow x = y$.

„$\Leftarrow$“ Presupunem că $x = y$. Se înmulțeşte la stânga cu z şi avem $zx = zy$.

2) Analog. ■

Observații. **1)** Dacă legea este dată aditiv atunci teorema se scrie:

1) $z + x = z + y \Leftrightarrow x = y$;

2) $x + z = y + z \Leftrightarrow x = y$.

2) Proprietatea de a împărți o egalitate printr-un număr real nenul rezultă din această teoremă. La fel, proprietatea de a reduce termenii egali situați în membri diferiți rezultă de aici.

Teoremă. Fie $(G,\cdot)$ un grup şi $x \in G$ fixat. Atunci:

1) $x^n x^m = x^{n+m}$,

2) $\left(x^n\right)^m = x^{nm}$, $(\forall) n, m \in \mathbb{Z}$.

Demonstrație. Analogă celei de la monoizi. ■

Observație. Dacă grupul G este aditiv, atunci rezultatele din teoremă au forma:

1) $nx + mx = (n + m)x$,

2) $n(mx) = (nm)x$, $(\forall) n, m \in \mathbb{Z}$.

Următorul rezultat simplu pentru elementele unui grup poate stabili dacă acesta este comutativ. Mai precis are loc

Teorema. Dacă în grupul $(G,\cdot)$ avem $x^2 = e, (\forall) x \in G$, atunci grupul este **abelian**.

Demonstrație. Fie $x, y \in G$, arbitrare. Să probăm că $xy = yx$.

Din $x, y \in G$ rezultă $xy \in G$ şi deci $x^2 = e,\ y^2 = e,\ (xy)^2 = e$.

Scriem egalitatea $(xy)^2 = e$ succesiv astfel:

$(xy)(xy) = x^2y^2 \Leftrightarrow x(yx)y = x(xy)y \Leftrightarrow yx = xy$ (după simplificare la stânga cu x şi la dreapta cu y). ■

Probleme propuse

1. Fie $(G,\cdot)$ un grup cu element neutru e. Arătați că $(G,\cdot)$ este grup abelian dacă este adevărată una din condițiile de mai jos:

1) $x^3 = e, \forall x \in G, x^2y^2 = y^2x^2, \forall x, y \in G$;

2) $x^3 = e, \forall x \in G, (xy)^2 = (yx)^2, \forall x, y \in G$;

3) există $n \in N^*$ astfel încât pentru orice $x, y \in G$ avem: $(xy)^n = x^n y^n, (xy)^{n+1} = x^{n+1}y^{n+1}$ şi $(xy)^{n+2} = x^{n+2}y^{n+2}, \forall x, y \in G$.

2. Se consideră $(G,\cdot)$ un grup abelian cu n elemente. Să se arate că $x^n = e, \forall x \in G$, unde e este elementul neutru al grupului.

3. Fie $(G,\cdot)$ grup şi $x, y \in G$, astfel încât: 1) $x^5 = y^4 = e$; 2) $xy = yx^3$. Arătați că: $yx = x^2y$ şi $xy^3 = y^3x^2$.

4. Fie $(G,\cdot)$ un grup cu element neutru e. Arătați că $(G,\cdot)$ este grup abelian dacă este adevărată una din condițiile de mai jos:

1) $x = x^{-1}, \forall x \in G$; 2) $(xy)^{-1} = x^{-1}y^{-1}, \forall xy \in G$; 3) $xy^{-1} = yx^{-1}, \forall x, y \in G - \{e\}$.

5. Fie $(G,\cdot)$ grup şi $x, y \in G$, astfel încât $x^2 = y^2 = (xy)^2$. Să se arate că $x^4 = y^4 = e$.

6. Pe $G = \mathbb{C} - \{i\}$ se consideră aplicația $x * y = x + y + ixy, \forall x, y \in G$.

1)Arătați că $(G,*)$ este grup comutativ.

2) Calculați $(-i)^3, (1+i)^2, x^n, n \in N^*, n \geq 2$.

7. Pe $G = (3,\infty)$ se consideră aplicația $x * y = xy - 3x - 3y + 12, x, y \in G$.

1)Arătați că $(G,*)$ este grup abelian.

2) Arătați că $\underbrace{a * a * ... * a}_{n \text{ ori}} = (a-3)^n + 3, \forall a \in G, n \in \mathbb{N}, n \geq 2$.

8. **Fie** $G=\left\{\begin{pmatrix}1 & 3a\\ 0 & 1\end{pmatrix}\middle| a\in\mathbb{Z}\right\}$.

1) Arătați că $(G,\cdot)$ este grup abelian.

2) Fie $A(a)=\begin{pmatrix}1 & 3a\\ 0 & 1\end{pmatrix}$. Calculați $A^2(1), A^3(-3), A(a)A(b), A^n(a), A(a)+A^2(a)+..+A^n(a)$.

1.4.3. Subgrupuri

Printre submulțimile nevide ale unui grup *G*, există unele care formează grup relativ la operația de pe *G*. Astfel de submulțime se numeşte subgrup a lui *G*.

Definiție. Fie *G* un grup. O submultime nevidă *H* a lui *G* se numeşte **subgrup** al grupului *G* dacă legea de compoziție din *G* induce pe *H* o lege de compoziție împreună cu care *H* este grup.

Exemple. **1) $(\mathbb{Z},+)$ este subgrup al grupului $(\mathbb{Q},+)$.**

2) $(\mathbb{R},+)$ este subgrup al grupului $(\mathbb{C},+)$.

3) $(U_n,\cdot)$ este subgrup al grupului $(\mathbb{C}^*,\cdot)$.

Următoarea afirmație vine să precizeze în ce condiții o submulțime *H* unui grup *G* este un subgrup.

Teoremă. O submulțime *H* a unui grup (multiplicativ) *G* este subgrup al grupului *G* dacă şi numai dacă sunt îndeplinite condițiile:

1) $(\forall)x, y\in H \Rightarrow xy\in H$,

2) $(\forall)x\in H \Rightarrow x^{-1}\in H$.

Demonstrație. Presupunem că *H* este subgrup al lui *G*. Atunci din definiție rezultă că legea de compoziție din *G* induce o lege de compoziție pe *H,* adică se verifică **1)**. Legea indusă posedă element neutru $u\in H$, astfel încât oricare ar fi $x\in H$, $ux=xu=x$. În particular, *uu* = *u* şi din unicitatea lui *u* rezultă $u=uu^{-1}=e$. Prin urmare *H* conține elementul neutru din *G*. Cum *H* este subgrup, orice element $x\in H$ este inversabil în *H* şi inversul lui *x* în *H* coincide cu inversul lui *x* în *G,* deoarece inversul este unic, adică $x\in H \Rightarrow x^{-1}\in H$ şi **2)** are loc.
Reciproc, presupunem verificate condițiile **1)** şi **2)**. Din **1)** rezultă legea lui *G* induce o lege pe *H* care este asociativă, deoarece legea din *G* este asociativă. Din **2)** se deduce că pentru fiecare $x\in H \Rightarrow x^{-1}\in H$ deci $xx^{-1}=e\in H$. Cu aceasta *H* împreună cu legea indusă este grup, adică subgrup al lui G.■

Observații. 1) Dacă legea în G este notată aditiv, atunci condițiile **1)** și **2)** se scriu sub forma:

1') $(\forall)x, y \in H \Rightarrow x + y \in H$,

2') $(\forall)x \in H \Rightarrow -x \in H$.

2) Să reținem că un subgrup H al grupului G este o submulțime a sa care odată cu două elemente conține și produsul lor (l)), iar odată cu un element îi conține și inversul (2)). Teorema precedentă se poate reformula și sub forma:

> **Teoremă**. O submulțime nevidă H a unui grup G este subgrup al lui G, dacă și numai dacă este îndeplinită condiția:
> $$(\forall)x, y \in H \Rightarrow xy^{-1} \in H .$$

Demonstrație. Fie H subgrup al lui G. Atunci, condiția este îndeplinită conform teoremei precedente, deoarece din $x, y \in H \Rightarrow x, y^{-1} \in H$ și deci $xy^{-1} \in H$.

Reciproc, dacă $x \in H \Rightarrow xx^{-1} = e \in H$. Din $e, x \in H \Rightarrow ex^{-1} = x^{-1} \in H$ adică se verifică **2)** din teorema precedentă.

Dacă $x, y \in H \Rightarrow x, y^{-1} \in H$ și deci $x(y^{-1})^{-1} = xy \in H$, adică are loc și **1)** din teorema precedentă.■

Observație. 1) Dacă G este aditiv, atunci condiția din teoremă se scrie
$$(\forall)x, y \in G \Rightarrow x - y \in G .$$
2) Dacă H este subgrup al lui G, atunci notăm $H \leq G$.

Exemple

1. Fie G un grup și $e \in G$ elementul neutru. Submulțimile G și $\{e\}$ ale lui G sunt subgrupuri, numite subgrupuri improprii. Orice subgrup H al lui G, diferit de G și $\{e\}$ se numește subgrup propriu.

2. Grupul $(\{1,-1\},\cdot)$ este subgrup al lui $(\mathbb{R}^*,\cdot)$

3. Fie $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}, n \in \mathbb{Z}$, submulțime a grupului $(\mathbb{Z},+)$. Atunci $(n\mathbb{Z},+)$ este subgrup al lui $\mathbb{Z}$, deoarece $(\forall)nk_1, nk_2 \in n\mathbb{Z}$ rezultă

1) $nk_1 + nk_2 = n(k_1 + k_2) \in \mathbb{Z}$ și

2) $-nk = n(-k) \in n\mathbb{Z}$.

4. Submulțimea $H = \{z \in \mathbb{C} \mid |z| = 1\}$ este un subgrup infinit al lui $(\mathbb{C}^*,\cdot)$ deoarece $(\forall)x,y \in H \Rightarrow xy^{-1} \in H$ pentru că $\left|xy^{-1}\right| = \left|\frac{x}{y}\right| = \frac{|x|}{|y|} = \frac{1}{1} = 1$ și odată cu $z \in H \Rightarrow z^n \in H, (\forall)n \in \mathbb{Z}$.

5. Submulțimea $H = \{1, -1, i, -i\}$ este subgrup finit al grupului $\left(\mathbb{C}^*,\cdot\right)$. Pentru aceasta considerăm tabla operației.

$\cdot$	1	-1	i	-1
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Se constată că $(\forall)x,y\in H \Rightarrow xy\in H$. În plus, $1^{-1}=1\in H$, $(-1)^{-1}=-1\in H, i^{-1}=-i\in H, (-i)^{-1}=i\in H$. Deci $(H,\cdot)$ este subgrup al lui $(\mathbb{C}^*,\cdot)$. De fapt, $H=U_4$, grupul multiplicativ al rădăcinilor de ordin 4 ale unității.

6. Submulțimea $H=\{\hat{0},\hat{2},\hat{4},6\}$ este subgrup finit al grupului $(\mathbb{Z}_8,+)$. Tabla operației pe *H* este dată alăturat.
Observăm că $(\forall)x,y\in H \Rightarrow x+y\in H$. Simetricul fiecărui element din *H* este tot în *H*, $-\hat{0}=0\in H, -\hat{2}=\hat{6}\in H, -\hat{4}=\hat{4}\in H, -\hat{6}=\hat{2}\in H$. Asemănător probați că $H=\{\hat{1},\hat{2},\hat{4}\}$ este subgrup al grupului $(\mathbb{Z}_7^*,\cdot)$.

$+$	$\hat{0}$	$\hat{2}$	$\hat{4}$	$\hat{6}$
$\hat{0}$	$\hat{0}$	$\hat{2}$	$\hat{4}$	$\hat{6}$
$\hat{2}$	$\hat{2}$	$\hat{4}$	$\hat{6}$	$\hat{0}$
$\hat{4}$	$\hat{4}$	$\hat{6}$	$\hat{0}$	$\hat{2}$
$\hat{6}$	$\hat{6}$	$\hat{0}$	$\hat{2}$	$\hat{4}$

7. Fie $H=\{\hat{2},\hat{4},\hat{6},\hat{8}\}\subseteq\mathbb{Z}_{10}$. Utilizând tabla operației cu înmulțirea arătați că $(H,\cdot)$ este grup. Totuși, $(H,\cdot)$ nu este subgrup al lui $\mathbb{Z}_{10}$, deoarece $\mathbb{Z}_{10}$ cu înmulțirea nu este grup.

8. Dacă *G* este un grup, atunci: 1) $\mathbb{Z}(G)=\{z\in G \mid zg=gz, \forall g\in G\}$ se numeşte centrul grupului *G*.

9. Dacă $g\in G$, atunci $C(g)=\{x\in G \mid xg=gx\}$ (elementele grupului care comută cu *g*) este subgrup al lui *G* (numit centralizatorul lui *g* în *G*). Care este relația între aceste subgrupuri şi $\mathbb{Z}(G)$?

Următoarea teoremă dă informații despre comportarea subgrupurilor unui grup față de operația de intersecție a mulțimilor. Mai precis are loc:

Teorema. Fie o $\{H_i\}$ familie de subgrupuri ale lui *G*. Atunci intersecția $\bigcap H_i$ este un subgrup al lui G.

Demonstrație. Cum elementul neutru *e* al grupului aparține fiecărui subgrup H_i se deduce că $e\in\bigcap H_i$, adică $\bigcap H_i\neq\varnothing$.

Dacă $x,y\in\bigcap H_i$, atunci $x,y\in H_i, (\forall)i$. Cum H_i este subgrup rezultă că $xy^{-1}\in H_i$, $(\forall)i$ şi deci $xy^{-1}\in\bigcap H_i$, ceea ce arată că $\bigcap H_i$ este subgrup al lui *G*. ■

Exemplu. Să se arate că $2\mathbb{Z}\cap 3\mathbb{Z}=6\mathbb{Z}$.
R. Egalitatea de mulțimi se probează prin dubla incluziune.
Fie $x\in 2\mathbb{Z}\cap 3\mathbb{Z}$. Deci există $k, m\in\mathbb{Z}$ astfel încât $x=2k=3m$. Deci *x* se divide prin 2 şi 3, adică se divide prin 6, ceea ce înseamnă $x=6n, n\in\mathbb{Z}\Rightarrow x\in 6\mathbb{Z}$. De aici $2\mathbb{Z}\cap 3\mathbb{Z}\subseteq 6\mathbb{Z}$, (1). Din $x\in 6\mathbb{Z}\Rightarrow$ $\Rightarrow x=6p, p\in\mathbb{Z}$. Cum $x=2(3p)\in 2\mathbb{Z}$ şi $x=3(2p)\in 3\mathbb{Z}$, deducem $x\in 2\mathbb{Z}\cap 3\mathbb{Z}\subseteq 6\mathbb{Z}$, (2). Din (1) şi (2) rezultă egalitatea.

Următoarea propoziție precizează că o **submulțime finită** a unui grup G devine subgrup cu operația indusă de pe G. Mai precis are loc

> **Teorema.** Fie $(G,\cdot)$ un grup şi H **o submulțime finită** a lui G. Următoarele afirmații sunt echivalente:
>
> **1)** H este subgrup al lui G;
>
> **2)** H este parte stabilă față de operația din G.

Demonstrație. Vom demonstra dubla implicație **1)** $\Rightarrow$ **2)** şi **2)** $\Rightarrow$ **1)**

1) $\Rightarrow$ **2)** este adevărată deoarece din H subgrup al lui G avem că $(\forall)x,y\in H\Rightarrow$ $\Rightarrow xy\in H$, ceea ce arată că H este parte stabilă față de operația din G.

2) $\Rightarrow$ **1)** Presupunem că H este parte stabilă față de operația din G, adică $(\forall)x,y\in H\Rightarrow$ $\Rightarrow xy\in H$.

Fie $H=\{x_1,x_2,x_3,...,x_n\}$. Mai avem de verificat a doua condiție ca H să fie subgrup, adică $(\forall)x\in H\Rightarrow x^{-1}\in H$.

Fie $x\in H$ un element arbitrar fixat. Atunci elementele (conform cu **2)**)

$xx_1, xx_2,....,xx_n\in H$. (1)

Mai mult, ele sunt distincte două câte două. Într-adevăr, dacă prin absurd $xx_i=xx_j$, $i\neq j$, atunci simplificând la stânga (în G) rezultă $x_i=x_j$, fals deoarece elementele din H sunt distincte două câte două. Aşadar H conține cele n elemente din (1). Cum H are exact n elemente, rezultă că elementele din (1) sunt chiar $x_1,x_2,...,x_n$ eventual în altă ordine. Deci există $1\le i\le n$ pentru care $xx_i=x$. De aici simplificând prin x (în G) se obține $x_i=e\in H$. În fine există $1\le j\le n$ pentru care $x\cdot x_j=e$, iar de aici $x_j=x^{-1}\in H$. ■

Exemple. 1. Subgrupurile finite cu n elemente ale grupului $(\mathbb{C}^*,\cdot)$ sunt grupurile de rădăcini ale unității $U_n, n\in N^*$. Arătați că singurele părți finite ale lui $\mathbb{C}^*$, stabile față de înmulțire sunt U_n, $n\in\mathbb{N}^*$. Se ia $x\in H$ şi se calculează $xx_1,...,xx_n\in H$, care sunt chiar $x_1,x_2,...x_n$ în altă ordine. Din $(xx_1)(xx_2)...(xx_n)=xx_1...x_n\Rightarrow x^n=1\Rightarrow x\in U_n$. Deci $H\subset U_n$. Cum H şi U_n au exact n elemente $\Rightarrow H=U_n$.

2. Grupul $(\mathbb{R}^*,\cdot)$ este infinit. Determinați o submulțime a lui $\mathbb{R}^*$ care este parte stabilă față de înmulțire, dar nu este subgrup al lui $(\mathbb{R}^*,\cdot)$. Se ia $H=\{x>1\}$ pentru care $x^{-1}=\dfrac{1}{x}\notin H$.

Pentru reguli de calcul într-un grup se adaugă:

> **Teorema.** Fie $(G,\cdot)$ un grup şi H un subgrup al lui G, $H \neq G$.
> Dacă $x \in H$, $y \in G - H$, atunci $xy, yx \in G - H$.

Demonstraţie. Fie $z = xy$. Presupunem, prin absurd că $z \in H$.
Din $z = xy$ rezultă $y = x^{-1}z$. Cum $x, z \in H$, rezultă $y \in H$, fals.
Analog se probează că $yx \in G - H$. ■

Exemplu. **$(\mathbb{Q},+)$ este subgrup al lui $(\mathbb{R},+)$. Dacă luăm $x = 3 \in \mathbb{Q}$ şi $y = \sqrt{3} \in \mathbb{R} - \mathbb{Q}$, atunci (conform teoremei) $x + y = 3 + \sqrt{3} \in \mathbb{R} - \mathbb{Q}$.**
Dacă luăm $x, y \in \mathbb{R} - \mathbb{Q}$, atunci $x + y$ poate fi atât în $\mathbb{Q}$ cât şi $\mathbb{R} - \mathbb{Q}$, după cum arată exemplele de mai jos: $x = 1 + \sqrt{2}$, $y = 1 - \sqrt{2} \in \mathbb{R} - \mathbb{Q}$ şi $x + y = 2 \in \mathbb{Q}$;
$x = \sqrt{3}$, $y = \sqrt{2}$, $x, y \in \mathbb{R} - \mathbb{Q}$ şi $x + y = \sqrt{3} + \sqrt{2} \in \mathbb{R} - \mathbb{Q}$.

Exemple remarcabile de subgrupuri

1) Subgrupurile grupului aditiv ale numerelor întregi

Să considerăm grupul aditiv al numerelor întregi $(\mathbb{Z},+)$. Dorim să determinăm subgrupurile acestui grup. Rezultatul este furnizat de următoarea:

> **Teoremă.** Fie H o submulţime nevidă a lui $\mathbb{Z}$. Atunci H este subgrup al lui $\mathbb{Z}$, dacă şi numai dacă există $n \in \mathbb{N}$ astfel încât $H = n\mathbb{Z}$.

Demonstraţie. Am văzut mai sus că dacă $H = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$, atunci H este subgrup al lui $\mathbb{Z}$.
Reciproc, dacă H este subgrup al lui $\mathbb{Z}$ să probăm existenţa lui $n \in \mathbb{N}$ pentru care $H = n\mathbb{Z}$.
Analizăm două cazuri:
a) Dacă $H = \{0\}$, atunci evident $n = 0$, când $H = 0\mathbb{Z} = \{0\}$.
b) Dacă $H \neq \{0\}$, atunci există în H elemente nenule.
Fie $m \in H$, $m \neq 0$. Cum H este subgrup, atunci şi $-m \in H$. Dar $m, -m \in \mathbb{Z}$ şi sunt nenule. Deci cel puţin unul este număr natural nenul. Fie n cel mai mic număr natural nenul aparţinând lui H. Să arătăm că atunci $H = n\mathbb{Z}$. Vom proceda prin dubla incluziune.
Fie deci $x \in n\mathbb{Z}$. Atunci $x = nk$, $k \in \mathbb{Z}$ sau $x = \underbrace{n + n + ... + n}_{k} \in H$ deoarece $n \in H$.
Aşadar $n\mathbb{Z} \subset H$, (1).
Fie acum $x \in H$. Conform teoremei împărţirii cu rest pe $\mathbb{Z}$, există $q, r \in \mathbb{Z}$ astfel încât $x = nq + r$, $0 \le r < n$. De aici $r = x - nq \in H$ pentru că $x, nq \in H$. Cum n a fost

cel mai mic număr natural nenul din H, iar $0 \le r < n$, $r \in H$, atunci neapărat $r = 0$, adică $x = nq$ şi deci $x \in n\mathbb{Z}$.
În fine pentru $x \in H$, am găsit $x \in n\mathbb{Z}$, adică $H \subset n\mathbb{Z}$, (2).
Din (1) şi (2) rezultă $H = n\mathbb{Z}$.■
Observație. Deduceți de aici că singurul subgrup finit al lui $(\mathbb{Z},+)$ este $H = \{0\}$.

2) Subgrup generat de un element. Grup ciclic

Fie $(G,\cdot)$ un grup şi $x \in G$.
Subgrupul generat de x se notează **<** x **>** şi are ca elemente puterile întregi ale lui x $\ldots, x^{-2}, x^{-1}, e = x^0, x, x^2, \ldots$ şi este numit **grup ciclic generat** de x. Aşadar

$$\boxed{< x >= \{x^k | k \in \mathbb{Z}\}}$$

Definiție. Grupul G se numeşte **ciclic** dacă este generat de un element al său. Acest element se numeşte **generator** al grupului.

Observații. 1) Dacă G este un **grup aditiv** şi $x \in G$, atunci: $< x >= \{kx | k \in \mathbb{Z}\}$.
2) Orice grup ciclic este abelian pentru că orice două puteri întregi ale unui element comută. Reciproca este falsă (vezi grupul lui Klein, care este abelian dar nu este ciclic).

Exemple

1. Elementele $-1, 1 \in \mathbb{Z}$ (ca grup aditiv). Atunci $<-1>=\{k(-1) | k \in \mathbb{Z}\} = \{(-k)\cdot 1 | k \in \mathbb{Z}\} = \mathbb{Z}$, $< 1 >= \{k \cdot 1 | k \in \mathbb{Z}\} = \mathbb{Z}$, ceea ce arată că grupul aditiv al numerelor întregi este un grup ciclic generat de elementul –1 sau 1. Observăm că acest grup este infinit.
2. Grupul $(U_n,\cdot)$ al rădăcinilor de ordinul n ale unității este

$$U_n = \left\{ z_k \middle| z_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, k = \overline{0, n-1} \right\}.$$

Elementul $z_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ are proprietatea că $z_1^0 = 1$, $z_1^k = z_k$, $k = \overline{1, n-1}$, ceea ce arată că $U_n = \{z_1^k | k = \overline{0, n-1}\}$, adică este grup ciclic finit de ordin n, generat de z_1.

3. Dacă luăm grupul $(\mathbb{C}^*,\cdot)$ atunci $< i >= \{i^k | k \in \mathbb{Z}\} = \{-i, i, 1, -1\}$ este un subgrup ciclic de ordin 4, generat de unitatea imaginară.
4. Grupul claselor de resturi modulo n cu adunarea $(\mathbb{Z}_n,+)$ este ciclic deoarece $\mathbb{Z}_n =< \hat{1} >=$ $= \{k \cdot \hat{1} | k \in \mathbb{Z}\}$. Mai mult este un grup ciclic finit, de ordin n. Arătați că pentru grupul $(\mathbb{Z}_6,+)$, avem $\mathbb{Z}_6 =< \hat{1} >=< \hat{5} >$.
5. Grupul cuaternionilor $(G = \{\pm 1, \pm i, \pm j, \pm k\},\cdot)$ nu este ciclic, dar are subgrupul ciclic $< i >= \{\pm 1, \pm i\}$.

Probleme rezolvate

1. Fie $(\mathbb{C}^*,\cdot)$ grupul multiplicativ al numerelor complexe nenule, ε o rădăcină a ecuației $x^2+x+1=0$ și $H=\{1,\varepsilon,\varepsilon^2\}$. Arătați că:

a) H este subgrup al grupului $(\mathbb{C}^*,\cdot)$

b) Orice subgrup cu trei elemente al grupului $(\mathbb{C}^*,\cdot)$ coincide cu H.

R. a) Știm că $H\subset\mathbb{C}^*$ este subgrup al lui $(\mathbb{C}^*,\cdot)$ dacă:

1) $(\forall)x,y\in H\Rightarrow xy\in H$; 2) $(\forall)x\in H\Rightarrow x^{-1}\in H$.

Din $\varepsilon^2+\varepsilon+1=0$ prin înmulțire cu $\varepsilon-1$ rezultă $\varepsilon^3=1$ și avem tabla legii pe H:

$\cdot$	1	ε	ε^2
1	1	ε	ε^2
ε	ε	ε^2	1
ε^2	ε^2	1	ε

Din tablă rezultă că 1) se verifică, iar din $1^{-1}=1,\ \varepsilon^{-1}=\varepsilon^2,\ \left(\varepsilon^2\right)^{-1}=\varepsilon$ se verifică și 2).

b) Fie $H'=\{1,a,b\}$ subgrup cu trei elemente al grupului $(\mathbb{C}^*,\cdot)$. Avem $a^2\neq 1$ (căci altfel a = 1, fals, iar dacă $a=-1$, atunci $b^2=1$ sau $b^2=-1$. Dacă $b^2=1$, atunci $b=\pm1$ și H' = {– 1, 1} are doar două elemente, iar pentru $b^2=-1$ rezultă $b=\pm i$ când $H'=\{\pm1,\pm i\}$ are patru elemente). La fel $a^2\neq a$. Rămâne $b=a^2$ și $a^3=1$. Deci $H'=\{1,a,a^2\}$ cu $a^3=1,\ a\neq 1$.

2. Pe mulțimea matricelor $\mathcal{M}_2(\mathbb{Z})$ se consideră operația de adunare și submulțimea $H=\left\{\begin{pmatrix}2a & 3b\\ 4c & 5d\end{pmatrix}\middle| a,b,c,d\in\mathbb{Z}\right\}$. Să se arate că H este subgrup al grupului $(\mathcal{M}_2(\mathbb{Z}),+)$.

R. Avem de verificat pentru H și operația de adunare cele două proprietăți:

1) $(\forall)A,B\in H\Rightarrow A+B\in H$;

2) $(\forall)A\in H\Rightarrow -A\in H$.

Pentru a demonstra 1) fie $A=\begin{pmatrix}2a_1 & 3b_1\\ 4c_1 & 5d_1\end{pmatrix}, B=\begin{pmatrix}2a_2 & 3b_2\\ 4c_2 & 5d_2\end{pmatrix}$, $a_i,b_i,c_i,d_i\in\mathbb{Z}$. Atunci $A+B=$

$=\begin{pmatrix}2(a_1+a_2) & 3(b_1+b_2)\\ 4(c_1+c_2) & 5(d_1+d_2)\end{pmatrix}\in H$ deoarece $a_1+a_2,b_1+b_2,c_1+c_2,d_1+d_2\in\mathbb{Z}$ și

$-A=\begin{pmatrix}2(-a_1) & 3(-b_1)\\ 4(-c_1) & 5(-d_1)\end{pmatrix}\in H$ pentru că $-a_1,-b_1,-c_1,-d_1\in\mathbb{Z}$.

3. Fie matricele $I_2=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, A=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, B=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}, C=\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}$ și mulțimea $G=\{I_2,A,B,C\}$.

1) Arătați că G cu operația de înmulțire a matricelor este subgrup al lui $(\mathcal{M}_2(\mathbb{R}),\cdot)$

2) Determinați subgrupurile grupului $(G,\cdot)$.

R. 1) Tabla legii este dată mai jos

$\cdot$	I_2	A	B	C
I_2	I_2	A	B	C
A	A	I_2	C	B
B	B	C	I_2	A
C	C	B	A	I_2

Verificăm cele două proprietăți ale subgrupului:

a) $(\forall)A,B\in G\Rightarrow AB\in G$ (din tabla operației această proprietate se verifică).

b) $(\forall)A\in G\Rightarrow A^{-1}\in G$. Avem $I_2^{-1}=I_2,\ A^{-1}=A,\ B^{-1}=B,\ C^{-1}=C$.

2) Din faptul că $A^2 = B^2 = C^2 = I_2$ şi $AB = C, BC = A, CA = B$ deducem că subgrupurile lui G sunt: $\{I_2\}, \{I_2, A\}, \{I_2, B\}, \{I_2, C\}$ şi $\{I_2, A, B, C\}$.

4. Fie $(G, \cdot)$ grup.

1) Să se arate că mulțimea $Z(G) = \{a \in G \mid ax = xa, (\forall) x \in G\}$ numită centrul grupului G este un subgrup al lui G.

2) Să se arate că $Z(G)$ este abelian.

3) Dacă $x, y \in G$, astfel încât $xy \in Z(G)$, atunci $xy = yx$.

4) Dacă $(G,.)$ este abelian, care este $Z(G)$?

R. 1) Să arătăm că dacă $a, b \in Z(G)$, atunci $ab \in Z(G)$.

Din $a, b \in Z(G) \Rightarrow ax = xa, by = yb, (\forall) x, y \in G$. Atunci avem: $(ab)x = a(bx) = a(xb) =$ $= (xa)b = x(ab)$ şi deci $ab \in Z(G)$.

Fie $a \in Z(G)$ şi să arătăm că $a^{-1} \in Z(G)$. Pentru $x \in G$ arbitrar avem: $ax^{-1} = x^{-1}a \Rightarrow$ $\Rightarrow \left(ax^{-1}\right)^{-1} = \left(x^{-1}a\right)^{-1} \Rightarrow xa^{-1} = a^{-1}x$, adică $a^{-1} \in Z(G)$. Prin urmare $Z(G)$ este subgrup al lui G.

2) Fie $a, b \in Z(G)$. Deci $ax = xa, (\forall) x \in G$. În particular pentru $x = b \in Z(G)$ rezultă $ab = ba$.

3) Fie $z = xy \in Z(G)$. Atunci $y = x^{-1}z$ şi $yx = \left(x^{-1}z\right)x = x^{-1}(zx) = x^{-1}(xz) = z = xy$.

4) Din cele de mai sus $Z(G) = G$.

Probleme propuse

0. Arătați că H este subgrup al lui G în raport cu operația $*$, unde:

a) $H = \left\{3^n \mid n \in \mathbb{Z}\right\}, G = \mathbb{Q}_+^*, * = \cdot$; **b)** $H = \left\{\hat{0}, \hat{2}, \hat{4}\right\}, G = \mathbb{Z}_6, * = +$;

c) $H = \left\{3a + 2bi \mid a, b \in \mathbb{Z}\right\}, G = \mathbb{Z}(i), * = +$; **d)** $H = \left\{\frac{2n}{5} \mid n \in \mathbb{Z}\right\}, G = \mathbb{Q}, * = +$;

e) $H = \left\{3^n 5^m \mid n, m \in \mathbb{Z}\right\}, G = \mathbb{Q}^*, * = \cdot$; **f)** $H = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}, G = \mathbb{R}, * = +$;

g) $H = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\right\}, G = \mathbb{R}, * = +$; **h)** $H = \left\{i^n \mid n \in \mathbb{Z}\right\}, G = \mathbb{C}^*, * = \cdot$;

i) $H = \left\{a + bi\sqrt{2} \mid a, b \in \mathbb{Z}\right\}, G = \mathbb{C}, * = +$; **j)** $H = \left\{f \in \mathbb{Q}[X] \mid f(\sqrt[3]{2}) = 0\right\}, G = \mathbb{Q}[X], * = +$;

k) $H = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}, a^2 - 2b^2 = 1\right\}, G = \mathbb{Q}^*, * = \cdot$;

l) $H = \left\{\begin{pmatrix} a & b \\ 3a & b \end{pmatrix} \middle| a, b \in \mathbb{Q}, a^2 - 3b^2 = 1\right\}, G = \mathcal{M}_2(\mathbb{Q}), * = \cdot$

1. 1) Arătați că $H = \left\{z \in \mathbb{C} \mid |z| = 1\right\} \subset \mathbb{C}$ este un subgrup al lui $(\mathbb{C}^*, \cdot)$.

2) Determinai subgrupurile finite ale grupurilor: $\left(\mathbb{R}^*, \cdot\right), \left(\mathbb{R}_+^*, \cdot\right), \left(\mathbb{C}^*, \cdot\right)$.

2. 1) Să se arate că submulțimile de numere întregi $H_1 = \{4k_1 + 6k_2 \mid k_1, k_2 \in \mathbb{Z}\}, H_2 = \{3k_1 + 5k_2 \mid k_1, k_2 \in \mathbb{Z}\}$ împreună cu adunarea formează subgrupuri ale lui $(\mathbb{Z}, +)$.

2) Fie $(\mathbb{Z},+)$ grupul întregilor. Determinați o submulțime a lui $\mathbb{Z}$, parte stabilă în raport cu adunarea, dar care nu este subgrup al lui $\mathbb{Z}$.

3. Fie mulțimile: $H_1=\left\{\begin{pmatrix}0 & 0\\ a & a\end{pmatrix} \middle| a\in\mathbb{Z}\right\}$, $H_2=\left\{\begin{pmatrix}0 & a\\ 2b & 3c\end{pmatrix} \middle| a,b,c\in\mathbb{Z}\right\}$, $H_3=\left\{\begin{pmatrix}a & 2b\\ 3c & 4d\end{pmatrix} \middle| a,b,c,d\in\mathbb{Z}\right\}$.

Arătați că H_1, H_2, H_3 sunt subgrupuri ale lui $(\mathcal{M}_2(\mathbb{Z}),+)$.

4. 1) Să se arate că mulțimea $H=\left\{A_a=\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix} \middle| a\in\mathbb{R}\right\}$ este un subgrup al grupului matricelor inversabile din $\mathcal{M}_2(\mathbb{R})$, cu înmulțirea. Aceeași cerință și pentru mulțimile: $H_1=\left\{\begin{pmatrix}a & -b\\ b & a\end{pmatrix} \middle| a^2+b^2=1\right\}$,

$H_2=\left\{\begin{pmatrix}1 & a\\ 0 & b\end{pmatrix} \middle| b\neq 0\right\}$, $H_3=\left\{I_2, \begin{pmatrix}1 & 0\\ -1 & -1\end{pmatrix}, \begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}, \begin{pmatrix}-1 & -1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}-1 & -1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right\}$.

2) Fie grupul $\left(G=\left\{A\in\mathcal{M}_2(\mathbb{C}) \middle| \det(A)\neq 0\right\},\ \cdot\right)$. Arătați că $H\subset G$ este subgrup în raport cu înmulțirea matricelor în cazurile:

a) $H=\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\right\}$; b) $H=\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}, \begin{pmatrix}-i & 0\\ 0 & i\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\right\}$

3) Fie $M=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix} \middle| ad\neq 0\right\}$ pe care definim legea $*$ astfel: $\begin{pmatrix}a & b\\ c & d\end{pmatrix}*\begin{pmatrix}x & y\\ z & t\end{pmatrix}=\begin{pmatrix}ax & b+ay\\ c+dz & dt\end{pmatrix}$.

Arătați că $(M,*)$ este grup necomutativ, iar $M'=\left\{\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix} \middle| ab\neq 0\right\}$ este subgrup al lui M.

5. Fie mulțimile $H_1=\{A\in\mathcal{M}_n(\mathbb{C}) \mid {}^tA=A\}$, $H_2=\{A\in\mathcal{M}_n(\mathbb{C}) \mid {}^tA=-A\}$. Arătați că $(H_1,+)$, $(H_2,+)$ sunt subgrupuri ale lui $(\mathcal{M}_n(\mathbb{C}),+)$.

6. Fie $G=\{e,\sigma_1,\sigma_2,\sigma_3\}$ unde $e=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{pmatrix}$, $\sigma_1=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 2 & 1\end{pmatrix}$, $\sigma_2=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}$, $\sigma_3=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 4 & 1 & 2\end{pmatrix}$.

Arătați că operația de compunere (înmulțire) a permutărilor determină pe G o structură de grup abelian. Stabiliți subgrupurile grupului G.

7. Fie S_4 grupul permutărilor mulțimii $\{1, 2, 3, 4\}$ și fie $H\subset S_4$ mulțimea formată din permutările ce lasă neschimbat elementul 4. Arătați că H este subgrup al lui $(S_4,\circ)$.

8. Să se arate că dacă subgrupul H al lui S_4 conține transpozițiile (12), (13), (14), atunci $H=S_4$.

9. Fie funcția $f:\mathbb{R}\to\mathbb{R}$, cu proprietatea că există $p\in\mathbb{R},\ p>0$ astfel încât $f(x+p)=f(x), (\forall)x\in\mathbb{R}$.

Notăm $P=\{p'\in\mathbb{R} \mid f(x+p')=f(x), (\forall)x\in\mathbb{R}\}$. Să se arate că $P\subset\mathbb{R}$ este un subgrup al lui $(\mathbb{R},+)$.

10. Să se arate că: a) $3\mathbb{Z}\cap 4\mathbb{Z}=12\mathbb{Z}$; b) $4\mathbb{Z}\cap 6\mathbb{Z}=12\mathbb{Z}$; c) $m\mathbb{Z}\cap n\mathbb{Z}=[m,n]\mathbb{Z}$, unde $[m,n]=$ c.m.m.m.c.(m,n).

11. Să se arate că dacă: $\mathcal{C}(\mathbb{R})=\{f:\mathbb{R}\to\mathbb{R} \mid f \text{ continuă}\}$; $\mathcal{P}(\mathbb{R})=\{f:\mathbb{R}\to \mid f \text{ are primitive}\}$ atunci: $(\mathcal{C}(\mathbb{R}),+)$, $(\mathcal{P}(\mathbb{R}),+)$ sunt subgrupuri ale lui $(\mathcal{F}(\mathbb{R}),+)$.

12. **Pentru grupurile considerate stabiliți subgrupurile ciclice indicate:**

a) $(G=\{\pm1,\pm i\},.), <1>, <-1>, <i>$ **; b)** $(\mathbb{Z}_{16},+), <\hat{6}>$ **; c)** $(\mathbb{Z}_5^*,\cdot), <\hat{2}><\hat{3}>$ **;**

d) $(G=\{A\in\mathcal{M}_2(\mathbb{R}) \mid \det(A)\neq 0\},\cdot)$, $<A>$ **unde** $A=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, $<A>$ **unde** $A=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$**;**

e) $(G=\mathcal{M}_2(\mathbb{Z}_5),+), <A>$ **, unde** $A=\begin{pmatrix}\hat{2} & \hat{0}\\ \hat{0} & \hat{3}\end{pmatrix}$ **și respectiv** $A=\begin{pmatrix}\hat{0} & \hat{1}\\ \hat{2} & \hat{4}\end{pmatrix}$.

13. **Fie** $(G,\cdot)$ **un grup comutativ și** $H=\{x\in G \mid (\exists)k\in\mathbb{Z},\, x^k=e\}$. **Arătați că** H **este subgrup al lui** G**.**

14. **Fie** $(G,\cdot)$ **un grup abelian și** H_1,H_2 **două subgrupuri ale lui** G**.**

Să se arate că mulțimea $H=H_1\cdot H_2=\{h_1h_2 \mid h_1\in H_1,\, h_2\in H_2\}$ **este subgrup al lui** G**.**

15. **Fie** H **un subgrup al grupului** G **și** $a\in G$ **un element oarecare. Să se arate că mulțimea** $aHa^{-1}=\{aha^{-1} \mid h\in H\}$ **este un subgrup al lui** G**. În ce caz** $aHa^{-1}=H$ **?**

16*. **Fie** S_n **grupul permutărilor de** n **elemente și** $A_n\subset S_n$ **mulțimea permutărilor pare de** n **elemente. Determinați** $Z(A_n)$ **iar pentru** $n\geq 3$ **arătați că** $Z(S_n)=\{e\}$**.**

17. **Fie** G **un grup și** H**,** K **două subgrupuri ale lui** G**. Să se demonstreze că** $H\cup K$ **este subgrup dacă și numai dacă** $H\subset K$ **sau** $K\subset H$**.**

18. **Pe G = [0,1) definim legea de compoziție** $x*y=\{x+y\}$**, unde** $\{a\}$ **reprezintă partea fracționară a numărului real** a**. Să se arate că:**

a) $(G,*)$ **este grup abelian;**

b) $\left(G_5=\left\{0,\frac{1}{5},\frac{2}{5},\frac{3}{5},\frac{4}{5}\right\},*\right)$ **este subgrup al lui** G**.**

1.5. GRUPURI FINITE

Tabla operației

Un grup finit G, format din elementele $g_1,g_2,...,g_n$ poate fi descris cu ajutorul tablei lui Cayley. Aceasta este o tabelă pătrată în care la intersecția liniei i cu coloana j se află elementul g_ig_j. De exemplu, dacă ordinul grupului este 2 și grupul este format din elementele e (unitatea) și $g\neq e$, atunci g^2 poate fi egal doar cu e (în caz contrar $g^2=g\Rightarrow g=e$!). De aceea tabla lui Cayley are forma:

$\cdot$	e	g
e	e	g
g	g	e.

Dacă ordinul grupului este 3, e este elementul unitate al său iar $g \neq e$, atunci se constată uşor că $g^2 \neq g$ şi $g^2 \neq e$, de aceea G = $\{e, g, h\}$ cu $g^2 = h$. La fel de simplu se arată că gh = e. Tabla lui Cayley are forma:

$\cdot$	e	g	h
e	e	g	h
g	g	h	e
h	h	e	g

Din tabla grupului se poate deduce comutativitatea lui (dacă tabla este simetrică în raport cu diagonala principală); **se poate determina elementul unitate, inversul pentru fiecare element al grupului. Existența unui izomorfism între două grupuri** (aşa cum apare la izomorfisme de grupuri) **înseamnă că** (abstracție făcând de notațiile elementelor) **tablele Cayley corespunzătoare lor coincid**. Tablele Cayley pot fi scrise efectiv doar pentru grupuri cu ordinul mic.

În cazul grupului multiplicativ finit cu *n* elemente, $G = \{x_1, x_2, ..., x_n\}$ în tabla legii (Cayley) **pe fiecare linie sau coloană, fiecare element al lui *G* apare o dată şi numai o singură dată.**

Într-adevăr fie $x_i \in G$, fixat $i \in \{1, 2, ..., n\}$. În linia lui x_i din tabla operației se găsesc elementele: $x_i x_1, x_i x_2, ..., x_i x_n$.

Pentru $k \neq l$ avem $x_i x_k \neq x_i x_l$. În caz contrar din $x_i x_k = x_i x_l$ prin compunere la stânga cu x_i^{-1} ar rezulta $x_k = x_l$, fals.

Aşadar elementele $x_i x_1, x_i x_2, ..., x_i x_n$ sunt distincte două câte două şi în plus sunt în *G*. Cum *G* are exact *n* elemente înseamnă că $G = \{x_i x_1, x_i x_2, ..., x_i x_n\}$, altfel spus aceste elemente sunt chiar $x_1, x_2, ..., x_n$ eventual în altă ordine.

Exemple remarcabile de grupuri finite

1) Grupul rădăcinilor de ordin *n* ale unității

Fie $n \in \mathbb{N}^*$ şi $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ mulțimea rădăcinilor de ordinul *n* ale unității. Se ştie că acestea sunt date de relația $z_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$, $k = 0, 1, ..., n-1$.

Pe U_n considerăm operația de înmulțire de pe $\mathbb{C}$.

Are loc următoarea:

> **Teoremă.** Cuplul $(U_n, \cdot)$ este grup abelian finit, numit grupul **rădăcinilor de ordin** *n* **ale unității**.

Demonstrație. Verificăm axiomele grupului.

G$_1$) Înmulțirea de pe $\mathbb{C}$ este **lege de compoziție** pe U_n, adică să arătăm că $(\forall) z_k, z_l \in U_n \Rightarrow z_k \cdot z_l \in U_n$.

Avem $(z_k z_l)^n = z_k^n \cdot z_l^n = 1 \cdot 1 = 1$.

G$_2$) **Asociativitatea înmulțirii** are loc, deoarece înmulțirea pe $\mathbb{C}$ este asociativă.

G$_3$) **Elementul neutru**. Cum 1 este element neutru pentru înmulțirea de pe $\mathbb{C}$ și $1 \in U_n$ (pentru $k = 0,\ z_0 = 1$) se deduce că 1 este element unitate și față de înmulțirea de pe U_n.

G$_4$) **Elemente inverse** (simetrizabile). Pentru $x \in U_n$, există $x' \in U_n$ astfel încât $xx' = 1 = x'x$. De aici $x' = \frac{1}{x} \in U_n$ deoarece $\left(\frac{1}{x}\right)^n = \frac{1}{x^n} = \frac{1}{1} = 1$, ceea ce arată că inversul lui *x* din U_n (adică $\frac{1}{x}$) se menține în U_n.

G$_5$) **Comutativitatea înmulțirii** are loc pe U_n deoarece înmulțirea este comutativă pe $\mathbb{C}$.

Observație. Elementele lui U_n au ca imagini geometrice în plan vârfurile unui poligon regulat cu *n* laturi înscris în cercul unitate.

În Fig. 5 avem ilustrate cazurile *n* = 3, *n* = 4.

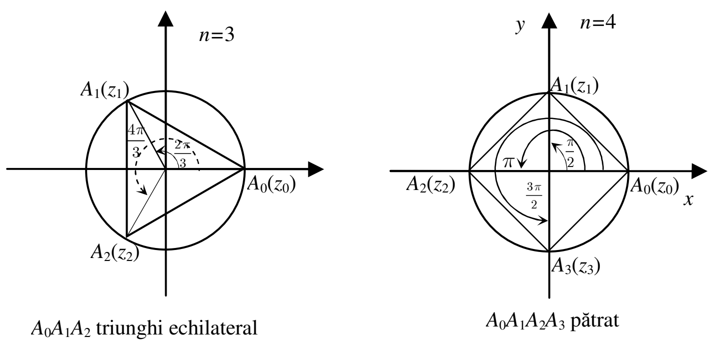


Fig. 5

2) Grupul lui Klein

Fie planul $\mathcal{P} = \mathbb{R} \times \mathbb{R}$ în care avem reperul cartezian *xOy*. Considerăm următoarele transformări geometrice ale planului.

1) $i: \mathcal{P} \to \mathcal{P},\ M(x, y) \to M(x, y)$

$i((x, y)) = (x, y)$, aplicația identică a planului.

2) $s_x : \mathcal{P} \to \mathcal{P}$, $M(x,y) \to M'(x,-y) =$ simetricul lui M în raport cu Ox (Fig. 6),
$s_x((x,y)) = (x,-y)$, s_x este simetria în raport cu Ox.

3) $s_y : \mathcal{P} \to \mathcal{P}$, $M(x,y) \to M''(-x,y)$
$s_y((x,y)) = (-x,y)$, s_y este simetria în raport cu Oy.

4) $s_O : \mathcal{P} \to \mathcal{P}$, $M(x,y) \to M'''(-x,-y)$, $s_O((x,y)) = (-x,-y)$, s_O este simetria în raport cu O.

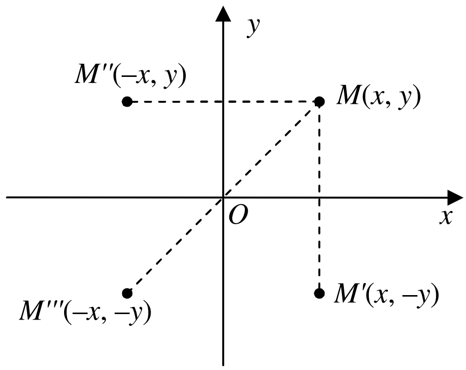


Fig. 6

Notăm prin $\mathcal{K} = \{i, s_x, s_y, s_O\}$ şi considerăm operaţia de compunere a funcţiilor pe $\mathcal{K}$.
Atunci are loc următorul rezultat:

Teoremă. Cuplul $(\mathcal{K}, \circ)$ este un grup abelian, numit **grupul lui Klein**.

Demonstraţie. Tabla operaţiei este dată alăturat.
Verificăm axiomele grupului comutativ.

$\circ$	i	s_x	s_y	s_O
i	i	s_x	s_y	s_O
s_x	s_x	i	s_O	s_y
s_y	s_y	s_O	i	s_x
s_O	s_O	s_y	s_x	i

G_1) **Asociativitatea compunerii**. Întotdeauna compunerea funcţiilor este asociativă, deci este la fel şi în acest caz particular.
G_2) **Elementul neutru** este funcţia identică a planului, i.
G_3) **Elemente inversabile**. Avem imediat (din tabla legii) $i^{-1} = i$, $s_x^{-1} = s_x$, $s_y^{-1} = s_y$, $s_O^{-1} = s_O$.
G_4) **Comutativitatea compunerii** rezultă din faptul că tabla legii este simetrică faţă de diagonala principală.
Aşadar cuplul $(\mathcal{K}, \circ)$ este un grup abelian, având ordinul 4.

Observaţii. 1) Mai general considerăm mulţimea $K = \{e, a, b, c\}$ pe care definim o operaţie multiplicativă dată de tabla alăturată. Atunci $(K, \cdot)$ este grupul lui Klein. Observăm că într-un astfel de grup avem: $a^2 = b^2 = c^2 = e$, $ab = ba = c$, $ac = ca = b$, $bc = cb = a$.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

2) Dacă se consideră G = $\{e, a, b, c\}$ împreună cu o lege multiplicativă dată de tabla alăturată atunci se constată că $(G, \cdot)$ este un grup tot de ordin 4. Numai că în acest caz observăm că $a^2 = b$, $a^3 = c$ şi $a^4 = e$, adică elementele acestui grup sunt generate de elementul a.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Deci $G=\{e,a,a^2,a^3\}$ şi se numeşte **grup ciclic generat** de elementul *a*.

3) Se poate demonstra că nu există decât două grupuri diferite de ordin 4. Altfel spus, nu există decât două moduri de a aranja cele patru elemente *e, a, b, c* în tabla legii „·" astfel încât $(G,\cdot)$ să fie grup. Primul mod generează grupul lui Klein, iar cel de-al doilea mod din **2)** furnizează grupul ciclic de ordin 4.

4) Determinaţi $C(g),\ g\in K$.

3) Grupul de simetrii ale triunghiului echilateral

Printr-o **mişcare rigidă** a triunghiului înțelegem o bijecție de la mulțimea punctelor triunghiului (de pe cele trei laturi ale sale) pe ea însăşi care păstrează distanța între orice două puncte ale sale. O astfel de mişcare trebuie să ducă un vârf pe un alt vârf al triunghiului şi întreaga aplicație este determinată de imaginile vârfurilor *A*, *B*, *C*. Aceste mişcări rigide se numesc **simetrii**, care împreună cu operația de compunere formează grup.

Fie mulțimea $E=\{A,B,C\}$ a vârfurilor unui triunghi echilateral *ABC*. Notăm cu l_1, l_2, l_3 mediatoarele laturilor triunghiului echilateral care trec prin *A*, *B* şi respectiv *C* şi cu *O* punctul de intersecție al mediatoarelor (Fig. 7).

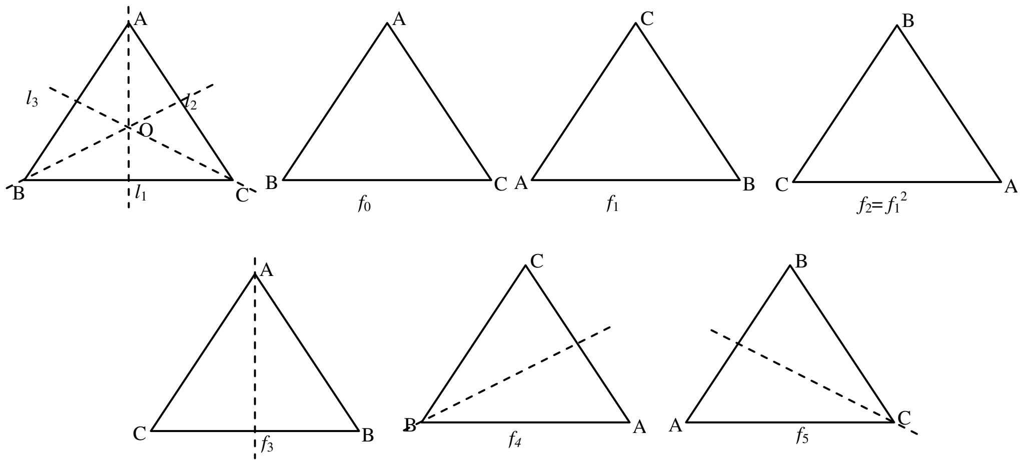


Fig. 7

Considerăm mulțimea: $S=\{f_0,f_1,f_2,f_3,f_4,f_5\},\ f_i:E\to E,\ i=\overline{0,5}$, f_i bijecții definite astfel:

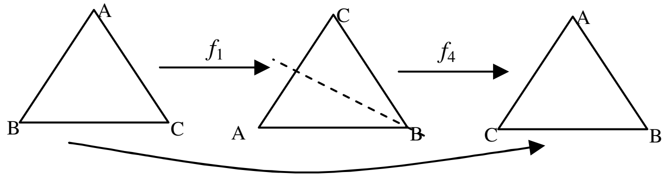
- $f_0(A)=A,\ f_0(B)=B,\ f_0(C)=C$

(f_0 aplicația identică a lui *E* lasă punctele neschimbate);

- $f_1(A)=B,\ f_1(B)=C,\ f_1(C)=A$ (f_1 este rotația de unghi 120^0 în sens trigonometric în jurul lui *O*);

• $f_2(A)=C,\ f_2(B)=A,\ f_2(C)=B$ (f_2 este rotația de unghi 240^0 în sens trigonometric în jurul lui O);
• $f_3(A)=A,\ f_3(B)=C,\ f_3(C)=B$ (f_3 este simetria în raport cu mediatoarea l_1);
• $f_4(A)=C,\ f_4(B)=B,\ f_4(C)=A$ (f_4 este simetria în raport cu mediatoarea l_2);
• $f_5(A)=B,\ f_5(B)=A,\ f_5(C)=C$ (f_5 este simetria în raport cu mediatoarea l_3);.
Compunând elementele două câte două obținem tabla:

$\circ$	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_2	f_0	f_4	f_5	f_3
f_2	f_2	f_0	f_1	f_5	f_3	f_4
f_3	f_3	f_5	f_4	f_0	f_2	f_1
f_4	f_4	f_3	f_5	f_1	f_0	f_2
f_5	f_5	f_4	f_3	f_2	f_1	f_0



$f_4 \circ f_1 = f_3$
Fig. 8

Teoremă. Cuplul $(S,\circ)$ este un grup de ordin 6 şi se numeşte **grupul de simetrii ale triunghiului echilateral.**

Demonstrație. Verificăm axiomele grupului.
G$_1$) **Asociativitatea compunerii** are loc deoarece întotdeauna compunerea funcțiilor are această calitate.
G$_2$) **Elementul neutru** este aplicația identică f_0.
G$_3$) **Elemente inverse**. Avem $f_0^{-1}=f_0,\ f_1^{-1}=f_2,\ f_2^{-1}=f_1,\ f_3^{-1}=f_3,\ f_4^{-1}=f_4,\ f_5^{-1}=f_5$.
Observații. **1)** Grupul nu este abelian deoarece, de exemplu $f_2\circ f_5=f_4\neq f_5\circ f_2=f_3$.
2) Se poate asocia, în acelaşi mod, un grup D_n, numit **grup diedral**, la fiecare poligon regulat cu n laturi; se demonstrează că el are ordinul $2n$.
3) Arătați că $H=\{f_0,f_1,f_2\}$ este subgrup al grupului $(S,\circ)$, iar $S=\left\{f_0,f_1,f_1^2,f_3,\right.$ $\left.f_3\circ f_1,f_3\circ f_1^2\right\}$, ultimele trei elemente având ordinul 2, iar f_1,f_1^2 au ordinul 3. De regulă, S se notează cu D_3 şi se numeşte **grupul diedral** cu 6 elemente.
4) Dacă A, B, C le identificăm prin 1, 2, 3, atunci asociați fiecărei funcții o permutare din S_3. De exemplu: $f_0\rightarrow e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $f_1\rightarrow \sigma=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$.
5) Asociați pătratului de vârfuri 1, 2, 3, 4 şi axe de simetrie d_1,d_2,l_1,l_2 (Fig. 9) grupul de simetrii (numit **grupul octic**) şi realizați tabla operației. Scrieți simetriile ca permutări din S_4.

Arătați că grupul octic $D_4 = \left\{I, R, R^2, R^3, S, RS, R^2S, R^3S\right\}$, unde I este aplicația identică, R este rotația de unghi 90^0, iar S este simetria față de diagonala AC a pătratului. Transformările $R^k S$ au ordinul 2 şi sunt simetrii în raport cu „diametrele“ ce trec prin vârfurile poligonului (aici diagonalele pătratului d_1, d_2) sau în raport cu mediatoarele laturilor $\left(l_1, l_2\right)$. Verificați că $R^4 = S^2 = I$, $SR = R^3S$.

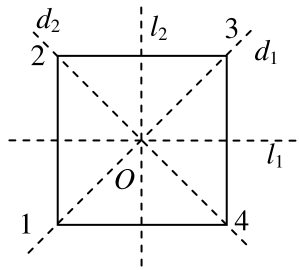


Fig. 9

Aplicații în diverse domenii

Noțiunea de grup a apărut mai întâi sub forma noțiunii de grup de permutări (transformări) şi tot în această formă se întâlneşte aproape întotdeauna în matematică şi în fizica matematică. Transformările bijective ale spațiului euclidian ce păstrează distanța între puncte formează grupul izometriilor spațiului. Dacă toate păstrează fix un acelaşi punct al spațiului, atunci avem de-a face cu grupul transformărilor ortogonale. Grupul format din transformările ce păstrează (invariază) un obiect poate fi interpretat ca fiind grupul simetriilor sale. Faptul că un triunghi este neisoscel (oarecare), este isoscel şi nu este echilateral, sau este echilateral, se poate „măsura“ prin grupul izometriilor planului ce invariază triunghiul. În primul caz acest grup este format doar din transformarea identică, în al doilea caz apare şi o simetrie față de o dreaptă (axa de simetrie a triunghiului), iar în al treilea caz grupul este format din următoarele şase transformări: cea identică, rotațiile de unghi 120^0 sau 240^0 în jurul centrului O al triunghiului, şi simetriile în raport cu cele trei axe (cele trei mediatoare ale triunghiului).

Prin **simetrie a unei molecule** se înțelege o transformare a spațiului ce transformă fiecare atom al moleculei într-un atom de acelaşi tip, păstrând totodată valențele între atomi. Astfel o moleculă de fosfor este formată din patru atomi, repartizați în vârf urile unui tetraedru regulat, iar grupul simetriilor ei coincide cu grupul simetriilor tetraedrului regulat.

Grupul simetriilor unui cristal este una dintre caracteristicile importante ale cristalului. Aici prin simetrie se înțelege o transformare a spațiului, încât se păstrează poziția atomilor cristalului precum şi legăturile între atomi (deci transformând fiecare atom într-unul de acelaşi tip).

Simetriile intervin uneori şi în **fenomene fizice**. De exemplu, conform unei teoreme a lui E. Noether, dacă un sistem dinamic X este descris de funcția lui Lagrange $\mathcal{L}$ ce are ca grup de simetrii un grup de transformări depinzând de un parametru, atunci sistemul are o integrală care se descrie simplu. Astfel, în cazul mişcării unui sistem de puncte materiale, faptul că rămâne invariant față de translații conduce la legea de mişcare a centrului maselor, iar faptul că rămâne invariant faţă de rotaţii conduce la legea momentului cinetic.

Exemple clasice de grupuri finite de rotaţii ale spaţiului sunt legate de poliedrele regulate (cunoscute încă din antichitate, din care cauză se mai numesc şi corpuri platonice): fiecărui poliedru regulat M îi corespunde grupul G_M al tuturor transformărilor ce invariază poliedrul. „Regularitatea“ poliedrului se reflectă în faptul că el are multe simetrii. Fiecărui poliedru regulat îi este asociat un dual, ale cărui vârfuri sunt centrele feţelor poliedrului original. Evident, poliedrul dual are acelaşi grup G_M ca şi poliedrul M. Tetraedrul este autodual, cubul are ca dual octaedrul, iar dodecaedrul are ca dual icosaedrul. În acest fel se obţin trei grupuri ale poliedrelor regulate: cel al tetraedrului (notat cu **T**), cel al octaedrului (O) şi cel al icosaedrului (Y) pentru care $|T| = 12, |O| = 24, |Y| = 60$.

Grupurile poliedrelor regulate se întâlnesc în natură ca grupuri de simetrie ale moleculelor. De exemplu grupul de simetrie al moleculei $H_3C - CCl_3$ (Fig. 10.a)) este grupul rotaţiilor în jurul unui punct cu unghiuri $\frac{2k\pi}{3}, k = 0, 1, 2$.

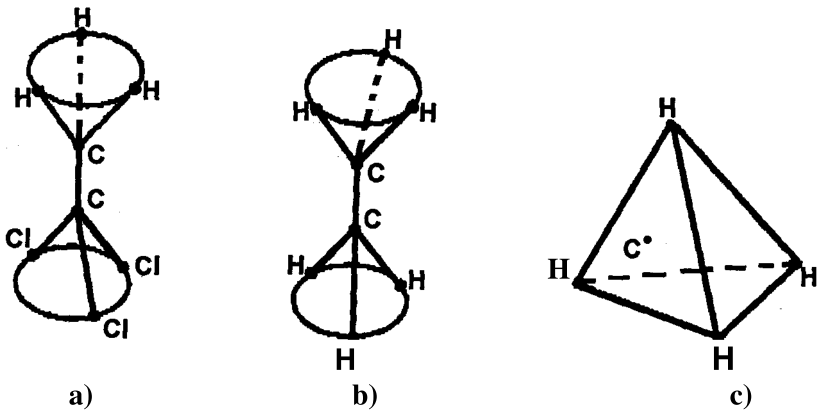


Fig. 10

Grupul de simetrie al moleculei C_2H_6 (Fig. 10.b)) este grupul triunghiului echilateral. Grupul moleculei de metan CH_4 (Fig. 10.c)) este grupul **T** (atomul C se află în centrul tetraedrului, iar atomii H în vârfuri).

Spre deosebire de cristale, grupurile de simetrie ale moleculelor nu conţin translaţii. Ele se mai numesc grupuri punctuale.

Forme de simetrie apar şi în muzică sau dans, ritmul fiind o repetare la intervale egale a unui motiv muzical.

Aplicaţii ale teoriei grupurilor le întâlnim la ornamente, în clasificarea scoarţelor, etc.

Ordinul unui element

Definiție. Fie $(G,\cdot)$ un grup și $x \in G$. Cel mai mic număr natural nenul $n \in N^*$ cu proprietatea $x^n = e$ se numește **ordinul elementului** x în grupul G. Dacă pentru orice $n \in N^*$, $x^n \neq e$, atunci se spune că ordinul elementului x este ∞.

Notație. Dacă n este ordinul elementului x, atunci notăm acest lucru prin ord(x) = n.
Observație. În orice grup ordinul unui element este egal cu ordinul inversului acestui element $\left(x^k = e \Leftrightarrow x^{-k} = e\right)$.

Exemple. 1. În grupul $(\{1,-1,i,-i\},\cdot)$ elementul –1 are ordinul 2 deoarece $(-1)^2 = 1$. Așadar ord(–1) = 2. Analog ord(i) = ord(–i) = 4. Atunci $i^{2006} = i^{4\cdot 501+2} = \left(i^4\right)^{501} \cdot i^2 = -1$.

2. În grupul $(\mathbb{Z}_5^*,\cdot)$ avem $\mathrm{ord}(\hat{2}) = 4$ pentru că $\hat{2}^4 = \hat{1}$, ord$(\hat{3}) = 4$, $(\hat{3}^4 = \hat{1})$, ord$(\hat{4}) = 2$, $(\hat{4}^2 = \hat{1})$.

Pentru a calcula $\hat{2}^{2007}$ utilizăm $\hat{2}^4 = \hat{1}$, când avem $\hat{2}^{2007} = \left(\hat{2}^4\right)^{501+3} = \left(\hat{2}^4\right)^{501} \cdot \hat{2}^3 = \hat{1} \cdot \hat{3} = \hat{3}$ (am folosit teorema împărțirii cu rest pentru 2007 și 4, $2007 = 4 \cdot 501 + 3$).

3. În grupul lui Klein $\mathcal{K} = \{i, s_x, s_y, s_0\}$ cum $s_x^2 = s_y^2 = s_0^2 = i$ rezultă $\mathrm{ord}(s_x) = \mathrm{ord}(s_y) = = \mathrm{ord}(s_0) = 2$.

4. Fie S_3 grupul permutărilor de grad 3 și $\sigma \in S_3$, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

Calculăm puterile lui σ și avem: $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\sigma^3 = \sigma^2 \cdot \sigma =$

$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$. Așadar ord(σ) = 3.

Pentru calculul permutării σ^{2008}, ținem seama de $\sigma^3 = e$ și $2008 = 3 \cdot 669 + 1$, când avem $\sigma^{2008} = \sigma^{3\cdot 669+1} = \left(\sigma^3\right)^{669} \cdot \sigma^1 = e\sigma = \sigma$.

Fie $(G,\cdot)$ un grup și $x \in G$. Atunci $\left\{x^k \middle| k \in \mathbb{Z}\right\} \overset{\text{not.}}{=} < x >$ cu operația „$\cdot$“ este grup, cum ușor se verifică (numit **grup ciclic generat de** x). Dacă grupul este aditiv, $(G,+)$, atunci $< x > = \left\{kx \middle| k \in \mathbb{Z}\right\}$.

Exemple. 1. Pentru $\left(\mathbb{Z}_5^*,\cdot\right), < \hat{2} > = \{\hat{1}, \hat{2}, \hat{2}^2, \hat{2}^3\} = \{\hat{1}, \hat{2}, \hat{3}, \hat{4}\}$, iar $< \hat{4} > = \{\hat{1}, \hat{4}\}$.

2. Pentru $(\mathbb{Z}_8,+), < \hat{2} > = \left\{\widehat{2k} \middle| k \in \mathbb{Z}\right\} = \{\hat{0}, \hat{2}, \hat{4}, \hat{6}\}$.

3. Pentru $(\mathbb{Z},+), < 1 > = < -1 > = \mathbb{Z}$.

Observație. Dacă $(G,\cdot)$ este grup, iar $H \subseteq G$ și $(H,\cdot)$ are structură de grup, atunci H se numește **subgrup al lui** G și se notează $H \leq G$.
În cazul de mai sus $< x >$ este subgrup al lui G și anume **subgrupul ciclic al lui** G.

Am văzut că pentru un element $x \in G$ subgrupul ciclic generat de x este $<x>=\{x^k \mid k \in \mathbb{Z}\}$.
Care este forma acestui sub grup dacă x are ordin finit?
Răspunsul este dat de:

> **Teoremă.** Cuplul $(G,\cdot)$ este un grup și $x \in G$ un element de ordin n.
> Atunci $< x >= \{e, x, x^2, ..., x^{n-1}\}$ și $\text{ord}(< x >) = n$.

Demonstrație. Egalitatea de mulțimi o vom demonstra prin dubla incluziune. Este clar că $\{e, x, ..., x^{n-1}\} \subset < x >$, (1).

Fie acum $x^k \in < x >, k \in \mathbb{Z}$. Atunci din teorema împărțirii cu rest pe $\mathbb{Z}$ există $q, z \in \mathbb{Z}$, astfel încât $k = nq + r, 0 \leq r \leq n-1$.

Deci $x^k = x^{nq+r} = (x^n)^q \cdot x^r = e \cdot x^r = x^r \in \{e, x, ..., x^{n-1}\}$.

Așadar $< x > \subset \{e, x, ..., x^{n-1}\}$ (2). Din (1) și (2) rezultă egalitatea. Este clar că elementele $x^i, x^j, 1 \leq i < j \leq n-1$ sunt distincte, căci altfel $x^i = x^j$ ar da $x^{j-i} = e$ și $j - i < n$, în contradicție cu ord(x) = n .■

Observație. Teorema afirmă că dacă $x \in G$ este un element de ordin *n,* atunci subgrupul ciclic generat de x are tot ordinul *n.*

Exemple. Le examinăm pe cele prezentate la ordinul unui element.

1. Subgrupul $\{-i, i, 1, -1\}$ al lui $(\mathbb{C}^*, \cdot)$

Pentru $x = -i$, ord$(-i) = 4$ și deci $< -i >= \{1, -i, (-i)^2, (-i)^3\} = \{1, -i, -1, i\}$.

Pentru $x = i$, ord$(i) = 4$ când $< i >= \{1, i, i^2, i^3\} = \{1, i, -1, -i\}$. Pentru $x = -1$, ord(–1) = 2 când avem $< -1 >= \{1, (-1)^1\} = \{1, -1\}$.

2. În grupul $(\mathbb{Z}_5^*, \cdot)$ avem:

ord$(\hat{2}) = 4$ și deci $< \hat{2} >= \{\hat{1}, \hat{2}, \hat{2}^2, \hat{2}^3\} = \{\hat{1}, \hat{2}, \hat{4}, \hat{3}\}$;

ord$(\hat{4}) = 2$ când $< \hat{4} >= \{\hat{1}, \hat{4}\}$.

3. Grupul lui Klein $\mathcal{K} = \{i, s_x, s_y, s_o\}$

Pentru $x = s_x$, ord$(s_x) = 2$ și avem $< s_x >= \{i, s_x\}$.

Pentru $x = s_y$, ord$(s_y) = 2$ și deci $< s_y >= \{i, s_y\}$.

În fine $x = s_o$, ord$(s_o) = 2$ dă $< s_o >= \{i, s_o\}$.

4. Pentru grupul S_3 și $\sigma \in S_3, \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ cu ord$(\sigma) = 3$, avem: $< \sigma >= \{e, \sigma, \sigma^2\}$.

Probleme propuse

1. **Să se determine ordinul elementului** $A=\begin{pmatrix}\hat{1} & \hat{2}\\ \hat{0} & \hat{1}\end{pmatrix}$ **în grupul** $\left(G=\left\{\begin{pmatrix}\hat{1} & \hat{a}\\ \hat{0} & \hat{1}\end{pmatrix}\middle| a\in\mathbb{Z}_8\right\},\cdot\right)$ **şi** A^{2007}.

2. **a) Să se determine subgrupul generat de elementul** $\hat{2}$ **în grupul** $(\mathbb{Z}_{12},+)$.

b) Să se determine subgrupul generat de elementul i **în grupul** $(U_4,\cdot)$.

3. **Fie** $G=\left\{A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\middle| \det A=1\right\}$. **Arătaţi că:**

a) $(G,\cdot)$ **este grup; b) dacă** $A=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$, $B=\begin{pmatrix}1 & 1\\ -1 & 0\end{pmatrix}$, **atunci ord($A$) = 4, ord($B$) = 6 şi** $\text{ord}(AB)=\infty$. **Calculaţi** A^{2007}, B^{2008}.

4. **Să se verifice ordinele elementelor pentru fiecare caz în parte: 1)** $\text{ord}(\sigma)=3$, **unde** $\sigma=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$ **şi** $\text{ord}(\delta)=2, \delta=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$; **Calculaţi** σ^{2007}, δ^{2008};

2) $\text{ord}(P_1)=2$, **unde** $P_1=\begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{pmatrix}$; $\text{ord}(P_5)=3$, **unde** $P_5=\begin{pmatrix}0 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}$, **cu înmulţirea matricelor; calculaţi** P_1^{2007}, P_5^{2008}.

Excursie matematică (facultativ)

* * * * *

Teorema lui Lagrange. Consecinţe. Aplicaţii

Următorul rezultat fundamental pentru grupurile finite se referă la relaţia dintre ordinul oricărui subgrup al său şi ordinul grupului. Mai precis are loc

> ***Teorema lui Lagrange***. *Ordinul oricărui subgrup al unui grup finit este un divizor al ordinului grupului.*

> ***Corolar***. *Într-un grup finit, ordinul oricărui element este finit şi este un divizor al ordinului grupului.*

Demonstraţie. *Fie* $(G,\cdot)$ *un grup de ordin n şi* $x\in G$. *Ordinul elementului x nu poate fi infinit, deoarece subgrupul ciclic generat de el < x > ar avea ordinul infinit, absurd pentru că < x > este subgrup al unui grup finit. Deci ord(x) = k. Atunci s-a văzut că < x > are ordinul tot k, iar din teorema lui Lagrange k divide pe n.* ■

Corolar. *Fie $(G,\cdot)$ grup finit de ordin n. Atunci*

$$x^n = e, (\forall) x \in G .$$

Demonstrație. *Fie* $x \in G$ *cu ord(x) = k divizor al lui n. Deci* $n = kp,\ p \in N^*$ *când* $x^n = \left(x^k\right)^p = e^p = e$. ■

Corolar. *Orice grup de ordin un număr prim este ciclic.*

Demonstrație. *Fie* $(G,\cdot)$ *grup cu ord(G) = p, p număr prim. Cum* $p \geq 2$ *se poate alege* $x \in G, x \neq e$. *Subgrupul ciclic generat de x, <x> are* $\mathrm{ord}(<x>) = k \geq 2\ (x, e \in <x>)$. *Din teorema lui Lagrange k îl divide pe p. Cum p este prim rezultă k = p. Aşadar <x>= G, ceea ce arată că G este ciclic.* ■

PIONIERI AI MATEMATICII	
J.L. LAGRANGE (1736–1813) **Matematician francez**	**L. EULER (1707-1783)** **Matematician elvețian**
	
CONTRIBUȚII	**CONTRIBUȚII**
• ***analiză*** • ***mecanică analitică*** • ***probabilități*** • ***teoria numerelor***	• ***toate domeniile matematicii***

Următoarele două rezultate au aplicații importante în teoria numerelor.

Teorema lui Euler. *Fie* $n \in \mathbb{N},\ n \geq 2,\ a \in \mathbb{Z},\ (a,n) = 1$.

Atunci $$a^{\varphi(n)} \equiv 1 (\bmod n),$$

unde φ *este indicatorul lui Euler.*

Demonstrație. *Fie grupul multiplicativ $U(\mathbb{Z}_n)$ al elementelor inversabile din monoidul $(\mathbb{Z}_n,\cdot)$. Am văzut că ordinul acestui grup este $\varphi(n)$ (=numărul de numere mai mici decât n, prime cu n). Din (a, n) = 1 rezultă $\hat{a}\in U(\mathbb{Z}_n)$. Atunci s-a văzut că orice element dintr-un grup finit la puterea ordinul grupului coincide cu elementul unitate al grupului. În cazul nostru $\hat{a}^{\varphi(n)}=\hat{1}\Leftrightarrow \widehat{a^{\varphi(n)}}=\hat{1}\Leftrightarrow a^{\varphi(n)}\equiv 1(\bmod n)$.* ■

Caz particular al acestei teoreme îl constituie:

> ***Teorema lui Fermat***. *Fie $p>0$ un număr prim și $a\in\mathbb{Z}, (a,p)=1$.*
> *Atunci* $a^{p-1}\equiv 1(\bmod p)$

Demonstrație. *Dacă p este prim atunci $\varphi(p)=p-1$ și suntem în condițiile teoremei lui Euler. Deci $a^{\varphi(n)}\equiv 1(\bmod p)$ sau $a^{p-1}\equiv 1(\bmod p)$.* ■

Aplicații. 1. Să se afle restul împărțirii lui 17^{319} prin 73. Luăm a = 17, p = 73, (17,73) = 1 și conform teoremei $17^{72}\equiv 1$ (mod 73), iar de aici $17^{319}\equiv 17^3$(mod 73) ≡ 22(mod 73). Deci restul cerut este egal cu 22.

2. O altă aplicație a teoremei lui Lagrange este dată de determinarea grupurilor cu un număr finit de elemente. Aici ne propunem să determinăm care sunt grupurile de ordin 4.

Fie G un grup de ordinul 4. Dacă există un element $a\in G$ având ordinul egal cu 4, atunci $|<a>|=4$ și deci G=<a>, adică G este un grup ciclic. În caz contrar pentru orice $a\in G, a\neq e$, avem ord(a) = 2 (din teorema lui Lagrange ordinul elementului divide ordinul grupului). Rezultă $x^2=e, (\forall)x\in G$ și deci grupul G este abelian.

Dacă $a\in G, a\neq e$, atunci $H=<a>=\{e,a\}$. Dacă $b\in G-H$, atunci $G=\{e,a,b,ab\}$. Grupul G este definit de generatorii a și b și relațiile $a^2=e, b^2=e, ab=ba$, iar tabla sa de multiplicare este:

·	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

. Acesta este de fapt grupul lui Klein.

Rezultă că există două tipuri de grupuri de ordinul 4: grupul ciclic generat de un element și grupul lui Klein.

Pentru grupurile cu trei elemente există un singur tip (vezi ultimul corolar al teoremei lui Lagrange) de grup și anume cel ciclic.

* * * * *

1.6. MORFISME ŞI IZOMORFISME DE GRUPURI

Existenţa unui morfism între două grupuri poate dezvălui informaţii importante şi interesante relative la structura grupurilor. Un morfism „conservă“ operaţia de grup. Două consecinţe ale acestei condiţii sunt:
1) elementele neutre se corespund prin morfism;
2) simetricul unui element, se aplică în simetricul imaginii elementului.

Definiţie. Fie $(G,*)$ şi $(G',\circ)$ două grupuri. O funcţie $f:G\to G'$ se numeşte **morfism** (sau **omomorfism**) de grupuri dacă are loc condiţia:

$$f(x*y)=f(x)\circ f(y),\ (\forall)x,y\in G.$$

Mulţimea morfismelor de la G la G' se notează cu $\mathrm{Hom}(G,G')$.

Observaţii. 0) Schematic, acţiunea morfismului *f* este redată mai jos (Fig. 11).

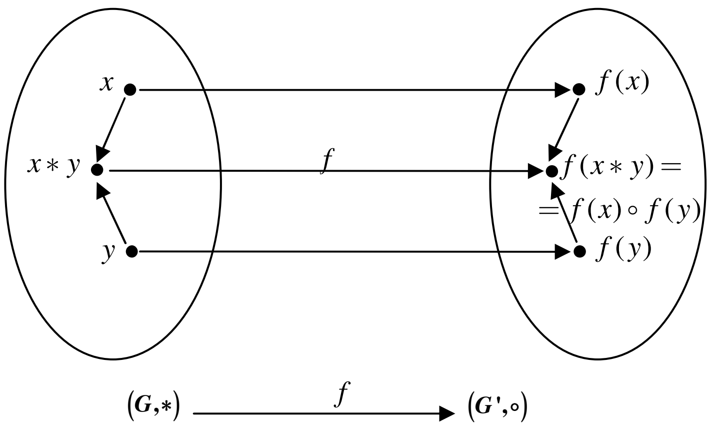
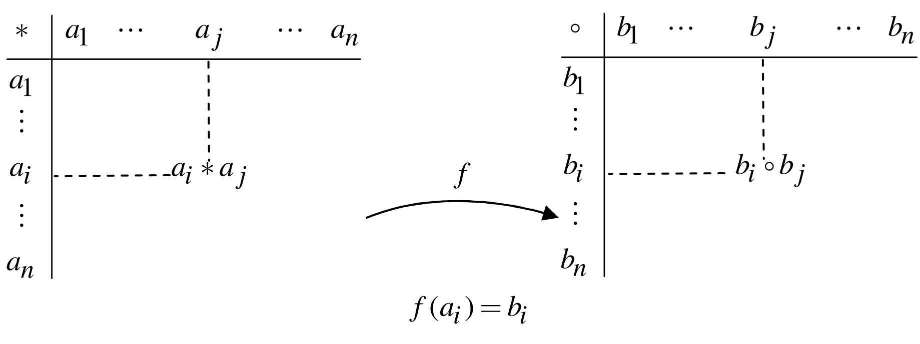


Fig. 11

În cazurile când G, G' sunt finite, avem reprezentarea:



1) Un morfism de grupuri de la un grup la el însuşi se numeşte **endomorfism** al acelui grup. Pentru grupul G mulțimea tuturor endomorfismelor se notează cu End(G).
2) Un morfism de grupuri $f : G \to G'$ se numeşte **morfism injectiv** (sau **monomorfism**) dacă aplicația *f* este injectivă.
Un morfism de grupuri $f : G \to G'$ se numeşte morfism **surjectiv** (sau **epimorfism**) dacă aplicația *f* este surjectivă.
3) Orice grup fiind față de aceeaşi lege şi monoid, din definiție rezultă că orice morfism de grupuri este şi morfism de monoizi.

Exemple cunoscute de morfisme de grupuri

1. Funcția $f_n : (\mathbb{Z},+) \to (\mathbb{Z},+),\ n \in \mathbb{Z}$, fixat $f_n(x) = nx,\ x \in \mathbb{Z}$ este endomorfism al grupului $\mathbb{Z}$, deoarece: $f_n(x+y) = n(x+y) = nx + ny = f_n(x) + f_n(y), (\forall) x, y \in \mathbb{Z}$.

2. Funcția $f : (\mathbb{R},+) \to (\mathbb{R}^*,\cdot),\ f(x) = e^x$ este morfism de grupuri pentru că
$f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y), (\forall) x, y \in \mathbb{R}$.

3. Funcția $f : (\mathbb{R}_+^*,\cdot) \to (\mathbb{R},+),\ f(x) = \log_a x,\ a > 0,\ a \neq 1$, este morfism de grupuri deoarece:
$f(x \cdot y) = \log_a(xy) = \log_a x + \log_a y = f(x) + f(y), (\forall) x, y \in \mathbb{R}$.

4. Funcția $\varepsilon : (S_n,\cdot) \to (\{1,-1\},\cdot),\ \varepsilon(\sigma) = \begin{cases} 1, \sigma = \text{ permutare pară} \\ -1, \sigma = \text{permutare impară} \end{cases}$ este morfism de grupuri pentru că $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau), (\forall) \sigma, \tau \in S_n$.

5. Funcția $f : (\mathbb{Z},+) \to (G,\cdot),\ f(n) = a^n,\ a \in G$, fixat este morfism de grupuri deoarece $f(n+m) = a^{n+m} = a^n \cdot a^m = f(n) f(m), (\forall) m, n \in \mathbb{Z}$.

6. Funcția $f : (\mathbb{Z},+) \to (< a >,\cdot), (< a >$ grup ciclic infinit$)$ $f(n) = a^n$ este (ca mai sus) morfism de grupuri.

7. Funcția $f : (\mathbb{R}^*,\cdot) \to \left(\left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \middle| x \in \mathbb{R}^* \right\}, \cdot \right),\ f(x) = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$, este morfism de grupuri pentru că:

$f(xy) = \begin{pmatrix} xy & 0 \\ 0 & xy \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} = f(x) f(y), (\forall) x, y \in \mathbb{R}^*$.

8. Funcția $f : (G,\cdot) \to (G,\cdot)$ G grup comutativ, $f(x) = x^{-1}$ este endomorfism al grupului G deoarece: $f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x) f(y), (\forall) x, y \in G$.

9. Funcția $f : (GL(n,\mathbb{R}),\cdot) \to (\mathbb{R}^*,\cdot),\ f(A) = \det A$ este morfism de grupuri pentru că:
$f(AB) = \det(AB) = \det(A)\det(B) = f(A) f(B), (\forall) A, B \in GL(n,\mathbb{R})$.

10. Funcția $f : (G,*) \to (G,\circ),\ f(x) = e'$, unde e' este elementul neutru al lui G', se numeşte morfismul constant, fiindcă: $f(xy) = e' = e' \circ e' = f(x) \circ f(x), (\forall) x, y \in G$.

Observație. Morfismul de la 1 $(n \neq 0)$, 2, 3, 5, 6, 7, 8 sunt injective, iar morfismele de la 1 (pentru $n \neq \pm 1$), 3, 4, 6, 7, 8 sunt morfisme surjective.

Vom utiliza din nou notația multiplicativă pentru grupurile care apar, dacă nu se face o altă precizare.

Teoremă. Compunerea a două morfisme de grupuri este tot un morfism de grupuri.

Demonstrație. Fie $f:G\to G'$, $g:G'\to G''$ morfisme de grupuri.
Atunci $g\circ f:G\to G''$ este de asemenea un morfism pentru că
$(g\circ f)(xy)=g(f(xy))=g(f(x)f(y))=g(f(x))g(f(y))=(g\circ f)(x)(g\circ f)(x)$,
$(\forall)x,y\in G$. ■

Teoremă. Fie $f:(G,\cdot)\to(G',\cdot)$ un morfism de grupuri. Dacă e, e' sunt elementele neutre din grupurile G şi respectiv G', atunci:

1) $f(e)=e'$;

2) $f(x^{-1})=(f(x))^{-1}$, $(\forall)x\in G$;

3) $f(x^n)=(f(x))^n$, $(\forall)x\in G$, $(\forall)n\in\mathbb{Z}$.

Demonstrație. Mai întâi reformulăm în cuvinte cerințele teoremei (Fig. 12):
1) morfismul duce elementul neutru al unui grup în elementul neutru al celuilalt grup;
2) imaginea simetricului unui element printr-un morfism de grupuri $(f(x^{-1}))$ este simetricul imaginii acelui element $((f(x))^{-1})$;
3) imaginea puterii unui element printr-un morfism de grupuri $(f(x^n))$ este puterea imaginii elementului $((f(x))^n)$.
1) Avem $f(e)=f(e\cdot e)=f(e)f(e)$. Prin simplificare cu $f(e)$ rezultă $e'=f(e)$.

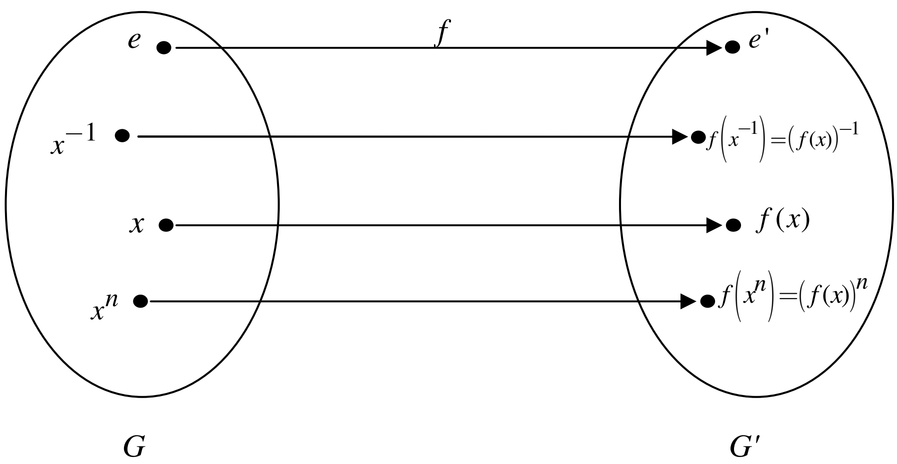


Fig. 12

2) Avem: $e' = f(e) = f(xx^{-1}) = f(x)f(x^{-1})$. Înmulțim aici la stânga cu $(f(x))^{-1}$ și avem $(f(x))^{-1} = f(x^{-1})$.

3) Dacă $n = 0$ se verifică **1)**.

Dacă $n \in \mathbb{N}^*$, atunci $f(x^n) = f(\underbrace{x...x}_{n}) = \underbrace{f(x)...f(x)}_{n} = (f(x))^n$.

Dacă $n < 0$, atunci punem $n = -n', n' \in \mathbb{N}^*$ și deci $f(x^n) = f(x^{-n'}) = f((x^{-1})^{n'}) = (f(x^{-1}))^{n'} = ((f(x))^{-n'}) = (f(x))^{-n'} = (f(x))^n$. ■

Observație. Reformulați teorema în cazul grupurilor aditive.

> **Definiție.** Fie $f:(G,\cdot) \to (G',\cdot)$ un morfism de grupuri. Submulțimea lui G definită prin $\mathrm{Ker}\, f = \{x \in G \mid f(x) = e'\}$ se numește **nucleul** morfismului *f*.
> Submulțimea lui G' definită prin $\mathrm{Im}\, f = \{f(x) \mid x \in G\}$ se numește **imaginea** morfismului *f*.

Observație. $\mathrm{Ker}\, f \neq \varnothing$ pentru că $e \in \mathrm{Ker}\, f$ $(f(e) = e')$.

Exemple. **1. Morfismul constant $f_0 : (\mathbb{Z},+) \to (\mathbb{Z},+)$, $f_0(x) = 0$, are $\mathrm{Ker}\, f = \mathbb{Z}$ și $\mathrm{Im}\, f = \{0\}$.**

2. Morfismul $f:(\mathbb{R},+) \to (\mathbb{R}_+^*,\cdot)$, $f(x) = e^x$ are $\mathrm{Ker}\, f = \{0\}$ și $\mathrm{Im}\, f = (0,\infty)$.

3. Morfismul $\varepsilon : (S_n,\cdot) \to (\{-1,1\},\cdot)$, ε fiind funcția semn pentru permutări are $\mathrm{Ker}\, \varepsilon = A_n$ (grupul altern) și $\mathrm{Im}\, \varepsilon = \{-1,1\}$.

4. Morfismul $f:(\mathbb{Z},+) \to (<a>,\cdot)$, $\mathrm{ord}(<a>) = q$, $f(n) = a^n$ are $\mathrm{Ker}\, f = \{l \cdot q \mid l \in \mathbb{Z}\}$ și $\mathrm{Im}\, f = <a>$.

5. Morfismul $f:(GL(n,\mathbb{R}),\cdot) \to (\mathbb{R}^*,\cdot)$, $f(A) = \det(A)$ are $\mathrm{Ker}\, f = SL(n,\mathbb{R})$, $\mathrm{Im}\, f = \mathbb{R}^*$.

6. Morfismul $f:(\mathbb{R},+) \to (\mathbb{C}^*,\cdot)$, $f(x) = \cos 2\pi x + i \sin 2\pi x$ are $\mathrm{Ker}\, f = \mathbb{Z}$ și $\mathrm{Im}\, f = \{z \in \mathbb{C}^* \mid |z| = 1\}$.

> **Teoremă.** Fie $f:(G,\cdot) \to (G',\cdot)$ un morfism de grupuri. Atunci:
> **1)** $\mathrm{Ker}\, f$ este un subgrup al grupului *G;*
> **2)** *f* este injectiv (monomorfism) $\Leftrightarrow \mathrm{Ker}\, f = \{e\}$;
> **3)** $(\forall) H$ subgrup al lui $G \Rightarrow f(H)$ subgrup al lui G' (Imaginea unui subgrup printr-un morfism este un subgrup); în particular $\mathrm{Im}\, f = f(G)$ este un subgrup al lui G'.

Demonstrație. **1)** Trebuie dovedit că $(\forall) x, y \in \mathrm{Ker}\, f \Rightarrow xy^{-1} \in \mathrm{Ker}\, f$. Din $x, y \in \mathrm{Ker}\, f \Rightarrow f(x) = f(y) = e'$. A arăta că $xy^{-1} \in \mathrm{Ker}\, f$ înseamnă a verifica egalitatea $f(xy^{-1}) = e'$. Ori avem $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)(f(y))^{-1} = e' \cdot (e')^{-1} = e'$.

2) Presupunem că f este injectiv şi probăm că Ker $f = \{e\}$.
Fie $x \in \operatorname{Ker} f$. Deci $f(x) = e' = f(e)$. Cum f este injectiv rezultă $x = e$. Deci $\operatorname{Ker} f \subset \{e\}$. Cum evident $\{e\} \subset \operatorname{Ker} f$ rezultă egalitatea Ker $f = \{e\}$.
Reciproc, fie Ker $f = \{e\}$ şi să arătăm că f este injectiv.
Fie deci $f(x) = f(y)$, $x, y \in G$. De aici $f(x)(f(y))^{-1} = e' \Leftrightarrow f(xy^{-1}) = e' \Leftrightarrow xy^{-1} \in \operatorname{Ker} f = \{e\}$, adică $xy^{-1} = e$ sau (înmulţind la dreapta cu y) $x = y$. Aşadar din $f(x) = f(y) \Rightarrow x = y$, ceea ce arată că f este injectiv.
3) Trebuie probat că pentru $y_1, y_2 \in f(H) \Rightarrow y_1 y_2^{-1} \in f(H)$. Din $y_1, y_2 \in f(H)$ se deduce că există $x_1, x_2 \in H$ pentru care $f(x_1) = y_1$, $f(x_2) = y_2$, Atunci $y_1 y_2^{-1} =$
$= f(x_1)(f(x_2))^{-1} = f(x_1) f(x_2^{-1}) = f(x_1 x_2^{-1}) \in f(H)$, deoarece din $x_1 x_2 \in H \Rightarrow$
$\Rightarrow x_1 x_2^{-1} \in H$ (H fiind subgrup). În final deducem că $f(H)$ este subgrup al lui G'.
Dacă $H = G$, rezultă $f(G) = \operatorname{Im} f$ este subgrup al lui G'. ■

Ideea fundamentală care stă în „spatele“ cuvântului izomorfism este următoarea: grupurile care sunt izomorfe au aceeaşi structură relativ la operaţiile respective ale grupurilor. Grupurile sunt din punct de vedere algebric aceleaşi, deşi elementele lor pot diferi sau legile să fie diferite.
Deoarece izomorfismul conservă operaţiile între două grupuri, atunci este de aşteptat ca elementele neutre din cele două grupuri să se conserve, imaginea inversului să fie inversul imaginii, ordinul unui element să fie egal cu ordinul imaginii acelui element, etc.
Mai precis, formulăm următoarea:

Definiţie. Fie $(G, *)$ şi $(G', \circ)$ două grupuri. O aplicaţie $f : G \to G'$ se numeşte **izomorfism de grupuri** dacă:

1) f este **morfism de grupuri**;

2) f **este bijecţie.**

Dacă între două grupuri G, G' există cel puţin un izomorfism spunem că grupurile sunt izomorfe şi scriem $G \simeq G'$.

Observaţii. 1) Un izomorfism de grupuri este un izomorfism de monoizi.
2) Un izomorfism de grupuri $f : G \to G$ se numeşte **automorfism** al lui G. Altfel spus, un endomorfism bijectiv al lui G se numeşte automorfism al lui G. Mulţimea tuturor automorfismelor lui G se notează cu Aut (G). Arătaţi că $(\operatorname{Aut}(G), \circ)$ este grup, unde „$\circ$“ este operaţia de compunere a funcţiilor.
3) Dacă $f : G \to G'$ este izomorfism de grupuri, atunci şi $f^{-1} : G' \to G$ are aceeaşi calitate (demonstraţi !).

Exemple cunoscute de izomorfisme de grupuri

1. Aplicația identică $1_G : G \to G, 1_G(x) = x$ este izomorfism de grupuri, deci este un automorfism al lui *G*.

2. Aplicația $f : (\mathbb{R},+) \to (\mathbb{R}_+^*,\cdot),\ f(x) = e^x$ este izomorfism de grupuri, deoarece am văzut la morfisme de grupuri că această aplicație este morfism şi în plus este bijectiv.

3. Morfismul $f : (\mathbb{Z},+) \to (< a >,\cdot), < a >$ grup ciclic infinit, $f(n) = a^n$ este izomorfism, deoarece această aplicație este bijectivă. Aşadar orice grup ciclic infinit este izomorf cu grupul aditiv al numerelor întregi.

4. Aplicațiile $f_1, f_{-1} : (\mathbb{Z},+) \to (\mathbb{Z},+),\ f_1(x) = x,\ f_{-1}(x) = -x$ sunt automorfisme ale lui $\mathbb{Z}$ (şi sunt singurele !).

5. Aplicația $f : (\mathbb{Z}_n,+) \to (U_n,\cdot),\ f(\hat{k}) = \omega^k$, unde $\omega = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$ (este bine definită adică dacă $\hat{l} = \hat{k} \Rightarrow f(\hat{l}) = f(\hat{k})$) este izomorfism de grupuri. Cum $f(\hat{k}+\hat{l}) = f(\widehat{k+l}) = \omega^{k+l} =$ $= \omega^k \cdot \omega^l = f(\hat{k})f(\hat{l})$ rezultă *f* este morfism.

De asemenea *f* este surjectiv (elementele lui U_n sunt puteri întregi ale lui ω) şi cele două mulțimi $\mathbb{Z}_n$ şi U_n au acelaşi număr de elemente rezultă *f* este bijectivă. Deci *f* este izomorfism.

Observație. Se poate arăta uşor că orice două grupuri ciclice finite având acelaşi ordin sunt izomorfe.

Dacă două grupuri sunt izomorfe, atunci ele se bucură de aceleaşi proprietăți algebrice (dacă unul este comutativ, atunci şi celălalt este la fel; dacă unul este ciclic, la fel este şi celălalt). Prin urmare toate grupurile izomorfe între ele se comportă la fel. Clasa tuturor acestor grupuri formând ceea ce se numeşte tipul grupului.

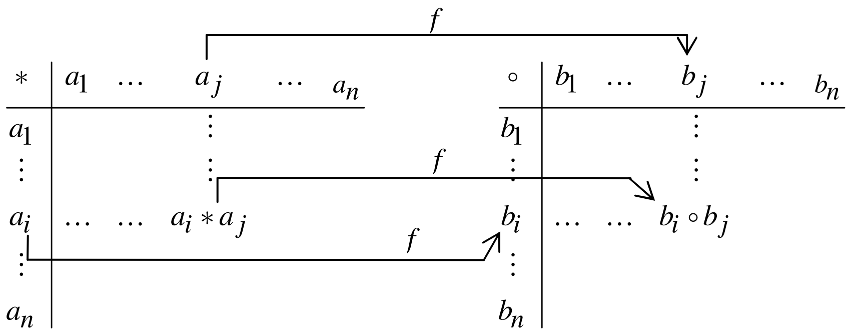
Pentru studiul algebric al acestor grupuri se alege unul dintre ele. Noțiunile de „grupuri izomorfe“ şi „tipul unui grup“ sunt analoge cu noțiunile de „mulțimi echipotente“ (două mulțimi *A, B* se numesc echipotente dacă există o aplicație bijectivă $f : A \to B$) şi „cardinalul unei mulțimi“ (cardinalul unei mulțimi *A* este clasa tuturor mulțimilor echipotente cu *A*) din teoria mulțimilor.

De exemplu, toate grupurile ciclice de ordin *n* constituie un tip de grupuri, iar un reprezentant al acestui tip este $(\mathbb{Z}_n,+)$ sau $(U_n,\cdot)$.

Grupul $(\mathbb{Z},+)$ este un reprezentant pentru toate grupurile ciclice infinite.

În cazul a două grupuri finite, de acelaşi ordin, izomorfismul între ele poate fi dedus utilizând tablele operațiilor. Dacă cele două table sunt la fel organizate, adică un element dintr-un grup şi imaginea sa în celălalt grup prin izomorfism să ocupe în cele două table aceleaşi poziții.

Dacă $(G,*)$, $(G',\circ)$, $G=\{a_1,...,a_n\}$, $G'=\{b_1,...,b_n\}$ sunt două grupuri izomorfe, atunci $f:G\to G'$, $f(a_i)=b_i$, $i=\overline{1,n}$ este izomorfism dacă şi numai dacă pentru orice $1\le i,\ j\le n$, imaginea prin f a elementului $a_i * a_j$ de la intersecția liniei lui a_i cu coloana lui a_j din tabla operației lui G coincide cu elementul $b_i \circ b_j$ de la intersecția liniei lui $b_i=f(a_i)$ cu coloana lui $b_j=f(a_j)$ din tabla operației lui G'.



Un element ajutător pentru aranjarea mai rapidă a tablelor este furnizat de următoarea:

Teoremă. Fie $(G_1,\cdot),(G_2,\cdot)$ două grupuri finite, iar $f:G_1\to G_2$ un izomorfism de grupuri. Dacă $x_1\in G_1$ şi $x_2=f(x_1)\in G_2$, atunci:

$$\operatorname{ord}(x_1)=\operatorname{ord} f(x_1).$$

Ordinul unui element este egal cu ordinul imaginii acestuia printr-un izomorfism de grupuri finite.

Deci, date fiind două grupuri finite se determină ordinele elementelor din cele două grupuri. Izomorfismul de construit între ele trebuie să ducă un element x_k din grupul G_1 în imaginea $f(x_k)$ din G_2, astfel încât $\operatorname{ord}(x_k)=\operatorname{ord}(f(x_k))$ şi $f(e_1)=e_2$, e_1,e_2 elementele neutre din cele două grupuri.
Aplicăm această schemă pentru a demonstra că grupul $(G=\{1,-1,i,-i\},\cdot)$ este izomorf cu grupul $(\mathbb{Z}_4,+)$. Definim $f:G\to\mathbb{Z}_4$, prin $f(1)=\hat{0}$, $f(-1)=\hat{2}$, $f(i)=\hat{1}$, $f(-i)=\hat{3}$. Evident *f* este bijectivă. Pentru a arăta că *f* este izomorfism de la G la $\mathbb{Z}_4$, vom utiliza tabla operațiilor pe G şi $\mathbb{Z}_4$. Fiecărui element $x\in G$ îi construim imaginea $f(x)$ din $\mathbb{Z}_4$. Deoarece tabla rezultată astfel este chiar tabla adunării pe $\mathbb{Z}_4$,

deducem că are loc egalitatea $f(xy)=f(x)+f(y), (\forall)x,y\in G$. Deci f este izomorfism de grupuri, $G\simeq\mathbb{Z}_4$.

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Tabla lui G

$\xrightarrow{f}$

$+$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{3}$	$\hat{0}$	$\hat{1}$
$\hat{3}$	$\hat{3}$	$\hat{0}$	$\hat{1}$	$\hat{2}$

Tabla lui $f(xy)$

Altfel, pentru evidențierea izomorfismului să observăm că $\operatorname{ord}(i)=\operatorname{ord}(\hat{1})=4$ și deci putem pune $f(i)=\hat{1}$. Analog, $\operatorname{ord}(-1)=$ $=\operatorname{ord}(\hat{2})=2$ și avem $f(-1)=\hat{2}$. În fine, $\operatorname{ord}(-i)=\operatorname{ord}(\hat{3})=4$ și punem $f(-i)=\hat{3}$, iar $f(1)=\hat{0}$. Altfel, izomorfismul îl realizăm ușor dacă observăm că $G=<i>=\left\{i^k \middle| k=\overline{0,3}\right\}$. Deci $f:G\to\mathbb{Z}_4$ este dat de $f\left(i^k\right)=\hat{k},\ k=\overline{0,3}$.

Alteori, se utilizează așa numitul „Transport de structură“ pentru realizarea de izomorfisme de grupuri. Mai precis are loc următoarea:

Teoremă. Fie $(G,*)$ un grup și H o mulțime astfel încât există $f:G\to H$ bijectivă.

Atunci: **1)** $(H,\circ)$ este grup, unde $x\circ y=f\left(f^{-1}(x)*f^{-1}(y)\right), (\forall)x,y\in H$;

2) $(G,*)\simeq(H,\circ)$ prin $f:G\to H$.

Evident $e_\circ\in H$ element neutru, $e_\circ=f(e_*)$, e_* fiind elementul neutru din G; simetricul lui $x\in H$ este $x_\circ'=f\left(f^{-1}\left(x_*'\right)\right)$, unde x_*' este simetricul lui $x\in G$.

Această teoremă ne arată cum putem înzestra o mulțime H cu o structură algebrică dacă avem dat (este cunoscut) un grup $(G,*)$ și o aplicație bijectivă $f:G\to H$. Arătați că *f* este și morfism.

Probleme rezolvate

1. Să se demonstreze că: a) toate grupurile de ordin doi sunt izomorfe; b) toate grupurile de ordinul trei sunt izomorfe.

R. a) Fie $(G,\cdot)$ grup cu două elemente $G=\{e,a\}$. Tabla legii este:

$\cdot$	e	a
e	e	a
a	a	e

.

Considerăm acum $(\mathbb{Z}_2,+)$ grupul aditiv al claselor de resturi modulo doi. Tabla legii este:

$+$	$\hat{0}$	$\hat{1}$
$\hat{0}$	$\hat{0}$	$\hat{1}$
$\hat{1}$	$\hat{1}$	$\hat{0}$

Observăm că dacă notăm $f:G\to\mathbb{Z}_2,\ f(e)=\hat{0},\ f(a)=\hat{1}$, atunci cele două table sunt la fel de structurate (pozițiilor ocupate de *e* în prima tablă le corespunde $\hat{\mathbf{0}}$ în a doua tablă – am marcat elementele *e* şi $\hat{0}$ cu roşu în cele două table – şi lui *a* din prima tablă elementul $\hat{1}$ din a doua tablă), ceea ce arată că cele două grupuri sunt izomorfe.
Aşadar orice grup de ordinul doi este izomorf cu $(\mathbb{Z}_2,+)$ şi deci toate grupurile de ordin doi sunt izomorfe.
b) Se consideră grupul multiplicativ $(G=\{e,a,b\},\cdot)$ şi grupul aditiv $(\mathbb{Z}_3,+)$. Fie $f:G\to\mathbb{Z}_3$, $f(e)=\hat{0},\ f(a)=\hat{1},\ f(b)=\hat{2}$. Tabla grupului G şi cea rezultată înlocuind fiecare element $x\in G$ cu elementul $f(x)\in\mathbb{Z}_3$ sunt date mai jos.

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Tabla lui *G*

$\xrightarrow{f}$

$+$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{0}$	$\hat{1}$

Tabla lui $f(xy)$

Observăm că tabla rezultată $(f(xy))$ este chiar tabla pentru adunarea pe $\mathbb{Z}_3$. Deci *f* este morfism. Cum *f* este şi bijecție, deducem că *f* este izomorfism.

Se constată că cele două table sunt la fel structurate (pozițiilor lui *e* din prima tablă le corespunde $\hat{0}$ în a doua tablă, pozițiilor lui *a* din prima tablă le corespunde $\hat{1}$ din a doua tablă etc.), ceea ce arată că orice grup cu trei elemente este izomorf cu $(\mathbb{Z}_3,+)$. Aşadar, toate grupurile de ordin trei sunt izomorfe.

Observație. Grupul $(G=\{f_1,f_2,f_3\},\circ)$ unde $f_i:\mathbb{R}\setminus\{0,1\}\to\mathbb{R}\setminus\{0,1\},\ f_1(x)=x,\ f_2(x)=\dfrac{1}{1-x},\quad f_3(x)=\dfrac{x-1}{x}$, este izomorf cu $(\mathbb{Z}_3,+)$.

2. Fie grupul $(\mathbb{Z},+)$. Să se arate că:

1) Funcţii $f_m:\mathbb{Z}\to\mathbb{Z},\ f_m(x)=mx$ sunt morfisme de grup;

2) Orice endomorfism al lui $\mathbb{Z}$ este de acelaşi tip;

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

R. 1) A spune că f_m este endomorfism al lui $\mathbb{Z}$ revine la a arăta că $f_m(x+y)=f_m(x)+f_m(y)$, $(\forall)x,y\in\mathbb{Z}$.

Avem: $f_m(x+y)=m(x+y)=mx+my=f_m(x)+f_m(y)$.

2) Vom construi efectiv un morfism şi arătăm că este un f_m.

Ținem seama de faptul că $(\mathbb{Z},+)$ este un grup ciclic generat de 1 (de exemplu).

Fie $\varphi:\mathbb{Z}\to\mathbb{Z}$ cu $\varphi(1)=n_0\in\mathbb{Z}$. Atunci $\varphi(2)=\varphi(1+1)=\varphi(1)+\varphi(1)=2\varphi(1)=2n_0$. Din aproape în aproape avem $\varphi(n)=n\cdot n_0$. Această exprimare are loc pentru orice $n\in N^*$ (se arată prin inducție).

Din $\varphi(x+y)=\varphi(x)+\varphi(y),\ (\forall)x,y\in\mathbb{Z}$ rezultă pentru $x=y=0,\ \varphi(0)=0$. De aici $\varphi(0)=0=\varphi(x-x)=\varphi(x)+\varphi(-x)$, adică $\varphi(-x)=-\varphi(x)$, $x\in\mathbb{Z}$.

Extindem definiția lui φ la numerele întregi negative.

Fie $x=-n,\ n\in\mathbb{N}^*$. Atunci $\varphi(x)=\varphi(-n)=-\varphi(n)=(-n)n_0$.

Aşadar, putem conchide că dacă $\varphi \in \text{End}(\mathbb{Z})$, atunci există $n_0 \in \mathbb{N}$ astfel încât $\varphi(n) = nn_0 = f_{n_0}(n)$, $(\forall) n \in \mathbb{Z}$. Deci $\varphi = f_{n_0}$.

3) Funcţiile $f_1(x) = x,\ f_{-1}(x) = -x$ sunt izomorfisme, adică $f_1, f_{-1} \in \text{Aut}(\mathbb{Z})$.

Morfismele $f_m(x) = mx$, cu $m \neq \pm 1$ nu sunt surjective, deoarece $f_m(\mathbb{Z}) = m\mathbb{Z} \subset \mathbb{Z}$.

3. Arătaţi că: 1) pe mulţimea $G = (2,\infty)$ aplicaţia $x \top y = xy - 2x - 2y + 6$ determină o structură de grup abelian;

2) pe mulţimea $G' = (3,\infty)$ aplicaţia $x * y = xy - 3x - 3y + 12$ determină o structură de grup abelian;

3) Să se arată că între grupul de la 1) şi grupul de la 2) există un izomorfism $f : (2,\infty) \to (3,\infty)$ de forma $f(x) = x + a$.

4) Arătaţi că $(\mathbb{R}_+^*, \cdot)$ este izomorf cu $(G', *)$ printr-un izomorfism de forma $f(x) = mx + n$.

R. 1)-2) Lăsăm în seama cititorului să probeze că cele două structuri algebrice $(G,\top), (G',*)$ sunt grupuri. Reţinem pentru primul grup că elementul neutru este $e = 3 \in G$ şi $x' = \dfrac{2x-3}{x-2}$ (arătaţi că $x' > 2$ dacă $x > 2$).

Pentru al doilea grup găsim $e = 4$ şi $x' = \dfrac{3x-8}{x-3} (> 3)$.

3) Dacă *f* este morfism de grupuri, atunci duce elementul neutru al primului grup în elementul neutru al celui de-al doilea grup, adică $f(3) = 4$ şi deci $3 + a = 4$, adică $a = 1$. Deci $f(x) = x + 1$.

Arătăm că *f* este morfism de grupuri, adică $f(x \top y) = f(x) * f(y), (\forall) x, y \in G$.

Avem $f(x \top y) = x \top y + 1 = xy - 2x - 2y + 7$ şi $f(x) * f(y) = (x+1) * (y+1) = (x+1)(y+1) - -3(x+1) - 3(y-1) + 12 = xy - 2x - 2y + 7$, şi cei doi membri sunt egali.

Mai trebuie probat că *f* este bijectivă.

Funcţia este injectivă deoarece din $f(x) = f(y),\ x, y \in G \Rightarrow x + 1 = y + 1$, adică $x = y$.

Funcţia este şi surjectivă pentru că $(\forall) y \in G'$, $(\exists) x \in G$ astfel încât $f(x)=y$. Avem $x + 1 = y \Leftrightarrow \Leftrightarrow x = y - 1 > 2 \Leftrightarrow y > 3$, adevărat.

Cum *f* este bijectivă şi morfism, se deduce *f* izomorfism de grupuri.

4) Cum *f* este morfism de grupuri $f(1) = 4$, adică $m + n = 4$, (1).

A doua ecuaţie pentru m, n se obţine din cerinţa ca *f* să fie morfism adică $f(xy) = f(x) + f(y)$, $(\forall) x, y > 0 \Leftrightarrow mxy + n = m^2xy + (mn - 3m)x + (mn - 3my) + n^2 - 6n + 12, (\forall) x, y > 0$. De aici rezultă $m = m^2,\ mn - 3m = 0, n^2 - 6n + 12 = n$. Găsim $m_1 = 0,\ m_2 = 1$. Valoarea $m = 0$, nu este bună deoarece $f(x) = n$ nu este injectivă. Rămâne $m = 1$, când $n = 3$. Aşadar funcţia căutată este $f(x) = x + 3$. Faptul că *f* este morfism de grupuri, adică $f(xy) = f(x) * f(y)$, $(\forall) x, y > 0$, rezultă din modul în care am determinat parametrii *m*, *n*. Funcţia *f* este injectivă pentru că din $f(x) = f(y) \Rightarrow x + 3 = y + 3 \Rightarrow x = y$.

Funcţia *f* este şi surjectivă deoarece $(\forall) y \in G', (\exists) x \in (0,\infty)$ pentru care $f(x) = y$. Avem $x + 3 = y \Leftrightarrow x = y - 3 > 0$ deoarece $y > 3$. Aşadar *f* este izomorfism de grupuri.

4. Fie mulţimea $G = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \middle| n \in \mathbb{Z} \right\}$. Să se arate că:

a) *G* formează grup comutativ în raport cu operaţia de înmulţire a matricelor; b) $(G,\cdot) \simeq (\mathbb{Z},+)$.

R. a) Fie $A_n=\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}$. Atunci avem: $A_n\cdot A_m=\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & n+m\\ 0 & 1\end{pmatrix}=A_{n+m},\ n,m\in\mathbb{Z}$, ceea ce arată că înmulțirea pe G este lege de compoziție.
Să observăm că $A_n=A_m\Leftrightarrow n=m$.
Înmulțirea, matricelor întotdeauna este *asociativă*, deci şi în acest caz particular. Din $A_nA_m=A_{n+m}=$ $=A_{m+n}=A_mA_n$ rezultă că înmulțirea este *comutativă* pe G.
Element neutru. Să arătăm că există $A_e\in G$ astfel încât $A_a\cdot A_e=A_a,(\forall)A_a\in G$ sau $A_{a+e}=A_a\Leftrightarrow$ $\Leftrightarrow a+e=a,(\forall)a\in\mathbb{Z}$. De aici $e=0$. Aşadar elementul neutru este $A_a=I_2=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$. *Elemente inversabile*. Fiind vorba de înmulțirea obişnuită şi cum fiecare element A_n din G are $\det(A_n)=1\neq 0$ rezultă că fiecare A_n este inversabilă. Rămâne de arătat că şi inversa lui A_n este tot în G. Din $A_n\cdot A_{n'}=A_0$ rezultă $A_{n+n'}=A_0$, adică $n+n'=0$ şi deci $n'=-n\in\mathbb{Z}$. Aşadar $(A_n)'=A_{-n}\in G$. Deci $(G,\cdot)$ este grup abelian.
b) Definim $f:\mathbb{Z}\to G, f(n)=A_n$ aplicația care realizează izomorfismul. Într-adevăr f este *morfism de grupuri* pentru că $f(n+m)=A_{n+m}=A_n\cdot A_m=f(n)f(m),\ (\forall)n,m\in\mathbb{Z}$.
Funcția f este *injectivă* deoarece din $f(n)=f(m)\Rightarrow A_n=A_m\Rightarrow n=m$.
Funcția f este *surjectivă* deoarece $(\forall)A_n\in G$, există $n\in\mathbb{Z}$ pentru care $f(n)=A_n$. Deci f este şi bijectivă. În concluzie f este izomorfism de grupuri.

5. Se consideră mulțimile

$$G_1=\{z\in\mathbb{C}\,|\,z=a+bi,\ a,b\in\mathbb{R},\ a^2+b^2=1\}\qquad G_2=\left\{\begin{pmatrix}a & b\\ -b & a\end{pmatrix}\Bigg|\ a,b\in\mathbb{R},\ a^2+b^2=1\right\}.$$

1) Arătați că $(G_1,\cdot)$ şi $(G_2,\cdot)$ sun grupuri izomorfe.

2) Calculați $\begin{pmatrix}\frac{\sqrt{3}}{2} & \frac{1}{2}\\ -\frac{1}{2} & \frac{\sqrt{3}}{2}\end{pmatrix}^n,\ n\in\mathbb{N}^*$.

R. 1) Nu vom insista asupra verificărilor necesare pentru a proba că cele două structuri sunt grupuri.
Funcția $f:G_1\to G_2,\ f(a+bi)=\begin{pmatrix}a & b\\ -b & a\end{pmatrix}$ este funcția care realizează izomorfismul. Arătăm că f este *morfism de grupuri*, adică $f(z_1z_2)=f(z_1)f(z_2),\ (\forall)z_1,z_2\in G_1$.
Fie $z_1=a_1+ib_1, z_2=a_2+ib_2$. Atunci $z_1z_2=a_1a_2-b_1b_2+i(a_1b_2+a_2b_1)$ şi deci:

$$f(z_1z_2)=\begin{pmatrix}a_1a_2-b_1b_2 & a_1b_2+a_2b_1\\ -(a_1b_2+a_2b_1) & a_1a_2-b_1b_2\end{pmatrix}=\begin{pmatrix}a_1 & b_1\\ -b_1 & a_1\end{pmatrix}\begin{pmatrix}a_2 & b_2\\ -b_2 & a_2\end{pmatrix}=f(z_1)f(z_2).$$

Funcția f este *injectivă* deoarece din $f(z_1)=f(z_2)\Rightarrow\begin{pmatrix}a_1 & b_1\\ -b_1 & a_1\end{pmatrix}=\begin{pmatrix}a_2 & b_2\\ -b_2 & a_2\end{pmatrix}\Rightarrow a_1=a_2$ şi $b_1=b_2$, adică $z_1=z_2$.
Funcția f este *surjectivă* deoarece $(\forall)A=\begin{pmatrix}a & b\\ -b & a\end{pmatrix}, a^2+b^2=1$, există $z=a+bi\in G_1$ pentru care $f(z)=A$.

Cum f este morfism bijectiv se deduce că f este izomorfism.

2) Să observăm că matricea $A=\begin{pmatrix} \frac{\sqrt{3}}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$ este în $G_2\left(\left(\frac{\sqrt{3}}{2}\right)^2+\left(\frac{1}{2}\right)^2=1\right)$.

Pentru a calcula A^n utilizăm izomorfismul de mai sus.

Avem: $f((a+bi)^n)=(f(a+bi))^n=\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^n$, $n\in\mathbb{N}^*$.

Deci: $A^n=f\left(\left(\frac{\sqrt{3}}{2}+\frac{i}{2}\right)\right)^n=f\left(\left(\frac{\sqrt{3}}{2}+\frac{i}{2}\right)^n\right)=f\left(\left(\cos\frac{\pi}{6}+i\sin\frac{\pi}{6}\right)^n\right)=f\left(\cos\frac{n\pi}{6}+i\sin\frac{n\pi}{6}\right)=$

$$=\begin{pmatrix} \cos\frac{n\pi}{6} & \sin\frac{n\pi}{6} \\ -\sin\frac{n\pi}{6} & \cos\frac{n\pi}{6} \end{pmatrix}.$$

6. a) Să se arate că pe mulțimea $G_1=\{x+y\sqrt{5}\mid x,y\in\mathbb{Q},\ x^2-5y^2=1\}$ înmulțirea determină o structură de grup.

b) Să se demonstreze că pe mulțimea

$$G_2=\left\{\begin{pmatrix} x & 2y \\ \frac{5y}{2} & x \end{pmatrix}\middle|\, x,y\in\mathbb{Q},\ x^2-5y^2=1\right\}$$ **înmulțirea matricelor determină o structură de grup.**

c) Arătați că $f:G_1\to G_2$, $f(x+y\sqrt{5})=\begin{pmatrix} x & 2y \\ \frac{5y}{2} & x \end{pmatrix}$ este un izomorfism de grupuri.

R. Lăsăm în seama cititorului verificarea punctelor a), b).

c) Arătăm că f este *morfism de grupuri*. Avem:

$$f((x_1+y_1\sqrt{5})(x_2+y_2\sqrt{5}))=f((x_1x_2+5y_1y_2+\sqrt{5}(x_1y_2+x_2y_1))=$$

$$=\begin{pmatrix} x_1x_2+5y_1y_2 & 2(x_1y_2+x_2y_1) \\ \frac{5}{2}(x_1y_2+x_2y_1) & x_1x_2+5y_1y_2 \end{pmatrix}=\begin{pmatrix} x_1 & 2y_1 \\ \frac{5}{2}y_1 & x_1 \end{pmatrix}\begin{pmatrix} x_2 & 2y_2 \\ \frac{5}{2}y_2 & x_2 \end{pmatrix}=f(x_1+y_1\sqrt{5})f(x_2+y_2\sqrt{5}),$$

$(\forall)x_1+y_1\sqrt{5},\ x_2+y_2\sqrt{5}\in G_1$.

Funcția f este *injectivă* deoarece din $f(x_1+y_1\sqrt{5})=f(x_2+y_2\sqrt{5})\Rightarrow\begin{pmatrix} x_1 & 2y_1 \\ \frac{5}{2}y_1 & x_1 \end{pmatrix}=$

$$=\begin{pmatrix} x_2 & 2y_2 \\ \frac{5}{2}y_2 & x_2 \end{pmatrix}\Rightarrow x_1=x_2 \text{ și } y_1=y_2\Rightarrow x_1+y_1\sqrt{5}=x_2+y_2\sqrt{5}.$$

În fine, funcția f este și *surjectivă* deoarece pentru orice matrice $A_{x,y}=\begin{pmatrix} x & 2y \\ \frac{5y}{x} & x \end{pmatrix}\in G_2$, există $z=x+y\sqrt{5}\in G_1$ pentru care $f(z)=A_{x,y}$.

Putem concluziona că f este izomorfism de grupuri.

7. Să se arate că următoarele perechi de grupuri nu sunt izomorfe:

a) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$; b) $(\mathbb{Q},+)$, $(\mathbb{R},+)$; c) $(\mathbb{Q},+)$, $(\mathbb{Q}_+^*,\cdot)$.

R. a) Dacă grupurile sunt izomorfe, atunci ele ar trebui să aibă aceleași proprietăți. Cum $\mathbb{Z}$ este grup ciclic (generat de 1), iar $\mathbb{Q}$ nu este ciclic rezultă că cele două grupuri nu sunt izomorfe.

b) Mulțimile $\mathbb{Q}, \mathbb{R}$ nu sunt echipotente, adică nu există o bijecție $f:\mathbb{Q}\to\mathbb{R}$. Mulțimea $\mathbb{Q}$ este numărabilă în timp ce $\mathbb{R}$ este nenumărabilă.

c) Prin reducere la absurd. Presupunem că există un izomorfism $f:(\mathbb{Q},+)\to(\mathbb{Q}_+^*,\cdot)$, $f(x+y)=f(x)f(y), (\forall)x,y\in\mathbb{Q}$ cu $f(0)=1$.

Fie $a\in\mathbb{Q}$ astfel încât $f(a)=2$. Atunci $2=f(a)=f\left(\frac{a}{2}+\frac{a}{2}\right)=f\left(\frac{a}{2}\right)f\left(\frac{a}{2}\right)=\left(f\left(\frac{a}{2}\right)\right)^2$. De aici $f\left(\frac{a}{2}\right)=\sqrt{2}$, contradicție deoarece $\sqrt{2}\notin\mathbb{Q}$ în timp ce $f\left(\frac{a}{2}\right)\in\mathbb{Q}_+^*$.

8.* Arătați că grupurile aditive $(\mathbb{Z},+)$ și $(\mathbb{Z}[X],+)$ nu sunt izomorfe.

R. Dacă, prin absurd, cele două grupuri ar fi izomorfe, atunci ar trebui ca ele să aibă aceleași proprietăți. Știm că grupul $(\mathbb{Z},+)$ este ciclic $=<1>$. Dacă $\mathbb{Z}[X]$ (mulțimea polinoamelor de nedeterminată X cu coeficienți întregi) ar fi ciclic generat de polinomul $f\in\mathbb{Z}[X]$, grad(f) = k, $k\in\mathbb{N}^*$, atunci $\mathbb{Z}[X]=<f>=\{nf \mid n\in\mathbb{Z}\}$ ceea ce înseamnă că toate polinoamele lui $\mathbb{Z}[X]$ ar avea gradul zero sau k, ceea ce este fals. Deci cele două grupuri nu pot fi izomorfe.

9.* Să se determine toate subgrupurile G ale grupului $(\mathbb{R},+)$ astfel încât $f:(G,+)\to(\mathbb{R}^*,\cdot)$, $f(x)=\sin(2x+1)\frac{\pi}{2}$ să fie morfism de grupuri.

R. Fie G un subgrup aditiv al grupului $(\mathbb{R},+)$.

Pentru $x\in G$ avem $1=f(0)=f(x+(-x))=f(x)f(-x)$ sau $\sin(2x+1)\frac{\pi}{2}\sin(-2x+1)\frac{\pi}{2}=1\Leftrightarrow$

$\Leftrightarrow\frac{\cos 2x\pi-\cos\pi}{2}=1\Leftrightarrow\cos 2x\pi=1\Leftrightarrow x\in\mathbb{Z}$.

Deci pentru $x\in G\Rightarrow x\in\mathbb{Z}$, adică $G\subset\mathbb{Z}$, arată că G este de fapt subgrup al lui $\mathbb{Z}$. Se știe că G are forma $G=n\mathbb{Z}, n\in\mathbb{N}$.

Reciproc, dacă $G=n\mathbb{Z}$, atunci f este morfism de grupuri $f(x+y)=(-1)^{x+y}=(-1)^x(-1)^y=$ $=f(x)f(y), (\forall)x,y\in G$.

10.* Să se determine endomorfismele grupului $(\mathbb{Q},+)$.

R. Fie $f:\mathbb{Q}\to\mathbb{Q}$ un morfism de grupuri. Procedând ca la problema rezolvată 2 găsim că punând $f(1)=a\in\mathbb{Q}, f(x)=ax, (\forall)x\in\mathbb{Z}$. Extindem construcția lui f la $\mathbb{Q}_+$.

$$a=f(1)=f\Bigg(\underbrace{\frac{1}{n}+\frac{1}{n}+...+\frac{1}{n}}_{n}\Bigg)=nf\left(\frac{1}{n}\right).$$ Deci $f\left(\frac{1}{n}\right)=\frac{1}{n}a,\ n\in\mathbb{N}^*$ şi $f\left(\frac{m}{n}\right)=f\Bigg(\underbrace{\frac{1}{n}+...+\frac{1}{n}}_{m}\Bigg)=$

$=mf\left(\frac{1}{n}\right)=\frac{m}{n}a,\ m,n\in\mathbb{N}^*$.

Deci $f(x)=ax, (\forall)x\in\mathbb{Q}_+$. Dacă $x=-y,\ y\in\mathbb{Q}_+$, atunci $f(x)=f(-y)=-f(y)=a(-y)=ax$. Aşadar pentru orice $x\in\mathbb{Q},\ f(x)=ax$.

Evident că $(\forall)a\in\mathbb{Q},\ f(x)=ax$ este endomorfism al grupului $(\mathbb{Q},+)$, cum uşor se poate vedea $f:(\mathbb{Z},\circ)\to(\mathbb{Z},*)$, ceea ce este imediat.

11.* Fie $(G,\cdot)$ un grup. Arătaţi că $f:G\to G,\ f(x)=x^{-1}$ este un izomorfism de grupuri dacă şi numai dacă G este abelian.

R. Presupunem că f este izomorfism de grupuri. Avem (f morfism): $f(xy)=f(x)f(y), (\forall)x,y\in G$ sau ţinând seamă de forma lui f $(xy)^{-1}=x^{-1}y^{-1}, (\forall)x,y\in G\Leftrightarrow e=xyx^{-1}y^{-1}$.

Compunând ultima egalitate la dreapta cu y şi apoi cu x obţinem $yx=xy, (\forall)x,y\in G$ egalitate care arată că G este comutativ.

Reciproc, presupunem că G este grup abelian. Să arătăm că $f:G\to G,\ f(x)=x^{-1}$ este un izomorfism. Se arată uşor că f este bijectivă, iar din $f(xy)=(xy)^{-1}=y^{-1}x^{-1}=x^{-1}y^{-1}=\ f(x)f(y), (\forall)x,y$ rezultă că f este şi morfism.

Prin urmare f este izomorfism.

12.* Fie $(G,\cdot)$ un grup finit cu proprietatea că funcţia $f:G\to G,\ f(x)=x^2$ este automorfism de grupuri. Arătaţi că mulţimea G are un număr impar de elemente.

R. Ideea de rezolvare a problemei este de a arăta că orice element $x\in G,\ x\neq e$ (e elementul neutru) este diferit de inversul său.

Presupunem prin absurd că ar exista $x\in G,\ x\neq e$ astfel încât $x=x^{-1}\Leftrightarrow x^2=e\Leftrightarrow f(x)=e=$ $=f(e)\Rightarrow x=e$ (ultima implicaţie are loc deoarece f este injectivă), absurd.

Aşadar $(\forall)x\in G,\ x\neq e\Rightarrow x\neq x^{-1}$. Aceasta ne permite să grupăm elementele lui $G-\{e\}$ în perechi (x,x^{-1}), ceea ce înseamnă că numărul de elemente din $G-\{e\}$ este par. Acum este clar că numărul de elemente din G este impar.

13*. Fie $G=\left\{A_{(a,b)}=\begin{pmatrix} a & b & b\\ b & a & b\\ b & b & a\end{pmatrix}\middle|\ a,b\in\mathbb{Z}_5,\ \det(A)=\hat{1}\right\}$.

Să se arate că:

1) $(G,\cdot)$ este grup comutativ.

2) $(G,\cdot)\simeq(\mathbb{Z}_4,+)$.

R. 1) Din $\det(A)=\hat{1}$ rezultă egalitatea $a^3+2b^3-3ab^2=\hat{1}$ sau $(a+\hat{2}b)(a-b)^2=\hat{1}$. Soluțiile ecuației sunt soluțiile sistemelor:

$\begin{cases} a+\hat{2}b=\hat{1} \\ (a-b)^2=\hat{1} \end{cases}$; $\begin{cases} a+\hat{2}b=\hat{4} \\ (a-b)^2=\hat{4} \end{cases}$. A doua ecuație din primul sistem este echivalentă cu reuniunea ecuațiilor $a-b=\hat{1}, a-b=\hat{4}$. În primul caz găsim soluția $(\hat{1},\hat{0})$, iar în al doilea caz $(\hat{3},\hat{4})$. Asemănător, din al doilea sistem obținem soluțiile: $(\hat{0},\hat{2}), (\hat{1},\hat{4})$. Prin urmare, grupul G are patru elemente: $I_2=A(\hat{1},\hat{0})$, $A=A(\hat{0},\hat{2}), B=A(\hat{1},\hat{4}), C=A(\hat{3},\hat{4})$. Cum $A^2=C$, grupul nu este de tip Klein și deci este izomorf cu $(\mathbb{Z}_4,+)$.

14*. 1) Să se determine automorfismele grupului aditiv $\mathbb{Z}_6$.

2) Fie $G=\left\{A_{(a)}=\begin{pmatrix}\hat{1} & \hat{2}a \\ \hat{3}a & \hat{1}\end{pmatrix} \middle| a\in\mathbb{Z}_6\right\}$. Arătați că $(G,\cdot)$ este grup și determinați automorfismele grupului G.

R. 1) Fie $f:\mathbb{Z}_6\to\mathbb{Z}_6$ un morfism de grupuri. Deci $f(x+y)=f(x)+f(y), (\forall)x,y\in\mathbb{Z}_6$. De aici se obține $f(\hat{0})=\hat{0}$ și $f(x)=xf(\hat{1})$. Punem $f(\hat{1})=a$ și deci $f(x)=ax$ este forma unui endomorfism al lui $\mathbb{Z}_6$. Să observăm că f este injectiv $(f(x)=f(y)\Rightarrow x=y)$ numai dacă $a\in\mathbb{Z}_6$ este inversabil, adică dacă $a\in\{\hat{1},\hat{5}\}$. Deci $f_1(x)=x,\ f_2(x)=\hat{5}x$ sunt singurele automorfisme ale lui $\mathbb{Z}_6$.

2) Avem $A(a)A(b)=A(a+b)$ și se verifică ușor că $(G,\cdot)$ este grup. Să determinăm elementele lui G. Punem $A(\hat{1})=A$. Atunci $A(\hat{2})=A(\hat{1}+\hat{1})=\left(A(\hat{1})\right)^2=A^2, A(\hat{3})=A^3, A(\hat{4})=A^4, A(\hat{5})=A^5, A(\hat{0})=I_2$. Deci G are șase elemente și $(G,\cdot)\simeq(\mathbb{Z}_6,+)$ prin izomorfismul $f:G\to\mathbb{Z}_6, f(A(x))=x$. Acum G are atâtea automorfisme câte are grupul $\mathbb{Z}_6$ cu care este izomorf. Acestea sunt: $f(A(x))=A(x)$ și $f(A(x))=A(\hat{5}x)=A^5(x)$.

15.* Fie $G=\left\{A_{a,b}=\begin{pmatrix}a+\hat{3}b & b \\ \hat{4}b & a+\hat{3}b\end{pmatrix} \middle| a,b\in\mathbb{Z}_6, \det(A)=\hat{1}\right\}$.

1) Arătați că $(G,\cdot)$ este grup abelian izomorf cu grupul Klein.

2) Determinați subgrupurile grupului G.

R. 1) $\det(A)=\hat{1}$ ne dă ecuația $a^2+\hat{5}b^2=\hat{1}$ cu soluțiile $(a,b):(\hat{1},\hat{0}), (\hat{2},\hat{3}), (\hat{4},\hat{3}), (\hat{5},\hat{0})$. Prin urmare, G are elementele: $I_2=\begin{pmatrix}\hat{1} & \hat{0} \\ \hat{0} & \hat{1}\end{pmatrix}, A=\begin{pmatrix}\hat{5} & \hat{3} \\ \hat{0} & \hat{5}\end{pmatrix}, B=\begin{pmatrix}\hat{1} & \hat{3} \\ \hat{0} & \hat{1}\end{pmatrix}, C=\begin{pmatrix}\hat{5} & \hat{0} \\ \hat{0} & \hat{5}\end{pmatrix}$, pentru care se verifică egalitățile $A^2=B^2=C^2=I_2$, $AB=BA=C,\ AC=BC=A,\ CA=AC=B$. Deci G este izomorf cu grupul Klein.

2) Cum G este izomorf cu grupul lui Klein, subgrupurile lui G vor fi de același tip cu subgrupurile grupului lui Klein. Acestea sunt: $\{I_2\}, \{I_2,A\}, \{I_2,B\}, \{I_2,C\}, G$.

Probleme propuse

1. 1) Să se arate că aplicația $f:(\mathbb{Z},+)\to(U_n,\cdot),\ f(k)=\varepsilon^k$, unde $\varepsilon=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$ este morfism de grupuri.

2) Arătați că aplicația $f:(\mathbb{Z},+)\to(\mathbb{R}^*,\cdot),\ f(n)=\begin{cases}1, & n \text{ par}\\ -1, & n \text{ impar}\end{cases}$ este morfism de grupuri.

3) $G\subseteq\mathcal{M}_2(\mathbb{R})$, G conține matricele inversabile în raport cu înmulțirea. Arătați că $f:(G,\cdot)\to(\mathbb{R}^*,\cdot)$, $f\left(\begin{pmatrix}a & b\\ c & d\end{pmatrix}\right)=ad-bc,\ (\forall)\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in G$ este morfism de grupuri.

4) Arătați că $f:(\mathbb{C}^*,\cdot)\to(\mathbb{R}_+^*,\cdot),\ f(x+iy)=\sqrt{x^2+y^2},\ x,y\in\mathbb{R}$ este morfism de grupuri.

5) Să se arate că funcția $f_m:(2\mathbb{Z},+)\to(3\mathbb{Z},+),\ f(x)=\frac{3m}{2}x$ este morfism de grupuri, iar $g:(3\mathbb{Z},+)\to(3\mathbb{Z},+),\ g(x)=\frac{ax}{3},\ a=g(3)$, este endomorfosm.

2. Să se arate că:
1) aplicația $x*y=x+y-2$ determină pe $\mathbb{Z}$ o structură de grup abelian;
2) aplicația $x\circ y=x+y+1$ determină pe $\mathbb{Z}$ o structură de grup abelian;
3) între grupurile de la 1) şi 2) există un izomorfism de forma $f:\mathbb{Z}\to\mathbb{Z},\ f(x)=x+a,\ a\in\mathbb{Z}$ ce se va determina.

3. Pe mulțimea $G=(-1,1)$ se consideră aplicația $x*y=\frac{x+y}{1+xy}$. Arătați că:

a) $(G,*)$ este grup comutativ;

b) Între grupurile $(\mathbb{R}_+^*,\cdot)$ şi $(G,*)$ se poate stabili un izomorfism de forma $f(x)=\frac{ax-1}{x+1}$ cu $a\in\mathbb{R}$ convenabil determinat.

4. Să se arate că aplicația $x*y=\frac{3xy-4x-4y+6}{2xy-3x-3y+5}$ determina pe $(1,2)$ o structură de grup comutativ izomorf cu grupul $((0,\infty),\cdot)$ printr-un izomorfism $f:(0,\infty)\to(1,2),\ f(x)=\frac{x+m}{x+1}$.

5. 1) Pe $\mathbb{R}$ se defineşte legea $*$ dată de $x*y=\sqrt[1995]{x^{1995}+y^{1995}}$. Arătați că $(\mathbb{R},*)$ este grup abelian izomorf cu $(\mathbb{R},+)$.

2) Rezolvați în $\mathbb{R}\times\mathbb{R}$ sistemul: $\begin{cases}x*y*(-2)=1\\ x^3-y^3=-7.\end{cases}$

6. Fie $G=(-k,k),\ k>0$ şi aplicația $x*y=\frac{k^2(x+y)}{k^2+xy}$. Arătați că:

1) $(G,*)$ este grup comutativ; 2) $f:G\to\mathbb{R},\ f(x)=\frac{1}{2k}\ln\frac{k+x}{k-x}$ este izomorfism între grupurile $(G,*)$ şi $(\mathbb{R},+)$.

7. Să se arate că: 1) aplicația $x \perp y = x^{\ln y}$ defineşte pe $G=(0,\infty)-\{1\}$ o structură de grup abelian. 2) $(G,\perp) \simeq (\mathbb{R}^*,\cdot)$.

8. Fie $G=(1,\infty)$.

a) Să se arate că $\sqrt{x^2y^2-x^2-y^2+2} \in G$ dacă $x,y \in G$.

b) Arătați că $(G,*)$ este grup abelian, $x*y=\sqrt{x^2y^2-x^2-y^2+2}$.

c) Să se determine $a,b \in \mathbb{R}$ astfel încât $f:\mathbb{R}_+^* \to G,\ f(x)=\sqrt{ax+b}$ să fie un izomorfism între grupurile $\left(\mathbb{R}_+^*,\cdot\right)$ şi $(G,*)$.

9. Fie mulțimea de funcții $G=\{f:R \to (0,\infty) \mid f(x)=e^{\alpha x},\ \alpha \in \mathbb{R}\}$.

Să se arate că: a) G este grup multiplicativ; b) $(G,\cdot) \simeq (\mathbb{R},+)$; c) G admite un subgrup izomorf cu grupul aditiv al numerelor raționale.

10. a) Fie $a,b \in \mathbb{R}^*$. Se consideră pe $\mathbb{R}$ aplicația $x*y=ax+by+1$.

1) Determinați pe *a* şi *b* astfel încât $(\mathbb{R},*)$ să fie grup.

2) Pentru *a, b* găsiți la 1), arătați că $(\mathbb{R},*)$ este izomorf cu $(\mathbb{R},+)$.

b) Pe $\mathbb{C}$ definim operațiile $x*y=x+y+ai,\ x\circ y=x+y-a,\ x,y \in \mathbb{C},\ a \in \mathbb{R}$. Arătați că:

1) $(\mathbb{C},*), (\mathbb{C},\circ)$ sunt grupuri abeliene.

2) $f:(\mathbb{C},*) \to (\mathbb{C},\circ),\ f(z)=iz$ este izomorfism de grupuri.

11. Se consideră pe $\mathbb{R}$ aplicația $x*a=xy-ax-ay+a^2+a,\ a \in \mathbb{R}$ şi $G_a=(a,\infty)$. Arătați că:

1) $(G_a,*)$ este grup abelian;

2) $(\forall) a,b \in \mathbb{R},\ (G_a,*) \simeq (G_b,*) \simeq (\mathbb{R},+)$.

12. Fie $\mathbb{Z}_{12}$ grupul aditiv al claselor de resturi modulo 12 şi *G* mulțimea elementelor inversabile. Arătați că înmulțirea pe *G* determină o structură de grup abelian izomorf cu grupul lui Klein.

13. Fie $G=\left\{\begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \middle| \alpha \in [-\pi,\pi)\right\}$. Arătați că *G* are o structură de grup abelian în raport cu operația de înmulțire a matricelor, izomorf cu grupul multiplicativ al numerelor complexe de modul 1.

14. a) Fie $G=\left\{\begin{pmatrix} 2-x & 1-x \\ 2(x-1) & 2x-1 \end{pmatrix} \middle| x \in \mathbb{R}^*\right\}$.

1) Arătați că $(G,\cdot)$ este grup abelian. 2) $(\mathbb{R}^*,\cdot) \simeq (G,\cdot)$.

b) Fie $G=\left\{A(x)=\begin{pmatrix} 1-x & 2x \\ \dfrac{x}{2} & 1-x \end{pmatrix} \middle| x \in \mathbb{R}\right\}$.

1) Arătați că $A(x)A(y)=A(x+y-2xy)$ şi $I_2 \in G$.

2) Pentru $x \in \mathbb{R}-\{s\}$, determinați *s* astfel încât $(G,\cdot)$ să fie grup.

15. Se consideră mulțimile:

$$G_1=\left\{\begin{pmatrix} a+2b & 3b \\ 2b & a-2b \end{pmatrix} \middle| a,b \in \mathbb{Q},\ a^2-10b^2=1\right\},$$

$$G_2=\{a+b\sqrt{10}\,|\,a,b\in\mathbb{Q},\,a^2-10b^2=1\}.$$

a) Arătați că $(G_1,\cdot),(G_2,\cdot)$ sunt grupuri abeliene infinite;

b) $(G_1,\cdot)\simeq(G_2,\cdot)$.

16. **1) Se consideră mulțimile:** $G_1=\left\{I_2=\begin{pmatrix}1&0\\0&1\end{pmatrix},A=\begin{pmatrix}0&1\\1&0\end{pmatrix},B=\begin{pmatrix}-1&0\\0&-1\end{pmatrix},C=\begin{pmatrix}0&-1\\-1&0\end{pmatrix}\right\}$,

$G_2=\left\{e=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\sigma_1=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},\sigma_2=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\sigma_3=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}\right\}$.

Arătați că: a) G_1 este grup în raport cu înmulțirea matricelor; b) G_2 este grup în raport cu compunerea permutărilor. c) $(G_1,\cdot)\simeq(G_2,\circ)$

2) Să se arate următoarele izomorfisme de grupuri:

a) $\left(\mathbb{Z}_4,+\right)\simeq\left(\mathbb{Z}_5^*,\cdot\right)$; **b)** $\left(G=\{\pm1,\pm i\},\cdot\right)\simeq\left(H,\cdot\right)$, **unde** $H=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}i&0\\0&-i\end{pmatrix},\begin{pmatrix}-i&0\\0&i\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\right\}$;

c) $\left(G=\{I_2,M_1,M_2,M_3,M_4,M_5\},\cdot\right)\simeq\left(H=\{e,\rho,\rho^2,\sigma,\gamma,\delta\},\circ\right)$, **unde** $I_2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $M_1=\begin{pmatrix}1&0\\-1&-1\end{pmatrix}$,

$M_2=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$, $M_3=\begin{pmatrix}-1&-1\\1&0\end{pmatrix}$, $M_4=\begin{pmatrix}-1&-1\\0&1\end{pmatrix}$, $M_5=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, **iar** $e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $\rho=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$,

$\sigma=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$, $\gamma=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$, $\delta=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$; **d)** $\left(\mathbb{Z}\left(\sqrt{3}\right),+\right)\simeq\left(\mathbb{Z}\left(\sqrt{5}\right),+\right)$.

3) Fie $G=\left\{\begin{pmatrix}x&ax+b\\0&1\end{pmatrix}\middle|\,x\in\mathbb{R}^*\right\}$. **Să se determine $a,b\in\mathbb{R}^*$ astfel încât $\left(G,\cdot\right)$ să fie grup și arătați apoi că $\left(G,\cdot\right)\simeq\left(\mathbb{R}^*,\cdot\right)$.**

17. **1) Se consideră matricea** $A=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}$.

Să se arate că $G=\{A^n\,|\,n\in\mathbb{N}\}$ împreună cu operația de înmulțire a matricelor formează un grup abelian. Indicați un grup de numere complexe izomorf cu G.

2) Arătați că grupul de simetrii ale triunghiului echilateral și grupul de matrice permutare (ex. 24.2) de la grupuri, sunt izomorfe.

3) Arătați că grupul de simetrii ale triunghiului echilateral de vârfuri 1, 2, 3 este izomorf cu grupul de permutări din S_3, $H=\{e,\sigma,\sigma^2,\tau,\gamma,\delta\}$ unde $e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $\sigma=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, $\sigma^2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$,

$\tau=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$, $\gamma=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$, $\delta=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$.

4) a) Construiți tabla legii grupului G al simetriilor unui pătrat cu vârfurile 1, 2, 3, 4 (Aplicației identice i se asociază permutarea identică $e=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$, **etc.);**

b) Asociați fiecărei transformări de la a) o permutare din S_4 și arătați că mulțimea acestora împreună cu operația de compunere este grup izomorf cu cel de la a).

5) a) Construiți tabla legii grupului G al simetriilor unui dreptunghi (care nu este pătrat) cu vârfurile 1, 2, 3, 4 (Aplicației identice i se asociază permutarea identică $e=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$, etc.).

b) Determinați un izomorfism de la grupul de la a) la grupul multiplicativ $(H,\cdot)$, unde $H=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\right\}$.

18. Fie mulțimea $G=\left\{\begin{pmatrix}1&1&x\\0&0&1\\0&0&1\end{pmatrix}\middle| x\in 2\mathbb{Z}+1\right\}$.

a) Arătați că $(G,\cdot)$ este grup abelian. b) $(G,\cdot)\simeq(2\mathbb{Z},+)$; c) $(2\mathbb{Z},+)\simeq(3\mathbb{Z},+)$; d) Determnați $\mathrm{Aut}(3\mathbb{Z},+)$.

19. Fie matricea $A=\begin{pmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{pmatrix}$ şi mulțimea $G=\{A^k \mid k\in N^*\}$. Considerăm $G_1=\{e,\sigma_1,\sigma_2,\sigma_3\}$, unde

$$e=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\sigma_1=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},\sigma_2=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\sigma_3=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}.$$

Arătați că: a) G este grup abelian în raport cu operația de înmulțire a matricelor; b) G_1 este grup abelian în raport cu operația de compunere a permutărilor; c) $G\simeq G_1$; d) G este izomorf cu grupul multiplicativ $G_2=\left\{\cos\frac{2k\pi}{4}+i\sin\frac{2k\pi}{4};\,k\in\overline{1,4}\right\}$?

20. Se consideră mulțimea $G=\left\{\begin{pmatrix}1&0&a\\-a&1&-\frac{a^2}{2}\\0&0&1\end{pmatrix}\middle| a\in\mathbb{R}\right\}$. Arătați că G împreună cu operația de înmulțire formează grup abelian izomorf cu grupul $(\mathbb{R},+)$.

21. Fie $G=\left\{\begin{pmatrix}1&\ln a&0\\0&1&0\\0&0&a\end{pmatrix}\middle| a>0\right\}$.Arătați că $(G,\cdot)$ este grup abelian izomorf cu $(\mathbb{R}_+^*,\cdot)$

22. Fie $A=\begin{pmatrix}2&-1&-1\\-1&2&-1\\-1&-1&2\end{pmatrix}$ şi $B=\begin{pmatrix}1&1&1\\1&1&1\\1&1&1\end{pmatrix}$, iar $M_t=-\frac{t}{3}A+\frac{1}{3}t^2B$ şi $G=\{M_t \mid t\in\mathbb{R}^*\}$.

Arătați că $(G,\cdot)\simeq(\mathbb{R}^*,\cdot)$

23. Arătați că funcția $f:(\mathcal{M}_n(\mathbb{C}),+)\to(\mathbb{C},+),\ f(A)=\mathrm{Tr}(A)$, unde Tr(A) este urma matricei A, este morfism surjectiv de grupuri.

24. Fie $M=\left\{\begin{pmatrix} a & 0 & a \\ 0 & k & 0 \\ a & 0 & a \end{pmatrix} \middle| a,k\in\mathbb{C}^*\right\}$, atunci:

1) $(M,\cdot)$ este grup abelian; 2) $(M,\cdot)$ are un subgrup izomorf cu $(\mathbb{Q}^*,\cdot)$.

25. Fie $G=\left\{A_{a,b}=\begin{pmatrix} a & 0 & ib \\ 0 & 0 & 0 \\ ib & 0 & a \end{pmatrix} \middle| a,b\in\mathbb{R}^*, a^2+b^2\neq 0, i^2=-1\right\}$.

Arătați că $(G,\cdot)$ este grup izomorf cu $(\mathbb{C}^*,\cdot)$ și calculați $A_{1,1}^{2001}$.

26. Fie matricea $A=\begin{pmatrix} 0 & 0 & x & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & y \\ 0 & 1 & 0 & 0 \end{pmatrix}$, $x,y\in[-1,0)$. Să se determine *x, y* astfel încât împreună cu înmulțirea matricelor mulțimea $\{A^n \mid n\in N^*\}$ să fie grup izomorf cu $(\mathbb{Z}_4,+)$.

27. 1) Fie $M\neq\varnothing$, Pe $\mathcal{P}(M)$ definim operația $X+Y=(X\cap CY)\cup(CX\cap Y)$. Arătați că:

a) $X+X=\varnothing, (\forall)X\in\mathcal{P}(M)$;

b) $(\mathcal{P}(M),+)$ este grup abelian.

2) Fie $G=\mathcal{P}(I)$ mulțimea funcțiilor reale care admit primitive pe *I*. Atunci:

a) $(G,+)$ este grup abelian;

b) $G'=\left\{F_f:G\to G \middle| f\in G, F_f(h)=f+h\right\}$ cu compunerea este grup abelian izomorf cu *G*.

3) Fie $f,g:[a,b]\to\mathbb{R}$, funcții continue și $G_f=\left\{f_c\in\mathbb{R} \middle| f_c=\int_a^b (f(x)+c)dx, c\in\mathbb{R}\right\}$, $G_g=\left\{g_c\in\mathbb{R} \middle| g_c=\int_a^b (g(x)+c)dx, c\in\mathbb{R}\right\}$ și operațiile $f_c * f_{c'}=f_{c+c'}, (\forall)f_c, f_{c'}\in G_f$ și $g_c\circ g_{c'}=g_{c+c'}, (\forall)g_c, g_{c'}\in G_g$.

a) Arătați că $(G_f,*), (G_g,\circ)$ sunt grupuri abeliene izomorfe cu $(\mathbb{R},+)$;

b) Dacă $G(f)=\left\{F_c:G_f\to G_f \middle| F_{f_c}(f_{c'})=f_c*f_{c'}, (\forall)f_{c'}\in G_f\right\}$, atunci F_{f_c} este bijectivă, $(\forall)f_c\in G_f$ și $(G(f),\circ)$ este grup abelian, unde $\circ$ este compunerea funcțiilor și $(G(f),\circ)\simeq(G(f),*)$.

28. Fie funcțiile $f_1,f_2,f_3:\mathbb{R}-\{0,1\}\to\mathbb{R}-\{0,1\}$ definite astfel: $f_1(x)=x$, $f_2(x)=\frac{x-1}{x}$, $f_3(x)=\frac{1}{1-x}$ și $G=\{f_1,f_2,f_3\}$. Arătați că *G* împreună cu operația de compunere a funcțiilor formează un grup izomorf cu $(\mathbb{Z}_3,+)$.

29. 1) Fie mulțimea: $G=\{f_n:(2,\infty)\to(2,\infty),\ f_n(x)=2+(x-2)^{2^n},\ m\in\mathbb{Z}\}$. Arătați că $(G,\circ)$ este grup abelian izomorf cu $(\mathbb{Z},+)$

2) Fie $H=\{f:\mathbb{R}\to\mathbb{R}\,|\,f(x+y)=f(x)+f(y),\ x,y\in\mathbb{R}\}$,

$G=\{f:\mathbb{R}\to(,\infty)\,|\,f(x+y)=f(x)f(y),\ x,y\in\mathbb{R}\}$.

Arătați că $(H,+)\simeq(G,\cdot)$.

30.* Arătați că următoarele perechi de grupuri nu sunt izomorfe:

a) $(\mathbb{Q},+),(\mathbb{Q}^*,\cdot)$; b) $(\mathbb{Q}_+^*,\cdot),(\mathbb{Q}^*,\cdot)$; c) $(\mathbb{R}^*,\cdot),(\mathbb{R}_+^*,\cdot)$; d) $(\mathbb{Q}^*,\cdot),(\mathbb{R}^*,\cdot)$; e) $(\mathbb{R}^*,\cdot),(\mathbb{C}^*,\cdot)$.

31.* Să se arate că singurul morfism de grupuri de la grupul $(\mathbb{Q},+)$ la $(\mathbb{Z},+)$ este cel nul.

32.* Să se arate că singurul morfism de grupuri de la $(\mathbb{Z}_n,+)$ la $(\mathbb{Z},+)$ este cel nul.

33.* Să se determine morfismele de grupuri de la $(\mathbb{Z}_m,+)$ la $(\mathbb{Z}_n,+)$. Determinați morfismele de la $\mathbb{Z}_6$ la $\mathbb{Z}_4$.

34.* 1) Arătați că există izomorfismul de grupuri: 1) $\mathbb{Z}_2\times\mathbb{Z}_2\simeq\mathcal{K}$ (grupul lui Klein); $\mathbb{Z}_2\times\mathbb{Z}_3\simeq\mathbb{Z}_6$.

2) $\mathbb{Z}_m\times\mathbb{Z}_n\simeq\mathbb{Z}_{mn}\Leftrightarrow(m,n)=1,\ m,n\in\mathbb{N}^*$.

35.* Fie $G=\left\{A_{x,y}=\begin{pmatrix}\hat{1} & \hat{3}x\\ \hat{5}y & \hat{1}\end{pmatrix}\middle|\, x,y\in\mathbb{Z}_{15}\right\}\subset\mathcal{M}_2(\mathbb{Z}_{15})$.

1)Arătați că $(G,\cdot)$ este grup abelian.

2) $(G,\cdot)\simeq(\mathbb{Z}_{15},+)$.

36.* Fie $G_1=\left\{A_a=\begin{pmatrix}\hat{1} & \hat{4}a\\ \hat{6}a & \hat{1}\end{pmatrix}\middle|\, a\in\mathbb{Z}_{12}\right\}$ și $G_2=\left\{A_{a,b}=\begin{pmatrix}\hat{1} & \hat{4}a\\ \hat{6}b & \hat{1}\end{pmatrix}\middle|\, a,b\in\mathbb{Z}_{12}\right\}$.

Arătați că $(G_1,\cdot)\simeq(G_2,\cdot)$.

37.* Fie $G=\left\{A_{a,b}=\begin{pmatrix}\hat{1} & \hat{2}a & \hat{2}b\\ \hat{3}a & \hat{1} & \hat{0}\\ \hat{3}b & \hat{0} & \hat{1}\end{pmatrix}\middle|\, a,b\in\mathbb{Z}_6\right\}$, $G_1=\left\{A_{\hat{0},a}\,\middle|\, a\in\mathbb{Z}_6\right\}$ și $G_2=\left\{A_{a,\hat{0}}\,\middle|\, a\in\mathbb{Z}_6\right\}$.

1) Arătați că $(G,\cdot),(G_1,\cdot),(G_2,\cdot)$ sunt grupuri.

2) $G\simeq G_1\times G_2\simeq\mathbb{Z}_6\times\mathbb{Z}_6$.

38.* Fie $G=\left\{A_{a,b}=\begin{pmatrix}a+\hat{2}b & b\\ \hat{4}b & a+\hat{3}b\end{pmatrix}\middle|\, a,b\in\mathbb{Z}_5,\ \det(A)=\hat{1}\right\}$.

1) Arătați că G este grup comutativ izomorf cu $(\mathbb{Z}_6,+)$

2) Determinați subgrupurile lui G.

Excursie matematică (facultativ)

* * * * *

Noțiuni suplimentare despre grupuri finite de permutări. Teorema lui Cayley

Fie $X \neq \varnothing$. *Prin permutare a mulțimii X se înțelege o aplicație bijectivă* $f : X \to X$. *Dacă* $X_n = \{1, 2, ..., n\}$, *atunci am notat permutările mulțimii* X_n *prin litere grecești* $\alpha, \beta, \gamma, \sigma...$. *Structura unei astfel de permutări este* $\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$, *unde în prima linie figurează elementele din domeniul de definiție, iar în a doua linie valorile funcției. Mulțimea lor am notat-o cu* S_n. *Această mulțime împreună cu operația de compunere a funcțiilor formează grup (în general necomutativ), numit grupul permutărilor de* n *elemente.*

*1. (**Ciclu**) Dacă există mulțimea* $\{i_1, i_2, ..., i_r\} \subseteq \{1, 2, ..., n\}$ *și* $\sigma \in S_n$ *astfel încât* $\sigma(i_1) = i_2, \sigma(i_2) = i_3, ..., \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1$ *și* σ *lasă pe loc celelalte elemente (adică* $\sigma(i) = i, i \notin \{i_1, i_2, ..., i_r\}$, *atunci* σ *se numește **ciclu de lungime** r.*

Pentru un astfel de ciclu se utilizează notația $\sigma = (i_1, i_2, ..., i_r)$ *sau schematic:* $i_1 \to i_2 \to i_3 \to ... \to i_{r-1} \to i_r$.

De exemplu, permutarea $\alpha = \begin{pmatrix} 1 & \mathbf{2} & 3 & \mathbf{4} & 5 & \mathbf{6} & \mathbf{7} \\ 1 & \mathbf{6} & 3 & \mathbf{7} & 5 & \mathbf{4} & \mathbf{2} \end{pmatrix}$ *se poate scrie sub formă de ciclu* $\alpha = (2, 6, 4, 7)$ *sau* $\alpha = (6, 4, 7, 2) = (4, 7, 2, 6) = (7, 2, 6, 4)$.

*2. (**Orbitele unei permutări**) Fie* $\sigma = \begin{pmatrix} 1 & 3 & 2 & 8 & 4 & 6 & 5 & 7 & 9 \\ 3 & 2 & 8 & 1 & 6 & 4 & 7 & 9 & 5 \end{pmatrix} \in S_9$ *o permutare pe care o scriem aranjând coloanele astfel: dacă* $\sigma(p) = q$, *atunci coloana care are în frunte pe q (ca element în domeniul de definiție) se scrie imediat după coloana care are pe p în frunte. De exemplu,* $\sigma(1) = 3 (p = 1, q = 3)$, *dă prima coloană* $\begin{pmatrix} 1 \\ 3 \end{pmatrix}$, *atunci a doua coloană în descrierea lui* σ *este* $\begin{pmatrix} 3 \\ 2 \end{pmatrix}$. *În acest mod elementele lui* σ *din prima linie se aranjează astfel încât* σ *acționează asupra lor astfel:* $1 \to 3 \to 2 \to 8 \to 1, 4 \to 6 \to 4, 5 \to 7 \to 9 \to 5$.

Submulțimile $\{1, 3, 2, 8\}, \{4, 6\}, \{5, 7, 9\}$ *sunt disjuncte și se numesc **orbitele lui*** σ.

Fiecărei submulțimi îi atașăm ciclul corespunzător $c_1 = (1,3,2,8), c_2 = (4,6), c_3 = (5,7,9)$ *și în plus* $\sigma = c_1 c_2 c_3 = (1,3,2,8)(4,6)(5,7,9)$.

Verificați că acești cicli, fiind pe mulțimi disjuncte, comută între ei!

Ciclii care nu sunt pe mulțimi disjuncte, în general, nu comută!

Fie $\sigma=(1,3,2,4), \beta=(1,7,6,2), \sigma,\beta\in S_7$. *Atunci* $\alpha\beta=(1,3,2,4)(1,7,6,2)=(1,7,6,4)(2,3)$

deoarece $1\xrightarrow[\beta]{}7\xrightarrow[\alpha]{}7,\ 7\xrightarrow[\beta]{}6\xrightarrow[\alpha]{}6,\ 6\xrightarrow[\beta]{}2\xrightarrow[\alpha]{}4, 2\xrightarrow[\beta]{}1\xrightarrow[\alpha]{}3,$

$3\xrightarrow[\beta]{}3\xrightarrow[\alpha]{}2, 5\xrightarrow[\beta]{}5\xrightarrow[\alpha]{}5$.

Analog, $\beta\alpha=(1,7,6,2)(1,3,2,4)=(1,3)(2,4,7,6)$.

Exercițiu. Arătați că avem egalitățile:

1) $\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 4 & 5 & 3 & 1 & 2\end{pmatrix}=(1,4)(2,5)$ *; 2)* $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 3 & 4 & 5 & 6 & 1 & 2 & 7\end{pmatrix}=(1,3,5)(2,4,6)$.

*3. (**Produs de cicluri scris ca produs de cicluri disjuncte**). Fie* $\alpha,\beta,\gamma\in S_6$, $\alpha=(1,4,3,2)$, $\beta=(1,6,2,5), \gamma=(1,5,3,6,2)$. *Atunci:* $\alpha\beta\gamma=(1,4,3,2)(1,6,2,5)(1,5,3,6,2)=(1,4,3)(2,6,5)$

deoarece:

$$1\xrightarrow{\gamma}5\xrightarrow{\beta}1\xrightarrow{\alpha}4$$
$$4\xrightarrow{\gamma}4\xrightarrow{\beta}4\xrightarrow{\alpha}3$$
$$3\xrightarrow{\gamma}6\xrightarrow{\beta}2\xrightarrow{\alpha}1$$

....

$$2\xrightarrow{\gamma}1\xrightarrow{\beta}6\xrightarrow{\alpha}6$$
$$6\xrightarrow{\gamma}2\xrightarrow{\beta}5\xrightarrow{\alpha}5$$
$$5\xrightarrow{\gamma}3\xrightarrow{\beta}3\xrightarrow{\alpha}2$$

Linia punctată separă cele două cicluri disjuncte.

Exercițiu. Arătați că au loc egalitățile (în dreapta lor sunt produse de cicli disjuncți):

1) $(1,9,2,3)(1,9,6,5)(1,4,8,7)=(1,4,8,7,2,3)(5,9,6)$ *;*

2) $(1,4,8,7)(1,9,6,5)(1,5,3,2,9)=(1,4,8,7)(2,6,5,3)$.

*4. (**Puterea unui ciclu**) Fie* $\sigma\in S_n$. *Atunci* $\sigma^k=\sigma\circ\sigma\circ...\circ\sigma$, *un* σ *apare de k ori în compunere,* $k\in\mathbb{N}^*$. *Dacă* σ *este ciclu, atunci* σ^k *va aplica fiecare întreg din ciclu cu k locuri mai departe.*

Fie ciclul $\sigma=(1,2,3,4,5,6,7,8,9)$. *Atunci:*

$\sigma^2=(1,3,5,7,9,2,4,6,8)=(1,3,5,7,9)(2,4,6,8)$ $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\end{pmatrix}$

$\sigma^3=(1,4,7,2,5,8,3,6,9)=(1,4,7)(2,5,8)(3,6,9)$ $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\end{pmatrix}$

*5. (**Orice permutare este produs de transpoziții**) Orice ciclu este produs de transpoziții. Se verifică uşor că:* $(i_1, i_2, ..., i_r) = (i_1, i_r)(i_1, i_{r-1})...(i_1, i_3)(i_1, i_2)$. *De exemplu,* $\sigma \in S_6, \sigma = (1,4,5) = (1,5)(1,4)$.

Exercițiu. Verificați egalitățile:

1) $(1,9,2,3)(1,9,6,5)(1,4,8,7) = (1,3)(1,2)(1,7)(1,8)(1,4)(5,6)(5,9)$;

2) $(1,4,8,7)(1,9,6,5)(1,5,3,2,9) = (1,7)(1,8)(1,4)(2,3)(2,5)(2,6)$.

Teorema lui Cayley

Grupurile de permutări pot servi ca modele pentru toate grupurile.
Mai precis, orice grup este izomorf cu un grup de permutări. De aici decurge importanța grupurilor de permutări în algebră. Are loc următoarea

> ***Teoremă** (Cayley). Orice grup este izomorf cu un grup de permutări.*

Demonstrația conține trei paşi:
***1)** Construcția permutărilor;*
***2)** Mulțimea acestor permutări cu compunerea este grup;*
***3)** Izomorfismul dintre grupul dat şi cel de la 2).*

Fie G un grup. Permutările pe care le utilizăm în demonstrație sunt aplicații definite pe mulțimea G.

Pentru fiecare $a \in G$, *definim* $f_a : G \to G,\ f_a(x) = ax, (\forall) x \in G$. *Să probăm că* f_a *este bijectivă.*

Din $f_a(x) = f_a(y),\ x, y \in G$ *rezultă* $ax = ay$, *iar de aici prin simplificare la stânga cu a în grupul G deducem* $x = y$. *Aceasta arată că* f_a *este injectivă.*

Fie $b \in G$ *(codomeniu). Atunci* $x = a^{-1}b \in G$ *şi* $f_a(x) = ax = a\left(a^{-1}b\right) = b$, *ceea ce arată că* f_a *este surjectivă (b a fost ales arbitrar din G).*

2) Să arătăm acum că mulțimea $G' = \{f_a \mid a \in G\}$, *împreună cu operația de compunere a permutărilor este un grup.*

Verificăm axiomele grupului.

Compunerea permutărilor pe G' este lege internă. Într-adevăr, fie $f_a, f_b \in G$. *Atunci:*

$\left(f_a \circ f_b\right)(x) = f_a\left(f_b(x)\right) = f_a(bx) = a(bx) = (ab)x = f_{ab}(x), (\forall) x \in G$.

Deci $f_a \circ f_b = f_{ab} \in G'$.

Compunerea funcțiilor întotdeauna este asociativă. Rămâne la fel şi în acest caz particular.

Elementul neutru este f_e*, unde e este elementul neutru din G, deoarece* $f_a \circ f_e = f_{ae} = f_a$ *şi* $f_e \circ f_a = f_{ea} = f_a$*, unde* $f_e(x) = x, (\forall) x \in G$.

Elemente simetrizabile. Pentru $f_a \in G', f_{a^{-1}} \in G'$ *este simetricul, deoarece* $f_a \circ f_{a^{-1}} = f_{aa^{-1}} = f_e$ *şi* $f_{a^{-1}} \circ f_a = f_{a^{-1}a} = f_e$*. Deci,* $\left(f_a\right)^{-1} = f_{a^{-1}}$.

3) Să arătăm izomorfismul de grupuri $(G, \cdot) \simeq (G', \circ)$.

Fie $F: G \to G', F(a) = f_a$*. Funcţia F este bijectivă deoarece este injectivă* $\left(F(a) = F(b) \Rightarrow f_a = f_b \Rightarrow a = b\right)$ *şi surjectivă (Pentru* $f_a \in G'$*, luăm* $a \in G$ *cu* $F(a) = f_a$*).*

Funcţia F este morfism de grupuri, deoarece $F(ab) = f_{ab} = f_a \cdot f_b = F(a)F(b), \forall a, b \in G$.

Cu aceasta teorema este complet demonstrată. ■

Aplicaţii. 1. Fie grupul $(G = \{\pm 1, \pm i\}, \cdot)$***. Să determinăm grupul G' de permutări cu care G este izomorf.***

R. Conform teoremei $G' = \left\{f_a : G \to G \mid a \in G, f_a(x) = ax\right\}$***. Deci*** $G' = \left\{f_1, f_{-1}, f_i, f_{-i}\right\}$***, unde*** $f_1(x) = x, (\forall) x \in G, f_{-1}(x) = -x, (\forall) x \in G, f_i(x) = ix, (\forall) x \in G, f_{-i}(x) = -ix, (\forall) x \in G$***. Funcţia care realizează izomorfismul este:*** $F: G \to G'$, $F(1) = f_1, F(-1) = f_{-1}, F(i) = f_i, F(-i) = f_{-i}$ ***sau cu ajutorul tablei:***

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$\xrightarrow{F}$

$\circ$	f_1	f_{-1}	f_i	f_{-i}
f_1	f_1	f_{-1}	f_i	f_{-i}
f_{-1}	f_{-1}	f_1	f_{-i}	f_i
f_i	f_i	f_{-i}	f_{-1}	f_1
f_{-i}	f_{-i}	f_i	f_1	f_{-1}

Compunând funcţiile din G' în tabla legii găsim că ea coincide cu cea din dreapta. Din acest motiv spunem că grupurile (finite– pentru care utilizăm tablele) sunt izomorfe dacă au tablele la fel structurate.

2. Fie $\left(G = \{\hat{2}, \hat{4}, \hat{6}, \hat{8}\} \subseteq \mathbb{Z}_{10}, \cdot\right)$ ***grupul multiplicativ cu element neutru*** $e = \hat{6}$***. Să se determine grupul de permutări G' cu care este izomorf G.***

R. Definim permutările din G' astfel: $f_{\hat{2}}, f_{\hat{4}}, f_{\hat{6}}, f_{\hat{8}} : G \to G$, $f_{\hat{2}}(x) = \hat{2}x, f_{\hat{4}}(x) = \hat{4}x, f_{\hat{6}}(x) = \hat{6}x$, $f_{\hat{8}}(x) = \hat{8}x, (\forall) x \in G$***. Funcţia care realizează izomorfismul este:*** $F: G \to G', F(\hat{2}) = f_{\hat{2}}, F(\hat{4}) = f_{\hat{4}}$, $F(\hat{6}) = f_{\hat{6}}, F(\hat{8}) = f_{\hat{8}}$***. Tabla lui G şi a imaginii ei prin F sunt date mai jos.***

$\cdot$	$\hat{2}$	$\hat{4}$	$\hat{6}$	$\hat{8}$
$\hat{2}$	$\hat{4}$	$\hat{8}$	$\hat{2}$	$\hat{6}$
$\hat{4}$	$\hat{8}$	$\hat{6}$	$\hat{4}$	$\hat{2}$
$\hat{6}$	$\hat{2}$	$\hat{4}$	$\hat{6}$	$\hat{8}$
$\hat{8}$	$\hat{6}$	$\hat{2}$	$\hat{8}$	$\hat{4}$

$\xrightarrow{F}$

$\circ$	$f_{\hat{2}}$	$f_{\hat{4}}$	$f_{\hat{6}}$	$f_{\hat{8}}$
$f_{\hat{2}}$	$f_{\hat{4}}$	$f_{\hat{8}}$	$f_{\hat{2}}$	$f_{\hat{6}}$
$f_{\hat{4}}$	$f_{\hat{8}}$	$f_{\hat{6}}$	$f_{\hat{4}}$	$f_{\hat{2}}$
$f_{\hat{6}}$	$f_{\hat{2}}$	$f_{\hat{4}}$	$f_{\hat{6}}$	$f_{\hat{8}}$
$f_{\hat{8}}$	$f_{\hat{6}}$	$f_{\hat{2}}$	$f_{\hat{8}}$	$f_{\hat{4}}$

Prin calcul verificați veridicitatea tablei a doua (de exemplu, $f_{\hat{2}} \circ f_{\hat{4}}(x) = f_{\hat{2}}(\hat{4}x) = \hat{8}x = f_{\hat{8}}(x)$).
Deci, cele două grupuri sunt izomorfe.

3. ***Fie*** $\left(G = \left\{ I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, M_1 = \begin{pmatrix} i & 0 \\ 0 & -1 \end{pmatrix}, M_2 = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, M_3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}, \cdot \right)$ ***grup multiplicativ. Să se determine grupul de permutări G' cu care este izomorf grupul G.***

R. ***În loc de I_2 scriem f_0, iar în loc de f_{M_k} scriem simplu $f_k, k = 1, 2, 3$. Permutările cerute sunt $f_0, f_k : G \to G, k = 1,2,3$, unde $f_0(X) = I_2 X = X$, $f_1(X) = M_1 X, f_2(X) = M_2 X, f_3(X) = M_3 X, (\forall) X \in G$.***
Izomorfismul este dat de $F : G \to G', F(I_2) = f_0, F(M_1) = f_1, F(M_2) = f_2, F(M_3) = f_3$. Avem tabla:

$\cdot$	I_2	M_1	M_2	M_3
I_2	I_2	M_1	M_2	M_3
M_1	M_1	M_3	I_2	M_2
M_2	M_2	I_2	M_3	M_1
M_3	M_3	M_2	M_1	I_2

$\xrightarrow{F}$

$\circ$	f_0	f_1	f_2	f_3
f_0	f_0	f_1	f_2	f_3
f_1	f_1	f_3	f_0	f_2
f_2	f_2	f_0	f_3	f_1
f_3	f_3	f_2	f_1	f_0

În plus, tabla pentru G' coincide cu tabla a doua.
De exemplu, $f_1 \circ f_1(X) = f_1(M_1 X) = M_1^2 X = M_3 X = f_3(X), (\forall) X \in G$. Deci $G \simeq G'$.

* * * * *

REZUMATUL CAPITOLULUI

Noțiuni. Proprietăți	Explicitare. Notații	Exemple
Lege de compoziție internă $M \neq \varnothing$ $f : M \times M \to M$	$(x, y) \to f(x, y)$. Pentru f se utilizează diverse notații: $*, \circ, \top, \bigcup, \oplus ...$ (M, f) = structură algebrică	1) $M = (1,2)$ cu $x * y = xy - x - y + 2$. Pentru $x, y \in M$ să arătăm că $x * y \in M$. Observăm că $x \in M \Leftrightarrow 1 < x < 2 \Leftrightarrow 0 < x - 1 < 1$, evident. Deci, $x * y \in M \Leftrightarrow 0 < x * y - 1 < 1 \Leftrightarrow$ $\Leftrightarrow 0 < (x-1)(y-1) < 1$ evident. 2) $M = \left\{ A(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle\vert a \in \mathbb{R} \right\}$ cu operația de înmulțirea a matricelor. Pentru $A(a), A(b) \in M$ să arătăm că $A(a)A(b) \in M$. Avem: $A(a)A(b) = A(a+b) \in M$.
	M finită, legea se dă prin tabla legii (Cayley): $\begin{array}{c\|ccc} * & \cdots & a_j & \cdots \\ \hline \vdots & & \vdots & \\ a_i & \cdots & a_i * a_j & \\ \vdots & & & \end{array}$	$M = \{1,2,3\}$ cu $x * y = \min(x, y)$ $\begin{array}{c\|ccc} * & 1 & 2 & 3 \\ \hline 1 & 1 & 1 & 1 \\ 2 & 1 & 2 & 2 \\ 3 & 1 & 2 & 3 \end{array}$
Parte stabilă $(M, *)$ structură algebrică, $H \subset M$, $H \neq \varnothing$ este parte stabilă a lui M în raport cu „ $*$ “	$\forall x, y \in H \Rightarrow x * y \in H$	1) $M = \{0,1,2,3\}$ cu $x * y =$ restul împărțirii lui $x + y$ la 4, este parte stabilă a lui N. Rezultă din tabla legii $\begin{array}{c\|cccc} \oplus & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array}$ 2) $M = \left\{ A(\alpha) = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \in \mathcal{M}_2(\mathbb{R}) \middle\vert \alpha \in \mathbb{R} \right\}$ este parte stabilă a lui $\mathcal{M}_2(\mathbb{R})$ în raport cu înmulțirea matricelor. Trebuie probat că pentru $A(\alpha), A(\beta) \in M \Rightarrow$ $\Rightarrow A(\alpha)A(\beta) \in M$. Avem $A(\alpha)A(\beta) =$ $= A(\alpha + \beta) \in M$.
Proprietăți generale ale legilor de compoziție:	$(M, *)$ structură algebrică	$M = \mathbb{R}$ cu $x * y = x + y - 1$
P$_1$. Asociativitatea	$(x * y) * z = x * (y * z)$, $(\forall) x, y, z \in M$	Avem: $(x * y) * z = (x + y - 1) * z =$ $= x + y - 1 + z - 1 =$ $= x + y + z - 2$ (1)

		$x*(y*z)=x*(y+z-1)=$ $=x+y+z-1-1=$ $=x+y+z-2$ (2) Din (1) şi (2) $\Rightarrow$ „$*$" este asociativă
P$_2$. Comutativitatea	$x*y=y*x, \forall x,y\in M$	$M=\left\{A(\alpha)=\begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix} \middle\| \alpha\in\mathbb{R}\right\}$ cu înmulțirea matricelor. Trebuie arătat că : $A(\alpha), A(\beta)\in M \Rightarrow A(\alpha)A(\beta)=A(\beta)A(\alpha)$ Avem: $A(\alpha)A(\beta)=A(\alpha+\beta)=A(\beta+\alpha)=A(\beta)A(\alpha)$ deoarece $\alpha+\beta=\beta+\alpha$
P$_3$. Elementul neutru	$e\in M$ este element neutru pentru „$*$" dacă $x*e=e*x=x, \forall x\in M$	$M=\mathbb{R}$ cu $x*y=xy+x+y$ $x*e=x, \forall x\in\mathbb{R} \Leftrightarrow xe+x+e=x \Leftrightarrow$ $\Leftrightarrow x(e+1)=0 \Rightarrow e=-1$
P$_4$. Elemente simetrizabile $(x')'=x$ $(x*y)'=y'*x'$	$x\in M$ este simetrizabil în raport cu „$*$" dacă există $x'\in M$ cu $x*x'=x'*x=e$ ● Dacă $*=+$, atunci x' este opusul lui x, $x'=-x$ ● Dacă $*=\cdot$, atunci x' este inversul lui x, $x'=x^{-1}$	$M=\mathbb{Z}$ cu $x*y=x+y-xy$ Se obține: $e=0$. Din $x*x'=0 \Rightarrow x+x'-xx'=0 \Rightarrow$ $\Rightarrow x'(1-x)=-x \Rightarrow x'=-\dfrac{x}{1-x}, x\neq 1$ Din $x'\in\mathbb{Z} \Rightarrow x\in\{0,2\}$. Pentru $x=0\Rightarrow x'=0$; pentru $x=2\Rightarrow x'=2$
Monoid $(M,*)$, $M\neq\varnothing$ cu axiomele: M$_1$) „$*$" asociativă M$_2$) element neutru	M$_1$) $(x*y)*z=x*(y*z)$, $\forall x,y,z\in M$ M$_2$) $\exists e\in M$, astfel încât $x*e=e*x=x$, $\forall x\in M$	$(\mathbb{Z},+)$ = monoid aditiv al numerelor întregi. M$_1$) + este asociativă pe $\mathbb{Z}$ M$_2$) $e=0$, deoarece $x+0=0+x=x, \forall x\in\mathbb{Z}$
Grup $(G,*)$, $G\neq\varnothing$ cu axiomele: G$_1$) „$*$" asociativă G$_2$) element neutru G$_3$) elemente simetrizabile	G$_1$) $(x*y)*z=x*(y*z)$, $\forall x,y,z\in G$ G$_2$) $\exists e\in G, x*e=e*x=x$, $\forall x\in G$ G$_3$) $x\in G, \exists x'\in G$, $x*x'=$ $=x'*x=e, \forall x\in G$.	$G=\mathbb{R}-\left\{\dfrac{1}{2}\right\}$, $x*y=2xy-x-y+1$ G$_1$) $(x*y)*z=(2xy-x-y+1)*z=$ $=2(2xy-x-y+1)z-2xy+x+y-1-z+1=$ $=4xyz-2(xy+xz+yz)+x+y+z,$ (1) $x*(y*z)=x*(2yz-y-z+1)=$ $=2x(2yz-y-z+1)-x-(2yz-y-z+1)+1=$ $=4xyz-2(xy+xz+yz)+x+y+z$ (2) 1) și (2) $\Rightarrow$ „$*$" asociativă; G$_2$) $x*e=x, \forall x\in G \Leftrightarrow 2xe-x-e+1=x,$ $\forall x\in G \Leftrightarrow e(2x-1)=2x-1, \forall x\in G \Rightarrow$ $\Rightarrow e=1\in G$ G$_3$) $x\in G, \exists x'\in G, x*x'=e \Rightarrow$ $2xx'-x-x'+1=1 \Leftrightarrow x'=\dfrac{x}{2x-1}$ Avem $x'\neq\dfrac{1}{2} \Leftrightarrow 2x\neq 2x-1$

Grupuri speciale: **1) Grup abelian** **Grupul $(G,*)$ este abelian (comutativ) dacă: G_4) „$*$“ comutativă**	**G_4) $x*y=y*x, \forall x,y\in G$**	**G_4)** **$x*y=2xy-x-y+1=2yx-y-x+1=$** **$=y*x, \forall x,y\in G$**
2) Grup ciclic generat de $x\in G$. Ordinul unui element $x\in G$	**$<x>=\{x^k \mid k\in\mathbb{Z}\}$, puterile întregi ale lui x.** **ord(x) = n dacă $x^n=e$ şi $n\in N$ este cel mai mic număr cu această proprietate.**	**$i\in\mathbb{C}\Rightarrow <i>=\{i^k \mid k\in\mathbb{Z}\}=\{-1,1,-i-i\}$.** **ord (–1) = 2 pentru că $(-1)^2=1$, ord (i)=4 deoarece $i^4=1$**
3) Grup finit **G are un număr finit de elemente. Acest număr este ordinul grupului**		**1) Grupul rădăcinilor de ordin n ale unităţii** **$U_n=\{z\in\mathbb{C} \mid z^n=1\}$, $(U_n,\cdot)$** **2) grupul claselor de resturi modulo n în raport cu adunarea: $\mathbb{Z}_n=\{\hat{0},\hat{1},...,\widehat{n-1}\},(\mathbb{Z}_n,+)$**
Subgrup **$(G,*)$ grup şi $H\subseteq G, H\neq\varnothing$** **$(H,*)$ este subgrup al lui G dacă $(H,*)$ este grup**	**Criteriu** **$(H,*)$ este subgrup dacă** **$\forall x,y\in H\Rightarrow x*y^{-1}\in H$**	**$(\mathbb{Z},+)$ subgrup al lui $(\mathbb{Q},+)$** **$(\mathbb{Q},+)$ subgrup al lui $(\mathbb{R},+)$** **$(\mathbb{R}^*,\cdot)$ subgrup al lui $(\mathbb{C}^*,\cdot)$** **$(n\mathbb{Z},+)$ subgrup al lui $(\mathbb{Z},+)$** **$x=nk_1,\ y=nk_2,k_1,k_2\in\mathbb{Z}\Rightarrow$** **$\Rightarrow x-y=n(k_1-k_2)\in n\mathbb{Z}$**
Morfism de grupuri	**$(G_1,*)$, $(G_2,\circ)$ grupuri.** **$f:G_1\to G_2$ este morfism de grupuri dacă** **$f(x*y)=f(x)\circ f(y)$** **$\forall x,y\in G_1$**	**$f:(\mathbb{R},+)\to(\mathbb{R}^*,\cdot), f(x)=e^x$** **$f(x+y)=e^{x+y}=e^x\cdot e^y=f(x)f(y)$,** **$(\forall)x,y\in\mathbb{R}$**
Izomorfism de grupuri	**$f:G_1\to G_2$, dacă** **1) f este bijectivă;** **2) f este morfism de grupuri**	**$(\mathbb{R},+)\simeq((0,\infty),\cdot)$** **$f:\mathbb{R}\to(0,\infty),\ f(x)=e^x$.** **1) f este bijectivă** **2) f este morfism de grupuri** **$f(x+y)=e^{x+y}=e^x\cdot e^y=f(x)f(y)$,** **$\forall x,y\in\mathbb{R}$**

Teste de evaluare

TESTUL 1

VARIANTA A

1. Fie $G=(2,\infty)$ şi pe $\mathbb{R}$ legea de compoziţie: $x*y=xy-2x-2y+a,\ x,y,a\in\mathbb{R}$. Să se determine a astfel încât G să fie parte stabilă a lui $\mathbb{R}$ în raport cu legea „$*$“.

2. Pe mulţimea $\mathbb{R}$ a numerelor reale se consideră legea de compoziţie internă $x*y=xy+x+my$. Să se determine $m\in\mathbb{R}$ astfel încât legea să fie asociativă.

3. Fie $a,b\in\mathbb{R}^*$.Pe mulţimea $(0,\infty)$ definim operaţia $x*y=e^{a\ln x-b\ln y}$, $\forall x,y>0$. Să se determine a şi b astfel încât legea să fie comutativă şi asociativă.

4. Pe mulţimea $E=\{1,2,3,4\}$ se defineşte legea de compoziţie $x*y=$ restul împărţirii lui x^y la 5, pentru orice $x,y\in E$.

Fie $A=\{x\in E\,|\,4*x=1\}$, $S=\sum\limits_{x\in A}x$, $B=\{x\in E\,|\,x*4=3\}$. Să se determine S şi B.

5. Fie mulţimea matricelor:

$$M=\left\{A(a)\,\middle|\,A(a)=\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}, a\in\mathbb{R}\right\}.$$

1) Demonstraţi că M împreună cu operaţia de înmulţire a matricelor formează grup abelian.

2) Arătaţi că grupurile $(\mathbb{R},+)$ şi $(M,\cdot)$ sunt izomorfe.

3) Calculaţi $A^n,\ n\in\mathbb{N}^*$.

6. Se consideră în $\mathbb{Z}_7$ sistemul :

$$\begin{cases}ax+\hat{3}y+\hat{3}z=\hat{2}\\ \hat{6}x+\hat{4}y+\hat{2}z=\hat{6}\\ \hat{3}x+\hat{2}y+\hat{4}z=\hat{3}.\end{cases}$$

Fie $A=\{a\in\mathbb{Z}_7\,|\,\text{sistemul este compatibil}\}$, $S=\sum\limits_{a\in A}a$ şi $V=\tilde{x}^2+\tilde{y}^2+\tilde{z}^2$, unde $(\tilde{x},\tilde{y},\tilde{z})$ este soluţia sistemului pentru $a=\hat{2}$. Să se determine S şi V.

VARIANTA B

1. Să se determine $a\in\mathbb{R}$ pentru care mulţimea $A=[a,\infty)$ este parte stabilă faţă de operaţia $x*y=xy+x+y$.

2. Să se determine valorile parametrului real a, astfel încât legea de compoziţie pe $\mathbb{R}$, definită prin $x*y=a(x+y)-xy, \forall x,y\in\mathbb{R}$ să fie asociativă.

3. Pe $\mathbb{R}$ se defineşte legea de compoziţie $x*y=xy+2ax+by,\ x,y,a,b\in\mathbb{R}$. Determinaţi toate valorile lui a şi b astfel încât legea să fie comutativă şi asociativă.

4. Pe mulţimea $G=(2,\infty)$ se defineşte legea de compoziţie $x*y=xy-2x-2y+6$, $\forall x,y\in G$. Fie S_1 suma elementelor nesimetrizabile în raport cu legea „$*$“ şi S_2 suma soluţiilor ecuaţiei $x*x=11$. Să se precizeze S_1 şi S_2.

5. Fie mulţimea matricelor:

$$G=\left\{A(x)=\begin{pmatrix}1 & x & 0\\ 0 & 1 & 0\\ 0 & 0 & 3^x\end{pmatrix}\,\middle|\,x\in\mathbb{R}\right\}.$$

1) Arătaţi că G împreună cu operaţia de înmulţire a matricelor este grup comutativ.

2) Arătaţi că grupurile $(\mathbb{R},+)$ şi $(G,\cdot)$ sunt izomorfe.

3) Să se calculeze $A^n(2)$.

6. Se consideră sistemul de ecuaţii cu coeficienţi în $\mathbb{Z}_5$: $\begin{cases}x+y+z=\hat{1}\\ \hat{2}x+\hat{3}y+z=\hat{1}\\ \hat{4}x+\hat{4}y+\hat{3}z=\hat{1}.\end{cases}$

Fie Δ, S determinantul sistemului şi respectiv suma soluţiilor. Să se determine Δ şi S.

7. Să se arate că mulţimea:

$$H=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\right\}$$

este subgrup al matricelor pătratice de ordin doi inversabile în raport cu înmulţirea.

7. Să se arate că mulţimea:

$$H=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}i&0\\0&-i\end{pmatrix},\begin{pmatrix}-i&0\\0&i\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\right\}$$

este subgrup al matricelor din $\mathcal{M}_2(\mathbb{C})$ inversabile în raport cu înmulţirea.

TESTUL 2

VARIANTA A

1. Pe $\mathbb{C}$ definim operaţia $z_1 * z_2 = (1-i)z_1z_2$.

1) Este asociativă legea „ $*$ “?

2) Să se determine elementul neutru al operaţiei.

3) Să se rezolve ecuaţia $z*(1+i)=2i$, $z\in\mathbb{C}$.

2. Pe intervalul $(1,\infty)$ se consideră operaţia: $x*y=1+(x-1)^{\lg(y-1)}$. Să se arate că:

1) legea „ $*$ “ este o lege de compoziţie pe $(1,\infty)$;

2) legea „ $*$ “ este asociativă şi comutativă.

3. Pe $\mathbb{Z}$ se consideră legea:

$x*y=xy+ax+7y+b$, $a,b\in\mathbb{R}$

Să se determine a, b pentru care legea „ $*$ “ este asociativă.

4. Să se determine valorile parametrului real λ astfel încât intervalul $(1,\infty)$ să fie parte stabilă a mulţimii $\mathbb{R}$ în raport cu legea: $x*y=xy-x-y+\lambda-2$.

5. Pe $\mathbb{R}$ se definesc legile de compoziţie:

$a*b=3a+3b+5ab+2$,

$a\circ b=2a+2b+2ab+1$.

Să se rezolve sistemul:

$$\begin{cases}(x+y)*4=60\\(x-y)\circ 3=39.\end{cases}$$

6. Fie $t\in\mathbb{R}$ fixat. Pentru $a>0$ definim

$$f_a:\mathbb{R}\to\mathbb{R},\ f(x)=\begin{cases}ax+t-at,\ x<t\\ \dfrac{1}{a}x+r-\dfrac{t}{a},x\ge t.\end{cases}$$

1) Să se arate că $M=\{f_a \mid a>0\}$ are structură de grup în raport cu operaţia de compunere a funcţiilor.

2) Să se arate izomorfismul de grupuri: $(M,\circ)\simeq(\mathbb{R}_+^*,\cdot)$.

VARIANTA B

1. Pe $\mathbb{C}$ se defineşte operaţia: $z_1*z_2=$ $=z_1z_2+i(z_1+z_2)-1-i$.

1) Să se arate că „ $*$ “ este asociativă.

2) Să se determine elementul neutru.

3) Să se rezolve ecuaţia $z*(2-i)=3+i$, $z\in\mathbb{C}$.

2. Să se determine $m\in\mathbb{R}$ pentru care legea $x*y=xy+3x+5y+m$ este asociativă pe $\mathbb{R}$.

3. Pe $\mathbb{R}$ se consideră legea :

$x*y=xy+a(x+y), a\in\mathbb{R}$.

Să se determine a pentru care „ $*$ “ este asociativă.

4. Pe $\mathbb{R}$ definim operaţia $x*y=xy-$ $-4(x+y)+\alpha$. Să se determine $\alpha\in\mathbb{R}$ pentru care mulţimea $G=[4,\infty)$ este parte stabilă a lui $\mathbb{R}$ în raport cu „ $*$ “.

5. Pe $\mathbb{R}$ se defineşte legea de compoziţie $a*b=ab-2(a+b)+6$. Fie S suma elementelor din $\mathbb{R}$ care coincid cu simetricele lor faţă de legea „ $*$ “ şi

$A=\{x\in\mathbb{R} \mid x*x*x+25=0\}$.

Precizaţi S şi A.

6. Se consideră funcţiile:

$$f_i:\mathbb{R}-\left\{\pm\frac{\sqrt3}{3}\right\}\to\mathbb{R}, f_1(x)=x,\ f_2(x)=\frac{x+\sqrt3}{1-x\sqrt3},$$

$$f_3(x)=\frac{x-\sqrt3}{1+x\sqrt3}.$$

1) Să se arate că $G=\{f_1,f_2,f_3\}$ este grup în raport cu operaţia de compunere a funcţiilor.

2) Să se demonstreze izomorfismul de grupuri: $(G,\circ)\simeq\left(\left\{1,\dfrac{-1\pm i\sqrt3}{2}\right\},\cdot\right)$.

7. Fie $M=\left\{\begin{pmatrix} a & b \\ \hat{0} & \hat{1}\end{pmatrix} \middle| a,b\in\mathbb{Z}_7\right\}$. Să se determine ord (A), unde $A=\begin{pmatrix} \hat{1} & \hat{1} \\ \hat{0} & \hat{1}\end{pmatrix}$.

7. Fie $M=\left\{\begin{pmatrix} a & b \\ \hat{0} & \hat{1}\end{pmatrix} \middle| a,b\in\mathbb{Z}_7\right\}$. Să se determine ord (A), unde $A=\begin{pmatrix} \hat{3} & \hat{0} \\ \hat{0} & \hat{1}\end{pmatrix}$.

TESTUL 3 (grilă)

VARIANTA A

1. Pe $\mathbb{R}$ se defineşte legea de compoziție $x*y=xy-2x-2y+m,\ m\in\mathbb{R}$. Legea de compoziție admite element neutru pentru:
a) $m=4$; b) $m=6$; c) $m=-6$.

2. Fie $M=\left\{A(x)=\begin{pmatrix} x & 0 & x \\ 0 & 0 & 0 \\ x & 0 & x\end{pmatrix} \middle| x\in\mathbb{R}^*\right\}\subset\mathcal{M}_3(\mathbb{R})$

şi operația de înmulțire a matricelor. Atunci elementul neutru din M în raport cu înmulțirea este:

a) I_3; b) nu există; c) $A\left(\frac{1}{2}\right)$.

3. Pentru orice $x,y\in\mathbb{R}$ se defineşte legea $x*y=\ln(e^x+e^y)$. Mulțimea soluțiilor ecuației $(x*x)*x=0$ este:

a) $\{-\ln 3\}$; b) $\{\ln\sqrt{3}\}$; c) $\left\{-\ln\frac{1}{3}\right\}$.

4. Pe mulțimea $\mathbb{Z}_7$ a claselor de resturi modulo 7 definim legea de compoziție $a*b=ab+\hat{5}(a+b)+\hat{6}$. Dacă x' este simetricul lui x în raport cu legea de compoziție „$*$“, notăm $A=\{x\in\mathbb{Z}_7 \mid x'=x\}$. Atunci:

a) $A=\{\hat{1},\hat{2}\}$; b) $A=\{\hat{1},\hat{3}\}$; c) $A=\{\hat{2},\hat{4}\}$.

5. În $\mathbb{Z}_8$ se consideră sistemul:

$$\begin{cases}\hat{2}x+y+\hat{4}z=\hat{2}\\ \hat{3}x+\hat{2}y+z=\hat{4}\\ \hat{6}x+\hat{4}y+\hat{5}z=\hat{1}.\end{cases}$$

Dacă Δ este determinantul matricei sistemului, $(\tilde{x},\tilde{y},\tilde{z})$ soluția sistemului şi $\alpha=\tilde{x}^2+$

VARIANTA B

1. Pe $\mathbb{R}$ se defineşte legea de compoziție $x*y=xy-ax+by$. Valorile lui a, b pentru care $(\mathbb{R},*)$ este monoid sunt:

a) $(a=b=0$ sau $a=-1, b=1)$; b) $a=1$, $b=-1$; c) $a=1, b=2$.

2. Fie $M=\left\{A(x)=\begin{pmatrix} 3^x & 0 & 0 \\ 0 & 1 & 0 \\ 0 & x & 1\end{pmatrix} \middle| x\in\mathbb{R}\right\}\subset\mathcal{M}_3(\mathbb{R})$

şi operația de înmulțire a matricelor. Atunci elementul neutru din M în raport cu înmulțirea este:

a) $A(1)$ b) $A(0)$; c) $A\left(\frac{1}{2}\right)$.

3. Pe $\mathbb{C}$ se consideră legea de compoziție: $x*y=xy-i(x+y)-1+i$. Mulțimea soluțiilor ecuației $(x*x)*x=1+i$ este:

a) $\{\pm1,\pm i\}$; b) $\{\pm i, 1\pm i\}$; c) $\{1\pm i, 0, 2i\}$.

4. Pe mulțimea $\mathbb{Z}$ se defineşte legea de compoziție: $x*y=2xy-3x-3y+6$. Dacă p este numărul elementelor simetrizabile în raport cu legea „$*$“, atunci:

a) $p=1$; b) $p=2$; c) $p=3$.

5. În $\mathbb{Z}_5$ se consideră sistemul:

$$\begin{cases}\hat{3}x+\hat{2}y+z=\hat{1}\\ x+\hat{3}y+\hat{2}z=\hat{3}\\ \hat{2}x+y+\hat{3}z=\hat{0}.\end{cases}$$

Dacă Δ este determinantul matricei sistemului, $(\bar{x},\bar{y},\bar{z})$ este soluția sistemului, iar

$+\tilde{y}^2+\tilde{z}^2$, atunci:

a) $\Delta=\hat{3}, \alpha=\hat{2}$; b) $\Delta=\hat{5}, \alpha=\hat{4}$; c) $\Delta=\hat{3}$, $\alpha=\hat{5}$.

6. Pe $\mathbb{R}$ se defineşte legea de compoziţie:
$$x*y=2xy-6x-6y+21.$$

Atunci: $\underbrace{x*x*...*x}_{n}$, $x\in\mathbb{R}, n\in\mathbb{N}^*$ este egal cu:

a) $2^{n-1}(x-3)^n+3$;

b) $2^{n-1}(x-6)^n+3$; c) $2^{n-1}(x-2)^n+3$.

7. Fie $G=(2,\infty)$ şi legea $x\circ y=xy-2x-y+6$ şi $G'=(3,\infty)$ şi legea $x*y=xy-3x-3y+12$, iar $f:G\to G'$ izomorfism de grupuri, $f(x)=mx+n$. Atunci:

a) $m=n=1$; b) $m=n=-1$; c) $m=1$, $n=-1$.

$\beta=\overline{x}^{-2}+\overline{y}^{-2}+\overline{z}^{-2}$, atunci:

a) $\Delta=\hat{3}, \beta=\hat{3}$; b) $\Delta=\hat{3}, \beta=\hat{1}$; c) $\Delta=\hat{5}$, $\beta=\hat{3}$.

6. Pe $\mathbb{R}-\left\{\frac{1}{2}\right\}$ se defineşte legea de compoziţie: $x*y=2xy-x-y+1$. Atunci: $\underbrace{x*x*...*x}_{n}$, $x\in\mathbb{R}-\left\{\frac{1}{2}\right\}, n\in\mathbb{N}^*$ este egal cu:

a) $\frac{1}{2}(2x-1)^n+1$; b) $\frac{1}{2}(2x-1)^n+\frac{1}{2}$;

c) $\frac{1}{2}(2x-1)^n+\frac{1}{3}$.

7. Pe $\mathbb{Z}$ se consideră legile :
$x\circ y=x+y+5$, $x*y=x+y-5$, iar $f:(\mathbb{Z},\circ)\to(\mathbb{Z},*)$, $f(x)=x+m, m\in\mathbb{R}$ un izomorfism de grupuri. Atunci:

a) $m=1$; b) $m=10$; c) $m=9$.

2. INELE ŞI CORPURI

În acest capitol se studiază două structuri algebrice mai complexe decât cele abordate în capitolul precedent şi anume cele de inel şi corp. Se consideră o mulţime nevidă împreună cu două operaţii şi un set de axiome pentru aceste operaţii. Sunt ilustrate exemple semnificative de inele şi corpuri. Se dau reguli generale de calcul într-un inel şi corp. O atenţie specială este acordată inelului de polinoame, de nedeterminată X, cu coeficienţi în corpul $K \in \left\{\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p, p \text{ prim}\right\}$, $K[X]$.

Este prezentată aritmetica acestui inel în care domină cele două teoreme fundamentale: teorema împărţirii cu rest şi teorema de descompunere în factori ireductibili. Numeroasele exemple vin să ilustreze partea teoretică. Sunt prezentate, în particular, polinoame cu coeficienţi în $\mathbb{Z}, \mathbb{Q}$ şi $\mathbb{R}$ şi se dau caracterizări ale rădăcinilor acestora; se evidenţiază relaţiile între rădăcinile polinomului şi coeficienţii acestuia (relaţiile lui Viète).

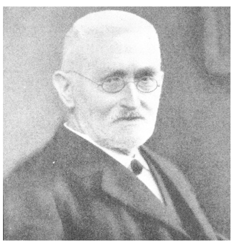
Ultima parte a capitolul se referă la rezolvarea ecuaţiilor cu coeficienţi întregi, raţionali, reali, complecşi. Problemele rezolvate conţin una sau mai multe metode de abordare prezentate detaliat.

Problemele propuse ilustrează prin varietate toate conceptele teoretice discutate, ele având corespondent în problemele rezolvate.

Istoric. Conceptele de inel şi corp s-au impus în secolele XIX–XX. Matematicianul german Dedekind (1831–1916) – şi-a luat doctoratul sub conducerea lui Gauss (1777–1855) – este considerat „fondatorul algebrei abstracte“. El a introdus conceptele de inel şi corp. Dedekind este cunoscut în analiza matematică prin tehnica de construcţie a numerelor reale utilizând conceptul de „tăietură“ (a lui Dedekind). Contribuţii remarcabile în domeniul algebrei abstracte a avut matematiciana germană Emmy Noether (1882–1935).

Problema rezolvabilităţii ecuaţiilor a fost tratată de Lagrange, Ruffini şi Abel.

Dar cel care o abordează aprofundat este E. Galois (1811–1832). F. Viète (1540–1603, matematician francez) este considerat unul dintre creatorii algebrei, stabilind relaţii între rădăcinile şi coeficienţii unei ecuaţii algebrice.

PIONIERI AI MATEMATICII	
R. DEDEKIND (1831–1916)	A.E. NOETHER (1882–1935)
Matematicieni germani	
	
CONTRIBUŢII	CONTRIBUŢII
• *algebră abstractă* • *analiză matematică*	• *algebră abstractă* • *teoria relativităţii*

2.1. INELE

1. DISTRIBUTIVITATE

Structurile algebrice ($\mathbb{Z}$, +), ($\mathbb{Z}, \cdot$) au fost pentru noi primele exemple de monoizi. Mai mult ($\mathbb{Z}$, +) a devenit mai târziu grup abelian (chiar ciclic). Totuşi, aşa cum aţi avut ocazia să studiaţi până acum în liceu, aceste structuri sunt reunite împreună pentru a da ceea ce se numeşte în matematică structura de inel. Una din legile importante ale aritmeticii elementare este distributivitatea înmulţirii în raport cu adunarea $a(b + c) = ab + ac$, $(b + c)a = ba + ca$, $(\forall)a, b, c \in \mathbb{Z}$.

Dacă se încearcă să se reunească, de exemplu, structurile algebrice ($\mathbb{Z}$, +), ($\mathbb{Z}, \circ$), unde $a \circ b = a + b + ab$ nu mai are loc distributivitatea legii $\circ$ în raport cu legea +

deoarece $\quad a \circ (b + c) = a + b + c + a(b + c) = a + b + c + ab + ac$, (1)

iar $\quad a \circ b + a \circ c = a + b + ab + a + c + ac = 2a + b + c + ab + ac$, (2)

ceea ce arată că $(\exists)a, b, c \in \mathbb{Z}$ pentru care $a \circ (b + c) \neq a \circ b + a \circ c$.

Definiţie. Fie $*$ şi $\circ$ două operaţii pe aceeaşi mulţime *M*.
Se spune că operaţia $*$ este **distributivă la stânga** faţă de operaţia $\circ$ dacă:

$$x * (y \circ z) = (x * y) \circ (x * z), (\forall)x, y, z \in M, \qquad (1).$$

Se spune că operaţia $*$ este **distributivă la dreapta** faţă de operaţia $\circ$ dacă:

$$(y \circ z) * x = (y * x) \circ (z * x), (\forall)x, y, z \in M, \qquad (2).$$

Se spune că operaţia $*$ este **distributivă** faţă de operaţia $\circ$ dacă este **distributivă la dreapta şi la stânga,** adică dacă au loc (1) şi (2).

Pentru a arăta că legea „$*$“ nu este distributivă în raport cu legea „$\circ$“ găsim $x, y, z \in M$ pentru care $x * (y \circ z) \neq (x * y) \circ (x * z)$ sau $(y \circ z) * x \neq (y * x) \circ (z * x)$.

Observaţii. 1) Dacă operaţia $*$ este **comutativă,** atunci (1) şi (2) sunt evident echivalente şi deci se reţine ca definiţie una din ele.

2) Dacă $H \subset M$ stabilă faţă de operaţiile $*$ şi $\circ$ iar $*$ este distributivă în raport cu $\circ$ atunci proprietatea se păstrează şi pe submulţimea *H*.

Exemple cunoscute

1. Înmulţirea este distributivă în raport cu adunarea pe $\mathbb{C}$ (şi evident pe submulţimile lui $\mathbb{C}, \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$).

2. În mulţimea matricelor pătratice $\mathcal{M}_n(\mathbb{C})$ înmulţirea este distributivă în raport cu adunarea (cum înmulţirea matricelor nu este comutativă; aici putem vorbi de distributivitate laterală, la stânga şi la dreapta a înmulţirii faţă de adunare).

3. **Pe $\mathcal{F}(\mathbb{R})$ considerăm adunarea şi compunerea funcţiilor. Atunci se ştie compunerea funcţiilor este distributivă în raport cu adunarea funcţiilor (Cum prima operaţie, compunerea, nu este comutativă şi aici se poate vorbi de distributivitate laterală) când avem:**

$$f\circ(g+h)=f\circ g+f\circ h \text{ şi } (g+h)\circ f=g\circ f+h\circ f,(\forall)f,g,h\in\mathcal{F}(\mathbb{R}).$$

4. **Pe mulţimea $\mathcal{P}(M)$ a părţilor lui M, am definit operaţiile $\cup$ (reuniune) şi $\cap$ (intersecţie). Ştim că una din legi este distributivă în raport cu cealaltă, adică**

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

$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$, $(\forall)A,B,C\in\mathcal{P}(M)$.

Alte exemple

1. **Pe mulţimea numerelor reale se consideră legile de compoziţie:**

a) $x\circ y=x+y-1,\quad x*y=x+y-xy$;

b) $x\circ y=x+y-5,\quad x*y=3xy-15(x+y)+80$;

Arătaţi că pentru fiecare caz a doua lege este distributivă în raport cu prima lege.

R. Pentru fiecare caz trebuie să verificăm egalitatea (deoarece $*$ este comutativă):

$$x*(y\circ z)=(x*y)\circ(x*z),(\forall)x,\ y,\ z\in\mathbb{R}\ .$$

Se calculează separat fiecare membru şi apoi se compară.

a) Avem: $x*(y\circ z)=x*(y+z-1)=x+y+z-1-x(y+z-1)=2x+y+z-xy-xz-1$ (1) şi $(x*y)\circ(x*z)=(x+y-xy)\circ(x+z-xz)=(x+y-xy)+(x+z-xz)-1=2x+y+z-xy-xz-1$ (2).

Din (1) şi (2) se deduce egalitatea celor doi membri. Prin urmare $*$ este distributivă în raport cu $\circ$.

b) Exerciţiu.

Probleme propuse

1. **Arătaţi că a doua lege de compoziţie este distributivă în raport cu prima lege pe mulţimea M în cazurile:**

a) $x\circ y=x+y+1,\ x*y=xy+x+x,\ M=\mathbb{Z}$;

b) $x\circ y=x+y-3,\ x*y=xy+3(x+y)+6,\ M=\mathbb{Z}$;

c) $x\circ y=x+y-3,\ x*y=3(x+y)-xy-6,\ M=\mathbb{R}$;

d) $z_1\circ z_2=z_1+z_2,\ z_1*z_2=a_1a_2+ib_1b_2,\ M=\mathbb{C},\ z_k=a_k+ib_k,\ k=1,2$.

2. **Pe $\mathbb{R}$ se consideră legile de compoziţie: $x\circ y=x+y+a,\ x*y=xy+2x+2y+b,\ a,b\in\mathbb{C}$**
Să se determine a, b, astfel încât a doua lege să fie distributivă în raport cu prima lege.

3. **Pe $\mathbb{C}$ se consideră legile de compoziţie: $x\circ y=x+y+i,\ x*y=xy+ax+by+c,\ a,b,c\in\mathbb{C}$.**
Să se determine a, b, c astfel încât a doua lege să fie distributivă în raport cu prima lege.

4. **Pe $\mathcal{M}_2(\mathbb{R})$ se definesc legile de compoziţie: $A\circ B=A+B+cI_2$, $A*B=AB+a(A+B)+bI_2$, $a,b,c\in\mathbb{R}$. Determinaţi a, b, c pentru care a doua lege este distributivă în raport cu prima lege.**

2. INELE

Definiție. Se numește **inel unitar** un triplet $(A, +, \cdot)$, $A \neq \varnothing$ unde + și $\cdot$ sunt două operații pe A, numite **adunarea** și respectiv **înmulțirea** pentru care:

A_1) $(A, +)$ este grup abelian;

A_2) $(A, \cdot)$ este monoid;

A_3) Înmulțirea este **distributivă** față de adunare.

Dacă, în plus, înmulțirea pe A este **comutativă**, adică $xy = yx, (\forall)x, y \in A$, atunci spunem că inelul este comutativ.

Observații. 1) Folosim pentru inel ca mulțime litera A de la cuvântul *anneau* (din franceză) care înseamnă inel.

2) Inelul va fi notat de regulă cu $(A, +, \cdot)$ punând în evidentă în acest fel rolul diferit al celor două operații; prima operație va fi totdeauna cea față de care mulțimea A are structură de grup comutativ. Structura $(A, +)$ se numește **grupul aditiv al inelului**. Elementul neutru al grupului $(A, +)$, notat cu 0, se numește **elementul nul al inelului**. A doua operație este cea distributivă față de prima și în plus $(A,\cdot)$ este monoid numit **monoidul multiplicativ al inelului**. Se vede că mulțimea A are o structură mai săracă față de cea de-a doua operație, cea multiplicativă. Pentru un inel unitar, elementul neutru în raport cu înmulțirea va fi notat cu simbolul 1, numit **element unitate** al inelului. Axioma A_3) face legătura între cele două operații.

3) Explicitând condițiile din definiția inelului avem:

A_1) $(A, +)$ **grup abelian** $\Leftrightarrow \begin{cases} G_1) + \text{ este asociativă;} \\ G_2) + \text{ este comutativă;} \\ G_3) + \text{ admite element neutru, notat cu 0, numit} \\ \qquad \textbf{element nul;} \\ G_4) \text{ Orice element din } A \text{ are un opus față de } +. \end{cases}$

A_2) $(A,\cdot)$ **monoid** $\Leftrightarrow \begin{cases} M_1) \text{ Înmulțirea este asociativă;} \\ M_2) \text{ Înmulțirea are element neutru.} \end{cases}$

A_3) înmulțirea este distributivă față de adunare. Grupul de axiome G_1) – G_4), A_2) și A_3) se numesc **axiomele inelului**.

Definiție.* Fie $(A,+,\cdot)$ un inel. O submulțime A' nevidă a inelului A se numește **subinel** al inelului A, dacă legile de compoziție din A induc legi de compoziție pe A' împreună cu care A' formează un inel.

* Facultativ.

Observație. Putem reformula definiția şi astfel:

Dacă $(A,+,\cdot)$ este inel, iar $A' \neq \varnothing$, $A' \subset A$, atunci A' este subinel al lui A dacă:

1) $(A',+)$ este subgrup al grupului $(A, +)$.

2) $(A',\cdot)$ este submonoid al monoidului $(A,\cdot)$.

Condițiile 1), 2) se rescriu echivalent:

1') $(\forall)x, y \in A' \Rightarrow x - y \in A'$;

2') $(\forall)x, y \in A' \Rightarrow xy \in A', 1 \in A'$.

> **Definiție.** Într-un inel $(A,+,\cdot)$ cu element unitate, grupul $(U(A),\cdot)$ al elementelor inversabile din monoidul $(A,\cdot)$ se numeşte **grupul elementelor inversabile** (sau încă **grupul unităților**) din inelul A.

Exemple cunoscute de inele şi subinele

1. Mulțimea numerelor întregi $\mathbb{Z}$ cu adunarea şi înmulțirea obişnuită formează un inel numit inelul numerelor întregi notat $(\mathbb{Z},+,\cdot)$. Acesta este un inel comutativ. Elementul nul este 0, iar elementul unitate este 1.

Mulțimea $n\mathbb{Z}$ a numerelor întregi divizibile prin n este un subinel comutativ al lui $\mathbb{Z}$ (fără element unitate dacă $n \in \mathbb{N}^*, n > 1$).

În cazul inelului $(\mathbb{Z},+,\cdot)$ avem $U(\mathbb{Z}) = \{-1,1\}$.

2. $(\mathbb{Q},+,\cdot)$ este inel comutativ, numit inelul numerelor raționale. Cum $\mathbb{Z} \subset \mathbb{Q}$, $(\mathbb{Z},+,\cdot)$ este un subinel al lui $\mathbb{Q}$. Elementul nul este 0, iar elementul unitate este 1.

Pentru inelul $(\mathbb{Q},+,\cdot)$, $U(\mathbb{Q}) = \mathbb{Q}^*$.

3. $(\mathbb{R},+,\cdot)$ este inel comutativ, numit inelul numerelor reale. Cum $\mathbb{Z},\mathbb{Q} \subset \mathbb{R}$ se deduce că $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$ sunt subinele ale lui $\mathbb{R}$. Elementul nul este 0, iar elementul unitate este 1. Aici $U(\mathbb{R}) = \mathbb{R}^*$.

4. $(\mathbb{C},+,\cdot)$ este inel comutativ, numit inelul numerelor complexe pentru care $(\mathbb{Z},+,\cdot), (\mathbb{Q},+,\cdot), (\mathbb{R},+,\cdot)$ sunt subinele ale sale. Pentru $(\mathbb{C},+,\cdot)$ avem $U(\mathbb{C}) = \mathbb{C}^*$.

Inelele din exemplele 1 – 4 se numesc inele numerice.

5. Inelul format dintr-un singur element (elementul nul) se numeşte inel nul. Orice inel care conține cel puțin două elemente se numeşte inel nenul.

6. Dacă $M \neq \varnothing$ este o mulțime, atunci tripletul $(\mathcal{P}(M),\Delta,\cap)$ este un inel comutativ, unde Δ se numeşte diferența simetrică definită astfel $A\Delta B = (A-B)\cup(B-A), (\forall)A,B \in \mathcal{P}(M)$.

Elementul nul este $\varnothing$, iar elementul unitate este M.

Verificați axiomele inelului comutativ. În acest inel $U(\mathcal{P}(M)) = \{M\}$.

7. (Inele de matrice pătratice). Mulțimea matricelor pătratice de ordin n, $\mathcal{M}_n(\mathbb{C})$ împreună cu operațiile obişnuite de adunare şi înmulțire a matricelor formează inelul matricelor pătratice de

ordin n cu elemente din $\mathbb{C}$. Elementul nul este O_n (matricea nulă). Acest inel este unitar, 1 = I_n (matricea unitate de ordin n). Cum pentru $n \geq 2$ înmulțirea matricelor este necomutativă, inelul $(\mathcal{M}_n(\mathbb{C}), +, \cdot)$ este necomutativ. Aici $U(\mathcal{M}_n(\mathbb{C})) = GL(n,\mathbb{C}) = \{A \in \mathcal{M}_n(\mathbb{C}) | \det(A) \neq 0\}$. Acest inel conține ca subinele pe $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$, $(\mathcal{M}_n(\mathbb{Q}), +, \cdot)$, $(\mathcal{M}_n(\mathbb{Z}), +, \cdot)$.

Să observăm că se poate construi un inel de matrice pătratice $\mathcal{M}_n(A)$ pe un inel comutativ arbitrar A deoarece şi înmulțirea matricelor $X, Y \in \mathcal{M}_n(A)$ dau o nouă matrice cu elemente în A şi distributivitatea înmulțirii în raport cu adunarea este consecință a legii analoge din A.

8. (Inele de funcții reale). Mulțimea $\mathcal{F}(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R}\}$ împreună cu operațiile de

1) adunare,

dacă $f, g \in \mathcal{F}(\mathbb{R})$, atunci $f + g : \mathbb{R} \to \mathbb{R}, (f+g)(x) = f(x) + g(x), x \in \mathbb{R}$

şi

2) înmulțire

dacă , $f, g \in \mathcal{F}(\mathbb{R})$ atunci $f \cdot g : \mathbb{R} \to \mathbb{R}, (fg)(x) = f(x)g(x), x \in \mathbb{R}$, formează un inel numit inelul funcțiilor reale.

Acest inel conține ca subinele:

- **$(\mathcal{M}(\mathbb{R}), +, \cdot)$ - inelul funcțiilor mărginite,**
- **$(\mathcal{C}(\mathbb{R}), +, \cdot)$ - inelul funcțiilor continue,**
- **$(\mathcal{D}(\mathbb{R}), +, \cdot)$ - inelul funcțiilor derivabile.**

Pentru inelul $(\mathcal{F}(\mathbb{R}), +, \circ)$ avem

$U(\mathcal{F}(\mathbb{R})) = \mathcal{B}(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} | \, f \text{ bijecție}\}$.

Această problemă se poate trata într-un cadru mai general considerând $\mathcal{F}(X, A) = \{f : X \to A\}$, unde $X \neq \varnothing$, iar $(A, \oplus, \odot)$ este un inel oarecare. Pe această mulțime de funcții introducem două legi numite adunarea şi înmulțirea funcțiilor şi definite după cum urmează:

$$(f+g)(x) = f(x) \oplus g(x),$$
$$(fg)(x) = f(x) \odot g(x), \; x \in X.$$

Dacă 0, 1 sunt elementul nul şi respectiv unitate din A, atunci

$$O_X : X \to A, O_X(x) = 0 \in A, \quad 1 : X \to A, 1(x) = 1, x \in X.$$

Dacă A este comutativ, atunci şi $\mathcal{F}(X, A)$ are aceeaşi proprietate.

9. (Inelul claselor de resturi modulo n). Pe mulțimea claselor de resturi modulo n, $n \geq 2, \mathbb{Z}_n$, am definit operațiile de adunare şi înmulțire astfel: $\hat{a} + \hat{b} \overset{\text{def}}{=} \widehat{a+b}, \hat{a} \cdot \hat{b} \overset{\text{def}}{=} \widehat{ab}$. Am arătat că $(\mathbb{Z}_n, +)$ este grup abelian.

Evident înmulțirea pe $\mathbb{Z}_n$ este asociativă căci

$$(\hat{a} \cdot \hat{b})\hat{c} = \widehat{ab} \cdot \hat{c} = \widehat{a(bc)} = \hat{a} \cdot \widehat{bc} = \hat{a}(\hat{b} \cdot \hat{c}), (\forall) \hat{a}, \hat{b}, \hat{c} \in \mathbb{Z}_n.$$

(am utilizat că înmulțirea pe $\mathbb{Z}$ este asociativă).

Distributivitatea în raport cu adunarea se verifică imediat deoarece

$$\hat{a}(\hat{b} + \hat{c}) = \hat{a}(\widehat{b+c}) = \widehat{a(b+c)} = \widehat{ab+ac} = \widehat{ab} + \widehat{ac} = \hat{a} \cdot \hat{b} + \hat{a} \cdot \hat{c}, (\forall) \hat{a}, \hat{b}, \hat{c} \in \mathbb{Z}_n.$$

Tripletul $(\mathbb{Z}_n, +, \cdot)$ este un inel comutativ, numit inelul claselor de resturi modulo *n*. Elementul nul este $\hat{0}$, iar elementul unitate este $\hat{1}$. Aici $U(\mathbb{Z}_n) = \{\hat{k} \in \mathbb{Z}_n \mid (k,n) = 1\}$.

Prezentăm mai jos trei exemple simple de inele, indicând pentru fiecare tabelele legilor de adunare şi înmulţire:

$\mathbb{Z}_2$:

$+$	$\hat{0}$	$\hat{1}$
$\hat{0}$	$\hat{0}$	$\hat{1}$
$\hat{1}$	$\hat{1}$	$\hat{0}$

$\cdot$	$\hat{0}$	$\hat{1}$
$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$

; $\mathbb{Z}_3$:

$+$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{0}$	$\hat{1}$

$\cdot$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{2}$	$\hat{0}$	$\hat{2}$	$\hat{1}$

; $\mathbb{Z}_4$:

$+$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{3}$	$\hat{0}$	$\hat{1}$
$\hat{3}$	$\hat{3}$	$\hat{0}$	$\hat{1}$	$\hat{2}$

$\cdot$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{2}$	$\hat{0}$	$\hat{2}$	$\hat{0}$	$\hat{2}$
$\hat{3}$	$\hat{0}$	$\hat{3}$	$\hat{2}$	$\hat{1}$

Inelul $\mathbb{Z}_n$ al claselor de resturi modulo *n* a atras de mult timp atenţia specialiştilor în teoria numerelor şi a servit în algebră ca punct de plecare pentru tot felul de generalizări.

Observaţie. Atragem atenţia că $\hat{0} \in \mathbb{Z}_3$ şi $\hat{0} \in \mathbb{Z}_4$ nu reprezintă aceeaşi mulţime, deoarece: $\hat{0} = \{... -6, -3, 0, 3, 6, ...\} \in \mathbb{Z}_3$ şi respectiv $\hat{0} = \{... -8, -4, 0, 4, 8, ...\} \in \mathbb{Z}_4$. Corect scris este $\hat{0}_3$ şi respectiv $\hat{0}_4$ pentru a indica clasa de resturi modulo 3 şi respectiv modulo 4. Scrierea fără indici $\mathbb{Z}_3 = \{\hat{0}, \hat{1}, \hat{2}\}, \mathbb{Z}_4 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}\}$ poate conduce la o concluzie falsă, gen $\mathbb{Z}_3 \subseteq \mathbb{Z}_4$!

10. (Inelul întregilor lui Gauss). Pe mulţimea $\mathbb{Z}[i], i^2 = -1, \mathbb{Z}[i] = \{a + bi \mid a,b \in \mathbb{Z}\} \subset \mathbb{C}$ se definesc operaţiile obişnuite de adunare şi înmulţire ale numerelor complexe. Tripletul $(\mathbb{Z}[i], +, \cdot)$ este un inel comutativ, numit inelul întregilor lui Gauss. Elementul nul este 0 = 0 + 0*i*, iar elementul unitate 1 = 1 + $0 \cdot i$. Aici $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$. Evident $(\mathbb{Z}, +, \cdot)$ este subinel al lui $\mathbb{Z}[i]$, iar $\mathbb{Z}[i]$ este subinel al lui $\mathbb{C}$. Mai general dacă $d \in \mathbb{Z}$ este un întreg liber de pătrate (nu se divide prin pătratul nici unui număr natural diferit de 1), atunci $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d}, a,b \in \mathbb{Z}\}$ cu adunarea şi înmulţirea este inel comutativ. Dacă $d = -1$ obţinem inelul întregilor lui Gauss.

Reguli generale de calcul într-un inel

Am văzut că tripletul $(A, +, \cdot)$ este inel dacă (*A*, +) este grup abelian, $(A, \cdot)$ este monoid şi are loc distributivitatea celei de-a doua legi $(\cdot)$ în raport cu prima (+). Aceasta înseamnă că regulile de calcul de la grupuri rămân valabile şi pentru (*A*, +).
De asemenea regulile de calcul de la monoizi se păstrează şi pentru $(A, \cdot)$. În plus apar noi reguli de calcul în inel ţinând seamă de legătura dintre cele două legi (distributivitatea). Mai precis are loc:

Teorema. Fie $(A, +, \cdot)$ un inel. Atunci:

1) $(\forall) x \in A \Rightarrow x \cdot 0 = 0 \cdot x = 0$.

2) Într-un inel cu cel puțin două elemente $1 \neq 0$.

3) (**regula semnelor**). Pentru orice $x, y \in A$ avem:

$$(-x)y = x(-y) = -xy,\ (-x)(-y) = xy,\ (-x)^n = \begin{cases} x^n, \text{ dacă } n \text{ este par} \\ -x^n, \text{ dacă } n \text{ este impar}, n \in N^* \end{cases}$$

4) (**distributivitatea înmulțirii față de scădere**). Pentru orice $x, y, z \in A$ avem:

$$x(y - z) = xy - xz,$$
$$(y - z)x = yx - zx.$$

Demonstrație. **1)** Fie $x \in A$. Atunci $x + 0 = 0 + x = x$ şi deci (distributivitate) $x \cdot 0 = x(0 + 0) = x0 + x0$ şi $0x = (0 + 0)x = 0x + 0x$, de unde, adunând în prima relație opusul lui $x0$ şi în a doua opusul lui $0x$ se obține $x0 = 0x = 0$.

2) Prin absurd, dacă 1 **=** 0, atunci avem:

$x = 1x = 0x \overset{1)}{=} 0$ pentru orice $x \in A$, ceea ce dă A = {0}, fals.

3) Avem $xy + (-x)y = [x + (-x)]y = 0 \cdot y = 0$ şi $xy + x(-y) = x[y + (-y)] = x0 = 0$, de unde elementul opus fiind unic, rezultă $(-x)y = x(-y) = -(xy)$.

Din egalitatea $x(-y) = (-x)y$ şi din faptul că $-(-x) = x$, rezultă $(-x)(-y) = [-(-x)]y = xy$.

Relația se demonstrează prin inducție matematică.

4) Avem $$x(y - z) = x[y + (-z)] = xy + x(-z) \overset{3)}{=} xy - xz$$

$$(y - z)x = [y + (-z)]x = yx + (-z)x \overset{3)}{=} yx - zx. \ \blacksquare$$

Observații. **1)** Într-un inel A suma unui element $x \in A$ cu opusul unui element $y \in A$, $x + (-y) = (-y) + x$ se notează cu $x - y$. Deoarece la orice două elemente $x, y \in A$ corespunde un element unic $x - y \in A$, am definit pe A încă o operație algebrică, numită **scădere.**

2) Să remarcăm că dat fiind un inel, calculele permise pe acesta sunt: **adunarea, scăderea** şi **înmulțirea** (luați inelul $(\mathbb{Z}, +, \cdot)$).

Reguli de calcul într-un inel comutativ

Prezentăm aici câteva proprietăți remarcabile pentru un inel comutativ. Evident că proprietățile generale discutate mai sus rămân valabile şi aici.

Teoremă. Fie $(A, +, \cdot)$ un **inel comutativ.** Atunci $(\forall) a\ b \in A, (\forall) n \in \mathbb{N}$ avem: $a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + ... + b^{n-1}\right)$,

$$a^{2n+1} + b^{2n+1} = (a+b)\left(a^{2n} - a^{2n-1}b + a^{2n-2}b^2 - ... + b^{2n}\right).$$

Demonstrație. Utilizând proprietatea de distributivitate a înmulțirii față de scădere, regula semnelor la înmulțire precum şi asociativitatea şi comutativitatea operațiilor de înmulțire şi adunare, avem:

$$(a-b)\left(a^{n-1} + a^{n-2}b + ... + b^{n-1}\right) =$$

$$= a\left(a^{n-1} + a^{n-2}b + ... + b^{n-1}\right) - b\left(a^{n-1} + a^{n-2}b + ... + b^{n-1}\right) =$$

$$= a^n + a^{n-1}b + ... + ab^{n-1} - a^{n-1}b - a^{n-2}b^2 - ... - b^n = a^n - b^n.$$

Analog se procedează pentru a doua relație.■

Observații. 1) Să remarcăm că într-un inel comutativ sunt valabile formulele de calcul prescurtat: $a^2 - b^2 = (a-b)(a+b)$, $a^3 - b^3 = (a-b)\left(a^2 + ab + b^2\right)$, $a^3 + b^3 =$

$= (a+b)\left(a^2 - ab + b^2\right)$ etc.

2) Analog se arată că într-un inel comutativ

$$(a_1 + a_2 + ... + a_n)^2 = a_1^2 + a_2^2 + ... + a_n^2 + 2(a_1a_2 + ... + a_1a_n + ... + a_{n-1}a_n),$$
$$(\forall) a_1, a_2, ... a_n \in A$$

În particular $(a+b)^2 = a^2 + 2ab + b^2$, $(a-b)^2 = a^2 - 2ab + b^2$.

Dacă inelul n-ar fi comutativ atunci $(a+b)^2$ are exprimarea

$$(a+b)^2 = (a+b)(a+b) = a(a+b) + b(a+b) = a^2 + ab + ba + b^2.$$

Aici nu mai avem $ab = ba$.

4) Prin inducție după n se arată că într-un inel comutativ este valabilă formula binomului lui Newton:

$$(a+b)^n = a^n + C_n^1 a^{n-1}b + ... + C_n^k a^{n-k}b^k + ... + b^n, (\forall) a, b \in A, (\forall) n \in \mathbb{N}^*$$

3. INEL INTEGRU

Definiție. Fie $(A, +, \cdot)$ un inel. Un element $x \in A$, $x \neq 0$, (0 este elementul neutru pentru +) se numeşte **divizor la stânga (la dreapta) al lui zero** dacă există $y \in A$, $y \neq 0$ astfel încât $xy = 0$ (respectiv $yx = 0$).

Observație. Dacă inelul este comutativ noțiunile de divizor al lui zero la stânga respectiv la dreapta coincid.

Exemple. 1. În inelul matricelor pătratice de ordinul doi, cu elemente din $\mathbb{R}$, $\mathcal{M}_2(\mathbb{R})$ matricele

$A=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, $A\neq O_2$ **(matricea nulă - elementul nul al inelului $\mathcal{M}_2(\mathbb{R})$)**

$B=\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$, $B\neq O_2$, **sunt divizori ai lui zero deoarece** $AB=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}=O_2$.

În general în inelul $(\mathcal{M}_n(\mathbb{R}),+,\ )$ există divizori ai lui zero.

2. În inelul $(\mathbb{Z}_6,+,\cdot)$, $\hat{2}\neq\hat{0}$, $\hat{3}\neq\hat{0}$ şi totuşi $\hat{2}\cdot\hat{3}=\hat{0}$, ceea ce arată că elementele $\hat{2}$, $\hat{3}$ sunt divizori ai lui zero.

3. Inelele $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ nu au divizori ai lui zero.

> **Definiție.** Inelul $(A,+,\cdot)$ **are divizori ai lui zero** dacă A conține cel puțin un divizor al lui zero.
> Un inel nenul **care nu are divizori ai lui zero, comutativ,** se numeşte **inel integru** (sau **domeniu de integritate).**

Observație. Dacă $(A,+,\cdot)$ este un inel şi dacă $x\in A$ este inversabil (deci $x\in U(A)$) atunci x nu este divizor al lui zero. (Arătați acest lucru prin reducere la absurd).

Exemple. 1. Inelele $(\mathcal{M}_2(\mathbb{R}),+,\cdot)$, $(\mathbb{Z}_6,+,\cdot)$ sunt cu divizori ai lui zero. Mai general inelele $(\mathcal{M}_n(\mathbb{R}),+,\cdot)$, $(\mathbb{Z}_n,+,\cdot)$ (aici n = număr compus (neprim)) sunt cu divizori ai lui zero.

2. Inelul $(\mathcal{F}(\mathbb{R}),+,\cdot)$ este cu divizori ai lui zero. N-avem decât să luăm $f,g:\mathbb{R}\to\mathbb{R}$,

$f(x)=\begin{cases}0, & x\leq 0\\ 1, & x>0\end{cases}$, $g(x)=\begin{cases}1, & x\leq 0\\ 0, & x>0\end{cases}$ **pentru care $f\neq 0, g\neq 0$ şi totuşi $(f\cdot g)(x)=f(x)g(x)=0, (\forall)x\in\mathbb{R}$.**

3. Inelele $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C}+,\cdot)$, $(\mathbb{Z}_p,+,\cdot)$ (cu p – număr prim) sunt inele integre.

Reguli de calcul într-un inel integru

Faptul că inelul $(A,+,\cdot)$ nu are divizori ai lui zero furnizează noi reguli de calcul prezentate în următoarele două teoreme.
Următoarea propoziție are un caracter de generalitate pentru un inel integru şi oferă explicații în legătură cu rezolvarea unor ecuații date printr-un produs egal cu zero.

Teoremă. Fie $(A, +, \cdot)$ un inel. Următoarele afirmații sunt echivalente:

1) A este inel integru.

2) $(\forall) x, y \in A,\ x \neq 0$ şi $y \neq 0 \Rightarrow xy \neq 0$.

3) $(\forall) x, y \in A$ cu $xy = 0 \Rightarrow x = 0$ sau $y = 0$.

Demonstrație. **1)** $\Rightarrow$ **2)**. Dacă **1)** este adevărată atunci să probăm **2)**.
Vom face acest lucru prin reducere la absurd. Presupunem că există $x, y \in A,\ x \neq 0,\ y \neq 0$ cu $xy = 0$. Dar aceasta înseamnă că x şi y sunt divizori ai lui zero, fals (A fiind inel integru).

2) $\Rightarrow$ **3)** De fapt aceste afirmații sunt echivalente pentru că $p \Rightarrow q$ este echivalentă cu non $q \Rightarrow$ non p.

3) $\Rightarrow$ **1)** Prin reducere la absurd. ■

Teoremă. Fie $(A, +, \cdot)$ un inel integru. Pentru orice trei elemente $a, x, y \in A$, cu $a \neq 0$, avem echivalențele:

1) $ax = ay \Leftrightarrow x = y$ **(simplificare la stânga printr-un element nenul)**

2) $xa = ya \Leftrightarrow x = y$ **(simplificare la dreapta printr-un element nenul)**

Demonstrație. **1)** „$\Rightarrow$" Avem (ținând seamă de **3)** de la teorema precedentă): $ax = ay \Leftrightarrow a(x - y) = 0 \Leftrightarrow a = 0$ sau $x - y = 0$. Cum $a \neq 0$ rezultă cu necesitate $x - y = 0$, adică $x = y$.
Această proprietate, într-un inel integru, este cunoscută sub denumirea de simplificare la stânga, printr-un element diferit de elementul nul al inelului.
„$\Leftarrow$" Evidentă.
Analog se procedează pentru **2)**. ■

Probleme rezolvate

1. Să se arate că pe mulțimea numerelor întregi $\mathbb{Z}$, legile: $x \oplus y = x + y + 1,\ x \odot y = xy + x + y$ determină o structură de inel comutativ şi fără, divizori ai lui zero. Determinați elementele inversabile ale inelului.

R. Verificăm axiomele inelului.

1) $(\mathbb{Z}, \oplus)$ grup abelian.

G_1) $\oplus$ *este lege de compoziție* deoarece din $x, y \in \mathbb{Z}$, rezultă $x \oplus y = x + y + 1 \in \mathbb{Z}$ (adunări de numere întregi).

G_2) $\oplus$ *este asociativă*, adică $(x \oplus y) \oplus z = x \oplus (y \oplus z), (\forall) x, y, z \in \mathbb{Z}$. Într-adevăr avem pentru membrul stâng: $(x \oplus y) \oplus z = (x + y + 1) \oplus z = (x + y + 1) + z + 1 = x + y + z + 2$, (1), iar pentru membrul drept: $x \oplus (y \oplus z) = x \oplus (y + z + 1) = x + (y + z + 1) + 1 = x + y + z + 2$, (2).

Din (1) şi (2) rezultă egalitatea celor doi membri, adică legea este asociativă.

G_3) $\oplus$ *este comutativă* deoarece $x \oplus y = y \oplus x, (\forall) x, y \in \mathbb{Z}$, adică $x + y + 1 = y + x + 1, (\forall) x, y \in \mathbb{Z}$ (adunarea pe $\mathbb{Z}$ fiind comutativă).

G_4) *Element neutru* pentru $\oplus$. Să arătăm că există $e \in \mathbb{Z}$ astfel încât $e \oplus x = x, (\forall) x \in \mathbb{Z}$. Avem $e + x + 1 = x, (\forall) x \in \mathbb{R} \Leftrightarrow e = -1 \in \mathbb{Z}$.

G_5) *Elemente simetrizabile*. Pentru $x \in \mathbb{Z}$, arbitrar, să găsim $x' \in \mathbb{Z}$ astfel încât $x \oplus x' = -1 \Leftrightarrow$ $\Leftrightarrow x + x' + 1 = -1 \Leftrightarrow x' = -2 - x \in \mathbb{Z}$.

2) $(\mathbb{Z}, \odot)$ monoid comutativ.

M_1) $\odot$ *este lege de compoziţie* pe $\mathbb{Z}$ deoarece din $x, y \in \mathbb{Z}$ rezultă $x \odot y = xy + x + y \in \mathbb{Z}$ (înmulţire şi adunări de numere întregi).

M_2) $\odot$ *este asociativă*, adică $(x \odot y) \odot z = x \odot (y \odot z), (\forall) x, y, z \in \mathbb{Z}$. Calculăm pe rând cei doi membri ai egalităţii. Pentru membrul stâng avem:

$(x \odot y) \odot z = (xy + x + y) \odot z = (xy + x + y)z + xy + x + y + z = xyz + xz + yz + xy + x + y + z$, (1).

Pentru membrul drept obţinem:

$x \odot (y \odot z) = x \odot (yz + y + z) = x(yz + y + z) + x + (yz + y + z) = xyz + xy + xz + yz + x + y + z$, (2).

Din (1) şi (2) rezultă egalitatea celor doi membri şi deci legea $\odot$ este asociativă.

M_3) $\odot$ *este comutativă* deoarece $x \odot y = y \odot x, (\forall) x, y \in \mathbb{Z}$ sau $xy + x + y = yx + y + x, (\forall) x, y \in \mathbb{Z}$ (înmulţirea şi adunarea pe $\mathbb{Z}$ sunt comutative).

M_4) *Element neutru* pentru $\odot$. Să arătăm că există $u \in \mathbb{Z}$ astfel încât $x \odot u = x, (\forall) x \in \mathbb{Z} \Leftrightarrow xu + x + u = x \Leftrightarrow$ $\Leftrightarrow u(x+1) = 0, (\forall) x \in \mathbb{Z} \Leftrightarrow u = 0 \in \mathbb{Z}$.

3) Legea $\odot$ este distributivă în raport cu legea $\oplus$.

Într-adevăr $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z), (\forall) x, y, z \in \mathbb{Z}$.

Pentru aceasta calculăm, pe rând, cei doi membri.

Pentru membrul stâng avem: $x \odot (y \oplus z) = x \odot (y + z + 1) = x(y + z + 1) + x + (y + z + 1) =$ $= xy + xz + 2x + y + z + 1$, (1).

Membrul drept devine $(x \odot y) \oplus (x \odot z) = (xy + x + y) \oplus (xz + x + z) = (xy + x + y) + (xz + x + z) + 1 =$ $= xy + xz + 2x + y + z + 1$, (2).

Din (1) şi (2) rezultă egalitatea propusă spre demonstrat.

În fine, să probăm că inelul este fără divizori ai lui zero, adică să arătăm că dacă $x, y \neq -1$ (-1 este elementul nul al inelului), atunci $x \odot y \neq -1$. Într-adevăr $x \odot y \neq -1 \Leftrightarrow xy + x + y \neq -1 \Leftrightarrow (x+1)(y+1) \neq 0$, ceea ce-i adevărat deoarece $x \neq -1,\ y \neq -1$.

Din cele de mai sus rezultă $(\mathbb{Z}, \oplus, \odot)$) este inel comutativ şi fără divizori ai lui zero.

Să determinăm elementele inversabile ale inelului. Fie $x \in \mathbb{Z}$. Să găsim $x' \in \mathbb{Z}$ pentru care $x \odot x' = 0 \Leftrightarrow$ $\Leftrightarrow xx' + x + x' = 0 \Leftrightarrow x'(1 + x) = -x$.

Dacă $x \neq -1$, atunci $x' = -\frac{x}{1+x} = -\frac{x+1-1}{x+1} = -1 + \frac{1}{x+1} \in \mathbb{Z} \Leftrightarrow x+1$ divide pe 1, adică dacă $x+1 \in \{\pm 1\}$. De aici $x + 1 = 1$ dă $x = 0$, iar pentru $x + 1 = -1$ avem $x = -2$. Deci doar $x = 0$ şi $x = -2$ sunt elemente inversabile când $x' = 0$ şi respectiv $x' = -2$. Deci $U(\mathbb{Z}) = \{-2;0\}$.

2*. a) Determinaţi subinelele inelului $\mathbb{Z}$ al numerelor întregi.

b) Arătaţi că mulţimea $\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{a}{2^n} \middle| a \in \mathbb{Z}, n \in \mathbb{N}\right\} \subset \mathbb{Q}$ formează un subinel al inelului $\mathbb{Q}$ numerelor raţionale.

R. a) Orice subinel al lui $\mathbb{Z}$ trebuie să fie un subgrup al grupului aditiv $(\mathbb{Z},+)$. Am văzut la exemple remarcabile de subgrupuri (1) că forma acestor subgrupuri este $n\mathbb{Z}, n \in \mathbb{N}$. Produsul a doi multipli ai lui n este încă multiplu de n. Aşadar mulţimile $n\mathbb{Z}$ reprezintă subinelele lui $(\mathbb{Z}, +, \cdot)$. Deoarece subinelele trebuie să fie unitare se impune $1 \in n\mathbb{Z}$, ceea ce conduce la $n = 1$, când găsim $1 \cdot \mathbb{Z} = \mathbb{Z}$. Deci $\mathbb{Z}$ este subinel al lui $\mathbb{Z}$ (subinelul $\mathbb{Z}$ al lui $\mathbb{Z}$ se numeşte subinel impropriu).

b) Probăm cele două proprietăţi ale subinelului:

1) $(\forall) x, y \in \mathbb{Z}\left[\frac{1}{2}\right] \Rightarrow x - y \in \mathbb{Z}\left[\frac{1}{2}\right] \left(\left(\mathbb{Z}\left[\frac{1}{2}\right], +\right) \text{ este subgrup al lui } (\mathbb{Q}, +)\right)$.

2) $(\forall) x, y \in \mathbb{Z}\left[\frac{1}{2}\right] \Rightarrow xy \in \mathbb{Z}\left[\frac{1}{2}\right]$.

Verificăm 1). Fie $x, y \in \mathbb{Z}\left[\frac{1}{2}\right]$, adică $x = \frac{a}{2^n}, \ y = \frac{b}{2^m}, \ a,b \in \mathbb{Z}, \ n,m \in \mathbb{N}$.

Fie $n \geq m$. Avem $x - y = \frac{a}{2^n} - \frac{b}{2^m} = \frac{a - b \cdot 2^{n-m}}{2^n} \in \mathbb{Z}\left[\frac{1}{2}\right]$.

Analog dacă $n < m$, avem $x - y = \frac{a}{2^n} - \frac{b}{2^m} = \frac{a \cdot 2^{m-n} - b}{2^m} \in \mathbb{Z}\left[\frac{1}{2}\right]$.

Verificăm 2). Pentru $x = \frac{a}{2^n}, \ y = \frac{b}{2^m}, \ x, y \in \mathbb{Z}\left[\frac{1}{2}\right]$ avem $xy = \frac{ab}{2^{n+m}} \in \mathbb{Z}\left[\frac{1}{2}\right]$.

Observaţie. Mulţimea $\mathbb{Z}\left[\frac{1}{2}\right]$ este „cel mai mic“ subinel al lui $\mathbb{Q}$ care conţine pe $\mathbb{Z}$ şi $\frac{1}{2}$. Este clar că $1 = \left(\frac{1}{2}\right)^0 \in \mathbb{Z}\left[\frac{1}{2}\right]$.

Dacă p este un număr prim, atunci $\mathbb{Z}\left[\frac{1}{p}\right] = \left\{\frac{a}{p^n} \middle| a \in \mathbb{Z}, \ n \in \mathbb{N}\right\} \subset \mathbb{Q}$ reprezintă (împreună cu + şi $\cdot$ de pe $\mathbb{Q}$) un subinel al lui $\mathbb{Q}$.

3. Să se arate că $\mathbb{Z}\left[\sqrt[3]{2}\right] = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \middle| a,b,c \in \mathbb{Z}\right\}$ împreună cu adunarea şi înmulţirea obişnuită este un inel (subinel al lui $(\mathbb{R}, +, \cdot)$).

R. Arătăm mai întâi că $a + b\sqrt[3]{2} + c\sqrt[3]{4} = 0, \ a, \ b, \ c \in \mathbb{Z} \Leftrightarrow a = b = c = 0$.

„$\Leftarrow$“ este imediată.

„$\Rightarrow$" Presupunem prin absurd că dacă $a+b\sqrt[3]{2}+c\sqrt[3]{4}=0$, atunci nu toate numerele întregi *a*, *b*, *c* sunt nule. Mai mult presupunem că două câte două sunt prime între ele (altfel se împarte relația prin cel mai mare divizor comun al numerelor *a*, *b*, *c*). Înmulțim egalitatea dată prin $\sqrt[3]{2}$ şi $\sqrt[3]{4}$ când avem alte două relații $a\sqrt[3]{2}+b\sqrt[3]{4}+2c=0,\ a\sqrt[3]{4}+2b+2\sqrt[3]{2}c=0.$

Avem sistemul: $\begin{cases} a+b\sqrt[3]{2}+c\sqrt[3]{4}=0 \\ 2c+a\sqrt[3]{2}+b\sqrt[3]{4}=0 \\ 2b+2\sqrt[3]{2}c+a\sqrt[3]{4}=0 \end{cases}$ sau $\begin{cases} ax+by+cz=0 \\ 2cx+ay+bz=0 \\ 2bx+2cy+az=0 \end{cases}$ cu soluția $x=1,\ y=\sqrt[3]{2},\ z=\sqrt[3]{4}$.

Cum ultimul sistem liniar este omogen şi admite soluția nebanală $x=1,\ y=\sqrt[3]{2},\ z=\sqrt[3]{4}$ rezultă că determinantul acestui sistem trebuie să fie egal cu zero:

$\begin{vmatrix} a & b & c \\ 2c & a & b \\ 2b & 2c & a \end{vmatrix}=0$ sau după unele calcule $a^3+2b^3+4c^3-6abc=0$.

De aici $a^3=2\left(-b^3-2c^3+3abc\right)$, ceea ce arată că $2|a$. Fie deci $a=2a', a'\in\mathbb{Z}$. Înlocuind în relația de mai sus $a=2a'$ avem: $4a'^3+b^3+2c^3-6a'bc=0$. De aici (ca mai sus) rezultă $2|b$ şi mai apoi $2|c$. Am ajuns că $2|a,\ 2|b,\ 2|c$ în contradicție cu presupunerea că *a*, *b*, *c* sunt prime între ele.

Această observație preliminară arată că elementele din $\mathbb{Z}\left[\sqrt[3]{2}\right]$ se scriu unic sub forma $a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2$, $a,b,c\in\mathbb{Z}$.

Verificăm cele două proprietăți ale subinelului.

1) dacă $z_1,z_2\in\mathbb{Z}\left[\sqrt[3]{2}\right]$ atunci $z_1-z_2\in\mathbb{Z}\left[\sqrt[3]{2}\right]$.

Într-adevăr fie $z_i=a_i+b_i\sqrt[3]{2}+c_i\sqrt[3]{4},\ i=1,2$. Atunci:

$$z_1-z_2=(a_1-a_2)+(b_1-b_2)\sqrt[3]{2}+(c_1-c_2)\sqrt[3]{4}\in\mathbb{Z}\left[\sqrt[3]{2}\right].$$

2) dacă $z_1,z_2\in\mathbb{Z}\left[\sqrt[3]{2}\right]$, atunci $z_1z_2\in\mathbb{Z}\left[\sqrt[3]{2}\right]$. Avem:

$z_1z_2=\left(a_1+b_1\sqrt[3]{2}+c_1\sqrt[3]{4}\right)\left(a_2+b_2\sqrt[3]{2}+c_2\sqrt[3]{4}\right)=a_1a_2+2b_1c_2+2c_1b_2+\left(a_1b_2+b_1a_2+2c_1c_2\right)\sqrt[3]{2}+$
$+\left(a_1c_2+b_1b_2+c_1a_2\right)\sqrt[3]{4}\in\mathbb{Z}\left[\sqrt[3]{2}\right]$.

De asemenea $1=1+0\cdot\sqrt[3]{2}+0\cdot\sqrt[3]{4}\in\mathbb{Z}\left[\sqrt[3]{2}\right]$.

Cu acestea $\left(\mathbb{Z}\left[\sqrt[3]{2}\right],+,\cdot\right)$ este un subinel al lui $(\mathbb{R},+,\cdot)$.

4. Pe $\mathbb{R}$ se consideră legea de compoziție $x*y=ax+by+c$, cu $a,b,c\in\mathbb{R}$.

1) Determinați *a*, *b* şi *c* astfel ca $(\mathbb{R},*)$ să fie grup abelian.

2) Considerând înmulțirea uzuală pe $\mathbb{R}$ ca a doua operație determinați parametrul *c* astfel încât $(\mathbb{R},*,\cdot)$ să fie inel.

R. 1) Trebuie să verificăm axiomele grupului.

G$_1$) *Asociativitatea legii* $*$ înseamnă $(x*y)*z = x*(y*z), (\forall) x, y, z \in \mathbb{R} \Leftrightarrow a^2x + aby + bz + ac + c =$
$= ax + aby + b^2z + bc + c, (\forall) x, y, z \in \mathbb{R}$.

De aici rezultă sistemul: $\begin{cases} a^2 = a \\ b = b^2 \\ ac = bc. \end{cases}$

G$_2$) *Legea* $*$ *este comutativă* dacă $x*y = y*x, (\forall) x, y \in \mathbb{R} \Leftrightarrow ax + by + c = ay + bx + c, (\forall) x, y \in \mathbb{R}$. De aici $a = b$.

G$_3$) *Elementul neutru pentru* $*$ este $e \in \mathbb{R}$ astfel încât $x*e = x, (\forall) x \in \mathbb{R} \Leftrightarrow ax + ae + c = x, (\forall) x \in \mathbb{R}$. De aici $a = 1, e = -c$ (c fixat arbitrar din $\mathbb{R}$).

G$_4$) *Elemente simetrizabile*. Pentru $x \in \mathbb{R}$, există $x' \in \mathbb{R}$ astfel încât $x*x' = -c \Leftrightarrow ax + bx' + c = -c$. Cum $a = b = 1$ rezultă $x' = -2c - x$. Deci pentru $a = b = 1, c \in \mathbb{R}$ cuplul $(\mathbb{R}, *)$ este grup abelian.

2) Înmulțirea uzuală este asociativă, având pe 1 ca element neutru. Trebuie să impunem condiția ca înmulțirea obişnuită să fie distributivă în raport cu legea $*$. Mai precis trebuie să avem egalitățile:
$x(y*z) = (xy)*(yz), (x*y)z = (xz)*(yz), (\forall) x, y, z \in \mathbb{R}$ sau $x(y + z + c) = xy + xz + c$, $(x + y + c)z =$
$= xz + yz + c, (\forall) x, y, z \in \mathbb{R}$. De aici se deduce $c = 0$.

5. Fie $\mathcal{A} = \left\{ M_{a,x} = \begin{pmatrix} a & x \\ 0 & a \end{pmatrix} \middle| a \in \mathbb{Q}, x \in \mathbb{R} \right\}$. Arătați că $\mathcal{A}$ este un inel comutativ în raport cu adunarea şi înmulțirea matricelor din $\mathcal{M}_2(\mathbb{R})$.

R. Trebuie să verificăm axiomele inelului comutativ.

1) $(\mathcal{A}, +)$ este grup abelian deoarece au loc axiomele:

G$_1$) + *este lege de compoziție* pe $\mathcal{A}$.

Fie $M_{a,x}, M_{b,y} \in \mathcal{A}$. Atunci $M_{a,x} + M_{b,y} = \begin{pmatrix} a & x \\ 0 & a \end{pmatrix} + \begin{pmatrix} b & y \\ 0 & b \end{pmatrix} = \begin{pmatrix} a+b & x+y \\ 0 & a+b \end{pmatrix} = M_{a+b, x+y} \in \mathcal{A}$.

G$_2$) Întotdeauna *adunarea matricelor* pe $\mathcal{M}_2(\mathbb{R})$ *este asociativă*. Deci rămâne la fel şi pe submulțimea $\mathcal{A} \subset \mathcal{M}_2(\mathbb{R})$.

G$_3$) *Adunarea matricelor* pe $\mathcal{M}_2(\mathbb{R})$ *este comutativă*. Proprietatea se conservă şi pe $\mathcal{A}$.

G$_4$) *Elementul neutru* este $M_{e_1, e_2} \in \mathcal{A}$ astfel încât $M_{a,x} + M_{e_1,e_2} = M_{a,x}, (\forall) M_{a,x} \in \mathcal{A}$.

De aici $M_{a+e_1, x+e_2} = M_{a,x} \Leftrightarrow a + e_1 = a$ şi $x + e_2 = x \Leftrightarrow e_1 = 0, e_2 = 0$. Prin urmare $M_{0,0} = O_2$ (matricea nulă) este elementul neutru.

Aici am folosit că $M_{a,x} = M_{b,y} \Leftrightarrow a = b$ şi $x = y$ (ceea ce-i imediat din egalitatea matricelor).

G$_5$) *Elemente simetrizabile*. Pentru $M_{a,x} \in \mathcal{A}$, există $M_{a',x'} \in \mathcal{A}$ astfel încât $M_{a,x} + M_{a',x'} = M_{0,0} \Leftrightarrow$
$\Leftrightarrow M_{a+a', x+x'} = M_{0,0} \Leftrightarrow a + a' = 0$ şi $x + x' = 0 \Leftrightarrow a' = -a, x' = -x$.

Deci simetricul lui $M_{a,x}$ este $M_{-a,-x} \in \mathcal{A}$ adică matricea $M_{-a,-x} = \begin{pmatrix} -a & -x \\ 0 & -a \end{pmatrix} = -\begin{pmatrix} a & x \\ 0 & a \end{pmatrix} = -M_{a,x}$ rezultat de aşteptat, pentru că operația este cea de adunare obişnuită a matricelor. Prin urmare simetricul lui $M_{a,x} \in \mathcal{A}$ este chiar opusa matricei $M_{a,x}$.

2) $(\mathcal{A}, \cdot)$ este monoid comutativ, adică se verifică axiomele:

M$_1$) *înmulţirea matricelor este lege de compoziţie* pe $\mathcal{A}$ pentru că oricare ar fi $M_{a,x}, M_{b,y} \in \mathcal{A}$ avem:

$M_{a,x} \cdot M_{b,y} = \begin{pmatrix} a & x \\ 0 & a \end{pmatrix}\begin{pmatrix} b & y \\ 0 & b \end{pmatrix} = \begin{pmatrix} ab & ay+bx \\ 0 & ab \end{pmatrix} = M_{ab,\ ay+bx} \in \mathcal{A}$ (evident din $a,b \in \mathbb{Q} \Rightarrow ab \in \mathbb{Q}$ şi $ay+bx \in \mathbb{R}$ dacă $x, y \in \mathbb{R}$).

M$_2$) *Înmulţirea matricelor* pe $\mathcal{M}_2(\mathbb{R})$ *este întotdeauna asociativă*. Deci rămâne la fel şi pe submulţimea $\mathcal{A}$ a lui $\mathcal{M}_2(\mathbb{R})$.

M$_3$) *Înmulţirea* pe $\mathcal{A}$ *este comutativă* deoarece avem $M_{a,x} \cdot M_{b,y} = M_{ab,ay+bx} = M_{ba,bx+ay} =$, $= M_{b,y} \cdot M_{a,x}, (\forall) M_{a,x}, M_{b,y} \in \mathcal{A}$.

M$_4$) *Elementul neutru*. Să arătăm că există $M_{u_1,u_2} \in \mathcal{A}$ astfel încât $M_{a,x} \cdot M_{u_1,u_2} = M_{a,x}, (\forall) M_{a,x} \in \mathcal{A} \Leftrightarrow$ $\Leftrightarrow M_{au_1,au_2+xu_1} = M_{a,x}, (\forall) M_{a,x} \in \mathcal{A} \Leftrightarrow au_1 = a$ şi $au_2 + xu_1 = x, (\forall) a \in \mathbb{Q}, (\forall) x \in \mathbb{R}$. De aici $u_1 = 1, u_2 = 0$. Deci $M_{1,0} \in \mathcal{A}$ este elementul neutru, care coincide cu $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ matricea unitate.

3) Înmulţirea matricelor este distributivă în raport cu adunarea pe $\mathcal{M}_2(\mathbb{R})$, deci rămâne la fel şi pe $\mathcal{A} \subset \mathcal{M}_2(\mathbb{R})$.

Observăm că inelul este cu divizori ai lui zero. N-avem decât să luăm $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}$, $A, B \neq O_2$ pentru care $AB = O_2$.

6. 1) Să se arate că matricea $A = \begin{pmatrix} 5 & 4 \\ -4 & -3 \end{pmatrix}$ satisface relaţia $A^2 - 2A + I_2 = 0$.

2) Fie $\mathcal{M}_A = \{B \in \mathcal{M}_2(\mathbb{Z}) | B = aA + bI_2, a,b \in \mathbb{Z}\}$.

Să se arate că $(\mathcal{M}_A, +, \cdot)$ este un inel în raport cu operaţiile obişnuite de adunare şi înmulţire a matricelor.

R. 1) Relaţia se verifică, prin calculul direct (este ecuaţia caracteristică pentru matricea pătratică de ordinul doi).

2) Se verifică axiomele inelului.

1) $(\mathcal{M}_A, +)$ este grup abelian adică au loc axiomele:

G$_1$) *Adunarea este lege de compoziţie* pe $\mathcal{M}_A$.

Fie $B_1 = a_1A + b_1I_2$ şi $B_2 = a_2A + b_2I_2, B_1, B_2 \in \mathcal{M}_A$. Atunci $B_1 + B_2 = (a_1 + a_2)A + (b_1 + b_2)I_2 \in \mathcal{M}_A$.

G$_2$) *Adunarea matricelor este întotdeauna asociativă* pe $\mathcal{M}_2(\mathbb{Z})$. Deci rămâne la fel pe $\mathcal{M}_A$.

G$_3$) *Adunarea matricelor* pe $\mathcal{M}_2(\mathbb{Z})$ *este comutativă*. Va rămâne la fel şi pe submulţimea $\mathcal{M}_A$ a lui $\mathcal{M}_2(\mathbb{Z})$.

G$_4$) *Elementul neutru* este matricea $U \in \mathcal{M}_A$ pentru care $B + U = B, (\forall) B$. De aici $U = O_2 = 0A + 0I_2 \in \mathcal{M}_A$.

G$_4$) *Elemente simetrizabile*. Pentru $B \in \mathcal{M}_A$, există $B' \in \mathcal{M}_A$ astfel încât $B + B' = O_2$. De aici $B' = -B = (-a)A + (-b)I_2 \in \mathcal{M}_A$.

2) $(\mathcal{M}_A, \cdot)$ este monoid.

M$_1$) *Înmulțirea matricelor* pe $\mathcal{M}_A$ *este lege de compoziție* deoarece din $B_i = a_i A + b_i I_2,\ i = 1,2,\ B_i \in \mathcal{M}_A$ rezultă $B_1 B_2 = (a_1 A + b_1 I_2)(a_2 A + b_2 I_2) = a_1 a_2 A^2 + (a_1 b_2 + a_2 b_1) A + b_1 b_2 I_2 = (a_1 b_2 + a_2 b_1 + 2a_1 a_2) A +$ $+ (b_1 b_2 - a_1 a_2) I_2 \in \mathcal{M}_A$ (în ultima egalitate am utilizat punctul 1), $A^2 = 2A - I_2$).

M$_2$) Înmulțirea matricelor întotdeauna este *asociativă*. Deci rămâne la fel şi pe $\mathcal{M}_A$.

M$_3$) *Elementul neutru* este $I_2 = 0 \cdot A + 1 \cdot I_2$.

D) Înmulțirea matricelor este distributivă în raport cu adunarea.

Observație. Se poate considera $B = aA + bI_2$ ca fiind $B = B(a,b)$. Avem $B(a,b) = B(a',b') \Leftrightarrow (a = a'$ şi $b = b')$ cum uşor se verifică.

Apoi $B(a,b) + B(a',b') = B(a + a', b + b')$. Analog $B(a,b)B(a',b') = B(ab' + a'b + 2aa', bb' - aa')$.

7. Fie $\mathcal{A} = \{f : [0,1] \to \mathbb{R} \mid f$ continuă$\}$.

a) Să se arate că $\mathcal{A}$ împreună cu adunarea şi înmulțirea funcțiilor formează un inel comutativ.

b) Pentru $f \in \mathcal{A}, f \neq 0$, există $g \in \mathcal{A}, g \neq 0$ astfel încât $f \cdot g = 0$ dacă şi numai dacă $\{x \mid f(x) = 0\}$ conține un interval.

R. a) Operațiile de adunare şi înmulțire ale funcțiilor din $\mathcal{A}$ sunt definite astfel: pentru orice $f, g \in \mathcal{A}$,

$$f + g : [0,1] \to \mathbb{R}, (f + g)(x) = f(x) + g(x), (\forall) x \in [0,1],$$

$$f \cdot g : [0,1] \to \mathbb{R}, (f \cdot g)(x) = f(x) \cdot g(x), (\forall) x \in [0,1].$$

Verificăm axiomele inelului.

1) $(\mathcal{A}, +)$ este grup abelian, adică au loc axiomele:

G$_1$) *Adunarea este lege de compoziție*, deoarece din $f, g \in \mathcal{A}$, rezultă $f + g \in \mathcal{A}$ (sumă de funcții continue este o funcție continuă).

G$_2$) *Adunarea funcțiilor este întotdeauna asociativă*, deci se păstrează proprietatea şi pe $\mathcal{A} \subset \mathcal{F}(A,B) = \{f : A \to B \mid A, B \subseteq \mathbb{R}\}$.

G$_3$) *Adunarea funcțiilor este întotdeauna comutativă*. Proprietatea se conservă şi pe $\mathcal{A}$.

G$_4$) *Elementul neutru* pentru adunare este funcția zero, $0 : [0,1] \to \mathbb{R}, 0(x) = 0, (\forall) x \in [0,1]$ pentru care $f + 0 = f, (\forall) f \in \mathcal{A}$.

G$_5$) *Elemente simetrizabile*. Pentru $f \in \mathcal{A}$, arbitrar, există $-f \in \mathcal{A}$ ($-f$ opusa funcției *f*), astfel încât $f + (-f) = 0$.

2) $(\mathcal{A}, \cdot)$ este monoid comutativ, adică se verifică axiomele:

M$_1$) *Înmulțirea pe* $\mathcal{A}$ *este lege de compoziție* deoarece din $f, g \in \mathcal{A} \Rightarrow fg \in \mathcal{A}$ (produs de funcții continue este o funcție continuă).

M$_2$) *Întotdeauna înmulțirea funcțiilor este asociativă* pe $\mathcal{F}(A,B)$, deci rămâne cu aceeaşi proprietate şi pe submulțimea $\mathcal{A}$.

M$_3$) *Înmulțirea funcțiilor pe* $\mathcal{F}(A,B)$ *este comutativă* întotdeauna, deci se conservă proprietatea şi pe $\mathcal{A}$.

M$_4$) *Elementul neutru* pentru înmulțire este funcția constantă 1, $1 : [0,1] \to \mathbb{R}, 1(x) = 1, (\forall) x \in [0,1]$, care se ştie este o funcție continuă, deci $1 \in \mathcal{A}$. Avem evident $f \cdot 1 = f, (\forall) f \in \mathcal{A}$.

3) În fine se ştie că înmulțirea funcțiilor este distributivă în raport cu adunarea funcțiilor pe $\mathcal{F}(A,B)$. Deci proprietatea se păstrează şi pe $\mathcal{A}$.

b) „$\Rightarrow$“ Dacă $g:[0,1]\to\mathbb{R},\ g\neq 0$ atunci există $x_0\in[0,1]$ astfel încât $g(x_0)\neq 0$. Să presupunem că $g(x_0)>0$. Cum g este continuă în x_0, se deduce că există $V\in\mathcal{V}_{x_0}$ astfel încât $g(x)>0, (\forall)x\in V$ (dacă $x_0=0$, se ia $V=[0,\varepsilon)$, iar pentru $x_0=1$ se ia $V=(1-\varepsilon,1], \varepsilon>0$). Dar $f(x)g(x)=0,\ x\in V$, ceea ce conduce la $f(x)=0,\ x\in V$.

„$\Leftarrow$“ Să presupunem că $f(x)=0$ pentru $x\in[x_1,x_2],\ x_1,x_2\in[0,1],\ x_1<x_2$

Considerăm $g(x)=\begin{cases}0, & x\in[0,1]-[x_1,x_2]\\ (x-x_1)(x-x_2), & x\in[x_1,x_2].\end{cases}$

Se verifică uşor că g este continuă pe [0, 1], $g\neq 0$ şi este clar că $f(x)g(x)=0,\ x\in[0,1]$.

8. Pe mulțimea $A=\mathbb{R}\times\mathbb{R}$ definim legile de compoziție:

$$(a,b)*(c,d)=(a+c,b+d),\ (a,b)\circ(c,d)=(ac,ad+bc).$$

a) Arătați că aceste legi conferă mulțimii A o structură de inel comutativ cu divizori ai lui zero.
b) Precizați forma divizorilor lui zero.
c*) Fie A_1 mulțimea elementelor din A de forma $(a, 0)$.

Să se arate că A_1 este subinel al lui A în raport cu operațiile induse. (Cuplurile (a, b), (c, d) sunt egale dacă $a = c$ şi $b = d$).

R. a) Verificăm axiomele inelului comutativ, cu divizori ai lui zero.

1) $(A,+)$ este grup abelian, adică se verifică axiomele:

G1) *Legea $*$ este asociativă*, deoarece $[(a,b)*(c,d)]*(e,f)=(a,b)*[(c,d)*(e,f)]$, oricare ar fi $(a, b), (c, d), (e, f)\in A$. Într-adevăr egalitatea de mai sus se rescrie:

$(a+c,b+d)*(e,f)=(a,b)*(c+e,d+f)$ sau $((a+c)+e,(b+d)+f)=(a+(c+e),b+(d+f))$

Sau $\begin{cases}(a+c)+e=a+(c+e)\\ (b+d)+f=b+(d+f)\end{cases}$, ceea ce-i adevărat pentru că adunarea pe $\mathbb{R}$ este asociativă.

G2) *Legea $*$ este comutativă*, fiindcă $(a,b)*(c,d)=(c,d)*(a,b), (\forall)(a,b),(c,d)\in A$, ceea ce se rescrie $(a+c,b+d)=(c+a,d+b)$ sau încă $\begin{cases}a+c=c+a\\ b+d=d+b\end{cases}$, egalități adevărate deoarece adunarea pe $\mathbb{R}$ este comutativă.

G3) *Elementul neutru în raport cu $*$* este $(e_1,e_2)\in A$, pentru care $(a,b)*(e_1,e_2)=(a,b), (\forall)(a,b)\in A$. De aici rezultă $(a+e_1,b+e_2)=(a,b)$ sau $\begin{cases}a+e_1=a\\ b+e_2=b\end{cases}$ adică $e_1=e_2=0$.

Aşadar elementul $(0,0)\in A$ este element neutru pentru $*$.

G4) *Elemente simetrizabile*. Pentru $(a,b)\in A$ să găsim $(a',b')\in A$ astfel încât $(a,b)*(a',b')=(0,0)$. De aici se obține $(a+a',b+b')=(0,0)$ sau $a+a'=0$ şi $b+b'=0$, adică $a'=-a, b'=-b$. Deci simetricul lui (a,b) este $(-a,-b)$ (aici fiind vorba de legea $*$ care înseamnă adunarea pe componente, vom numi $(-a,-b)$ opusul lui (a, b)).

2) $(A,\circ)$ este monoid comutativ, adică au loc axiomele:

M_1) *Legea* $\circ$ *este asociativă*, adică $[(a,b)\circ(c,d)]\circ(e,f)=(a,b)\circ[(c,d)\circ(e,f)]$, $(\forall)(a,b),(c,d)$, $(e,f)\in A$. Pentru a verifica egalitatea calculăm fiecare membru separat. Pentru membrul stâng avem: $[(ac,ad+bc)]\circ(e,f)=((ac)e,(ac)f+(ad+bc)e)=(ace,acf+ade+bce)$ (1).

Membrul drept al egalității devine: $(a,b)\circ[(ce,cf+de)]=(a(ce),a(cf+de)+b(ce))=(ace,acf+ade+bce)$ (2).

Din (1) şi (2) rezultă egalitatea propusă.

M_2) *Legea* $\circ$ *este comutativă*, adică $(a,b)\circ(c,d)=(c,d)\circ(a,b)$, $(\forall)(a,b),(c,d)\in A$.

Într-adevăr avem: $(ac,ad+bc)=(ca,cb+da)$, adevărat dacă ţinem seama că înmulţirea şi adunarea pe $\mathbb{R}$ sunt comutative.

M_3) *Elementul neutru* pentru legea $\circ$ este $(u_1,u_2)\in A$ astfel încât $(a,b)\circ(u_1,u_2)=(a,b)$, $(\forall)(a,b)\in A$ sau $(au_1,au_2+bu_1)=(a,b)$, $(\forall)(a,b)\in A$ sau $au_1=a$ şi $au_2+bu_1=b$, $(\forall)a,b\in\mathbb{R}$. De aici $u_1=1$, $u_2=0$. Prin urmare (1, 0) $\in A$ este elementul unitate al inelului.

3) Legea $\circ$ este distributivă în raport cu legea $*$, adică $(a,b)\circ[(c,d)*(e,f)]=[(a,b)\circ(c,d)]*[(a,b)\circ(e,f)]$, $(\forall)(a,b),(c,d),(e,f)\in A$. Se calculează cei doi membri ai egalităţii de demonstrat. Pentru membrul stâng avem: $(a,b)\circ(c+e,d+f)=(a(c+e),a(d+f)+b(c+e))=(ac+ae,\ ad+af+$ $+bc+be)$, (1).

Membrul drept devine: $[(ac,ad+bc)]*[(ae,af+be)]=(ac+ae,ad+bc+af+be)$, (2).

Din (1) şi (2), via comutativitatea şi asociativitatea adunării şi înmulţirii pe $\mathbb{R}$, se deduce afirmaţia din 3). Elementul unitate al inelului este (1,0).

În fine, *inelul este cu divizori ai lui zero* deoarece din $(0,1)\neq(0,0)$, $(0,2)\neq(0,0)$, $(0,1),(0,2)\in A$ rezultă $(0,1)\circ(0,2)=(0,0)$.

b) Fie $(a, b)\neq(0, 0)$ şi $(c, d)\neq(0, 0)$ astfel încât $(a, b)\circ(c, d) = (0, 0)$ sau $(ac, ad + bc) = (0, 0)$. De aici avem sistemul: $\begin{cases} ac=0 \\ ad+bc=0 \end{cases} \Leftrightarrow \left(\begin{cases} \text{a=0} \\ \text{bc=0} \end{cases} \text{sau} \begin{cases} c=0 \\ ad=0 \end{cases}\right)$.

Din $(a, b)\neq(0, 0)$ şi $a = 0$, $bc = 0$, deducem $b\neq0$. Analog din $(c, d)\neq(0,0)$ şi $c = 0$, $ad = 0$ rezultă cu necesitate $d\neq0$. Deci divizorii lui zero sunt de forma $(0,b)$, $b\neq0$, $b\in\mathbb{R}$.

c) Se verifică cele două proprietăţi ale subinelului:

1) $(\forall)x,y\in A_1\Rightarrow x-y\in A_1$;

2) $(\forall)x,y\in A_1\Rightarrow x\circ y\in A_1$ şi $(1,0)\in A_1$.

Pentru 1) luăm $x=(a,0)$, $y=(b,0)\in A_1$ şi avem $x-y=(a,0)+(-b,0)=(a-b,0)\in A_1$.

Pentru 2) asemănător avem $x\circ y=(a,0)\circ(b,0)=(ab,0)\in A_1$.

Probleme propuse

1. **Stabiliți care din următoarele mulțimi de numere împreună cu operațiile obişnuite de adunare şi înmulțire sunt inele:**

1) $\mathbb{Z}$ **; 2)** $2\mathbb{Z}$ **(numerele întregi pare); 3)** $m\mathbb{Z}$ **(numerele întregi, multiplu de** m**); 4)** $\mathbb{Q}$ **; 5)** $\{a+b\sqrt{3}\,|\,a,b\in\mathbb{Z}\}$

6) $\{a+b\sqrt{3}\,|\,a,b\in 2\mathbb{Z}\}$**; 7)** $\{a+b\sqrt{3}\,|\,a,b\in\mathbb{Q}\}$**; 8)** $\{a+bi\,|\,a,b\in\mathbb{Z}\}$ **(inelul întregilor lui Gauss);**

9) $\{a+bi\,|\,a,b\in 3\mathbb{Z}\}$**; 10)** $\{a+bi\,|\,a,b\in\mathbb{Q}\}$ **; 11)** $\{a+b\sqrt{3}i\,|\,a,b\in\mathbb{Z}\}$**;**

12) $\left\{\dfrac{a+bi\sqrt{3}}{2}\,\middle|\,a,b\in\mathbb{Z},\, a,b \text{ au aceeaşi paritate}\right\}$**; 13)** $\{a+bi\sqrt{3}\,|\,a,b\in\mathbb{Q}\}$ **.**

Determinați pentru fiecare inel elementele inversabile. Precizați perechi de inele dintre care unul este subinel al celuilalt*.

2. **Stabiliți care din următoarele mulțimi de matrice împreună cu operațiile obişnuite de adunare şi înmulțire sunt inele:**

1) $\mathcal{M}_n(\mathbb{Z})$**; 2)** $\mathcal{M}_n(\mathbb{Q})$**; 3)** $\mathcal{M}_n(\mathbb{R})$**; 4)** $\mathcal{M}_n(\mathbb{C})$**; 5)** $\left\{\begin{pmatrix} a & 3b\\ b & a\end{pmatrix}\,\middle|\,a,b\in\mathbb{Z}\right\}$**; 6)** $\left\{\begin{pmatrix} a & 3b\\ b & a\end{pmatrix}\,\middle|\,a,b\in 2\mathbb{Z}\right\}$**;**

7) $\left\{\begin{pmatrix} a & 3b\\ b & a\end{pmatrix}\,\middle|\,a,b\in\mathbb{Q}\right\}$**; 8)** $\left\{\begin{pmatrix} a & -b\\ b & a\end{pmatrix}\,\middle|\,a,b\in\mathbb{Z}\right\}$**; 9)** $\left\{\begin{pmatrix} a & -b\\ b & a\end{pmatrix}\,\middle|\,a,b\in 3\mathbb{Z}\right\}$**; 10)** $\left\{\begin{pmatrix} a & -b\\ b & a\end{pmatrix}\,\middle|\,a,b\in\mathbb{Q}\right\}$**;**

11) $\left\{\begin{pmatrix} a & -3b\\ b & a\end{pmatrix}\,\middle|\,a,b\in\mathbb{Z}\right\}$**; 12)** $\left\{\begin{pmatrix} \frac{a}{2} & -\frac{3b}{2}\\ \frac{b}{2} & \frac{a}{2}\end{pmatrix}\,\middle|\,a,b\in\mathbb{Z} \text{ de aceeaşi paritate}\right\}$**; 13)** $\left\{\begin{pmatrix} a & -3b\\ b & a\end{pmatrix}\,\middle|\,a,b\in\mathbb{Q}\right\}$**;**

14) $\left\{\begin{pmatrix} a & b\\ b & a\end{pmatrix}\,\middle|\,a,b\in\mathbb{Z}\right\}$**; 15)** $\left\{\begin{pmatrix} a & 0\\ 0 & b\end{pmatrix}\,\middle|\,a,b\in\mathbb{Z}\right\}$**; 16)** $\left\{\begin{pmatrix} a & b & c\\ 0 & a & b\\ 0 & 0 & a\end{pmatrix}\,\middle|\,a,b,c\in\mathbb{Z}\right\}$**.**

Care din aceste inele sunt comutative? Precizați elementele inversabile. În inelele cu divizori ai lui zero precizați toți divizorii lui zero. Precizați perechile inele dintre care unul este subinel al celuilalt*.

3. **Arătați că fiecare din următoarele mulțimi de funcții reale definite pe** $[-1,1]$ **împreună cu operațiile obişnuite de adunare şi înmulțire este un inel comutativ:**

1) mulțimea tuturor funcțiilor continue; 2) mulțimea tuturor funcțiilor pare; 3) mulțimea tuturor funcțiilor polinomiale; 4) mulțimea tuturor funcțiilor derivabile; 5) mulțimea tuturor funcțiilor mărginite. Determinați în aceste inele elementele inversabile. În care din aceste inele există divizori ai lui zero ? Precizați perechi de inele dintre care unul este subinel al celuilalt*.

4. **Să se arate că mulțimea** $\mathbb{Z}\times\mathbb{Z}$ **cu următoarele operații este inel comutativ în fiecare din cazurile:**

1) $(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2)$, $(a_1,b_1)\cdot(a_2,b_2)=(a_1a_2,b_1b_2)$**. (Se obține** ***produsul direct de inele al inelului*** $(\mathbb{Z},+,\cdot)$ ***cu el însuşi*****).**

2) $(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2)$, $(a_1,b_1)\cdot(a_2,b_2)=(a_1a_2+b_1b_2,a_1b_2+a_2b_1)$**.**

3) $(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2)$, $(a_1,b_1)\cdot(a_2,b_2)=(a_1a_2+3b_1b_2,a_1b_2+a_2b_1)$**.**

4) $(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2)$, $(a_1,b_1)\cdot(a_2,b_2)=(a_1a_2-3b_1b_2,a_1b_2+a_2b_1)$**.**

Determinați în aceste inele elementele inversabile. În inelele cu divizori ai lui zero găsiți acești divizori ai lui zero. (Două elemente $(a,x),(b,y)\in\mathbb{Z}\times\mathbb{Z}$ sunt egale dacă și numai dacă $a=b$ și $x=y$).

5. Arătați că următoarele mulțimi împreună cu aplicațiile considerate în dreptul lor au structurile indicate:

1) $\mathbb{Z}$; $x\top y=x+y-3,\ x\perp y=xy-3(x+y)+12;\ (\mathbb{Z},\top,\perp)$ este domeniu de integritate. Determinați elementele inversabile și inversele lor.

2) $\mathbb{Z}$; $x\oplus y=x+y+3;\ x\odot y=xy+3(x+y)+6;\ (\mathbb{Z},\otimes,\odot)$ este domeniu de integritate. Determinați elementele inversabile și inversele lor.

3) $\mathbb{Z}$; $x\top y=x+y+2,\ x\perp y=xy+2(x+y)+2;\ (\mathbb{Z},\top,\perp)$ este domeniu de integritate. Determinați elementele inversabile și inversele lor.

4) $2\mathbb{Z}+1;\ x*y=x+y-1,\ x\circ y=\frac{1}{2}(xy-x-y+3),\ (2\mathbb{Z}+1,*,\circ)$ este domeniu de integritate. Determinați elementele inversabile și inversele lor.

5) $\mathbb{Z}[i];\ z_1*z_2=z_1z_2+\mathrm{Im}(z_1)\mathrm{Im}(z_2)$ unde $\mathrm{Im}(a+ib)=b,\ a,b\in\mathbb{R}$, $(\mathbb{Z}[i],+,*)$ este domeniu de integritate. Determinați elementele inversabile.

6) $\mathcal{P}(M),\ M=\{a,b\};\ A\Delta B=(A-B)\cup(B-A),\ A\cdot B=A\cap B,\ (\mathcal{P}(M),\Delta,\cdot)$ este inel comutativ cu divizori ai lui zero.

7) $\mathcal{A}=\left\{\begin{pmatrix}x & y\\ -y & x\end{pmatrix}\middle|\, x,y\in\mathbb{Z}\right\};\ (\mathcal{A},+,\cdot)$ este inel comutativ, în raport cu adunarea și înmulțirea obișnuită a matricelor.

8) $\mathcal{M}_a=\left\{A\in\mathcal{M}_2(\mathbb{R})\,\middle|\, A\begin{pmatrix}a & 1\\ 0 & a\end{pmatrix}=\begin{pmatrix}a & 1\\ 0 & a\end{pmatrix}A,\ a\in\mathbb{R}\right\};\ (\mathcal{M}_a,+,\cdot)$ este un inel în raport cu adunarea și înmulțirea matricelor;

9) $\mathcal{A}=\left\{\begin{pmatrix}a+ib & c+id\\ -c+id & a-ib\end{pmatrix}\middle|\, a,b,c,d\in\mathbb{R},\ i^2=-1\right\};\ (\mathcal{A},+,\cdot)$ este inel în raport cu adunarea și înmulțirea matricelor.

10) $\mathcal{A}=\left\{\begin{pmatrix}x & 0 & x\\ 0 & 0 & 0\\ x & 0 & x\end{pmatrix}\middle|\, x\in\mathbb{R}\right\};\ (\mathcal{A},+,\cdot)$ este domeniu de integritate în raport cu adunarea și înmulțirea matricelor.

11) $\mathcal{A}=\left\{\begin{pmatrix}a & 0 & 0\\ 0 & b & 0\\ 0 & 0 & c\end{pmatrix}\middle|\, a,b,c\in\mathbb{R}\right\};\ (\mathcal{A},+,\cdot)$ este inel comutativ cu divizori ai lui zero.

12) $\mathcal{A}=\left\{A\in\mathcal{M}_3(\mathbb{R})\,\middle|\, A=\begin{pmatrix}a & b & c\\ 0 & a & d\\ 0 & 0 & a\end{pmatrix},\ a,b,c,d\in\mathbb{R}\right\};(\mathcal{A},+,\cdot)$ inel necomutativ. Determinați elementele inversabile din inel.

13) a) $\mathcal{A}=\left\{\begin{pmatrix} a & 0 & b \\ 0 & c & 0 \\ d & 0 & e \end{pmatrix} \middle| a,b,c,d,e\in\mathbb{Z}_2\right\}$; $(\mathcal{A},+,\cdot)$ este inel necomutativ în raport cu operațiile uzuale.

b) $\mathcal{A}=\left\{\begin{pmatrix} a & 0 & b \\ 0 & c & 0 \\ -b & 0 & a \end{pmatrix} \middle| a,b,c\in\mathbb{R}\right\}$; $(\mathcal{A},+,\cdot)$ este inel comutativ cu divizori ai lui zero.

14) $\mathcal{A}=\left\{M=xI_2+yJ \middle| J=\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, x,y\in\mathbb{R}\right\}$; $(\mathcal{A},+,\cdot)$ este un inel în raport cu operațiile uzuale.

15) $\mathcal{A}=\left\{M=xI_2+yA \middle| A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}, a,b,c,d\in\mathbb{R}\right\}$; $(\mathcal{A},+,\cdot)$ este inel comutativ în raport cu operațiile uzuale.

16) $\mathcal{A}=\{f:\{0,1\}\to\mathbb{R}\}$; $(\mathcal{A},+,\cdot)$ este un inel comutativ cu divizori ai lui zero în raport cu adunarea și înmulțirea funcțiilor.

17) $\mathbb{Q}\times\mathbb{R}$; $(a,x)+(b,y)=(a+b,\ x+y)$, $(a,x)\cdot(b,y)=(ab,ay+bx+xy)$; $(\mathbb{Q}\times\mathbb{R},+,\cdot)$ este inel comutativ. Determinați elementele inversabile. (Două elemente $(a,x),(b,y)\in\mathbb{Q}\times\mathbb{R}$ sunt egale dacă și numai dacă $a=b$ și $x=y$).

18) $\mathcal{A}=\left\{x\in\mathbb{R} \middle| x=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}, a,b,c,d\in\mathbb{Q}\right\}$; $(\mathcal{A},+,\cdot)$ este inel comutativ.

6. Fie A un inel și $a,b\in A$ astfel încât $a(ab-ba)=(ab-ba)a$.

Demonstrați pentru orice $n\in\mathbb{N}, n\geq 1$ că are loc egalitatea $a^nb-ba^n=n(ab-ba)a^{n-1}$.

7. Fie A un inel cu proprietatea $x^2=x, \forall x\in A$. Să se arate că A este inel comutativ.

8. Fie $(A,+,\cdot)$ un inel cu şapte elemente. Să se arate că 1+1+1+1+1+1+1= 0.

9. Arătați că în inelul $\mathbb{Z}_n$ au loc egalitățile:

a) $(a+b)^2=a^2+b^2, (a+b)^n=a+b, (\forall)a,b\in\mathbb{Z}_2$;

b) $(a+b)^2=a^2-ab+b^2, (a+b)^3=a^3+b^3=a+b, (\forall)a,b\in\mathbb{Z}_3$;

c) $(a+b)^2=a^2-2ab+b^2, (a+b)^4=a^4-2a^2b^2+b^4, (\forall)a,b\in\mathbb{Z}_4$;

d) $(a+b)^5=a^5+b^5=a+b, (\forall)a,b\in\mathbb{Z}_5$;

e) $(a+b)^p=a^p+b^p=a+b, (\forall)a,b\in\mathbb{Z}_p$, p prim.

10. În inelul $(A,+,\cdot)$ pentru orice $a\in A, x^6=x$. Arătați că: a) $x^2=x,(\forall)x\in A$; b) inelul A este comutativ.

11. Fie A un inel în care $x^2=x, (\forall)x\in A$. (Un astfel de inel se numeşte *inel boolean*) Arătați că $x+x=0,(\forall)x\in A$.

12. **Fie A un inel cu element unitate $1 \neq 0$. Un element $x \in A$ se numeşte *idempotent* dacă $x^2 = x$. Fie M mulţimea elementelor idempotente din A. Arătaţi că:**
a) dacă M este finită, atunci card(M) este un număr par;
b) produsul elementelor din M este egal cu 1 sau cu 0.

13. **Fie inelul $\left(\mathcal{M}_2(\mathbb{Z}_6), +, \cdot\right)$ şi matricele $A = \begin{pmatrix} \hat{3} & \hat{5} \\ \hat{1} & \hat{2} \end{pmatrix}, B = \begin{pmatrix} \hat{3} & \hat{5} \\ \hat{5} & \hat{4} \end{pmatrix}$. Arătaţi că $A, B \in U\left(\mathcal{M}_2(\mathbb{Z}_6)\right)$ şi calculaţi A^{-1}, B^{-1}.**

14*. **Fie $(A, +, \cdot)$ un inel unitar şi $x, y \in A$ două elemente inversabile, astfel încât $x^{-1} = y$ şi $y^{-1} = x$. Arătaţi că:**

a) dacă elementele $a = 1 + x + x^2, b = 1 + x + y, c = 1 + y + y^2$ sunt elemente inversabile, atunci $a^{-1} + b^{-1} + c^{-1} = 1$;

b) dacă $1 + x$ şi $1 + y$ sunt inversabile, atunci $(1 + x)^{-1} + (1 + y)^{-1} = 1$.

15. **Fie A un inel, iar pentru orice $x \in A$ cu $x^2 = 0$, avem $x = 0$. Să se arate că dacă $x_1, x_2, x_3 \in A$ sunt astfel încât $x_1x_2x_3 = 0$, atunci avem: a) $x_2x_3x_1 = 0$; b) $x_3x_1x_2 = 0$; c) $x_1ax_2bx_3 = 0, (\forall)a, b \in A$.**

16*. **Fie $(A, +, \cdot)$ un inel. Dacă $\left(x^2 + x + 1\right)y = y\left(x^2 + x + 1\right), (\forall)x, y \in A$, atunci inelul este comutativ.**

17*. **Fie $(A, +, \cdot)$ un inel unitar astfel încât $x^3 = x^2, (\forall)x \in A$. Arătaţi că $x^2 = x, (\forall)x \in A$ şi A este un inel comutativ.**

18*. **Fie $(A, +, \cdot)$ un inel astfel încât există un element unic $x \in A$, cu proprietatea $x^2 = x + 1$. Să se arate că 1 + 1 + 1 + 1 + 1 = 0.**

19*. **(Caracteristica unui inel). Fie $(A, +, \cdot)$ un inel unitar. Se numeşte *caracteristica inelului A* cel mai mic număr natural $n \in \mathbb{N}^*$ cu proprietatea $n \cdot 1 = 0$. Dacă nu există $n \in \mathbb{N}^*$ cu proprietatea $n \cdot 1 = 0$, atunci inelul are caracteristica zero. a) Dacă n este caracteristica inelului A, atunci el este ordinul elementului 1 în grupul $(A, +)$; b) Inelul $(\mathbb{Z}_n, +, \cdot)$ are caracteristica n; c) Inelele $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[i]$ au caracteristica zero; d) Dacă n este caracteristica lui A, atunci $nx = 0, (\forall)x \in A$; e) Dacă A este domeniu de integritate, atunci caracteristica este zero sau număr prim; f) Într-un inel A de caracteristică n avem: $(x + y)^n = x^n + y^n, (x - y)^n = x^n - y^n, (\forall)x, y \in A$.**

2.2. CORPURI

Am văzut că pentru inelul $(A, +, \cdot)$, mulţimea A are o structură mai săracă cu privire la cea de-a doua operaţie, cea multiplicativă. S-a putut constata ca proprietăţi suplimentare pentru înmulţire (comutativitate, element unitate) dau mai multe proprietăţi pentru inel.
În cele ce urmează vom studia inele (cu cel puţin două elemente) în care cât mai multe elemente nenule ale sale sunt simetrizabile (inversabile) în raport cu operaţia de

înmulțire (elementul neutru la adunare 0 nu poate fi inversabil deoarece $x \cdot 0 = 0 \cdot x \neq 1$, $(\forall) x \in A$).

Deci existenta simetricului poate fi pusă pentru mulțimea $A^* = A - \{0\}$, nu şi pentru elementul nul.

Definiție. Se numeşte **corp** un triplet $(K, +, \cdot)$, în care K este o mulțime cu cel puțin două elemente, iar „+" şi „$\cdot$" două operații pe K (numite „adunare" şi respectiv „înmulțire"), satisfăcând următoarele trei axiome:

K_1) $(K, +)$ este grup abelian, cu elementul neutru 0.

K_2) $(K - \{0\}, \cdot)$ este grup, cu elementul neutru 1.

K_3) Înmulțirea este distributivă față de adunare.

Dacă, în plus, este satisfăcută şi axioma:

K_4) Înmulțirea este comutativă,

atunci $(K, +, \cdot)$ se numeşte **corp comutativ** (sau **câmp**).

Observații. 1) Grupul $(K, +)$ se numeşte **grupul aditiv** al corpului, iar $(K - \{0\}, \cdot)$ se numeşte **grupul multiplicativ al elementelor nenule** ale corpului (sau cu notația cunoscută $U(K) = K - \{0\}$).

2) Dacă corpul K este **comutativ**, atunci $(K - \{0\}, \cdot)$ este **grup comutativ**.

3) Orice corp K conține cel puțin două elemente distincte, un element neutru față de adunare şi un element neutru față de înmulțire, deci pe 0 şi 1.

Reciproc, pe orice mulțime formată din două elemente distincte există o singură structură de corp. Dacă notăm aceste elemente cu 0 şi 1, atunci adunarea şi înmulțirea nu pot fi definite decât în modul următor:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Acest corp cu două elemente joacă un rol important în teoria informației unde fiecare literă se codifică utilizând simbolurile 0 şi 1. Se arată că receptarea unui mesaj este mai bună (corectă) cu cât fiecărei litere i se asociază un vector cu mai multe componente (formate din 0 şi 1), influența factorilor parazitari (de perturbare a mesajului transmis) fiind mult redusă (Shannon).

4) Toate proprietățile puse în evidență la inele sunt valabile şi pentru corpuri.

5) Definiția dată corpului poate fi reformulată şi astfel:

Un inel K se numeşte **corp** dacă orice element nenul al lui K este inversabil, adică dacă $x \in K$, $x \neq 0$, $(\exists) x^{-1} \in K$ astfel încât $xx^{-1} = x^{-1}x = 1$.

Definiție*. O submulțime nevidă K' a unui corp K se numeşte **subcorp al lui *K*** dacă legile de compoziție interne din K induc legi de compoziție interne pe K', împreună cu care K' este corp.

Având în vedere definiția dată pentru corp cu ajutorul celor trei axiome K_1), K_2), K_3), definiția subcorpului poate fi reformulată utilizând caracterizarea pentru subgrupuri astfel:

Teoremă*. Fie $(K, +, \cdot)$ un corp. O submulțime K' a lui K, care conține cel puțin două elemente este subcorp al lui K dacă şi numai dacă:

1) $(\forall) x, y \in K' \Rightarrow x - y \in K'$;

2) $(\forall) x, y \in K'\ x, y \neq 0 \Rightarrow xy^{-1} \in K'$.

Altfel spus K' submulțime a corpului K este subcorp dacă şi numai dacă este subgrup al grupului aditiv al corpului K şi submulțimea elementelor nenule din K' este nevidă şi este subgrup al grupului multiplicativ al elementelor nenule din K.
Dacă K' este subcorp al lui K, atunci K se numeşte supracorp al lui K', sau încă **extensie** (sau **extindere**) a corpului K'.
Să observăm că fiind dat un corp, calculele permise pe acesta sunt: **adunarea**, **scăderea**, **înmulțirea** şi **împărțirea** (prin elemente nenule $\frac{a}{b} = a \cdot b^{-1}$).

Exemple cunoscute de corpuri şi subcorpuri

1. Mulțimea numerelor raționale împreună cu operațiile obişnuite de adunare şi înmulțire, formează, un corp comutativ, numit corpul numerelor raționale şi notat $(\mathbb{Q}, +, \cdot)$.

2. Mulțimea numerelor reale cu aceleaşi operații de adunare şi înmulțire formează un corp comutativ, numit corpul numerelor reale şi notat $(\mathbb{R}, +, \cdot)$.

Cum $\mathbb{Q} \subset \mathbb{R}$, corpul numerelor raționale este un subcorp al lui $\mathbb{R}$ sau încă $\mathbb{R}$ este o extindere a lui $\mathbb{Q}$.

3. Mulțimea numerelor complexe cu adunarea şi înmulțirea formează un corp comutativ, numit corpul numerelor complexe şi notat $(\mathbb{C}, +, \cdot)$.

Din $\mathbb{Q} \subset \mathbb{C}$ şi $\mathbb{R} \subset \mathbb{C}$, deducem că $\mathbb{Q}$ şi $\mathbb{R}$ sunt subcorpuri ale lui $\mathbb{C}$ sau $\mathbb{C}$ este o extindere a lui $\mathbb{Q}$ sau $\mathbb{R}$.

Corpurile de la 1, 2, 3 se numesc corpuri numerice.

Alte exemple remarcabile de corpuri

1) Corpul claselor de resturi modulo *p*. Am văzut la inele că tripletul $(\mathbb{Z}_n, +, \cdot)$ este un inel pentru $n \in \mathbb{N}, n \geq 2$. Se pune problema pentru ce $n \in \mathbb{N}^*$, $\mathbb{Z}_n$ este corp, adică pentru ce $n \in N^*$, $(\forall) x \in \mathbb{Z}_n$, $x \neq \hat{0}$ este inversabil? Răspunsul este dat de următoarea:

> **Teoremă.** Inelul $(\mathbb{Z}_n, +, \cdot)$ al claselor de resturi modulo *n* este corp dacă şi numai dacă *n* este număr prim.

Demonstraţie. Într-adevăr dacă *n* este număr prim, atunci $(\forall) x \in \mathbb{Z}_n$, $x \neq \hat{0}$ este inversabil pentru că $(x, n) = 1$.

Reciproc, s-a văzut (la grupul claselor de resturi modulo *n*) că dacă $x \in \mathbb{Z}_n$, $x \neq \hat{0}$, există $x^{-1} \in \mathbb{Z}_n$ pentru $(x, n) = 1$. ■

De fapt $\mathbb{Z}_n$ este corp dacă şi numai dacă $U(\mathbb{Z}_n) = \mathbb{Z}_n - \{\hat{0}\} = \{\hat{1}, \hat{2}, ..., \widehat{n-1}\}$ dacă şi numai dacă $(n, k) = 1$, $k = \overline{1, n-1}$.

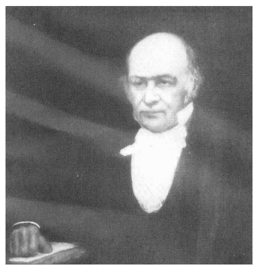
Ultima afirmaţie are loc dacă *n* = *p* este un număr prim.

Evident $(\mathbb{Z}_n, +, \cdot)$ este corp comutativ.

UN PIONIER AL MATEMATICII

W.R. HAMILTON (1805–1865)

Matematician irlandez



CONTRIBUŢII

- ***teoria numerelor complexe***
- ***teoria cuaternionilor***

2) Corpul cuaternionilor. Fie $i \in \mathbb{C}$, unitatea imaginară ($i^2 = -1$). Considerăm *j*, *k* două obiecte matematice între care introducem o înmulţire (ce prelungeşte pe cea obişnuită din $\mathbb{C}$) astfel: $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ik = -ki = j$.

Expresia formală $a + bi + cj + dk$, $a, b, c, d \in \mathbb{R}$ se numeşte **cuaternion**. Fie *H* mulţimea tuturor cuaternionilor. Evident $\mathbb{C} \subset H$, pentru că $(\forall) z \in \mathbb{C}$, $z = a + bi$, $a, b \in \mathbb{R}$ se poate scrie $z = a + bi + 0j + 0k \in H$. Pe mulţimea *H* se definesc două operaţii astfel:

1) **Adunarea cuaternionilor**

Dacă $q_1 = a_1 + b_1 i + c_1 j + d_1 k$, $q_2 = a_2 + b_2 i + c_2 j + d_2 k \in H$, atunci $q_1 + q_2 = a_1 + a_2 + {}$ $+ (b_1 + b_2) i + (c_1 + c_2) j + (d_1 + d_2) k \in H$ reprezintă **suma** cuaternionilor q_1 şi q_2.

2) **Înmulțirea cuaternionilor**

Dacă $q_1, q_2 \in H$ atunci $q_1 \cdot q_2 = (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + a_2b_1 + c_1d_2 - c_2d_1)i + (a_1c_2 - b_1d_2 + a_2c_1 + b_2d_1)j + (a_1d_2 + b_1c_2 - b_2c_1 + a_2d_1)k \in H$ reprezintă **produsul** cuaternionilor q_1 și q_2. (Practic la înmulțirea lui q_1 cu q_2 funcționează distributivitatea înmulțirii față de adunare la care se ține seamă de definițiile date pentru i, j, k – se înmulțeşte fiecare termen al lui q_1 cu fiecare termen al lui q_2, în această ordine).

Dacă $q = a + bi + cj + dk \in H$, atunci $\overline{q} = a - bi - cj - dk \in H$ se numeşte **conjugatul** lui q.

Definim funcția $N : H \to \mathbb{R}_+$, $N(q) = q \cdot \overline{q} = a^2 + b^2 + c^2 + d^2$, care se numeşte funcție **normă**.

Are loc următoarea:

Teoremă. Tripletul $(H, +, \cdot)$ este un corp necomutativ numit **corpul cuaternionilor.**

Demonstrație. Se arată uşor că $(H, +, \cdot)$ este inel $(0 = 0 + 0i + 0j + 0k, 1 = 1 + 0i + 0j + 0k)$.

Să arătăm că $(\forall) q \in H$, $q \neq 0$ este inversabil.

Dacă $q = a + bi + cj + dk \neq 0$, atunci cel puțin unul din numerele *a*, *b*, *c*, *d* este nenul. Prin urmare $N(q) = a^2 + b^2 + c^2 + d^2 > 0$.

Avem egalitățile: $q \cdot \dfrac{\overline{q}}{N(q)} = \dfrac{\overline{q}}{N(q)} \cdot q = 1$, ceea ce arată că q este inversabil şi

$$q^{-1} = \frac{\overline{q}}{N(q)} = \frac{a}{N(q)} - \frac{b}{N(q)}i - \frac{c}{N(q)}j - \frac{d}{N(q)}k \in H . \blacksquare$$

3) Corpuri pătratice. Fie $d \in \mathbb{Z} - \{1\}$ un întreg liber de pătrate (deci d nu se divide prin pătratul nici unui număr întreg diferit de unu). Definim mulțimea $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$, pe care se consideră operațiile obişnuite de adunare şi înmulțire a numerelor complexe.

Are loc următoarea

Teoremă. Tripletul $(\mathbb{Q}(\sqrt{d}), +, \cdot)$ este un corp comutativ, numit **corp pătratic**.

Demonstrație. Se verifică uşor că adunarea şi înmulţirea sunt legi interme pe $\mathbb{Q}[\sqrt{d}]$. Într-adevăr fie $z_1 = a_1 + b_1\sqrt{d}$, $z_2 = a_2 + b_2\sqrt{d}$, $z_1, z_2 \in \mathbb{Q}[\sqrt{d}]$. Atunci:

$$z_1 + z_2 = a_1 + a_2 + (b_1 + b_2)\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$$

şi

$$z_1 z_2 = a_1 a_2 + b_1 b_2 d + (a_1 b_2 + b_1 a_2)\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$$

Se verifică uşor axiomele inelului comutativ $\left(\mathbb{Q}[\sqrt{d}], +, \cdot\right)$.

Elementul nul este $0 = 0 + 0\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, iar elementul unitate este $1 = 1 + 0\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$.

Să verificăm că dacă $z \in \mathbb{Q}[\sqrt{d}]$, $z \neq 0$, atunci $z^{-1} \in \mathbb{Q}[\sqrt{d}]$.

Într-adevăr fie $z = a + b\sqrt{d} \neq 0$, adică a sau b este nenul. Atunci:

$$z^{-1} = \frac{1}{z} = \frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - b^2 d} = \frac{a}{a^2 - b^2 d} - \frac{b}{a^2 - b^2 d}\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$$

Se verifică cerința $a^2 - b^2 d \neq 0$ dacă $a \neq 0$ sau $b \neq 0$.

Numerele de forma $a + b\sqrt{d}$, $a, b \in \mathbb{Q}[\sqrt{d}]$, d întreg liber de pătrate, se numesc **numere pătratice**. Pentru $z = a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, numărul $\bar{z} = a - b\sqrt{d} \in \mathbb{Q}[\sqrt{2}]$ se numeşte **conjugatul pătratic** a lui z.

Corpul $\mathbb{Q}[\sqrt{d}]$ este o extindere a corpului $\mathbb{Q}$ (orice $x \in \mathbb{Q}$ se scrie $x = x + 0\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$) sau mai spunem că $\mathbb{Q}$ este un subcorp al corpului pătratic $\mathbb{Q}[\sqrt{d}]$.

De exemplu în $\mathbb{Q}$ ecuația $x^2 = 2$ nu are soluții, dar în $\mathbb{Q}[\sqrt{2}]$ are soluția $x = \sqrt{2}$. Iată de ce apare natural procesul de extindere al unui corp.

Câteva observații generale asupra regulilor de calcul dintr-un corp.

Produsul ab^{-1}, $b \neq 0$ cu $a, b \in K$, se mai scrie şi sub formă de fracție (sau raport) $\frac{a}{b}$.

Deci, fracția $\frac{a}{b}$, care n-are sens decât pentru $b \neq 0$ este soluția unică a ecuației $bx = a$. Regulile de calcul ale fracțiilor sunt următoarele:

$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc,\ b, d \neq 0$; $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, b, d \neq 0$; $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$, $b \neq 0$,

$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$, $b, d \neq 0$; $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$, $a, b \neq 0$.

Acestea sunt regulile uzuale din gimnaziu pentru operațiile pe $\mathbb{Q}$. Raționamentele care se fac pentru a le proba în cazul corpului K țin de operațiile din K. Aşa de pildă pentru a obține a doua relație dintre cele scrise mai sus se poate proceda astfel: fie

$x = \frac{a}{b}$, $y = \frac{c}{d}$ soluții ale ecuațiilor $bx = a$ şi respectiv $dy = c$. Atunci $dbx = da$, $dby = bc \Rightarrow bd(x+y) = da + bc$ şi deci $t = x + y = \frac{da+bc}{bd}$ este unica soluție a ecuației $bdt = da + bc$.

Am abordat, anul precedent, sistemele de ecuații liniare cu coeficienți în $\mathbb{Q}, \mathbb{R}$ sau $\mathbb{C}$.

De asemenea teoria determinanților am realizat-o pentru matrice din $\mathcal{M}_n(\mathbb{Q}), \mathcal{M}_n(\mathbb{R})$ sau $\mathcal{M}_n(\mathbb{C})$.

Nimic nu ne împiedică acum de a lua în locul acestor numere (raționale, reale sau complexe), elemente dintr-un corp comutativ arbitrar *K*.

În acest caz, rezultatele obținute trebuie enunțate în termenii corpului *K:* componentele soluției unui sistem liniar şi valorile funcției **det** vor aparține corpului *K*. Metoda lui Gauss de rezolvare a sistemelor de ecuații liniare, teoria determinanților, formulele lui Cramer rămân valabile (fără modificări importante) pentru un corp comutativ oarecare *K*, cu precizarea că în corpul *K* scrierea $\frac{a}{b}$ înseamnă ab^{-1}.

Mulțimea matricelor pătratice de ordin *n* cu coeficienți într-un corp arbitrar *K* formează un inel de matrice $\mathcal{M}_n(K)$, iar submulțimea tuturor matricelor $A \in \mathcal{M}_n(K)$ pentru care $\det(A) \neq 0$ (elementul nul al corpului *K)* conduce la noțiunea de **grup liniar complet** $\mathrm{GL}(n, K)$ pe *K*. Făcând să varieze corpul *K* se poate obține natural toată seria de grupuri importante.

Corpurile de tipul $\mathbb{Q}, \mathbb{Q}[\sqrt{2}], \mathbb{R}$ etc. sunt în general numite **corpuri numerice**. Corpul $\mathbb{Z}_p$, *p* – prim este un exemplu de corp nenumeric: ar fi incorect să numim elementele sale numere pentru singura rațiune că uneori se identifică cu elementele mulțimii $\{0, 1, ..., p-1\}$.

4) Corpuri de matrice. În cele ce urmează fie *A* un inel comutativ în care $1 \neq 0$ (uneori în loc de *A* se consideră corpul comutativ *K*). Notăm $\mathcal{M}_n(A), n \in N^*$, mulțimea matricelor pătratice de ordin *n* cu elemente în inelul *A*.

Spunem că două matrice $X, Y \in \mathcal{M}_n(A)$, $X = (a_{ij}), Y = (b_{ij})$ sunt egale dacă şi numai dacă $a_{ij} = b_{ij}, 1 \le i, j \le n$.

Pe această mulțime se definesc cele două operații **de adunare** şi **de înmulțire** a matricelor, exact ca în cazul $\mathcal{M}_n(\mathbb{C})$, adică:

Dacă $X=\left(a_{ij}\right), Y=\left(b_{ij}\right), X, Y\in\mathcal{M}_n(A)$, atunci $X+Y=\left(a_{ij}+b_{ij}\right), 1\le i,\ j\le n$ reprezintă **suma** matricelor X şi Y, iar $XY=\left(c_{ij}\right), c_{ij}=\sum\limits_{k=1}^{n} a_{ik}b_{kj}, 1\le i,\ j\le n$ reprezintă **produsul** dintre matricea X şi matricea Y în această ordine.

Exemplu. **Fie în $\mathcal{M}_3(\mathbb{Z}_4)$ matricele** $X=\begin{pmatrix}\hat{1} & \hat{0} & \hat{2}\\ \hat{3} & \hat{1} & \hat{1}\\ \hat{2} & \hat{1} & \hat{0}\end{pmatrix}, Y=\begin{pmatrix}\hat{0} & \hat{1} & \hat{2}\\ \hat{3} & \hat{2} & \hat{3}\\ \hat{2} & \hat{1} & \hat{2}\end{pmatrix}$.

Atunci: $X+Y=\begin{pmatrix}\hat{1}+\hat{0} & \hat{0}+\hat{1} & \hat{2}+\hat{2}\\ \hat{3}+\hat{3} & \hat{1}+\hat{2} & \hat{1}+\hat{3}\\ \hat{2}+\hat{2} & \hat{1}+\hat{1} & \hat{0}+\hat{2}\end{pmatrix}=\begin{pmatrix}\hat{1} & \hat{1} & \hat{0}\\ \hat{2} & \hat{3} & \hat{0}\\ \hat{0} & \hat{2} & \hat{2}\end{pmatrix}$ **şi**

$$XY=\begin{pmatrix}\hat{1}\cdot\hat{0}+\hat{0}\cdot\hat{3}+\hat{2}\cdot\hat{2} & \hat{1}\cdot\hat{1}+\hat{0}\cdot\hat{2}+\hat{2}\cdot\hat{1} & \hat{1}\cdot\hat{2}+\hat{0}\cdot\hat{3}+\hat{2}\cdot\hat{2}\\ \hat{3}\cdot\hat{0}+\hat{1}\cdot\hat{3}+\hat{1}\cdot\hat{2} & \hat{3}\cdot\hat{1}+\hat{1}\cdot\hat{2}+\hat{1}\cdot\hat{1} & \hat{3}\cdot\hat{2}+\hat{1}\cdot\hat{3}+\hat{1}\cdot\hat{2}\\ \hat{2}\cdot\hat{0}+\hat{1}\cdot\hat{3}+\hat{0}\cdot\hat{2} & \hat{2}\cdot\hat{1}+\hat{1}\cdot\hat{2}+\hat{0}\cdot\hat{1} & \hat{2}\cdot\hat{2}+\hat{1}\cdot\hat{3}+\hat{0}\cdot\hat{2}\end{pmatrix}=\begin{pmatrix}\hat{0} & \hat{3} & \hat{2}\\ \hat{1} & \hat{2} & \hat{3}\\ \hat{3} & \hat{0} & \hat{3}\end{pmatrix}.$$

De asemenea dacă $X\in\mathcal{M}_n(A)$, atunci definim determinantul matricei X, elementul (din A): $\det\left(X\right)=\sum\limits_{\sigma\in S_n}\varepsilon(\sigma)a_{i\sigma(1)}a_{2\sigma(2)}\ldots a_{n\sigma(n)}$.

După cum se observă, definiţia este aceeaşi ca pentru $X\in\mathcal{M}_n(\mathbb{C})$, numai că aici elementele $a_{k\sigma(k)}$ aparţin inelului A şi evident se află în aceeaşi mulţime produsele de astfel de elemente ca şi sumele lor.

Au loc proprietăţile cunoscute de la determinanţi de matrice din $\mathcal{M}_n(\mathbb{C})$.

Exemplu. **Considerând matricele din exemplul de mai sus, calculăm determinantul lor cu regula lui Sarrus (X) şi cu regula triunghiului (Y).**

Avem: $\det\left(X\right)=\begin{vmatrix}\hat{1} & \hat{0} & \hat{2}\\ \hat{3} & \hat{1} & \hat{1}\\ \hat{2} & \hat{1} & \hat{0}\end{vmatrix}=\hat{1}\cdot\hat{1}\cdot\hat{0}+\hat{3}\cdot\hat{1}\cdot\hat{2}+\hat{2}\cdot\hat{0}\cdot\hat{0}-\left(\hat{2}\cdot\hat{1}\cdot\hat{2}+\hat{1}\cdot\hat{1}\cdot\hat{1}+\hat{0}\cdot\hat{0}\cdot\hat{3}\right)=\hat{2}-\hat{1}=\hat{1}$

$$\begin{matrix}\hat{1} & \hat{0} & \hat{2}\\ \hat{3} & \hat{1} & \hat{1}\end{matrix}$$

Observăm că $\det\left(X\right)=\hat{1}$ este inversabil în $\mathbb{Z}_4, \hat{1}^{-1}=\hat{1}$.

$\det\left(Y\right)=\begin{vmatrix}\hat{0} & \hat{1} & \hat{2}\\ \hat{3} & \hat{2} & \hat{3}\\ \hat{2} & \hat{1} & \hat{2}\end{vmatrix}=\hat{0}\cdot\hat{2}\cdot\hat{2}+\hat{1}\cdot\hat{3}\cdot\hat{2}+\hat{3}\cdot\hat{1}\cdot\hat{2}-\left(\hat{2}\cdot\hat{2}\cdot\hat{2}+\hat{0}\cdot\hat{1}\cdot\hat{3}+\hat{2}\cdot\hat{3}\cdot\hat{1}\right)=\hat{0}-\hat{2}=\hat{2}$. **În acest caz** $\det\left(Y\right)=\hat{2}$ **nu este inversabil în** $\mathbb{Z}_4$.

Pentru mulțimea $\mathcal{M}_n(A)$ înzestrată cu operațiile de adunare şi înmulțire are loc următoarea:

Teoremă. Fie A un inel comutativ cu $1 \neq 0$.
Tripetul $(\mathcal{M}_n(A), +, \cdot)$ este un **inel necomutativ** şi cu **divizori ai lui zero**, numit **inelul matricelor pătrate de ordin** n, cu elemente din A.

Demonstrație. Se verifică axiomele inelului, urmând analogia verificării axiomelor pentru $(M_n(\mathbb{C}), +, \cdot)$.

Să mai spunem că elementul nul este matricea $O_n \in \mathcal{M}_n(A)$ formată numai cu **elementul nul** 0 din A. Elementul unitate este matricea notată I_n având elementele de pe diagonala principală egale cu 1 (1 este unitatea inelului A), iar în rest elementele sunt egale cu 0 (0 este elementul nul al inelului A), $I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}$.

Uneori pentru I_n folosim scrierea $I_n = \left(\delta_{ij}\right)_{1 \leq i,\ j \leq n}$, unde $\delta_{ij} = \begin{cases} 1, \text{ dacă } i = j \\ 0, \text{ dacă } i \neq j \end{cases}$ se numeşte **simbolul lui Kronecker.** ■

În continuare vom preciza care sunt elementele inversabile (unitățile sau matricele inversabile) din $\mathcal{M}_n(A)$. Are loc următoarea:

Teoremă. Fie $X \in \mathcal{M}_n(A)$. Matricea X este inversabilă dacă şi numai dacă $\det(X)$ este element inversabil în inelul A.

Deci, $U(\mathcal{M}_n(A)) = \left\{X \in \mathcal{M}_n(A) \middle| \det(X) \in U(A)\right\}$.

Demonstrație. Se procedează, ca idee de lucru, ca în cazul $\mathcal{M}_n(\mathbb{C})$ când $X \in \mathcal{M}_n(\mathbb{C})$ este inversabilă $\Leftrightarrow \det(A) \neq 0$. (Aici $A = \mathbb{C}$ este corp şi deci orice $a \in \mathbb{C},\ a \neq 0$ este inversabil).

Fie $X \in \mathcal{M}_n(A)$ o matrice inversabilă. Deci există $X^{-1} \in \mathcal{M}_n(A)$ pentru care $XX^{-1} = X^{-1}X = I_n$. Luând în această egalitate determinantul avem: $\det\left(X \cdot X^{-1}\right) = \det(I_n) \Leftrightarrow$

$\Leftrightarrow \det(X)\det\left(X^{-1}\right)=1$ (am utilizat proprietatea pentru determinanți: determinantul produsului este egal cu produsul determinanților).

De aici se deduce că $\det(A)\in A$ este element inversabil în *A*.

Reciproc, presupunem că det(*X*) este un element inversabil în *A*, deci $\det(X)\in U(A)$.

Probăm că *X* este inversabilă construind X^{-1}.

Tehnica este aceeaşi cu cea utilizată în cazul $\mathcal{M}_n(\mathbb{C})$.

Construcția inversei lui *X* comportă următoarele etape:

1) Construcția transpusei lui X, ${}^tX \in \mathcal{M}_n(A)$ (prin schimbarea liniilor cu coloane).

2) Construcția adjunctei $X^* \in \mathcal{M}_n(A)$. Se obține din ${}^tX$, înlocuind fiecare element cu complementul lui algebric.

3) Construcția inversei $X^{-1} \in \mathcal{M}_n(A)$.

Avem: $X^{-1}=\left[\det(X)\right]^{-1}\cdot X^* \in \mathcal{M}_n(A)$.

Se arată că $XX^{-1}=X^{-1}X=I_n$ ■.

Observație. Pentru K *corp* avem că $\left(\mathcal{M}_n(K),+,\cdot\right)$ *este corp de matrice,* dacă $(\forall)A\in\mathcal{M}_n(K),\ A\neq O_n \Rightarrow \det(A)\neq 0$.

Exemplu. Fie K un corp şi $S_2(K)=\left\{\begin{pmatrix} x & y \\ -y & x\end{pmatrix}\middle| x,y\in K\right\}$. Atunci să arătăm că $S_2(K)$ este corp în raport cu operațiile de adunare şi înmulțire a matricelor pentru $K=\mathbb{Z}_3$, dar nu este corp pentru $K=\mathbb{Z}_5$.

Într-adevăr , adunarea şi înmulțirea sunt legi de compoziție interne pe $S_2(K)$ din egalitățile:

$$\begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1\end{pmatrix}+\begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2\end{pmatrix}=\begin{pmatrix} x_1+x_2 & y_1+y_2 \\ -(y_1+y_2) & x_1+x_2\end{pmatrix},\begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1\end{pmatrix}\cdot\begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2\end{pmatrix}=\begin{pmatrix} x_1x_2-y_1y_2 & x_1y_2+x_2y_1 \\ -(x_1y_2+x_2y_1) & x_1x_2-y_1y_2\end{pmatrix}$$

Elementul neutru pentru adunare este $\begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0}\end{pmatrix}$, iar pentru înmulțire este $\begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1}\end{pmatrix}$.

Dacă $M\in S_2(K)$, atunci $-M\in S_2(K)$. Evident, adunarea şi înmulțirea matricelor sunt asociative, în general, deci rămân la fel şi în acest caz. Înmulțirea este distributivă în raport cu adunarea matricelor. În general, înmulțirea matricelor nu este comutativă. În acest caz se verifică, prin calcul, comutativitatea înmulții acestor matrice.

Presupunem că matricea $\begin{pmatrix} x & y \\ -y & x\end{pmatrix}$ are inversă matricea $\begin{pmatrix} a & b \\ -b & a\end{pmatrix}$.

Din $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} x & y \\ -y & x \end{pmatrix}=\begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}$ rezultă $ax-by=\hat{1}, ay+bx=\hat{0}$, iar de aici soluția $a=x\left(x^2+y^2\right)^{-1}$, $b=-y\left(x^2+y^2\right)^{-1}$.

Deoarece K este corp, elementul x^2+y^2 are invers în K dacă $x^2+y^2\neq\hat{0}$. Dacă $x=y=\hat{0}$, matricea nulă nu are un invers. Rămâne de verificat dacă $x^2+y^2\neq\hat{0}$ cu $x,y\in K$, $x\neq\hat{0}$ sau $y\neq\hat{0}$.

În $\mathbb{Z}_3$ se verifică $x^2+y^2\neq\hat{0}$ când $(x,y)\neq(\hat{0},\hat{0})$. Într-adevăr,

x	$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{2}$	$\hat{2}$
y	$\hat{1}$	$\hat{2}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
x^2+y^2	$\hat{1}$	$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{2}$	$\hat{1}$	$\hat{2}$	$\hat{2}$

Deci, orice matrice nenulă din $S_2(\mathbb{Z}_3)$ are o inversă şi deci $(S_2(\mathbb{Z}_3),+,\cdot)$ este corp. Dar în $S_2(\mathbb{Z}_5)$, avem pentru $x=\hat{1}, y=\hat{2}, \hat{1}^2+\hat{2}^2=\hat{0}$ şi deci matricea $\begin{pmatrix} \hat{1} & \hat{2} \\ \hat{3} & \hat{1} \end{pmatrix}$ nu are inversă. Deci $(S_2(\mathbb{Z}_5),+,\cdot)$ nu este corp.

Arătați că: 1) $S_2(\mathbb{Z}_3)$ are nouă elemente; 2) Grupul aditiv nu este ciclic; 3) Grupul multiplicativ este ciclic.

Exemple. 1. **Stabiliți care din matricele $X,Y\in\mathcal{M}_3(\mathbb{Z}_{12})$**

$X=\begin{pmatrix} \hat{1} & \hat{2} & \hat{3} \\ \hat{4} & \hat{5} & \hat{1} \\ \hat{4} & \hat{2} & \hat{1} \end{pmatrix}, Y=\begin{pmatrix} \hat{7} & \widehat{11} & \hat{4} \\ \hat{5} & \hat{6} & \hat{5} \\ \hat{4} & \hat{2} & \hat{3} \end{pmatrix}$, **este inversabilă.**

R. Calculăm pentru fiecare matrice determinantul. Avem: $\det(X)=\hat{3}$ şi $\det(Y)=\hat{7}$.

Cum $\hat{3}\in\mathbb{Z}_{12}$ nu este inversabil rezultă că matricea X nu este inversabilă. Matricea Y este inversabilă deoarece $\hat{7}\in\mathbb{Z}_{12}$ este inversabil în $\mathbb{Z}_{12}$. Determinăm inversa lui Y.

1) *Transpusa* lui Y este: ${}^tY=\begin{pmatrix} \hat{7} & \hat{5} & \hat{4} \\ \widehat{11} & \hat{6} & \hat{2} \\ \hat{4} & \hat{5} & \hat{3} \end{pmatrix}$;

2) *Adjuncta* Y^* este: $Y^*=\begin{pmatrix} \hat{8} & \widehat{11} & \hat{5} \\ \hat{5} & \hat{7} & \hat{9} \\ \widehat{10} & \hat{6} & \widehat{11} \end{pmatrix}$.

3) *Inversa* lui *Y* este $Y^{-1}=\hat{7}^{-1}Y^{*}$, unde $\hat{7}^{-1}=\hat{7}$ şi deci $Y^{-1}=\hat{7}Y^{*}=\begin{pmatrix}\hat{8} & \hat{5} & \widehat{11}\\ \widehat{11} & \hat{1} & \hat{3}\\ \widehat{10} & \hat{6} & \hat{5}\end{pmatrix}$.

2. Stabiliţi care din matricele $X, Y \in \mathcal{M}_2(\mathbb{Z})$ sun inversabile, unde $X=\begin{pmatrix}2 & -1\\ -5 & 3\end{pmatrix}$, $Y=\begin{pmatrix}1 & -2\\ 0 & 3\end{pmatrix}$.

R. Din nou se calculează determinantul fiecărei matrice şi obţinem:
det(*X*) = 1, det(*Y*) = 3.
Numai matricea *X* este inversabilă în $\mathcal{M}_2(\mathbb{Z})$, deoarece 1 este element inversabil în $\mathbb{Z}$, în timp ce 3 nu este inversabil în $\mathbb{Z}$.

Calculul inversei lui *X*. 1) *Transpusa* lui *X* este: ${}^{t}X=\begin{pmatrix}2 & -5\\ -1 & 3\end{pmatrix}$;

2) *Adjuncta* lui *X* este: $X^{*}=\begin{pmatrix}3 & 1\\ 5 & 2\end{pmatrix}$;

3) *Inversa* lui *X* este: $X^{-1}=\left(\det(X)\right)^{-1}X^{*}=1\cdot X^{*}=\begin{pmatrix}3 & 1\\ 5 & 2\end{pmatrix}$.

Observaţie. Dacă *Y* este considerată în $\mathcal{M}_2(\mathbb{Q})$ (sau $\mathcal{M}_2(\mathbb{R})$ sau $\mathcal{M}_2(\mathbb{C})$) atunci det(*Y*) = 3 este inversabil în $\mathbb{Q}$ (sau $\mathbb{R}$ sau $\mathbb{C}$) şi deci în aceste mulţimi Y este inversabilă !

Definiţie. Grupul multiplicativ $U\left(\mathcal{M}_n(A)\right)$ al matricelor inversabile cu elemente din inelul *A* se numeşte **grupul liniar de ordinul *n* peste inelul** A şi se notează $\mathrm{GL}(n, A)$.

Deci $\mathrm{GL}(n,A)=\left\{X\in\mathcal{M}_n(A) \,\middle|\, \det(X)\in U(A)\right\}$.

În cazul în care *A* = *K*, corp comutativ, atunci $\mathrm{GL}(n,K)=\left\{X\in\mathcal{M}_n(K) \,\middle|\, \det(X)\neq 0\right\}$.

Domeniile de integritate şi corpurile

Am văzut că există inele cu divizori ai lui zero. În cazul unui corp acest lucru nu are loc. Avem următoarea:

Teoremă. Un corp nu admite divizori ai lui zero, adică din $x, y\in K$, $x\neq 0,\ y\neq 0 \Rightarrow xy\neq 0$.

Deci, orice corp este domeniu de integritate.

Demonstrație. Într-un corp orice element nenul este inversabil, iar un element inversabil nu poate fi divizor al lui zero într-un inel. ■
Este clar că nu orice domeniu de integritate este corp.
De exemplu, în inelul integru $(\mathbb{Z}, +, \cdot)$, numai elementele 1 şi –1 sunt inversabile. Dacă însă domeniul de integritate este finit, atunci acesta devine corp. Avem următoarea:

> **Teoremă.** Orice domeniu de integritate finit este corp.

Demonstrație. Fie *A*, domeniu de integritate finit, $A = \{a_1, a_2, ..., a_n\}$, iar $a \in A,\ a \neq 0$, un element arbitrar. Considerăm mulțimea produselor $\{aa_1, aa_2, ..., aa_n\}$. Aceste produse sunt toate distincte, deoarece din $aa_i = aa_j$ şi $a \neq 0$, rezultă $a_i = a_j$ (*A* nu are divizori ai lui zero). Cum $aa_i \in A, (\forall) i$ şi sunt distincte două câte două produsele, deducem că *A* este formată din aceste produse. În particular, unitatea inelului 1 este unul din aceste produse, adică $aa_k = 1$, pentru un anume a_k. Cum înmulțirea în *A* este comutativă, avem $a_k a = aa_k = 1$, adică a_k este inversul lui *a*. ■
Se pune întrebarea dacă există corpuri finite necomutative. Răspunsul este negativ. Rezultatul care afirmă că **orice corp finit este comutativ** a fost stabilit în 1905 şi este cunoscut sub numele de teorema lui Wedderburn.

> **Teoremă*.** Orice intersecție de subcorpuri ale unui corp *K* este subcorp al lui *K*.

Demonstrație. Fie $\{K_i'\}_{i\in I}$ o familie de subcorpuri ale lui *K* şi fie $K' = \bigcap_{i\in I} K_i'$.
Verificăm cele două proprietăți de la caracterizarea unui subcorp.
1) Dacă $x, y \in K'$, atunci să arătăm că $x - y \in K'$.

Din $x, y \in K' = \bigcap_{i\in I} K_i' \Rightarrow x, y \in K_i', (\forall) i \in I$. Cum K_i' este subcorp rezultă $x - y \in K'$, $(\forall) i \in I$, adică $x - y \in \bigcap_{i\in I} K_i'$.

2) Dacă $x, y \in K', x, y \neq 0$, atunci să probăm că $xy^{-1} \in K'$.

Într-adevăr din $x, y \in K' = \bigcap_{i\in I} K_i'$ se obține $x, y \in K_i', (\forall) i \in I$.

Deoarece K_i' este subcorp al lui *K*, se deduce $xy^{-1} \in K_i', (\forall) i \in I$, adică $xy^{-1} \in \bigcap_{i\in I} K_i'$.

Probleme propuse

1. Pentru A, B, matrice date mai jos, să se calculeze $A + B$, $A - B$, $\det(A)$ şi $\operatorname{rang}(A)$.

1) $A=\begin{pmatrix}\hat{3} & \hat{4}\\ \hat{1} & \hat{2}\end{pmatrix}, B=\begin{pmatrix}\hat{2} & \hat{1}\\ \hat{4} & \hat{3}\end{pmatrix}, A, B\in \mathcal{M}_2(\mathbb{Z}_5)$; 2) $A=\begin{pmatrix}\hat{0} & \hat{1}\\ \hat{2} & \hat{0}\end{pmatrix}, B=\begin{pmatrix}\hat{1} & \hat{2}\\ \hat{3} & \hat{1}\end{pmatrix}, A, B\in \mathcal{M}_2(\mathbb{Z}_4)$;

3) $A=\begin{pmatrix}\hat{1} & \hat{0} & \hat{2}\\ \hat{0} & \hat{1} & \hat{1}\\ \hat{3} & \hat{2} & \hat{4}\end{pmatrix}, B=\begin{pmatrix}\hat{1} & \hat{1} & \hat{3}\\ \hat{2} & \hat{2} & \hat{1}\\ \hat{4} & \hat{1} & \hat{3}\end{pmatrix}, A, B\in \mathcal{M}_3(\mathbb{Z}_5)$; 4) $A=\begin{pmatrix}\hat{2} & \hat{1} & \hat{0}\\ \hat{1} & \hat{3} & \hat{2}\\ \hat{2} & \hat{1} & \hat{1}\end{pmatrix}, B=\begin{pmatrix}\hat{0} & \hat{1} & \hat{0}\\ \hat{2} & \hat{0} & \hat{3}\\ \hat{0} & \hat{3} & \hat{0}\end{pmatrix}, A, B\in \mathcal{M}_3(\mathbb{Z}_4)$

2. Să se rezolve ecuațiile matriceale:

1) $X^2=\begin{pmatrix}\hat{2} & \hat{1}\\ \hat{1} & \hat{2}\end{pmatrix}$ în $M_2(\mathbb{Z}_3)$; 2) $X^2=\begin{pmatrix}\hat{1} & \hat{3}\\ \hat{2} & \hat{0}\end{pmatrix}$ în $M_2(\mathbb{Z}_4)$; 3) $X^2=\begin{pmatrix}\hat{1} & \hat{0}\\ \hat{1} & \hat{1}\end{pmatrix}$ în $M_2(\mathbb{Z}_3)$.

3. Să se calculeze inversa matricei A şi rezolvați ecuația matricală $XA = B$, în cazurile:

1) $A=\begin{pmatrix}\hat{1} & \hat{2}\\ \hat{3} & \hat{1}\end{pmatrix}, B=\begin{pmatrix}\hat{1} & \hat{3}\\ \hat{2} & \hat{2}\end{pmatrix}, A, B\in \mathcal{M}_2(\mathbb{Z}_4)$; 2) $A=\begin{pmatrix}\hat{1} & \hat{3}\\ \hat{2} & \hat{4}\end{pmatrix}, B=\begin{pmatrix}\hat{0} & \hat{4}\\ \hat{1} & \hat{3}\end{pmatrix}, A, B\in \mathcal{M}_2(\mathbb{Z}_4)$;

3) $A=\begin{pmatrix}\hat{2} & \hat{1} & \hat{4}\\ \hat{3} & \hat{2} & \hat{1}\\ \hat{6} & \hat{4} & \hat{5}\end{pmatrix}, B=\begin{pmatrix}\hat{1} & \hat{0} & \hat{6}\\ \hat{2} & \hat{4} & \hat{7}\\ \hat{1} & \hat{3} & \hat{2}\end{pmatrix}, A, B\in \mathcal{M}_3(\mathbb{Z}_8)$; 4) $A=\begin{pmatrix}\hat{1} & \hat{1} & \hat{1}\\ \hat{2} & \hat{3} & \hat{1}\\ \hat{4} & \hat{4} & \hat{3}\end{pmatrix}, B=\begin{pmatrix}\hat{0} & \hat{1} & \hat{3}\\ \hat{2} & \hat{0} & \hat{4}\\ \hat{1} & \hat{2} & \hat{0}\end{pmatrix}, A, B\in \mathcal{M}_3(\mathbb{Z}_5)$

4. Să se rezolve sistemele de ecuații:

1) $\begin{cases}\hat{2}x+y+z=\hat{1}\\ x+\hat{2}y+z=\hat{2}\\ x+y+\hat{2}z=\hat{3}\end{cases}$ în $\mathbb{Z}_5$; 2) $\begin{cases}\hat{2}x+\hat{3}y+z=\hat{3}\\ \hat{4}x+\hat{2}y+\hat{3}z=\hat{1}\\ \hat{6}x+\hat{3}y+\hat{2}z=\hat{2}\end{cases}$ în $\mathbb{Z}_8$; 3) $\begin{cases}x+\hat{2}y+\hat{3}z=\hat{4}\\ x+y+\hat{3}z=\hat{1}\\ \hat{2}x+\hat{3}y+\hat{5}z=\hat{2}\end{cases}$ în $\mathbb{Z}_9$;

4) $\begin{cases}x+\hat{3}y+\hat{3}z=\hat{9}\\ \hat{3}x+\hat{2}y+z=\hat{1}\\ \hat{2}x+\widehat{11}y+z=\hat{2}\end{cases}$ în $\mathbb{Z}_{12}$; 5) $\begin{cases}\hat{2}x+y+\hat{3}z=\hat{3}\\ x+\hat{2}y+z=\hat{2}\\ \hat{3}x+\hat{4}y+\hat{2}z=\hat{6}\end{cases}$ în $\mathbb{Z}_7$; 6) $\begin{cases}x+y+\hat{2}z=\hat{6}\\ \hat{2}x+\hat{6}y+\hat{2}z=\hat{3}\\ \hat{4}x+y+\hat{4}z=\hat{5}\end{cases}$ în $\mathbb{Z}_7$.

5. Să se rezolve şi discute sistemele:

1) $\begin{cases}mx+y+z=\hat{1}\\ x+my+z=\hat{2}\\ x+y+mz=\hat{3}\end{cases}$ în $\mathbb{Z}_5, m\in\mathbb{Z}_5$; 2) $\begin{cases}x+y-\hat{2}mz=\hat{0}\\ x-y+mz=\hat{1}\\ \hat{2}x+y+\hat{3}z=\hat{2}\end{cases}$ în $\mathbb{Z}_5, m\in\mathbb{Z}_5$;

3) $\begin{cases}\hat{2}x+\hat{2}y+z=\hat{4}\\ x+my+z=\hat{1}\\ \hat{3}x+y+\hat{3}z=\hat{3}\end{cases}$ în $\mathbb{Z}_5, m\in\mathbb{Z}_5$; 4) $\begin{cases}\hat{2}x+y+mz=\hat{2}\\ x+\hat{3}y+z=\hat{2}\\ \hat{3}x+\hat{2}y+z=\hat{3}\end{cases}$ în $\mathbb{Z}_5, m\in\mathbb{Z}_5$;

5) $\begin{cases}\hat{5}x+y-mz=\hat{3}\\ \hat{2}x+\hat{5}y+\hat{2}z=\hat{1}\\ x+\hat{2}y+z=\hat{5}\end{cases}$ în $\mathbb{Z}_6, m\in\mathbb{Z}_6$.

6. **Să se rezolve sistemele:**

1) $\begin{cases} x+y+\hat{3}z=\hat{2} \\ x^2+y^2+\hat{3}z^2=\hat{1} \\ x^3+y^3+\hat{3}z^3=\hat{2} \end{cases}$ **în** $\mathbb{Z}_5$ **; 2)** $\begin{cases} x(y+z)=\hat{2} \\ y(z+x)=\hat{2} \\ z(x+y)=\hat{2} \end{cases}$ **în** $\mathbb{Z}_6$ **; 3)** $\begin{cases} \hat{3}x+\hat{3}y+\hat{4}z=\hat{0} \\ x^2+y^2+\hat{4}z^2=\hat{5} \\ x^2+y^2+\hat{2}z^2=\hat{3} \end{cases}$ **în** $\mathbb{Z}_7$ **.**

Probleme rezolvate

1. Să se arate că aplicațiile $x*y=x+y+2,\ x\circ y=xy+2(x+y)+2$ determină pe mulțimea $\mathbb{Q}$ a numerelor raționale o structură de corp comutativ.

R. Verificăm axiomele corpului comutativ.

K$_1$) $(\mathbb{Q}*)$ este grup abelian, adică au loc axiomele:

G$_1$) *Legea $*$ este asociativă*, adică $(x*y)*z=x*(y*z),(\forall)x,y,z\in\mathbb{Q}$. Într-adevăr avem:

$(x*y)*z=(x+y+2)*z=(x+y+2)+z+2=x+y+z+4$, (1)

şi

$x*(y*z)=x*(y+z+2)=x+(y+z+2)+2=x+y+z+4$, (2)

Din (1) şi (2) se deduce că legea $*$ este asociativă.

G$_2$) *Legea $*$ este comutativă*, adică are loc egalitatea $x*y=y*x,(\forall)x,y\in\mathbb{Q}$.

Avem: $x+y+2=y+x+2,(\forall)x,y\in\mathbb{Q}$, deoarece adunarea pe $\mathbb{Q}$ este comutativă ($x+y=y+x$).

G$_3$) *Elementul neutru*. Să arătăm că există $e\in\mathbb{Q}$ astfel încât $x*e=x,(\forall)x\in\mathbb{Q}\Leftrightarrow x+e+2=x,(\forall)x\in\mathbb{Q}$. De aici $e=-2\in\mathbb{Q}$ este elementul neutru.

G$_4$) *Elemente simetrizabile*. Să arătăm că pentru $x\in\mathbb{Q}$, arbitrar ales, există $x'\in\mathbb{Q}$ astfel încât $x*x'=e\Leftrightarrow x+x'+2=-2\Leftrightarrow x'=-4-x\in\mathbb{Q}$. Deci orice $x\in\mathbb{Q}$ are un simetric $x'=-4-x\in\mathbb{Q}$.

K$_2$) $(\mathbb{Q}-\{-2\},\circ)$ este grup abelian, adică se verifică axiomele:

G$_1$) *Aplicația $\circ$ este lege de compoziție* pe $\mathbb{Q}-\{-2\}$, adică $(\forall)x,y\in\mathbb{Q}-\{-2\}\Rightarrow x\circ y\in\mathbb{Q}-\{-2\}$.

Într-adevăr $x\circ y\in\mathbb{Q}-\{-2\}\Leftrightarrow x,y\in\mathbb{Q}-\{-2\},\ x\circ y\neq-2\Leftrightarrow x,y\in\mathbb{Q}-\{-2\},\ xy+2(x+y)+2\neq-2\Leftrightarrow$

$\Leftrightarrow x,y\in\mathbb{Q}-\{-2\},(x+2)(y+2)\neq 0$, evident.

G$_2$) *Legea $\circ$ este asociativă*, $(x\circ y)\circ z=x\circ(y\circ z),(\forall)x,y,z\in\mathbb{Q}-\{-2\}$. Avem succesiv:

$(x\circ y)\circ z=[xy+2(x+y)+2]\circ z=[xy+2(x+y)+2]z+2[xy+2(x+y)+2+z]+2=xyz+$

$+2(xy+xz+yz)+4(x+y+z)+6$, (1)

$x\circ(y\circ z)=x\circ[yz+2(y+z)+2]=x[yz+2(y+z)+2]+2[x+yz+2(y+z)+2]+2=xyz+$

$+2(xy+xz+yz)+4(x+y+z)+6$, (2).

Din (1) şi (2) se deduce asociativitatea legii $\circ$.

Observăm că $x\circ y=(x+y)(y+2)-2$ şi atunci s-ar fi scris mai simplu:

$(x\circ y)\circ z=[(x+2)(y+2)-2]\circ z=(x+y)(y+2)(z+2)-2$ etc.

G$_3$) *Legea $\circ$ este comutativă*, deoarece $x\circ y=y\circ x,(\forall)x,y\in\mathbb{Q}-\{-2\}\Leftrightarrow xy+2(x+y)+2=$ $=yx+2(y+x)+2,(\forall)x,y\in\mathbb{Q}-\{-2\}$, adevărat dacă ținem seama că, adunarea şi înmulțirea pe $\mathbb{Q}$ sunt comutative.

G_4) *Elementul neutru* (unitate). Arătăm că există $u \in \mathbb{Q} - \{-2\}$ astfel încât $x \circ u = x, (\forall) x \in \mathbb{Q} - \{-2\}$. De aici $xu + 2(x+u) + 2 = x \Leftrightarrow u(x+2) = -(x+2) \Leftrightarrow u = -1 \in \mathbb{Q} - \{-2\}$.

G_5) *Elemente simetrizabile*. Fie $x \in \mathbb{Q} - \{-2\}$. Să arătăm că există $x'' \in \mathbb{Q} - \{-2\}$ astfel încât $x \circ x'' = -1$.

De aici avem: $xx'' + 2(x + x'') + 2 = -1 \Leftrightarrow x'' = -\dfrac{2x+3}{x+2}$.

Trebuie verificat că $x'' \in \mathbb{Q} - \{-2\}$. Evident $x'' \in \mathbb{Q}$. Rămâne să arătăm că $x'' \neq -2 \Leftrightarrow -\dfrac{2x+3}{x+2} \neq -2 \Leftrightarrow$ $\Leftrightarrow -2x - 3 \neq -2x - 4$, evident.

K_3) Să verificăm distributivitatea legii $\circ$ în raport cu $*$, adică să arătăm că $x \circ (y * z) = (x \circ y) * (x \circ z)$, $(\forall) x, y, z \in \mathbb{Q}$.

Calculăm fiecare membru şi avem:

$x \circ (y * z) = x \circ (x + z + 2) = x(y + z + 2) + 2(x + y + z + 2) + 2 = xy + xz + 4x + 2y + 2z + 6$, (1)

şi

$(x \circ y) * (x \circ z) = [xy + 2(x+y) + 2] * [xz + 2(x+z) + 2] = xy + 2(x+y) + 2 + xz + 2(x+z) + 2 + 2 =$
$= xy + xz + 4x + 2y + 2z + 6$, (2).

Din (1) şi (2) rezultă egalitatea propusă.

Cum cele trei axiome K_1), K_2), K_3) s-au verificat rezultă că tripletul $(\mathbb{Q}, *, \circ)$ este un corp comutativ.

2. Pe mulţimea $\mathbb{R}$ se definesc două legi de compoziţie $x * y = ax + by - 1$, $x \circ y = 2xy - 2(x+y) + c$, $a, b, c \in \mathbb{R}$.

Să se determine numerele a, b, c astfel încât tripletul $(\mathbb{R}, *, \circ)$ să fie corp comutativ.

R. Şi în acest caz se verifică cele trei axiome K_1, K_2, K_3 din definiţia corpului comutativ.

K_1) $(\mathbb{R}, *)$ este grup abelian, adică au loc axiomele:

G_1) *Legea $*$ este asociativă*, adică $(x * y) * z = x * (y * z), (\forall) x, y, z \in \mathbb{R}$. Scriem explicit egalitatea şi obţinem: $(ax + by - 1) * z = x * (ay + bz - 1), (\forall) x, y, z \in \mathbb{R}$, sau $a(ax + by - 1) + bz - 1 = ax +$ $+ b(ay + bz - 1) - 1, (\forall) x, y, z \in \mathbb{R}$.

De aici rezultă sistemul: $\begin{cases} a^2 = a \\ b = b^2 \\ -a - 1 = -b - 1 \Rightarrow a = b. \end{cases}$

G_2) *Legea $*$ este comutativă*, adică $x * y = y * x, (\forall) x, y \in \mathbb{R} \Leftrightarrow ax + by - 1 = ay + bx - 1, (\forall) x, y \in \mathbb{R}$, adevărată deoarece $a = b$ de mai sus.

G_3) *Elementul neutru*. Să găsim $e \in \mathbb{R}$ pentru care $x * e = x, (\forall) x \in \mathbb{R}$. De aici $ax + ae - 1 = c, (\forall) x \in \mathbb{R}$ sau $ae = 1 + x - ax, (\forall) x \in \mathbb{R}$. Cum elementul neutru al legii $*$ este unic (deci nu depinde de x) trebuie ca $a = 1$, când $e = 1$. Ţinând seama de cele de mai sus avem $a = b = 1$. Deci legea este $x * y = x + y - 1$.

G_4) *Elemente simetrizabile*. Pentru $x \in \mathbb{R}$, arbitrar ales, să arătăm că există $x' \in \mathbb{R}$ astfel încât $x * x' = 1 \Leftrightarrow x + x' - 1 = 1 \Leftrightarrow x' = 2 - x \in \mathbb{R}$. Deci orice $x \in \mathbb{R}$ este simetrizabil în raport cu legea $*$ şi are simetricul $x' = 2 - x$.

K_2) $(\mathbb{R}-\{1\},\circ)$ este grup abelian, adică se verifică axiomele:

G_4) *Aplicația „ $\circ$ “ este lege de compoziție* pe $\mathbb{R}-\{1\}$, adică din $x,y\in\mathbb{R}-\{1\}\Rightarrow x\circ y\in\mathbb{R}-\{1\}$.

Este clar că $x\circ y\in\mathbb{R}$. Rămâne de verificat că $x\circ y\neq 1\Leftrightarrow 2xy-2(x+y)+c\neq 1\Leftrightarrow 2(x-1)(y-1)\neq 3-c$.

Cum $x,y\neq 1$ rezultă $x-1,\ y-1\neq 0$. Deci $c-3=0$ dă $c=3$.

G_2) *Asociativitatea legii „ $\circ$ “* se verifică prin calcul.

Observație. De obicei valoarea parametrului c se determină din cerința de asociativitate sau comutativitate a legii $\circ$.

G_3) Comntativitatea legii „ $\circ$ “ se verifică ușor.

G_4) *Elementul neutru* (unitate) al legii „ $\circ$ “ este $u=\dfrac{3}{2}$.

G_5) *Elemente simetrizabile*. Pentru $x\in\mathbb{R}-\{1\}$, există $x"\in\mathbb{R}-\{1\}$ pentru care $x\circ x"=-\dfrac{3}{2}$. De aici $x"=\dfrac{4x-3}{4x-4}\in\mathbb{R}-\{1\}$.

K_3) Prin calcul se verifică distributivitatea legii „ $\circ$ “ în raport cu legea „ $*$ “. Acum putem concluziona că tripletul $(\mathbb{R},*,\circ)$ este corp comutativ

3. Să se arate că mulțimea $\mathcal{K}=\left\{M_{a,b}=\begin{pmatrix}a+b & b\\ b & a-b\end{pmatrix}\middle| a,b\in\mathbb{Q}\right\}$ împreună cu operațiile uzuale de adunare și înmulțire a matricelor formează un corp comutativ.

R. Vom face verificarea axiomelor corpului comutativ.

K_1) $(\mathcal{K},+)$ este grup abelian.

G_1) *Adunarea este lege de compoziție* pe $\mathcal{K}$, adică $(\forall)M_{a,b},M_{x,y}\in\mathcal{K}\Rightarrow M_{a,b}+M_{x,y}\in\mathcal{K}$.

Într-adevăr avem: $M_{a,b}+M_{x,y}=\begin{pmatrix}a+b & b\\ b & a-b\end{pmatrix}+\begin{pmatrix}x+y & y\\ y & x-y\end{pmatrix}=\begin{pmatrix}a+b+x+y & b+y\\ b+y & a-b+x-y\end{pmatrix}=$
$=M_{a+x,b+y}\in\mathcal{K}$.

G_2-G_3) *Întotdeauna adunarea matricelor pe $\mathcal{M}_2(\mathbb{Q})$ este asociativă și comutativă*. Deci și pe $\mathcal{K}\subset\mathcal{M}_2(\mathbb{Q})$ adunarea va avea aceste proprietăți.

G_4) *Elementul neutru.* Să arătăm că există $M_{e_1,e_2}\in\mathcal{K}$ astfel încât $M_{a,b}+M_{e_1,e_2}=M_{a,b},(\forall)M_{a,b}\in\mathcal{K}$. De aici rezultă $M_{a+e_1,b+e_2}=M_{a,b},(\forall)M_{a,b}\in\mathcal{K}$. Cum $M_{a,b}=M_{x,y}\Leftrightarrow(a=x \text{ și } b=y)$ rezultă $a+e_1=a$ și $b+e_2=b$ sau $e_1=e_2=0$. Așadar elementul neutru este $M_{0,0}=O_2\in\mathcal{K}$.

G_5) *Elemente simetrizabile*. Pentru $M_{a,b}\in\mathcal{K}$ să arătăm că există $M_{a',b'}\in\mathcal{K}$ astfel încât $M_{a,b}+M_{a',b'}=M_{0,0}\Leftrightarrow M_{a+a',b+b'}=M_{0,0}\Leftrightarrow(a+a'=0 \text{ și } b+b'=0)\Leftrightarrow(a'=-a,\ b'=-b)$. Deci simetricul lui $M_{a,b}\in\mathcal{K}$ este $M_{-a,-b}\in\mathcal{K}$, adică $M_{-a,-b}=\begin{pmatrix}-a-b & -b\\ -b & -a+b\end{pmatrix}=-M_{a,b}$ (opusa matricei $M_{a,b}$). Era de așteptat acest rezultat fiindcă avem adunarea obișnuită pe $\mathcal{K}$, elementul neutru fiind matricea nulă.

K_2) $(\mathcal{K}-\{O_2\},\cdot)$ este grup abelian. Deci verificăm axiomele grupului.

G$_1$) *Înmulțirea este lege de compoziție* pe $\mathcal{K}-\{O_2\}$, adică $(\forall)M_{a,b}, M_{x,y} \in \mathcal{K}-\{O_2\} \Rightarrow$

$\Rightarrow M_{a,b}\cdot M_{x,y} \in \mathcal{K}-\{O_2\}$. Într-adevăr $M_{a,b}\cdot M_{x,y} = \begin{pmatrix} a+b & b \\ b & a-b \end{pmatrix}\cdot\begin{pmatrix} x+y & y \\ y & x-y \end{pmatrix} =$

$= \begin{pmatrix} (ax+2by)+(bx+ay) & bx+ay \\ bx+ay & ax+2by-(bx+ax) \end{pmatrix} = M_{ax+2by,\ bx+ay} \in \mathcal{K}$.

G$_2$) *Întotdeauna înmulțirea matricelor este asociativă* pe $\mathcal{M}_2(\mathbb{Q})$. Deci rămâne la fel și pe $\mathcal{K}$.

G$_3$) Prin calcul se arată că *înmulțirea matricelor este comutativă* pentru că $M_{a,b}\cdot M_{x,y} = M_{ax+2by,bx+ay}$ și $M_{x.y}\cdot M_{a,b} = M_{xa+2yb,ya+xb}$ apoi se ține seama de egalitatea a două matrice.

G$_4$) *Elementul neutru* (unitate). Trebuie să găsim $M_{u_1,u_2} \in \mathcal{K}-\{O_2\}$ astfel încât $M_{a,b}\cdot M_{u_1,u_2} = M_{a,b}$, $(\forall)M_{a,b} \in \mathcal{K}-\{O_2\}$.

Egalitatea se mai scrie: $M_{au_1+2bu_2,bu_1+au_2} = M_{a,b}$ iar de aici avem sistemul $\begin{cases} au_1+2bu_2 = a \\ bu_1+au_2 = b \end{cases}$, $(\forall)a,b \in \mathbb{Q},\ a \neq 0$ sau $b \neq 0$.

Găsim ușor $u_1 = 1$ și $u_2 = 0$. Deci elementul unitate al inelului este $M_{1,0} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$.

G$_5$) *Elemente simetrizabile* (inversabile) Remarcăm că este înmulțirea obișnuită a matricelor, iar elementul unitate este chiar matricea unitate I_2. Dacă $M_{a,b} \in \mathcal{K}-\{O_2\}$, atunci $M_{a',b'} \in \mathcal{K}-\{O_2\}$ simetricul lui $M_{a,b}$ coincide cu inversa, deoarece trebuie să avem: $M_{a,b}\cdot M_{a',b'} = I_2$. Ori matricea $M_{a,b}$ este inversabilă dacă $\det(M_{a,b}) = a^2-2b^2 \neq 0$, ceea ce-i adevărat, căci în caz contrar din $a^2-2b^2 = 0$ și $b \neq 0$ (dacă $a = 0$, atunci $b = 0 \Rightarrow M_{0,0} \notin \mathcal{K}-\{O_2\}$) rezultă $2 = \dfrac{a^2}{b^2}$ sau $\dfrac{a}{b} = \pm\sqrt{2}$, fals pentru că membrul stâng este un număr rațional iar cel drept este irațional. Găsim ușor că $M_{a,b}^{-1} = M_{\frac{a}{a^2-2b^2},\frac{-b}{a^2-2b^2}} \in \mathcal{K}$.

Altfel din $M_{a,b}\cdot M_{a',b'} = M_{1,0}$ ar rezulta $M_{aa'+2bb',ab'+ba'} = M_{1,0}$, adică sistemul $\begin{cases} aa'+2bb' = 1 \\ ab'+ba' = 0 \end{cases}$ cu soluția $a' = \dfrac{a}{a^2-2b^2}$, $b' = \dfrac{-b}{a^2-2b^2}$.

K$_3$) Înmulțirea matricelor este întotdeauna distributivă în raport cu adunarea lor și deci rămâne la fel și pe $\mathcal{K}$.

Observație. Pentru partea a doua (verificările din K$_2$)) s-ar fi procedat mai ușor dacă se remarca faptul că, $M_{a,b} = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = aI_2 + bJ$, unde J are proprietatea $J^2 = 2I_2$.

4*. Fie A un inel cu patru elemente. Arătați că A este un corp dacă și numai dacă ecuația $x^2+x+1=0$ are o rădăcină în A.

R. Fie $A=\{0, 1, a, b\}$. Presupunem că ecuația $x^2+x+1=0$ are soluție în A. Este vizibil că 0 nu este soluție. Nici 1 nu este soluție pentru că în acest inel $1+1+1+1=0$ ((A, +) fiind grup, atunci (Lagrange) 1+ 1+ 1+ 1 = 0). Pe de altă parte 1+1+ 1 = 0, iar din ultimele relații deducem 1 = 0, fals. Fie a soluție a ecuației. Deci $a^2+a+1=0$. Avem $a+1=b$, deoarece $a+1\neq 0\left((-1)^2+(-1)+1=0\Leftrightarrow 1=0\right)$, $a+1\neq 1\ (a\neq 0),\ a+1\neq a\ (1\neq 0)$. Din $a^2+a+1=0$ se deduce $a(a+1)=-1$ și deci $ab=1$, ceea ce arată că a și b sunt inversabile în A, adică A este corp. Reciproc, presupunem că $A=\{0, 1, a, b\}$ este corp. Atunci $A^*=\{1, a, b\}$ este grup multiplicativ. Am văzut la grupuri izomorfe că orice grup cu trei elemente este izomorf cu grupul multiplicativ al rădăcinilor de ordinul trei ale unității în care orice element x verifică relația $x^3=1$. În particular $a^3=1$. Dar $a^3-1=(a-1)\left(a^2+a+1\right)=0$. Cum $a\neq 1$ rezultă $a^2+a+1=0$.

5. Fie $(K,+,\cdot)$ un corp și a, b două elemente distincte din $K-\{0\}$. DacĂ $a+b=a^{-1}+b^{-1}=1$, demonatrați că $a=b^{-1}$ și $b=a^{-1}$.

R. Avem: $a\cdot b=a\cdot 1\cdot b=a\left(a^{-1}+b^{-1}\right)b=\left(aa^{-1}\right)b+a\left(b^{-1}b\right)=b+a=1$ și $b\cdot a=b\cdot 1\cdot a=b\left(b^{-1}+a^{-1}\right)a=$ $=\left(bb^{-1}\right)a+b\left(a^{-1}a\right)=a+b=1$. De aici rezultă: $a=b^{-1}$ și $b=a^{-1}$.

Probleme propuse

1. Arătați că următoarele de numere împreună cu operațiile obișnuite de adunare și înmulțire sunt corpuri:

1) $\mathbb{Q}$; **2)** $\{a+b\sqrt{3}\,|\,a,b\in\mathbb{Q}\}$; **3)** $\{a+bi\,|\,a,b\in\mathbb{Q}\}$; **4)** $\{a+b\sqrt{3}i\,|\,a,b\in\mathbb{Q}\}$;

5) $\left\{a+b\varepsilon\,\middle|\,\varepsilon=\dfrac{-1+i\sqrt{3}}{2},\ a,b\in\mathbb{R}\right\}$; **6)** $\left\{a+b\sqrt[3]{2}+c\sqrt[3]{4}\,\middle|\,a,b,c\in\mathbb{Q}\right\}$.

2. Arătați că următoarele mulțimi de matrice împreună cu operațiile obișnuite de adunare și înmulțire sunt corpuri:

1) $\left\{\begin{pmatrix} a & 3b \\ b & a\end{pmatrix}\middle|\, a,b\in\mathbb{Q}\right\}$; **2)** $\left\{\begin{pmatrix} a & -b \\ b & a\end{pmatrix}\middle|\, a,b\in\mathbb{Q}\right\}$; **3)** $\left\{\begin{pmatrix} a & -3b \\ b & a\end{pmatrix}\middle|\, a,b\in\mathbb{Q}\right\}$; **4)** $\left\{\begin{pmatrix} a+b & 4b \\ -b & a-b\end{pmatrix}\middle|\, a,b\in\mathbb{Q}\right\}$;

5) $\left\{\begin{pmatrix} a & 0 \\ a & 0\end{pmatrix}\middle|\, a\in\mathbb{R}\right\}$; **6)** $\left\{\begin{pmatrix} a & b \\ -b & a\end{pmatrix}\middle|\, a,b\in\mathbb{R}\right\}$; **7)** $\left\{\begin{pmatrix} a & b \\ -b & a+b\end{pmatrix}\middle|\, a,b\in\mathbb{R}\right\}$; **8)** $\left\{\begin{pmatrix} a & -5b \\ b & a+3b\end{pmatrix}\middle|\, a,b\in\mathbb{R}\right\}$;

9) $\left\{\begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0}\end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1}\end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{1} & \hat{1}\end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & \hat{0}\end{pmatrix}\right\}\subset\mathcal{M}_2(\mathbb{Z}_2)$; **10)** $\left\{A_{x,y}=\begin{pmatrix} x & y \\ 2y & x\end{pmatrix}\middle|\, A\in\mathcal{M}_2(\mathbb{Z}_3)\right\}$;

11) $\left\{\begin{pmatrix} x & x \\ x & x\end{pmatrix}\middle|\, x\in\mathbb{R}\right\}$; **12)** $\left\{\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a\end{pmatrix}\middle|\, a,b,c,d\in\mathbb{Q}\right\}$.

3. Arătați că următoarele mulțimi împreună cu aplicațiile considerate în dreptul lor sunt corpuri:

1) $\mathbb{R}$; $x * y = x + y - 4$, $x \circ y = xy - 4(x + y) + 20$; $(\mathbb{R}, *, \circ)$;

2) $(0,\infty)$; $x * y = xy$, $x \circ y = x^{\ln y}$; $((0,\infty), *, \circ)$;

3) $\mathbb{R}$; $x * y = x + y - 2$, $x \circ y = 2xy - 4(x + y) + 10$; $(\mathbb{R}, *, \circ)$;

4) $\mathcal{K} = \left\{ f_a : \mathbb{R} \to \mathbb{R} \middle| f_a(x) = ax, a \in \mathbb{R} \right\}$, $(f + g)(x) = f(x) + g(x)$, $(f \circ g)(x) = f(g(x))$; $(\mathcal{K}, +, \circ)$;

5) $\mathcal{K} = \left\{ f_a : \mathbb{R} \to \mathbb{R} \middle| a \in \mathbb{Q},\ f_a(x) = \begin{cases} ax, & x \in \mathbb{Q} \\ 0, & x \in \mathbb{R} - \mathbb{Q} \end{cases} \right\}$ **împreună cu adunarea și compunerea funcțiilor.**

6) $\mathbb{C}$; $x * y = x + y - i$, $x \circ y = mixy + m(x + y) + i(1 - m)$, $m \in \mathbb{C}^*$, $(\mathbb{C}, *, \circ)$;

7) $\mathbb{R}$; $x * y = \sqrt[3]{x^3 + y^3}$, $x \circ y = xy$; $(\mathbb{R}, *, \circ)$.

4. Arătați că următoarele mulțimi împreună cu operațiile considerate în dreptul lor sunt corpuri comutative:

1) $\mathbb{Q} \times \mathbb{Q}$; $(a,b) + (a',b') = (a + a', b + b')$, $(a,b) \circ (a',b') = (aa' + 2bb', ab' + a'b)$;

2) $\mathbb{R} \times \mathbb{R}$; $(a,b) + (a',b') = (a + a', b + b')$, $(a,b) \circ (a',b') = (aa' - bb', ab' + a'b)$.

5. Fie $a, b \in \mathbb{R}$ și legile de compoziție: $x \perp y = ax + by - 2$, $x \top y = xy - 2(x + y) + 6$. Să se determitie a, b astfel încât tripletul $(\mathbb{R}, \perp, \top)$ să fie corp.

6. 1) $\mathcal{K} = \left\{ \begin{pmatrix} x & y \\ 2y & x \end{pmatrix} \middle| x, y \in \mathbb{Z}_3 \right\}$ împreună cu operațiile de adunare și înmulțire a matricelor este corp cu 9 elemente.

2) Fie mulțimea $\mathcal{K} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{Z}_7 \right\}$. Arătați tripletul $(\mathcal{K}, +, \cdot)$ este un corp comutativ cu 49 de elemente.

7. Fie $\mathcal{K}$ mulțimea tuturor matricelor $U_{a,b} \in \mathcal{M}_3(\mathbb{R})$ de forma :

$$U_{a,b} = \begin{pmatrix} -a-b & a & b \\ b & -a-b & a \\ a & b & -a-b \end{pmatrix}, a, b \in \mathbb{R}.$$

Să se arate că adunarea și înmulțirea matricelor determină pe $\mathcal{K}$ o structură de corp comutativ.

8. Se consideră $K = \{0, 1, a, b\}$ un corp cu patru elemente. Să se arate că: 1) $ab = 1 = ba$; 2) $a^2 = b, a^3 = 1$, $a^2 + a + 1 = 0$; 3) $1 + 1 = 0$; 4) Să se facă tabela de adunare pentru K.

2.3. MORFISME ȘI IZOMORFISME DE INELE ȘI CORPURI

Conceptul de izomorfism (morfism) de la grupuri poate fi aplicat la fel de bine la inele și corpuri. Definiția care urmează este o extindere a conceptului de izomorfism (morfism) de grupuri. Deoarece în definiția inelului și a corpului sunt două operații binare, vom cere ca izomorfismul (morfismul) să conserve aceste operații. Mai precis formulăm următoarea:

Definiție. Fie $(A, +, \cdot)$ şi $(A', \oplus, \odot)$ două inele. O aplicație $f : A \to A'$ se numeşte **morfism** (sau **omomorfism**) **de inele** dacă satisface următoarele două condiții:

1) $f(x+y) = f(x) \oplus f(y)$, pentru orice $x, y \in A$;

2) $f(xy) = f(x) \odot f(y)$, pentru orice $x, y \in A$.

Observații. **1)** Din definiție rezultă că orice morfism de inele este şi un morfism de grupuri, de la grupul aditiv al lui A la grupul aditiv al lui A'. Atunci, dacă $f : A \to A'$ este morfism de inele, din proprietățile morfismelor de grupuri, rezultă:
1°) $f(0) = 0'$ (unde 0 este elementul nul al lui A, iar $0'$ este elementul nul al lui A') (spunem simplu că un morfism de inele „duce“ elementul nul în elementul nul)
2°) $f(-x) = -f(x), (\forall) x \in A$ (imaginea opusului prin morfism este opusul imaginii).
2) Pentru inelele A şi A' din condiția **2)** nu se poate deduce că $f(1) = 1'$ (1 este elementul unitate pentru A, iar $1'$ este elementul unitate al lui A'). Dacă în plus A' este domeniu de integritate, atunci $f(1) = 1'$.

Definiție. Fie $(A, +, \cdot)$ şi $(A', \oplus, \odot)$ două inele. Un morfism de inele $f : A \to A'$ cu proprietatea $f(1) = 1'$

se numeşte **morfism unitar** de inele (1, respectiv 1' sunt elementele unitate din A şi respectiv A').

Un morfism de inele de la un inel la el însuşi se numeşte **endomorfism** al inelului respectiv.
Compunerea a două morfisme de inele este încă morfism de inele (Verificați!).

Exemple. 1. Fie A şi A' două inele. Aplicația $f : A \to A'$ definită prin $f(x) = 0', (\forall) x \in A$ este un morfism de inele, numit morfismul nul. Se verifică uşor cele două condiții din definiție:
1) $f(x+y) = 0' = 0' \oplus 0' = f(x) \oplus f(y), (\forall) x, y \in A$ **şi**
2) $f(xy) = 0' = 0' \odot 0' = f(x) \odot f(y), (\forall) x, y \in A$.

2. Fie A un inel. Aplicația identică $1_A : A \to A, 1_A(x) = x$ este un morfism unitar de inele, aparținând endomorfismelor lui A.

3. Fie inelul $\mathbb{Z}[\sqrt{2}]$. Atunci aplicația $f : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ definită prin $f(a + b\sqrt{2}) = a - b\sqrt{2}$ este un morfism de inele pentru că avem:

1) $f\left(a_1+b_1\sqrt{2}+a_2+b_2\sqrt{2}\right)=f\left(a_1+a_2+\left(b_1+b_2\right)\sqrt{2}\right)=a_1+a_2-\left(b_1+b_2\right)\sqrt{2}=\left(a_1-b_1\sqrt{2}\right)+$
$+\left(a_2-b_2\sqrt{2}\right)=f\left(a_1+b_1\sqrt{2}\right)+f\left(a_2+b_2\sqrt{2}\right)$

şi

2) $f\left(\left(a_1+b_1\sqrt{2}\right)\left(a_2+b_2\sqrt{2}\right)\right)=f\left(a_1a_2+2b_1b_2+\left(a_1b_2+a_2b_1\right)\sqrt{2}\right)=a_1a_2+2b_1b_2-\left(a_1b_2+a_2b_1\right)\sqrt{2}=$
$=a_2\left(a_1-b_1\sqrt{2}\right)+\sqrt{2}b_2\left(\sqrt{2}b_1-a_1\right)=\left(a_1-\sqrt{2}b_1\right)\left(a_2-\sqrt{2}b_2\right)=f\left(a_1+b_1\sqrt{2}\right)f\left(a_2+b_2\sqrt{2}\right).$

4. Aplicaţia $f:(\mathbb{Z},+,\cdot)\to(\mathbb{Z}_n,+,\cdot),\ n\geq 2,\ n\in\mathbb{N},\ f(x)=\hat{x}$, **este un morfism de inele, numit morfismul canonic. Într-adevăr avem:**

1) $f(x+y)=\widehat{x+y}=\hat{x}+\hat{y}=f(x)+f(y),\ (\forall)x,y\in\mathbb{Z}$ **şi**

2) $f(xy)=\widehat{xy}=\hat{x}\hat{y}=f(x)f(y),\ (\forall)x,y\in\mathbb{Z}$.

Dacă *f* are proprietate particulară, atunci morfismul se numeşte conform următoarelor:

Definiţii. 1) Un morfism de inele $f:A\to A'$ se numeşte **morfism injectiv**, dacă *f* este injectivă.

2) Un morfism de inele $f:A\to A'$ se numeşte **morfism surjectiv**, dacă *f* este surjectivă. În acest cau $A'=f(A)=\operatorname{Im} f$.

3) Un morfism de inele $f:A\to A'$ se numeşte **izomorfism**, dacă *f* este bijectivă.

Dacă între două inele *A*, *A'*, există cel puţin un izomorfism de inele spunem că inelele sunt **izomorfe** şi scriem $A\simeq A'$ (citim: inelul *A* este izomorf cu inelul *A'*).

Să reţinem conceptul important de izomorfism de inele.
Aplicaţia $f:A\to A'$ este **izomorfism de inele** dacă:
1) *f* este morfism de inele;
2) *f* este bijectivă.

Dacă două inele sunt izomorfe, atunci grupurile aditive $(A,+)$, $(A',\oplus)$ sunt izomorfe, iar monoizii $(A,\cdot)$, $(A',\odot)$ sunt de asemenea izomorfi.

Se verifică faptul că morfismul de inele $f:A\to A'$ este injectiv dacă $\operatorname{Ker} f=\{0\}$ ($\operatorname{Ker} f=\{x\in A \mid f(x)=0'\}$ se numeşte nucleul morfismului *f*).

Un izomorfism de la inelul *A* la el însuşi se numeşte **automorfism**. Compunerea a două izomorfisme de inele este încă izomorfism de inele (Verificaţi !).

Exemple. 1. **Fie A un inel. Aplicația identică $1_A : A \to A, 1_A(x) = x$ este un automorfism al inelului A. Am arătat mai sus (exemplul 3)) că 1_A este endomorfism al inelului A. Cum 1_A este o aplicație bijectivă, se deduce că 1_A este automorfism al inelului A.**

2. Funcția $f : (\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_n, +, \cdot), f(x) = \hat{x}, (\forall) x \in \mathbb{Z}$ este un morfism surjectiv de inele.

3. Morfismul $f : \mathbb{Z}\left[\sqrt{2}\right] \to \mathbb{Z}\left[\sqrt{2}\right], f\left(a + b\sqrt{2}\right) = a - b\sqrt{2}$ este bijectiv deoarece *f* este injectiv, adică dacă $f\left(a_1 + b_1\sqrt{2}\right) = f\left(a_2 + b_2\sqrt{2}\right) \Rightarrow a_1 - b_1\sqrt{2} = a_2 - b_2\sqrt{2} \Rightarrow a_1 = a_2$ și $b_1 = b_2$ ceea ce dă $a_1 + b_1\sqrt{2} = a_2 + b_2\sqrt{2}$.

(Se ştie că dacă $a + b\sqrt{2} = a' + b'\sqrt{2}, a, a', b, b' \in \mathbb{Z}$, atunci $a = a', b = b'$, deoarece scriind relația sub forma $(b - b')\sqrt{2} = a' - a$, atunci dacă $b \neq b'$, s-ar obține $\sqrt{2} = \dfrac{a' - a}{b - b'}$, fals deoarece $\sqrt{2} \notin \mathbb{Q}$ în timp ce $\dfrac{a' - a}{b - b'} \in \mathbb{Q}$. Deci $b = b'$ şi atunci evident $a = a'$. Reciproca este imediată).

Aplicația *f* este surjectivă deoarece pentru $z = a + b\sqrt{2}$, atunci există $\bar{z} = a - b\sqrt{2} \in \mathbb{Z}\left[\sqrt{2}\right]$ pentru care $f(\bar{z}) = z$.

> **Definiție.** Fie $(K, +, \cdot)$ şi $(K', \oplus, \odot)$ două corpuri. O aplicație $f : K \to K'$ se numeşte:
>
> a) **morfism de corpuri** dacă:
>
> 1) $f(x + y) = f(x) \oplus f(y), (\forall) x, y \in K$;
>
> 2) $f(xy) = f(x) \odot f(y), (\forall) x, y \in K$.
>
> b) **izomorfism de corpuri**, dacă
>
> 1) *f* este morfism de corpuri;
>
> 2) *f* este bijectiv.

Observăm din definiția de la a) că morfismul de corpuri fiind un morfism între domenii de integritate avem $f(1) = 1'$.

Un morfism de corpuri de la un corp la el însuşi se numeşte **endomorfism** al acelui corp.

Un izomorfism de corpuri de la un corp la el însuşi se numeşte **automorfism** al acelui corp.

Exemple. 1. Aplicația $f : \mathbb{Q} \to \mathbb{C}, f(x) = x$ este un morfism de corpuri numit morfismul-incluziune.

2. Aplicația $f : \mathbb{C} \to \mathbb{C}, f(z) = \bar{z}$ este un automorfism al lui $\mathbb{C}$ (Verificați!).

> **Teoremă.** Orice morfism de corpuri este injectiv.

Demonstrație. Fie $f: K \to K'$ un morfism de corpuri. Fie $x, y \in K$ pentru care $f(x) = f(y)$. Notăm $z = x - y$. Avem $f(z) = f(x + (-y)) = f(x) + f(-y) =$ $= f(x) + (-f(y)) = f(x) + (-f(x)) = 0'$.

Dacă $z \neq 0$, atunci $1' = f(1) = f(zz^{-1}) = f(z)f(z^{-1}) = 0' f(z^{-1}) = 0'$, contradicție deoarece $1' \neq 0'$. Deci $z = 0$, adică $x = y$, ceea ce inseamnă că f este injectiv.

Comportarea subinelelor (subcorpurilor) la morfisme de inele (corpuri) este dată, de următoarea

> **Teoremă.*** Fie $f: A \to A'$ un morfism de inele (respectiv de corpuri). Atunci:
>
> **1)** Pentru orice subinel (respectiv subcorp) B al lui A, mulțimea $B' = f(B)$ este subinel (respectiv subcorp) al lui A'; în particular $\operatorname{Im} f = f(A)$ este subinel (respectiv subcorp) al lui A'.
>
> **2)** Dacă f este morfism injectiv, atunci A este izomorf cu un subinel (respectiv subcorp) al lui B.

Observații. **1)** Prima afirmație din teoremă se poate formula astfel: imaginea unui subinel (subcorp) printr-un morfism de inele (corpuri) este de asemenea un subinel (subcorp).

Partea a doua a teoremei afirmă că inelul (corpul) A se poate scufunda izomorf într-un subinel (subcorp) al lui B printr-un morfism injectiv.

Demonstrație.* **1)** Dacă se traduce morfismul de inele (corpuri) în limbaj de morfism de grupuri aditive $\left(f:(A, +) \to (A', \oplus)\right)$ şi morfism de monoizi $\left(f:(A, \cdot) \to (A', \odot)\right)$, iar subinelul B al lui A ca subgrup al lui $(A, +)$ şi respectiv monoid al lui $(A, \cdot)$ şi se ține seama de propoziția de la morfisme de grupuri şi monoizi conform căreia imaginea unui subgrup al lui $(A, +)$ prin f este subgrup al lui $(A', \oplus)$ şi imaginea unui monoid al lui $(A, \cdot)$ este tot monoid al lui $(A', \odot)$ demonstrația lui 1) este imediată.

2) Dacă A este morfism injectiv de inele, atunci $A \simeq \operatorname{Im} f$ ($\operatorname{Im} f$ este subinel (subcorp) al lui A').

În consecință la 2), dacă $f: K \to K'$ este morfism injectiv de corpuri, corpul K este izomorf cu un subcorp al lui K'.

Probleme rezolvate

1. Să se arate că aplicația $f: \mathbb{Z} \to \mathbb{Z}_2$, $f(x) = \begin{cases} \hat{0}, \text{ dacă } x \text{ este par} \\ \hat{1}, \text{ dacă } x \text{ este impar} \end{cases}$, este morfism de inele.

R. Trebuie să verificăm cele două condiții ale morfismului de inele.

1) $f(x+y)=f(x)+f(y), (\forall)x,y\in\mathbb{Z}$,

2) $f(xy)=f(x)f(y), (\forall)x,y\in\mathbb{Z}$.

Pentru verificarea condiției 1) analizăm cazurile:

a) x, y numere întregi pare $(x, y \in 2\mathbb{Z})$. Atunci: $f(x+y)=\hat{0}$ (deoarece $x+y$ este par) şi $f(x)+f(y)=\hat{0}+\hat{0}=\hat{0}$. Deci în acest caz, 1) are loc.

b) $x,y\in\mathbb{Z}$ de parităţi diferite. Să spunem $x\in 2\mathbb{Z}, y\in 2\mathbb{Z}+1$. Atunci $f(x+y)=\hat{1}$ ($x+y$ este impar) şi $f(x)+f(y)=\hat{0}+\hat{1}=\hat{1}$.

Şi în acest caz, 1) se verifică. Analog se tratează cazul $x\in 2\mathbb{Z}+1, y\in 2\mathbb{Z}$.

c) x,y numere întregi impare $(x,y\in 2\mathbb{Z}+1)$. Avem: $f(x+y)=\hat{0}$ ($x+y$ este par) şi $f(x)+f(y)=\hat{1}+\hat{1}=\hat{0}$, ceea ce arată că 1) are loc.

Pentru verificarea condiției 2) se analizează aceleaşi cazuri.

Avem: a) $x,y\in 2\mathbb{Z}$, $f(xy)=\hat{0}$ şi $f(x)f(y)=\hat{0}\cdot\hat{0}=\hat{0}$, adică 2) are loc.

b) $x\in 2\mathbb{Z}$ şi $y\in 2\mathbb{Z}+1$ când $f(xy)=\hat{0}$ şi $f(x)f(y)=\hat{0}\cdot\hat{1}=\hat{0}$, adică 2) se verifică.

c) $x,y\in 2\mathbb{Z}+1$, când $f(xy)=\hat{1}$ şi $f(x)f(y)=\hat{1}\cdot\hat{1}=\hat{1}$, şi din nou 2) are loc.

2. Pe mulțimea $\mathbb{R}$ se consideră operațiile: $x\top y=x+y-1$, $x\perp y=x+y-xy$. Să se arate că $(\mathbb{R},\top,\perp)$ este inel izomorf cu $(\mathbb{R},+,\cdot)$ prin $f:\mathbb{R}\to\mathbb{R}, f(x)=1-x$.

R. Lăsăm în seama cititorului să verifice că tripletul $(\mathbb{R},\top,\perp)$ este un domeniu de integritate.

Probăm că $f:\mathbb{R}\to\mathbb{R}, f(x)=1-x$ este izomorfism de inele. Trebuie să verificăm că:

1) *f este morfism de inele*,
2) *f este bijectivă*.

1) Funcția *f* este morfism de inele dacă:

a) $f(x\top y)=f(x)+f(y), (\forall)x,y\in\mathbb{R}$, b) $f(x\perp y)=f(x)f(y), (\forall)x,y\in\mathbb{R}$.

Verificăm a). Avem $f(x\top y)=f(x+y-1)=1-(x+y-1)=2-x-y=1-x+1-y=f(x)+f(y)$.

Verificăm b). Avem: $f(x\perp y)=f(x+y-xy)=1-(x+y-xy)=1-x-y+xy=(1-x)(1-y)=f(x)f(y)$.

Cum a) şi b) au fost verificate deducem că *f* este morfism de inele.

2) Funcția liniară $f:\mathbb{R}\to\mathbb{R}, f(x)=ax+b$ se ştie că este bijectivă dacă, $a\neq 0$. Deci în cazul nostru $a=-1, b=1$, funcția f este şi bijectivă. Deoarece condițiile 1) şi 2) au fost verificate rezultă că f realizează izomorfismul între cele două inele.

3. Pe mulțimea numerelor întregi $\mathbb{Z}$ se definesc aplicațiile: $x*y=x+y-2$, $x\circ y=xy-2(x+y)+6$ împreună cu care devine domeniu de integritate. Să se arate că avem izomorfismul de inele $(\mathbb{Z},*,\circ)\simeq(\mathbb{Z},+,\cdot)$ dat de $f(x)=\alpha x+\beta$.

R. Se arată uşor că tripletul $(\mathbb{Z},*,\circ)$ este un domeniu de integritate. Atunci ştim că morfismul de inele are proprietățile $f(e_*)=0$ şi $f(u_\circ)=1$, unde e_*, este elementul neutru în raport cu legea $*$, iar $u_\circ$ este elementul unitate al inelului (în raport cu a doua lege $\circ$).

Găsim uşor $e_*=2, u_0=3$. Deci avem sistemul: $\begin{cases} f(2)=0 \\ f(3)=1 \end{cases}$ cu soluția $\alpha=1, \beta=-2$.

Prin urmare $f:\mathbb{Z}\to\mathbb{Z}, f(x)=x-2$. Probăm că *f* este izomorfism de inele, adică:

1) *f este morfism de inele*,
2) *f este bijectivă*.

Afirmația 1) se verifică dacă avem:

a) $f(x*y)=f(x)+f(y), (\forall)x,y\in\mathbb{Z}$; și b) $f(x\circ y)=f(x)\cdot f(y), (\forall)x,y\in\mathbb{Z}$.

Într-adevăr pentru a) avem: $f(x*y)=f(x+y-2)=(x+y-2)-2=x+y-4=(x-2)+(y-2)=$
$=f(x)+f(y)$.

Analog pentru b) se obține: $f(x\circ y)=f(xy-2x-2y+6)=(xy-2x-2y+6)-2=$
$=(x-2)(y-2)=f(x)f(y)$.

Demonstrăm 2). Aplicația *f* este bijectivă dacă: a') *f* este injectivă și b') *f* este surjectivă.

Verificăm a'). Funcția f este injectivă dacă din $f(x)=f(y), x,y\in\mathbb{Z}\Rightarrow x=y$. Avem $f(x)=f(y)\Leftrightarrow$
$\Leftrightarrow x-2=y-2$. De aici $x=y$.

Pentru b'), funcția *f* este surjectivă dacă pentru orice $y\in\mathbb{Z}$ (codomeniu) există $x\in\mathbb{Z}$ (domeniu) astfel încât $f(x)=y$.

Din $f(x)=y$ rezultă $x-2=y$, adică $x=y+2$, acesta fiind elementul căutat. Evident $x=y+2\in\mathbb{Z}$.

Din cele de mai sus rezultă că inelele sunt izomorfe.

4. Arătați că inelele $\left(\mathcal{A}=\{x+y\sqrt{3}\,|\,x,y\in\mathbb{Z}\},+,\cdot\right)$, $\left(\mathcal{A}'=\left\{\begin{pmatrix} x & y \\ 3y & x\end{pmatrix}\middle|\, x,y\in\mathbb{Z}\right\},+,\cdot\right)$ (+,· sunt adunarea și înmulțirea uzuală pe mulțimile respective) sunt izomorfe.

R. Se arată ușor că tripletele respective sunt domenii de integritate. Aplicația care realizează izomorfismul de inele este $f:\mathcal{A}\to\mathcal{A}'$, $f(x+y\sqrt{3})=\begin{pmatrix} x & y \\ 3y & x\end{pmatrix}$. Avem de verificat că:

1) *f este morfism de inele* și 2) *f este bijectivă.*

Afirmația 1) se traduce prin:

a) $f(z_1+z_2)=f(z_1)+f(z_2), (\forall)z_1,z_2\in\mathcal{A}$,

b) $f(z_1z_2)=f(z_1)\cdot f(z_2), (\forall)z_1,z_2\in\mathcal{A}$.

Verificăm a). Fie $z_1=x_1+y_1\sqrt{3},\ z_2=x_2+y_2\sqrt{3},\ z_1,\ z_2\in\mathcal{A}$. Avem:

$$f(z_1+z_2)=f(x_1+x_2+(y_1+y_2)\sqrt{3})=\begin{pmatrix} x_1+x_2 & y_1+y_2 \\ 3(y_1+y_2) & x_1+x_2\end{pmatrix}=\begin{pmatrix} x_1 & y_1 \\ 3y_1 & x_1\end{pmatrix}+\begin{pmatrix} x_2 & y_2 \\ 3y_2 & x_2\end{pmatrix}=f(z_1)+f(z_2).$$

Verificăm b). Avem: $f(z_1z_2)=f((x_1+y_1\sqrt{3})(x_2+y_2\sqrt{3}))=f(x_1x_2+3y_1y_2+(x_1y_2+x_2y_1)\sqrt{3})=$

$$=\begin{pmatrix} x_1x_2+3y_1y_2 & x_1y_2+x_2y_1 \\ 3(x_1y_2+x_2y_1) & x_1x_2+3y_1y_2\end{pmatrix}=\begin{pmatrix} x_1 & y_1 \\ 3y_1 & x_1\end{pmatrix}\begin{pmatrix} x_2 & y_2 \\ 3y_2 & x_2\end{pmatrix}=f(z_1)f(z_2).$$

Afirmația 2) inseamnă să arătăm că: a') *f* este injectivă și b') *f* este surjectivă.

Probăm a'). Fie $z_1=x_1+y_1\sqrt{3},\ z_2=x_2+y_2\sqrt{3},\ z_1,z_2\in\mathcal{A}$ pentru care $f(z_1)=f(z_2)$.

Să arătăm că $z_1=z_2$. Din $f(z_1)=f(z_2)$ rezultă $\begin{pmatrix} x_1 & y_1 \\ 3y_1 & x_1\end{pmatrix}=\begin{pmatrix} x_2 & y_2 \\ 3y_2 & x_2\end{pmatrix}$, iar de aici $x_1=x_2$ și $y_1=y_2$. Deci $z_1=z_2$.

Verificăm b') Fie $A=\begin{pmatrix} x & y \\ 3y & x\end{pmatrix}\in\mathcal{A}'$. Atunci există $z=x+y\sqrt{3}\in\mathcal{A}$ pentru care $f(z)=A$. Deci *f* este surjectivă. În concluzie *f* este izomorfism de inele.

5. **Fie $\mathcal{C}([0,1])$ mulțimea funcțiilor reale continue pe [0,1] şi $\mathcal{D}([0,1])$ mulțimea funcțiilor reale derivabile pe [0, 1]. Arătați că între inelele $(\mathcal{C}([0,1]),+,\cdot)$ şi $(\mathcal{D}([0,1]),+,\cdot)$, unde $+$ şi $\cdot$ sunt adunarea şi înmulțirea uzuală, nu există nici un izomorfism.**

R. Se verifică cu destulă uşurință că tripletele din enunț sunt inele comutative. Vom demonstra că nu există un izomorfism între cele două inele, prin metoda reducerii la absurd. Presupunem deci că ar exista $F:\mathcal{C}([0,1])\to\mathcal{D}([0,1])$ un astfel de izomorfism. Considerăm $f\in\mathcal{D}([0,1]),\ f(x)=x$. Din F surjectivă se deduce că există $g\in\mathcal{C}([0,1])$ astfel încât $F(g)=f$. Din $g\in\mathcal{C}([0,1])$ rezultă că şi $\sqrt[3]{g}\in\mathcal{C}([0,1])$. Utilizând faptul că F este morfism avem:

$f=F(g)=F\left(\sqrt[3]{g}\sqrt[3]{g}\sqrt[3]{g}\right)=F\left(\sqrt[3]{g}\right)F\left(\sqrt[3]{g}\right)F\left(\sqrt[3]{g}\right)=\left(F\left(\sqrt[3]{g}\right)\right)^3$. De aici $F\left(\sqrt[3]{g}\right)=\sqrt[3]{f}=\sqrt[3]{x}$. Aici am ajuns la o contradicție deoarece $x\to\sqrt[3]{x}$ nu este derivabilă la dreapta în $x=0$. Deci presupunerea făcută este falsă, adică nu există nici un isomorfism între cele două inele.

Observație. Ca şi în cazul grupurilor izomorfe şi pentru inelele izomorfe, o proprietate adevărată pe o structură algebrică se conservă şi pe structura algebrică izomodă. Aici se ştie că există funcții continue pe o mulțime fără a fi derivabile pe acea mulțime (aici într-un punct, $x=0$).

6. **Pe multimea $\mathcal{A}=\mathbb{R}\times\mathbb{R}$ se definesc legile de compozitie $(x,y)+(x',y')=(x+x',\ y+y')$, $(x,y)\cdot(x',y')=(xx',\ xy'+x'y)$, împreună cu care formează un inel comutativ.**

Arătati că acest inel este izomorf cu inelul matricelor $\mathcal{A}'=\left\{\begin{pmatrix} x & y\\ 0 & x\end{pmatrix}\middle|\, x,y\in\mathbb{R}\right\}$ (împreună cu operațiile de adunare şi înmulțire uzuale).

R. Se verifică uşor că tripletele $(\mathcal{A},+,\cdot),(\mathcal{A}',+,\cdot)$ sunt inele.

Verificăm că aplicația $f:\mathcal{A}\to\mathcal{A}',\ f((x,y))=\begin{pmatrix} x & y\\ 0 & x\end{pmatrix}$ este izomorfism. Trebuie să arătăm că:

1) *f este morfism de inele*, 2) *f este bijectivă*.

Pentru 1) se verifică egalitățle

a) $f(z_1+z_2)=f(z_1)+f(z_2),\ (\forall)z_1,z_2\in\mathcal{A}$,

b) $f(z_1\cdot z_2)=f(z_1)\cdot f(z_2),\ (\forall)z_1,z_2\in\mathcal{A}$.

Avem pentru a) (luăm $z_1=(x_1,y_1),\ z_2=(x_2,y_2)$):

$$f(z_1+z_2)=f((x_1,y_1)+(x_2,y_2))=f((x_1+x_2,\ y_1+y_2))=\begin{pmatrix} x_1+x_2 & y_1+y_2\\ 0 & x_1+x_2\end{pmatrix}=\begin{pmatrix} x_1 & y_1\\ 0 & x_1\end{pmatrix}+$$
$$+\begin{pmatrix} x_2 & y_2\\ 0 & x_2\end{pmatrix}=f(z_1)+f(z_2).$$

Analog pentru b) obținem: $f(z_1z_2)=f((x_1x_2,x_1y_2+x_2y_1))=\begin{pmatrix} x_1x_2 & x_1y_2+x_2y_1\\ 0 & x_1x_2\end{pmatrix}=$

$$=\begin{pmatrix} x_1 & y_1\\ 0 & x_1\end{pmatrix}\cdot\begin{pmatrix} x_2 & y_2\\ 0 & x_2\end{pmatrix}=f(z_1)f(z_2).$$

Faptul că *f* este bijectivă se verifică imediat.

7. **Fie $d,e\in\mathbb{Z}$, întregi liberi de pătrate, $d\neq e$. Să se arate că inelele $\left(\mathbb{Z}\left[\sqrt{d}\right],+,\cdot\right),\left(\mathbb{Z}\left[\sqrt{e}\right],+,\cdot\right)$ nu sunt izomorfe.**

R. Vom proceda prin reducere la absurd. Presupunem că ar exista $f:\mathbb{Z}\left[\sqrt{d}\right]\to\mathbb{Z}\left[\sqrt{e}\right]$ un izomorfism de inele (sunt chiar domenii de integritate). Deci $f(0)=0,\ f(1)=1$.

Se arată (vezi construcția endomorfismelor grupului $(\mathbb{Z},+,\cdot)$) că $f(n)=n,(\forall)n\in\mathbb{Z}$. Rămâne să extindem construcția lui *f* şi în puncte de forma $x=a+b\sqrt{d}$, cu $b\neq 0$. Avem:

$f(x)=f\left(a+b\sqrt{d}\right)=f(a)+f(b)f\left(\sqrt{d}\right)=a+bf\left(\sqrt{d}\right)$, ceea ce arată *f* este perfect determinat dacă ştim cine este $f\left(\sqrt{d}\right)$. Notăm $f\left(\sqrt{d}\right)=m+n\sqrt{e}\in\mathbb{Z}\left[\sqrt{e}\right]$. Atunci $d=f(d)=f\left(\sqrt{d}\sqrt{d}\right)=$ $=f\left(\sqrt{d}\right)f\left(\sqrt{d}\right)=\left(m+n\sqrt{e}\right)^2=m^2+n^2e+2mn\sqrt{e}$. De aici $d=m^2+n^2e$ şi $2mn=0$. Dacă $m=0$, atunci din $d=m^2+n^2e$ rezultă $d=en^2$ şi cum *d* este liber de pătrate rezultă $n=1$, adică $d=e$, fals. Dacă $n=0$, atunci $d=m^2$ şi cum *d* este liber de pătrate rezultă $m=\pm 1$, când $d=1$, fals.

Observație. Se arată că inelul $\left(\mathbb{Z}\left[\sqrt{d}\right],+,\cdot\right)$, $d\in\mathbb{Z}$, *d* întreg liber de pătrate este izomorf cu inelul de matrice $\mathcal{A}_d=\left\{\begin{pmatrix} a & b\\ db & a\end{pmatrix}\middle| a,,b\in\mathbb{Z}\right\}$.

Deci dacă $d\neq e, d,e\in\mathbb{Z}$, întregi liberi de pătrate, atunci nici inelele de matrice $\mathcal{A}_d,\mathcal{A}_e$ nu sunt izomorfe.

8. Să se determine endomorfismele inelului $(\mathbb{Z},+,\cdot)$.

R. Fie $f:\mathbb{Z}\to\mathbb{Z}$ un endomorfism al inelului $\mathbb{Z}$. În particular *f* este endomorfism al grupului aditiv $(\mathbb{Z},+)$. Am văzut la morfisme de grupuri (problema 2) rezolvată) că forma lui $f\in\mathrm{End}(\mathbb{Z})$ este $f(n)=na$, unde $f(1)=a\in\mathbb{Z}$. Vom preciza pe $a\in\mathbb{Z}$ din condiția $f(x\cdot y)=f(x)\cdot f(y),(\forall)x,y\in\mathbb{Z}$. Avem

$a=f(1)=f(1\cdot 1)=f(1)f(1)=(f(1))^2=a^2$.

Din $a=a^2$ rezultă $a_1=0, a_2=1$, când avem $f_1(x)=0$ (morfismul nul) şi $f_2(x)=x$ (morfismul identic - care este chiar automorfism al lui $\mathbb{Z}$).

9*. Să se determine automorfismele corpului $(\mathbb{Q}[\sqrt{d}],+,\cdot)$, unde $d\in\mathbb{Z}, d$ întreg liber de pătrate.

R. Fie $f:\mathbb{Q}\left[\sqrt{d}\right]\to\mathbb{Q}\left[\sqrt{d}\right]$ un astfel de izomorfism. Atunci $f(0)=0,\ f(1)=1$. Evident că $f:(\mathbb{Z},+,\cdot)\to(\mathbb{Z},+,\cdot)$ este morfism de inele, adică endomorfism al lui $\mathbb{Z}$. Deci $f(n)=n,(\forall)n\in\mathbb{Z}$.

Vom extinde construcția lui *f* la $\mathbb{Q}_+,\mathbb{Q}_-$ şi apoi la extinderea $\mathbb{Q}\left[\sqrt{d}\right]$.

Mai întâi să observăm că din $f(x+y)=f(x)+f(y),(\forall)x,y\in\mathbb{Q}\left[\sqrt{d}\right]$ rezultă $0=f(0)=$ $=f(x+(-x))=f(x)+f(-x)$, adică $f(-x)=-f(x),(\forall)x\in\mathbb{Q}\left[\sqrt{d}\right]$, ceea ce arată că *f* este impară.

Construcția lui f pe $\mathbb{Q}_+$. Avem:

$$1=f(1)=f\Big(\underbrace{\frac{1}{n}+\frac{1}{n}+\ldots+\frac{1}{n}}_{n\text{ ori}}\Big)=\underbrace{f\left(\frac{1}{n}\right)+\ldots+f\left(\frac{1}{n}\right)}_{n\text{ ori}}=nf\left(\frac{1}{n}\right).$$

De aici $f\left(\frac{1}{n}\right)=\frac{1}{n}$. Acum avem uşor:

$$f\left(\frac{m}{n}\right)=f\underbrace{\left(\frac{1}{n}+...+\frac{1}{n}\right)}_{m \text{ ori}}=mf\left(\frac{1}{n}\right)=m\frac{1}{n}=\frac{m}{n},\ (\forall)m,n\in\mathbb{N},\ n\neq 0.$$

Construcţia lui f pe $\mathbb{Q}_-$. Fie $\frac{m}{n}\in\mathbb{Q}_+$. Atunci (*f* este impară)

$$f\left(-\frac{m}{n}\right)=-f\left(\frac{m}{n}\right)=-\frac{m}{n}.$$

Aşadar am arătat că $f(x)=x,\ (\forall)x\in\mathbb{Q}$.

Construcţia lui f pe $\mathbb{Q}\left[\sqrt{d}\right]$. Pentru $x=a+b\sqrt{d}\in\mathbb{Q}\left[\sqrt{d}\right]$ trebuie să precizăm cine este $f(x)=f(a+b\sqrt{d})=f(a)+f(b\sqrt{d})=f(a)+f(b)f(\sqrt{d})=a+bf(\sqrt{d})$. Deci $f(x)$ este bine determinat dacă ştim cine este $f(\sqrt{d})=\alpha+\beta\sqrt{d}\in\mathbb{Q}\left[\sqrt{d}\right]$.

Avem: $d=f(d)=f(\sqrt{d}\sqrt{d})=f(\sqrt{d})f(\sqrt{d})=(\alpha+\beta\sqrt{d})^2$.

Din această egalitate rezultă sistemul $\begin{cases}\alpha^2+\beta^2 d=d\\ \alpha\beta=0.\end{cases}$

Dacă $\beta=0$ (în a doua ecuaţie), atunci din prima $d=\alpha^2$, fals; dacă $\alpha=0$ atunci $\beta^2=1$, adică $\beta=\pm 1$. Deci pentru $f(\sqrt{d})$, avem două posibilităţi $f(\sqrt{d})=\sqrt{d}$, când $f(a+b\sqrt{d})=a+b\sqrt{d}$ (*automorfismul identic*) şi $f(\sqrt{d})=-\sqrt{d}$, când $f(a+b\sqrt{d})=a-b\sqrt{d}$ (*automorfismul conjugat*).

10*. Să se determine endomorfismele corpului $(\mathbb{R},+,\cdot)$.

R. Din $f(0)=0,\ f(1)=1$ şi faptul că $f:\mathbb{R}\to\mathbb{R}$ este endomorfism de corp (este şi de inel al lui $\mathbb{Q}$) rezultă $f(x)=x,\ (\forall)x\in\mathbb{Q}$ (vezi problema 9 rezolvată mai sus).

Arătăm că *f* este strict crescătoare, observând mai întâi că dacă $x\in\mathbb{R},\ x>0$, există $y\in\mathbb{R}$ astfel incat $y^2=x$ şi de aici $f(x)=f(y^2)=f(y)f(y)=\left(f(y)\right)^2>0$, ceea ce arată că dacă $x>0$, atunci $f(x)>0$. Acum fie $x_1<x_2$, adică $x_2-x_1>0$. Conform observaţiei de mai sus $0<f(x_2-x_1)=f(x_2)-f(x_1)$ sau $f(x_2)>f(x_1)$, adică *f* este strict crescătoare pe $\mathbb{R}$. Arătăm acum că $f=1_{\mathbb{R}}$ (aplicaţia identică a lui $\mathbb{R}$). Presupunem, prin absurd, că $f\neq 1_{\mathbb{R}}$, adică există $x_0\in\mathbb{R}$ astfel încât $f(x_0)\neq x_0$.

Dacă $f(x_0)<x_0$, atunci există $a\in\mathbb{Q}$ astfel încât $f(x_0)<a<x_0$ ($\mathbb{Q}$ este densă în $\mathbb{R}$). De aici a $a=f(a)<f(x_0)$, fals. Analog se tratează cazul $f(x_0)>x_0$.

Prin urmare singurul endomorfism al corpului $(\mathbb{R},+,\cdot)$ este cel identic, $f(x)=x,\ (\forall)x\in\mathbb{R}$.

11*. Să se determine automorfismele corpului numerelor complexe $(\mathbb{C},+,\cdot)$ care invariază numerele reale $\left(f(x)=x,\ (\forall)x\in\mathbb{R}\right)$.

R. Fie $f:\mathbb{C}\to\mathbb{C}$ un astfel de automorfism pentru care $f(x)=x,\ x\in\mathbb{R}$. Aplicaţia *f* este bine determinată dacă ştim cum definim $f(i)$.

Într-adevăr fie $z=x+iy,\ x,y\in\mathbb{R}$. Atunci $f(z)=f(x+iy)=f(x)+f(iy)=f(x)+f(i)f(y)=$ $=x+f(i)y$.

Pentru aceasta să observăm că $-1 = f(-1) = f(i^2) = f(i\cdot i) = f(i)\cdot f(i) = (f(i))^2$. De aici $f(i) = \pm i$.
Aşadar avem doar două astfel de automorfisme $f(x+iy) = x+iy$ (cel *identic*) şi $f(x+iy)=x-iy$ (cel *conjugat*).

12. **Fie $(A,+,\cdot)$ un inel cu element unitate $1\neq 0$ cu proprietatea $x^2=1$ pentru orice $x\in A-\{0\}$. Să se arate că $(A,+,\cdot)$ este corp izomorf cu $\mathbb{Z}_2$ sau $\mathbb{Z}_3$.**

R. Relația $x^2=1$ arată că $x\neq 0$ este inversabil şi $x^{-1}=x$. Deci $(A,+,\cdot)$ este corp. Pe de altă parte să observăm că $(x+1)(x-1) = x^2 - x + x - 1 = 0$. Cum A este corp (n-are divizori ai lui zero) rezultă $x+1=0$ sau $x-1=0$, adică $x\in\{-1,1\}, (\forall)x\neq 0$. Prin urmare $A=\{0,1,-1\}$.
Avem două posibilități:
1) 1 = –1, adică A = {0, 1} şi atunci aplicația $\hat{0}\to\hat{0}, 1\to\hat{1}$ este izomorfismul de la A la $\mathbb{Z}_2$.
2) $1\neq -1$, adică $A=\{0,1,-1\}$ şi aplicația $0\to\hat{0}, 1\to\hat{1}, -1\to\hat{2}$ este izomorfismul de la A la $\mathbb{Z}_3$.

Probleme propuse

1. **1) Arătați că $f:(\mathbb{Z}_6,+,\cdot)\to(\mathbb{Z}_6,+,\cdot), f(\hat{x})=\widehat{4x}$ este morfism de inele şi $\operatorname{Ker} f=\{\hat{0},\hat{3}\}, \operatorname{Im}(f)=\{\hat{0},\hat{2},\hat{4}\}$**

2) Fie $\mathcal{A}=\left\{\begin{pmatrix} a & b\\ b & a\end{pmatrix}\middle| a,b\in\mathbb{Z}\right\}$ cu operațiile uzuale de adunare şi înmulțire. Aplicatia $f:\mathcal{A}\to\mathbb{Z}$, $f\left(\begin{pmatrix} a & b\\ b & a\end{pmatrix}\right)=a-b$ este un morfism de inele. Determinați nucleul morfismului.

3) Arătați că aplicațiile de mai jos sunt morfisme de inele:

a) $S=\left\{\begin{pmatrix} x & y\\ 0 & z\end{pmatrix}\middle| x,y,z\in\mathbb{Z}\right\}$, $f:(S,+,\cdot)\to(\mathbb{Z},+,\cdot)$, $f\begin{pmatrix} x & y\\ 0 & z\end{pmatrix}=z$ şi *f* surjecție;

b) $A=\left\{\begin{pmatrix} x & 0\\ y & 0\end{pmatrix}\middle| x,y\in\mathbb{Z}\right\}$, $f:(A,+,\cdot)\to(\mathbb{Z},+,\cdot)$, $f\begin{pmatrix} x & 0\\ y & 0\end{pmatrix}=x$ şi *f* surjecție;

c) $f:(\mathcal{M}_2(\mathbb{Z}),+,\cdot)\to(\mathcal{M}_2(\mathbb{Z}_2),+,\cdot)$, $f\begin{pmatrix} a & b\\ c & d\end{pmatrix}=\begin{pmatrix} \hat{a} & \hat{b}\\ \hat{c} & \hat{d}\end{pmatrix}$;

d) $A=\left\{\begin{pmatrix} m & 2n\\ n & m\end{pmatrix}\middle| m,n\in\mathbb{Z}\right\}$, $f:(A,+,\cdot)\to(\mathbb{Z}[\sqrt{2}],+,\cdot)$, $f\begin{pmatrix} m & 2n\\ n & m\end{pmatrix}=m+n\sqrt{2}$ şi *f* bijecție.

2. **Se consideră $\mathcal{C}([-1,1])$ inelul funcțiilor continue pe [–1,1] cu valori reale determinat de operațiile de adunare şi înmulțire a funcțiilor. Să se arate că aplicația $F:\mathcal{C}([-1,1])\to\mathbb{R}, F(f)=f\left(\frac{1}{2}\right)$ este morfism. Determinați nucleul morfismului.**

3. **Fie $\mathcal{A}=\mathbb{R}\times\mathbb{R}$. Definim pe A două aplicații:**

$$(a_1,b_1)*(a_2,b_2)=(a_1+a_2,b_1+b_2),\ (a_1,b_1)\circ(a_2,b_2)=(a_1a_2,\ a_1b_2+a_2b_1),$$

împreună cu care devine inel.

Arătați că aplicația $f:\mathcal{A}\to\mathbb{R},\ f\left((a,b)\right)=a$ este morfism surjectiv de inele, dar nu este injectiv.

4. **1) Pe mulțimea $\mathcal{A}=\mathbb{Z}\times\mathbb{Z}$ se definesc aplicațiile: $(a,b)+(c,d)=(a+c,b+d),\ (a,b)\cdot(c,d)=(ac-bd,ad+bc)$ împreună cu care devine inel. Arătati că $\mathcal{A}\simeq\mathbb{Z}[i]$.**

2) Fie $M=\{a,b\}$ şi $(\mathcal{P}(M),\Delta,\cap)$, unde $A\Delta B=(A-B)\cup(B-A)$ şi $(\mathbb{Z}_2\times\mathbb{Z}_2,+,\cdot)$ unde: $(x,y)+(x',y')=(x+x',\ y+y');(x,y)\cdot(x',y')=(xx',\ yy')$. Arătați că $(\mathcal{P}(M),\Delta,\cap)$ şi $(\mathbb{Z}_2\times\mathbb{Z}_2,+,\cdot)$ sunt inele izomorfe. Construiți tablele operațiilor.

3) Fie $A=\{a,b,c\}$ cu operațiile de adunare şi înmulțire date în tabelele:

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\cdot$	a	b	c
a	a	a	a
b	a	c	b
c	a	b	c

Arătați că $(A,+,\cdot)\simeq(\mathbb{Z}_3,+,\cdot)$.

4) Fie $A=\{a,b,c,d\}$ cu operațiile de adunare şi înmulțire date în tabelele:

$+$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	c	a	c
c	a	a	a	a
d	a	c	a	c

şi $A'=\{\hat{0},\ \hat{2},\ \hat{4},\hat{6}\}\subset\mathbb{Z}_8$. Arătați că $(A,+,\cdot)\simeq(A',+,\cdot)$.

5. **Pe mulțimea $\mathbb{Z}$ definim aplicațiile: $x*y=x+y-2,\ x\circ y=xy-2(x+y)+6$, împreună cu care devine domeniu de integritate. Arătați că $(\mathbb{Z},*,\circ)\simeq(\mathbb{Z},+,\cdot)$, unde izomorfismul este dat de $f:\mathbb{Z}\to\mathbb{Z},\ f(x)=\alpha x+\beta$.**

6. **1) Pe $\mathbb{Z}$ se definesc perechile de aplicații:** $\begin{cases}x\oplus y=x+y+1,\\ x\odot y=xy+x+y,\end{cases}\qquad\begin{cases}x*y=x+y-1\\ x\circ y=xy-x-y+2\end{cases}$.

Arătați că inelele $(\mathbb{Z},\oplus,\odot)$, $(\mathbb{Z},*,\circ)$ sunt izomorfe, printr-un izomorfism de forma $f:\mathbb{Z}\to\mathbb{Z},\ f(x)=\alpha x+\beta$.

2) Fie $\mathcal{K}=\left\{\begin{pmatrix}a & b\\ -b & a\end{pmatrix}\middle|\, a,b\in\mathbb{R}\right\}$. Folosind faptul că tripletul $(\mathcal{K},+,\cdot)$ este corp comutativ şi că funcția $f:\mathcal{K}\to\mathbb{C},\ f\left(\begin{pmatrix}a & b\\ -b & a\end{pmatrix}\right)=a+ib$, este izomorfism de corpuri, să se rezolve în $\mathcal{K}$ sistemul:

$X+Y=\begin{pmatrix}1 & 2\\ -2 & 1\end{pmatrix},\ X^3+Y^3=\begin{pmatrix}-2 & 1\\ -1 & -2\end{pmatrix}$ **şi ecuația:** $X^3-\begin{pmatrix}4 & -2\\ 2 & 4\end{pmatrix}X^2+\begin{pmatrix}7 & -10\\ 10 & 7\end{pmatrix}X+\begin{pmatrix}-6 & 12\\ -12 & -6\end{pmatrix}=0$

7. **Arătați că inelele $\mathcal{A}$ şi $\mathcal{A}'$ cu operațiile de adunare şi înmulțire uzuale sunt izomorfe, în cazurile:**

1) $\mathcal{A}=\left\{x+y\sqrt{7}\,\middle|\,x,y\in\mathbb{Z}\right\},\quad \mathcal{A}'=\left\{\begin{pmatrix}x & y\\ 7y & x\end{pmatrix}\middle|\,x,y\in\mathbb{Z}\right\}$;

2) $\mathcal{A}=\left\{x+y\sqrt{5}\,\middle|\,x,y\in\mathbb{Z}\right\}$, $\mathcal{A}'=\left\{\begin{pmatrix} x & -5y \\ -y & x \end{pmatrix}\,\middle|\,x,y\in\mathbb{Z}\right\}$;

3) $\mathcal{A}=\left\{x+y\sqrt{2}\,\middle|\,x,y\in\mathbb{Z}\right\}$, $\mathcal{A}'=\left\{\begin{pmatrix} x+2y & 2y \\ -2y & x-2y \end{pmatrix}\,\middle|\,x,y\in\mathbb{Z}\right\}$;

4) $\mathcal{A}=\left\{x+y\sqrt{3}\,\middle|\,x,y\in 2\mathbb{Z}\right\}$, $\mathcal{A}'=\left\{\begin{pmatrix} x & 3y \\ y & x \end{pmatrix}\,\middle|\,x,y\in 2\mathbb{Z}\right\}$;

5) $\mathcal{A}=\left\{x+iy\,\middle|\,x,y\in\mathbb{Z}\right\}$, $\mathcal{A}'=\left\{\begin{pmatrix} x & -y \\ y & x \end{pmatrix}\,\middle|\,x,y\in\mathbb{Z}\right\}$;

6) $\mathcal{A}=\left\{x+iy\,\middle|\,x,y\in 3\mathbb{Z}\right\}$, $\mathcal{A}'=\left\{\begin{pmatrix} x & -y \\ y & x \end{pmatrix}\,\middle|\,x,y\in 3\mathbb{Z}\right\}$;

7) $\mathcal{A}=\left\{x+y\sqrt{3}i\,\middle|\,x,y\in\mathbb{Z}\right\}$, $\mathcal{A}'=\left\{\begin{pmatrix} x & -3y \\ y & x \end{pmatrix}\,\middle|\,x,y\in\mathbb{Z}\right\}$;

8) $\mathcal{A}=\left\{\dfrac{x+y\sqrt{3}i}{2}\,\middle|\,x,y\in\mathbb{Z},\ x,y \text{ de ceeaşi paritate}\right\}$,

$\mathcal{A}'=\left\{\begin{pmatrix} \dfrac{x}{2} & \dfrac{-3y}{2} \\ \dfrac{y}{2} & \dfrac{x}{2} \end{pmatrix}\,\middle|\,x,y\in\mathbb{Z},\ x,y \text{ de aceeaşi paritate}\right\}$;

9) $\mathcal{A}=\left\{x+y\sqrt{3}i\,\middle|\,x,y\in\mathbb{Q}\right\}$, $\mathcal{A}'=\left\{\begin{pmatrix} x & -3y \\ y & x \end{pmatrix}\,\middle|\,x,y\in\mathbb{Q}\right\}$

10) $\mathcal{A}=\left\{x+y\sqrt{d}\,\middle|\,x,y\in\mathbb{Z}, d\in\mathbb{Z}, d \text{ liber de pătrate}\right\}$, $\mathcal{A}'=\left\{\begin{pmatrix} x & y \\ dy & x \end{pmatrix}\,\middle|\,x,y\in\mathbb{Z}\right\}$;

11) $\mathcal{A}=\left\{A\in\mathcal{M}_3(\mathbb{C})\,\middle|\,AX=XA, (\forall)X\in\mathcal{M}_3(\mathbb{C})\right\}$, $\mathcal{A}'=\mathbb{C}$.

8. Pe mulțimea $\mathcal{A}=\mathbb{Z}\times\mathbb{Z}$ se definesc operațiile „$+$“ şi „$\cdot$“, împreună cu care formează inele în cazurile:

1) $(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_1), (a_1,b_1)\cdot(a_2,b_2)=(a_1a_2, b_1b_2)$;

2) $(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_1), (a_1,b_1)\cdot(a_2,b_2)=(a_1a_2+b_1b_2, a_1b_2+a_2b_1)$;

3) $(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_1), (a_1,b_1)\cdot(a_2,b_2)=(a_1a_2, a_1b_2+a_2b_1)$.

Arătați izomorfismele de inele:

a) $\mathcal{A}(\text{de la 1)})\simeq\left(\mathcal{A}'=\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\,\middle|\,a,b\in\mathbb{Z}\right\},+,\cdot\right)$; b) $\mathcal{A}(\text{de la 2)})\simeq\left(\mathcal{A}'=\left\{\begin{pmatrix} a & b \\ b & a \end{pmatrix}\,\middle|\,a,b\in\mathbb{Z}\right\},+,\cdot\right)$;

c) $\mathcal{A}(\text{de la 3)})\simeq\left(\mathcal{A}'=\left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\,\middle|\,a,b\in\mathbb{Z}\right\},+,\cdot\right)$.

9. a) Arătați că inelul H al cuaternionilor este izomorf cu inelul de matrice $\mathcal{H} = \left\{ \begin{pmatrix} z & u \\ -\overline{u} & \overline{z} \end{pmatrix} \middle| u, z \in \mathbb{C} \right\}$ (cu adunarea și înmulțirea obişnuită a matricelor).

b) Să se arate că mulțimea $\mathbb{C}$ cu operațiile $z_1 \top z_2 = z_1 + z_2,\ z_1 \perp z_2 = z_1 z_2 + \mathrm{Im}(z_1)\mathrm{Im}(z_2)$, este inel izomorf cu inelul matricelor $\mathcal{M} = \left\{ \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \middle| x, y \in \mathbb{R} \right\}$ cu adunarea și înmulțirea uzuală a matricelor prin izomorfismul $f : \mathbb{C} \to \mathcal{M},\ f(x+iy) = \begin{pmatrix} x & y \\ 0 & x \end{pmatrix}$.

10.* Arătați că inelul $\mathcal{H}$ al matricelor de forma $\begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & a & b \end{pmatrix}$, $a, b, c, d \in \mathbb{R}$, este izomorf cu inelul H al cuaternionilor.

11.* Fie A un inel comutativ și $\mathcal{M}$ mulțimea de matrice cu elemente din A.

$$\mathcal{M} = \left\{ M(a,b,c,d) = \begin{pmatrix} a & 0 & b & 0 \\ 0 & a & 0 & b \\ c & 0 & d & 0 \\ 0 & c & 0 & d \end{pmatrix} \middle| a, b, c, d \in A \right\}.$$

Arătați că $\mathcal{M}$ este un inel (în raport cu operațiile de adunare şi înmulțire a matricelor) izomorf cu inelul $\mathcal{M}_2(A)$.

12.* Să se determine morfismele de inele de la $(\mathbb{Z}, +, \cdot)$ la $(\mathbb{Z}_n, +, \cdot)$. Determinați aceste morfisme pentru $n = 6$.

13.* Să se determine morfismele de inele de la $(\mathbb{Z}_n, +, \cdot)$ la $(\mathbb{Z}, +, \cdot)$.

14.* Să se determine endomorfismele inelului $(\mathbb{Z}_n, +, \cdot)$. Determinați aceste endomorfisme pentru $n = 6$.

15.* Să se determine morfismele de inele de la $(\mathbb{Z}_n, +, \cdot)$ la $(\mathbb{Z}_m, +, \cdot)$. Determinați aceste morfisme pentru $n = 4, m = 6$.

16. Pe $A = (0, \infty)$ se definesc aplicațiile $x \oplus y = xy,\ x \odot y = x^{\ln y}$. Arătăți că tripletul $(A, \oplus, \odot)$ este un corp comutativ izomorf cu corpul numerelor reale $\mathbb{R}$, printr-un izomorfism dat de $f : \mathbb{R} \to (0, \infty),\ f(x) = \alpha e^{\beta x}$.

17. Să se arate că aplicațiile $x * y = \sqrt[3]{x^3 + y^3},\ x \circ y = xy$, determină pe $\mathbb{R}$ o structură de corp comutativ, izomorf cu corpul numerelor reale, printr-un izomorfism $f : (\mathbb{R}, +, \cdot) \to (\mathbb{R}, *, \circ)$, $f(x) = \sqrt[3]{\alpha x + \beta}$.

18. Definim pe $\mathbb{R}$ aplicațiile: $x \top y = x + y - 2,\ x * y = 2xy - 4(x+y) + 10$. Arătați că tripletul $(\mathbb{R}, \top, *)$ este un corp izomorf cu $(\mathbb{R}, +, \cdot)$.

19. Să se demonstreze că $x \oplus y = x + y - 7, x \odot y = xy - 7(x + y) + 56$, determină pe $\mathbb{Q}$ o structură de corp comutativ, izomorf cu corpul numerelor raționale $(\mathbb{Q}, +, \cdot)$.

20. Arătați că pe mulțimea $(0,\infty)$ aplicațiile: $x * y = xy, x \circ y = x^{\ln\sqrt[3]{y}}$ determină o structură de corp comutativ, izomorf cu corpul numerelor reale $(\mathbb{R}, +, \cdot)$ printr-un izomorfism de forma $f:\mathbb{R} \to (0,\infty), f(x) = e^{mx} + n$.

21. Pe $\mathbb{R}$ se definesc legile de compoziție: $x \top y = x + y - 1, x * y = 2(xy - x - y) + 3$. Arătați că $(\mathbb{R}, \top, *)$ este corp izomorf cu $(\mathbb{R}, +, \cdot)$ printr-un izomorfism $f:(\mathbb{R}, \top, *) \to (\mathbb{R}, +, \cdot), f(x) = mx + n$.

22. Arătați izomorfismele de corpuri $\mathcal{K}$ și $\mathcal{K}'$ cu operațiile de adunare și înmulțire uzuale, în cazurile:

1) $\mathcal{K} = \mathbb{Q}[\sqrt{3}], \mathcal{K}' = \left\{\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \middle| a,b \in \mathbb{Q}\right\}$; 2) $\mathcal{K} = \mathbb{C}, \mathcal{K}' = \left\{\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \middle| x,y \in \mathbb{R}\right\}$;

3) $\mathcal{K} = \mathbb{Q}[\sqrt{5}], \mathcal{K}' = \left\{\begin{pmatrix} a & 5b \\ b & a \end{pmatrix} \middle| a,b \in \mathbb{Q}\right\}$;

4) $\mathcal{K} = \mathbb{Q}, \mathcal{K}' = \left\{f_a:\mathbb{R} \to \mathbb{R} \middle| f_a(x) = \begin{cases} ax, x \in \mathbb{Q} \\ 0, x \notin \mathbb{Q} \end{cases}, a \in \mathbb{Q}\right\}, (\mathcal{K}', +, \circ)$;

5) $\mathcal{K} = \mathbb{C}, \mathcal{K}' = \left\{\begin{pmatrix} a & b \\ -b & a+b \end{pmatrix} \middle| a,b \in \mathbb{R}\right\}$; 6) $\mathcal{K} = \mathbb{R},\ \mathcal{K}' = \left\{A_x = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & x & x & 0 \\ 0 & x & x & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \middle| x \in \mathbb{R}\right\}$;

7) $\mathcal{K} = \mathbb{R}, \mathcal{K}' = \left\{A_x = \begin{pmatrix} x & x \\ x & x \end{pmatrix} \middle| x \in \mathbb{R}\right\}$.

23. Fie $K = \left\{A_x \in \mathcal{M}_4(\mathbb{R}) \middle| A_x = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & x & x & 0 \\ 0 & x & x & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, x \in \mathbb{R}\right\}$.

a) Să se arate că tripletul $(K, +, \cdot)$ este corp comutativ.

b) Funcția $f:(K, +, \cdot) \to (\mathbb{R}, +, \cdot), f(A_x) = 2x$ este izomorfism de corpuri;

c) Să se calculeze $A_x^n,\ n \in \mathbb{N}$.

24. Fie matricea $A = (a_{ij}) \in \mathcal{M}_n(\mathbb{C})$, unde $a_{ij} = \begin{cases} 1-n, & i = j \\ 1, & i \neq j \end{cases}$ și mulțimea $M = \{zA | z \in \mathbb{C}\}$.

1) Arătați că $(M, +, \cdot) \simeq (\mathbb{C}, +, \cdot)$; 2) Calculați $B^m, B \in M, m \in \mathbb{N}$.

25. (*Teorema de transport de structură*) Fie $f:A \to \mathbb{R}, A \subseteq \mathbb{R}$, o funcție bijectivă și legile de compoziție pe $A, x \perp y = f^{-1}(f(x) + f(y)),\ \ x \top y = f^{-1}(f(x) \cdot f(y)), x,y \in A$. Arătați că $(A, \perp, \top)$ este corp comutativ izomorf cu $(\mathbb{R}, +, \cdot)$.

2.4. INELE DE POLINOAME CU COEFICIENȚI ÎNTR-UN CORP COMUTATIV

1. POLINOAME DE O NEDETERMINANTĂ. FORMA ALGEBRICĂ A UNUI POLINOM. OPERAȚII CU POLINOAME

Paragraful pe care-l prezentăm reprezintă un domeniu important şi bine studiat al algebrei tradiționale. Numeroase probleme de matematică dintre cele mai diverse, sunt enunțate şi rezolvate în termeni de polinoame.

Fie K un corp comutativ (ne interesează cazurile în care K este unul din corpurile $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$, p prim). Vom considera $\mathcal{F}(\mathbb{N}, K)=\{f:\mathbb{N}\to K\}$, mulțimea tuturor funcțiilor definite pe $\mathbb{N}=\{0, 1, 2,..., n, ...\}$cu valori în K. O astfel de funcție se numeşte **şir de elemente** din K. Funcția este bine definită, dacă ştim cum acționează pe fiecare element din $\mathbb{N}$, adică ce înseamnă $f(k)=a_k \in \mathbb{N}, \forall k \in \mathbb{N}$. Am notat acest şir prim mulțimea ordonată $(a_k)_{k\geq 0}$. Deci $f=(a_0, a_1, a_2, ...)$.

Din această mulțime de şiruri $\mathcal{F}(\mathbb{N}, K)$ ne interesează o submulțime $\mathcal{P}$, formată din şirurile $(a_k)_{k\geq 0}$ pentru care termenii lui sunt nuli cu excepția unui număr finit dintre ei. Deci, elementele lui $\mathcal{P}$ au forma $(a_0, a_1, ..., a_n, 0, 0, ...)$, notat $(a_0, a_1, ..., a_n, 0_\infty)$, cu $a_n \neq 0$ şi îl numim polinom cu coeficienți în K, unde a_n (elementul de rang maxim nenul) se numeşte **coeficientul dominant** al polinomului, la care se adaugă elementul $(0, 0, ..., 0, ...)$ (**polinomul nul**).

Pe mulțimea $\mathcal{P}$ a polinoamelor definim două operații algebrice interne şi una externă. Înainte de a trece la operațiile algebrice propriu-zise, pentru polinoame, prezentăm următoarea:

Definiție. (Egalitatea a două polinoame). Fie $f=(a_0, a_1, ..., a_n, 0_\infty)$, $g=(b_0, b_1, ..., b_m, 0_\infty)$ două polinoame. **Polinomul *f* este egal cu polinomul *g*** şi scriem $f=g$ dacă şi numai dacă $a_i=b_i, (\forall) i\geq 0$.

Două polinoame sunt egale dacă ele coincid pe componente.

1) Adunarea polinoamelor

Are loc următoarea:

Definiție. Fie $f=(a_0,a_1,...,a_n,a_\infty)$ și $g=(b_0,b_1,...,b_m,0_\infty)$ două polinoame. Polinomul $f+g=(a_0+b_0,\ a_1+b_1,a_2+b_2,...)$ se numește **suma polinoamelor *f*, *g*.**

Spunem că adunarea polinoamelor se face pe componente.

Operația prin care oricărui cuplu de polinoame (f,g) îi asociem polinomul $f+g$ se numește **adunarea polinoamelor**.

Deci $+:\mathcal{P}\times\mathcal{P}\to\mathcal{P},\ (f,g)\to f+g$.

Observații. 1) $f+g\in\mathcal{P}$ deoarece doar un număr finit de coeficienți sunt nenuli. Pentru $k>\max(n,m)$ avem $a_k=0$.

2) Din definiție se deduce că pentru $K=\mathbb{Z}\left(\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}_p\right)$ pentru $f,g\in\mathcal{P}$ rezultă $f+g$ polinom cu coeficienți întregi (respectiv raționali, reali, complecşi sau clase de resturi modulo *p*).

Exemple. 1. Fie $f=(0,2,i,-1,0_\infty)$, $g=(-i,1+i,0,3,0_\infty)$, $K=\mathbb{C}$. Atunci $f+g=(-i,3+i,i,2,0_\infty)$.

2. Fie $f=\left(\hat{1},\hat{2},\hat{3},\hat{4},\hat{0}_\infty\right)$, $g=\left(\hat{2},\hat{3},\hat{3},\hat{1},\hat{0}_\infty\right)$, $K=\mathbb{Z}_5$. Atunci $f+g=\left(\hat{3},\hat{0},\hat{1},\hat{0}_\infty\right)$.

Proprietățile adunării polinoamelor

Următoarele proprietăți se verifică ușor dacă se ține seama de proprietățile adunării de pe *K* și de egalitatea a două polinoame. Are loc următoarea:

Teoremă. A_1) (Comutativitatea adunării) Adunarea polinoamelor este comutativă, adică $f+g=g+f,\ (\forall)f,g\in\mathcal{P}$.

A_2) (Asociativitatea adunării) Adunarea polinoamelor este asociativă, adică $(f+g)+h=f+(g+h),\ (\forall)f,g,h\in\mathcal{P}$.

A_3) (Elementul neutru) Adunarea polinoamelor admite polinomul nul (0) ca element neutru, adică $0+f=f+0=f,\ (\forall)f\in\mathcal{P}$.

A_4) (Elemente opuse) Orice polinom *f* admite un element opus, notat cu $(-f)$ astfel încât $f+(-f)=(-f)+f=0$.

Observații. 1) Dacă $f=(a_0,a_1,...,a_n,0_\infty)$, atunci $-f=(-a_0,-a_1,...,-a_n,0_\infty)$ ($-f$ se obține din f prin schimbarea semnelor tuturor elementelor nenule din f).

2) Dacă $f,g\in\mathcal{P}$, atunci $f+(-g)$ se notează simplu $f-g$ şi se numeşte **diferența** dintre polinomul f şi polinomul g. Se scad pe componente elementele din f şi g.

3) Mulțimea $\mathcal{P}$ a polinoamelor cu coeficienți în K împreună cu operația de adunare şi proprietățile **A$_1$) – A$_4$)** formează **grup comutativ**.

Exemple. 1. Fie $f=(3,2\sqrt{2},-5,0_\infty)$, $g=(-1,\sqrt{2},0_\infty)$. Atunci $f-g=(4,\sqrt{2},-5,0_\infty)$.

2. Fie $f=(\hat{1},\hat{3},\hat{2},\hat{2},\hat{0}_\infty)$, $g=(\hat{2},\hat{4},\hat{2},\hat{4},\hat{0}_\infty)$, $K=\mathbb{Z}_5$. Atunci $f-g=(\hat{4},\hat{4},\hat{0},\hat{3},\hat{0}_\infty)$.

2) Înmulțirea polinoamelor

Înmulțirea a două polinoame este, sub această formă, mai dificilă.
Are loc următoarea:

Definiție. Fie $f=(a_0,a_1,...,a_n,0_\infty)$, $g=(b_0,b_1,...,b_m,0_\infty)$ două polinoame. Polinomul $f\cdot g=(c_0,c_1,c_2,...,c_k,...,c_{n+m},0_\infty)$, unde:

$c_0=a_0b_0,\ c_1=a_0b_1+a_1b_0,...,c_k=a_0b_k+a_1b_{k-1}+...+a_kb_0,...,c_{n+m}=a_nb_m$,

se numeşte **produsul polinoamelor** f, g.

Operația prin care asociem fiecărui cuplu de polinoame (f,g) polinomul $f\cdot g$ se numeşte **înmulțirea (produsul) polinoamelor.**

Deci $\cdot:\mathcal{P}\times\mathcal{P}\to\mathcal{P},\ (f,g)\to f\cdot g$.

Observații. 1) În loc de $f\cdot g$ vom scrie simplu fg şi $fg\in\mathcal{P}$ deoarece pentru $k>m+n,\ c_k=0$.

2) Să remarcăm că elementele c_k din structura produsului sunt sume de produse de forma a_ib_j cu $i+j=k,\ i,j\in\mathbb{N}$. Deci $c_k=\sum\limits_{i+j=k}a_ib_j=a_0b_k+a_1b_{k-1}+...+a_kb_0$.

Exemple. 1. Fie $f=(-1,i,1-i,3,0_\infty)$, $g=(0,1,-1,i,0_\infty)$, $K=\mathbb{C}$. Atunci:

$c_0=a_0b_0=(-1)\cdot 0=0,\ c_1=a_0b_1+a_1b_0=(-1)\cdot 1+i\cdot(0)=-1,\ c_2=a_0b_2+a_1b_1+a_2b_0=(-1)(-1)+$ $+i\cdot 1+(1-i)\cdot 0=1+i,\ c_3=a_0b_3+a_1b_2+a_2b_1+a_3b_0=(-1)\cdot i+i\cdot 1+(1-i)\cdot 1+3\cdot 0=1-i$, $c_4=a_0b_4+a_1b_3+a_2b_2+a_3b_1+a_4b_0=i,\ c_5=a_0b_5+a_1b_4+...+a_5b_0=i-2,\ c_6=a_0b_6+a_1b_5+...+$ $+a_6b_0=a_3b_3=3i,\ c_k=0,\ k\ge 7$. **Deci** $fg=(0,-1,1+i,1-i,i,i-2,3i,0_\infty)$.

2. Fie $f=\left(\hat{1},\hat{2},\hat{1},\hat{0}_{\infty}\right)$, $g=\left(\hat{3},\hat{4},\hat{0}_{\infty}\right)$, $K=\mathbb{Z}_5$. **Atunci:**

$c_0=a_0b_0=\hat{1}\cdot\hat{3}=\hat{3}$, $c_1=a_0b_1+a_1b_0=\hat{1}\cdot\hat{4}+\hat{2}\cdot\hat{3}=\hat{4}+\hat{1}=\hat{0}$, $c_2=a_0b_2+a_1b_1+a_2b_0=\hat{1}\cdot\hat{0}+$ $+\hat{2}\cdot\hat{4}+\hat{1}\cdot\hat{3}=\hat{3}+\hat{3}=\hat{1}$, $c_3=a_0b_3+...+a_3b_0=\hat{4}$, $c_k=\hat{0}$, $k\geq 4$. **Deci** $fg=\left(\hat{3},\hat{0},\hat{1},\hat{4},\hat{0}_{\infty}\right)$.

Proprietățile înmulțirii polinoamelor

Are loc următoarea:

Teoremă. I$_1$) (**Comutativitatea înmulțirii**) Înmulțirea polinoamelor este comutativă, adică $fg=gf$, $(\forall)f,g\in\mathcal{P}$.

I$_2$) (**Asociativitatea înmulțirii**) Înmulțirea polinoamelor este asociativă, adică $(fg)h=f(gh)$, $(\forall)f,g,h\in\mathcal{P}$.

I$_3$) (**Elementul unitate**) Înmulțirea polinoamelor admite polinomul constant $1=(1,0_{\infty})$ ca element neutru, adică $f\cdot 1=1\cdot f=f$, $(\forall)f\in\mathcal{P}$.

Mulțimea $\mathcal{P}$ a polinoamelor cu coeficienți din K împreună cu înmulțirea și proprietățile **I$_1$) – I$_3$)** formează **monoid comutativ.**
Cele două operații introduse mai sus, adunarea și înmulțirea, sunt legate între ele prin proprietatea de:

Distributivitate. Înmulțirea este distributivă în raport cu adunarea polinoamelor, adică

$$f(g+h)=fg+fh,\ (f+g)h=fh+gh,\ (\forall)f,g,h\in\mathcal{P}.$$

Cu aceste elemente putem formula următoarea:

Teoremă. Mulțimea polinoamelor cu coeficienți în corpul comutativ K, împreună cu operațiile de adunare și înmulțire formează un inel comutativ.

Deci $(\mathcal{P},+,\cdot)$ este inel comutativ.

Observații. 1) Pentru acest caz cu K corp comutativ, inelul polinoamelor este domeniu de integritate.
2) De obicei construcția inelului de polinoame se realizează plecând de la un inel A cu $0\neq 1$.

3) Înmulțirea cu scalari a polinoamelor

Are loc următoarea:

Definiție. Fie $k \in K$ şi polinomul $f = (a_0, a_1, ..., a_n, 0_\infty)$. Produsul dintre scalarul k şi polinomul f este polinomul $k \cdot f = (ka_0, ka_1, ..., ka_n, 0_\infty)$.

A înmulți un polinom cu un scalar înseamnă a-i înmulți toate componentele cu acel scalar.

Operația prin care asociem fiecărui cuplu (k, f) polinomul $k \cdot f$ se numeşte **înmulțirea cu scalari a polinoamelor.**

Deci $\cdot : K \times \mathcal{P} \to \mathcal{P}, (k, f) \to k \cdot f$.

Observații. **1)** Operația definită mai sus se numeşte **lege de compoziție externă** pe mulțimea $\mathcal{P}$ cu domeniul de operatori (scalari) K.
2) În loc de $k \cdot f$ vom scrie kf şi este clar $kf \in \mathcal{P}$.

Exemple. 1. Fie $K = \mathbb{C}, k = 3i, f = (0, i, 1-i, \sqrt{3}, 0_\infty)$. Atunci $3if = (0, -3, 3+3i, 3\sqrt{3}i, 0_\infty)$.

2. Fie $K = \mathbb{Z}_3, k = \hat{2}, f = (\hat{1}, \hat{2}, \hat{0}, \hat{1}, \hat{0}_\infty)$. Atunci $\hat{2}f = (\hat{2}, \hat{1}, \hat{0}, \hat{2}, \hat{0}_\infty)$.

Proprietăți ale înmulțirii polinoamelor cu scalari

Au loc proprietățile date de următoarea:

Teoremă.

S₁) $\lambda(\mu f) = (\lambda\mu) f, (\forall)\lambda, \mu \in K, (\forall) f \in \mathcal{P}$.

S₂) $\lambda(f + g) = \lambda f + \lambda g, (\forall)\lambda \in K, (\forall) f, g \in \mathcal{P}$.

S₃) $(\lambda + \mu) f = \lambda f + \mu f, (\forall)\lambda, \mu \in K, (\forall) f \in \mathcal{P}$.

S₄) $1f = f, 1 \in K, (\forall) f \in \mathcal{P}$.

Verificarea proprietăților este imediată (se apelează la asociativitatea înmulțirii de pe K, a distributivității înmulțirii în raport cu adunarea de pe K, a egalității a două polinoame).
Mulțimea $\mathcal{P}$ împreună cu adunarea polinoamelor şi înmulțirea polinoamelor cu scalari şi proprietățile **A₁) – A₄)**, **S₁) –S₄)** formează ceea ce se cheamă un **spațiu vectorial peste** K, numit **spațiul vectorial al polinoamelor peste corpul** K.

2. FORMA ALGEBRICĂ A UNUI POLINOM

Să observăm că polinoamele de forma $(a,0_\infty)$, $a \in K$ se adună şi se înmulţesc în acelaşi mod ca elementele lui *K*. Într-adevăr avem: $(a,0_\infty)+(b,0_\infty)=(a+b,\, 0_\infty)$, $(a,0_\infty)\cdot(b,0_\infty)=(ab,0_\infty)$.

Aceasta ne permite să identificăm (modulo *un* izomorfism) astfel de polinoame cu elementele corespunzătoare din *K*, adică $(a,0_\infty)=a,\ (\forall)a \in K$.

Desemnăm elementul $(0,1,0_\infty)=X$ şi numim *X* **nedeterminata** pe *K*. Utilizând operaţia de înmulţire din $\mathcal{P}$ rezultă:

$$X=(0,1,0_\infty),\ X^2=(0,0,1,0_\infty),\ X^3=(0,0,0,1,0_\infty),\dots,\ X^n=(\underbrace{0,0,\dots,0}_{n},1,0_\infty).$$

De asemenea pentru $a \in K$ avem: $(\underbrace{0,0,\dots,0}_{n},a,0_\infty)=aX^n=X^n a$.

Cu aceste observaţii polinomul $f=(a_0,a_1,a_2,\dots,a_n,0_\infty)$ se scrie succesiv:

$$f=(a_0,0_\infty)+(0,a_1,0_\infty)+(0,0,a_2,0_\infty)+\dots+(\underbrace{0,0,\dots,0}_{n},a_n,0_\infty)=$$

$$=a_0+a_1(0,1,0_\infty)+a_2(0,0,1,0_\infty)+\dots+a_n(0,0,\dots,0,1,0_\infty)=$$

$$=a_0+a_1X+a_2X^2+\dots+a_nX^n.$$

Am obţinut următoarea:

Definiţie. Scrierea polinomului *f*

$$f=a_0+a_1X+a_2X^2+..+a_nX^n=\sum_{i=0}^{n} a_iX^i \text{, unde } X^0=1,$$

reprezintă **forma algebrică a lui** *f*, ordonat după puterile crescătoarea ale nedeterminatei *X*.

Mulţimea polinoamelor de nedeterminată *X* cu coeficienţi în *K* se notează $K[X]$.

Polinoamele de forma $f=a_0, a_0 \in K$ se numesc **polinoame constante.**

Polinomul $f=0$ se numeşte **polinomul nul.**

Uneori vom folosi pentru *f* scrierea (numită de asemenea, forma algebrică):

$$f = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0,$$

unde am ordonat polinomul după puterile descrescătoare ale lui *X*.

Observații. **1)** Elementele $a_0, a_1, ..., a_n \in K$ se numesc **coeficienții polinomului**, iar monoamele $a_k X^k$, $k = \overline{0,n}$ se numesc **termenii polinomului**.

Dacă $a_k = 0$, atunci termenul $0 \cdot X^k$ nu se mai scrie ($f = 2 - 3X + X^3$, aici $a_2 = 0$), iar dacă $a_k = 1$, atunci în loc de $1 \cdot X^k$ se scrie simplu X^k.

2) Dacă $a_0 = 0,\ a_1 = 1,\ a_2 = ... = a_n = 0$, atunci $f = X$ reprezintă un polinom.

3) Inelul $K[X]$ conține, atât pe *K* (polinoamele constante) cât şi pe *X*. Inelul $K[X]$ este „cel mai mic“ inel care conține pe *K* şi pe *X*, în sensul că orice inel care conține pe *K* şi *X* trebuie să conțină toate polinoamele $a_0 + a_1 X + ... + a_n X^n$.

4) În forma algebrică a unui polinom simbolurile $X, X^2, X^3, ...$ pot fi privite ca „etichete“ pentru pozițiile coeficienților.

5) Se impune să avem grijă în a nu considera litera *X* ca reprezentând un element variabil din *K*; litera *X* desemnează un **polinom particular** (obs. **2**)). Ideea că *X* reprezintă un element variabil din *K* provine din confuzia ce se face între un polinom cu coeficienți în *K* şi funcția polinomială definită pe *K* cu valori în *K*, ataşată polinomului respectiv (despre care vorbim mai jos).

6) Pentru $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p,\ p \text{ prim}\}$ se obțin mulțimile de polinoame:

$\mathbb{Q}[X]$ = mulțimea polinoamelor de nedeterminată *X* cu coeficienți în $\mathbb{Q}$ (sau peste $\mathbb{Q}$),

$\mathbb{R}[X]$ = mulțimea polinoamelor de nedeterminată *X* cu coeficienți în $\mathbb{R}$ (sau peste $\mathbb{R}$),

$\mathbb{C}[X]$ = mulțimea polinoamelor de nedeterminată *X* cu coeficienți în $\mathbb{C}$ (sau peste $\mathbb{C}$),

$\mathbb{Z}_p[X]$ = mulțimea polinoamelor de nedeterminată *X* cu coeficienți în $\mathbb{Z}_p$ (sau peste $\mathbb{Z}_p$),

Au loc incluziunile: $\mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X]$.

Exemple. $f_1 = \frac{1}{2} - 3X + \frac{3}{5}X^3 \in \mathbb{Q}[X]$, $f_2 = 1 + \sqrt{2}X - \frac{1}{3}X^2 \in \mathbb{R}[X]$,

$f_3 = 1 + i - 2X^2 + iX^3 - (1-i)X^4 \in \mathbb{C}[X]$, $f_4 = \hat{1} + \hat{2}X^2 + \hat{3}X^4 \in \mathbb{Z}_5[X]$, $f_5 = -1 + 3X^2 - 5X^3 \in \mathbb{Z}[X]$.

3. OPERAȚIILE CU POLINOAME SCRISE SUB FORMĂ ALGEBRICĂ

Reformulăm operațiile cu polinoame descrise mai sus, ținând seama de forma algebrică a acestora, în următoarea:

Teoremă. Fie $f, g \in K[X]$, $f = a_0 + a_1X + a_2X^2 + ... + a_nX^n$,

$$g = b_0 + b_1X + b_2X^2 + ... + b_mX^m.$$

1) (Egalitatea a două polinoame) Polinomul *f* **este egal cu polinomul** g şi scriem $f = g \Leftrightarrow a_i = b_i, (\forall) i \geq 0$. În particular $f = 0 \Leftrightarrow a_i = 0, (\forall) i \geq 0$.

Două polinoame sunt egale dacă coeficienții termenilor care conțin pe X **la aceleaşi puteri sunt egali.**

În particular, un polinom este nul dacă toți coeficienții săi sunt nuli.

2) (Adunarea a două polinoame) Suma polinomului *f* **cu polinomul** g este polinomul notat $f + g$ şi egal cu:

$$f + g = (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + ... \overset{\text{notație}}{=} \sum_{i \geq 0} (a_i + b_i)X^i.$$

Adunarea polinoamelor se face adunând între ei termenii asemenea (cu puteri egale ale lui X**).**

3) (Înmulțirea a două polinoame) Produsul polinomului *f* **cu polinomul** g este polinomul notat $f \cdot g$, sau simplu fg şi egal cu:

$$fg = a_0b_0 + (a_1b_0 + a_0b_1)X + (a_ob_2 + a_1b_1 + a_2b_0)X^2 + ...$$

Înmulțirea a două polinoame se face înmulțind fiecare termen din primul polinom cu fiecare termen din al doilea polinom, după care se adună termenii asemenea.

4) (Înmulțirea cu scalari a polinoamelor) Produsul dintre scalarul $k \in K$ **şi polinomul** *f* este polinomul kf egal cu:

$$kf = ka_0 + ka_1X + ... + ka_nX^n.$$

A înmulți un scalar cu un polinom înseamnă a înmulți fiecare termen al polinomului cu acel scalar.

În fine, mulțimea $K[X]$ înzestrată cu operațiile de adunare şi înmulțire a polinoamelor are o structură algebrică precizată de următoarea:

Teoremă. Tripletul $(K[X], +, \cdot)$ este inel comutativ numit **inelul polinoamelor de nedeterminată** X **cu coeficienți în corpul** K (sau simplu **inelul polinoamelor peste corpul** K).

Demonstrație. Se verifică ușor axiomele inelului comutativ.
Elementul nul al inelului $K[X]$ este polinomul nul $0(0 \in K)$, iar **elementul unitate** este polinomul constant $1(1 \in K)$.■
Să observăm că avem $K \subset K[X]$ și $(K, +, \cdot)$ este un subinel al lui $(K[X], +, \cdot)$.

Probleme rezolvate

1. Să se determine parametrii reali *a, b, c, d* astfel încât polinomul: $f = (a-1)X^3 + 2bX^2 + (c-2)X + 3d + 1$ să fie egal cu polinomul $g = (X-1)(X+2)(X-3)$.

R. Se aduce polinomul g la forma $g = X^3 - 2X^2 - 5X + 6$.

Deci $f = g \Leftrightarrow \begin{array}{l|l} X^3 & a-1=1 \\ X^2 & 2b=-2 \\ X & c-2=-5 \\ X^0 & 3d+1=6 \end{array}$ (am identificat coeficienții lui X^3, X^2, X, X^0 din cele două polinoame).

De aici găsim $a = 2, b = -1, c = -3, d = \frac{5}{3}$.

2. Se consideră polinoamele $f, g \in \mathbb{R}[X]$, $f = X^3 - 3X^2 + 2X - 5$, $g = a + b(X+1) + c(X+1)^2 + d(X+1)^3$. Să se determine $a, b, c, d \in \mathbb{R}$ pentru care $f = g$.

R. Se scrie g sub forma (ordonăm după puterile descrescătoare ale lui X):

$$g = dX^3 + (c+3d)X^2 + (b+2c+3d)X + a+b+c+d$$

Din condiția $f = g$ rezultă sistemul: $\begin{array}{l|l} X^3 & 1=d \\ X^2 & -3=c+3d \\ X & 2=b+2c+3d \\ X^0 & -5=a+b+c+d \end{array}$ cu soluția $a=-11, b=11, c=-6, d=1$.

3. Să se calculeze $f+g$ și $f \cdot g$ în cazurile:

a) $f = 1 + X + X^2, g = 1 - X$; b) $f = 1 - X + X^2, g = 1 + X$;

c) $f = iX + (1-i)X^2, g = 1 + i - iX + 2iX^2$; d) $f = \hat{3} + \hat{2}X, g = X^2 + \hat{4}X, f, g \in \mathbb{Z}_5[X]$

R. a) Pentru $f+g$ avem: $f+g = 2 + X^2$, iar pentru a calcula $f \cdot g$ aplicăm distributivitatea înmulțirii în raport cu operația de adunare și avem:

$$f \cdot g = (1+X+X^2)(1-X) = (1+X+X^2)\cdot 1 - (1+X+X^2)X = 1+X+X^2-X-X^2-X^3 =$$
$$= 1 - X^3.$$

b) Avem: $f+g = 2+X^2$ și $f \cdot g = 1-X+X^2+(1-X+X^2)X = 1-X+X^2+X-X^2+X^3 = 1+X^3$.

c) $f+g=1+i+(1+i)X^2$ şi $f\cdot g=\left[iX+(1-i)X^2\right](1+i)+\left[iX+(1-i)X^2\right](-iX)+$

$+\left[iX+(1-i)X^2\right]2iX^2=(i-1)X+2X^2+X^2+(-i-1)X^3-2X^3+(2i+2)X^4=(i-1)X+$

$+3X^2+(-3-i)X^3+(2i+2)X^4$.

d) $f+g=\hat{3}+X+X^2$, $f\cdot g=\hat{2}X+X^2+\hat{2}X^3$, $f+g,\ fg\in\mathbb{Z}_5[X]$.

4. GRADUL UNUI POLINOM

Fie polinomul $f=a_0+a_1X+...+a_nX^n\in K[X]$. Are loc următoarea:

Definiție. Se numeşte **gradul polinomului** $f\neq 0$, notat grad (*f*) , cel mai mare număr natural *n* cu proprietatea $a_n\neq 0$.
Dacă $f=0$, atunci $\text{grad}(f)=-\infty$.

Deci, $\text{grad}:K[X]\to\mathbb{N}\cup\{-\infty\}$, unde

$$-\infty+n=-\infty,\ (\forall)n\in\mathbb{N},\ -\infty-\infty=-\infty$$

$$\text{grad}(f)=\begin{cases}\max\{i\,|\,a_i\neq 0\},\ f\neq 0\\ -\infty,\ f=0.\end{cases}$$

Să observăm că gradul unui polinom este dat de cel mai mare exponent al nedeterminatei *X*, al cărei coeficient este nenul. În particular, gradul unui polinom constant nenul este zero.

Dacă $\text{grad}(f)=n$, atunci $f=a_0+a_1X+...+a_nX^n,\ a_n\neq 0$. Termenul a_0 se numeşte **termenul liber** al polinomului *f*, iar coeficientul $a_n\neq 0$ se numeşte **coeficientul dominant** al polinomului *f*. Polinoamele $f\in K$ se numesc **polinoame constante**. Din definiție rezultă că **elementele nenule ale lui** *K* sunt polinoame de grad zero.

Exemple. 1. Polinomul $f=-3-\frac{4}{5}X^3+5X\in\mathbb{Q}[X]$ îl scriem $f=-3+5X-\frac{4}{5}X^3$ şi deci $\text{grad}(f)=3$. Termenul liber este $a_0=-3$ şi coeficientul dominant este egal cu $-\frac{4}{5}$. Termenul care îl conține pe X^2 lipsind, are coeficientul zero.

2. Polinomul $g=\sqrt{3}-5X^2+2X^4\in\mathbb{R}[X]$ are gradul egal cu 4 şi coeficientul dominant egal cu 2. Termenul liber este $\sqrt{3}$. Termenii care conțin pe *X* şi X^3 are coeficienții zero.

3. Polinomul $f=-3$ are $\text{grad}(f)=0$.

4. **Polinomul** $f = 1 + 2X - (m+1)X^2 + (m^2 - 1)X^3 \in \mathbb{R}[X]$ **are** $\mathrm{grad}(f) = 3$ **dacă** $m \neq \pm 1$; $\mathrm{grad}(f) = 1$ **dacă** $m = -1$ **când** $f = 1 + 2X$; $\mathrm{grad}(f) = 2$ **dacă** $m = 1$ **când** $f = 1 + 2X - 2X^2$.

Proprietăți ale gradului

Gradul fiind o funcție pe mulțimea polinoamelor (nenule) este interesant de văzut comportarea ei față de operațiile cu polinoame. Formulăm următoarea:

Teoremă. Fie $f, g \in K[X]$. Avem:

1) $\mathrm{grad}(f+g) \leq \max(\mathrm{grad}(f), \mathrm{grad}(g))$.

Gradul sumei a două polinoame este cel mult maximul dintre gradele celor două polinoame.

2) $\mathrm{grad}(fg) = \mathrm{grad}(f) + \mathrm{grad}(g)$.

Gradul produsului a două polinoame este egal cu suma gradelor celor două polinoame.

Demonstrație. Fie $f = a_0 + a_1X + ... + a_nX^n$, $a_n \neq 0$, $g = b_0 + b_1X + ... + b_mX^m$, $b_m \neq 0$.

1) Dacă $n > m$, atunci $\mathrm{grad}(f+g) = n$, deoarece a_nX^n este termenul de grad cel mai mare din $f+g$. Deci $\mathrm{grad}(f+g) = \mathrm{grad}(f)$.

Dacă $m = n$, atunci $(a_n + b_n)X^n$ este termenul de grad cel mai mare dacă $a_n + b_n \neq 0$ și deci $\mathrm{grad}(f+g) = n = \mathrm{grad}(f)$, iar dacă $a_n + b_n = 0$, atunci $\mathrm{grad}(f+g) < n = \mathrm{grad}(f) = \mathrm{grad}(g)$.
Cazul $m > n$ este analog cazului $n > m$.

2) Pentru $f \cdot g$ termenul de grad maxim este $a_nb_mX^{n+m}$, $a_nb_m \neq 0$, deoarece $a_n \neq 0$, $b_m \neq 0$ și K este inel fără divizori ai lui zero.
Deci $\mathrm{grad}(f \cdot g) = n + m = \mathrm{grad}(f) + \mathrm{grad}(g)$. ■

Corolar. Inelul $(K[X], +, \cdot)$ este un domeniu de integritate.

Deci, $[f \neq 0,\ g \neq 0,\ f, g \in K[X] \Rightarrow f \cdot g \neq 0] \Leftrightarrow [fg = 0 \Rightarrow f = 0 \text{ sau } g = 0]$.

Demonstrație. Din $f \neq 0,\ g \neq 0$ rezultă $\mathrm{grad}(f) \geq 0,\ \mathrm{grad}(g) \geq 0$, iar din teorema (**2**)) se deduce $\mathrm{grad}(fg) = \mathrm{grad}(f) + \mathrm{grad}(g) \geq 0$. De aici $fg \neq 0$. ■

Aplicație (Elemente inversabile din $K[X]$). Un polinom $f \in K[X]$ **este inversabil** dacă şi numai dacă există $g \in K[X]$ astfel încât $fg = 1$.

Să arătăm că $U\left(K[X]\right) = K^* = K - \{0\}$.

Este clar că avem $K^* \subset U\left(K[X]\right)$, (1). Reciproc, fie $f \in U\left(K[X]\right)$. Deci există $g \in K[X]$ astfel încât $fg = 1$. Trecând în această egalitate la grad obținem $\text{grad}(f) + \text{grad}(g) = 0$, iar de aici $\text{grad}(f) = \text{grad}(g) = 0 \Rightarrow f \in K^*$. Prin urmare $U\left(K[X]\right) \subset K^*$, (2).

Din (1) şi (2) rezultă $U\left(K[X]\right) = K^*$.

5. EVALUAREA POLINOAMELOR. FUNCȚIA POLINOMIALĂ. RĂDĂCINI ALE UNUI POLINOM

Fie $f \in K\left[X\right]$, $f = a_0 + a_1 X + ... + a_n X^n$ şi $\alpha \in K$. Atunci formulăm următoarele:

Definiții. 1) Se numeşte **valoarea polinomului** f în α elementul:

$$f(\alpha) = a_0 + a_1\alpha + ... + a_n\alpha^n .$$

$f(\alpha)$ se obține din f **înlocuind nedeterminata** X **cu** α.

A calcula $f(\alpha)$ înseamnă **a evalua** polinomul f în α.

2) Elementul α **este o rădăcină a polinomului** f dacă $f(\alpha) = 0$.

Evaluarea sumei şi produsului a două polinoame este dată de următoarea:

Teoremă. Fie $f, g \in K\left[X\right]$ şi $\alpha \in K$. Atunci

1) $(f+g)(\alpha) = f(\alpha) + f(\alpha)$.

Valoarea sumei este egală cu suma valorilor.

2) $(fg)(\alpha) = f(\alpha)g(\alpha)$.

Valoarea produsului este egală cu produsul valorilor.

Pentru calculul valorii polinomului $f = a_n X^n + a_{n-1} X^{n1} + ... + a_1 X + a_0$ în α se utilizează scrierea $f(\alpha) = a_o + \alpha\left[a_1 + \alpha(a_2 + ... + a_n\alpha^{n-2})\right]$, evitându-se astfel ridicările la putere ale lui α.

Exemplu. Fie polinomul $f = 5X^3 + 2X^2 - 3X + 1$. Aducem polinomul la forma $f = X\left(5X^2 + 2X - 3\right) + 1$ sau $f = X\left[X(5X+2) - 3\right] + 1$ şi deci $f(3) = 3\left[3(5\cdot 3 + 2) - 3\right] + 1 = 145$.

Calculele pot fi aranjate ca în schema de mai jos (utilizând coeficienţii termenilor polinomului şi adunând numerele din fiecare coloană). Se coboară coeficientul dominant în linia 3.

	X^3	X^2	X	X^0	
	5	2	– 3	1	**Coeficienţii polinomului *f***
3	↓	$\times 3 = 15$ $\downarrow +$	$\times 3 = 51$ $\downarrow +$	$\times 3 = 144$ $\downarrow +$	**Coeficienţii din următoarea linie înmulţiţi cu 3**
	5	15 + 2 = 17 ①	51 – 3 = 48 ②	144 + 1 = 145 ③ = *f*(3)	**Valoarea parantezelor**

$$f(3) = 3[3(\underbrace{5\cdot 3 + 2}_{①}) - 3] + 1 = 3(\underbrace{17\cdot 3 - 3}_{②}) + 1 = \underbrace{3\cdot 48 + 1}_{③} = 145$$

Urmăriţi cum se corespund parantezele din schemă cu cele din *f* (3). Ele sunt marcate cu acelaşi număr închis într-un cerculeţ.
În final aranjarea calculelor se face pe două linii:

	X^3	X^2	X	X^0
	5	2	– 3	1
3	5	$3\cdot 5 + 2 = 17$	$3\cdot 17 - 3 = 48$	$3\cdot 38 + 1 = 145 = f(3)$

Schema descrisă mai sus se numeşte *schema lui Horner*.

Fie $f \in K[X]$ şi $\alpha \in K$. Atunci $f(\alpha) \in K$. Am pus astfel în evidenţă funcţia $\overline{f} : K \to K$, $\overline{f}(\alpha) = f(\alpha)$, $(\forall)\alpha \in K$. Are loc următoarea:

> **Definiţie.** Funcţia $\overline{f} : K \to K$, $\overline{f}(\alpha) = f(\alpha)$, $(\forall)\alpha \in K$ se numeşte **funcţia polinomială asociată polinomului** *f* sau simplu **funcţia polinomială.**

Se vede că un polinom *f* şi funcţia polinomială sunt noţiuni distincte. Ele **nu se confundă.** Fiecare polinom $f \in K[X]$ defineşte o funcţie polinomială. De exemplu, polinomul $f = X$ defineşte funcţia $\overline{f} : K \to K$, $\overline{f}(x) = x$, $(\forall)x \in K$, motiv pentru care se confundă uneori argumentul $x \in K$ cu polinomul X. În descrierea polinomului *f* apare **litera mare** *X*, **care desemnează necunoscuta**, iar în descrierea funcţiei *f* apare **litera mică** *x* **care precizează argumentul funcţiei** *f*. De aceea vom nota funcţia asociată tot cu *f*.

Reamintim că în anii precedenţi de liceu am introdus noţiunea de funcţie polinomială plecând de la cea de polinom, gândit ca o sumă finită de monoame de forma $a_k X^k$, aşa cum se poate vedea din tabelul de mai jos.

Polinomul f	Funcția polinomială asociată $f:\mathbb{R}\to\mathbb{R}$	Ecuația asociată
$aX+b$, $a,b\in\mathbb{R}$, $a\neq 0$	Funcția de gradul întâi $f(x)=ax+b$	Ecuația de gradul întâi $ax+b=0$
aX^2+bX+c, $a,b,c\in\mathbb{R}$, $a\neq 0$	Funcția de gradul doi $f(x)=ax^2+bx+c$	Ecuația de gradul doi $ax^2+bx+c=0$
aX^3+bX^2+cX+d, $a,b,c,d\in\mathbb{R}$, $a\neq 0$	Funcția cubică $f(x)=ax^3+bx^2+cx+d$	Ecuația de gradul trei $ax^3+bx^2+cx+d=0$
X = **nedeterminată**	x = **variabilă**	x = **necunoscută**

Gradul polinomului dă gradul funcției polinomiale. Coeficienții polinomului sunt coeficienții funcției polinomiale. **A determina funcția polinomială înseamnă a-i preciza coeficienții.** Dacă $\alpha\in K$ este rădăcină a polinomului *f*, atunci α **se numeşte zero al funcției polinomiale** $f:K\to K$.

Întotdeauna pentru un polinom $f\in K[X]$ trebuie precizată mulțimea în care se determină rădăcinile. Polinomul $f=2X+1\in\mathbb{Z}[X]$ nu are rădăcini în $\mathbb{Z}$, dar are rădăcina $x_0=-\dfrac{1}{2}\in\mathbb{Q}$; polinomul $g=X^2-2\in\mathbb{Q}[X]$ nu are rădăcini în $\mathbb{Q}$, dar are rădăcinile $\pm\sqrt{2}$ în $\mathbb{R}$.

Printre altele vom vedea când un polinom $f\in A[X]$ are rădăcini în *A*. În acest context $A=\mathbb{C}$ joacă un rol deosebit deoarece: **orice polinom** $f\in\mathbb{C}[X]$ **de gradul** n **are** n **rădăcini în** $\mathbb{C}$.

Definiție. Fie $K\in\{\mathbb{Q},\mathbb{R},\mathbb{C}\}$. Un număr $x_0\in\mathbb{C}$ se numeşte **algebric peste** *K* dacă există un polinom nenul $f\in K[X]$ pentru care $f(x_0)=0$. În caz contrar se spune că x_0 este **transcendent** peste *K*.

Din definiție se deduce că orice număr complex este sau algebric sau transcendent.

Exemple. 1. **Orice număr rațional** $\dfrac{m}{n}\in\mathbb{Q}, m,n\in\mathbb{Z}, n\neq 0$ **este algebric peste** $\mathbb{Z}$**, deoarece există polinomul** $f=nX-m\in\mathbb{Z}[X]$ **pentru care** $f\left(\dfrac{m}{n}\right)=0$.

2. **Numărul** $\sqrt{p}\in\mathbb{R}\text{-}\mathbb{Q}$, p **– prim este algebric peste** $\mathbb{Z}$ **deoarece există polinomul** $f=X^2-p\in\mathbb{Z}[X]$ **pentru care** $f(\sqrt{p})=0$.

3. Numărul $i \in \mathbb{C}$ este algebric peste $\mathbb{R}$ deoarece există polinomul $f = X^2 + 1 \in \mathbb{R}[X]$ pentru care $f(i) = 0$.

4. Numerele π, e sunt transcendente peste $\mathbb{Q}$.

Legat de rădăcinile unui polinom prezentăm următoarea:

> **Teoremă.** Fie $f \in K[X]$ un polinom de grad cel mult n. Dacă corpul K are cel puțin $n+1$ elemente şi f are cel puțin $n+1$ rădăcini distincte în K, atunci f este polinomul nul.

Probleme rezolvate

1. Se consideră polinoamele $f = 1 - 3X^2 + 2X^3 \in \mathbb{Q}[X]$ şi $g = 1 - \sqrt{3}X + 5X^3 \in \mathbb{R}[X]$.

a) Calculați $f\left(1-\sqrt{3}\right)$, $f\left(1+\sqrt{3}\right)$ şi observați legătura între cele două valori. Generalizați.

b) Calculați $g(1-i)$, $g(i+1)$ şi observați legătura între cele două valori. Generalizați.

R. a) Avem: $f\left(1-\sqrt{3}\right) = 1 - 3\left(1-\sqrt{3}\right)^2 + 2\left(1-\sqrt{3}\right)^3 = 1 - 3\left(1 - 2\sqrt{3} + 3\right) + 2\left(1 - 3\sqrt{3} + 9 - 3\sqrt{3}\right) = 9 - 6\sqrt{3}$.

$f\left(1+\sqrt{3}\right) = 1 - 3\left(1+\sqrt{3}\right)^2 + 2\left(1+\sqrt{3}\right)^3 = 1 - 3\left(1 + 2\sqrt{3} + 3\right) + 2\left(1 + 3\sqrt{3} + 9 + 3\sqrt{3}\right) = 9 + 6\sqrt{3}$.

Un număr de forma $a + b\sqrt{p}$, $a, b \in \mathbb{Q}$, $p \in N$, p prim, se numeşte număr pătratic. Numărul $a - b\sqrt{p}$ se numeşte conjugatul pătratic al numărului $a + b\sqrt{p}$. De remarcat că numerele $a \pm b\sqrt{p} \notin \mathbb{Q}$ dacă $b \neq 0$.

Polinomul dat f are însă coeficienții din $\mathbb{Q}$.

Deci, dacă un polinom are coeficienții raționali şi calculăm valorile lui în două puncte conjugat pătratice de forma $a \pm b\sqrt{p}$, atunci valorile obținute sunt de asemenea numere conjugat pătratice de forma $A \pm B\sqrt{p}$, unde $A, B \in \mathbb{Q}$.

Mai precis dacă $f\left(a + b\sqrt{p}\right) = A + B\sqrt{p}$, atunci $f\left(a - b\sqrt{p}\right) = A - B\sqrt{p}$. Este uşor de văzut că utilizând dezvoltarea binomului lui Newton avem: $\left(a + b\sqrt{p}\right)^n = X + Y\sqrt{p}$, $X, Y \in \mathbb{Q}$ şi $\left(a - b\sqrt{p}\right)^n = X - Y\sqrt{p}$, iar de aici rezultatul anunțat mai sus este foarte simplu.

b) Avem: $g(1-i) = 1 - \sqrt{3}(1-i) + 5(1-i)^3 = 1 - \sqrt{3}(1-i) + 5(1 - 3i - 3 + i) = -9 - \sqrt{3} + (-10 + \sqrt{3})i$ şi

$g(1+i) = 1 - \sqrt{3}(1+i) + 5(1+i)^3 = 1 - \sqrt{3}(1+i) + 5(1 + 3i - 3 - i) = -9 - \sqrt{3} - (-10 + \sqrt{3})i$.

Am calculat valoarea polinomului cu coeficienți reali g în punctele $1-i, 1+i$ care sunt complex conjugate. Valorile obținute în aceste puncte $g(1-i), g(1+i)$ sunt de asemenea numere complex conjugate.

Mai general dacă $g \in \mathbb{R}[X]$ şi $z = a+bi, b \neq 0, a,b \in \mathbb{R}$ atunci $g(a+bi) = A+Bi, A,B \in \mathbb{R}$ iar $g(a-bi) = \overline{g(a+bi)} = \overline{A+Bi} = A-Bi$ (am utilizat proprietățile conjugatului unui număr complex pentru sumă şi produs (putere)).

2. Să se determine funcția de gradul al doilea $f : \mathbb{R} \to \mathbb{R}$ dacă $f(-1)=1, f(0)=0, f(1)=-1$.

R. Forma funcției de gradul al doilea $f : \mathbb{R} \to \mathbb{R}$ este $f(x) = ax^2+bx+c, a,b,c \in \mathbb{R}, a \neq 0$. Condițiile din problemă se transcriu sub forma: $f(-1)=1 \Leftrightarrow a-b+c=1$; $f(0)=0 \Leftrightarrow c=0$; $f(1)=-1 \Leftrightarrow a+b+c=-1$.

Sistemul obținut în necunoscutele a,b,c: $\begin{cases} a-b+c=1 \\ c=0 \\ a+b+c=-1 \end{cases}$ are soluția $a=0, b=-1, c=0$.

Cum a trebuie să fie nenul deducem că nu există funcție de gradul al doilea.

3. Să se arate că funcția polinomială $f : \mathbb{R} \to \mathbb{R}, f(x) = x^3+3x+4$ se poate scrie ca produsul dintre o funcție de gradul întâi şi alta de gradul al doilea.

R. Trebuie să arătăm că există funcțiile $g,h : \mathbb{R} \to \mathbb{R}$, $g(x) = x+a$, $h(x) = bx^2+cx+d$, $a,b,c,d \in \mathbb{R}, b \neq 0$ astfel încât $x^3+3x+4 = (x+a)(bx^2+cx+d), (\forall) x \in \mathbb{R}$ sau după unele calcule $x^3+3x+4 = bx^3+(c+ab)x^2+(d+ac)x+ad$.

De aici prin identificare (a termenilor de acelaşi grad din cei doi membri) rezultă sistemul:

$$\begin{array}{c|l} x^3 & 1=b \\ x^2 & 0=c+ab \\ x & 3=d+ac \\ x^0 & 4=ad \end{array}$$

cu soluția $a=b=1, c=-1, d=4$. Deci $f(x) = (x+1)(x^2-x+4)$.

Observație. Metoda prin care am determinat coeficienții a, b, c, d se numeşte metoda coeficienților nedeterminați (sau metoda identificării).

4. Se consideră polinomul $f = (1+X)^{30} = a_0+a_1X+a_2X^2+...+a_{30}X^{30}$.

a) Să se calculeze $a_0+a_2+a_4+...+a_{30}$;

b) Să se calculeze $a_1+a_3+...+a_{29}$;

c) Să se calculeze a_{19}, a_{27}.

R. a)-b) Calculând valoarea polinomului f în $x=1$ obținem suma tuturor coeficienților acestuia:

$f(1) = 2^{30} = a_0+a_1+a_2+a_3+...+a_{29}+a_{30}$, (1).

Pentru $x=-1$ avem $f(-1) = 0 = a_0-a_1+a_2-a_3+....-a_{29}+a_{30}$, (2).

Adunând (1) cu (2) rezultă $2^{30} = 2(a_0+a_2+...+a_{30})$, adică $a_0+a_2+...+a_{30} = 2^{29}$.

Ținând seama de această ultimă egalitate şi de (1) rezultă: $a_1+a_3+...+a_{29} = 2^{29}$.

c) Să observăm că a_{19} este coeficientul lui X^{19} Scriem formula termenului de rang $k+1$ din binomul lui Newton şi avem: $T_{k+1} = C_{30}^k X^{30-k}$. Impunând condiția ca $30-k=19$ rezultă $k=11$. Deci $a_{19} = C_{30}^{11}$. Analog $a_{27} = C_{30}^3$.

5. **Să se determine funcțiile polinomiale de gradul al doilea $f:\mathbb{R}\to\mathbb{R}$, $f(x)=x^2+ax+b, a,b\in\mathbb{R}$ care admit ca rădăcini pe a şi b.**

R. Dacă ecuația $x^2+ax+b=0$ are rădăcinile $x_1=a, x_2=b$, atunci conform relațiilor lui Viète putem scrie $a+b=-a$ şi $ab=b$.
Rezolvând sistemul găsim $a=b=0$ sau $a=1, b=-2$.

Deci funcțiile căutate sunt $f(x)=x^2, f(x)=x^2+x-2$.

6. **a) Dacă $f:\mathbb{R}\to\mathbb{R}$ este o funcție polinomială de grad n, $n\geq 1$, atunci funcția polinomială $g:\mathbb{R}\to\mathbb{R}, g(x)=f(x+1)-f(x)$ are gradul $n-1$.**

b) Determinați funcția polinomială f dacă $f(x+1)-f(x)=3x^2+3x+1, (\forall)x\in\mathbb{R}$.

R. a) Fie $f(x)=a_0+a_1x+...+a_nx^n, a_n\neq 0$. Atunci:

$$g(x)=f(x+1)-f(x)=a_n(x+1)^n+a_{n-1}(x+1)^{n-1}+...+a_1(x+1)+a_0-a_nx^n-a_{n-1}x^{n-1}-$$
$$-...-a_1x-a_0=\left(a_nx^n+C_n^1a_nx^{n-1}+...+a_n\right)+\left(a_{n-1}x^{n-1}+C_{n-1}^1a_{n-1}x^{n-2}+...+a_{n-1}\right)+...+$$
$$+a_0-a_nx^n-a_{n-1}x^{n-1}-...-a_1x-a_0=na_nx^{n-1}+...$$ pentru care $na_n\neq 0$, adică $\text{grad}(g)=n-1$.

b) Dacă gradul lui g este 2, atunci gradul lui f este egal cu 3.

Fie deci $f(x)=a_3x^3+a_2x^2+a_1x+a_0$. Avem

$$g(x)=f(x+1)-f(x)=3a_3x^3+(3a_3+2a_2)x+a_3+a_2+a_1.$$

Din $g(x)=3x^2+3x+1$ şi exprimarea de mai sus, prin identificare, găsim sistemul:

$$\begin{array}{l|l} x^2 & 3=3a_3 \\ x & 3=3a_3+2a_2 \\ x^0 & 1=a_3+a_2+a_1 \end{array}$$ cu soluția $a_1=a_2=0, a_3=1$. Deci $f(x)=x^3+a_0, a_0\in\mathbb{R}$.

7. **Să se determine $m,n\in\mathbb{R}$ astfel încât polinomul $f=X\left(X^2-1\right)\left(X+m\right)+n$ să fie pătratul unui alt polinom.**

R. Cum grad(f) = 4, iar coeficientul dominant al lui este 1, atunci se cere să găsim polinomul $g=X^2+\alpha X+\beta$ cu proprietatea că $f=g^2$. Ridicând pe g la pătrat şi ordonând cele două polinoame f, g se obțin, în urma identificării, valorile $\left(m=0, n=\frac{1}{4}\right), \left(m=2, n=1\right), \left(m=-2, n=1\right)$.

8. **Să se determine funcția polinomială $f:\mathbb{R}\to\mathbb{R}$ pentru care:**

$$f\left(f(x)\right)=x^4-4x^3+8x^2-8x+6, (\forall)x\in\mathbb{R}.$$

R. Dacă f ar fi de gradul întâi, atunci şi $f\circ f$ ar avea aceeaşi proprietate. Deci nu este o funcție bună pentru problema noastră. Dacă f are gradul doi, atunci $f\circ f$ are gradul patru. Deci astfel de funcții trebuie să analizăm. Fie deci $f(x)=ax^2+bx+c, a,b,c\in\mathbb{R}, a\neq 0$ pentru care

$$f\left(f(x)\right)=a\left(ax^2+bx+c\right)^2+b\left(ax^2+bx+c\right)+c=a^3x^4+2a^2bx^3+\left(ab^2+2a^2c+ab\right)x^2+$$
$$+\left(2abc+b^2\right)x+ac^2+bc+c.$$

Identificăm şi avem sistemul: $\begin{array}{c|l} x^4 & 1=a^3 \\ x^3 & -4=2a^2b \\ x^2 & 8=ab^2+2a^2c+ab \\ x & -8=2abc+b^2 \\ x^0 & 6=ac^2+bc+c \end{array}$ cu soluția $a=1, b=-2, c=3$.

6. TEOREMA ÎMPĂRȚIRII CU REST

1) Împărțirea polinoamelor

Aritmetica inelelor de polinoame $K[X]$ este similară aritmeticii inelului $\mathbb{Z}$ al numerelor întregi în care avem două teoreme remarcabile: **teorema împărțirii cu rest** şi **teorema de descompunere în factori primi**.

Teorema împărțirii cu rest din $\mathbb{Z}$ ne spune că fiind date două numere întregi a şi b, $b\neq 0$, există exact două numere întregi unice q şi r astfel încât are loc egalitatea: $a=bq+r$, unde $0\leq r<|b|$, unde a este deîmpărțitul, b împărțitorul, q câtul, iar r restul.

În teoria împărțirii polinoamelor se întâlneşte o proprietate analogă. Reamintim că am notat prin K unul din corpurile $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$, p prim.

Are loc următoarea:

Teoremă. (**Teorema împărțirii cu rest a polinoamelor**). Fie $f,g\in K[X]$, $g\neq 0$. Atunci există polinoamele unice $q,r\in K[X]$ astfel încât: $f=gq+r$ şi $\text{grad}(r)<\text{grad}(g)$ (*).

Polinomul f se numeşte **deîmpărțit**, polinomul g este **împărțitorul**, polinomul q este **câtul**, iar polinomul r se numeşte **restul** împărțirii polinomului f la polinomul g.

Dacă $r=0$, adică dacă $f=gq$, atunci spunem că polinomul f **se divide** prin polinomul g (sau că f este **multiplu** de polinomul g) sau g **divide** polinomul f (sau că g **este divizor** al polinomului f).

Dacă f se divide prin g, atunci scriem: $f\,\vdots\,g$ (citim: f se divide prin g) sau $g\,|\,f$ (citim: g divide f).

Demonstrație. **1) Existența polinoamelor** q, r. Dacă $f=0$, atunci se iau $q=r=0$ şi (*) se verifică.

Dacă $f\neq 0$, $\text{grad}(f)<\text{grad}(g)$, atunci luăm $q=0$, $r=f$ şi (*) este verificată.

Fie $f \neq 0$, $\mathrm{grad}(f) \geq \mathrm{grad}(g)$, unde $f = a_0 + a_1 X + ... + a_n X^n$, $a_n \neq 0$, $g = b_0 + b_1 + ... + b_m X^m$, $b \neq 0$.

În cele ce urmează descriem **algoritmul împărțirii lui** f la g (însoțit de un caz particular; etapele sunt numerotate)

1) Pentru aceasta scriem cele două polinoame ordonate după puterile descrescătoare ale lui X.

2) Se dispun polinoamele ca mai jos:

$$f = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0 \quad \Big| \; b_m X^m + ... + b_1 X + b_0 = g$$

Exemplu: 2) $f = 6X^5 - 17X^3 - X^2 + 3$, $g = 3X^2 - 6X + 2$, $f, g \in \mathbb{Q}[X]$

$$f = 6X^5 + 0X^4 - 17X^3 - X^2 + 0X + 3 \quad \Big| \; 3X^2 - 6X + 2 = g$$

3) Se împarte primul termen al lui f la primul termen al lui g și avem $a_n X^n : a_m X^m = a_n a_m^{-1} X^{n-m}$. Acest termen se pune în schemă sub împărțitor.

Se înmulțeşte rezultatul astfel obținut cu împărțitorul g și se scade acest produs din deîmpărțitorul f (adică, se adună acest produs cu semn schimbat la f) și se obține polinomul $f_1 = f - a_n b_m^{-1} X^{n-m} g$.

$$\begin{array}{l|l} f = a_n X^n + a_{n-1} X^{n-1} + ... + a_0 & b_m X^m + ... + b_1 X + b_0 = g \\ \quad -a_n X^n - ... & \overline{a_n b_m^{-1} X^{n-m}} \\ \hline f_1 = f - a_n b_m^{-1} X^{n-m} & \end{array}$$

Polinomul f_1 are gradul cel mult $n-1$

3) $6X^5 : 3X^2 = 2X^3$

$$\begin{array}{l|l} f = 6X^5 + 0X^4 - 17X^3 - X^2 + 0X + 3 & 3X^2 - 6X + 2 = g \\ \quad -6X^5 + 12X^4 - 4X^3 & \overline{2X^3} \\ \hline \quad / \; f_1 = 12X^4 - 21X^3 - X^2 + 0X + 3 & \end{array}$$

$\mathrm{grad}(f_1) = 4$

4) Dacă $\mathrm{grad}(f_1) \geq m = \mathrm{grad}(g)$, atunci se repetă pasul 3) cu f_1 în locul lui f. Fie $f_1 = a'_{n_1} X^{n_1} + ... + a'_0$, $n_1 < n$.

Se obține: $f_2 = f_1 - a'_{n_1} b_m^{-1} X^{n_1 - m}$, unde $\mathrm{grad}(f_2) = n_2$ și $n_2 < n_1$.

4) $\mathbf{grad}(f_1) = 4 > \mathbf{grad}(g) = 2$, $f_1 = 12X^4 - 21X^3 - X^2 + 0X + 3$, $g = 3X^2 - 6X + 2$

$12X^4 : 3X^2 = 4X^2$

$$\begin{array}{l|l} f_1 = 12X^4 - 21X^3 - X^2 + 0X + 3 & 3X^2 - 6X + 2 = g \\ \cline{2-2} \quad \underline{-12X^4 + 24X^3 - 8X^2} & 4X^2 \\ \quad / \qquad 3X^3 - 9X^2 + 0X + 3 = f_2 & \end{array}$$

5) Dacă $\mathrm{grad}(f_2) \geq m = \mathrm{grad}(g)$, atunci pentru f_2 şi g se aplică 3) $f_2 = a''_{n_2} X^{n_2} + ... + a''_0$, atunci $f_3 = f_2 - a''_{n_2} b_m^{-1} X^{n_2 - m}$, unde $\mathrm{grad}(f_3) = n_3$ şi $n_3 < n_2$.

5) $\mathbf{grad}(f_2) = 3 > \mathbf{grad}(g) = 2$, $f_2 = 3X^3 - 9X^2 + 3$, $g = 3X^2 - 6X + 2$; $3X^3 : 3X^2 = X$

$$\begin{array}{l|l} f_2 = 3X^3 - 9X^2 + 0X + 3 & 3X^2 - 6X + 2 = g \\ \cline{2-2} \quad \underline{-3X^3 + 6X^2 - 2X} & X \\ \qquad -3X^2 - 2X + 3 = f_3 & \end{array}$$

6) După un număr finit de paşi se obține numărul $n_p < m$. Algoritmul se termină când gradul restului (pentru f_p, $\mathrm{grad}(f_p) = n_p$) este strict mai mic decât gradul împărțitorului.

6) $\mathbf{grad}(f_3) = 2 = \mathbf{grad}(g) = 2$, $f_3 = -3X^2 - 2X + 3$, $g = 3X^2 - 6X + 2$; $-3X^2 : 3X^2 = -1$

$$\begin{array}{l|l} f_3 = -3X^2 - 2X + 3 & 3X^2 - 6X + 2 = g \\ \cline{2-2} \qquad \underline{3X^2 - 6X + 2} & -1 \\ \qquad\quad -8X + 5 = f_4 & \end{array}$$

Unde $\mathbf{grad}(f_4) = 1 < \mathbf{grad}(g) = 2$

Din egalitățile de mai sus rezultă:

$$f = a_n b_m^{-1} X^{n-m} g + f_1,$$

$$f_1 = a'_{n_1} b_m^{-1} X^{n_1 - m} g + f_2,$$

....

$$f_p = a_{n_{p-1}} b_m^{-1} X^{n_{p-1} - m} g + f_p.$$

Prin adunarea lor, membru cu membru, rezultă:

$$f = \left(a_n b_m^{-1} X^{n-m} + a'_{n_1} b_m^{-1} X^{n_1 - m} + ... + a_{n_{p-1}} b_m^{-1} X^{n_{p-1} - m} \right) g + f_p.$$

Punem $q = a_n b_m^{-1} X^{n-m} + a'_{n_1} b_m^{-1} X^{n_1-m} + \ldots + a_{n_{p-1}} b_m^{-1} X^{n_{p-1}-m}$, $r = f_p$ şi avem: $f = gq + r$ cu $\text{grad}(r) < \text{grad}(q)$

În exemplul nostru reunim etapele precedente într-o singură schemă şi avem:

$$
\begin{array}{l|l}
f = 6X^5 + 0X^4 - 17X^3 - X^2 + 0X + 3 & 3X^2 - 6X + 2 = g \\ \cline{2-2}
\underline{-6X^5 + 12X^4 - 4X^3} & 2X^3 + 4X^2 + X - 1 = q \\
\;/ \quad 12X^4 - 21X^3 - X^2 + 0X + 3 & \\
\quad \underline{-12X^4 + 24X^3 - 8X^2} & \\
\qquad / \quad 3X^3 - 9X^2 + 0X + 3 & \\
\qquad \underline{-3X^3 + 6X^2 - 2X} & \\
\qquad\quad / \quad -3X^2 - 2X + 3 & \\
\qquad\qquad \underline{3X^2 - 6X + 2} & \\
\qquad\qquad / \quad -8X + 5 = r &
\end{array}
$$

Am arătat că există polinoamele q şi r pentru care (*) are loc.

2) Unicitatea polinoamelor q, r. Prin metoda reducerii la absurd. Presupunem că mai există q_1, r_1, două polinoame care verifică (*) cu $q_1 \neq q$ şi $r_1 \neq r$.

Deci: $f = gq + r$, $f = gq_1 + r_1$, iar de aici prin scădere rezultă $g(q - q_1) = r - r_1$, fals, deoarece $\text{grad}(r - r_1) \leq \max\{\text{grad}(r), \text{grad}(r_1)\} < \text{grad}(g) \leq \text{grad}\left(g(q - q_1)\right)$. Deci q, r din (*) sunt unice. ■

Observaţie. Teorema enunţată este adevărată şi în $A[X]$, unde A este inel comutativ cu element unitate cu condiţia ca b_m, coeficientul dominant al lui *g*, să fie inversabil.

Exemplu. Să se determine câtul şi restul împărţirii polinomului *f* la polinomul *g* în cazurile:

1) $f = 3X^3 + 2X^2 - X + 5,\ g = X^2 - X,\ f, g \in \mathbb{Z}[X]$;

2) $f = \hat{2}X^3 + \hat{3}X^2 + \hat{2}X + \hat{1},\ g = \hat{5}X^2 + \hat{2}X,\ f, g \in \mathbb{Z}_6[X]$;

3) $f = \hat{4}X^4 + \hat{3}X^2 + \hat{3}X + \hat{2},\ g = \hat{2}X^2 + \hat{3}X + \hat{1},\ f, g \in \mathbb{Z}_6[X]$.

R. 1) Avem schema de împărţire cunoscută (observaţi coeficientul dominant al lui *g* este 1, inversabil în $\mathbb{Z}$; $U(\mathbb{Z}) = \{\pm 1\}$):

$$
\begin{array}{r|l}
3X^3 + 2X^2 - X + 5 & X^2 - X \\ \cline{2-2}
\underline{-3X^3 + 3X^2 \qquad\qquad} & 3X + 5 = q \\
5X^2 - X + 5 & \\
\underline{-5X^2 + 5X \qquad} & \\
4X + 5 = r &
\end{array}
$$

2) Să observăm că ne plasăm cu împărţirea într-un inel cu divizori ai lui zero. Dar elementul dominant al lui *g* este $\hat{5}$, care este inversabil în $\mathbb{Z}_6[X]$ şi $\hat{5}^{-1} = \hat{5}$.

$$\begin{array}{ll|l}
 & \hat{2}X^3+\hat{3}X^2+\hat{2}X+\hat{1} & \hat{5}X^2+\hat{2}X \\ \cline{3-3}
 & -\hat{2}X^3-\hat{2}X^2 & \hat{4}X+\hat{5} \\ \cline{2-2}
 & \qquad\quad X^2+\hat{2}X+\hat{1} & \\
 & \qquad -X^2-\hat{4}X & \\ \cline{2-2}
 & \qquad\qquad -\hat{2}X+\hat{1}=\hat{4}X+\hat{1} &
\end{array}$$

Deci $q=\hat{4}X+\hat{5}$ şi $r=\hat{4}X+1$.

Pentru a găsi coeficientul primului element al câtului trebuie să avem egalitatea $\hat{2}=\hat{5}\cdot c_1$. De aici $\hat{2}\cdot\hat{5}^{-1}=c_1$, adică $c_1=\hat{4}$.

Pentru a găsi coeficientul celui de-al doilea termen al câtului rezolvăm ecuația $\hat{1}=\hat{5}\cdot c_2$. De aici $c_2=\hat{5}^{-1}=\hat{5}$.

3) Să remarcăm că în acest caz coeficientul dominant al lui g este egal cu $\hat{2}$, care însă nu este inversabil în $\mathbb{Z}_6[X]$ şi deci nu mai funcționează algoritmul de la teorema împărțirii cu rest, când câtul şi restul erau unice. Totuşi, scriem pentru f,g egalitatea $\hat{4}X^4+\hat{3}X^2+\hat{3}X+\hat{2}=\left(\hat{2}X^2+\hat{3}X+\hat{1}\right)\left(aX^2+bX+c\right)+mX+n, a,b,c,m,n\in\mathbb{Z}_6$.

Efectuăm calculele în membrul drept şi avem: $\hat{4}X^4+\hat{3}X^2+\hat{3}X+\hat{2}=\hat{2}aX^4+\left(\hat{2}b+\hat{3}a\right)X^3+\left(\hat{2}c+\hat{3}b+a\right)X^2+\left(\hat{3}c+b+m\right)X+c+n$. Prin identificare rezultă sistemul:

$$\begin{cases}\hat{2}a=\hat{4}\\ \hat{2}b+\hat{3}a=\hat{0}\\ \hat{2}c+\hat{3}b+a=\hat{3}\\ \hat{3}c+b+m=\hat{3}\\ c+n=\hat{2}\end{cases}$$

. Găsim cel puțin două soluții ale sistemului:

$$a_1=\hat{2}, b_1=\hat{3}, c_1=\hat{2}, m_1=\hat{0}, n_1=\hat{0};$$
$$a_2=\hat{2}, b_2=\hat{3}, c_2=\hat{5}, m_2=\hat{3}, n_2=\hat{3};$$

Deci f se poate scrie la împărțirea prin g în cel puțin două moduri:

$$f=g\left(\hat{2}X^2+\hat{3}X+\hat{2}\right),\quad f=g\left(\hat{2}X^2+\hat{3}X+\hat{5}\right)+\hat{3}X+\hat{3}.$$

Probleme rezolvate

1. Să se efectueze împărțirea polinomului $f=6X^3-7X^2+3X+2$ la polinomul $g=2X^2-3X+2$ şi apoi să se facă proba.

R. *Metoda* 1. Aplicăm algoritmul descris mai sus şi avem:

$$\begin{array}{l|l}
6X^3-7X^2+3X+2 & 2X^2-3X+2 \\ \cline{2-2}
-6X^3+9X^2-6X & 3X+1 \\ \hline
/ \qquad 2X^2-3X+2 & \\
\qquad -2X^2+3X-2 & \\ \hline
\qquad\ / \qquad / \qquad / &
\end{array}$$

Deci câtul împărțirii este $q = 3X + 1$, iar restul este polinomul nul $r = 0$, ceea ce înseamnă că polinomul f se divide prin polinomul g.

Proba are loc deoarece $\left(2X^2 - 3X + 2\right)\left(3X + 1\right) = 6X^3 - 7X^2 + 3X + 2$.

Metoda 2 (*Metoda identificării*). Evident apelează la teorema împărțirii cu rest

$$\boxed{f = g \cdot q + r \text{, unde } \operatorname{grad}(r) < \operatorname{grad}(g)\text{,} \qquad (1)}$$

Este clar că $\operatorname{grad}(f) = \operatorname{grad}(g) + \operatorname{grad}(q)$, adică

$$\boxed{\operatorname{grad}(q) = \operatorname{grad}(f) - \operatorname{grad}(g)\text{,} \qquad (2)}$$

Pentru q se ia un polinom cu coeficienți literali (coeficienți nedeterminați) care să satisfacă relația (2), iar pentru r se ia un polinom cu coeficienți nedeterminați de grad mai mic cu o unitate decât gradul lui g (împărțitorul). Se introduc aceste polinoame în egalitatea împărțirii cu rest și se efectuează calculele în membrul drept al relației. Se identifică coeficienții termenilor de același grad în X din cei doi membri și se obține un sistem având ca necunoscute coeficienții lui q și r. Se rezolvă acest sistem și se obțin q și r. În cazul nostru $q = aX + b$, iar $r = cX + d$ $\left(\operatorname{grad}(r) < \operatorname{grad}(g)\right)$.

Din identitatea împărțirii cu rest, avem: $6X^3 - 7X^2 + 3X + 2 = \left(2X^2 - 3X + 2\right)\left(aX + b\right) + cX + d$ sau după efectuarea calculelor în membrul drept și ordonarea descrescătoare după puterile lui X, $6X^3 - 7X^2 + 3X + 2 = 2aX^3 - \left(3a - 2b\right)X^2 + \left(2a - 3b + c\right)X + \left(2b + d\right)$.

De aici prin identificare rezultă sistemul:

$$\begin{array}{l|l} X^3 & 6 = 2a \\ X^2 & -7 = -3a + 2b \\ X & 3 = 2a - 3b + c \\ X^0 & 2 = 2b + d \end{array} \quad \text{cu soluția } a = 3, b = 1, c = 0, d = 0\text{, adică } q = 3X + 1, r = 0.$$

2. Să se afle câtul și restul împărțirii polinomului $f = X^6 - X^5 + X^4 - X^3 + X^2$ prin polinomul $g = X - i$.

R. Efectuăm împărțirea directă a polinomului f prin polinomul g când avem:

$$\begin{array}{l|l}
X^6 - 5X^5 + X^4 - X^3 + X^2 + 0X + 0 & X - i \\ \cline{2-2}
-X^6 + iX^5 & X^5 + \left(i - 1\right)X^4 - iX^3 + X + i \\ \cline{1-1}
/\ (i-1)X^5 + X^4 - X^3 + X^2 & \\
-(i-1)X^5 + i(i-1)X^4 & \\ \cline{1-1}
/\quad -iX^4 - X^3 + X^2 & \\
\quad iX^4 + X^3 & \\ \cline{1-1}
/\quad X^2 & \\
\quad -X^2 + iX & \\ \cline{1-1}
/\quad iX & \\
\quad -iX - 1 & \\ \cline{1-1}
/\quad -1 &
\end{array}$$

Deci $q = X^5 + (i-1)X^4 - iX^3 + X + i$ şi $r = -1$.

3. Să se determine câtul şi restul împărţirii polinomului $f = \hat{3}X^3 + \hat{4}X^2 + \hat{3}X + \hat{2}$ la $g = \hat{2}X^2 + \hat{3}X$, $f, g \in \mathbb{Z}_5[X]$.

R. Suntem în inelul $\mathbb{Z}_5[X]$, care este un domeniu de integritate în care are loc teorema împărţirii cu rest, cu q (câtul) şi r (restul) unice. Avem:

$$
\begin{array}{r|l}
\hat{3}X^3 + \hat{4}X^2 + \hat{3}X + \hat{2} & \hat{2}X^2 + \hat{3}X \\
\cline{2-2}
-\hat{3}X^3 - \hat{2}X^2 \qquad\qquad & c_1(=\hat{4})X + c_2(=\hat{1}) \\
\cline{1-1}
/ \qquad \hat{2}X^2 + \hat{3}X + \hat{2} & \\
-\hat{2}X^2 - \hat{3}X \quad & \\
\cline{1-1}
/ \qquad\quad / \quad \hat{2} &
\end{array}
$$

Deci $q = \hat{4}X + \hat{1}$ şi $r = \hat{2}$.

Pentru determinarea lui c_1 rezolvăm ecuaţia $\hat{3} = \hat{2}c_1$, când găsim $c_1 = \hat{4}$.

Pentru determinarea lui c_2 se rezolvă ecuaţia $\hat{2} = \hat{2}c_2$, când $c_2 = \hat{1}$.

2) Împărţirea polinoamelor prin *X*-a. Teorema restului. Teorema factorului

În cazul particular când împărţitorul $g = X - a \in K[X]$, restul se poate determina simplu. Are loc următoarea:

> **Teoremă (Teorema restului).** Restul împărţirii polinomului $f \in K[X]$, $f \neq 0$, prin polinomul $g = X - a \in K[X]$ este egal cu valoarea numerică a polinomului f pentru $x = a$, adică $r = f(a)$.

Demonstraţie. Conform teoremei împărţirii cu rest a polinomului f prin polinomul g putem scrie $f = (X - a)q + r$, unde $\operatorname{grad}(r) < 1$. De aici $\operatorname{grad}(r) = 0$ sau $\operatorname{grad}(r) = -\infty$, adică r este un polinom constant sau respectiv $r = 0$. Prin urmare: $f(x) = (x-a)q(x) + r$, $(\forall) x \in K$. Pentru $x = a$ rezultă $f(a) = r$. ■

Această teoremă precizează că în cazul în care un polinom f se împarte la polinomul $X - a$, atunci restul acestei împărţiri se poate calcula luând valoarea funcţiei polinomiale asociate lui f în $x = a$, adică $f(a)$.

Dacă g are forma $g = aX + b,\ a \neq 0$ atunci se aduce la forma $g = a\left[X - \left(-\frac{b}{a}\right)\right]$ şi restul este $r = f\left(-\frac{b}{a}\right)$. Din teorema restului se obţine cunoscuta **teoremă a lui**

Bézout (**teorema factorului**), care stabileşte legătura între divizorii de gradul întâi ai polinomului $f \in K[X]$ şi rădăcinile din K ale acestui polinom. Mai precis are loc:

Teorema factorului (**Bézout**). Un element $a \in K$ este rădăcină a polinomului $f \in K[X]$ dacă şi numai dacă $X - a$ divide pe f.

Deci, $f \vdots X - a \Leftrightarrow f(a) = 0$.

Demonstrație. Din teorema restului $r = f(a)$. Elementul a este rădăcină a polinomului dacă $f(a) = 0$. Dacă $f \vdots X - a$, atunci $f = (X - a)g$, $g \in K[X]$, iar de aici $f(a) = 0$, adică a este rădăcină pentru f.■

Observații. **1)** Dacă $a_1, a_2 \in K$ sunt rădăcini ale lui f, atunci $f = (X - a_1)(X - a_2)q$, $q \in K[X]$.

2) Dacă $\text{grad}(f) = n$ şi $f(a_i) = 0,\ i = \overline{1,n}$, atunci $f = a(X - a_1)(X - a_2)...(X - a_n)$.

Mai general are loc următoarea:

Definiție. Elementul $a \in K$ **este rădăcină de ordin** $p \in \mathbb{N}^*$ **pentru polinomul** $f \in K[X]$ dacă f se divide prin $(X - a)^p$, dar nu se divide prin $(X - a)^{p+1}$.

Pentru funcția polinomială asociată elementul *a* este zero de ordin *p*.

Dacă $p = 1$, atunci a este **rădăcină simplă** pentru $f\left(f \vdots X - a \text{ şi } f \not\vdots (X - a)^2\right)$.

Dacă $p = 2$, atunci a este **rădăcină dublă** pentru $f\left(f \vdots (X - a)^2 \text{ şi } f \not\vdots (X - a)^3\right)$.

Dacă $p = 3$, atunci a este **rădăcină triplă** pentru $f\left(f \vdots (X - a)^3 \text{ şi } f \not\vdots (X - a)^4\right)$.

Rădăcinile multiple ale unei funcții polinomiale $f : \mathbb{C} \to \mathbb{C}$ pot fi caracterizate cu ajutorul derivatelor de ordin superior ale lui f prin următoarea:

Teoremă. Funcția *f* are pe a ca zero multiplu de ordin p dacă și numai dacă $f(a)=f'(a)=...=f^{(p-1)}(a)=0$ și $f^{(p)}(a)\neq 0,\ p\in\mathbb{N}^*$.

În particular: 1) $x=a$ este **zero simplu** pentru *f* dacă: $f(a)=0,\ f'(a)\neq 0$.

2) $x=a$ este **zero dublu** pentru *f* dacă: $f(a)=f'(a)=0,\ f''(a)\neq 0$.

3) $x=a$ este **zero triplu** pentru *f* dacă: $f(a)=f'(a)=f''(a)=0,\ f'''(a)\neq 0$.

Exemple. 1. Să se determine restul împărțirii polinomului *f* prin $g=X-a$ în cazurile:

1°) $f=2X^3-3X^2+4X-4,\ g=X-1$;

2°) $f=X^4-3X^2+5,\ g=2X+1$;

3°) $f=\hat{3}X^3+\hat{2}X^2+\hat{4},\ g=X+\hat{2},\ f,g\in\mathbb{Z}_5[X]$.

R. 1°) Avem: $r=f(1)=2\cdot 1^3+4\cdot 1-5=2-3+4-5=-2$.

2°) Scriem pe *g* sub forma: $g=2\left[X-\left(-\frac{1}{2}\right)\right]$ și atunci $r=f\left(-\frac{1}{2}\right)=\frac{69}{16}$.

3°) Se pune *g* sub forma $g=X-\left(-\hat{2}\right)=X-\hat{3}$ (deoarece $-\hat{2}=\hat{3}$) și deci restul împărțirii lui *f* la *g* este egal cu $r=f(\hat{3})=\hat{3}$.

2. Să se arate că *a* scris în dreptul polinomului *f* este rădăcină a acestuia în cazurile:

1°) $f=X^3-2X^2+3X-2,\ a=1$

2°) $f=\hat{2}X^3+\hat{3}X^2+\hat{2},\ a=\hat{2},\ f\in\mathbb{Z}_5[X]$.

R. 1°) Avem $f(1)=0$, ceea ce arată că $a=1$ este rădăcină pentru *f*.

2°) Calculăm $f(\hat{2})=\hat{2}\cdot\hat{3}+\hat{3}\cdot\hat{4}+\hat{2}=\hat{1}+\hat{2}+\hat{2}=\hat{0}$. Deci $a=\hat{2}$ a este rădăcină a lui *f*.

3. Să se precizeze pentru polinomul $f=X^6-7X^5+15X^4-40X^2+48X-16$ ordinul de multiplicitate al rădăcinii $a=2$.

R. Considerăm funcția polinomială $f:\mathbb{R}\to\mathbb{R},\ f(x)=x^6-7x^5+15x^4-40x^2+48x-16$, pentru care $f'(x)=6x^5-7x^4+60x^3-80x+48$, $f''(x)=30x^4-28x^3+180x^2-80$, $f'''(x)=120x^3-84x^2+360x$, $f^{(4)}(x)=360x^2-168x+360$.

Avem $f(2)=f'(2)=f''(2)=f'''(2)=0$ și $f^{(4)}(2)\neq 0$, ceea ce arată că $a=2$ este rădăcină multiplă de ordin patru pentru *f*.

Altfel, se împarte *f* la $X-2$. Câtul se împarte din nou la $X-2$, etc. Vom reveni asupra acestei probleme la Schema lui Horner.

3) Schema lui Horner (1786-1837)

Am întâlnit mai sus schema lui Horner (William Georges, 1786-1837, matematician englez, publică în 1819 metoda care-i poartă numele) când a trebuit să calculăm valoarea unui polinom într-un punct, utilizând pentru funcția polinomială o anumită scriere. Am văzut că la împărțirea unui polinom prin $X-a$, restul este dat de

$r = f(a)$, deci el se poate determina prin schema lui Horner. Mai mult, în acest caz, schema ne dă şi coeficienţii câtului de la împărţire.

Fie $\quad f = a_n X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0$ şi

$$q = b_{n-1}X^{n-1} + b_{n-2}X^{n-2} + ... + b_1 X + b_0 .$$

Din $f = (X-a)q + r$, prin identificare, rezultă egalităţile: $a_n = b_{n-1}, b_k = ab_{k+1} + a_{k+1}$, $0 \le k \le n-2$.

Schema lui Horner arată astfel:

Deîmpărţitorul f

	X^n	X^{n-1}	X^{n-2}	$\cdots$	X^2	X	X^0
	a_n	a_{n-1}	a_{n-2}	$\cdots$	a_2	a_1	a_0
a	a_n $\Vert$ b_{n-1}	$a \cdot b_{n-1}$ $\downarrow +$ $ab_{n-1} + a_{n-1}$ $\Vert$ b_{n-2}	ab_{n-2} $\downarrow +$ $ab_{n-2} + a_{n-2}$ $\Vert$ b_{n-3}	$\cdots$	b_1	ab_1 $\downarrow +$ $ab_1 + a_1$ $\Vert$ b_0	ab_0 $\downarrow +$ $ab_0 + a_0$ $\Vert$ r
	X^{n-1}	X^{n-2}	X^{n-3}	$\cdots$	X	X^0	Restul

Câtul q

Coeficientul dominant al câtului, b_{n-1}, coincide cu coeficientul dominant al deîmpărţitului, a_n.

Formula $b_{k-1} = ab_k + a_k$, $k = \overline{1, n-1}$, ne spune că dacă am aflat coeficientul b_k al lui X^k din cât, atunci coeficientul lui X^{k-1}, tot din cât se obţine înmulţind pe b_k cu a şi rezultatul se adună cu a_k (coeficientul lui X^k din deîmpărţit).

Se trec puterile lui *X*, de la deîmpărţit în ordine descrescătoare (inclusiv puterile care lipsesc – acestea au coeficienţii egali cu zero). Sub fiecare putere a lui *X* se trece coeficientul cu care apare în scrierea lui *f*. Pe linia următoare se coboară coeficientul dominant (a_n care este b_{n-1}, primul coeficient al câtului). Pe această linie, în faţa lui a_n, se scrie termenul *a* din binomul $X - a$. Această linie se completează cu ceilalţi coeficienţi ai câtului după relaţiile:

$b_{n-2} = a \cdot b_{n-1} + a_{n-1}, b_{n-3} = ab_{n-2} + a_{n-2}$ etc. Sub coeficienţii $b_{n-1}, b_{n-2}, ...,$ se scriu puterile lui X : $X^{n-1}, X^{n-2}, ...$ pentru a scrie mai uşor polinomul *q*.

Exemple. 1) $f=3X^5-2X^3+3X^2-5$, $g=X-2$

	X^5	X^4	X^3	X^2	X	X^0
	3	0	-2	3	0	-5
	$\downarrow$	$\cdot 2\nearrow$ 6 $\downarrow +$	$\cdot 2\nearrow$ 12 $\downarrow +$	$\cdot 2\nearrow$ 20 $\downarrow +$	$\cdot 2\nearrow$ 46 $\downarrow +$	$\cdot 2\nearrow$ 92 $\downarrow +$
2	3	6	10	23	46	$87=r$
	X^4	X^3	X^2	X	X^0	

Deci, $q=3X^4+6X^3+10X^2+23X+46$, $r=87$

2) $f=2X^3-3X^2+4X-6$, $g=X+1$

	X^3	X^2	X	X^0
	2	-3	4	-6
-1	2	-5	9	$-15=r$
	X^2	X	X^0	

Deci, câtul este $q=2X^2-5X+9$ şi restul $r=-15$.

3) $f=2X^3+8X^2-4X+2$, $g=2X+1$

În acest caz, teorema împărţirii cu rest este $f=(2X+1)q+r$ sau împărţind la 2 avem: $\frac{1}{2}f=\left(X+\frac{1}{2}\right)q+\frac{r}{2}$. Deci pentru polinomul $\frac{1}{2}f$ şi $g=X+\frac{1}{2}=X-\left(-\frac{1}{2}\right)$ se aplică schema lui Horner. Avem:

	X^3	X^2	X	X^0
	1	4	-2	1
$-\frac{1}{2}$	1	$\frac{7}{2}$	$-\frac{15}{4}$	$\frac{23}{8}=\frac{r}{2}$
	X^2	X	X^0	

Deci: $q=X^2+\frac{7}{2}X-\frac{15}{4}$, iar $\frac{r}{2}=\frac{23}{8}$ dă $r=\frac{23}{4}$.

4) $f=\hat{2}X^3+\hat{3}X^2+\hat{1}$, $g=\hat{3}X+\hat{1}$, $f,g\in\mathbb{Z}_5[X]$

Avem: $g=\hat{3}\left(X+\hat{2}\right)=\hat{3}\left(X-(-\hat{2})\right)=\hat{3}\left(X-\hat{3}\right)$ şi deci $f=\hat{3}\left(X-\hat{3}\right)q+r$ sau $\hat{2}f=\left(X-\hat{3}\right)q+\hat{2}r$.

Aplicăm schema lui Horner pentru $\hat{2}f$ şi $X-\hat{3}$. Avem:

	X^3	X^2	X	X^0
	$\hat{4}$	$\hat{1}$	$\hat{0}$	$\hat{2}$
$\hat{3}$	$\hat{4}$	$\hat{3}$	$\hat{4}$	$\hat{4}=\hat{2}r$
	X^2	X	X^0	

Deci: $q=\hat{4}X^2+\hat{3}X+\hat{4}$, iar $\hat{2}r=\hat{4}$, adică $r=\hat{2}$.

Probleme rezolvate

1. Utilizând schema lui Horner să se determine ordinul de multiplicitate al rădăcinii $a=2$ pentru polinomul $f=X^6-7X^5+15X^4-40X^2+48X-16$.

R. Se aplică repetat schema lui Horner (pentru fiecare cât). Avem:

	X^6	X^5	X^4	X^3	X^2	X	X^0
	1	-7	15	0	-40	48	-16
2	1	-5	5	10	-20	8	$0=r_1 \Rightarrow a=2$ rădăcină simplă
2	1	-3	-1	8	-4	$0=r_2 \Rightarrow a=2$ rădăcină dublă	
2	1	-1	-3	2	$0=r_3 \Rightarrow a=2$ rădăcină triplă		
2	1	1	-1	$0=r_4 \Rightarrow a=2$ rădăcină de ordin patru			
2	1	3	$5\neq 0 \Rightarrow a=2$ nu este rădăcină de ordin cinci				
	X^2	X	X^0				

Deci, $f=(X-2)^4\left(X^2+3X+5\right)$.

2. Se consideră polinomul $f=X^{60}+X^{40}+X^{20}+2$. Să se determine restul împărțirii acestui polinom prin polinomul $g=X\left(X^2-1\right)$.

R. Scriem teorema împărțirii cu rest pentru polinoamele f și g când avem: $f=X\left(X^2-1\right)q+r$, $\text{grad}(r)<\text{grad}(g)=3$. Deci $\text{grad}(r)$ este cel mult 2. Fie $r=aX^2+bX+c$. A determina acest rest revine la a găsi coeficienții *a*, *b*, *c*.

Din egalitatea de funcții polinomiale $f(x)=x\left(x^2-1\right)q(x)+ax^2+bx+c, \left(\forall\right)x\in\mathbb{R}$ rezultă prin particularizare următoarele ecuații în *a*, *b*, *c*:

– dacă $x=0$ avem: $f(0)=0\cdot q(0)+c=2$, adică $c=2$;

– dacă $x=1$ se obține $5=a+b+c$ sau $a+b=3$;

– dacă $x=-1$ găsim $5=a-b+c$ sau $a-b=3$.

Din ultimele două ecuații se obțin valorile $\boldsymbol{a=3, b=0}$. Așadar restul căutat este $\boldsymbol{r=3X^2+2}$.

3. Fie $f\in\mathbb{R}[X]$, grad$(f)\geq 2$. Să se determine restul împărțirii lui *f* prin polinomul X^2-1, dacă suma coeficienților termenilor de grad impar ai polinomului f este 3, iar suma coeficienților termenilor de grad par ai aceluiași polinom este – 5.

R. Din teorema împărțirii avem egalitatea $f=\left(X^2-1\right)q+aX+b$. (*)

Fie $f=a_0+a_1X+a_2X^2+\ldots+a_nX^n$ polinomul dat. Avem: $f(1)=a_0+a_1+a_2+\ldots+a_n$ și $f(-1)=a_0-a_1+a_2+\ldots+(-1)^n a_n$. De aici prin adunare și scădere rezultă egalitățile: $\dfrac{f(1)+f(-1)}{2}=a_0+a_2+a_4+\ldots$ și $\dfrac{f(1)-f(-1)}{2}=a_1+a_3+a_5+\ldots$.

Din ipoteză avem $\dfrac{f(1)+f(-1)}{2}=-5, \dfrac{f(1)-f(-1)}{2}=3$, (**).

Din (*) pentru $x=1$ rezultă $f(1)=a+b$, iar pentru $x=-1$ se deduce $f(-1)=-a+b$.

Cu acestea relațiile (**) dau $b=-5$ și $a=3$. Deci $r=3X-5$.

7. DESCOMPUNEREA ÎN FACTORI IREDUCTIBILI ÎN INELUL $K[X]$

1) Polinoame ireductibile

Reamintim că studiem inelul de polinoame de nedeterminată *X* cu coeficienți în corpul comutativ *K*, unde $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p, p \text{ prim}\}$.

Am văzut că dacă $f, g \in K[X]$, $g \neq 0$, atunci *f* se divide prin *g* (şi notăm $f \vdots g$) dacă există un polinom $q \in K[X]$, astfel încât $f = gq$ (se mai spune că *g* divide pe *f* şi scriem $g | f$). Polinomul *g* se mai spune că este un divizor (sau factor) al lui *f*, iar polinomul *f* este un multiplu al lui *g*.
Am găsit că pentru $f \in K[X]$, $X - a$ este factor al lui *f* dacă $f(a) = 0$ (teorema Bézout), adică dacă *a* este rădăcină a lui *f*.

Este imediat că pentru $f \in K[X], a \in K^*$ şi *af* sunt divizori ai lui $f\left(f = a\left(a^{-1}f\right); f = a^{-1}(af)\right)$. Cu aceasta putem formula următoarea:

> **Definiție.** Divizorii de forma *a* şi *af*, $a \in K^* = K - \{0\}$ se numesc **divizori improprii** ai lui *f*. Ceilalți divizori ai lui *f*, dacă există, se numesc **divizori proprii.**

Problema care ne interesează, în continuare, este de a vedea cum se scrie un polinom $f \in K[X]$ ca un produs de factori de un anumit tip. Vom formula o proprietate similară celei din $\mathbb{Z}$ în care orice număr întreg se exprimă ca produs de numere prime. Pentru clarificare formulăm următoarea:

> **Definiție.** Un polinom $f \in K[X]$ se numeşte **ireductibil peste corpul** K (sau încă **ireductibil în inelul** $K[X]$) dacă are gradul cel puțin unu şi dacă nu are divizori proprii.
>
> În caz contrar, el se numeşte **reductibil peste** *K* (sau încă **reductibil în** $K[X]$)
>
> *f* reductibil peste $K \Leftrightarrow (\exists) g, h \in K[X]$, grad($g$), grad($h$) ≥ 1, $f = gh$.

Am văzut că se pot construi polinoame şi pe structuri care nu sunt corpuri (de exemplu inele). Dacă luăm $K' \subset K$, K' cu aceleaşi legi de pe K, atunci se poate construi familia de polinoame $K'[X] \subset K[X]$.

În $K'[X]$ se pot defini analog relația de divizibilitate şi noțiunea de polinom ireductibil. Este posibil ca un polinom $f \in K'[X]$ să fie ireductibil în această mulțime, dar reductibil în $K[X]$.

Exemple. 1. $f = X - 1$ **este ireductibil în** $\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{R}[X], \mathbb{C}[X]$.

2. $f = X^2 - 3$ **este ireductibil în** $\mathbb{Z}[X], \mathbb{Q}[X]$, **dar reductibil în** $\mathbb{R}[X], \mathbb{C}[X]$, **deoarece** $f = \left(X - \sqrt{3}\right)\left(X + \sqrt{3}\right)$, **unde** $g = X - \sqrt{3}, h = X + \sqrt{3}$ **sunt polinoame din** $\mathbb{R}[X]$ **(şi respectiv** $\mathbb{C}[X]$**).**

3. Polinomul $f = X^2 + 1$ **este ireductibil în** $\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{R}[X]$, **dar este reductibil în** $\mathbb{C}[X]$, **deoarece** $f = (X - i)(X + i)$, **unde** $g = X - i, h = X + i \in \mathbb{C}[X]$.

Probleme rezolvate

1. Arătați că polinomul $f \in \mathbb{Z}[X], f = 6X^2 + 13X - 5$ **este reductibil peste** $\mathbb{Z}$.

R. Într-adevăr observăm că $f = (3X - 1)(2X + 5)$ unde factorii $3X - 1, 2X + 5$ sunt polinoame din acelaşi inel $\mathbb{Z}[X]$.

2. Arătați că polinomul $f = X^2 + 1 \in \mathbb{N}[X]$ **este ireductibil peste** $\mathbb{N}$**, dar este reductibil în** $\mathbb{C}[X]$.

R. Presupunem, prin absurd, că f ar fi reductibil peste $\mathbb{N}$. Deci există $g = aX + b$, $h = mX + n$, $a, b, m, n \in \mathbb{N}, a \neq 0, m \neq 0$, astfel încât $f = (aX + b)(mX + n)$.

De aici (după calcule): $X^2 + 1 = amX^2 + (an + bm)X + bn$.

Ținând cont de egalitatea a două polinoame, se obține sistemul: $\begin{cases} am = 1 \\ an + bm = 0 \\ bn = 1 \end{cases}$.

Din prima şi ultima ecuație rezultă $a = m = b = n = 1$, care însă nu verifică a doua ecuație. Deci nu există $g, h \in \mathbb{N}[X]$ cu $f = gh$.

În final polinomul $f = X^2 + 1$ este ireductibil în $\mathbb{N}[X]$.

Acest polinom însă este reductibil peste $\mathbb{C}$ deoarece $f = (X - i)(X + i)$.

3. Arătați că polinomul $f = X^2 - 5 \in \mathbb{Z}[X]$ **este ireductibil peste** $\mathbb{Z}$**, dar este reductibil peste** $\mathbb{R}$.

R. Presupunem că f ar fi reductibil peste $\mathbb{Z}$, deci ar admite o scriere de forma $f = (aX + b)(mX + n)$, $a, b, m, n \in \mathbb{Z}, a, m \neq 0$, sau după calcule $X^2 - 5 = amX^2 + (an + bm)X + bn$.

De aici rezultă sistemul $\begin{cases} am=1 \\ an+bm=0 \\ bn=-5 \end{cases}$, sistem care nu are soluții în $\mathbb{Z}$. Deci *f* este ireductibil peste $\mathbb{Z}$.

Cum $X^2-5=\left(X-\sqrt{5}\right)\left(X+\sqrt{5}\right)$, unde $X-\sqrt{5},\ X+\sqrt{5}\in\mathbb{R}[X]$, se deduce că *f* este reductibil peste $\mathbb{R}$.

4. Arătați că polinomul $f=\hat{2}X^2+\hat{3}X+\hat{1}\in\mathbb{Z}_4[X]$ este reductibil în inelul $\mathbb{Z}_4[X]$.

R. Ca *f* să fie reductibil, va trebui să arătăm că există $g=aX+b,\ h=cX+d,\ g,h\in\mathbb{Z}_4[X],\ a,\ c\neq\hat{0}$, astfel încât $f=gh\Leftrightarrow\hat{2}X^2+\hat{3}X+\hat{1}=acX^2+(ad+bc)X+bd$. De aici rezultă, sistemul: $\begin{cases} ac=\hat{2} \\ ad+bc=\hat{3} \\ bd=\hat{1} \end{cases}$

cu soluția $a=\hat{1},\ c=\hat{2},\ b=d=\hat{1}$. Deci $f=\left(X+\hat{1}\right)\left(\hat{2}X+\hat{1}\right)$, ceea ce arată că *f* este reductibil peste $\mathbb{Z}_4[X]$.

Altfel observăm că $f(\hat{3})=\hat{0}$ şi deci $f\,\vdots\,X+\hat{1}$ şi se aplică schema lui Horner pentru a găsi câtul $\hat{2}X+1$.

Următoarea propoziție precizează o clasă de polinoame ireductibile în $K[X]$.

Teoremă. Orice polinom de gradul unu cu coeficienți într-un corp comutativ este ireductibil.

Demonstrație. Imediat. ■

Rezultatul de mai jos este important pentru că asigură existența unei exprimări a unui polinom *f* în funcție de polinoame ireductibile. Mai precis are loc:

Teorema (de descompunere în factori ireductibili). Fie $f\in K[X]$. Atunci *f* se poate scrie ca un produs finit de polinoame ireductibile din inelul $K[X]$.

Demonstrație. Fie grad(*f*) = *n.* Dacă *f* este ireductibil, atunci teorema este demonstrată, numărul factorilor ireductibili din produs fiind egal cu 1. Dacă *f* este reductibil în *K*[*X*], atunci el se poate exprima sub forma unui produs de cel puțin două polinoame din *K*[*X*], iar pentru fiecare din acestea se raționează ca mai sus. Deoarece gradul fiecărui divizor pe care îl găsim scade, în final nu putem obține decât sau divizori proprii având gradele mai mici decât *n*, dar mai mari ca unu, sau divizori de gradul întâi despre care ştim (teorema precedentă) că sunt ireductibili. Numărul acestora este finit, deoarece suma gradelor lor este egală cu *n*. ■

Observație. Mai mult scrierea este unică (abstracție făcând, eventual de factori constanți).
Legătura între proprietatea de a avea divizori ireductibili şi proprietatea de a avea rădăcini în K pentru polinoamele din $K[X]$, K corp comutativ este dată de:

> **Teorema**. Fie K corp comutativ. Următoarele afirmații sunt echivalente:
> **1)** Orice polinom ireductibil din $K[X]$ are gradul unu.
> **2)** Orice polinom din $K[X]$ de grad mai mare sau egal cu unu are rădăcini în K.

Demonstrație. **1)** $\Rightarrow$ **2)** Fie $f \in K[X]$, $\text{grad}(f) \geq 1$. Conform teoremei precedente f se poate scrie ca un produs finit de factori ireductibili (de gradul unu).
Deci $f = (a_1 X + b_1)(a_2 X + b_2)...(a_k X + b_k)$.
Ori ecuația $a_i x + b_i = 0$, $i = \overline{1,k}$ are soluția $x = -b_i a_i^{-1} \in K$.
2) $\Rightarrow$ **1)** Fie $f \in K[X]$ polinom ireductibil. Conform cu **2)** există $a \in K$ astfel încât $f(a) = 0$, adică $X - a \mid f$. Cum $X - a$ are gradul unu şi f are numai divizori improprii rezultă $X - a = bf$, $b \in K - \{0\}$ sau $f = b^{-1}(X - a)$, iar de aici $\text{grad}(f) = 1$. ■
Remarcăm faptul că această teoremă afirmă numai echivalența celor două afirmații. Apare firesc întrebarea dacă există corpuri comutative K pentru care una din cele două afirmații este adevărată (rezultă, evident, şi cealaltă adevărată).

> **Definiție**. Un corp comutativ K se numeşte **algebric închis** dacă orice polinom $f \in K[X]$, $\text{grad}(f) \geq 1$ are în K cel puțin o rădăcină (adică dacă pentru K afirmația **2)** din teoremă este adevărată).

Corpul $\mathbb{Q}$ nu este algebric închis, deoarece, de exemplu, polinomul $X^2 - 3 \in \mathbb{Q}[X]$ nu are rădăcini în $\mathbb{Q}$; nici $\mathbb{R}$ nu este algebric închis, deoarece, de exemplu, polinomul $X^2 + 1 \in \mathbb{R}[X]$ nu are rădăcini în $\mathbb{R}$. Corpul $\mathbb{C}$ este algebric închis. Acest rezultat foarte important este cunoscut sub numele de **teorema fundamentală a algebrei**.
Avem:

> **Teorema** (**d'Alembert-Gauss**). Orice polinom cu coeficienți complecşi de grad mai mare sau egal cu unu are cel puțin o rădăcină în $\mathbb{C}$.

Până acum nu s-a găsit o demonstrație pur algebrică a acestei teoreme importante. Pentru demonstrația ei se utilizează aparatul analizei matematice.
Următoarea teoremă pune în evidență polinoamele ireductibile de grad mai mare sau egal cu doi dintr-un inel oarecare $K[X]$.

UN PIONIER AL MATEMATICII

C.F. GAUSS (1777 – 1855)

Matematician german

CONTRIBUȚII

- ***algebră (teorema fundamentală)***
- ***teoria numerelor***
- ***astronomie***

Teoremă. Fie $f \in K[X]$, $\text{grad}(f) \geq 2$.

1) Dacă *f* este ireductibil, atunci *f* nu are rădăcini în *K*.

2) Dacă $\text{grad}(f) \in \{2, 3\}$, condiția necesară de la **1)** este și suficientă, adică *f* este ireductibil $\Leftrightarrow f$ nu are rădăcini în *K*.

Vom preciza acum polinoamele ireductibile în principalele inele de polinoame: $\mathbb{C}[X]$ și $\mathbb{R}[X]$. Are loc următoarea:

Teoremă. 1) Un polinom $f \in \mathbb{C}[X]$ este **ireductibil**, dacă și numai dacă

$$f = aX + b,\ \ a, b \in \mathbb{C},\ a \neq 0$$

2) Un polinom $f \in \mathbb{R}[X]$ este **ireductibil**, dacă și numai dacă

$$f = aX + b,\ a,\ b \in \mathbb{R},\ a \neq 0$$

sau

$$f = aX^2 + bX + c,\ a,\ b,\ c \in \mathbb{R},\ a \neq 0,\ b^2 - 4ac < 0.$$

Demonstrație. 1) Fie $f \in \mathbb{C}[X]$ un polinom ireductibil. Deoarece $\text{grad}(f) \geq 1$, din teorema fundamentală a algebrei rezultă că *f* admite o rădăcină $x_0 \in \mathbb{C}$. Conform teoremei lui Bézout avem: $f = (X - X_0)g$, $g \in \mathbb{C}[X]$. De aici $g \mid f$ și cum *f* este ireductibil rezultă divizorul *g* este de forma *a* sau *af,* unde $a \in \mathbb{C}^*$. Dacă *g* ar fi de forma af atunci $f=(X-X_0)af$ sau $(f\neq 0)\,1=(X-x_0)a$, adică $X-x_0$ ar fi inversabil, adică ar avea gradul zero, fals.

Prin urmare $g=a\in\mathbb{C}^*$, adică $\text{grad}(f)=1$. Ori am văzut că toate polinoamele de grad unu sunt ireductibile.

2) Conform teoremei precedente, polinoamele de gradul unu şi cele de gradul doi care nu au rădăcini în $\mathbb{R}$ sunt ireductibile peste $\mathbb{R}$. Să arătăm că nu mai există altele.

Pentru aceasta arătăm că orice polinom ireductibil din $\mathbb{R}[X]$ de grad mai mare sau egal cu doi „se reduce" la un polinom de gradul doi fără rădăcini reale.

Fie deci $f\in\mathbb{R}[X]$ ireductibil, cu $\text{grad}(f)\geq 2$. Conform teoremei fundamentale a algebrei polinomul f are o rădăcină $x_0\in\mathbb{C}$. Să observăm că $x_0\notin\mathbb{R}$, conform cu teorema precedentă pct. **1)**. Prin urmare $x_0\in\mathbb{C}-\mathbb{R}$. Cum f are coeficienţi reali, va admite şi rădăcina complex conjugată $\overline{x}_0\in\mathbb{C}-\mathbb{R}$. Aplicând teorema lui Bézout, deducem că f se divide prin $g=(X-x_0)(X-\overline{x}_0)=X^2-(x_0+\overline{x}_0)X+x_0\overline{x}_0\in\mathbb{R}[X]$ în $\mathbb{C}[X]$. Deci $f=g\cdot h,\ h\in\mathbb{C}[X]$. Cum f este ireductibil, divizorul său h ar trebui să fie de forma a sau af, $a\in\mathbb{C}^*$. Dacă $h=af$, atunci din $f=gh$, ar rezulta $1=ag$, adică g ar fi inversabil şi deci de grad zero, contradicţie. Rămâne $h=a,\ a\in\mathbb{C}^*$ când $f=ag$ şi deci $\text{grad}(f)=2$, f având rădăcinile complex conjugate x_0 şi $\overline{x}_0$. ■

Aplicând teorema de descompunere în factori ireductibili şi teorema precedentă se obţine următoarea:

Teoremă. 1) Orice polinom $f\in\mathbb{C}[X]$, $f\neq 0$, f neinversabil, **se descompune în mod unic în factori liniari** în inelul $\mathbb{C}[X]$.

2) Orice polinom $f\in\mathbb{R}[X]$, $f\neq 0$, f neinversabil, se **descompune în mod unic în inelul $\mathbb{R}[X]$ într-un produs de factori liniari sau factori de gradul doi fără rădăcini reale.**

Exemple. 1. $f=X^2+2\in\mathbb{C}[X],\ f=(X-\sqrt{2}i)(X+\sqrt{2}i)$;

2. $f\in\mathbb{C}[X],\ f=X^2+X+1-i=(X-i)(X+i+1)$;

3. $f\in\mathbb{R}[X],\ f=X^2-3X+2=(X-1)(X-2)$;

4. $f\in\mathbb{R}[X],\ f=X^3-X^2-X-2=(X-2)(X^2+X+1)$.

Din această teoremă rezultă următoarele consecințe:

Corolar. Fie $f = a_0 + a_1X + ... + a_nX^n$, $a_n \neq 0$, $n \geq 1$ un polinom care are rădăcinile distincte $x_1, ..., x_n$.

Atunci $f = a_n(X - x_1)(X - x_2)...(X - x_n)$.

Exemple. 1. $f = 2X^2 + X - 1 \in \mathbb{Q}[X]$, **are rădăcinile** $x_1 = \frac{1}{2}$, $x_2 = -1$. **Deci** $f = 2\left(X - \frac{1}{2}\right)(X + 1)$;

2. $f = \sqrt{2}X^2 + \left(2\sqrt{2} + 1\right)X + 2 \in \mathbb{R}[X]$, **are rădăcinile** $x_1 = -\frac{\sqrt{2}}{2}$, $x_2 = -2$ **și deci** $f = \sqrt{2}\left(X + \frac{\sqrt{2}}{2}\right)(X + 2)$;

3. $f = 2iX^2 + (6 + i)X + 3 \in \mathbb{C}[X]$, **are rădăcinile** $x_1 = 3i$, $x_2 = -\frac{1}{2}$ **și deci** $f = 2i(X - 3i)\left(X + \frac{1}{2}\right)$.

Corolar. Dacă un polinom $f \in \mathbb{C}[X]$ cu gradul cel mult n se anulează pentru $n + 1$ valori distincte, atunci $f = 0$.

Demonstrație. Dacă $\text{grad}(f) = n \geq 1$, atunci $f = a(X - x_1)(X - x_2)...(X - x_n)$ se anulează în n valori distincte. Dacă în plus $f(x_{n+1}) = 0$, $x_{n+1} \neq x_k$, $k = \overline{1,n}$, atunci $a = 0$, adică $f = 0$.■

Probleme rezolvate

1. Să se descompună în factori ireductibili peste *K* polinomul *f*, în cazurile:

1) $f = X^4 + 1 \in \mathbb{Z}[X]$, $K = \mathbb{Z}$, $K = \mathbb{Q}$, $K = \mathbb{R}$, $K = \mathbb{C}$;

2) $f = X^4 + 3X^2 + 2 \in \mathbb{Z}[X]$, $K = \mathbb{Z}$, $K = \mathbb{Q}$, $K = \mathbb{R}$, $K = \mathbb{C}$;

3) $f = X^3 + X + \hat{3} \in \mathbb{Z}_5[X]$, $K = \mathbb{Z}_5$.

R. 1) Să observăm că $f = X^4 + 2X^2 + 1 - 2X^2 = \left(X^2 + 1\right)^2 - \left(\sqrt{2}X\right)^2 = \left(X^2 + \sqrt{2}X + 1\right)\left(X^2 - \sqrt{2}X + 1\right) =$

$= (X - x_1)(X - \overline{x}_1)(X - x_2)(X - \overline{x}_2)$, unde $x_1 = \frac{-1 - i}{\sqrt{2}}$, $x_2 = \frac{1 - i}{\sqrt{2}}$.

Polinomul *f* este ireductibil peste $\mathbb{Z}$ și peste $\mathbb{Q}$. Probăm că este ireductibil peste $\mathbb{Z}$. Cum *f* nu are rădăcini întregi sau raționale, el nu se poate scrie ca un produs dintre un factor de gradul întâi și altul de gradul trei. Scrierea lui *f* ca produs de două polinoame de gradul doi este $f = \left(X^2 + \sqrt{2}X + 1\right)\left(X^2 - \sqrt{2}X + 1\right)$. Dar cele două polinoame nu au coeficienții în $\mathbb{Z}$ (sau în $\mathbb{Q}$).

Altfel. Prin reducere la absurd. Dacă $f=\left(aX^2+bX+c\right)\left(\alpha X^2+\beta X+\gamma\right), a, b, c, \alpha, \beta, \gamma\in\mathbb{Z}$, atunci prin identificare sistemul obținut în numere întregi nu are soluții.

Polinomul *f* este reductibil peste $\mathbb{R}$ din scrierea $f=\left(X^2+\sqrt{2}X+1\right)\left(X^2-\sqrt{2}X+1\right)$, cei doi factori fiind din $\mathbb{R}[X]$. De asemenea aceşti doi factori fiind de gradul doi cu discriminantul $\left(\pm\sqrt{2}\right)^2-4=-2<0$, sunt ireductibili.

În fine *f* este reductibil peste $\mathbb{C}$, având descompunerea în factori ireductibili:

$$f=(X-x_1)(X-\overline{x}_1)(X-x_2)(X-\overline{x}_2).$$

2) Polinomul *f* admite scrierile: $f=\left(X^2+1\right)\left(X^2+2\right)=(X-i)(X+i)\left(X-i\sqrt{2}\right)\left(X+i\sqrt{2}\right)$.

De aici deducem că *f* este reductibil peste $K=\mathbb{Z}, K=\mathbb{Q}$ şi $K=\mathbb{R}$ având descompunerea în factori ireductibili $f=\left(X^2+1\right)\left(X^2+2\right)$.

Polinomul *f* este reductibil şi peste $K=\mathbb{C}$, când admite descompunerea în factori ireductibili $f=(X-i)(X+i)\left(X-i\sqrt{2}\right)\left(X+i\sqrt{2}\right)$.

3) Să observăm că $f(\hat{1})=\hat{0}$, adică $x=\hat{1}$ este rădăcină a polinomului *f* când avem: $f=\left(X-\hat{1}\right)\left(X^2+X+\hat{2}\right)=\left(X+\hat{4}\right)\left(X^2+X+\hat{2}\right)$.

Polinomul $g=X^2+X+\hat{2}$ este ireductibil în $\mathbb{Z}_5[X]$, deoarece are gradul doi şi nu are rădăcini în corpul $\mathbb{Z}_5$, pentru că: $g(\hat{0})=\hat{2}, g(\hat{1})=\hat{4}$, $g(\hat{2})=\hat{3}, g(\hat{3})=\hat{4}, g(\hat{4})=\hat{2}$.

Deci $f=\left(X+\hat{4}\right)\left(X^2+X+\hat{2}\right)\in\mathbb{Z}_6[X]$ reprezintă descompunerea lui *f* în factori ireductibili peste $\mathbb{Z}_5$.

2. Să se arate că polinomul $f=\hat{2}X^3+X^2+X+\hat{3}\in\mathbb{Z}_4[X]$ nu are nici o rădăcină în $\mathbb{Z}_4$, dar este reductibil în $\mathbb{Z}_4[X]$,

R. Se verifică prin calcul că $f(\hat{0}), f(\hat{1}), f(\hat{2}), f(\hat{3})\neq\hat{0}$

Punem $f=(aX+b)\left(cX^2+dX+e\right), a,b,c,d,e\in\mathbb{Z}_4$.

Dezvoltând în membrul drept şi apoi identificând găsim $a=\hat{2}, b=\hat{1}, c=d=e=\hat{3}$, ceea ce arată că $f=\left(\hat{2}X+\hat{1}\right)\left(\hat{3}X^2+\hat{3}X+\hat{3}\right)$ şi deci *f* este reductibil peste $\mathbb{Z}_4$.

3. Să se determine polinoamele *f* cu coeficienți reali care verifică relația $xf(x)=(x-3)f(x+1), (\forall)x\in\mathbb{R}$

R. Pentru $x=0$ relația devine $0=-3f(1)$. De aici $x=1$ este rădăcină a polinomului *f*. Punem $x=1$ în aceeaşi relație şi rezultă $f(1)=0=-2f(2)$, adică $x=2$ este rădăcină a lui *f*.

Dacă $x=2$, atunci relația devine $2f(2)=0=-f(3)$ şi deci $x=3$ este, de asemenea, rădăcină a lui *f*.

Dacă luăm $x=3$, relația dă $3f(3)=0=0\cdot f(4)$, adică 0 = 0, deci nici o informație despre o altă rădăcină a lui *f*. Din cele de mai sus $f(x)=x(x-1)(x-2)g(x)$, $g:\mathbb{R}\to\mathbb{R}$, funcție polinomială. Înlocuind această scriere a lui *f* în relație se obține după simplificarea prin $x(x-1)(x-2)$, $g(x)=g(x+1)$,

$(\forall)x\in\mathbb{R}$. Notăm $h(x)=g(x)-g(x+1)$. Dacă gradul lui h este n (de exemplu), atunci din $h(x)=0, (\forall)x\in\mathbb{R}$ rezultă h este funcția nulă și deci g este funcția constantă $g=k\in\mathbb{R}^*$.

Deci $\boldsymbol{f=kX(X-1)(X-2)}$.

4. Determinați parametrii reali *a, b* astfel încât polinomul *f* să se dividă prin polinomul *g* în cazurile:

1) $\boldsymbol{f=X^3+aX^2+6X+6,\ g=X^2-X-2}$**;**

2) $\boldsymbol{f=X^4+(a-1)X^3+(b+2)X^2+X+c-3,\ g=(X-1)^3}$**.**

R. 1) *Metoda* 1. Să observăm că împărțitorul se poate scrie, descompus în factori ireductibili peste $\mathbb{R}$ sub forma $g=(X-2)(X+1)$, ceea ce arată că – 1 și 2 sunt rădăcinile polinomului *g*.

Cum *f* se divide prin *g* rezultă că rădăcinile lui *g* trebuie să fie rădăcini și pentru *f*, adică:

$$\begin{cases} f(-1)=0 \\ f(2)=0 \end{cases} \text{ sau } \begin{cases} a-b+5=0 \\ 4a+2b+14=0 \end{cases}$$

sistem din care rezultă valorile lui *a* și *b*. Găsim ușor $a=-4, b=1$.

Metoda 2. (*Prin împărțire directă*). Efectuând împărțirea lui f la g avem $f=g(X+a+1)+$ $+(a+b+3)X+2a+8$.

Dar $f\,\vdots\, g$ și deci restul împărțirii trebuie să fie polinomul nul, adică $(a+b+3)X+2a+8=0\Leftrightarrow$ $\Leftrightarrow(a+b+3=0,\ 2a+8=0)\Leftrightarrow(a=-4,\ b=1)$.

Metoda 3. (*Metoda coeficienților nedeterminați*). Polinomul *f* se divide prin *g* dacă există $h\in\mathbb{R}[X]$ astfel încât *f* = *gh*. Trecând în această egalitate la grade rezultă $\text{grad}(f)(=\text{grad}(g\cdot h))=\text{grad}(g)+\ \text{grad}(h)$ sau $3=2+\text{grad}(h)$. Deci $\text{grad}(h)=1$. Se ia $f=X+\alpha$. Se identifică coeficienții lui *X* la aceeași putere și se obține un sistem în a, b, α.

Metoda 4. (*Schema lui Horner*). Se aplică schema lui Horner pentru *f* și $\boldsymbol{X-2}$ și apoi pentru cât și $X+1$.

	X^3	X^2	X	X^0
	1	a	b	6
2	1	$a+2$	$b+2a+4$	$4a+2b+14=0$
-1	1	$a+1$	$b+a+3=0$	

Sistemul $\begin{cases} 4a+2b+14=0 \\ b+a+3=0 \end{cases}$ are soluția $a=-4,\ b=1$.

2) Metoda de rezolvare *utilizează derivatele*. Remarcăm că împărțitorul *g* are rădăcina triplă *x* = 1. Dacă *f* se divide prin *g*, atunci *x* = 1 este rădăcină triplă și pentru *f*, adică $\begin{cases} f(1)=0 \\ f'(1)=0 \\ f''(1)=0 \\ f'''(1)\neq 0 \end{cases}$.

Calculăm derivatele formale ale polinomului f și avem: $D(f)=4X^3+3(a-1)X^2+2(b+2)X+1$, $D^2(f)=12X^2+6(a-1)X+2(b+2)$.

Prin urmare se obține sistemul: $\begin{cases} a+b+c=0 \\ 3a+2b+6=0 \\ 6a+2b+10=0 \end{cases}$ cu soluția $a=-\frac{4}{3}, b=-2, c=\frac{10}{3}$.

Observație. Se pot aplica și celelalte metode descrise la problema precedentă.

5. Să se arate că polinomul $f=\left(X+1\right)^{3n+2}+X+2, n\in\mathbb{N}$ se divide prin $g=X^2+3X+3$.

R. În încercarea de a găsi rădăcinile împărțitorului g constatăm că acestea sunt complexe $x_1, \overline{x_1}$. Trebuie arătat că $f(x_1)=f(\overline{x_1})=0$ pentru ca $f\,\vdots\, g$. Ori $f(x_1)$ sau $f(x_2)$ comportă niște calcule. De aceea vom proceda altfel. Vom considera α o rădăcină arbitrară a lui $g(x_1$ sau $\overline{x_1})$. Deci $\alpha^2+3\alpha+3=0$, (1). Vom arăta că $f(\alpha)=0$, ceea ce spune că f admite pe α ca rădăcină. Cum α este o rădăcină oarecare a lui g deducem că $f\,\vdots\, g$. Pentru a proba că $f(\alpha)=0$, utilizăm relația (1).

Avem: $f(\alpha)=(\alpha+1)^{3n+2}+\alpha+2=\left[(\alpha+1)^3\right]^n(\alpha+1)^2+\alpha+2=(\alpha^3+3\alpha^2+3\alpha+1)^n(\alpha+1)^2+$

$+\alpha+2=\left[\alpha(\alpha^2+3\alpha+3)+1\right]^n(\alpha+1)^2+\alpha+2=(\alpha+1)^2+\alpha+2=\alpha^2+3\alpha+3=0$.

6. a) Să se arate că polinomul $f=X^{6n-1}+X+1, n\in\mathbb{N}^*$ se divide prin polinomul $g=X^2+X+1$.

b) Pentru ce valori ale lui $n\in\mathbb{N}$, polinomul $f=(X+1)^n-X^n-1$ se divide prin polinomul $g=X^2+X+1$?

R. a) Se vede ușor că rădăcinile lui g sunt complex conjugate. Nu le determinăm efectiv. Arătăm că $f\,\vdots\, g$, probând că o rădăcină arbitrară a lui g este rădăcină și pentru *f*. Fie α o rădăcină a lui g.

Deci $\alpha^2+\alpha+1=0$, (1). Înmulțind cu $\alpha-1$ relația (1) rezultă: $\alpha^3-1=0$, (2).

Pentru a arăta că $f(\alpha)=0$ vom întrebuința relațiile (1) și (2). Avem:

$$f(\alpha)=\alpha^{6n-1}+\alpha+1=(\alpha^3)^{2n}\cdot\frac{1}{\alpha}+\alpha+1\overset{(2)}{=}\frac{1}{\alpha}+\alpha+1=\frac{1+\alpha^2+\alpha}{\alpha}\overset{(1)}{=}0.$$

Deci orice rădăcină a împărțitorului g este rădăcină și pentru *f*. Prin urmare *f* se divide prin g.

Observație. Trebuie observat că rădăcinile lui g sunt simple. Dacă g are rădăcini multiple acestea trebuie să fie rădăcini și pentru *f* cu cel puțin același ordin.

b) Fie α rădăcină oarecare a lui g. Deci avem relațiile: $\alpha^2+\alpha+1=0$, (1) și $\alpha^3=1$, (2).

Ca *f* să se dividă prin g trebuie ca $f(\alpha)=0$. Ori avem: $f(\alpha)=(\alpha+1)^n-\alpha^n-1=(-\alpha^2)^n-\alpha^n-1=$

$=(-1)^n\alpha^{2n}-\alpha^n-1$.

Cum $(-1)^n$ se discută după cum n este par sau impar, iar α^n după n de forma $3k, 3k+1, 3k+2, k\in\mathbb{N}$, vom lua n de una din formele: $6k, 6k+1, 6k+2, 6k+3, 6k+4, 6k+5, k\in\mathbb{N}$.

Cazul 1. $n=6k, k\in\mathbb{N}$. În acest caz $f(\alpha)=1-1-1=-1\neq 0$.

Deci $n=6k$ nu corespunde cerinței problemei.

Cazul 2. $n=6k+1, k\in\mathbb{N}$. Avem: $f(\alpha)=-\alpha^2-\alpha-1=-(\alpha^2+\alpha+1)=0$.

Deci pentru $n=6k+1, f\,\vdots\, g$.

Cazul 3. $n=6k+2, k\in\mathbb{N}$. Avem $f(\alpha)=(-\alpha^2)^{6k+2}-\alpha^{6k+2}-1=(\alpha^3)^{4k}\cdot\alpha^4-(\alpha^3)^{2k}\cdot\alpha^2-1=$

$=\alpha-\alpha^2-1=\alpha-(-\alpha)=2\alpha\neq 0$.

Cazul 4. $n=6k+3, k\in\mathbb{N}$. În acest caz $f(\alpha)=(-\alpha^2)^{6k+3}-\alpha^{6k+3}-1=-(\alpha^3)^{4k}\cdot\alpha^6-(\alpha^3)^{2k}\cdot\alpha^3-1=$ $=1-1-1=-1\neq 0$.

Cazul 5. $n=6k+4, k\in\mathbb{N}$. Avem $f(\alpha)=(-\alpha^2)^{6k+4}-\alpha^{6k+4}-1=-(\alpha^3)^{4k}\cdot\alpha^8-(\alpha^3)^{2k}\cdot\alpha^4-1=$ $=\alpha^2-\alpha-1=2\alpha^2\neq 0$.

Cazul 6. $n=6k+5, k\in\mathbb{N}$. În fine $f(\alpha)=(-\alpha^2)^{6k+5}-\alpha^{6k+5}-1=-(\alpha^3)^{4k}\cdot\alpha^{10}-(\alpha^3)^{2k}\cdot\alpha^5-1=$ $=-(\alpha^2+\alpha+1)=0$.

Deci şi pentru $n=6k+5, k\in\mathbb{N}, f\,\vdots\,X^2+X+1$.

În concluzie pentru $n\in\{6k+1, 6k+5\}$ polinomul *f* se divide prin X^2+X+1.

7. a) Să se arate că polinomul $f=(X-1)^{n+2}+X^{2n+1}, n\in\mathbb{N}$ se divide prin polinomul $g=X^2-X+1$.

b) Pentru ce valori ale lui *n* polinomul $f=(X-1)^n-X^n+1$ se divide prin $g=X^2-X+1$?

R. a) Arătăm că fiecare rădăcină α a lui *g* este rădăcină şi pentru *f*.

Fie α o rădăcină oarecare a lui *g*. Deci $\alpha^2-\alpha+1=0$, (1). De aici prin înmulțire cu $\alpha+1$ rezultă $\alpha^3+1=0$, (2). Acestea sunt cele două relații pe care le utilizăm pentru a proba că $f(\alpha)=0$.

Avem: $f(\alpha)=(\alpha-1)^{n+2}+\alpha^{2n+1}\overset{(1)}{=}(\alpha^2)^{n+2}+\alpha^{2n+1}=\alpha^{2n+1}\cdot\alpha^3+\alpha^{2n+1}=\alpha^{2n+1}(\alpha^3+1)\overset{(2)}{=}0$.

Deci *f* se divide cu *g*.

b) Se procedează analog punctului b) de la problema precedentă. Găsim $n\in\{6k+1, 6k+5, k\in\mathbb{N}\}$.

8. Să se arate că polinomul $f=X^{5n_1}+X^{5n_2+1}+X^{5n_3+2}+X^{5n_4+3}+X^{5n_5+4}, n_i\in\mathbb{N}$ este divizibil prin polinomul $g=X^4+X^3+X^2+X+1$.

R. Pentru rezolvare utilizăm teorema $f\,\vdots\,g \Leftrightarrow$ orice rădăcină a lui *g* este rădăcină şi pentru *f* cu acelaşi ordin de multiplicitate cel puțin ca şi pentru *g*.

Fie α rădăcină a lui *g*. Deci $\alpha^4+\alpha^3+\alpha^2+\alpha+1=0$, (1) care prin înmulțire cu $\alpha-1$ dă $\alpha^5-1=0$, (2).

Pentru a proba că $f(\alpha)=0$, utilizăm relațiile (1) şi (2) (Se arată uşor că rădăcinile ecuației $g(x)=0$ sunt simple).

Avem: $f(\alpha)=\alpha^{5n_1}+\alpha^{5n_2+1}+\alpha^{5n_3+2}+\alpha^{5n_4+3}+\alpha^{5n_5+4}=(\alpha^5)^{n_1}+(\alpha^5)^{n_2}\cdot\alpha+(\alpha^5)^{n_3}\cdot\alpha^2+$ $+(\alpha^5)^{n_4}\cdot\alpha^3+(\alpha^5)^{n_5}\cdot\alpha^4\overset{(2)}{=}1+\alpha+\alpha^2+\alpha^3+\alpha^4\overset{(1)}{=}0$.

Deci *f* se divide prin *g*.

9. Să se determine restul împărțirii polinomului $f=X^{20}+X^{19}+...+X^2+X+1$ la $X(X-1)^2$.

R. Conform teoremei împărțirii cu rest a polinoamelor avem:

$$X^{20}+X^{19}+...+X+1=X(X-1)^2q+aX^2+bX+c.$$

Trecând la funcții polinomiale asociate avem:

$$x^{20}+x^{19}+...+x+1=x(x-1)^2q(x)+ax^2+bx+c, (\forall)x\in\mathbb{R} \ (*).$$

Se face $x=0$ şi se obţine $c=1$. Punând acum $x=1$ rezultă: $21=a+b+c$, (1).
Se derivează egalitatea (*) şi apoi se face $x=1$, când avem:
$20x^{19}+19x^{18}+...+2x+1=(x-1)^2q(x)+2x(x-1)q(x)+x(x-1)^2q'(x)+2ax+b$, $210=2a+b$, (2).
Rezolvând sistemul format din (1) şi (2) găsim $a=190, b=-170$.

2) Divizibilitatea polinoamelor

Am văzut că dacă $f,g\in K[X]$, $g\neq 0$, atunci *f* se divide prin *g* dacă există $q\in K[X]$ astfel încât $f=gq$ (mai spune că *f* este multiplu de *g* sau că *g* este divizor al lui *f*). Deci *f* se divide prin *g* dacă şi numai dacă $r=0$ (acesta devine un criteriu prin care probăm că polinomul *f* se divide prin *g* – se face împărţirea celor două polinoame şi se constată că restul împărţirii este polinomul nul).
În cazul particular când $g=X-a$, atunci *f* se divide prin $X-a$, dacă şi numai dacă $f(a)=0$ (Bézout).

Exemple: 1. $f=X^2-1, g=X+1$. **Atunci** $f=(X+1)(X-1)$, **cu** $q=X-1$;

2. $f=X^3+1, g=X^2-X+1$. **Atunci** $f=(X^2-X+1)(X+1)$, **cu** $q=X+1$.

Pentru polinoamele numerice o proprietate de importanţă este următoarea:

Teoremă. Fie $f,g\in\mathbb{C}[X]$. Polinomul *f* este divizibil prin polinomul *g* dacă şi numai dacă orice rădăcină a polinomului *g* este rădăcină şi a polinomului *f* având şi pentru acesta un ordin de multiplicitate cel puţin egal cu cel pe care îl are pentru polinomul *g*.

Demonstraţie. Presupunem că *f* se divide prin *g*. Deci există $h\in\mathbb{C}[X]$ astfel încât $f=g\cdot h$. Presupunem că $x=a$ este rădăcină a polinomului *g*. Deci $f=(X-a)g_1$, $g_1\in\mathbb{C}[X]$ şi prin urmare $f=(X-a)g_1\cdot h$. De aici $X-a|f$, adică $x=a$ este rădăcină şi pentru polinomul *f*. Deci dacă *f* se divide prin *g*, atunci orice rădăcină a lui *g* este rădăcină şi pentru *f*.
Reciproc, să presupunem că oricare ar fi o rădăcină a polinomului *g*, aceasta este rădăcină şi a polinomului *f*. Atunci $X-a$, care este un factor ireductibil al lui *g*, va fi la fel şi pentru *f*. Deci toţi factorii liniari din descompunerea polinomului *g* vor fi prezenţi şi în descompunerea lui *f*. Dacă $x=a$ este o rădăcină multiplă de ordin *k* a polinomului *g*, atunci acesta va fi divizibil prin $(X-a)^k$. Înseamnă că polinomul *f* pentru a fi divizibil prin *g*, va trebui să fie divizibil şi prin $(X-a)^k$, adică să aibă pe $x=a$ rădăcină multiplă de ordin $p\geq k$.■

Exemplu. Să se determine parametrii reali *a, b, c* pentru care polinomul $f = X^3 + aX^2 + bX + c$ se divide cu polinomul $g = X^3 - 2X^2 + X$.

R. Împărțitorul are rădăcinile $x_1 = 0$ (rădăcină simplă) și $x_2 = 1$ (rădăcină dublă). Pentru ca *f* să se divide prin *g* se impune condiția ca aceste rădăcini să fie și pentru *f*.
Deci $f(0) = 0$, $f(1) = 0$ și $f'(1) = 0$. De aici obținem $a = -2, b = 1, c = 0$ și deci $f = g$. *Altfel*, cu schema lui Horner, aplicată de trei ori (pentru $x = 0$ și de două ori pentru $x = 1$).
***Altfel*, prin împărțirea directă se impune condiția ca restul $r = 0$.**

Proprietăți ale relației de divizibilitate

Fie K un **corp comutativ**. Vom prezenta în continuare unele proprietăți ale relației de divizibilitate.

> **P₁.** Relația divizibilitate este: 1) **reflexivă** (adică $f \mid f, (\forall) f \in K[X]$) și 2) **tranzitivă** (adică dacă $f \mid g$, $g \mid h$, atunci $f \mid h$, $f, g, h \in K[X]$).

Demonstrație. 1) Avem $f \mid f, (\forall) f \in K[X]$ deoarece $f = 1 \cdot f$.
2) Din $f \mid g$ se deduce că există $f_1 \in K[X]$ pentru care $g = f \cdot f_1$, (1)
Din $g \mid h$ se deduce că există $g_1 \in K[X]$ astfel încât $h = g \cdot g_1$, (2).
Din (1) și (2) rezultă $h = f \cdot f_1 \cdot g_1 = f(f_1 \cdot g_1)$. Cum $f_1, g_1 \in K[X]$ rezultă $f_1 \cdot g_1 \in K[X]$ și deci $f \mid h$.■

> **P₂.** Fie f, g_i, $i = \overline{1,m}$ polinoame din $K[X]$.
>
> Dacă $f \mid g_i, i = \overline{1,m}$, atunci $f \mid \sum_{i=0}^{m} q_i g_i$, cu $q_i \in K[X], i = \overline{1,m}$.

Demonstrație. Proprietatea spune că dacă un polinom *f* divide polinoamele $g_i, i = \overline{1,m}$, atunci *f* divide orice „combinație“ de aceste polinoame, adică $f \mid \sum_{i=0}^{m} q_i g_i$.

Într-adevăr din $f \mid g_i$ se deduce că există $f_i \in K[X]$ pentru care $g_i = f \cdot f_i, i = \overline{1,m}$.

Atunci $\sum_{i=0}^{n} q_i g_i = \sum_{i=0}^{m} q_i f \cdot f_i = f \left(\sum_{i=0}^{m} q_i f_i \right)$. Din această relație și din faptul că $\sum_{i=0}^{m} q_i f_i \in K[X]$ rezultă că $f \mid \sum_{i=0}^{m} q_i g_i$. ■

P_3. Fie $f, g \in K[X]$, $f|g$ şi $g \neq 0$. Atunci $f \neq 0$ şi $\text{grad}(f) \leq \text{grad}(g)$.

Un divizor (*f*) al unui polinom nenul (*g*) este un polinom nenul de grad cel mult egal cu al polinomului.

Demonstraţie. Din $f|g$ rezultă că există $f_1 \in K[X]$ astfel încât $g = f \cdot f_1$. Evident $f \neq 0,\ f_1 \neq 0$ şi deci $\text{grad}(f) \geq 0,\ \text{grad}(f_1) \geq 0$.

Cum *K*[*X*] este domeniu de integritate avem din $f \cdot f_1 = g$, $\text{grad}(g) = \text{grad}(f) + \text{grad}(f_1)$, iar de aici $(\text{grad}(f_1) \geq 0)$ deducem $\text{grad}(f) \leq \text{grad}(g)$. ■

P_4. Fie $f, g \in K[X]$, $f \neq 0$, astfel încât $f|g$ şi $g|f$. Atunci există $a \in K$, $a \neq 0$, astfel încât $f = ag$.

Demonstraţie. Din $f \neq 0$ şi $g|f$ rezultă $g \neq 0$ şi există $g_1 \in K[X]$ astfel încât $f = gg_1$. Din $f|g$ rezultă că există $f_1 \in K[X]$ astfel încât $g = ff_1$. Din $f = gg_1$ şi $g = ff_1$ se obţine $f = ff_1g_1$ sau $(f \neq 0)$, $g_1f_1 = 1$. Trecând în această relaţie la grad rezultă $0 = \text{grad}(1) = \text{grad}(f_1) + \text{grad}(g_1)$.

Cum $f_1, g_1 \neq 0$ rezultă $\text{grad}(f_1), \text{grad}(g_1) \geq 0$, adică (via relaţia de mai sus) $\text{grad}(f_1) = \text{grad}(g_1) = 0$, ceea ce înseamnă că $f_1, g_1 \in K - \{0\}$.

Aşadar $f = g_1 \cdot g$ unde $g_1 = a \in K - \{0\}$. ■

Observaţii. 1) Această proprietate afirmă că dacă două polinoame se divid reciproc, atunci ele „diferă" printr-o constantă nenulă $a (f = ag)$ sau coincid abstracţie făcând de o constantă nenulă *a*..

2) Dacă *f* şi *g* au acelaşi coeficient dominant şi dacă $f|g$ şi $g|f$, atunci $f = g$.

Definiţie. Spunem că polinoamele $f, g \in K[X]$ **sunt asociate în divizibilitate** dacă $f|g$ şi $g|f$ (deci dacă se divid reciproc) şi scriem $f \sim g$.

Conform proprietăţii P_4, dacă $f \neq 0$, atunci *g* este asociat în divizibilitate cu *f* dacă şi numai dacă există $a \in K - \{0\}$ astfel încât $g = af$; dacă $f = 0$, atunci $g \sim f$ dacă şi numai dacă $g = 0$, caz în care $g = af$, este banal verificată.

P$_5$. Fie $f, g \in \mathbb{C}[X]$. Atunci $f \mid g$, dacă orice rădăcină a polinomului f (cu ordinul de multiplicitate respectiv) este rădăcină şi pentru polinomul g (cu acelaşi ordin de multiplicitate, cel puţin) .

Această proprietate este deosebit de utilă în problemele de divizibilitate a polinoamelor.

Probleme rezolvate

1. Să se determine parametrii reali *m, n, p* astfel încât polinomul *f* să se dividă prin polinomul *g*, în cazurile:

a) $f = X^3 + (m+1)X^2 - 2X + 3m,\ g = X + 1$;

b) $f = X^3 + (2n+1)X^2 + mX - m - n,\ g = (X-1)(X+1)$;

c) $f = X^4 + (m+n)X^3 + (m-1)X^2 + X + 1 + 2n,\ g = X^2 + 2X + 3$;

d) $f = X^4 + 5X^3 + mX^2 + nX + p + 1,\ g = \left(X^2 - 1\right)(X+2)$.

R. a) Polinomul f se divide prin polinomul $g = X - (-1)$ dacă restul împărţirii lui f la g este $r = 0$. Cum $r = f(-1)$ deducem $f(-1) = 4m + 2$. Din $f(-1) = 0$ rezultă $m = -\dfrac{1}{2}$.

b) *Metoda* 1 (*Metoda coeficienţilor nedeterminaţi*). Dacă f se divide prin g, atunci trebuie să aibă loc egalitatea $f = g(X + \alpha) \Leftrightarrow X^3 + (2n+1)X^2 + mX - m - n = X^3 + \alpha X^2 - X - \alpha$. De aici, prin identificare, rezultă sistemul: $\begin{array}{c|l} X^2 & 2n+1 = \alpha \\ X & m = -1 \\ X^0 & -m-n = -\alpha \end{array}$ cu soluţia $m = -1,\ n = -2,\ \alpha = -3.$

Metoda 2. Din P$_5$ rezultă că orice rădăcină a împărţitorului este rădăcină şi pentru deîmpărţit. În cazul nostru $x_1 = 1,\ x_2 = -1$ sunt rădăcinile împărţitorului. Aceste valori trebuie să fie rădăcini şi pentru f, adică $f(1) = 0,\ f(-1) = 0$. Acest sistem are soluţia $m = -1,\ n = -2$.

Metoda 3 (*Prin împărţire directă*). Aplicând algoritmul de împărţire a lui f prin g avem: $f = g(X + 2n + 1) + (m+1)X - m + n + 1$.

Polinomul f se divide prin g dacă restul $r = (m+1)X - m + n + 1$ este polinomul nul, adică dacă $m + 1 = 0$ şi $-m + n + 1 = 0$, ceea ce dă $m = -1,\ n = -2$.

Metoda 4 (*Schema lui Horner*). Se aplică de două ori schema lui Horner: o dată pentru f şi rădăcina $x = 1$ şi apoi pentru câtul obţinut şi rădăcina $x = -1$.

	X^3	X^2	X	X^0
	1	$2n+1$	m	$-m-n$
1	1	$2n+2$	$2n+m+2$	$n+2=0$
– 1	1	$2n+1$	$m+1=0$	

Găsim $n=-2, m=-1$.

c) Aplicăm algoritmul de împărțire celor două polinoame şi avem:

$$f = g\left[X^2+(m+n-2)X-m-2n\right]+(n-m+7)X+3m+8n+1$$

Condiția $g|f$ se traduce prin restul egal cu polinomul nul, adică $\begin{cases} n-m+7=0 \\ 3m+8n+1=0 \end{cases}$ cu condiția $m=5, n=-2$.

d) Rădăcinile împărțitorului fiind $x_1=-1,\ x_2=1,\ x_3=-2$ se impune condiția să fie rădăcini şi pentru deîmpărțit, adică $f(-1)=0,\ f(1)=0,\ f(-2)=0$ ceea ce conduce la sistemul:

$\begin{cases} m-n+p=3 \\ m+n+p=-7 \\ 4m-2n+p=23 \end{cases}$ cu soluția $m=5, n=-5,\ p=-7$.

2. Arătați că polinomul $f=nX^{n+1}-(n+1)X^n+1, n\in\mathbb{N}^*$ se divide la polinomul $g=(X-1)^2$ şi determinați câtul acestei împărțiri.

R. Vom aplica schema lui Horner de două ori: o dată pentru *f* şi rădăcina $x=1$ şi apoi pentru câtul obținut şi rădăcina $x=1$. Avem:

	X^{n+1}	X^n	X^{n-1}	X^{n-2}	...	X^2	X	X^0
	n	$-(n+1)$	0	0	...	0	0	1
1	n	-1	-1	-1	...	-1	-1	0
1	n	$n-1$	$n-2$	$n-3$	...	1	0	

Deci câtul la împărțirea lui *f* prin *g* este: $g=nX^{n-1}+(n-1)X^{n-2}+...+2X+1$.

3) Cel mai mare divizor comun a două polinoame. Algoritmul lui Euclid

Definițiile, teoremele şi chiar demonstrațiile de la această secțiune şi următoarea sunt similare celor de la divizibilitatea din $\mathbb{Z}$.

Fie *K* un corp comutativ.

Definiție. Fie $f,g\in K[X]$. Spunem că polinomul $d\in K[X]$ este **un cel mai mare divizor comun al polinoamelor** f,g dacă:

1) *d* este divizor comun pentru *f, g*, adică $d|f$ şi $d|g$;

2) orice alt divizor comun pentru *f* şi *g* îl divide pe *d,* adică $(\forall)d'\in K[X],\ d'|f,\ d'|g \Rightarrow d'|d$.

Cel mai mare divizor comun (c.m.m.d.c.) al polinoamelor *f, g* va fi notat cu (*f,g*).

Vom arăta că oricare ar fi două polinoame din $f,g\in K[X]$, există *c.m.m.d.c.* al lor şi-l vom construi efectiv prin aşa numitul **algoritm al lui Euclid**.

Pentru început prezentăm următoarea:

> **Lemă**. Dacă $f, g, q, r \in K[X]$ astfel încât $f = gq + r$, şi dacă există (g,r), atunci există (f,g) şi mai mult $(f,g) = (g,r)$.

Demonstrație. Fie $d = (g,r)$. Deci $d|g$, $d|r$ şi $d|gq + r$ (combinație de g şi r). Prin urmare $d|f$, adică d este un divizor pentru f şi g. Dacă d' este un alt divizor comun pentru f şi g, atunci avem $d'|f - gq$, adică $d'|r$. Deci d' este un divizor comun pentru g şi r. Cum $d = (g,r)$ rezultă $d'|d$. În final $d = (f,g)$. ■

> **Teoremă**. Orice două polinoame din $K[X]$ au un c.m.m.d.c.

Demonstrație. Fie $f, g \in K[X]$. Dacă $f = 0$, atunci $(0, g) = g$, deoarece $g|0$, $g|g$, iar dacă d' este un divizor pentru 0 şi g, atunci evident $d'|g$. Deci am arătat că $(0, g) = g$. Analog dacă $f \neq 0$, $g = 0$, $(f, 0) = f$.

Presupunem acum că $f \neq 0$ şi $g \neq 0$. Considerăm următorul lanț de împărțiri cu rest

$f = gq_1 + r_1$, $\quad \text{grad}(r_1) < \text{grad}(g)$

$g = r_1 q_2 + r_2$, $\quad \text{grad}(r_2) < \text{grad}(r_1)$

$r_1 = r_2 g_3 + r_3$, $\quad \text{grad}(r_3) < \text{grad}(r_2)$

....

$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}, \text{grad}(r_{n-1}) < \text{grad}(r_{n-2})$

$r_{n-2} = r_{n-1} q_n + 0.$

Să observăm că resturile obținute în împărțirile de mai sus au proprietatea $\text{grad}(r_1) > \text{grad}(r_2) > \cdots$.

Gradele sunt distincte două câte două şi aparțin mulțimii $\{0, 1, 2, ..., \text{grad}(r_1)\}$. Prin urmare în inegalitățile de mai sus cu grade întâlnim o egalitate care să aibă restul zero. Fie acesta $r_n = 0$.

Să arătăm că ultimul rest nenul r_{n-1} reprezintă cel mai mare divizor comun al polinoamelor f, g.

Aplicăm lema în mod repetat (de jos în sus în lanțul de relații) şi avem:

$$r_{n-1} = (r_{n-1}, 0) = (r_{n-2}, r_{n-1}) = (r_{n-3}, r_{n-2}) = ... = (r_1, r_2) = (g, r_1) = (f, g). \blacksquare$$

Prin urmare, date fiind două polinoame $f, g \in K[X]$, $f, g \neq 0$ (cazul interesant) pentru a determina c.m.m.d.c. al polinoamelor *f*, *g* se realizează lanțul de împărțiri cu rest de mai sus dacă $\text{grad}(f) \geq \text{grad}(g)$. Dacă $\text{grad}(g) \geq \text{grad}(f)$, atunci se inversează rolul lui *f* cu *g*.

Modul de a obține c.m.m.d.c. a două polinoame se numeşte **algoritmul lui Euclid**.

Să observăm că c.m.m.d.c. a două polinoame **este unic până la o asociere în divizibilitate**. În sensul că dacă $d = (f, g)$ şi $d' = (f, g)$, atunci $d \sim d'$, adică există $a \in K - \{0\}$, astfel încât $d = ad'$.

Într-adevăr din $d = (f, g)$ şi $d' | f$, $d' | g \Rightarrow d' | d$.

Analog din $d' = (f, g)$ şi $d | f$, $d | g \Rightarrow d | d'$. Acum din $d' | d$ şi $d | d' \Rightarrow d \sim d'$.

Observații. **1)** Dacă *f*, *g* sunt descompuse în factori ireductibili, atunci (f, g) se obține luând factori comuni la puterea cea mai mică (similar cu determinarea c.m.m.d.c a două numere naturale din aritmetică).

2) Dacă în lanțul de împărțiri o egalitate se înmulțeşte cu $a \in K - \{0\}$, atunci, în final c.m.m.d.c. nu se modifică, acesta fiind unic până la o constantă nenulă din *K*, adică $(f, g) = (af, ag)$, $(\forall) a \in K - \{0\}$.

3) Dacă $f_1, f_2, f_3 \in K[X]$ atunci se arată uşor că $(f_1, f_2, f_3) = ((f_1, f_2), f_3) = (f_1, (f_2, f_3))$ indicând astfel cum se determină cel mai mare divizor comun pentru trei polinoame. Analog se procedează şi pentru mai multe polinoame.

Corolar. Fie $f, g \in K[X]$, $d = (f, g)$. Atunci există $u, v \in K[X]$ astfel încât

$$d = uf + vg.$$

Această consecință a teoremei precedente afirmă că c.m.m.d.c. pentru polinoamele *f*, *g* se exprimă ca o combinație de ele. Demonstrația este imediată începând de jos în sus cu exprimarea ultimului rest nenul r_{n-1}.

Definiție. Fie $f, g \in K[X]$. Spunem că polinoamele *f* şi g sunt **prime între ele** dacă $(f, g) = 1$.

Ținând seama de corolarul precedent dacă două polinoame $f, g \in K[X]$ sunt prime între ele atunci există $u, v \in K[X]$ astfel încât $1 = uf + vg$.

O propoziție utilă în rezolvarea unor probleme cu polinoame este următoarea:

Teoremă. Fie $f, g \in K[X]$ astfel încât $f \mid gh$, $(f, g) = 1$. Atunci $f \mid h$.

Demonstrație. Cum $(f, g) = 1$, atunci există $u, v \in K[X]$ astfel încât $1 = uf + vg$. Înmulțind această relație cu h rezultă $h = ugh + vgh$. Deoarece $f \mid gh$, există $f_1 \in K[X]$ astfel încât $gh = ff_1$, iar egalitatea precedentă devine $h = ufh + vff_1$ sau $h = f(uf + vf_1)$. De aici $f \mid h$. ■

Să observăm că dacă $f, g \in \mathbb{Z}[X]$, atunci $(f, g) \in \mathbb{Z}[X]$; dacă $f, g \in \mathbb{Q}[X]$, atunci $(f, g) \in \mathbb{Q}[X]$.

Se demonstrează ușor următoarea:

Teoremă. Rădăcinile comune a două polinoame sunt rădăcinile celui mai mare divizor comun al lor (cu ordinele de multiplicitate respective).

Probleme rezolvate

1. Să se determine cel mai mare divizor comun al polinoamelor f, *g* în cazurile următoare:

1) $f = X^4 + X^3 - 7X^2 - X + 6,\ g = X^3 - X^2 - 4X + 4,\ f, g \in \mathbb{Z}[X]$;

2) $f = \frac{1}{3}X^3 - X^2 - \frac{1}{12}X + \frac{1}{4},\ g = \frac{1}{9}X^3 - \frac{1}{18}X^2 - X + \frac{1}{2},\ f, g \in \mathbb{Q}[X]$;

3) $f = X^3 + 2X^2 + X + 2,\ g = X^3 - iX^2 - 4X + 4i,\ f, g \in \mathbb{C}[X]$;

4) $f = X^3 + \hat{3}X^2 + \hat{4}X + \hat{2},\ g = X^2 + \hat{4}X^2 + X + \hat{1},\ f, g \in \mathbb{Z}_5[X]$.

R. 1) Aplicăm algoritmul lui Euclid și avem:

Prima împărțire.

$$\begin{array}{rr|l}
 & X^4 + X^3 - 7X^2 - X + 6 & X^3 - X^2 - 4X + 4 \\ \cline{3-3}
 & -X^4 + X^3 + 4X^2 - 4X\phantom{{}+6} & X + 2 \\ \cline{2-2}
 / & 2X^3 - 3X^2 - 5X + 6 & \\
 & -2X^3 + 2X^2 + 8X - 8 & \\ \cline{2-2}
 / & -X^2 + 3X - 2 &
\end{array}$$

A doua împărțire. Se împarte câtul $X^3 - X^2 - X + 4$ la noul rest $X^2 - 3X + 2$ (c.m.m.d.c. este unic până la o constantă nenulă din $\mathbb{Z}$ – deci se poate înmulți restul obținut $-X^2 + 3X - 2$ cu (–1)). Avem:

$$\begin{array}{rr|l}
 & X^3 - X^2 - 4X + 4 & X^2 - 3X + 2 \\ \cline{3-3}
 & -X^3 + 3X^2 - 2X\phantom{{}+4} & X + 2 \\ \cline{2-2}
 / & 2X^2 - 6X + 4 & \\
 & -2X^2 + 6X - 1 & \\ \cline{2-2}
 & /\quad\ /\quad\ / &
\end{array}$$

Cum ultimul rest nenul este X^2-3X+2, acesta reprezintă c.m.m.d.c. pentru *f, g*.

Observație. Dacă am fi descompus în factori ireductibili peste $\mathbb{Z}$, atunci $f=(X-1)(X-2)(X+1)$, $g=(X-1)(X-2)(X+2)$ și deci $(f,g)=(X-1)(X-2)=X^2-3X+2$.

2) Pentru că c.m.m.d.c. a două polinoame este unic până la o constantă, atunci în loc de f luăm $12f=4X^3-12X^2-X+3$, iar în locul lui g luăm $18g=2X^3-X^2-18X+9$.

Algoritmul lui Euclid este descris mai jos

Prima împărțire.

$$\begin{array}{rrrr|l}
4X^3 & -12X^2 & -X & +3 & 2X^3-X^2-18X+9 \\ \cline{5-5}
-4X^3 & +2X^2 & +36X & -18 & \mathbf{2} \\ \cline{1-4}
/ & -10X^2 & +35X & -15 &
\end{array}$$

A doua împărțire. Noul rest îl împărțim cu (– 5) și avem $2X^2-7X+3$ și continuăm algoritmul

$$\begin{array}{rrrr|l}
2X^3 & -X^2 & -18X & +9 & 2X^2-7X+3 \\ \cline{5-5}
-2X^3 & +7X^2 & -3X & & X+3 \\ \cline{1-3}
/ & 6X^2 & -21X & +9 & \\
 & -6X^2 & +21X & -9 & \\ \cline{2-4}
 & / & / & / &
\end{array}$$

Deci $(f,g)=2X^2-7X+3$.

Dacă am fi descompus în factori am fi obținut $12f=(2X-1)(2X+1)(X-3)$

$$18g=(2X-1)(X-3)(X+3)$$

și deci $(12f,18g)=(2X-1)(X-3)=2X^2-7X+3$.

3) Aplicăm algoritmul lui Euclid și obținem împărțirile cu rest de mai jos:

Prima împărțire.

$$\begin{array}{rrrr|l}
X^3 & +2X^2 & +X & +2 & X^3-iX^2-4X+4i \\ \cline{5-5}
-X^3 & +iX^2 & +4X & -4i & 1 \\ \cline{1-4}
/ & (2+i)X^2 & +5X & -2-4i &
\end{array}$$

A doua împărțire. Vom înmulți noul deîmpărțit $X^3-iX^2-4X+4i$ cu $(2+i)$ și apoi pentru $(2+i)X^3-(-1+2i)X^2-4(2+i)X+4(-1-2i)$ și $(2+i)X^2+5X+2-4i$ se continuă algoritmul.

Avem

$$\begin{array}{rrrr|l}
(2+i)X^3 & -(-1+2i)X^2 & -4(2+i)X & +4(-1+2i) & (2+i)X^2+5X+2-4i \\ \cline{5-5}
-(2+i)X^3 & -5X^2 & -(2-4i)X & & X-2 \\ \cline{1-3}
/ & -2(2+i)X^2 & -10X & +4(-1+2i) & \\
 & 2(2+i)X^2 & +10X & -4(-1+2i) & \\ \cline{2-4}
 & / & / & / &
\end{array}$$

Ultimul rest nenul este $(2+i)X^2+5X+2-4i$ şi acesta este c.m.m.d.c. al polinoamelor *f, g*. Dacă am fi descompus în factori ireductibili peste $\mathbb{C}$ am fi obținut:

$$f=(X-i)(X+i)(X+2),\ g=(X-i)(X+2)(X-2).$$

Aşadar $(f,g)=(X-i)(X+2)=X^2+(2-i)X-2i$, care este asociat în divizibilitate cu cel obținut mai sus pentru că $(2+i)\left[x^2+2(2-i)X-2i\right]=(2+i)X^2+5X+2-4i$.

4) Vom descompune în factori ireductibili peste $\mathbb{Z}_5$ polinoamele şi avem:

$$f=\left(X+\hat{1}\right)\left(X+\hat{3}\right)\left(X+\hat{4}\right),\ g=\left(x+\hat{2}\right)\left(X+\hat{3}\right)\left(X+\hat{4}\right).$$

Prin urmare $(f,g)=\left(X+\hat{3}\right)\left(X+\hat{4}\right)$.

Altfel aplicând algoritmul lui Eudid avem:

Prima împărțire.

$$\begin{array}{rl|l}
 & X^3+\hat{3}X^2+\hat{4}X+\hat{2} & X^3+\hat{4}X^2+X+\hat{4} \\ \cline{3-3}
 & -X^3-\hat{4}X^2-\ \ X-\hat{4} & \hat{1} \\ \cline{1-2}
/ & \hat{4}X^2+\hat{3}X+\hat{3} &
\end{array}$$

A doua împărțire. Înmulțim noul deîmpărțit $X^3+\hat{4}X^2+X+\hat{1}$ cu $\hat{4}$ şi continuăm împărțirile

$$\begin{array}{rl|l}
 & \hat{4}X^3+X^2+\hat{4}X+\hat{1} & \hat{4}X^2+\hat{3}X+\hat{3} \\ \cline{3-3}
 & -\hat{4}X^3-\hat{3}X^2-\hat{3}X & X+\hat{2} \\ \cline{1-2}
/ & \hat{3}X^2+\ \ X+\hat{1} & \\
 & -\hat{3}X^2-\ \ X-\hat{1} & \\ \cline{2-2}
 & /\qquad /\quad / &
\end{array}$$

Deci ultimul rest nenul reprezintă cel mai mare divizor comun al polinoamelor.

Aici $(f,g)=\hat{4}X^2+\hat{3}X+\hat{3}\sim\left(X+\hat{4}\right)\left(X+\hat{3}\right)$.

2. Să se arate că următoarele polinoame sunt prime între ele:

1) $\boldsymbol{f=4X^3+8X^2-X-2,\ g=X^2+X+1,\ f,g\in\mathbb{Z}[X]}$**;**

2) $\boldsymbol{f=X^3+X^2+\hat{3},\ g=X^2+\hat{2}X,\ f,g\in\mathbb{Z}_6[X]}$**.**

R. 1) Aplicăm algoritmul lui Eudid şi avem:

Prima împărțire.

$$\begin{array}{rl|l}
 & 4X^3+8X^2-\ \ X-2 & X^2+X+1 \\ \cline{3-3}
 & -4X^3-4X^2-4X & 4X+4 \\ \cline{1-2}
/ & 4X^2-5X-2 & \\
 & -4X^2-4X-4 & \\ \cline{2-2}
 & /\quad -9X-6=-3(3X+2) &
\end{array}$$

A doua împărțire. Noul deîmpărțit X^2+X+1 îl înmulțim cu 3, iar restul obținut îl împărțim prin (-3). Continuăm algoritmul cu împărțirea:

$$\begin{array}{r|l}
3X^2+3X+3 & 3X+2 \\ \cline{2-2}
-3X^2-2X & \boldsymbol{X} \\ \cline{1-1}
X+3 &
\end{array}$$

A treia împărțire. Noul rest $X+3$ îl înmulțim cu 3 şi avem

$$\begin{array}{r|l} 3X+9 & 3X+2 \\ \cline{2-2} \underline{-3X-2} & 1 \\ 7 & \end{array}$$

A patra împărțire.

$3X+2=7\left(\frac{3}{7}X+\frac{2}{7}\right)+0$.

Deci ultimul rest nenul este 1 şi reprezintă c.m.m.d.c. al polinoamelor *f, g*. Cum $(f,g)=1$, se deduce că polinoamele *f, g* sunt prime între ele. Dacă s-ar fi descompus în factori am fi obținut $f=(2X+1)(2X-1)(X+2)\in\mathbb{Z}[X]$, iar $g=X^2+X+1\in\mathbb{Z}[X]$ (este ireductibil peste $\mathbb{Z}$ cum uşor se poate vedea). Acum este clar că $(f,g)=1$.

2) Aici fiind vorba de $\mathbb{Z}_5$, căutăm eventuale rădăcini ale celor două polinoame în $\mathbb{Z}_5$. Avem $f(\hat{1})=\hat{0}, f(\hat{2})=\hat{0}$ şi se obține descompunerea $f=\left(X+\hat{4}\right)^2\left(X+\hat{3}\right)$. Pentru *g,* găsim $g(\hat{0})=\hat{0}, g(\hat{3})=\hat{0}$, când $g=X\left(X+\hat{2}\right)$. Ori este clar că $(f,g)=1$ şi deci *f* şi *g* sunt prime între ele.

Cu algoritmul lui Eudid am fi obținut acelaşi lucru după cum se vede mai jos:

Prima împărțire.

$$\begin{array}{r|l} X^3+X^2+\hat{3} & X^2+\hat{2}X \\ \cline{2-2} \underline{-X^3-\hat{2}X^2} & X+\hat{4} \\ \hat{4}X^2+\hat{3} & \\ \underline{-\hat{4}X^2+\hat{2}X} & \\ \hat{2}X+\hat{3} & \end{array}$$

A doua împărțire.

$$\begin{array}{r|l} X^2+\hat{2}X & \hat{2}X+\hat{3} \\ \cline{2-2} \underline{-X^2-\hat{4}X} & \hat{3}X+\hat{4} \\ /\quad \hat{3}X & \\ \underline{-\hat{3}X-\hat{2}} & \\ /\quad \hat{3} & \end{array}$$

A treia împărțire.

$$\begin{array}{r|l} \hat{2}X+\hat{3} & \hat{3} \\ \cline{2-2} \underline{-\hat{2}X} & \hat{4}X+\hat{1} \\ +\hat{3} & \\ \underline{-\hat{3}} & \\ / & \end{array}$$

Ultimul rest nenul este: $\hat{3}\sim\hat{1}$, ceea ce arată că $(f,g)=\hat{1}$.

Modalități de determinare a c.m.m.d.c.

Am indicat până acum două modalități de obținere a c.m.m.d.c. pentru două polinoame:
1) Descompunerea în factori a celor două polinoame şi formarea divizorului comun, luându-se factorii polinomiali comuni la puterile cele mai mici; metoda se poate aplica atunci când polinoamele se pot descompune uşor în factori.

Exemple. Să se determine (f,g) în cazurile:

1) $f = X^4 + X^2 - X^2 - X,\ g = X^5 - X^4 - X^3 + X^2,\ f,g \in \mathbb{Q}[X]$;

2) $f = X^4 + \hat{6}X^3 + \hat{6}X^2 + X,\ g = X^5 + X^4 + \hat{6}X^3 + \hat{6}X^2,\ f,g \in \mathbb{Z}_7[X]$.

R. 1) Descompunem în factori ireductibili cele două polinoame (peste $\mathbb{Q}$) şi avem:

$f = X(X-1)(X+1)^2,\ g = X^2(X-1)^2(X+1)$. Deci $(f,g) = X(X-1)(X+1)$.

În acest caz rădăcinile comune ale celor două polinoame sunt date de rădăcinile polinomului (f,g). Acestea sunt: $x_1 = 0,\ x_2 = -1,\ x_3 = 1$.

2) Avem $f = X\left(X+\hat{6}\right)^2\left(X+\hat{1}\right),\ g = X^2\left(X+\hat{6}\right)\left(X+\hat{1}\right)^2$, iar $(f,g) = X^3 + \hat{6}X$. Rădăcinile comune ale celor două polinoame sunt date de rădăcinile polinomului (f,g) şi acestea sunt: $x_1 = 0,\ x_2 = \hat{1},\ x_3 = \hat{6}$.

2) Algoritmul lui Euclid, în cazul în care prima metodă nu este aplicabilă şi nu se cunoaşte, apriori, gradul divizorului comun.
Indicăm în continuare o altă metodă de a obține c.m.m.d.c. a două polinoame numită:
3) Metoda scăderilor succesive, aplicabilă în cazul în care se cunoaşte de la început gradul divizorului comun, iar polinoamele luate în considerare nu sunt de grad prea mare. Să ilustram această metodă pentru polinoamele: $f = X^3 - 3X + 2$, $g = X^4 - 2X^3 + 2X^2 - 2X + 1$, dacă c.m.m.d.c. al lor este un polinom de gradul doi.
Ideea este următoarea: dacă $f = (X-a)f_1,\ g = (X-a)g_1$ sunt două polinoame al căror divizor comun este $X - a$, atunci construim polinomul $h = k_1 f \pm k_2 g$, care conține ca factor pe $X - a$.
De regulă pentru formarea lui h se aleg k_1, k_2 constante sau polinoame astfel încât polinomul h **să aibă gradul mai mic decât** $\text{grad}(f)$ sau $\text{grad}(g)$. În cazul de față, $h = g - Xf = -2X^3 + 5X^2 - 4X + 1$. Polinoamele h şi f au acelaşi divizor comun. Atunci construim polinomul $k = h + 2f = 5(X-1)^2$. Un divizor pentru h şi f este divizor şi pentru $h + 2f = k$. Evident $k \sim (X-1)^2$. Luăm atunci polinomul $k_1 = (X-1)^2$, $l = f - Xk_1 = 2(X-1)^2$.

Cum k_1 şi l au acelaşi divizor comun $(X-1)^2$ se deduce că acesta este divizor pentru f (din ultima relație), apoi pentru h (din $h + 2f = k$) şi în fine pentru g (din

$h = g - Xf$). Deci $(X-1)^2 \mid f$, $(X-1)^2 \mid g$. Cum ştim că c.m.m.d.c. al polinoamelor *f* şi *g* are gradul doi, acesta este chiar $(X-1)^2$. Deci $(f,g) = (X-1)^2$.

4) Cel mai mic multiplu comun

Fie *K* un corp comutativ. Are loc următoarea:

Definiție. Fie $f, g \in K[X]$. Spunem că polinomul *m* **este un cel mai mic multiplu comun al polinoamelor** *f, g* dacă

1) *m* este multiplu pentru *f, g* (adică $f \mid m$, $g \mid m$);

2) Orice alt multiplu comun m' pentru *f, g* este multiplu şi pentru *m* (adică, dacă $f \mid m'$, $g \mid m'$ atunci $m \mid m'$).

Cel mai mic multiplu comun al polinoamelor *f, g* se notează prin $[f,g]$.

Observații. 1) Dacă polinoamele *f, g* sunt descompuse în factori ireductibili, atunci $[f,g]$ se obține analog determinării c.m.m.m.c. a două numere naturale, luând produsul factorilor comuni şi necomuni, luați o singură dată, la puterea ce mai mare.

Exemple. 1. $f = X(X-1)^2$, $g = (X+1)^3(X-1)$. **Atunci** $[f,g] = X(X-1)^2(X+1)^3$.

2. $f = \left(X+\hat{1}\right)^2\left(X+\hat{2}\right)$, $g = X\left(X+\hat{1}\right)\left(X+\hat{3}\right)$, $f, g \in \mathbb{Z}_5[X]$. **Atunci** $[f,g] = X\left(X+\hat{1}\right)^2\left(X+\hat{2}\right)\left(X+\hat{3}\right)$.

2) Ca şi în teoria numerelor relația dintre polinoamele $f, g, (f,g)$ şi $[f,g]$ este dată de egalitatea $f \cdot g = (f,g)[f,g]$. De aici $[f,g] = \dfrac{fg}{(f,g)}$, egalitate care ne spune cum se poate determina $[f,g]$ dacă am calculat (f,g).

3) Pentru $f_1, f_2, f_3 \in K[X]$ se stabileşte uşor că avem: $[f_1, f_2, f_3] = [[f_1, f_2], f_3] = [f_1, [f_2, f_3]]$, precizând astfel cum se determină cel mai mic multiplu comun pentru trei polinoame. Analog se procedează pentru mai multe polinoame.

8. RĂDĂCINI ALE POLINOAMELOR. RELAȚIILE LUI VIÈTE

1) Polinoame cu coeficienți reali

Pentru polinoamele cu coeficienți reali următorul rezultat (fără demonstrație) este important.

Teoremă. Fie $f \in \mathbb{R}[X],\ f \neq 0$. Dacă $x_0 = a + ib,\ b \neq 0$ este o rădăcină, complexă a lui *f,* atunci:

1) $\overline{x_0} = a - ib$ este, de asemenea, o rădăcină complexă a lui *f*;

2) x_0 şi $\overline{x_0}$ au acelaşi ordin de multiplicitate.

Am văzut că pentru $f \in \mathbb{R}[X]$ şi $x_0 \in \mathbb{C} - \mathbb{R}$, avem $f\left(\overline{x_0}\right) = \overline{f\left(x_0\right)}$, ceea ce arată că dacă x_0 este rădăcină a lui *f,* atunci $\overline{x_0}$ este de asemenea, rădăcină a lui *f.*

Din teoremă rezultă că, dacă *f* **este un polinom cu coeficienți reali** care are o rădăcină complexă $x_0 = a + ib,\ b \neq 0$, atunci mai are ca rădăcină şi conjugata $\overline{x_0} = a - ib$ şi cele două rădăcini au acelaşi ordin de multiplicitate Dacă x_0 este o rădăcină simplă, atunci polinomul *f* se divide prin $X - x_0$. Cum şi $\overline{x_0}$ este de asemenea rădăcină rezultă, că *f* se divide şi prin $X - \overline{x_0}$.

Deci *f* se divide prin $\left(X - x_0\right)\left(X - \overline{x_0}\right) = (X - a - ib)(X - a + ib) = (X - a)^2 - (ib)^2 =$
$= X^2 - 2aX + a^2 + b^2$.

Din teoremă rezultă următorul:

Corolar. 1) Orice polinom cu coeficienți reali are un număr par de rădăcini complexe (care nu sunt reale).

2) Orice polinom cu coeficienți reali de grad impar are cel puțin o rădăcină, reală.

Am văzut că în mulțimea $\mathbb{R}[X]$ singurele polinoame ireductibile sunt cele de gradul întâi $aX + b,\ a, b \in \mathbb{R},\ a \neq 0$ precum şi cele de gradul al doilea $aX^2 + bX + c,\ a, b, c \in \mathbb{R}$, $a \neq 0,\ b^2 - 4ac < 0$.

Ținând seamă de teorema de descompunere în factori ireductibili avem următoarea:

Teoremă. Orice polinom $f = a_0 + a_1 X + ... + a_n X^n,\ a_n \neq 0$ se poate scrie ca un produs de polinoame de gradul întâi sau doi cu coeficienți reali:

$$f = a_n\left(X - x_1\right)^{k_1} ... \left(X - x_i\right)^{k_i}\left(X^2 + b_1 X + c_1\right)^{l_1} ... \left(X^2 + b_p X + c_p\right)^{l_p},$$

unde $b_s^2 - 4c_s < 0,\ s = \overline{1, p}$.

Probleme rezolvate

1. Să se determine parametrii reali m, n dacă polinomul $f = X^4 - 3X^3 + mX^2 - (n+2)X + 1$ are rădăcina complexă $x_0 = 1 - i$.

R. Cum polinomul $f \in \mathbb{R}[X]$, atunci odată cu rădăcina complexă $x_0 = 1 - i$ va admite şi rădăcina complex conjugată $\overline{x_0} = 1 + i$.

Prin urmare *f* se divide prin produsul $(X - x_0)(X - \overline{x_0}) = (X - 1 + i)(X - 1 - i) = X^2 - 2X + 2$.

Efectuând împărțirea lui *f* prin $X^2 - 2X + 2$, se impune condiția ca restul să fie polinomul nul. Avem: $f = (X^2 - 2X + 2)(X^2 - X + m - 4) + (2m - n - 8)X - 2m + 9$.

Deci $(2m - n + 8)X - 2m + 9 = 0 \Leftrightarrow (2m - n - 8 = 0 \text{ şi } -2m + 9 = 0)$ când $m = \frac{9}{2}, n = 1$.

2. Fie $f, g \in \mathbb{R}[X]$. Dacă $f(X^3) + Xg(X^3)$ se divide prin $X^2 + X + 1$, atunci *f* şi *g* au rădăcina 1.

R. Fie α rădăcină a ecuației $x^2 + x + 1 = 0$. Deci $\alpha^2 + \alpha + 1 = 0$ şi $\alpha^3 = 1$. Atunci $\alpha \in \left\{\frac{-1 - i\sqrt{3}}{2}, \frac{-1 + i\sqrt{3}}{2}\right\}$. Considerăm $\alpha = \frac{-1 + i\sqrt{3}}{2}$ (analog se tratează celălalt caz). Deci α este zero al funcției polinomiale $x \to f(x^3) + xg(x^3)$, adică $f(\alpha^3) + \alpha g(\alpha^3) = 0 \Leftrightarrow f(1) + \frac{-1 + i\sqrt{3}}{2} g(1) = 0 \Leftrightarrow$ $\Leftrightarrow 2f(1) - g(1) + i\sqrt{3}g(1) = 0 \Leftrightarrow (2f(1) - g(1) = 0,\ g(1) = 0)$. De aici $f(1) = g(1) = 0$, ceea ce arată că polinoamele *f*, *g* au rădăcina comună $x = 1$.

3. Să se descompună în factori ireductibili peste $\mathbb{R}$ polinomul $f = X^4 + X^2 + 1$.

R. Factorii ireductibili ai unui polinom cu coeficienți reali sunt cei de gradul întâi şi de gradul al doilea cu coeficienți reali, cei de gradul al doilea având discriminantul negativ.

Observăm că $f = X^4 + 2X^2 + 1 - X^2 = (X^2 + 1)^2 - X^2 = (X^2 - X + 1)(X^2 + X + 1)$.

Cum fiecare din factorii de gradul al doilea $X^2 - X + 1, X^2 + X + 1$ are discriminantul negativ $(\Delta = -3)$, aceştia sunt factori ireductibili din $\mathbb{R}[X]$ pentru *f*.

4. Fie $f \in \mathbb{R}[X]$ care nu are nici o rădăcină reală. Arătați că funcția polinomială asociată are semn constant pe $\mathbb{R}$.

R. În acest caz *f* se scrie sub forma: $f = a(X - x_1)(X - \overline{x_1})(X - x_2)(X - \overline{x_2})....(X - x_k)(X - \overline{x_k})$ unde $x_1, ..., x_k \in \mathbb{C} - \mathbb{R}$.

Deci funcția polinomială este egală cu: $f(x) = a\prod_{i=1}^{k}(x - x_i)(x - \overline{x_i}) = a\prod_{i=1}^{k}\left[x^2 - (x_i + \overline{x_i})x + x_i\overline{x_i}\right]$.

Ori am văzut că $g(x) = x^2 - (x_i + \overline{x_i})x + x_i\overline{x_i} > 0, (\forall)x \in \mathbb{R}$, deoarece discriminantul trinomului este negativ. Aşadar $f(x)$ are semnul lui $a, (\forall)x \in \mathbb{R}$.

2) Polinoame cu coeficienți raționali

Cum $\mathbb{Q}[X] \subset \mathbb{R}[X]$, înseamnă că rezultatele stabilite referitoare la polinoamele cu coeficienți reali rămân valabile şi pentru polinoamele cu coeficienți raționali sau întregi. Teorema următoare precizează proprietăți specifice polinoamelor cu coeficienți raționali sau întregi.

Teoremă. Fie $f \in \mathbb{Q}[X]$, $f \neq 0$. Dacă $x_0 = a + \sqrt{b}$, $a, b \in \mathbb{Q}$, $b > 0$, $\sqrt{b} \notin \mathbb{Q}$ este o rădăcină pătratică a lui *f*, atunci

1) $\widetilde{x_0} = a - \sqrt{b}$ este, de asemenea, o rădăcină (numită conjugata pătratică a lui x_0) a lui *f*;

2) x_0, $\widetilde{x_0}$ au acelaşi ordin de multiplicitate.

Teorema afirmă că dacă polinomul $f \in \mathbb{Q}[X]$, are ca rădăcină pe $x_0 = a + \sqrt{b}$ (număr pătratic), atunci *f* are ca rădăcină şi pe $\widetilde{x_0} = a - \sqrt{b}$ (conjugatul pătratic al lui x_0), şi mai mult cele două rădăcini au acelaşi ordin de multiplicitate. Dacă x_0 este rădăcină simplă a lui *f*, atunci *f* se divide $X - x_0$. Cum şi $\tilde{x}_0$ este rădăcină simplă a lui *f* rezultă că *f* se divide şi cu $X - \tilde{x}_0$. Deci *f* se divide prin produsul $(X - x_0)(X - \tilde{x}_0) =$ $= \left(X - a - \sqrt{b}\right)\left(X - a + \sqrt{b}\right) = (X - a)^2 - \left(\sqrt{b}\right)^2 = X^2 - 2aX + a^2 - b$.

Probleme rezolvate

1. Să se determine parametrii raționali *m*, *n* dacă polinomul $f = X^4 - X^3 + mX^2 + 13X + n$ are rădăcina $x_0 = 3 + \sqrt{2}$.

R. Polinomul fiind cu coeficienți raționali odată cu rădăcina pătratică $x_0 = 3 + \sqrt{2}$, va admite şi rădăcina pătratică conjugată $\tilde{x}_0 = 3 - \sqrt{2}$. Prin urmare polinomul dat se divide prin:

$$(X - x_0)(X - \tilde{x}_0) = \left(X - 3 - \sqrt{2}\right)\left(X - 3 + \sqrt{2}\right) = (X - 3)^2 - \left(\sqrt{2}\right)^2 = X^2 - 6X + 7.$$

Efectuând împărțirea cu rest a lui *f* prin $X^2 - 6X + 7$ găsim restul $r = (6m + 116)X + n - 7m - 161$ care trebuie să fie polinomul nul. De aici $6m + 116 = 0$ şi $n - 7m + 161 = 0$ cu soluția $m = -\frac{58}{3}$, $n = \frac{77}{3}$.

2. Există polinoame $f \in \mathbb{Q}[X]$ de grad impar care să nu aibă rădăcini în $\mathbb{Q}$?

R. Da. Polinomul $f = X^3 - 2 \in \mathbb{Q}[X]$ nu are nici o rădăcină în $\mathbb{Q}$.

3. **Fie $f_n \in \mathbb{Q}[X], n \in N^*$, unde $f_n = 1 + \frac{X}{1!} + \frac{X(X+1)}{2!} + ... + \frac{X(X+1)...(X+n-1)}{n!}$. Să se arate că f_n are pe $-1,-2,...,-n$ ca rădăcini.**

R. Avem relația de recurență $f_{n+1} = f_n + \frac{X(X+1)...(X+n-1)(X+n)}{(n+1)!}$.

Facem demonstrația prin inducție matematică.

Pentru $n=1,\ f = 1 + \frac{X}{1!}$ și are ca rădăcină pe -1.

Presupunem că f_n are rădăcinile $-1,-2,...,-n$ și să demonstrăm că f_{n+1} are rădăcinile $-1,-2,...,-n,-n-1$.

Din ipoteza de inducție $f_n = a(X+1)(X+2)...(X+n), a \in \mathbb{Q}$.

Cum $f_n(0)=1$ rezultă $a = \frac{1}{n!}$. Deci $f_{n+1} = \frac{1}{n!}(X+1)(X+2)...(X+n) + \frac{X(X+1)...(X+n)}{(n+1)!}$ sau $f_{n+1} = \frac{1}{n!}(X+1)(X+2)...(X+n)\left(1+\frac{X}{n+1}\right)$ adică $f_{n+1} = \frac{(X+1)(X+2)...(X+n+1)}{(n+1)!}$, ceea ce arată că f_{n+1} are ca rădăcini pe $-1, -2, ..., -n, -n-1$.

3) Polinoame cu coeficienți întregi

Următorul rezultat vizează mulțimea $\mathbb{Z}[X]$ și ne oferă un mod de a descoperi rădăcinile raționale sau întregi ale unui polinom. Mai precis are loc următoarea:

Teoremă. Fie $f = a_0 + a_1X + ... + a_nX^n, a_n \neq 0,\ f \in \mathbb{Z}[X]$.

1) Dacă $x_0 = \frac{p}{q}$ (*p, q* numere prime între ele) este o **rădăcină rațională** a lui *f*, atunci:

a) *p* **divide termenul liber** (adică $p|a_0$);

b) *q* **divide coeficientul dominant al polinomului** *f* (adică $q|a_n$).

2) În particular, dacă $x_0 = p$ este o **rădăcină întreagă** a lui *f*, atunci p este **divizor al termenului liber** (adică $p|a_0$).

Demonstrație. **1)** Din $f(x_0) = 0$ rezultă egalitatea

$a_0 + a_1\left(\frac{p}{q}\right) + ... + a_n\left(\frac{p}{q}\right)^n = 0$ sau $a_0q^n + a_1pq^{n-1} + ... + a_np^n = 0$ sau încă $a_0q^n = -p\left(a_1q^{n-1} + ... + a_np^{n-1}\right)$. De aici se deduce $p|a_0q^n$ și cum $(p,q)=1$

rezultă că $p|a_0$. Tot din scrierea de mai sus rezultă $a_n p^n = -q\left(a_0 q^{n-1} + a_1 q^{n-2} + ...\right)$

şi deci $q|a_n p^n$. Dar $(p,q)=1$ şi deci $q|a_n$.

2) Rezultă din **1)** când $q=1$. ■

Teorema afirmă că pentru un polinom f cu coeficienți întregi, rădăcinile raționale posibile se află printre fracțiile $\frac{p}{q}$, unde p este un divizor (în $\mathbb{Z}$) al termenului liber a_0, iar q este un divizor (în $\mathbb{Z}$) al coeficientului dominant a_n al polinomului. În particular, dacă pentru $f \in \mathbb{Z}[X]$ se caută rădăcinile întregi, atunci acestea se află printre divizorii întregi ai termenului liber a_0.

$a_0 + a_1 X + ... + a_n X^n \in \mathbb{Z}[X]$

$p|a_0$ $\quad$ $q|a_n$

$x_0 = \frac{p}{q}$

$a_0 + a_1 X + ... + a_n X^n \in \mathbb{Z}[X]$

$p|a_0$

$x_0 = p \in \mathbb{Z}$

Probleme rezolvate

1. Determinați rădăcinile raționale ale polinomului $f = 12X^4 - 16X^3 + X^2 + 4X - 1$.

R. Polinomul având coeficienți întregi, căutăm soluții întregi printre divizorii întregi al lui -1. Aceştia sunt ± 1. Cu schema lui Horner (de exemplu) găsim că $x=1$ este rădăcină a lui *f*. În continuare căutăm rădăcini raționale ale lui *f* realizând fracții de forma $\frac{p}{q}$, unde *p* este divizor al lui (-1), deci $p \in \{\pm 1\}$, iar *q* este divizor întreg al coeficientului dominant 12, adică, $q \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$. Deci avem fracțiile $\pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{1}{4}, \pm\frac{1}{6}, \pm\frac{1}{12}$.

Aplicăm schema lui Horner pentru câtul rezultat din împărțirea lui *f* prin $X-1$. Pentru acest cât şi fracțiile de mai sus testăm care este rădăcină.

	X^4	X^3	X^2	X	X^0
	12	– 16	1	4	– 1
1	12	– 4	– 3	1	0; $x=1$ este rădăcină
$\frac{1}{2}$	12	2	– 2	0	$x=\frac{1}{2}$ este rădăcină
$-\frac{1}{2}$	12	– 4	0	$x=-\frac{1}{2}$ este rădăcină	

Ultimul cât $12X-4$ are rădăcina $x=\frac{1}{3}$.

Deci polinomul *f* are rădăcinile $x_1 = 1, x_2 = \frac{1}{2}, x_3 = -\frac{1}{2}, x_4 = \frac{1}{3}$.

2. Să se arate că nu există $f \in \mathbb{Z}[X]$ pentru care $f(1)=5$, $f(3)=8$.

R. Pentru $f \in \mathbb{Z}[X]$ şi $a \neq b$, $a,b \in \mathbb{Z}$ se verifică uşor că $f(a)-f(b) \vdots a-b$. Dacă, în cazul nostru, ar exista $f \in \mathbb{Z}[X]$, atunci $f(3)-f(1) \vdots (3-1)$ sau $8-5 \vdots 2$, fals.

3. Să se arate că, dacă polinomul $f \in \mathbb{Z}[X]$ are două rădăcini întregi de parități diferite, atunci $f(k)$ este par, $(\forall) k \in \mathbb{Z}$.

R. Fie $x_1 = 2p$, $x_2 = 2q+1$, $p,q \in \mathbb{Z}$ cele două rădăcini de parități diferite ale lui f.

Deci $f = (X-2p)(X-2q-1)g$, $g \in \mathbb{Z}[X]$.

Fie acum $k \in \mathbb{Z}$. Dacă luăm $k = 2m$, $m \in \mathbb{Z}$, atunci:

$$f(k) = (2m-2p)(2m-2q-1)g(k) = 2(m-p)(2m-2q-1)g(2m).$$

ceea ce arată că $f(k)$ este par.

Dacă luăm $k = 2m+1$, $m \in \mathbb{Z}$, atunci factorul $X-2q-1=2(m-q)$ din $f(k)$ este par şi deci $f(k)$ este la fel.

4. Să se arate că dacă polinomul $f \in \mathbb{Z}[X]$ ia valoarea unu pentru trei numere întregi, atunci *f* nu are nici o rădăcină întreagă.

R. Dacă $a,b \in \mathbb{Z}$, $a \neq b$ atunci $f(a)-f(b) \vdots a-b$, ceea ce se verifică uşor prin calcul.

Fie $f(a)=f(b)=f(c)=1$, $a,b,c \in \mathbb{Z}$. Presupunem, prin absurd, că există $x_0 \in \mathbb{Z}$ pentru care $f(x_0)=0$. Atunci $f(a)-f(x_0)=f(b)-f(x_0)=f(c)-f(x_0)=1$ şi deci 1 se divide prin $a-x_0$, $b-x_0$, $c-x_0$, ceea ce atrage cel puțin două, numere egale, să zicem, $a-x_0=b-x_0$, adică $a=b$, fals (*a, b, c* fiind diferite două câte două).

4) Relațiile lui Viète

Ultimul rezultat al acestui paragraf stabileşte legătura între coeficienții polinomului $f = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{C}[X]$, $a_n \neq 0$ şi rădăcinile sale $x_1, x_2, \ldots, x_n$. Mai precis are loc următoarea

Teoremă. Numerele complexe $x_1, x_2, \ldots, x_n$ sunt rădăcinile polinomului $f \in \mathbb{C}[X]$, $f = a_nX^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \ldots + a_1X + a_0$, $a_n \neq 0$, dacă şi numai dacă au loc relațiile (lui Viète):

$$\begin{cases} x_1 + x_2 + \ldots + x_n = -\dfrac{a_{n-1}}{a_n} \\ x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_2x_n + \ldots + x_nx_{n-1} = \dfrac{a_{n-2}}{a_n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_1x_2\ldots x_n = (-1)^n \dfrac{a_0}{a_n} \end{cases}$$

Demonstrație. Dacă $x_1, x_2, ..., x_n$ sunt rădăcinile polinomului f de grad n, atunci $f = a_n(X - x_1)(X - x_2)...(X - x_n)$ sau după efectuarea calculelor şi ordonarea termenilor după puterile descrescătoare ale lui X,

$$f = a_n\Big[X^n - (x_1 + x_2 + ... + x_n)X^{n-1} + (x_1x_2 + ... + x_1x_n + x_2x_3 + ... + x_2x_n + ... + x_{n-1}x_n)X^{n-2} + ... + (-1)^n x_1x_2...x_n\Big].$$

Cum $f = a_nX^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + ... + a_1X + a_0$, prin identificarea celor două polinoame rezultă relațiile dorite.

Reciproca este imediată. ■

Particularizăm acum acest rezultat pentru $f \in \mathbb{C}[X]$ în cazul în care $\text{grad}(f) \in \{2,3,4\}$.

- Dacă $f = aX^2 + bX + c,\ a \neq 0$, are rădăcinile x_1, x_2 atunci relațiile lui Viète sunt:

$$\begin{cases} x_1 + x_2 = -\dfrac{b}{a} \\ x_1x_2 = \dfrac{c}{a} \end{cases}.$$

- Dacă $f = aX^3 + bX^2 + cX + d,\ a \neq 0$, cu rădăcinile x_1, x_2, x_3, atunci relațiile lui Viète sunt:

$$\begin{cases} x_1 + x_2 + x_3 = -\dfrac{b}{a} \\ x_1x_2 + x_1x_3 + x_2x_3 = \dfrac{c}{a} \\ x_1x_2x_3 = -\dfrac{d}{a} \end{cases}.$$

- Dacă $f = aX^4 + bX^3 + cX^2 + dX + e,\ a \neq 0$, cu rădăcinile x_1, x_2, x_3, x_4, atunci relațiile lui Viète sunt:

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = -\dfrac{b}{a} \\ x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 = \dfrac{c}{a} \\ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = -\dfrac{d}{a} \\ x_1x_2x_3x_4 = \dfrac{e}{a} \end{cases}.$$

Observații. **1)** Relațiile a doua şi a treia sunt uneori convenabil să se scrie sub forma $x_1x_2 + x_3x_4 + (x_1 + x_2)(x_3 + x_4) = \dfrac{c}{a}$ şi respectiv $x_1x_2(x_3 + x_4) + (x_1 + x_2)x_3x_4 = -\dfrac{d}{a}$.

2) Relațiile lui Viète se dovedesc deosebit de importante pentru un polinom (determinarea: unor parametri din structura lui, a rădăcinilor) ori de câte ori se dă o relație (sau mai multe) între unele dintre rădăcinile polinomului. Practic ori de câte ori avem o informație despre rădăcinile unui polinom, acesteia i se atașează relațiile lui Viète.
Nu vom insista prea mult aici cu astfel de probleme deoarece le vom regăsi la rezolvarea ecuațiilor algebrice de grad superior.

Probleme rezolvate

1. Fie polinomul $f = X^3 + 2X^2 - 23X + m \in \mathbb{R}[X]$. Să se determine parametrul m și să se afle rădăcinile polinomului dacă $x_1^2 = x_2^2 + x_3^2$.

R. Fiind dată relația $x_1^2 = x_2^2 + x_3^2$ între rădăcinile polinomului, acesteia îi vom asocia relațiile lui Viète

$$\begin{cases} x_1 + x_2 + x_3 = -2 \\ x_1x_2 + x_1x_3 + x_2x_3 = -23 \\ x_1x_2x_3 = -m \end{cases}$$

În felul acesta avem un sistem de patru ecuații cu patru necunoscute (x_1, x_2, x_3, m).

Avem egalitatea $x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3)$ sau $\left(x_1^2 = x_2^2 + x_3^2\right)$.

$2x_1^2 = (-2)^2 - 2(-23)$, adică $x_1^2 = 25$. De aici $x_1 = \pm 5$.
Dacă $x_1 = 5$, atunci $x_2 + x_3 = -7,\ x_2x_3 = 12$, de unde $x_2 = -3,\ x_3 = -4$.
Din ultima relație Viète rezultă $m = -60$.

Dacă $x_1 = -5$, atunci $x_2 + x_3 = 3,\ x_2x_3 = -8$ când $x_2 = \dfrac{3-\sqrt{41}}{2},\ x_3 = \dfrac{3+\sqrt{41}}{2}$ și $m = -40$.

2. Fie x_1, x_2, x_3 rădăcinile polinomului $f = X^3 - 3iX^2 - 4X + 2i$.

a) Să se formeze polinomul de gradul al treilea în Y care are ca rădăcini pe $y_1 = x_1^2,\ y_2 = x_2^2,\ y_3 = x_3^2$.

b) Determinați rădăcinile x_1, x_2, x_3.

R. a) Pentru a forma polinomul în Y vor trebui calculate sumele
$S_1 = y_1 + y_2 + y_3,\qquad S_2 = y_1y_2 + y_1y_3 + y_2y_3,\qquad S_3 = y_1y_2y_3$.

Polinomul Y este $g = Y^3 - S_1Y^2 + S_2Y - S_3$.
Mai întâi scriem relațiile lui Viète pentru f și avem:

$$x_1 + x_2 + x_3 = 3i,\quad x_1x_2 + x_1x_3 + x_2x_3 = -4,\quad x_1x_2x_3 = -2i$$

Acum avem $S_1 = y_1 + y_2 + y_3 = x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) = -1$.

$S_2 = y_1y_2 + y_1y_3 + y_2y_3 = (x_1x_2)^2 + (x_1x_3)^2 + (x_2x_3)^2 = (x_1x_2 + x_1x_3 + x_2x_3)^2 - 2x_1x_2x_3(x_1 + x_2 + x_3) = 4,$

$S_3 = y_1y_2y_3 = (x_1x_2x_3)^2 = -4$.

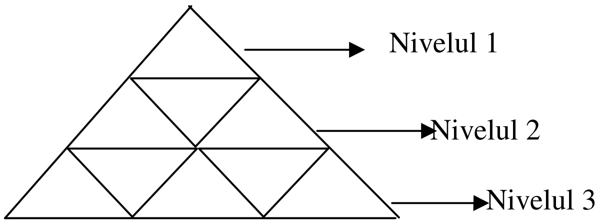
Deci: $g = Y^3 + Y^2 + 4Y + 4$.

b) Polinomul $g=(Y+1)(Y^2+4)$ are rădăcinile $y_1=-1, y_2=2i, y_3=-2i$. Deci $x_1^2=-1, x_2^2=2i, x_3^2=-2i$. Cum $-1=i^2, 2i=(1+i)^2, -2i=(1-i)^2$ deducem $x_1\in\{-i,i\}, x_2\in\{1+i,-1-i\}, x_3\in\{1-i,-1+i\}$. Verificând în ecuație găsim $x_1=i, x_2=1+i, x_3=-1+i$.

5) Polinoame în aplicații practice

1 (Căsătoria și polinoamele) Funcția $C(t)=3t+500$ (în €) modelează costul mediu al costumației mirilor, iar $N(t)=23t^2+125t+1000$ (în €) modelează costul mediu al nunții, unde $t=0$ reprezintă anul 2000 și $0\le t\le 10$.
Utilizând teorema restului stabiliți costul mediu al costumației, costul mediu al nunții în anul 2007 și anul 2010.
R. Anul 2007 corespunde la $t=7$. Obținem $C(7)=521$ € reprezintă costul mediu al costumației mirilor, iar $N(7)=2002$ € este costul mediu al nunții. Pentru anul 2010 se face $t=10$ și se calculează $C(10)$ și respectiv $N(10)$.

2 (Casă din cărți de joc și polinoame) Numărul de cărți necesar pentru a construi o casă din cărți de joc (figura alăturată) cu n nivele este dată de formula $C(n)=\frac{n}{2}(3n+1)$. Să se determine numărul de cărți necesar pentru a construi o astfel de casă cu $n=8$ nivele.



R. Se face $n=8$ și se calculează $C(8)=100$.

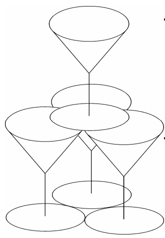
3 (Comitetul de elevi și polinoamele) O clasă de elevi trebuie să-și aleagă un șef de clasă, un adjunct și un casier. Numărul de moduri în care se poate face aceasta este dat de formula $P(n)=A_n^3=n^3-3n^2+2n$. Să se determine acest număr dacă în clasă sunt 20 elevi.

4 (Densitatea populației și polinoamele) Densitatea D a populației unui oraș (număr de persoane pe km^2) este legată de distanța x, în km, de la centrul orașului prin formula $D(x)=-30x^2+150x+500, 0<x<3$. Să se determine densitatea populației orașului la distanța de: 1) 1 km; 2) 2 km; 3) 3 km.

5 (Profitul și polinoamele) O companie de soft produce jocuri pe calculator. Conducerea companiei a determinat că profitul companiei, în €, de la fabricarea și vânzarea a x jocuri este dat de formula $P(x)=-0{,}00001x^3+78x-30.000, 0<x<3.000$. Care este profitul companiei dacă ea produce și vinde 20.000 de jocuri?

6 (Populația de gazele şi polinoamele) Un număr de 200 de gazele africane au fost aduse într-un parc pentru animale sălbatice. Populația de gazele după t ani este dată de formula $P(t) = -0{,}5t^3 + 12{,}3t^2 - 43{,}2t + 200,\ 0 < t \le 15$. Care este populația de gazele după: 1) 5 ani; 2) 10 ani?

7 (Piramida paharelor şi polinoamele) La o petrecere un grup de prieteni au construit o piramidă cu ajutorul paharelor. Primul rând de pahare aşezate pe masă sunt dispuse astfel încât să formeze un triunghi, iar cupele paharelor vecine sunt tangente. Următorul etaj de pahare se formează astfel: piciorul unui pahar se aşează pe zona delimitată de 3 pahare vecine (având cupele tangente) deja aşezate pe masă. Următorul etaj se construieşte în acelaşi mod.



Se ajunge la un etaj alcătuit din 3 pahare, iar deasupra acestora este etajul alcătuit dintr-un singur pahar (figura alăturată).
Considerând în sens invers nivelele: nivelul 1 format dintr-un pahar, nivelul 2 format din 3 pahare etc., găsim că numărul total de pahare dintr-o astfel de piramidă este dat de formula $P(k) = \frac{1}{6}\left(k^3 + 3k^2 + 2k\right)$, unde k este numărul de nivele ale piramidei. Care este numărul de pahare utilizate în piramidă, dacă acestea are: 1) 5 nivele; 2) 10 nivele?

9. ECUAȚII ALGEBRICE DE GRAD SUPERIOR

Definiție. Se numeşte **ecuație algebrică de necunoscută** x, o ecuație de forma $f(x) = 0$, unde f este un polinom nenul.

Gradul polinomului f dă gradul ecuației algebrice. Dacă $f = a_n X^n + a_{n-1} X^{n-1} + ... + a_0$ $a_n \ne 0$, atunci ecuația are gradul n, iar coeficienții $a_n, a_{n-1}, ..., a_0$ se numesc **coeficienții ecuației algebrice**. Dacă coeficienții sunt numere reale, atunci ecuația algebrică se spune că este cu coeficienți reali: dacă polinomul are coeficienți raționali, atunci ecuația se numeşte cu coeficienți raționali etc.
O ecuație care nu poate fi redusă la o ecuație algebrică prin operațiile de: adunare, înmulțire, ridicare la putere etc. se numeşte **ecuație transcendentă** (de exemplu ecuațiile: $\sin x = x^2 + x, \lg x + x - 1 = 0$). Noi ne vom ocupa în cele ce urmează de ecuații algebrice.

Definiție. Se spune că $a \in \mathbb{C}$ este **soluție** (sau **rădăcină**) a ecuației $f(x)=0$, dacă punând $x=a$ în ecuație, aceasta se verifică, adică $f(a)=0$.

Să observăm că dacă a este rădăcină a ecuației $f(x)=0$, atunci a este rădăcină şi pentru polinomul f şi reciproc. Prin urmare rezultatele stabilite pentru rădăcinile polinoamelor rămân valabile şi pentru ecuațiile algebrice definite de acestea.
A rezolva o ecuație algebrică înseamnă a-i determina soluțiile. Am văzut cum se rezolvă ecuațiile de gradul întâi ($ax+b=0, a\neq 0$), de gradul al doilea ($ax^2+bx+c=0,\ a\neq 0$). **Ecuațiile algebrice de grad superior vor fi acele ecuații algebrice având gradul mai mare sau egal cu trei**.
Pentru ecuația de gradul trei matematicianul italian Tartaglia a determinat formula de rezolvare, iar matematicianul italian Ferrari a determinat formula de rezolvare pentru ecuația de gradul patru (în secolul al XVI-lea).
Atât pentru ecuația de gradul trei cât şi pentru cea de gradul patru formulele care dau rădăcinile ecuațiilor se exprimă cu ajutorul radicalilor. Ecuațiile generale de grad strict mai mare decât patru nu pot fi rezolvate prin radicali (rezultat datorat matematicienilor H. Abel (norvegian) şi A. Ruffini). În continuare vom rezolva ecuații de grad mai mare decât patru în cazuri particulare (de fapt am rezolvat, deja, ecuații binome sau trinoame care au gradul mai mare decât patru).

1) Ecuații binome. Ecuații bipătrate

Reamintim din clasa a X-a, următoarele:

Definiții. 1) O ecuație de forma $z^n-a=0, n\in\mathbb{N}^*, n\geq 2, a\in\mathbb{C}$ se numeşte **ecuație binomă**.

2) O ecuație de forma $az^4+bz^2+c=0, a,b,c\in\mathbb{C}, a\neq 0, n\in\mathbb{N}^*$ se numeşte **ecuație bipătrată.**

Metodă de rezolvare pentru ecuația binomă. Se scrie ecuația sub forma $z^n=a$, iar numărul complex a se pune sub formă trigonometrică (a se vedea clasa a X-a) $a=r(\cos\alpha+i\sin\alpha)$, $\alpha\in[0,2\pi)$, $r=\sqrt{x^2+y^2}$ dacă $a=x+iy$. Are loc următoarea:

Teoremă. 1) Rădăcinile ecuației binome $z^n - a = 0$ sunt numerele complexe $z_k = \sqrt[n]{r}\left[\cos\left(\frac{\alpha + 2k\pi}{n}\right) + i\sin\left(\frac{\alpha + 2k\pi}{n}\right)\right]$, $k = \overline{0, n-1}$.

În particular, rădăcinile ecuației $z^n = 1$ se numesc **rădăcinile de ordin *n*** ale unității.

2) Imaginile geometrice ale rădăcinilor z_k, $k = \overline{0, n-1}$, sunt vârfurile unui poligon regulat cu n laturi înscris în cercul de centru O (originea reperului cartezian) şi de rază $\sqrt[n]{r}$ $\left(|z_k| = \sqrt[n]{r}\right)$.

În particular, imaginile geometrice ale rădăcinilor de ordin n ale unității sunt vârfurile unui poligon regulat înscris în cercul unitate (de centru O şi rază 1).

În Fig. 1 am reprezentat imaginile geometrice pentru $a = 1$ şi $n = 3$, $n = 4$.

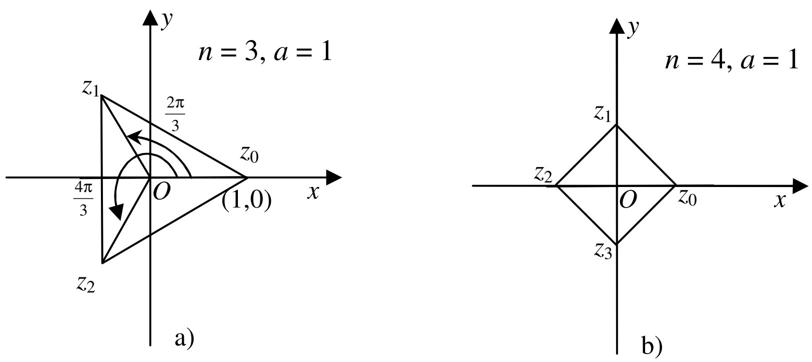


Fig.1

Exemplu. **Să se rezolve ecuațiile binome: 1) $z^5 = 1$; 2) $z^3 = \frac{1-i}{1+i}$.**

R. 1) Avem $1 = \cos 0 + i\sin 0$ şi deci *rădăcinile ecuației binome* (sunt rădăcinile de ordin 5 ale unității) *sunt*: $z_k = \cos\frac{2k\pi}{5} + i\sin\frac{2k\pi}{5}$, $k = \overline{0,4}$ sau scrise desfăşurat $z_0 = 1$, $z_1 = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$, $z_2 = \cos\frac{4\pi}{5} + i\sin\frac{4\pi}{5}$, $z_3 = \cos\frac{6\pi}{5} + i\sin\frac{6\pi}{5}$, $z_4 = \cos\frac{8\pi}{5} + i\sin\frac{8\pi}{5}$.

Imaginile geometrice ale acestor numere sunt vârfurile pentagonului regulat înscris în cercul unitate.

2) Observăm că $\frac{1-i}{1+i}=-i$, iar $-i=\cos\frac{3\pi}{2}+i\sin\frac{3\pi}{2}$. ***Soluțiile ecuației binome sunt*:**

$$z_k=\cos\left(\frac{\frac{3\pi}{2}+2k\pi}{3}\right)+i\sin\left(\frac{\frac{3\pi}{2}+2k\pi}{3}\right),\ k=0,1,2 \text{ sau explicitate } z_0=\cos\frac{\pi}{2}+i\sin\frac{\pi}{2}, z_1=\cos\frac{7\pi}{6}+i\sin\frac{7\pi}{6},$$

$z_2=\cos\frac{11\pi}{6}+i\sin\frac{11\pi}{6}$. **Imaginile geometrice ale acestor rădăcini sunt vârfurile unui triunghi echilateral înscris în cercul unitate ($|-i|=1$).**

Metodă de rezolvare pentru ecuația bipătrată. Se notează $z^2=y$ și se rezolvă ecuația $ay^2+by+c=0$. Se obțin soluțiile $y_1, y_2\in\mathbb{C}$. Se revine la substituție și se rezolvă ecuațiile binome $z^2=y_1,\ z^2=y_2$. Reuniunea acestor soluții constituie mulțimea de soluții a ecuației date.

Similar se rezolvă ecuația trinomă $az^{2n}+bz^n+c=0$.

Se notează $z^n=y$ și se obține ecuația $ay^2+by+c=0$ cu soluțiile $y_1, y_2\in\mathbb{C}$, după care se rezolvă ecuațiile binome $z^n=y_1,\ z^n=y_2$ etc.

Exemple. 1. Să se rezolve ecuațiile: a) $x^4-4x^2+3=0$; b) $x^6-2x^3-3=0$.

R. a) Se notează $x^2=y$ și avem $y^2-4y+3=0$, cu soluțiile $y_1=1,\ y_2=3$.

Revenind la substituție avem de rezolvat ecuațiile: $x^2=1,\ x^2=3$.

Prima ecuație are soluțiile $x_{1,2}=\pm1$, iar a doua ecuația are soluțiile $x_{3,4}=\pm\sqrt{3}$.

***Ecuația dată are soluțiile*: $\pm1, \pm\sqrt{3}$.**

b) Notăm $x^3=y$ și obținem ecuația $y^2-2y-3=0$ cu soluțiile $y_1=-1,\ y_2=3$.

Ecuațiile $x^3=-1,\ x^3=3$ dau soluțiile $x_k=\cos\left(\frac{\pi+2k\pi}{3}\right)+i\sin\left(\frac{\pi+2k\pi}{3}\right),\ k=0,1,2$ și respectiv

$$x'_k=\sqrt[3]{3}\left(\cos\frac{2k\pi}{3}+i\sin\frac{2k\pi}{3}\right),\ k=0,1,2.$$

***Ecuația dată are soluțiile*: $x_k,\ x'_k,\ k=0,1,2$.**

2. Să se determine natura rădăcinilor ecuației: $mx^4+2(m-1)x^2+m-2=0,\ m\in\mathbb{R}$.

R. Notăm $x^2=y$ și avem ecuația de gradul doi în $y: my^2+2(m-1)y+m-2=0$ pentru care $\Delta_y=1,\ P_y=\frac{m-2}{m},\ S_y=-\frac{2(m-1)}{m}$. Se rezolvă ecuațiile $x^2=y_1,\ x^2=y_2$.

Tabelul de discuție este cel de mai jos (funcție de semnul expresiilor Δ_y, P_y, S_y):

m	Δy	P_y	S_y	**Rădăcinile ecuației în y**	**Rădăcinile ecuației în x**
$m<0$	+	+	–	$y_1, y_2 \in \mathbb{R},\ y_1<0, y_2<0$	$x_i \in \mathbb{C},\ i=\overline{1,4}$
$m=0$	+	\	\	**Ecuația de gradul întâi:** $y+1=0$	$x_{1,2} \in \mathbb{C}$
$m \in (0,1)$	+	–	+	$y_1, y_2 \in \mathbb{R},\ y_1>0, y_2<0$	$x_{1,2} \in \mathbb{R}, x_{3,4} \in \mathbb{C}$
$m=1$	+	–	0	$y_1, y_2 \in \mathbb{R},\ y_1>0, y_2<0$	$x_{1,2} \in \mathbb{R}, x_{3,4} \in \mathbb{C}$
$m \in (1,2)$	+	–	–	$y_1, y_2 \in \mathbb{R},\ y_1>0, y_2<0$	$x_{1,2} \in \mathbb{R}, x_{3,4} \in \mathbb{C}$
$m=2$	+	0	–	$y_1, y_2 \in \mathbb{R},\ y_1=0, y_2<0$	$x_{1,2}=0, x_{3,4} \in \mathbb{C}$
$m>2$	+	+	–	$y_1, y_2 \in \mathbb{R},\ y_1<0, y_2<0$	$x_i \in \mathbb{C},\ i=\overline{1,4}$

2) Ecuații reciproce

Definiție. O ecuație de forma $a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0,\ a_n \neq 0$ pentru care $a_{n-i} = a_i$, $0 \leq i \leq n$ (termenii egali depărtați de extremi au coeficienții egali) se numește **ecuație reciprocă de gradul *n*.**

Iată forma ecuațiilor reciproce pe care le rezolvăm:

- $ax^3 + bx^2 + bx + a = 0,\ a \neq 0$, dacă $n=3$;
- $ax^4 + bx^3 + cx^2 + bx + a = 0,\ a \neq 0$, dacă $n=4$;
- $ax^5 + bx^4 + cx^3 + cx^2 + bx + a = 0,\ a \neq 0$ dacă $n=5$.

Metodă de rezolvare a euațiilor reciproce. Dacă gradul ecuației reciproce este *impar,* atunci ea admite soluția $x=-1$, iar rezolvarea acestei ecuații se reduce la rezolvarea ecuației $x+1=0$ (cu soluția $x=-1$) și a unei ecuații reciproce de grad par.

Rezolvarea ecuației reciproce de grad patru se face împărțind ecuația prin x^2 când obținem (se poate împărți prin x^2, deoarece $x=0$ nu este soluție a ecuației):

$$a\left(x^2 + \frac{1}{x^2}\right) + b\left(x + \frac{1}{x}\right) + c = 0, \qquad (1).$$

Acum se notează $x + \frac{1}{x} = y$ când $x^2 + \frac{1}{x^2} = y^2 - 2$ și (1) se scrie în funcție de y: $ay^2 + by + c - 2a =$ cu soluțiile y_1, y_2. Revenim la substituție și rezolvăm ecuațiile $x + \frac{1}{x} = y_1,\ x + \frac{1}{x} = y_2$. Toate soluțiile acestor ecuații sunt soluțiile ecuației date.

Probleme rezolvate

1. Să se rezolve ecuațiile reciproce :

a) $2x^3+3x^2+3x+2=0$ **; b)** $2x^4+7x^3+4x^2+7x+2=0$**; c)** $2x^5+3x^4+2x^3+2x^2+3x+2=0$**.**

R. a) Să observăm că este o ecuație reciprocă de grad impar.

Rezolvarea ei se reduce la rezolvarea ecuației $x+1=0$ (când $x=-1$) şi a unei ecuații (reciproce) de gradul al doilea. Pentru a găsi coeficienții acestei ecuații utilizăm schema lui Horner (coeficienții din ultima linie cu roşu sunt coeficienții căutați).

	x^3	x^2	x	x^0
	2	3	3	2
–1	2	1	2	0

Din schemă, rezultă ecuația $2x^2+x+2=0$ cu rădăcinile $\dfrac{-1\pm i\sqrt{15}}{4}$.

Ecuația dată are soluțiile: $-1, \dfrac{-1\pm i\sqrt{15}}{4}$.

b) Este o ecuație reciprocă de gradul patru. Tehnica de rezolvare a acesteia este de a împărți ecuația prin x^2, când avem:

$$2\left(x^2+\frac{1}{x^2}\right)+7\left(x+\frac{1}{x}\right)+4=0, \qquad (*).$$

Notăm $x+\dfrac{1}{x}=y$, iar de aici prin ridicare la pătrat $x^2+\dfrac{1}{x^2}=y^2-2$.

Ecuația (*) devine $2y^2+y=0$ cu soluțiile: $y_1=0,\ y_2=-\dfrac{7}{2}$.

Revenim la substituție şi avem ecuațiile $x+\dfrac{1}{x}=0,\ x+\dfrac{1}{x}=-\dfrac{7}{2}$ cu soluțiile $x_{1,2}=\pm i$ şi respectiv $\dfrac{-7\pm\sqrt{41}}{4}$. *Ecuația dată are soluțiile*: $\pm i, \dfrac{-7\pm\sqrt{41}}{4}$.

c) Ecuația propusă, este reciprocă de grad impar. Prin urmare rezolvarea ei se reduce la rezolvarea ecuației $x+1=0$ şi a unei ecuații reciproce de grad patru, ai cărei coeficienți se determină din schema lui Horner cerând că $x=-1$ să fie rădăcină a ecuației date.

	x^5	x^4	x^3	x^2	x	x^0
	2	3	2	2	3	2
– 1	2	1	1	1	2	0

Coeficienții din ultima linie a schemei (cu roşu) sunt coeficienții ecuației reciproce de gradul patru. Deci avem de rezolvat ecuația: $2x^4+x^3+x^2+x+2=0$.

Prin împărțire cu x^2 găsim $2\left(x^2+\dfrac{1}{x^2}\right)+\left(x+\dfrac{1}{x}\right)+1=0$, $\qquad$ (*).

Punem $x+\dfrac{1}{x}=y$, iar de aici $x^2+\dfrac{1}{x^2}=y^2-2$.

Cu acestea ecuația (*) devine $2y^2+y-3=0$ cu soluțiile $y_1=1, y_2=-\dfrac{3}{2}$.

Ecuațiile $x+\dfrac{1}{x}=1,\ x+\dfrac{1}{x}=-\dfrac{3}{2}$ au soluțiile $x_{1,2}=\dfrac{1\pm i\sqrt{3}}{2}$ și respectiv $x_{3,4}=\dfrac{-3\pm i\sqrt{7}}{4}$.

Ecuația dată are soluțiile: $-1,\ \dfrac{1\pm i\sqrt{3}}{2},\ \dfrac{-3\pm i\sqrt{7}}{4}$.

2. Să se rezolve ecuația $x^4-x^3-10x^2+2x+4=0$.

R. Fără a fi o ecuație reciprocă de gradul patru, utilizează pentru rezolvare o tehnică asemănătoare. Se împarte ecuația prin x^2 și se scrie sub forma $x^2+\dfrac{4}{x^2}-\left(x-\dfrac{2}{x}\right)-10=0$. Se notează $x-\dfrac{2}{x}=y$ etc.

Ecuația dată are soluțiile: $\dfrac{3\pm\sqrt{17}}{2},\ -1\pm\sqrt{3}$.

3) Ecuații în probleme practice

1 (Numărul de exemplare de ziar și ecuațiile). Valoarea V (în mii €) a unui ziar vândut în anul n este dată de formula $V(n)=n^3-6n^2+11n+4$. Deteminați anii în care valoarea vânzărilor a fost de 10 mii €.

R. Punând condiția $V(n)=10$ se ajunge la rezolvarea ecuației de gradul trei $n^3-6n^2+11n-6=0$. Soluțiile ei sunt $n_1=1,\ n_2=2,\ n_3=3$.

2 (Parapetul de protecție și ecuațiile) O furgonetă lovește parapetul de protecție de pe partea de deplasare determinând deformarea d (în cm) dată de formula: $d(t)=15t\left(t^3-6t-9\right)$, t fiind timpul exprimat în secunde. După câte secunde de la impact parapetul va reveni la poziția inițială?

R. Se impune condiția $d=0$, care conduce la rezolvarea ecuației $t^3-6t-9=0$. Se obține soluția (nebanală, $t>0$) $t=3$. Deci, după $t=3s$, deformarea este zero.

3 (Încălzirea planetei și ecuațiile). O planetă a Soarelui se încălzește. Temperatura T (în ^{0}C) a planetei după n milioane de ani este dată de formula $T(n)=10n^3-100n^2+270n-180$. După câți ani se va topi gheața de pe planetă? După câți ani va începe o nouă eră glaciară?

R. $T(n)=0\Rightarrow n=1$ milion de ani; $T(3)=0\Rightarrow$ după 2 milioane de ani.

4 (Topirea ghețarului și ecuațiile). Volumul unui ghețar tractat din Antartica spre Africa are volumul V după n zile, dat de formula $V=\dfrac{500\pi}{3}\left(2000-100n+20n^2-n^3\right)$. După câte zile se va topi complet ghețarul?

R. $V=0$ dacă $n=20$.

5 (Piscina şi ecuaţiile). O curte dreptunghiulară de 150 m lungime şi 80 m lăţime are în interior o piscină dreptunghiulară, având laturile paralele cu ale curţii şi situată la distanţa x de margini. Aria piscinei este egală cu aria porţiunii rămase din curte. Determinaţi valoarea lui x.

R. $(150-2x)(80-2x)=600 \Rightarrow x=\frac{35}{2}$.

6. O cutie are forma unui paralelipiped dreptunghic cu laturile $x, x+1, x+2$ (exprimate în m). Să se determine x astfel încât volumul cutiei să fie egal cu 24 m^3.

R. Volumul cutiei are expresia $V(x)=x(x+1)(x+2)$. Egalitatea $V(x)=24$ conduce la ecuaţia $x(x+1)(x+2)=24 \Leftrightarrow x^3+3x^2+2x-24=0$ cu unica soluţie reală $x=2$ m. Deci cutia are dimensiunile: 2 m, 3 m, 4 m.

7. Se consideră funcţia $f:\mathbb{R}\to\mathbb{R}, f(x)=4x^3+4x^2-x-1$. Să se determine punctele de intersecţie ale graficului funcţiei cu axa Ox.

R. Punctele graficului situate pe axa Ox au coordonaele $(x, f(x)=0)$. Ecuaţia $f(x)=0$ are soluţiile $x_1=-1, x_2=-\frac{1}{2}, x_3=\frac{1}{2}$. Deci punctele căutate sunt: $(-1,0)$, $\left(-\frac{1}{2},0\right)$, $\left(\frac{1}{2},0\right)$.

8. Să se rezolve inecuaţia $x^3+2\le x(2x+1)$.

R. Se aduce inecuaţia la forma $x^3-2x^2-x+2\le 0$ şi se consideră funcţia continuă $f:\mathbb{R}\to\mathbb{R}, f(x)=x^3-2x^2-x+2$. O astfel de funcţie păstrează semn constant pe un interval pe care nu se anulează. Vom determina valorile în care funcţia se anulează, rezolvând ecuaţia $f(x)=0$. Găsim soluţiile $x_1=-1, x_2=1, x_3=2$.

Tabelul de semn al funcţiei este:

x	$-\infty$		-1		1		2		$+\infty$
$f(x)$		$- - - - -$	0	$+ + + +$	0	$- - -$	0	$+ + + + +$	

De aici $f(x)\le 0$ dacă $x\in(-\infty,-1]\cup[1,2]$.

REZUMATUL CAPITOLULUI

Definiții. Proprietăți	Explicitare. Notații	Exemple
1) Inel Tripletul $(A,+\cdot)$ este inel unitar dacă: A_1) $(A,+)$ este grup comutativ; A_2) $(A,\cdot)$ este monoid; A_3) $\cdot$ este distributivă în raport cu $+$ Dacă în plus $\cdot$ este comutativă, atunci inelul este comutativ	A_1) $\begin{cases} G_1)\ + \text{ este asociativă} \\ G_2)\ + \text{ este comutativă} \\ G_3)\ + \text{ admite element neutru} \\ G_4) \text{ orice element din } A \text{ are un opus față de } + \end{cases}$ A_2) $\begin{cases} M_1)\ \cdot \text{ este asociativă} \\ M_2)\ \cdot \text{ admite element neutru} \end{cases}$ A_3) (D) $\begin{cases} x(y+z)=xy+xz \\ (x+y)z=xz+yz, (\forall)x,y,z\in A \end{cases}$ M_3) $\cdot$ este comutativă $xy=yx, (\forall)x,y\in A$	1) $(\mathbb{Z},+,\cdot)$ = inelul numerelor întregi 2) $(\mathcal{M}_n(\mathbb{C}),+,\cdot)$ = inelul matricelor pătratice de ordin *n*, $n\geq 2$, cu elemente din $\mathbb{C}$. 3) $(\mathbb{Z}_n,+,\cdot)$) inelul claselor de resturi modulo *n*, $n\in\mathbb{N}, n\geq 2$. 4) $(\mathbb{Z}[i],+,\cdot)$, $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$ este inelul întregilor lui Gauss.
Inelul integru (fără divizori ai lui zero)	$\left.\begin{matrix} xy=0 \\ x\neq 0 \end{matrix}\right] \Rightarrow y=0$	1) $(\mathbb{Z},+,\cdot),(\mathbb{Z}[i],+,\cdot)$ sunt inele integre 2) $(A,+,\cdot)$ unde $A=\{f:\{0,1\}\to\mathbb{R}\}$, este inel cu divizori ai lui zero. Într-adevăr, fie $f(0)=0, f(1)=1, f\neq 0$, $g(0)=1, g(1)=0, g\neq 0$. Atunci $fg=0$ $\big((fg)(0)=f(0)g(0)=0$ $(fg)(1)=f(1)g(1)=0\big)$; $(\mathbb{Z}_6,+,\cdot)$
2) Corp Tripletul $(K,+,\cdot)$ este corp dacă: K_1) $(K,+,\cdot)$ este inel unitar K_2) Orice element nenul din *K* este inversabil Dacă în plus $\cdot$ este comutativă, atunci copul este comutativ	K_1) K_2) $\begin{cases} (K,+) \text{ este grup abelian} \\ (K-\{0\},\cdot) \text{ este grup} \\ D)\cdot \text{este distributivă în} \\ \text{raport cu } + \end{cases}$	1) $(\mathbb{Q},+,\cdot)$ = corpul numerelor raționale 2) $(\mathbb{R},+,\cdot)$ = corpul numerelor reale 3) $(\mathbb{C},+,\cdot)$ = corpul numerelor complexe 4) $(\mathbb{Z}_p,+,\cdot)$, *p* prim, este corpul claselor de resturi modulo *p* 5) $(\mathbb{Q}(\sqrt{d}),+,\cdot), d\not\vert p^2, p\in\mathbb{Z}, p\neq 1$ $\mathbb{Q}(\sqrt{d})=\{a+b\sqrt{d} \mid a,b\in\mathbb{Q}\}$ corp pătratic
3) Morfisme de inele (corpuri) $(A,+,\cdot),(A',\oplus,\odot)$ inele (corpuri) $f:A\to A'$ este morfism de inele (corpuri) dacă:	1) $f(x+y)=f(x)\oplus f(y)$ 2) $f(x\cdot y)=f(x)\odot f(y), (\forall)x,y\in A$	$\left(A=\{x+y\sqrt{2} \mid x,y\in\mathbb{Z}\},+,\cdot\right)$, $\left(A'=\left\{\begin{pmatrix} x & y \\ 2y & x \end{pmatrix} \middle\vert x,y\in\mathbb{Z}\right\},+,\cdot\right)$ $f:A\to A'$, $f(x+y\sqrt{2})=\begin{pmatrix} x & y \\ 2y & x \end{pmatrix}$
4) Izomorfism de inele (corpuri) $f:A\to A'$ este izomorfism de inele	1) $\begin{cases} f(x+y)=f(x)\oplus f(y) \\ f(x\cdot y)=f(x)\odot f(y), (\forall)x,y\in A \end{cases}$	este morfism deoarece: 1) $f(z_1+z_2)=f(z_1)+f(z_2), z_1,z_2\in A$ $z_1=x_1+y_1\sqrt{2}, z_2=x_2+y_2\sqrt{2}\Rightarrow$

Definiții. Proprietăți	Explicitare. Notații	Exemple
(corpuri) dacă: **1) *f* este morfism;** **2) *f* este bijecție**	2) $\begin{cases} f \text{ este injectivă} \\ f \text{ este surjectivă} \end{cases}$	$\Rightarrow z_1+z_2 = x_1+x_2+(y_1+y_2)\sqrt{2} \Rightarrow$ $f(z_1+z_2)=\begin{pmatrix} x_1+x_2 & y_1+y_2 \\ 2(y_1+y_2) & x_1+x_2 \end{pmatrix}=$ $=\begin{pmatrix} x_1 & y_1 \\ 2y_1 & x_1 \end{pmatrix}+\begin{pmatrix} x_2 & y_2 \\ 2y_2 & x_2 \end{pmatrix}=f(z_1)+f(z_2)$ 2) $f(z_1z_2)=f(z_1)f(z_2), z_1,z_2 \in A$. $f(z_1z_2)=f(x_1x_2+2y_1y_2+(x_1y_2+x_2y_1)\sqrt{2})=$ $=\begin{pmatrix} x_1x_2+2y_1y_2 & x_1y_2+x_2y_1 \\ 2(x_1y_2+x_2y_1) & x_1x_2+2y_1y_2 \end{pmatrix}=$ $=\begin{pmatrix} x_1 & y_1 \\ 2y_1 & x_1 \end{pmatrix}\begin{pmatrix} x_2 & y_2 \\ 2y_2 & x_2 \end{pmatrix}=f(z_1)f(z_2)$.
5) Forma algebrică a unui polinom de nedeterminată *X* peste corpul *K*, $K \in \{\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}_p\}$, ***p* prim**	$f = a_0+a_1X+a_2X^2+...+a_nX^n =$ $= \sum_{i=0}^{n} a_iX^n$ **(ordonată după puterile crescătoare ale lui *X*)** $f = a_nX^n+a_{n-1}X^{n-1}+...+a_1X+a_0$ **(ordonat după puterile descrescătoare ale lui *X*)** $K[X]$ **= mulțimea polinoamelor de nedeterminată *X* cu coeficienți în *K*.** $f = a_0 \in K$ **, sunt polinoame constante.**	$f = \frac{1}{2}-3X^2+\frac{5}{3}X^3 \in \mathbb{Q}[X]$ $f = \sqrt{3}X^4-\frac{2}{3}X^2+X-\frac{1}{\sqrt{2}} \in \mathbb{R}[X]$ $f = \sqrt{3} \in \mathbb{R}[X]$, $f = \frac{1}{3} \in \mathbb{Q}[X]$, $f = 0 \in \mathbb{Z}[X]$
6) Gradul unui polinom	$\text{grad}(f) = \begin{cases} n, a_n \neq 0, a_i = 0, i \geq n \\ -\infty, f = 0 \end{cases}$ $\text{grad}(f+g) \leq \max\{\text{grad}(f),\text{grad}(g)\}$ $\text{grad}(fg) = \text{grad}(f)+\text{grad}(g)$	$f = 2X+X^3-3X^4$, $\text{grad}(f)=4$; $f = 5$, $\text{grad}(f)=0$; $f = 0$, $\text{grad}(f)=-\infty$.
7) Valoarea unui polinom într-un punct	$f = a_0+a_1X+a_2X^2+...+a_nX^n$, $\alpha \in K \Rightarrow f(\alpha)=a_0+a_1\alpha+...+a_n\alpha^n$. 1) $(f+g)(\alpha)=f(\alpha)+g(\alpha)$ 2) $(fg)(\alpha)=f(\alpha)g(\alpha), (\forall) f,g \in K[X]$, $\alpha \in K$.	$f = 1+X+X^2+X^3, \alpha = i \in \mathbb{C} \Rightarrow$ $f(i)=1+i+i^2+i^3=1+i-1-i=0$
8) Funcția polinomială asociată polinomului $f = a_0+a_1X+...+a_nX^n$	$f: K \to K$, $f(x)=a_0+a_1x+...+a_nx^n$, $x =$ **variabila**	1) $f:\mathbb{R}\to\mathbb{R}$, $f(x)=ax+b, a,b \in \mathbb{R}$, $a \neq 0$ **este funcție de gradul întâi.** 2) $f:\mathbb{R}\to\mathbb{R}$, $f(x)=ax^2+bx+c$, $a,b,c \in \mathbb{R}, a \neq 0$, **este funcția de gradul al doilea.**

Definiţii. Proprietăţi	Explicitare. Notaţii	Exemple
9) **Teorema împărţirii cu rest în $K[X]$ pentru două polinoame *f*, *g***	$f, g \in K[X], g \neq 0 \Rightarrow (\exists!) q, r \in K[X]$ astfel încât $f = gq + r$, $\text{grad}(r) < \text{grad}(g)$ *f* = deîmpărţitul, *g* = împărţitorul, *q* = câtul, *r* = restul Dacă $r = 0$, atunci *g* divide pe *f* ($g \mid f$) sau ($f \vdots g$ (*f* se divide prin *g*)	1) $f = X^4 + 3X^2 + 2X - 5$, $g = X^2 - 3X$, $f, g \in \mathbb{R}[X]$ $X^4 + \quad 3X^2 + 2X - 5 \mid X^2 - 3X$ $-X^4 + 3X^3 \qquad\qquad \mid X^2 + 3X + 12 = q$ $/ \quad 3X^3 + 3X^2$ $-3X^3 + 9X^2$ $/ \quad 12X^2 + 2X$ $-12X^2 + 36X$ $38X - 5 = r$ $X^4 + 3X^2 + 2X - 5 = (X^2 - 3X) \cdot$ $\cdot (X^2 + 3X + 12) + 38X - 5$. 2) $f = X^3 + \hat{2}X + \hat{1}$, $g = X^2 + \hat{1}$, $f, g \in \mathbb{Z}_3[X]$ $X^3 + \quad \hat{2}X + \hat{1} \mid X^2 + \hat{1}$ $2X^2 + \hat{2} \qquad\qquad \mid X = q$ $/ \quad \hat{2}X = r$ $X^3 + \hat{2}X + \hat{1} = (X^2 + \hat{1})X + \hat{2}X$
Teorema restului Împărţirea prin $X - a$	Restul împărţirii polinomului $f \neq 0$ prin $X - a$ este egal cu $f(a)$	
$x = a$ **este rădăcină a unui polinom *f* dacă**	$f(a) = 0$	1) $f = X^2 - 2 \in \mathbb{R}[X]$, $x = \sqrt{2}$ este rădăcină a lui *f* deoarece $f(\sqrt{2}) = 2 - 2 = 0$ 2) $f = X^2 + 1 \in \mathbb{C}[X]$, $x = i$ este rădăcină a lui *f* deoarece $f(i) = i^2 + 1 = -1 + 1 = 0$
Teorema factorului (Bézout) *f* se divide prin $X - a$	$\Leftrightarrow f(a) = 0 \Leftrightarrow f = (X - a)g$, $f, g \in K[X]$	1) $f = X^3 - 1$, $f(1) = 0 \Rightarrow$ $\Rightarrow f = (X - 1)(X^2 + X + 1)$ 2) $f = X^4 - 16$, $f(2) = 0 \Rightarrow$ $\Rightarrow f = (X - 2)(X^3 + 2X^2 + 4X + 8)$
$x = a$ **este rădăcină de ordin *p*, $p \in \mathbb{N}^*$, pentru polinomul *f***	$\Leftrightarrow \begin{cases} f(a) = 0 \\ f'(a) = f''(a) = \ldots = f^{(p-1)}(a) = 0 \\ f^{(p)}(a) \neq 0 \end{cases}$ $\Leftrightarrow f \vdots (X - a)^p$ şi $f \not\vdots (X - a)^{p+1}$	$x = 1$ este rădăcină de ordin 2 pentru polinomul $f = X^3 - 3X + 2$ deoarece $f(1) = 0$, $f'(1) = 0$, $f''(1) \neq 0 \Leftrightarrow$ $\Leftrightarrow f = (X - 1)^2 (X + 2)$.

Probleme propuse

1. Să se determine $a, b, c, d, e \in \mathbb{C}$ astfel încât polinomul f să fie egal cu polinomul g în cazurile:

1) $f = 2X^3 - X^2 + 3X + 6,\ g = a + b(X-1) + c(X-1)^2 + d(X-1)^3$;

2) $f = X^3 + (a-2b)X^2 + (b+3c)X + a + b + 2c,\ g = (X-1)^2(X+3)$;

3) $f = X^3 - 5X^2 + 3X + 1,\ g = (a+b)X^3 - (b+2c-a)X^2 + (b-c)X + a + b$;

4) $f = (a+1)X^3 + 2X^2 - (b+c)X + 1.\ g = bX^3 + (a+b+c)X^2 + (2b-c)X + c + 2a$;

5) $f = aX^4 + bX^3 + cX^2 + dX + e,\ g = iX^4 + aiX^3 + biX^2 + ciX + d$.

2. Să se calculeze $f+g$ şi $f \cdot g$ în cazurile:

1) $f = 3X^2 - 5X + 6,\ g = -3X^2 + 2X - 3,\ f, g \in \mathbb{Z}[X]$;

2) $f = \frac{1}{2}X + \sqrt{3},\ g = 2X^2 + \sqrt{3}X,\ f, g \in \mathbb{R}[X]$;

3) $f = (1+i)X^2 - 2iX + 3 - i,\ g = iX + 1 - i,\ f, g \in \mathbb{C}[X]$;

4) $f = \hat{2}X + 3,\ g = \hat{2}X^2 + \hat{3}X + \hat{1},\ f, g \in \mathbb{Z}_4[X]$;

5) $f = 3X^2 + \hat{2}X + \hat{1},\ g = \hat{2}X^3 + \hat{3}X^2 + \hat{4},\ f, g \in \mathbb{Z}_5[X]$.

3. În raport cu parametrul m discutați gradul următoarelor polinoame:

1) $f = \left(m^2 - 3m + 2\right)X^3 + \left(m^2 - 4m + 3\right)X^2 + \left(m^2 - 1\right)X + 6$;

2) $f = \left(m^2 + 1\right)X^4 + \left(m^4 - 1\right)X^2 + iX$;

3) $f = \left(\hat{2}m^2 + \hat{5}m + \hat{3}\right)X^3 + \left(m + \hat{5}\right)X^2 + \left(\hat{2}m + \hat{3}\right)X + \hat{3} \in \mathbb{Z}_7[X], m \in \mathbb{Z}_7$.

4. Fie $f, g \in \mathbb{Q}[X],\ f = \left(m^3 - 2\right)X^3 + mX + 5,\ g = \left(m^6 - 1\right)X^4 + (m-1)X^3 + 2mX^2 + 1$. Pentru ce valori ale lui m polinoamele au acelaşi grad?

5. Fie $f, g, h \in \mathbb{C}[X],\ f = X^4 - iX^2 - 1,\ g = X^4 + iX^2 - 1,\ h = f \cdot g$. Să se calculeze $h(1+i) - h(1-i)$.

6. Să se calculeze:

a) $(X-1)(X+1)\left(X^2+1\right)\left(X^4+1\right)\ldots\left(X^{2^n}+1\right)$;

b) $\left(X^2 + X + 1\right)\left(X^2 - X + 1\right)\left(X^4 - X^2 + 1\right)\ldots\left(X^{2^{n+1}} - X^{2^n} + 1\right)$.

7. Fie polinoamele: $f = 10X^{10} + 9X^9 + 8X^8 + \ldots + 2X^2 + X,\ g = 100X^{100} + 99X^{99} + 98X^{98} + \ldots +$ $+ 2X^2 + X$.

a) Calculați $f(1), f(-1), g(1), g(-1)$.

b) Aflați coeficientul lui X^{110} şi coeficientul lui X^{109} din $f \cdot g$.

8. Să se determine $m \in \mathbb{R}$ astfel încât $f(1) = 0$, unde $f = X^3 + mX^2 + 2X + m - 1$.

9. Fie $f \in \mathbb{C}[X],\ f = X^4 + aX^3 + bX^2 + 3X + 1$. Să se determine a, b dacă $f(i) = f(-i) = 0$.

10. Să se determine două polinoame de gradul întâi $f, g \in \mathbb{R}[X]$ astfel încât:

$$\left(X^2-2X+1\right)f+\left(X^2+X-1\right)g=1.$$

11. Să se determine polinomul $f \in \mathbb{R}[X]$ de gradul al doilea astfel încât pe rând: 1) $f(-1)=1$, $f(0)=-4$, $f(2)=-2$; 2) $f(1)=1$, $f(2)=2$, $f(3)=3$; 3) $f(1)=f(2)=2$, $f(3)=-2$.

12. Pentru ce valori reale ale parametrilor p şi q polinomul $X^4+4X^3-2X^2+pX+q$ este un pătrat perfect.

13. Să se determine constantele a, b, c astfel încât polinomul $f=a\left(X^3+2X\right)+b\left(X^3+4X-1\right)+$ $+c\left(X^3+2X^2+2\right)$ să fie un cub perfect.

14. Să se determine polinoamele $f \in \mathbb{R}[X]$ astfel încât să avem: $f(x+1)-f(x)=(3x+1)^2, (\forall)x \in \mathbb{R}$.

15. Să se determine polinoamele:

1) de gradul al doilea $f \in \mathbb{R}[X]$ pentru care pe rând:

a) $f\left(x^3\right)=\left(f(x)\right)^3, (\forall)x \in \mathbb{R}$;

b) $f(x)f(-x)=f\left(x^2\right), (\forall)x \in \mathbb{R}$.

2) de gradul al treilea $f \in \mathbb{R}[X]$ astfel încât $f(x)f(-x)=f\left(x^2\right)$.

16. Dacă $f \in \mathbb{R}[X]$, grad$(f)=n$, atunci funcția polinomială $g(x)=f(x+2)-2f(x+1)+f(x)$, $x \in \mathbb{R}$ este o funcție polinomială de gradul $(n-2)$.

Găsiți mulțimea polinoamelor f pentru care $g(x)=x^2+x+1, (\forall)x \in \mathbb{R}$.

17. Să se determine $f \in \mathbb{R}[X]$, grad$(f)=3$ astfel încât $f(1)+f(2)+...+f(n)=n^4, (\forall)n \in \mathbb{N}$.

18. Demonstrați egalitățile de polinoame $\left(n \in \mathbb{N}^*\right)$:

a) $\left(X+2X^2+3X^3+...+nX^n\right)(X-1)^2=nX^{n+2}-(n+1)X^{n+1}+X$;

b) $1+\dfrac{X}{1!}+\dfrac{1}{2!}X(X+1)+...+\dfrac{1}{n!}X(X+1)...(X+n-1)=\dfrac{1}{n!}(X+1)...(X+n)$.

19. În inelul $\mathbb{Z}_4[X]$ să se determine $f=aX^2+bX+c$ astfel încât $\left(\hat{2}X^2+\hat{2}X+\hat{3}\right)f=\hat{1}$.

20. Să se arate că dacă $f \in \mathbb{R}[X]$, grad$(f)=n$, atunci există numerele reale $a_0, a_1, ..., a_n$ unic determinate astfel încât $f=a_0+a_1X+a_2X(X-1)+...+a_nX(X-1)....(X-n+1)$.

21. Fie $f \in \mathbb{Z}_4[X]$, $f=X^3+\hat{2}X^2+X+\hat{1}$. Să se determine toate polinoamele $g=aX^3+bX^2+cX+d \in \mathbb{Z}_4[X]$ cu proprietatea că $\overline{f}=\overline{g}$ (unde $\overline{f}:\mathbb{Z}_4 \to \mathbb{Z}_4$ este funcția polinomială asociată lui f).

22. Se consideră funcția $f:\mathbb{Z}_5 \to \mathbb{Z}_5$ definită prin $f\left(\hat{0}\right)=\hat{2}$, $f\left(\hat{1}\right)=\hat{0}$, $f\left(\hat{2}\right)=\hat{3}$, $f\left(\hat{3}\right)=\hat{4}$, $f\left(\hat{4}\right)=\hat{1}$. Să se arate că f este o funcție polinomială.

23. a) Să se arate că dacă $f \in \mathbb{C}[X]$, grad$(f)\geq 1$, atunci funcția polinomială $\overline{f}:\mathbb{C} \to \mathbb{C}$ este surjectivă.

b) Care sunt polinoamele $f \in \mathbb{R}[X]$ de grad impar pentru care funcția $\overline{f}:\mathbb{R}\to\mathbb{R}$ este surjectivă ?

c)* Există $f \in \mathbb{C}[X]$ de grad$(f)=n$ astfel încât funcția $\overline{f}:\mathbb{R}\to\mathbb{C}$ să fie injectivă ?

24. Să se determine câtul și restul împărțirii polinomului *f* la polinomul *g* în cazurile:

1) $f=3X^3-2X^2+5X+5,\quad g=X-1,\quad f,g\in\mathbb{Z}[X]$;

2) $f=2X^5-X^4+6X^3+5X^2-3,\quad g=X+1,\quad f,g\in\mathbb{Z}[X]$;

3) $f=3X^2-2X+3,\quad g=2X-1,\quad f,g\in\mathbb{Q}[X]$;

4) $f=iX^3+(1-i)X^2+3X-i,\quad g=X^2-(i+1)X+3,\quad f,g\in\mathbb{C}[X]$;

5) $f=\hat{3}X^5+\hat{2}X^3+X^2+\hat{1},\ g=X+\hat{1},\ f,g\in\mathbb{Z}_4[X]$;

6) $f=\hat{2}X^4+\hat{3}X^2+\hat{4}X+\hat{3},\ g=\hat{3}X+\hat{2},\ f,g\in\mathbb{Z}_5[X]$;

7) $f=X^4+X^2+X+\hat{1},\ g=X^2+\hat{1},\ f,g\in\mathbb{Z}_4[X]$;

8) $f=\hat{6}X^4+\hat{2}X^3+\hat{5}X^2+4X+\hat{1},\ g=\hat{5}X^2+\hat{2}X+\hat{4},\ f,g\in\mathbb{Z}_7[X]$;

9) $f=x^6+\hat{4}X^4+\hat{2}X^2+\hat{3},\ g=X^3+\hat{5}X^2+\hat{3},\ f,g\in\mathbb{Z}_{11}[X]$.

25. Să se determine parametrul *m* astfel încât polinomul *f* să se dividă prin polinomul *g* în cazurile următoare:

1) $f=X^3+(m+1)X^2-2mX+3m-1,\ g=X-1,\ f,g\in\mathbb{R}[X],\ m\in\mathbb{R}$;

2) $f=mX^4+(2m-1)X^3-3mX+m-2,\ g=X+2,\ f,g\in\mathbb{R}[X],\ m\in\mathbb{R}$.

3) $f=(m+1)X^3-(2m+i)X^2+mX+m-i,\ g=X+i,\ f,g\in\mathbb{C}[X],\ m\in\mathbb{C}$;

4) $f=X^3+mX^2+X+1,\ g=X+i,\ f,g\in\mathbb{C}[X]$;

5) $f=X^6+4X^2+mX,\ g=iX+2,\ f,g\in\mathbb{C}[X]$;

6) $f=X^4+\hat{2}X^3+mX^2+m+\hat{1},\ g=X+\hat{2},\ f,g\in\mathbb{Z}_4[X],\ m\in\mathbb{Z}_4$;

7) $f=\hat{4}X^5+(m+1)X^4+\hat{3}X^2+\hat{3},\ g=X+\hat{3},\ f,g\in\mathbb{Z}_5[X],\ m\in\mathbb{Z}_5$.

26. Să se determine parametrul *m* astfel încât polinomul *f* împărțit la polinomul *g* să dea restul *r* în cazurile:

1) $f=3X^3-(2m+1)X^2+5X-m,\ g=X-2,\ r=3$;

2) $f=3X^4+(2i-1)X^3+mX^2+2m+i,\ g=X+i,\ r=1-3i$;

3) $f=\hat{5}X^3+\left(m+\hat{1}\right)X^2+\hat{3}m+2,\ g=X+\hat{4},\ r=\hat{2},\ f,g\in\mathbb{Z}_7[X],\ m\in\mathbb{Z}_7$.

27. Să se determine parametrii *m*, *n* astfel ca polinomul $f=2X^3-3X^2+mX+n$ împărțit cu $X-1$ și $X+2$ să dea resturi egale respectiv cu 4 și cu – 5.

28. Să se determine *m*, *n*, *p* astfel încât polinomul $f=X^5+mX^2+nX+p$ împărțit cu $X-1$, $X+1$ și $X-2$ dă resturile 1, – 1 și respectiv 41.

29. Fără a efectua împărțirea să se determine restul împărțirii polinomului *f* la polinomul *g* în cazurile:

1) $f=X^{100}-3X^{99}+5,\ g=(X-1)(X+1)$;

2) $f=X^{1000}+X+1,\ g=(X+1)(X+2)$

3) $f=X^5+X^4+X^3-X-1,\ g=(X-1)(X+1)(X-2)$;

4) $f = X^{200} + X^{101} + X,\ g = X\left(X^2 - 1\right)$.

30. **Un polinom împărțit prin $X-1$, $X-3$, $X+1$ dă resturile 2, 3 şi respectiv 4. Să se afle restul împărțirii polinomului prin $(X-1)(X-3)(X+1)$.**

31. **Fie $f \in \mathbb{R}[X]$ un polinom cu proprietatea $xf(x+1)+(x+2)f(x+3) = 2x^3+10, (\forall)x \in \mathbb{R}$. Să se determine restul împărțirii polinomului prin $(X-3)(X+1)$.**

32. **Să se arate că dacă un polinom *f* este divizibil prin $X-a$, $X-b$, $a \neq b$, atunci *f* este divizibil prin $(X-a)(X-b)$. Să se determine expresia restului împărțirii unui polinom oarecare din $\mathbb{C}[X]$ prin $(X-a)(X-b), a \neq b$.**

33. **Determinați valorile parametrilor m, n dacă polinomul *f* se divide cu polinomul *g* în cazurile:**

1) $f = X^6 + mX^5 + nX^2 + 4,\ g = X^2 - 1,\ f, g \in \mathbb{R}[X]$;

2) $f = X^4 + X^3 + mX^2 - m^2X + n,\ g = X^2 + X,\ f, g \in \mathbb{R}[X]$.

3) $f = X^5 + mX + n,\ g = X^2 - 4,\ f, g \in \mathbb{R}[X]$;

4) $f = X^4 + mX^3 + 9X^2 + n,\ g = X^2 - 3X + 2,\ f, g \in \mathbb{R}[X]$;

5) $f = mX^3 + (n-1)X^2 - X - 2,\ g = X^2 - 1,\ f, g \in \mathbb{R}[X]$;

6) $f = X^3 - (m+1)X^2 + (3n+2)X - 2n,\ g = X^2 - 3X + 2,\ f, g \in \mathbb{R}[X]$;

7) $f = X^4 + nX^3 + (n-2m)X^2 + 5X - 3m,\ g = X^2 + X + 2,\ f, g \in \mathbb{R}[X]$;

8) $f = 2X^4 - 4X^3 - 4X^2 + mX + n,\ g = X^2 - X - 6,\ f, g \in \mathbb{R}[X]$;

9) $f = mX^4 + nX^3 - 1,\ g = (X-1)^2,\ f, g \in \mathbb{R}[X]$;

10) $f = X^4 + 1,\ g = X^2 + mX + n,\ f, g \in \mathbb{R}[X]$;

11) $f = X^4 + X^3 + X^2 + mX + n,\ g = X^2 + X + \hat{4},\ f, g \in \mathbb{Z}_5[X]$.

34. **Determinați valorile lui m, n, p dacă polinomul *f* se divide cu polinomul *g* în cazurile:**

1) $f = X^4 + 3X^3 + mX^2 + nX + p,\ g = (X+2)(X^2+1),\ f, g \in \mathbb{R}[X]$;

2) $f = X^5 + mX^4 + 2X^3 + nX^2 - 3X + p,\ g = X^3 + 1,\ f, g \in \mathbb{R}[X]$;

3) $f = X^4 + mX^3 + X^2 + nX + p,\ g = X^3 + 2X^2 + 3X + 4,\ f, g \in \mathbb{R}[X]$;

4) $f = X^4 + 5X^3 + mX^2 + nX + p,\ g = (X^2-1)(X+3),\ f, g \in \mathbb{R}[X]$;

5) $f = X^3 + (m-1)X^2 + 2nX + p,\ g = \left(X^2 - 4\right)(X+1),\ f, g \in \mathbb{R}[X]$;

6) $f = X^4 + mX + n,\ g = X^2 + pX + 1,\ f, g \in \mathbb{Q}[X]$;

35. **Să se arate că dacă $f \in \mathbb{Z}[X]]$ admite două rădăcini întregi de parități diferite, atunci $f(k)$ este par, oricare ar fi $k \in \mathbb{Z}$.**

36. **Dacă polinomul $f \in \mathbb{Z}[X]$ are trei rădăcini întregi care dau resturi diferite la împărțirea cu trei, atunci să se arate că pentru orice $k \in \mathbb{Z}$, $f(k)$ este multiplu de trei.**

37. **Arătați că dacă valorile polinomului $f \in \mathbb{C}[X]$ pentru orice număr rațional *c* sunt raționale, atunci $f \in \mathbb{Q}[X]$.**

38. Fie $x_1, x_2,...,x_{n+1}$ numere complexe diferite, $c_1, c_2,...,c_{n+1}, n+1$ numere complexe oarecare. Să se arate că există un unic polinom $f \in \mathbb{C}[X]$ astfel încât $f(x_i) = c_i, i = \overline{1,n+1}$.

39. Arătaţi că nu există polinom *f* de gradul doi care pentru orice valoare $c \in \mathbb{R} - \mathbb{Q}$, $f(c) \in \mathbb{Q}$.

40. Să se determine *m*, *n* dacă prin împărţirea polinomului $f = mX^3 + nX - 1$ prin $g = X^2 - 3X + 2$ se obţine restul 7.

41. Prin împărţirea cu rest a polinomului *f* la *g* avem egalitatea $f = gq + r$. Determinaţi restul prin împărţirea:

1) polinomului f^2 la *g*, dacă $r = 7X^3 - X + 1$ şi grad(*g*) = 7;

2) polinomului *f* la g^2, dacă *r* = 2, iar restul la împărţirea lui f^2 la g^2 este egal cu 4;

3) polinomului *f* la *q*, dacă $q = 2X^3 + X + 3$ şi $r = 4X^4 + 2X^2 + 1$.

42. Arătaţi că polinomul $f \in \mathbb{Z}[X]$ nu se poate descompune în factori ireductibili peste $\mathbb{Z}$, în cazurile următoare:

1) $f = X^4 + X + 1$; 2) $f = X^4 + +X^3 - X^2 - X + 2$;

3) $f = (X-1)^2(X-2)^2 + 1$; 4) $f = X^4 + nX^3 - X^2 - nX + 2, n \in \mathbb{N}^*$;

5) $f = X^4 + nX^3 + n^2X^2 + n^3X - 1, n \in \mathbb{N}^*$.

43. Descompuneţi polinomul *f* în factori ireductibili peste $\mathbb{R}$ şi respectiv $\mathbb{C}$ în cazurile:

1) $f = X^3 - 8$; 2) $f = X^3 + 8$; 3) $f = X^4 - 16$;

4) $f = X^4 + 16$; 5) $f = X^4 - X^2 + 1$; 6) $f = X^6 - 27$;

7) $f = X^6 + 27$; 8) $f = X^8 - 6X^4 + 9$; 9) $f = X^4 + 6X^3 + 9X^2 - 9$;

10) $f = X^4 - 10X^3 + 25X^2 - 6$.

44. Arătaţi că polinomul $f = X^4 + X^2 + \hat{1} \in \mathbb{Z}_5[X]$ este reductibil peste $\mathbb{Z}_5$, dar nu are nici o rădăcină în $\mathbb{Z}_5$.

45. Descompuneţi în factori ireductibili polinoamele:

1) $f = X^3 + \hat{2}X^2 + \hat{4}X + \hat{3} \in \mathbb{Z}_5[X]$; 2) $f = \hat{3}X^4 + 5X^3 + \hat{6}X^2 + \hat{4}X + \hat{4} \in \mathbb{Z}_7[X]$;

3) $f = X^3 + X + \hat{1} \in \mathbb{Z}_2[X]$; 4) $f = X^4 + \hat{1} \in \mathbb{Z}_2[X]$;

5) $f = X^3 + X^2 + X + \hat{1} \in \mathbb{Z}_3[X]$; 6) $f = X^4 + 1 \in K[X], K = \mathbb{R}, K = \mathbb{C}, K = \mathbb{Z}_4$.

46. Arătaţi că polinomul $f = X^4 + X^3 + \hat{1} \in \mathbb{Z}_2[X]$ este ireductibil peste $\mathbb{Z}_2$.

47. Să se determine $m,n \in \mathbb{Z}_3, m \neq \hat{0}$, astfel încât polinomul $f = mX^3 + nX + \hat{2} \in \mathbb{Z}_3[X]$ să fie ireductibil peste $\mathbb{Z}_3$.

48. Fie polinomul $f = \hat{2}X^3 + \hat{2}X + \hat{1} \in \mathbb{Z}_3[X]$. Determinaţi polinoamele $g = mX^3 + nX^2 + pX + q \in \mathbb{Z}_3[X]$ cu proprietatea $\overline{f} = \overline{g}$.

49. Determinaţi $m,n \in \mathbb{Z}_3$ astfel încât polinomul $f = X^3 + mX + n \in \mathbb{Z}_3[X]$ să fie reductibil peste $\mathbb{Z}_3$. Descompuneţi în factori ireductibili polinoamele astfel obţinute.

50. Determinaţi polinoamele $f = X^2 + mX + n \in \mathbb{Z}_4[X]$ ireductibile peste $\mathbb{Z}_4$.

51. **Să se determine cel mai mare divizor comun şi cel mai mic multiplu comun al polinoamelor f, g în cazurile următoare:**

1) $f = X^3 - 2X^2 - 5X + 6, \quad g = X^4 + 4X^3 + 3X^2 - 4X - 4$;

2) $f = X^4 + 3X^3 + 2X^2 - 2, \quad g = X^3 + 2X^2 + 2X + 1$;

3) $f = 2X^4 + 5X^3 - 5X^2 - 5X + 3, \quad g = X^4 - X^3 - 7X^2 + X + 6$;

4) $f = X^4 + 2X^3 - X, \quad g = X^4 + 2X^3 + X^2 - 1$;

5) $f = 2X^5 + X^4 - 7X^3 + X^2 + 6X - 5, \quad g = 2X^4 + X^3 - 13X^2 - 4X + 2$;

6) $f = X^6 - 2X^4 + 2X^3 + X^2 - 2X + 1, \quad g = X^5 - X^3 + X^2$;

7) $f = X^4 + X^2 + \hat{1}, \quad g = X^3 + X, \ f, g \in \mathbb{Z}_2[X]$;

8) $f = X^3 + X + \hat{2}, \quad g = X^3 + \hat{2}X^2 + \hat{3}X + \hat{2}, \ f, g \in \mathbb{Z}_4[X]$;

9) $f = X^4 + \hat{4}X^3 + \hat{2}X, \quad g = X^3 + \hat{4}X^2 + \hat{3}X, \ f, g \in \mathbb{Z}_5[X]$.

10) $f = X^4 + \hat{6}X^3 + \hat{2}X^2 + \hat{4}X + \hat{5}, \ g = X^3 + \hat{5}X; \ f, g \in \mathbb{Z}_7[X]$.

52. **Să se arate că următoarele polinoame f, g sunt prime între ele:**

1) $f = 3X^3 - 2X^2 + X + 2, \quad g = X^3 - 2X^2 + 2X - 1$;

2) $f = X^4 + 2X^3 - X^2 - 2X, \quad g = X^5 - 2X^4 + 3X^3 - 6X^2 + 2X - 4$;

3) $f = X^3 + \hat{1}, \quad g = X^4 + X^3 + X^2, \ f, g \in \mathbb{Z}_3[X]$;

4) $f = X^3 + \hat{4}X^2 + \hat{5}X + \hat{2}, \quad g = X^4 + X^3, \ f, g \in \mathbb{Z}_6[X]$;

5) $f = X^3 + \hat{2}X^2 + \hat{4}X + \hat{1}, \quad g = X^4 + \hat{4}X^3 + \hat{2}X^2 + \hat{3}X + \hat{1}, \ f, g \in \mathbb{Z}_7[X]$.

53. **Să se determine α şi β astfel ca polinoamele $f = 2X^3 - 7X^2 + \alpha X + 3$, $g = X^3 - 3X^2 + \beta X + 3$ să aibă un divizor comun de gradul doi.**

54. **Dacă d este cel mai mare divizor comun al polinoamelor f, g, atunci determinați o relație liniară de forma $d = \alpha f + \beta g$ în cazurile:**

1) $f = X^4 + 4X^3 - 7X + 2, \quad g = X^3 + 3X^2 - 2$;

2) $f = X^5 - X^4 + X^3 - X^2 + 2X - 2, \quad g = X^5 - 1$;

3) $f = 3X^5 + 6X^4 + 3X^3 - X^2 - 2X - 1, \quad g = X^4 - 2X^2 + 1$.

55. **Să se arate că polinomul f se divide prin polinomul g în cazurile:**

1) $f = \left(X^2 + X + 1\right)^5 - X, \ g = X^2 + 1$; 2) $f = \left(X^2 + X + 1\right)^9 - X, \ g = X^2 + 1$;

3) $f = \left(2X^2 + X + 2\right)^3 + \left(2X^2 - X + 2\right)^7, \ g = X^2 + 1$;

4) $f = (X+1)^{2n-1} + (-1)^n (X+2)^{n+1}, \ g = X^2 + 3X + 3, \ n \in \mathbb{N}^*$.

56. **Să se arate că polinomul f se divide cu polinomul $g = X^2 + X + 1$ în cazurile următoare:**

1) $f = X\left(X^2 + 1\right)^{6n+1} + X^{3n+2}, n \in \mathbb{N}$; 2) $f = X^{6n-1} + X + 1, n \in \mathbb{N}^*$;

3) $f = X^{3n} + X^{3m+1} + X^{3l+2}, n, m, l \in \mathbb{N}$ 4) $f = (X+1)^{6n+1} + X^{6n+2}, n \in \mathbb{N}$;

5) $f = \left(X^2 + 1\right)^{6n+2} + X^4 + 1, n \in \mathbb{N}$.

57. **Să se arate că polinomul *f* se divide cu polinomul $g = X^2 - X + 1$ în cazurile următoare:**

1) $f = (X-1)^{n+3} + X^{2n+3}, n \in \mathbb{N}$; 2) $f = (X-1)^{2n+1} + (-1)^{n+1} X^{n+2}, n \in \mathbb{N}^*$;

3) $f = (X-1)^{n+2} - X^{2(n-1)}, n \in \mathbb{N}^*$.

58. **Pentru ce valori ale lui $n \in \mathbb{N}^*$ polinomul *f* se divide cu polinomul $g = X^2 + X + 1$, în cazurile următoare:**

1) $f = (X+1)^n + X^n + 1$; 2) $f = X^n + X^{n+1} + X^{n+2}$;

3) $f = \left(X^3 + X - 1\right)^n + \left(X^3 - X - 2\right)^{n+1} - 1$.

59. **Pentru ce valori ale lui $n \in \mathbb{N}$ polinomul *f* se divide cu polinomul $g = X^2 - X + 1$, în cazurile următoare:**

1) $f = (X-1)^n + X^n + 1$; 2) $f = (X-1)^{2n} + X^n + 1$;

3) $f = \left(X^2+1\right)^n + \left(X^4+1\right)^n + 1$; 4) $f = X^{2n} + X^n + 1$.

60. **Arătați că polinomul $f = X^{4n+3} + X^{4n+2} + X + 1, n \in \mathbb{N}$ se divide cu polinomul $g = X^3 + X^2 + X + 1$.**

61. **a) Să se arate că dacă funcția polinomială $p : \mathbb{C} \to \mathbb{C}, p(x) = f\left(x^3\right) + x^2 g\left(x^3\right)$ (unde $f, g \in \mathbb{R}[X]$) are rădăcină ω soluție a ecuației $x^2 + x + 1 = 0$, atunci $f(1) = g(1) = 0$.**

b) Fie $k : \mathbb{C} \to \mathbb{C}, k(x) = f\left(x^3\right) + xg\left(x^3\right) + x^2 h\left(x^3\right), f, g, h \in \mathbb{R}[X]$ care are ca rădăcini pe 1, ε, ε^2 unde $\varepsilon = \dfrac{-1 \pm i\sqrt{3}}{2}$. Să se arate că $f(1) = g(1) = h(1) = 0$.

62. *** Fie polinoamele nenule $f, g, h \in \mathbb{Q}[X]$. Să se arate că dacă funcția polinomială $g : \mathbb{C} \to \mathbb{C}$, $g(x) = f(x^3) + xg(x^3) + x^2 h(x^3)$ are ca zerouri rădăcinile ecuației $x^6 - 6x^3 + 8 = 0$, atunci polinoamele f, g, h se divid cu polinomul $X^2 - 6X + 8$.**

63. **Să se arate că polinomul $f = \left(X^8 + X^6\right)^{2n+1} + \left(X^4 + X^2 + 1\right)^{2n+1} + X^{10p+5} + 1$ se divide cu polinomul $g = X^4 - X^3 + X^2 - X + 1, (\forall) n, p \in \mathbb{N}$.**

64. **Se consideră polinomul $f = \left(X^3 + X\right)^n - X^n - X^3, n \in \mathbb{N}^*$. Să se determine *n* astfel încât (pe rând):**

a) *f* să fie divizibil prin $X^2 + 1$; b) *f* să fie divizibil prin $X^4 + X^2 + 1$.

65. **Demonstrați egalitatea de polinoame:**

$$1 + \frac{X}{1!} + \frac{X(X+1)}{2!} + \ldots + \frac{X(X+1)\ldots(X+n-1)}{n!} = \frac{1}{n!}(X+1)\ldots(X+n), (\forall) n \in \mathbb{N}^*$$

66. **1) Arătați că polinomul $f = X^7 + 4X^3 + 6X^2 + 5X + 2$ se divide prin $g = \left(X^2 + X + 1\right)^2$.**

2) Să se determine polinomul $f \in \mathbb{R}[X]$ pentru care are loc egalitatea $xf(x-1) = (x-26) f(x)$, $(\forall) x \in \mathbb{R}$.

67. **Să se rezolve ecuațiile:**

1) $x^9 = 1$; 2) $x^9 = -1$; 3) $x^{10} = i$;

4) $x^6 = -i$; 5) $x^4 = \frac{1+i\sqrt{3}}{2}$; 6) $x^8 = \frac{1}{2} + \frac{i\sqrt{3}}{2}$;

7) $x^5 = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$; 8) $(x+1)^n - (x-1)^n = 0$; 9) $(1+ix)^n - (1-ix)^n = 0$.

68. Să se rezolve ecuațiile

1) $x^6 = \frac{1+i}{1-i}$; 2) $x^5 = \left(\frac{1}{2} + \frac{i\sqrt{3}}{2}\right)^2$; 3) $x^7 = (1+i)^6$; 4) $x^{10} = \frac{(1+i)^3}{\left(\frac{1}{2} - \frac{i\sqrt{3}}{2}\right)^4}$;

5) $(1+iz)^n + (1-iz)^n = \left(\sqrt{1+z^2}\right)^n$; 6) $\left(\frac{1+iz}{1-iz}\right)^n = \frac{1+ai}{1-ai}, a \in \mathbb{R}$; 7) $z^{2n} = z$; 8) $z^n = |z|$;

9) $z^n = \bar{z}, n \in \mathbb{N}^*$; 10) $1 + z + z^2 + ... + z^n = 0$; 11) $1 - z + z^2 - z^3 + ... - z^{2n-1} + z^{2n} = 0$.

69. Dacă $m, n \in \mathbb{N}, (m,n) = d$, atunci soluțiile comune ale ecuațiilor $z^n - 1 = 0, z^m - 1 = 0$, sunt soluțiile ecuației $z^d - 1 = 0$.

70. Să se rezolve ecuațiile:

1) $x^4 - 5x^2 + 4 = 0$; 2) $x^{10} - 3x^5 - 4 = 0$; 3) $x^8 + 4x^4 + 3 = 0$;

4) $x^6 + 19x^3 - 216 = 0$; 5) $x^{100} - (1+i)x^{50} + i = 0$.

71. Să se determine natura rădăcinilor ecuațiilor:

1) $x^4 - (2m-1)x^2 + m^2 - 1 = 0$; 2) $(m-1)x^4 + 2(m-1)x^2 + m = 0$; 3) $x^4 - x^2 + m + 1 = 0$;

4) $x^4 + mx^2 - m = 0$; 5) $x^4 + (2m-1)x^2 + m^2 - m = 0$, când $m \in \mathbb{R}$.

72. Să se rezolve ecuațiile:

1) $\left(x - \frac{9}{2}\right)^4 + \left(x - \frac{11}{2}\right)^4 = 1$; 2) $(x+3)^4 + (x+5)^4 = 16$;

3) $(2x-3)^4 + (2x-5)^4 = 2$; 4) $2x^3 - 6x + 5 = 0$.

73. Să se rezolve ecuațiile reciproce:

a) 1) $3x^3 + 2x^2 + 2x + 3 = 0$; 2) $x^3 - 5x^2 - 5x + 1 = 0$;

b) 1) $3x^4 + 2x^3 - 11x^2 + 2x + 3 = 0$; 2) $2x^4 + x^3 - 2x^2 + x + 2 = 0$;

c) 1) $2x^5 + x^4 + x^3 + x^2 + x + 2 = 0$; 2) $3x^3 + x^4 - 3x^3 - 3x^2 + x + 3 = 0$.

74. Să se determine parametrul real a astfel încât ecuațiile de mai jos să aibă toate rădăcinile reale:

1) $x^4 + 3x^3 + ax^2 + 3x + 1 = 0$; 2) $x^4 + 3x^3 - 2ax^2 + 3x + 1 = 0$;

3) $3x^4 - 5x^3 + ax^2 - 5x + 3 = 0$.

75. Să se rezolve ecuațiile:

1) $2x^4 - 21x^3 + 74x^2 - 150x + 50 = 0$; 2) $x^4 - 5x^3 + 10x^2 - 10x + 4 = 0$;

3) $2x^4 - 13x^3 - 68x^2 - 52x + 32 = 0$; 4) $x^4 + 3x^3 - 2x^2 - 6x + 4 = 0$;

5) $\frac{x^2}{3} + \frac{48}{x^2} = 10\left(\frac{x}{3} - \frac{4}{x}\right)$; 6) $4x^4 + 6x^3 - 10x^2 - 9x - 9 = 0$.

76. **Să se rezolve ecuațiile:**

I.

1) $5x^3+10x^2-3x-6=0$; 2) $2x^3-13x^2+28x-20=0$;

3) $10x^4+11x^3+13x^2+11x+3=0$; 4) $9x^4-3x^3+7x^2-3x-2=0$;

5) $x^4-2x^3-4x^2+2x+3=0$; 6) $2x^4-x^3-7x^2+3x+3=0$.

II.

1) $3x^3-11x^2-x+1=0$, dacă are rădăcina $x_1=2+\sqrt{3}$;

2) $x^3-3x^2-5x+7=0$, dacă are rădăcina $x_1=1-2\sqrt{2}$;

3) $x^4-2x^3-2x-1=0$, dacă are rădăcina $x_1=1-\sqrt{2}$;

4) $x^4-6x^3+8x^2-2x-1=0$, dacă are rădăcina $x_1=2+\sqrt{5}$.

III.

1) $x^5-3x^4-x^3+7x^2-2x-2=0$, dacă are rădăcinile $x_1=-\sqrt{2},\ x_2=1+\sqrt{2}$;

2) $x^5-10x^4+3x^3-38x^2+6x+4=0$, dacă are rădăcinile $x_1=2+\sqrt{2},\ x_2=2+\sqrt{5}$;

3) $x^6-10x^5+32x^4-30x^3-19x^2+40x-14=0$, dacă are rădăcinile $x_1=2-\sqrt{2},\ x_2=3-\sqrt{2}$.

IV.

1) $x^3+x+10=0$, dacă are rădăcina $x_1=1-2i$;

2) $x^3-5x^2+7x+13=0$, dacă are rădăcina $x_1=3+2i$;

3) $x^4-6x^3+7x^2+18x-30=0$, dacă are rădăcina $x_1=3+i$;

4) $2x^4+x^3-x^2+x-3=0$, dacă are rădăcina $x_1=i$.

V.

1) $x^6-4x^5+10x^4-10x^3-x^2+14x-10=0$, dacă are rădăcinile $x_1=1+i, x_2=1-2i$;

2) $x^6-2x^5+x^4+2x^3-4x^2+4x-4=0$, dacă are rădăcinile $x_1=i, x_2=1-i$.

77. **a) Să se rezolve ecuațiile de mai jos dacă au cel puțin o rădăcină reală:**

1) $z^3+(2-i)z^2-(2i+15)z+15i=0$; 2) $z^3+(3-i)z^2-(1+4i)z-3i-3=0$;

3) $z^3-iz^2+(i-7)z+6i-6=0$; 4) $z^4+2z^3+(-6+5i)z^2+(-17+15i)z+10(i-1)=0$;

5) $z^4-(2+i)z^3+(-1+2i)z^2+(2+i)z-2i=0$.

b) Să se rezolve ecuațiile următoare știind că admit cel puțin o rădăcină întreagă:

1) $x^3-(8-\sqrt{3})x^2+2(\sqrt{3}-3)x+108-48\sqrt{3}=0$; 2) $x^3+(\sqrt{3}-3)x^2+(2-3\sqrt{3})x+2\sqrt{3}=0$;

3) $\sqrt{5}x^3+(1-\sqrt{5})x^2+(-4-2\sqrt{5})x+4=0$.

c) Să se rezolve ecuațiile de mai jos știind că admit rădăcini independente de m:

1) $x^3+(m+2)x^2+(m-5)x-6m-6=0$;

2) $-2x^3+(m+13)x^2-(7m+14)x+12(m+1)=0$;

3) $x^3-(3m+1)x^2+(3m-2)x+6m=0$;

4) $x^4-(m+2)x^3-(2m^2-3m+1)x^2+2(m^2+1)x+4m(m-1)=0$;

5) $x^4-(m-1)x^3-(2m^2+m+2)x^2-(2m^2-2m)x+4m^2=0$.

d) Să se arate că ecuațiile de mai jos au ca rădăcini numerele înscrise în dreptul lor:

1) $x^3+3\sqrt[3]{2}x-2=0,\ x=\sqrt[3]{\sqrt{3}+1}-\sqrt[3]{\sqrt{3}-1}$;

2) $x^3-3x-4=0,\ x=\sqrt[3]{2+\sqrt{3}}+\sqrt[3]{2-\sqrt{3}}$;

3) $x^3-9x-2\sqrt{31}=0,\ x=\sqrt[3]{\sqrt{31}+2}+\sqrt[3]{\sqrt{31}-2}$.

e) Să se arate că următoarele numere sunt întregi:

1) $\sqrt[3]{\sqrt{5}+2}-\sqrt[3]{\sqrt{5}-2}$; 2) $\sqrt[3]{38+\sqrt{1445}}+\sqrt[3]{38-\sqrt{1445}}$;

3) $\sqrt[3]{9+4\sqrt{5}}+\sqrt[3]{9-4\sqrt{5}}$.

f) Să se rezolve și discute ecuațiile după valorile parametrului real a:

1) $x^3-ax^2-(a+1)x+2a^2-2a=0$;

2) $x^3-(a+2)x^2+(2a+1)x-a^2-a=0$;

3) $x^3+(a-3)x^2+2x+a^2-2a=0$.

78. **Să se rezolve ecuațiile:**

I.

1) $x^5-2x^4-14x^3+28x^2+9x-18=0$, dacă are rădăcina $x_1=\sqrt{2}+\sqrt{5}$;

2) $x^5-3x^4-24x^3+72x^2+4x-12=0$, dacă are rădăcina $x_1=\sqrt{7}-\sqrt{5}$;

3) $x^5+x^4-16x^3-16x^2+4x+4=0$, dacă are rădăcina $x_1=-\sqrt{3}-\sqrt{5}$.

II.

1) $x^5+2x^3+6x^2+49x+147=0$, dacă are rădăcina $x_1=\sqrt{3}+2i$;

2) $x^5-x^4-4x^3+4x^2+16x-16=0$, dacă are rădăcina $x_1=\sqrt{3}-i$.

79. **Să se determine parametrii raționali m, n și să se rezolve ecuațiile de mai jos dacă acestea au soluțiile indicate în dreptul fiecăreia:**

1) $x^3+(m+2)x^2-(n-1)x+1=0,\ x=1-\sqrt{2}$;

2) $x^3+(m+1)x^2+nx-1=0,\ x=1+\sqrt{2}$;

3) $x^5-3x^4-3(m+n)x^3+72x^2+(m-n)x-12=0,\ x=\sqrt{7}+\sqrt{5}$;

4) $x^6-(2m+n)x^4+21x^2+7m-2n=0,\ x=\sqrt{2}-\sqrt{3}$.

80. **Să se determine parametrii reali m, n și să se rezolve ecuațiile dacă acestea au soluțiile indicate în dreptul fiecăreia:**

1) $x^4-2x^3+4x^2+2mx-n=0,\ x=1+i$;

2) $x^4-2mx^3+2(m+n)x^2+4x-20=0,\ x=1+3i$;

3) $x^4-2x^3+mx^2+(n+1)x+5=0,\ x=1-2i$;

4) $x^6-(2m+3n)x^5+14x^4-12x^3-5x^2+18x+2m-3n=0,\ x=2+i,\ x=1-i$.

81. **Să se determine parametrii reali m, n astfel încât ecuațiile de mai jos să aibă *rădăcina dublă* indicată:**

1) $x^4-mx^3+2mx^2+(m+n)x-m+4=0,\ x=-1$;

2) $x^3+x^2+mx-n=0,\ x=-1$;

3) $3x^4+(m-n)x^3+(n+1)x^2-2mx+2n-m=0,\ x=-1$;

4) $x^4-(m+n)x^3+(m+5)x^2-18x+27=0,\ x=3$.

82. **Să se determine parametrii reali m, n, p astfel încât ecuațiile de mai jos să aibă *rădăcina triplă* indicată:**

1) $x^4+8x^3-(m+3)x^2+(n+p)x+p-3=0,\ x=1$;

2) $x^4+3x^3-mx^2+(n+2)x+p-1=0,\ x=-1$;

3) $x^4-mx^3-nx+p=0,\ x=-1$;

4) $x^4+mx^3-(n+1)x^2+(p+2)x-2=0,\ x=1$;

5) $x^4+mx^3+nx+p=0,\ x=-1$.

83. Pentru fiecare din ecuațiile de mai jos să se calculeze sumele indicate (x_i fiind rădăcinile ecuației):

1) $x^3+2x^2+3x+4=0$;

a) $\sum x_1^2$; b) $\sum x_1^3$; c) $\sum x_1^4$; d) $\sum x_1^5$; e) $\sum \frac{1}{x_1}$; f) $\sum \frac{1}{x_1^2}$; g) $\sum \frac{1}{x_1+1}$;

h) $\begin{vmatrix} x_{\sigma(1)} & x_{\sigma(2)} & x_{\sigma(3)} \\ x_{\sigma(2)} & x_{\sigma(3)} & x_{\sigma(1)} \\ x_{\sigma(3)} & x_{\sigma(1)} & x_{\sigma(2)} \end{vmatrix},\ \sigma\in S_3$.

2) $x^3-3x^2+2x-6=0$;

a) $\sum x_1^2$; b) $\sum x_1^3$; c) $\sum x_1^4$; d) $\sum \frac{1}{x_1}$; e) $\sum \frac{1}{x_1^2}$; f) $\sum \frac{1}{x_1+1}$.

3) $x^3-5x^2+3x-1=0$;

a) $\sum x_1^2$; b) $\sum x_1^3$; c) $\sum x_1^4$; d) $\sum \frac{1}{x_1}$; e) $\sum \frac{1}{x_1^2}$; f) $\sum \frac{1}{x_1+1}$; g) $\begin{vmatrix} x_{\sigma(1)}^2 & x_{\sigma(2)} & x_{\sigma(3)} \\ x_{\sigma(2)} & x_{\sigma(3)}^2 & x_{\sigma(1)} \\ x_{\sigma(3)} & x_{\sigma(1)} & x_{\sigma(2)}^2 \end{vmatrix}$.

4) $x^3-2x^2+3x-1=0$;

a) $\sum x_1^2$; b) $\sum x_1^3$; c); $\sum \frac{1}{x_1}$ d) $\sum \frac{1}{x_1^2}$; e) $\sum \frac{1}{x_1^3}$;

84. Să se calculeze $P(x_1)+P(x_2)+P(x_3)$ unde x_i sunt rădăcinile ecuației, iar P reprezintă un polinom dat în cazurile:

1) $x^3+3x+1=0,\ P=X^4+2X^3-X^2+3X-2$;

2) $2x^3+3x-1=0,\ P=X^5+3X^4-2X^3+X^2-X+3$;

3) $x^3-4x+2=0,\ P=X^5-2X^4-4X^3-4X^2+5X-6$.

85. Să se determine parametrul real m şi să se rezolve ecuațiile ştiind că rădăcinile reale sunt în progresie aritmetică:

1) $x^3-12x^2+mx-28=0$;   2) $x^3-mx^2-2mx+8=0$;

3) $x^3-3mx^2+(2m-1)x+5m=0$;   4) $x^4+(m-5)x^3-2mx^2+2m-1=0$;

5) $x^4-(m+4)x^3+5(m+1)x^2-(8m+2)x+4m=0$.

86. Să se determine parametrii reali m, n pentru care rădăcinile ecuațiilor de mai jos sunt în progresie aritmetică:

1) $x^4-8x^3+(2m-n)x^2+(m-3n)x+41=0$;

2) $x^4-4x^3+(m-2n)x^2+(m+3n)x+17=0$;

3) $x^4-4x^3+(m+n)x^2+(m-n)x+52=0$.

87. Să se arate că rădăcinile ecuației $x^3+3(1-\sqrt{2})x^2+(5-6\sqrt{2})x+3-\sqrt{2}=0$ sunt în progresie aritmetică şi să se rezolve ecuația.

88. Să se determine parametrul real m dacă rădăcinile reale ale ecuațiilor de mai jos sunt în progresie geometrică:

1) $x^3-(2m+5)x^2+(4m+3)x-27=0$; 2) $x^3+3mx^2+(5m-1)x+8=0$;

3) $x^3-31x^2+155x-m-5=0$.

89. Să se determine parametrul real m şi să se rezolve ecuațiile de mai jos, dacă între rădăcini are loc relația indicată:

I.

1) $2x^3+x^2-13x+m=0,\ x_1x_2=1$;

2) $x^3-mx^2-4x+2=0,\ x_1+x_2=0$;

3) $x^3-mx^2+2mx-1=0, \sum x_1^2=0$;

4) $x^3+mx^2+11x+m=0,\ x_1+x_2=x_3^2$;

5) $mx^3-(m+2)x^2+9x-1=0,\ \dfrac{2}{x_2}=\dfrac{1}{x_1}+\dfrac{1}{x_3}$;

6) $x^3-(m+2)x^2+(2m+1)x-m=0,\ \dfrac{1}{x_1}+\dfrac{1}{x_2}=\dfrac{3}{2x_3}$.

II.

1) $x^4+mx^3-3x^2-4x+4=0,\ \ x_1=x_2,\ x_3=x_4$;

2) $x^4-2x^3+mx^2+8x+12=0,\ \ x_1x_2=-4$;

3) $x^4-4x^3+mx^2+4x-3=0,\ \ x_1+x_2=x_3+x_4$;

4) $x^4-2x^3-23x^2-12x+m=0,\ \ x_1x_2=x_3x_4$;

5) $x^4-x^3-2x^2+mx+m+2=0,\ \ x_1+x_2=x_3x_4$.

90. Să se determine parametrul real m dacă între rădăcinile ecuațiilor de mai jos există o relație indicată:

I.

1) $x^3-(m+1)x^2+2x+m-2=0$;

1°) $x_1x_2+x_1x_3+x_2x_3>(x_1+x_2+x_3)^2$; 2°) $(x_1+x_2+x_3)\left(\dfrac{1}{x_1}+\dfrac{1}{x_2}+\dfrac{1}{x_3}\right)\geq 9$;

3°) $\left(x_1^2+x_2^2+x_3^2\right)<\dfrac{(x_1+x_2+x_3)^2}{3}$; 4°) $x_1^3+x_2^3+x_3^3\geq(m+1)\left(x_1^2+x_2^2+x_3^2\right)-3m+6$;

5°) $\dfrac{x_1^2+x_2^2+x_3^2}{x_1x_2x_3}<2(x_1+x_2+x_3)$; 6°) $x_1^3+x_2^3+x_3^3\geq(x_1+x_2+x_3)^3$.

2) $x^3+mx^2+x+m-1=0$,

1°) $(\sum x_1)^2 \le \sum x_1^2$; 2°) $2m(\sum x_1)^2+\sum x_1^3 \ge m^2-1$;

3°) $(m-1)\sum\frac{1}{x_1^2} > 3\sum\frac{1}{x_1}$; 4°) $\sum\frac{1}{x_1+1} > \frac{1}{3}\sum x_1$;

5°) $\sum\frac{x_1+x_2}{x_3} \le \prod x_1$; 6°) $(\sum x_1)\left(\sum x_1^2\right) \ge \sum x_1^3$.

3) $x^3-mx^2+4x-m+2=0$,

1°) $(\sum x_1)\left(\sum\frac{1}{x_1}\right) < 3$; 2°) $\sum x_1^2 \le (\sum x_1)^2$;

3°) $\sum\frac{1}{x_1} > (m-2)\sum\frac{1}{x_1^2}$; 4°) $\sum x_1^3 \ge (\sum x_1)\left(\sum x_1^2\right)$;

5°) $\sum\frac{1}{x_1+1} \le 0$; 6°) $\sum x_1^3 \ge (\prod x_1)^3-1$.

4) $x^3-(m-1)x^2+2mx-1=0$,

1°) $(\sum x_1)(\sum x_1x_2) \le \sum x_1^2$; 2°) $\sum x_1^3 > \left(\sum x_1^2\right)(\sum x_1)$; 3°) $(\sum x_1x_2)(\sum x_1) \ge \sum\frac{1}{x_1^2}$.

II.

1) $x^4+(m-1)x^2-mx+1=0$,

1°) $\left(\sum x_1^2\right)\left(\sum x_1^3\right) \ge \sum\frac{1}{x_1^2}$; 2°) $\left(\sum x_1^2\right)\left(\sum\frac{1}{x_1^2}\right) \le -2\left(\sum\frac{1}{x_1}\right)^3$; 3°) $\frac{\sum\frac{1}{x_1^2}}{\sum x_1^2} \ge \sum x_1^3$;

4°) $\left(\sum\frac{1}{x_1}\right)^2 \ge \sum\frac{1}{x_1^2}$; 5°) $\left(\sum x_1^2\right)^2 < \left(\sum x_1^3\right)^3+4$;

2) $x^4+(m+1)x^3-2mx+m+3=0$,

1°) $(\sum x_1)^2+\sum x_1^2 \ge x_1x_2x_3x_4(\sum x_1x_2x_3)$; 2°) $(\sum x_1)\left(\sum\frac{1}{x_1}\right) \ge \sum\frac{1}{x_1^2}$;

3°) $-m\left(\sum x_1^2\right) < \sum x_1^3$; 4°) $(\sum x_1)^3 \le \sum x_1^3$; 5°) $(\sum x_1)\left(\sum\frac{1}{x_1^2}\right) > \sum\frac{1}{x_1}$.

3) $x^4-(m+1)x^2+m=0$,

1°) $(\sum x_1x_2)^2 > \sum x_1^2$; 2°) $\sum x_1^2+\sum x_1^3 \le \sum\frac{1}{x_1^2}$; 3°) $\sum x_1^4 \ge \sum x_1^3$;

4°) $\sum x_1^4 \ge \sum x_1^6$; 5°) $\sum\frac{1}{x_1^3} < \sum\frac{1}{x_1^2}$.

91. **Să se formeze ecuațiile de gradul trei având rădăcinile:**

1) $-1; 1; 3$; 2) $-2; 0; 1$; 3) $-\frac{1}{2}; \frac{1}{2}; 1$; 4) $-5; 1; 5$; 5) $2; 4; 6$.

92. Să se formeze ecuația de gradul patru de rădăcini:

1) $0; -1; 1; 2;$ 2) $-3; -1; 1; 3;$ 3) $-2; -1; 2; 3;$ 4) $\frac{1}{2}; \frac{1}{3}; -\frac{1}{2}; 1;$ 5) $1; 1; 1; 2.$

93. Utilizând ecuațiile de gradul trei să se rezolve sistemele simetrice de ecuații:

1) $\begin{cases} x+y+z=2 \\ xy+yz+zx=-1 \\ xyz=-2 \end{cases};$ 2) $\begin{cases} x+y+z=9 \\ \frac{1}{x}+\frac{1}{y}+\frac{1}{z}=1 \\ xyz=27 \end{cases};$ 3) $\begin{cases} x+y+z=1 \\ xy+yz+xz=-4 \\ x^3+y^3+z^3=1 \end{cases};$

4) $\begin{cases} x+y+z=0 \\ x^2+y^2+z^2=6 \\ x^3+y^3+z^3=6 \end{cases};$ 5) $\begin{cases} x+y+z=10 \\ x^2+y^2+z^2=38 \\ x^4+y^4+z^4=722. \end{cases}$

94. Dacă x_1, x_2, x_3 sunt rădăcinile ecuației în x, $x^3+2x^2+3x-2=0$, atunci să se formeze ecuațiile în y de rădăcini y_1, y_2, y_2 pentru cazurile de mai jos:,

1°) $y_1 = x_2+x_3;\ y_2 = x_1+x_3;\ y_3 = x_1+x_2;$ 2°) $y_1 = \frac{x_1}{x_2+x_3};\ y_2 = \frac{x_2}{x_1+x_3};\ y_3 = \frac{x_3}{x_1+x_2};$

3°) $y_1 = \frac{1}{x_1};\ y_2 = \frac{1}{x_2};\ y_3 = \frac{1}{x_3};$ 4°) $y_1 = \frac{1}{x_1^2};\ y_2 = \frac{1}{x_2^2};\ y_3 = \frac{1}{x_3^2};$

5°) $y_1 = \frac{x_2+x_3}{x_1+1};\ y_2 = \frac{x_1+x_3}{x_2+1};\ y_3 = \frac{x_1+x_2}{x_3+1};$ 6°) $y_1 = x_1^2; y_2 = x_2^2;\ y_3 = x_3^2;$

7°) $y_1 = x_1^3;\ y_2 = x_2^3;\ y_3 = x_3^3;$ 8°) $y_1 = x_1^4;\ y_2 = x_2^4;\ y_3 = x_3^4;$

9°) $y_1 = \frac{3x_1}{3x_1+x_2+x_3};\ y_2 = \frac{3x_2}{3x_2+x_1+x_3};\ y_3 = \frac{3x_3}{3x_3+x_1+x_2};$

10°) $y_1 = \frac{x_2^2+x_3^2}{x_1};\ y_2 = \frac{x_1^2+x_3^2}{x_2};\ y_3 = \frac{x_1^2+x_2^2}{x_3}.$

95. Dacă a este o rădăcină a ecuației x, atunci să se determine ecuația de grad minim în y, care are ca rădăcină expresia lui y indicată în fiecare caz:

1) $x^3-x-1=0,\quad y=2a^2-a;$ 2) $x^3-x+1=0,\quad y=a^6+2a-1;$

3) $x^3-2x-1=0,\quad y=a^4-a+1.$

96. Să se determine parametrul real a pentru care ecuațiile de mai jos au o singură rădăcină reală comună:

1) $x^2+ax-2=0;\ x^3+x^2-2x+a-1=0;$

2) $x^2+(a+1)x-2=0;\ 2x^3+ax^2-x-1=0;$

3) $x^2+3x+a-2=0;\ x^3+2x^2+ax+8=0.$

97. Să se determine parametrul real a pentru care ecuațiile de mai jos au o singură rădăcină reală comună:

1) $x^3-6x^2+11x+a=0;\ x^3+4x^2+x+a=0;$

2) $x^3+ax^2-x-1=0; x^3+ax-2=0.$

98. **Să se determine $a,b \in \mathbb{Z}$ ştiind că ecuaţiile $x^3+2x^2+ax+b=0,\ x^3-x^2+bx+a=0$ admit o rădăcină comună întreagă.**

99. **Să se determine parametrul real a pentru care ecuaţiile de mai jos să aibă două rădăcini comune:**

1) $x^3-4x^2+x+a=0;\ x^3+x^2-(a+1)x-4=0$;

2) $x^3+(a+7)x^2+x-6=0;\ x^3-(a-2)x^2+2x-5+a=0$;

3) $x^3-x^2-(a+10)x+24=0;\ \ x^3-ax^2+x+6=0$.

100. **Să se determine parametrii reali a, b pentru care ecuaţiile următoare au două rădăcini comune:**

1) $x^3+ax^2+18=0;\ x^3+bx+12=0;$

2) $x^4-2x^3-x+a=0;\ x^4-4x^3+6x^2-5x+b=0$;

3) $x^3+ax+b=0;\ \ x^4+3bx+a=0$.

101. **Să se arate că dacă ecuaţiile $x^5+ax^2+bx+1=0,\ x^5+mx^2+nx+1=0$, au o rădăcină dublă comună, atunci ele au toate rădăcinile comune.**

102. **Să se determine numerele reale a, b, c astfel încât ecuaţiile următoare să aibă aceleaşi rădăcini:**

1) $x^3+(2b+1)x^2+(b-c)x+b+c=0;\ \ 2x^3+(2a+2b)x^2+(a-c)x+2a=0$;

2) $x^3+(a+b)x^2-(b+c)x+a+c=0;\ x^3-(2a+3c)x^2+(2b-c)x+2c-a+3=0$;

3) $x^3+bx^2+(2a-b)x-a+c=0;\ x^3+(a-c)x^2+(2c+b)x+b+a=0$.

103. **Să se găsească un număr real nenul a pentru care ecuaţia $x^3+(-4+i)x^2-(1+i)x+a=0$ are o rădăcină reală.**

104. **Să se arate că ecuaţia $ax^3+x^2-ax+a=0$ nu admite nici o rădăcină reală dacă $a \in \mathbb{C}-\mathbb{R}$.**

105. **Să se arate că ecuaţia $x^4+(a+1)x^3+\left(a^2+\frac{a}{2}+1\right)x^2+bx+c=0,\ a,b,c \in \mathbb{R}$ are cel mult două rădăcini reale.**

Teste de evaluare

TESTUL 1

VARIANTA A

1. Pe mulțimea $\mathbb{Z}$ definim legile de compoziție $x \perp y = x + y - 3$, $x \top y = xy - 3(x+y) + 12$, $(\forall) x, y \in \mathbb{Z}$. Arătați că $(\mathbb{Z}, \perp, \top)$ este un inel integru și determinați elementele inversabile ale inelului.

2. Fie $a, b, c \in \mathbb{R}$. Pe $\mathbb{R}$ definim legile de compoziție $x \perp y = ax + by - 2$, $x \top y = xy - 2(x+y) + c$, $(\forall) x, a \in \mathbb{R}$.

1) Să se determine *a*, *b*, *c* astfel încât $(\mathbb{R}, \perp, \top)$ să fie corp;

2) Arătați că există un izomorfism de corpuri $f : (\mathbb{R}, +, \cdot) \to (\mathbb{R}, \perp, \top)$, $f(x) = \alpha x + \beta$, $\alpha, \beta \in \mathbb{R}$.

3. a) Să se determine $a \in \mathbb{Z}_3$ astfel încât polinomul: $P = \hat{2}X^3 + (a + \hat{2})X + \hat{1} \in \mathbb{Z}_3[X]$ să fie ireductibil pe $\mathbb{Z}_3$.

b) Să se rezolve sistemul următor în $\mathbb{Z}_5$:

$$\begin{cases} \hat{3}x + \hat{2}y = \hat{3} \\ \hat{2}x + \hat{3}y = \hat{2}. \end{cases}$$

4. Se consideră funcția $f : \mathbb{Z}_5 \to \mathbb{Z}_5$ definită prin următoarele condiții: $f(\hat{0}) = \hat{2}$, $f(\hat{1}) = \hat{0}$, $f(\hat{2}) = \hat{3}$, $f(\hat{3}) = \hat{4}$, $f(\hat{4}) = \hat{1}$. Să se determine funcția polinomială.

5. Să se determine parametrul real *a* astfel încât ecuația $x^4 + 2x^3 + ax^2 + 2x + 1 = 0$ să aibă toate rădăcinile reale.

6. a) Se consideră cilindrul circular drept cu raza bazei *x* și înălțimea *h*. Dacă aria totală este 300π cm², iar volumul este de 500π cm³, să se determine *x* și *h*.

b) Să se rezolve ecuația $x^3 + 24 < x(x + 14)$.

VARIANTA B

1. Fie $\mathcal{F} = \{f : \mathbb{R} \to \mathbb{R}\}$ împreună cu operațiile: $(f+g)(x) = f(x) + g(x), (fg)(x) = f(x)g(x)$, $(\forall) x \in \mathbb{R}$. Să se arate cp $(\mathcal{F}, +, \cdot)$ este inel comutativ cu divizori ai lui zero.

2. Să se arate că structurile de inel definite prin mulțimile $A = \left\{x + y\sqrt{2} \,\middle|\, x, y \in \mathbb{Z}\right\}$ și $B = \left\{x + y\sqrt{3} \,\middle|\, y, x \in \mathbb{Z}\right\}$ nu sunt izomorfe.

3. a) Să se arate că polinomul $f = X^4 + mX^3 + (2m^2 + 1) + nX + p$, $m, n, p \in \mathbb{R}$ are cel mult două rădăcini reale.

b) Să se determine $n \in \mathbb{N}^*$ astfel încât polinomul $f = (X^5 + 1)^{3n} + (X^4 + X)^n$ să se dividă la polinomul $g = X^3 - X^2 + 1$.

4. a) Să se arate că ecuația $(x+i)^n + (x-i)^n = 0$, $n \in \mathbb{N}, n \geq 2$ are toate rădăcinile reale.

b) Fie ecuația $x^4 - 2x^3 + x^2 - 1 = 0$, cu rădăcinile x_1, x_2, x_3, x_4 iar $f = X^6 + 5X^5 - 2X^4 + X^3 - 3X^2 + 1$. Să se calculeze:

$$f(x_1) + f(x_2) + f(x_3) + f(x_4).$$

5. Să se rezolve sistemele de ecuații:

a) $\begin{cases} x + y + z = -1 \\ x^2 + y^2 + z^2 = 9 \\ x^3 + y^3 + z^3 = -1 \end{cases}$ b) $\begin{cases} 2x + \widehat{10}x + z = 4 \\ x + \hat{3}z = \hat{2} \\ \widehat{10}x + \hat{2}y + \hat{2}z = \hat{1} \end{cases}$

în $\mathbb{Z}_{11}$.

6. a) Volumul unui ghețar tractat din Antarctica spre Africa este de *V* după *n* zile dat de formula $V(n) = \frac{400\pi}{3}(30 + 29n + 29n^2 - n^3)$.

După câte zile se va topi complet ghețarul?

b) Să se rezolve ecuația $\sqrt[3]{x+1} = \sqrt{x-3}$.

TESTUL 2

VARIANTA A

1. Fie $A=\begin{pmatrix}\hat{1} & \hat{1}\\ \hat{1} & \hat{0}\end{pmatrix}\in\mathcal{M}_2(\mathbb{Z}_2)$. Să se arate că mulțimea $\mathcal{K}=\{O_2, I_2, A, A^2\}$ înzestrată cu operațiile de adunare și înmulțire ale matricelor formează un corp.

2. Fie mulțimea $A=\{aX+b \mid a,b\in\mathbb{R}\}$. Pe $A\subset\mathbb{R}[X]$ considerăm operația de adunare obişnuită și operația „$*$“ definită astfel: dacă $f,g\in A$, atunci $f*g$ este restul împărțirii lui $f\cdot g$ la X^2-1.

a) Să se arate că $(A,+,*)$ este inel comutativ cu divizori ai lui zero;

b) Este $\varphi:(A,+,*)\to(\mathbb{C},+,\cdot), \varphi(aX+b)=a+bi$ izomorfism de inele?

3. Să se descompună în factori ireductibili polinoamele:

a) $f=X^3+\hat{2}X^2+\hat{4}X+\hat{3}\in\mathbb{Z}_5[X]$;

b) $f=X^4+1\in\mathbb{Q}[X]$ (peste $\mathbb{Q}$).

4. a) Să consideră matricea:

$$A=\begin{pmatrix}\hat{2} & \hat{1} & \hat{4}\\ \hat{3} & \hat{2} & \hat{1}\\ \hat{6} & \hat{4} & \hat{5}\end{pmatrix}\in\mathcal{M}_3(\mathbb{Z}_8).$$

Să se arate că A este inversabilă și să se calculeze A^{-1}.

b) Să se rezolve în $\mathbb{Z}_8$ sistemul:

$$\begin{cases}2x+y+\hat{4}z=\hat{2}\\ \hat{3}x+\hat{2}y+z=\hat{4}\\ \hat{6}x+\hat{4}y+\hat{5}=\hat{1}\end{cases}.$$

5. Să se determine parametrul real m pentru care ecuațiile $x^3+mx^2-2x-8=0$, $x^3+mx-10=0$ au o singură rădăcină reală comună.

6. a) Să se rezolve ecuația

$$3\left(27^x+27^{-x}\right)-5\sqrt{2}\left(9^x+9^{-x}\right)=0.$$

b) Să se determine punctele de intersecție ale graficului funcției $f:\mathbb{R}\to\mathbb{R}, f(x)=6x^3-7x^2+1$ cu axa Ox.

VARIANTA B

1. Fie $a,b,c,m,n\in\mathbb{Z}$. Pe $\mathbb{Z}$ definim legile de compoziție $x*y=ax+by+c$,

$$x\circ y=xy+m(x+y)+n.$$

a) Să se determine a,b,c,m,n astfel încât $(\mathbb{Z},*,\circ)$ să fie inel.

b) Este inelul $(\mathbb{Z},*,\circ)$ corp?

c) Arătați că inelul $(\mathbb{Z},*,\circ)$ este domeniu de integritate izomorf cu $(\mathbb{Z},+,\cdot)$.

2. Să se determine parametrii $a,b\in\mathbb{R}$ astfel încât ecuația $x^4+x^3+ax+b=0$ să admită o rădăcină triplă nenulă.

3. Se consideră ecuația $x^3-x+a=0$ cu rădăcinile x_1,x_2,x_3. Să se determine $a\in\mathbb{R}$ astfel încât $x_1^6+x_2^6+x_3^6\geq x_1^5+x_2^5+x_3^5$.

4. Se consideră polinomul cu coeficienți reali $f=X^4+2X^3+mX^2+nX+p$.

a) Să se determine parametrii reali m,n,p astfel încât polinomul f împărțit la $X-1$ să dea restul -15, iar ecuația $f(x)=0$ să aibă o rădăcină $x_1=-1+i$;

b) Să se rezolve ecuația $f(x)=0$, pentru m,n,p determinați la a).

5. Pe mulțimea $\mathbb{R}$ se definesc legile $x*y=ax+by-1$, $x\circ y=2(xy-x-y)+c$, $x,y\in\mathbb{R}$, $a,b,c\in\mathbb{R}$. Să se determine parametrii a,b,c astfel încât $(\mathbb{R},*\circ)$ să fie corp comutativ izomorf cu $(\mathbb{R},+,\cdot)$, printr-un izomorfism de forma $f(x)=px+q$.

6. a) Să se rezolve inecuația: $A_x^5\leq 12A_x^3$, $x\in\mathbb{N}$;

b) Să se rezolve sistemul:

$$\begin{cases}2^x+y=5\\ y^2+4y+11=2^{6-x}\end{cases}.$$

TESTUL 3 (grilă)

VARIANTA A

1. Pe $\mathbb{R}\times\mathbb{R}$ se definesc legile de compoziție $x\perp y=ax+by-2, x\top y=xy-2(x+y)+6$ $a\neq 0$, $x,y\in\mathbb{R}$. Valorile lui a, b pentru care tripletul $(\mathbb{R},\perp,\top)$ este inel comutativ sunt:
a) $a=b=-1$; b) $a=b=1$; c) nu există.

2. Fie $\mathbb{Q}(\sqrt{2})=\left\{a+b\sqrt{2}\,\middle|\,a,b\in\mathbb{Q}\right\}$ și $\mathcal{M}=\left\{\begin{pmatrix} a & b\\ 2b & a\end{pmatrix}\middle| a,b\in\mathbb{Q}\right\}$. Atunci funcția $f:(\mathbb{Q}(\sqrt{2}),+,\cdot)\to(\mathcal{M},+,\cdot)$, $f(a+b\sqrt{2})=\begin{pmatrix} a & b\\ \alpha b & a\end{pmatrix}$ este izomorfism de corpuri pentru:
a) $\alpha=2$; b) $\alpha=\sqrt{2}$; c) $\alpha=3$

3. Fie $f=X^3+aX^2+bX+c\in\mathbb{R}[X]$, cu rădăcinile x_1,x_2,x_3. Atunci $S=\frac{x_1}{f'(x_1)}+\frac{x_2}{f'(x_2)}+\frac{x_3}{f'(x_3)}$ este egal cu:
a) 0; b) 1; c) – 1.

4. Polinomul $f=X^3-2\in\mathbb{Q}[X]$ este reductibil
a) peste $\mathbb{Z}$; b) peste $\mathbb{Q}$; c) peste $\mathbb{R}$.

5. Polinomul $f=X^4-4X^3+4X^2+aX+b$ se divide prin polinomul $g=X^2-4X+3$, dacă:
a) $a=b=3$; b) $a=b=-4$; c) $a=-4, b=3$.

6. Rădăcinile ecuației $x^3+3x^2-x+m=0$, $m\in\mathbb{R}$ sunt în progresie aritmetică dacă:
a) $m=3$; b) $m=-3$; c) $m=2$.

7. Fie sistemul de ecuații în $\mathbb{Z}_5$:

$$\begin{cases} x+y+z=\hat{1}\\ \hat{2}x+\hat{3}y+z=\hat{1}\\ \hat{4}x+\hat{4}y+\hat{3}z=\hat{1}\end{cases}$$

cu soluția (x_0,y_0,z_0). Dacă $\alpha=x_0^2+y_0^2+z_0^2$, atunci: a) $\alpha=\hat{4}$; b) $\alpha=\hat{3}$; c) $\alpha=\hat{2}$.

8. Ecuația $x^3-6x^2+ax-8=0, a\in\mathbb{R}$ are toate rădăcinile reale și pozitive dacă:
a) $a=12$; b) $a=10$; c) $a=-12$.

VARIANTA B

1. Mulțimea $\mathcal{M}=\left\{M_a=\begin{pmatrix} a & 0 & a\\ 0 & 0 & 0\\ a & 0 & a\end{pmatrix}\middle| a\in\mathbb{C}\right\}$ cu adunarea și înmulțirea matricelor este:
a) inel cu divizori ai lui zero; b) corp; c) nici una din variante.

2. Pe $\mathbb{R}\times\mathbb{R}$ se definesc legile de compoziție $x\perp y=x+y-2$ și $x\top y=\frac{xy}{4}-\frac{1}{2}(x+y)+3$ $x,y\in\mathbb{R}$. Atunci $(\mathbb{R},\perp,\top)$ este corp izomorf $(\mathbb{R},+,\cdot)$ prin izmorfismul dat de $f:\mathbb{R}\to\mathbb{R}$:
a) $f(x)=x-\frac{1}{2}$; b) $f(x)=\frac{1}{2}(x-1)$;
c) $f(x)=\frac{1}{2}\left(\frac{1}{2}x-1\right)$.

3. Restul împărțirii polinomului: $f=1+X^2+X^4+...+X^{28}+X^{30}$ la polinomul $f=X^2-X$ este polinomul:
a) $r=15X+1$; b) $r=15X-1$; c) $r=15X$.

4. Polinomul $f=X^3+\hat{3}X^2+\hat{2}X+\hat{1}\in\mathbb{Z}_5[X]$ este:
a) ireductibil peste $\mathbb{Z}_5$; b) reductibil peste $\mathbb{Z}_5$.

5. Polinomul $f=X^4+aX^3+bX+c, a,b,c\in\mathbb{R}$ se divide prin polinomul $g=X^3-X$, dacă:
a) $a=0, b=1, c=-1$; b) nu există;
c) $a=-1, b=0, c=1$.

6. Fie ecuația $x^3+x+1=0$ cu rădăcinile $x_1,x_2,x_3\in\mathbb{C}$. Atunci $\Delta=\begin{vmatrix} x_1 & x_2 & x_3\\ x_3 & x_1 & x_2\\ x_2 & x_3 & x_1\end{vmatrix}$ este egal cu: a) 1; b) –1; c) 0.

7. Dacă a,b,c sunt zerourile funcției polinomiale $f:\mathbb{R}\to\mathbb{R}, f(x)=x^3-mx^2+nx-p, m,n,p\in\mathbb{R}$, iar $S=\frac{(b+c)bc}{f'(a)}+\frac{(c+a)ca}{f'(b)}+\frac{(a+b)ab}{f'(c)}$, atunci:
a) $S=m$; b) $S=m+n$; c) $S=m+n+p$.

9. Matricea $A=\begin{pmatrix}\hat{1} & \hat{0} & \alpha\\ \hat{2} & \hat{1} & \hat{0}\\ \hat{1} & \alpha & \hat{2}\end{pmatrix}\in\mathcal{M}_3(\mathbb{Z}_3)$ este inversabilă dacă:

a) $\alpha=\hat{1}$; b) $\alpha\in\{\hat{0},\hat{2}\}$; c) nu există α .

10. Fie $(A,+,\cdot)$ un inel cu proprietatea $a^2=a,(\forall)a\in\mathbb{R}$. Atunci:

a) A este inel comutativ şi $a^2=-a$;

b) A este inel necomutativ şi $a+a=0,(\forall)a\in A$;

c) A este inel comutativ şi $a+a=0,(\forall)a\in A$.

8. Sistemul de ecuații: $\begin{cases}ax+y+z=\hat{1}\\ \hat{2}x+\hat{3}y+az=a\\ x+ay+z=a^2\end{cases}$ cu coeficienți în $\mathbb{Z}_7$ este compatibil nedeterminat dacă:

a) $a\in\{\hat{2},\hat{4}\}$; b) $a\in\{\hat{5},\hat{6}\}$; c) $a\in\{\hat{1},\hat{3}\}$.

9. Matricea $A=\begin{pmatrix}\hat{1} & \hat{0} & \alpha\\ \alpha & \hat{1} & \hat{2}\\ \hat{4} & \hat{3} & \hat{1}\end{pmatrix}\in\mathcal{M}_3(\mathbb{Z}_6)$ este inversabilă dacă:

a) $\alpha=\hat{2}$; b) $\alpha=\hat{3}$; c) $\alpha=\hat{4}$.

10. Fie $(A,+,\cdot)$ inel în care $a^6=a,(\forall)a\in A$. Atunci:

a) $a^2=a,(\forall)a\in A$;

b) $a^2\neq a,(\forall)a\in A$;

c) $a+a\neq 0,(\forall)a\in A, a\neq 0$.

INDICAȚII ȘI RĂSPUNSURI

Capitolul 1. Grupuri

Parte stabilă. 6. $x\in H \Leftrightarrow 1<x<3 \Leftrightarrow -1<x-2<1 \Leftrightarrow |x-2|<1$; **7.** $x=4+\alpha, y=4+\beta, \alpha,\beta\ge 0\Rightarrow$ $\Rightarrow x\perp y=4+5\alpha\beta\ge 4$; **12.** $H\subseteq\mathbb{R}, H\ne\varnothing, x\in H\Rightarrow 2x=x+x, 3x, ..., nx, ...\in H$. Cum H este finită $(\exists)i\ne k$ pentru care $ix=kx$. De aici x = 0. Deci $H=\{0\}$. Dacă H este parte stabilă în raport cu înmulțirea, atunci din $x\in H\Rightarrow x^2, x^3, ..., x^n, ...\in H$. Din H finită $(\exists)i<j$ cu $x^i=x^j$ sau $x^i\left(1-x^{j-i}\right)=0$, ceea ce dă x = 0, x = 1 sau x = –1. Deci $H=\{-1,0,1\}$ sau $H=\{0\}, H=\{1\}, H=\{-1,1\}$; **15.** $A^4=E, B=A^2, C=A^3, F=AD, G=A^2D, H=A^3D$; **19.** $f:[a,\infty)\to[a,\infty)$, $f(x)=(y+1)x+y$; $y<-1\Rightarrow$ f s.d. de la $-\infty$ la $f(a)$ și acest caz nu este bun; $y\ge -1\Rightarrow$ f crescătoare și $f(a)\ge a, (\forall)y\ge -1$. Deci $(y+1)a+y\ge a\Leftrightarrow y(a+1)\ge 0, (\forall)y\ge -1$. Rezultă $a=-1$; **20.** 1) $a\ge 6$; 2) $a=1$; **21*.** Vezi problema 12.

Asociativitatea. 2. Toate; **6.** $m\in\{0,1\}$; **7.** $a\in\left\{0,\frac{1}{2}\right\}$; **8.** $a=b=1$; $c=3$;

Comutativitatea. 2. $2*3=3\ne 3*2=4$; **7.** Tabla legii este simetrică în raport cu diagonala principală; **8.** $A_a\cdot A_b=A_{ab}=A_{ba}=A_b\cdot A_a$; **12.** $x*y=y*x, (\forall)x,y\Rightarrow b=2a$, iar din asociativitate $\Rightarrow a_1=0, a_2=\frac{1}{2}$; $a_1=b_1=0\Rightarrow$ $x*y=xy$; $a_2=\frac{1}{2}, b_2=1\Rightarrow$ $x*y=xy+x+y$; **13.** $a=-b=1$; **14.** c); **15.** a) $a=5$; b) $a=2$; **16.** 1) $a=b\in\{0,1\}, c\in\mathbb{R}$; 2) a = 2; 3) $a=b\in\{-2,3\}$; 4) a = 12; 5) $a\in\{7,-6\}$; 6); $a=b=-2$.

Element neutru. 1. $1\circ 2=3\ne 2\circ 1=1, (1\circ 2)\circ 1=2\ne 1\circ(2\circ 1)=0, e=0$; **6.** $x,y\ge 2\Rightarrow x*y\ge 2\Rightarrow$ $\Rightarrow (x-2)(y-2)+m-4\ge 2\Rightarrow m\ge 6$; $e=3, m=6$; **8.** Din asociativitate rezultă $a_1=0, a_2=1$; $a=0\Rightarrow x*y=-xy$; $e=-1$; $a=1\Rightarrow$ $x*y=x+y-xy$, $e=0$; **9.** $c=3, e=\frac{3}{2}$; **10.** Asociativitatea $\Rightarrow a=b$ și $a^2=a+c$; $x*e=x, (\forall)x\Rightarrow a+e=1$ și $be+c=0$; **12.** $a=5, b=20, e=-4$.

Element simetric. 1. $e=1, 1^{-1}=1, 5^{-1}=5$; **3.** $e=-\frac{5}{3}, x'=-2+\frac{1}{9(x+2)}>-2$; **5.** $x\in H\Leftrightarrow |x|<1$; $e=0, x'=x$; **7.** $H=\left\{X, X^2, X^3, X^4=I_4\right\}, I_4^{-1}=I_4, X^{-1}=X^3, \left(X^2\right)^{-1}=X^2, \left(X^3\right)^{-1}=X$; **8.** $e=\frac{1}{2}, x'=1-x\in(0,1)$; **9.** $A_\alpha\cdot A_\beta=A_{\alpha+\beta}, A_0=I_2\in H, A_\alpha^{-1}=A_{-\alpha}$.

Grupuri. 2. $e=1, x'=2-x$; **3.** $e=0, x'=-\frac{x}{x+1}>-1$; **4.** $e=0, x'=\frac{x}{x-1}>1$; **6.** $u=e^{\frac{1}{3}}, x'=e^{\frac{1}{9\ln x}}>0$; **8.** $e=0, x'(1-ax)=-x$. Dacă $x=1\Rightarrow x'(1-a)=-1\Rightarrow x'=-\frac{1}{1-a}\in\mathbb{Z}\Leftrightarrow a-1\in\{\pm 1\}\Rightarrow a\in\{0;2\}$. Dacă $a=0$, ecuația $x'(2x-1)=x$ nu are soluții $x'\in\mathbb{Z}, (\forall)x\in\mathbb{Z}$. Dacă $a=0\Rightarrow x'=-x\in\mathbb{Z}$ și în acest caz $(\mathbb{Z},\circ)$ este grup abelian; **9.** a) $\lambda\ge 2$; b) $x^n=(x-1)^n+1, (\forall)n\in\mathbb{N}$, inductiv;

$e=2, x'=\frac{x}{x-1}>1$; 10. $e=m+1,\ x'=\frac{1-m^2+mx}{x-m}$; 11. $x\top e=x,(\forall)x\in G\Rightarrow m_1=2,\ m_2=-\frac{3}{2}$; $e\top x=x,\ (\forall)x\in G\Rightarrow e=-\frac{1}{2},\ m=2$ sau $m=-1$. Din $x\top e=e\top x=x,\ (\forall)x\in G\Rightarrow a=0$, $e=-\frac{1}{2},\ m=2,\ x'=-\frac{4x+3}{4(x+1)}\in G$; 12. $a=b=1$; 13. $a=b=1$; 14*. $x\circ e=e\circ x=x,\ (\forall)x\Rightarrow$ $\Rightarrow a=b,\ e=1-a>1$ ($\Rightarrow a<0$) și $c=a^2-a$. Din $x\circ x=x^2+2ax+a^2-a>1,\ (\forall)x\Rightarrow$ $\Rightarrow \lim\limits_{x\searrow 1}(x^2+2ax+a^2-a)=a^2+a+1\geq 1\Rightarrow a(a+1)\geq 0$. Cum $a<0\Rightarrow a+1\leq 0\Rightarrow a\leq -1$. Dacă $a<-1$, atunci $x=\frac{1-a}{2}\circ y>1,\ (\forall)y>1\Rightarrow y+a-2<0,\ (\forall)y>1$, fals. Deci $a=-1$; 19. 1) Dacă există $\alpha\in G, \alpha\neq 0$, atunci $2\alpha, 3\alpha, ...\in G\Rightarrow G$ infinit, fals. Deci $\alpha=0$ și $x_1=x_2=x_3=x_4=0$, adică $a=b=c=d=0$; 2) Dacă $\alpha\neq 0, \alpha\in G$, atunci $\alpha^2, \alpha^3, ...\in G$. Cum G este finit se obține $\alpha^k=1$. Cum $k\leq 4$ rezultă pentru $k=1, G=\{1\}$ și $x_1=x_2=x_3=x_4=1$, când $a=-4, b=6$, $c=-4, d=1$. Pentru $k=2$ avem $G=\{-1,1\}$, etc. 21. 1) $A(x)A(y)=A(x+y-2xy), x+y-2xy\neq\frac{1}{2}$, $A^n(x)=A\left(\frac{1-(1-2x)^n}{2}\right)$; 2) a) $M(a)M(b)=M\left(\frac{a+b}{1+ab}\right), I_3=M(0)$; b) $a_n=\frac{(1+a)^n-(1-a)^n}{(1+a)^n+(1-a)^n}$;

22. $G=\left\{I_3, A, A^2, A^3\right\}$; 25. Elementul neutru se obține pentru $a=b=c=\hat{0}$. Numărul de elemente este 27; 26. $I_2=A(\hat{0}), A^{-1}(x)=A(-x)$; 27. $A^2=B^2=C^2=AB=BC=CA=O_2$; 28. 1) $G=\left\{I_2, A, A^2, ..., A^9\right\}$; $\det(A)=\hat{1}$ și deci A este inversabilă; 29. 1) $(\hat{1}, \hat{0}, \hat{0})$; 2) $(\hat{3}, \hat{0}, \hat{1})$; 3) $(\hat{0}, \hat{1}, \hat{3})$; 7) $(\hat{0}, \hat{0}, \hat{1}), (\hat{3}, \hat{0}, \hat{4}), (\hat{3}, \hat{2}, \hat{0})$, $(\hat{0}, \hat{2}, \hat{3}), (\hat{3}, \hat{4}, \hat{2}), (\hat{0}, \hat{4}, \hat{5})$; 10) $(\hat{1}, \hat{2}, \hat{3}), (\hat{5}, \hat{2}, \hat{3}), (\hat{3}, \hat{6}, \hat{3}), (\hat{7}, \hat{6}, \hat{3})$; 11) $(\hat{5}, \hat{0}, \hat{3}), (\hat{5}, \hat{5}, \hat{8})$; 13) $\{x,y,z\}=\{\hat{1}, \hat{2}, \hat{3}\}$; 15) $\{x,y,z\}=\{\hat{1}, \hat{2}, \hat{4}\}$; 16) $\varnothing$; 33. a) Ecuația nu are soluții deoarece luând signatura în egalitate $\Rightarrow \varepsilon(x^2)=e(\sigma)\Leftrightarrow(\varepsilon(x))^2=-1\Leftrightarrow 1=-1$, fals; b) Se caută soluții de forma $x=\begin{pmatrix}1 & 2 & 3 & 4\\ a & b & c & d\end{pmatrix}$. Se analizează cazurile $a=1, a=2, a=3, a=4$; $x_1=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 1 & 3\end{pmatrix}, x_2=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 4 & 2\end{pmatrix}$. 34. Șase soluții.

Reguli de calcul într-un grup. 1. 1) $(xy)^3=e=e\cdot e=x^3\cdot y^3\Rightarrow xyxyxy=x^3y^3\Rightarrow yxyx=x^2y^2=y^2x^2\Rightarrow$ $\Rightarrow yx=xy$; 3) $x^{n+2}y^{n+2}=(xy)^{n+1}xy=x^{n+1}y^{n+1}xy\Rightarrow xy^{n+1}=y^{n+1}x$; analog $x^{n+1}y^{n+1}=$ $=(xy)^n xy=x^n y^n xy\Rightarrow xy^n=y^n x$; $y^{n+1}x=xy^{n+1}=xy^n y=y^n xy\Rightarrow yx=xy$; 2. $G=\{x_1, x_2, ..., x_n\}$ și $x\in G$ arbitrar. Atunci $xx_1, xx_2, ..., xx_n\in G$ și $xx_i\neq xx_j, i\neq j$. Deci $G=\{xx_1, xx_2, ..., xx_n\}$. De aici $xx_1xx_2...xx_n=x_1x_2...x_n$ sau $x^n(x_1x_2...x_n)=x_1x_2...x_n$ sau $x^n=e$; 3. $x^2y=x(xy)\overset{2)}{=}xyx^3\overset{2)}{=}yx^3\cdot x^3=$ $=yx^3\overset{1)}{=}yx$; $x^2y=yx\Rightarrow y^3x^2y=y^4x=x$ (am înmulțit relația cu y^3 și apoi am utilizat 1));

$y^3x^2y=x \Rightarrow y^3x^2y=x \Rightarrow y^3x^2y^4=xy^3$ (am înmulţit relaţia cu y^3) $\overset{1)}{\Rightarrow} y^3x^2=xy^3$; 4. 1) $xy=(xy)^{-1}=$ $=y^{-1}x^{-1}=yx, (\forall)x,y\in G$; 2) $(xy)^{-1}=x^{-1}y^{-1} \Rightarrow e=x^{-1}y^{-1}xy \Rightarrow x=y^{-1}xy \Rightarrow yx=xy$; 3) $x(y^{-1})^{-1}=y^{-1}x^{-1} \Rightarrow xy=y^{-1}x^{-1} \Rightarrow xy=(xy)^{-1} \Rightarrow (xy)^2=e$. Aici facem $y=x^2$ şi obţinem $x^6=e$ şi apoi $y=x$ când găsim $x^4=e$. Deci $x^2=e, (\forall)x\in G$.

Subgrupuri. 1. $x,y\in H \Rightarrow xy\in H$, deoarece $|xy|=|x||y|=1\cdot 1=1$; $x\in H \Rightarrow x^{-1}\in H$ pentru că $\left|x^{-1}\right|=\left|\frac{1}{x}\right|=\frac{1}{|x|}=\frac{1}{1}=1$; 2. 2) $H=\left\{x\in\mathbb{Z} \mid |x|\geq 2\right\}$, când $0\notin H$; 4. b) Realizaţi tablele subgrupurilor; 6. Subgrupurile sunt: $\{e\}, \{e,\sigma_1\}, \{e,\sigma_2\}, \{e,\sigma_3\}, \{e,\sigma_1,\sigma_2,\sigma_3\}$; 8. Evident $H\subseteq S_4$. Se ştie că orice permutare este produs de transpoziţii (ij). Cum $(ij)=(1i)(1j)(1i)$ se deduce că $\sigma\in H$, adică $S_4\subseteq H$; 10. Prin dublă incluziune; 12. a) $<1>=\{1\}, <-1>=\{(-1),(-1)^2\}=\{-1,1\}, <i>=\left\{i^k \mid k\in\mathbb{Z}\right\}=\{\pm 1,\pm i\}$; b) $<\hat{6}>=\left\{k\hat{6} \mid k\in\mathbb{Z}\right\}=\left\{\hat{0},\hat{2},\hat{4},\hat{6},\hat{8},\widehat{10},\widehat{12},\widehat{14}\right\}$; c) $<\hat{2}>=\left\{\hat{2}^k \mid k\in\mathbb{Z}\right\}=\left\{\hat{1},\hat{2},\hat{3},\hat{4}\right\}$; e) $<A>=\left\{kA \mid k\in\mathbb{Z}\right\}=\left\{A,2A,3A,4A,5A\right\}$; 16. $n=2\Rightarrow A_n=\{e\}\Rightarrow Z(A_n)=\{e\}, n=3\Rightarrow |A_n|=3$, $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ şi A_n este comutativ. Deci $Z(A_n)=A_n$, $n\geq 4, Z(A_n)=\{e\}$, prin reducere la absurd; 17. Dacă $H\subset K$, atunci $H\cup K=K$, iar dacă $K\subset H$, atunci $K\cup H=H$ şi deci $K\cup H$ este subgrup. Reciproc, dacă $H\cup K$ este subgrup, atunci să presupunem prin absurd că $H\not\subset K$ şi $K\not\subset H$, ceea ce înseamnă că există $x\in H, x\notin K$ şi există $y\in K, y\notin H$. Cum $x,y\in H\cup K \Rightarrow xy\in H\cup K \Rightarrow xy\in H$ sau $xy\in K$. Dacă $xy\in H$, cum $x\in H$ $\left(\Rightarrow x^{-1}\in H\right)\Rightarrow$ $\Rightarrow x^{-1}(xy)=y\in H$, fals. Analog, din $xy\in K, y\in K \Rightarrow (xy)y^{-1}=x\in K$, fals.

Morfisme şi izomorfisme de grupuri. 1. 2) Pentru a proba că *f* este morfism se discută patru cazuri după paritatea lui $m,n\in\mathbb{Z}$; 2. 3) $f(2)=-1\Rightarrow a=-3$; 3. b) $f(1)=0\Rightarrow a=1$; 4. $f(1)=\frac{3}{2}\Rightarrow m=2$; 5. 2) $(1,2)$; 7. 2) $f:G\to\mathbb{R}^*, f(x)=\ln x$; 8. c) $\operatorname{Im} f=(1,\infty)$, $\lim\limits_{x\searrow 0} f(x)=\sqrt{b}=1\Rightarrow b=1$, iar din $f(1)=\sqrt{2}$ se deduce $a=1$; 9. b) $f:G\to\mathbb{R}, f\left(e^{\alpha x}\right)=\alpha$; c) $G_1=\left\{e^{rx} \mid r\in\mathbb{Q}\right\}, g:G_1\to\mathbb{Q}, g\left(e^{rx}\right)=r$; 10. a) 1) $a=b=1, e=-1$; 2) $f(x)=x+1$; 11. 2) $f:G_a\to G_b, f(x)=x+b-a$ (se caută un izomorfism liniar). Pentru $b=0\Rightarrow G_a\simeq G_\circ=\left(\mathbb{R}_+^*,\cdot\right)$, iar $g:\left(\mathbb{R}_+^*,\cdot\right)\to(\mathbb{R},+), g(x)=\ln x$ este izomorfism; 13. $A_\alpha\cdot A_\beta=A_{\alpha+\beta}, f:(C_1,\cdot)\to(G_1,\cdot), f(\cos\alpha+i\sin\alpha)=A_\alpha$; 14. a) 1) $A_x\cdot A_y=A_{xy}, A_1=I_2$ elementul neutru; $\left(A_x\right)^{-1}=A_{\frac{1}{x}}$; 2) $f:\mathbb{R}^*\to G, f(x)=Ax$; b) $s=\frac{1}{2}$; 16. 1)–2) Realizaţi tablele legilor; 17. 1) $G=\left\{I_3, A, A^2\right\}, f:G\to U_3, f(I_3)=1, f(A)=\varepsilon, f(A^2)=\varepsilon^2$; 2)–5) Realizaţi tablele operaţiilor pentru a evidenţia izomorfismul de grupuri; 18. b) $f:G\to\mathbb{Z}, \left((A(x)\right)=x+1, A(x)\in G$; 19. $G=\left\{I_4, A, A^2, A^3\right\}, f:G\to G_1, f(I_3)=e, f(A)=\sigma_1, f(A^2)=\sigma_2, f(A^3)=\sigma_3$. Pentru a arăta că un grup este izomorf cu un grup de permutări recomandăm lectura ultimei *Excursii matematice*; 20. $f:\mathbb{R}\to G$, $f(x)=A_x, A_x\in G$; 22. $A^2=3A, B^2=3B, AB=BA=O_3, M_tM_r=M_{-tr}$, $f:G\to\mathbb{R}^*, f(M_t)=-t$; 23. Pentru orice $y\in\mathbb{C}$ există A cu elementul $a_{11}=y$, iar celelalte nule astfel încât $f(A)=y$; 24. 1) Fie $A_{a,k}, A_{a',k'}\in M$. Atunci $A_{a,k}\cdot A_{a',k'}=A_{2aa',kk'}$; elementul neutru $e=A_{\frac{1}{2},1}$; 2) $P=\left\{A_{\frac{1}{2},k}\,\middle|\,k\in\mathbb{Q}^*\right\}\subset M; f:P\to\mathbb{Q}^*, f\left(A_{\frac{1}{2},k}\right)=k$; 25. $f:G\to\mathbb{C}^*, f(A_{a,b})=a+bi$;

$A_{1,1}^{2001}=f^{-1}\left(f\left(A_{1,1}^{2001}\right)\right)=f^{-1}\left(\left[f(A_{1,1})\right]^{2001}\right)=f^{-1}\left((1+i)^{2001}\right)=f^{-1}\left(2^{1000}+i2^{1000}\right)=A_{2^{1000},2^{1000}}$;

26. Se impune $A^4=I_4, xy=1\Rightarrow x=y=-1; f:\left\{I_4, A, A^2, A^3\right\}\to\mathbb{Z}_4, f\left(A^k\right)=\hat{k}, k=\overline{0,3}$; 27. Pentru asociativitate utilizați funcția caracteristică $f_X:M\to\{0,1\}, f_X(x)=1$ dacă $x\in X$ și $f_X(x)=0$ dacă $x\notin X$; 29. 1) $f_n\circ f_m=f_m\circ f_n=f_{n+m}, f:\mathbb{Z}\to G, f(n)=f_n$ este izomorfismul; 30*. a) Prin reducerea la absurd, presupunem că există izomorfismul $f:(\mathbb{Q},+)\to(\mathbb{Q}^*,\cdot), f(x+y)=f(x)f(y)$, $(\forall)x,y\in\mathbb{Q}$ și $f(0)=1$. Atunci $f(x)=f\left(\frac{x}{2}+\frac{x}{2}\right)=f\left(\frac{x}{2}\right)f\left(\frac{x}{2}\right)=\left(f\left(\frac{x}{2}\right)\right)^2>0, (\forall)x\in\mathbb{Q}$, adică f nu este surjectivă; b) Prin reducerea la absurd. Avem $f(1)=1$ și $1=f(1)=f\left((-1)(-1)\right)=f(-1)f(-1)$ și de aici $f(-1)=1$, ceea ce arată că f nu este injectivă; c) Prin reducere la absurd. Din $f(x)=f\left(\sqrt{x}\cdot\sqrt{x}\right)=\left(f\left(\sqrt{x}\right)\right)^2>0\Rightarrow f$ nu este surjectivă; d) $\mathbb{Q}^*$ este numărabilă, iar $\mathbb{R}^*$ este nenumărabilă; 31*. $f:\mathbb{Q}\to\mathbb{Z}$ și $a\in\mathbb{Z}$ fixat $\Rightarrow(\exists)x\in\mathbb{Q}, f(x)=a; n\in\mathbb{N}^*, (\exists)y\in\mathbb{Q}$ cu $ny=x\Rightarrow$ $\Rightarrow f(ny)=nf(y)=f(x)=a\Rightarrow n|a, (\forall)n\in\mathbb{N}^*\Rightarrow a=0$; 32*. Punem $f\left(\hat{1}\right)=a\in\mathbb{Z}$. Cum $f\left(\hat{0}\right)=0\Rightarrow$ $0=f(\hat{0})=f(\hat{n})=na\Rightarrow a=0; f(\hat{2})=2f(\hat{1})=0$; 33*. $f:\mathbb{Z}_m\to\mathbb{Z}_n$. Notăm $f(\hat{1})=\hat{a}, f(\overline{0})=\hat{0}$. Avem $\hat{0}=f(\overline{0})=f(\overline{m})=m\hat{a}=\widehat{ma}\Rightarrow ma\,\vdots\, n$, etc. 34. 1) $e=(\hat{0},\hat{0}), a=(\hat{1},\hat{0}), \quad b=(\hat{0},\hat{1}), c=(\hat{1},\hat{1})$, $a+a=b+b=c+c=e, a+b=c, b+c=a, a+c=b$, adică $\mathbb{Z}_2\times\mathbb{Z}_2$ este grup de tip Klein; 2) $f:\mathbb{Z}_{mn}\to\mathbb{Z}_n\times\mathbb{Z}_m, (m,n)=1, f(\overline{x})=(\dot{x},\hat{x})$ este bine definită, adică dacă $\overline{x}=\overline{y}$, atunci $\left(\dot{x}=\dot{y} \text{ și } \hat{x}=\hat{y}\right)\left(mn|x-y\Rightarrow m|x-y \text{ și } n|x-y\right)$. Avem: $f(\overline{0})=(\dot{0},\hat{0})$ și $f(\overline{x}+\overline{y})=f(\overline{x+y})=$ $=\left(\dot{\overline{x+y}},\widehat{x+y}\right)=(\dot{x},\hat{x})+(\dot{y},\hat{y})=f(\overline{x})+f(\overline{y})$. Funcția f este injectivă deoarece din $f(\overline{x})=f(\overline{y})\Rightarrow$ $\Rightarrow\dot{x}=\dot{y}$ și $\hat{x}=\hat{y}$. De aici $m|x-y$ și $n|x-y$, adică $mn|x-y, (m,n)=1$. Deci $\overline{x}=\overline{y}$. Cum $\mathbb{Z}_{mn}, \mathbb{Z}_n\times\mathbb{Z}_m$ au același număr de elemente, iar f este injectivă, se deduce că f este și surjectivă. 35*. 1) $A_{x,y}\cdot A_{a,b}=A_{x+a,y+b}, A_{0,0}=I_2, A_{x,y}^{-1}=A_{-x,-y}$; 2) $A(1,1)=A, G=\left\{I_2, A, ..., A^{14}\right\}\simeq\mathbb{Z}_{15}$; 36*. G_1,G_2 sunt generate de $A=\begin{pmatrix}\hat{1}&\hat{4}\\\hat{6}&\hat{1}\end{pmatrix}$ și $G_1, G_2\simeq\mathbb{Z}_6$; 37*. 2) $A_{a,\hat{0}}\cdot A_{\hat{0},b}=A_{a,b}$ și deci

$G=\{AB \mid A\in G_1, B\in G_2\}, f:G_1\times G_2\to G, f(A,B)=AB$; **38*.** 1) $\det(A)=\hat{1}\Rightarrow G=\{I_2, A, A^2, A^3, A^4, A^5\}$, $A=\begin{pmatrix}\hat{0} & \hat{1}\\ \hat{4} & \hat{1}\end{pmatrix}$.

Teste de evaluare. Testul 1. Varianta A. 1. $a>6$; **2.** $m=1$; **3.** $a=1, b=-1$; **4.** $A=\{2,4\}, S=2+4=6$, $B=\varnothing$; **5.** 1) $A(a)\cdot A(b)=A(a+b)$; 2) $f:M\to\mathbb{R}, f(A(a))=a$; 3) $A^n(a)=A(na)$; **6.** $\Delta=\hat{5}a+\hat{5}$, $A=\mathbb{Z}_7, S=\hat{6}, (\tilde{x},\tilde{y},\tilde{z})=(\hat{1},\hat{0},\hat{0})\Rightarrow V=\hat{1}$; **7.** Tabla legii.

Varianta B. 1. $a\in\{-1\}\cup[0,\infty)$; **2.** $a\in\{0,1\}$; **3.** $a=b=0$ sau $a=\frac{1}{2}, b=1$; **4.** $S_1=2, S_2=4$; **5.** 1) $A(x)\cdot A(y)=A(x+y)$; 2) $f:G\to\mathbb{R}, f(A(x))=x$; 3) $A^n(2)=A(2n)$; **6.** $\Delta=\hat{4}, S=\hat{1}$; **7.** Tabla legii.

Testul 2. Varianta A. 1. 1) Da; 2) $e=\frac{1+i}{2}$; 3) $z=1$; **3.** $a=7, b=42$; **4.** $\lambda\ge 4$; **5.** $x=3, y=-1$; **6.** 1) $f_a\circ f_b=f_{ab}, f_1=1_{\mathbb{R}}, f_a^{-1}=f_{\frac{1}{a}}$; 2) $f:\mathbb{R}_+^*\to M, f(a)=f_a$; **7.** $\mathrm{ord}(A)=7$.

Varianta B. 1. 3) $z=\frac{3}{2}$; **2.** $m\in\varnothing$; **3.** $a\in\{0,1\}$; **4.** $\alpha\ge 20$; **5.** $e=3, a*a=3\Rightarrow a_1=1, a_2=3\Rightarrow$ $\Rightarrow S=4; A=\{-1\}$; **6.** 2) Tablele legilor la fel structurate $f(f_1)=1, f(f_2)=\varepsilon, f(f_3)=\varepsilon^2$; **7.** $\mathrm{ord}(B)=6$.

Testul 3 (grilă). Varianta A. 1. b); **2.** c); **3.** a); **4.** b); **5.** a); **6.** a); **7.** a).
Varianta B. 1. a); **2.** b): **3.** c); **4.** b); **5.** a); **6.** b); **7.** b).

Capitolul 2. Inele şi corpuri

Distributivitatea unei legi în raport cu altă lege. 1. a) „$*$“ este lege comutativă şi se verifică prin calcul egalitatea $x*(y\circ z)=(x*y)\circ(x*z), (\forall)x,y,z$; **2.** În $x*(y\circ z)=(x*y)\circ(x*z), (\forall)x,y,z$ se face $x=0, y=1, z=0\Rightarrow a=b$ şi apoi $x=y=1, z=0\Rightarrow a=b=2$; **3.** $a=b=i, c=-1-i$; **4.** $a=c=\alpha, b=\alpha^2-\alpha, \alpha\in\mathbb{R}$; **Inele. 1.** Inele: 1), 3) (dacă $m=1$), 4), 5), 7), 8), 10)–13); elemente inversabile: 1), 5), 8) 11) 1, –1; 4) 7) 10), 13) orice număr nenul; 12) $\pm 1, \frac{1\pm i\sqrt{3}}{2}$; [inel, subinel]: $[1), 2)], [1), 3)], [5), 6)], [7), 6)], [10), 8)]$ etc.; **2.** Inele comutative: 5) – 16); elemente inversabile: 1) matricele care au determinantul egal cu – 1 sau 1; 2) –4) orice matrice cu determinantul nenul; 5) $I_2, -I_2$; 7) orice matrice cu determinantul nenul; 8) $I_2, -I_2$; divizori ai lui zero: 1) – 4) generați de matrice nenule; 14) $\begin{pmatrix}a & a\\ a & a\end{pmatrix}, \begin{pmatrix}a & -a\\ -a & a\end{pmatrix}, a\ne 0$; 15) $\begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & b\end{pmatrix}, a,b\ne 0$; etc.; [inel, subinel]: $[5), 6)], [7), 5)], [7), 6)]$ etc.; **3.** Elemente inversabile se află în fiecare inel; divizori ai lui zero se află în inelele: 1), 2), 4), 5), $f(x)=x^2+x|x|, g(x)=x^2-x|x|\Rightarrow f\cdot g=0$; **4.** Elemente inversabile: 1) $(1,1), (1,-1), (-1,1), (-1,-1)$; 2) –4) $(1,0), (-1,0)$; divizori ai lui zero: 1) $(a,0), (0,b), a,b\ne 0$; 2) $(a,a), (a,-a), a\ne 0$; **5.** $e=$ element neutru în raport cu prima lege şi u = element neutru în raport cu a doua lege; 1) $e=3, u=4$; elemente inversabile $x=4$ şi $x=2$ când $x'=4$ şi respectiv $x'=2$; 2) $e=-3, u=-2$; elemente inversabile $x=-2, x=-4$ când $x'=-2$ şi respectiv $x'=-4$; 3) $e=-2, u=-1$; elemente inversabile $x=-1, x=-3$ când $x'=-1$ şi respectiv $x'=-3$; 5) $e=0+0\cdot i, u=1$; elemente inversabile $U(\mathbb{Z}[i])=\{\pm 1+bi \mid b\in\mathbb{Z}\}$; 6) $e=\varnothing$, $u=M$; inelul are divizori ai lui zero, $A=\{a\}$, $B=\{b\}\Rightarrow AB=A\cap B=\varnothing$; 7) $e=O_2$, $u=I_2$, etc.; 6. Inducţie matematică; 7. $x=-1\Rightarrow 1=-1\Leftrightarrow 1+1=0\Rightarrow x(1+1)=0\Leftrightarrow x+x=0, (\forall)x\in A$;

$x,y\in A\Rightarrow (x+y)^2=x+y\Leftrightarrow x^2+xy+yx+y^2=x+y\Leftrightarrow xy+yx=0\Leftrightarrow xy+(yx+yx)=yx\Leftrightarrow xy=yx$;

8. $x,y\in A\Rightarrow 1+x\neq 1+y$; $A=\{0,1,a,b,c,d,e\}\Rightarrow A=\{1,1+1,1+a,...,1+e\}$. Suma elementelor lui A este aceeaşi $\Rightarrow 0+1+a+...+e=1+(1+1)+...+(1+e)\Rightarrow$ q.e.d.; 10. a) $-x\to x$ în relaţie $\Rightarrow x+x=0$; $x+1\to x\Rightarrow x^4+x^2=0\underset{\cdot x^2}{\Rightarrow} x^6+x^4=0$; $x^4+x=0$ şi $x^4+x^2=0\Rightarrow x^2=x$;

11. $(x+x)^2=x+x\Rightarrow x^2+x^2+x^2+x^2=x+x+x+x$; 12. a) $x\in M\Rightarrow 1-x\in M$ şi $x\neq 1-x$ $\left(x=1-x\Rightarrow x^2=x-x^2\Rightarrow x=x-x\Rightarrow x=0\Rightarrow 0=1\right)$ $(x=1-x)$ fals $\Rightarrow$ elementele lui M se pot grupa în perechi; b) dacă 1 este singurul indempotent, atunci produsul este 1, iar dacă $x, 1-x\in M$, $x\Rightarrow x(1-x)=x-x^2=x-x=0$ şi deci produsul lor este 0; 14*. a) $a=xb, c=yb\Rightarrow a^{-1}+b^{-1}+c^{-1}=$ $=b^{-1}\left(x^{-1}+1+y^{-1}\right)=b^{-1}(y+1+x)=b^{-1}b=1$; 15. a) $(x_2x_3x_1)^2=x_2x_3x_1x_2x_3x_1=$ $=(x_2x_3)(x_1x_2x_3)x_1=x_2x_3\cdot 0\cdot x_1=0\Rightarrow x_2x_3x_1=0$; b) analog cu a); c) $y_1=x_1ax_2$, $y_2=b$, $y_3=x_3$ şi se arată că $y_2y_3y_1=0$; 16*. Relaţia dată devine $x^2y+xy=yx^2+yx$. Aici se pune $(-x)$ în locul lui x şi rezultă $x^2y-xy=yx^2-yx$, care se scade din precedenta; 17*. În $x^3=x^2$ se face $-x\to x, x+1\to x, x-1\to x$; 18*. $(1-x)^2=(1-x)+1\Rightarrow x=1-x\Rightarrow x+x=1\Rightarrow (x+x)^2=1\Rightarrow$ $\Rightarrow x^2+x^2+x^2+x^2=1\Rightarrow (1+x)+(1+x)=1\Rightarrow 1+1+1+(x+x)+(x+x)=1$.

Corpuri. Notăm prin e şi u elementele neutre în raport cu prima şi respectiv a doua lege de compoziţie. 1. 2) $e=0=0+0\sqrt{3}, u=1=1+0\sqrt{3}, x^{-1}=\dfrac{a}{(a^2-3b^2)}-\dfrac{b\sqrt{3}}{(a^2-3b^2)}$; 5) $e=0, u=1$, $x=a+b\varepsilon\Rightarrow x^{-1}=\dfrac{(a-b)}{(a^2-ab+b^2)}-\dfrac{b\varepsilon}{(a^2-ab+b^2)}$; 2. 1) $e=O_2, u=I_2, A^{-1}=\begin{pmatrix} a & -3b\\ -b & a\end{pmatrix}/(a^2-3b^2)$;

4) $e=O_2, u=I_2=A_{1,0}, A_{a,b}^{-1}=A_{a/(a^2+3b^2),-b/(a^2+3b^2)}$; 5) $e=O_2, u=A_{1/2}, A_a^{-1}=A_{1/4a}$; 9) Fie O_2, I_2, A, B matricele care apar în descriere. Din tabla legii pentru „$\cdot$" $\Rightarrow A^{-1}=B, B^{-1}=A$; 3. e şi u sunt elemente neutre în raport cu prima şi respectiv a doua lege; 1) $e=4, u=5$; 2) $e=1, u=e$; 3) $e=2, u=\dfrac{5}{2}$; 4) $e=f_0, u=1_{\mathbb{R}}$; 5) $e=f_0, u=f_1$; 6) $e=i, u=(m-1)i/m$; 7) $e=0, u=1$; 4. 1)–2) $e=(0,0), u=(1,0)$; 5. $a=b=1, e=2, u=3$; 6. $e=O_2, u=I_2$; 7. $e=O_3, u=U_{-\frac{1}{3},-\frac{1}{3}}$;

Morfisme şi izomorfisme de inele şi corpuri: 1. a) $f(\hat{x}+\hat{y})=4(\hat{x}+\hat{y})=\widehat{4x}+\widehat{4y}=f(\hat{x})+f(\hat{y})$, $f(\hat{x}\hat{y})=f(\widehat{xy})=\widehat{4xy}$ şi $f(\hat{x})f(\hat{y})=4\hat{x}4\hat{y}=16\hat{x}\hat{y}=16\widehat{xy}=\widehat{4xy}$; $\mathrm{Ker}(f)=\{\hat{x}\in\mathbb{Z}_6 \mid f(\hat{x})=0\}=$ $=\{\hat{x}\in\mathbb{Z}_6 \mid \widehat{4x}=0\}=\{\hat{0},\hat{3}\}$, $\mathrm{Im}f=\{f(\hat{x}) \mid \hat{x}\in\mathbb{Z}_6\}=\{f(\hat{0}),f(\hat{1}),...,f(\hat{5})\}=\{\hat{0},\hat{2},\hat{4}\}$; 2) $\begin{pmatrix} a & a \\ a & a \end{pmatrix}$, $a\in\mathbb{Z}$; 2. $\mathrm{Ker}(F)=\left\{f\in\mathcal{C}([-1,1]) \,\middle|\, f\left(\frac{1}{2}\right)=0\right\}$; 3. f nu este injectiv, $(\exists)(a,0)\neq(a,1)$ cu $f(a,0)=f(a,1)=a$; 5. $f(2)=0,\ f(3)=1\Rightarrow\alpha=1,\beta=-2\Rightarrow f(x)=x-2$; 6. 1) $f(-1)=1,\ f(0)=2\Rightarrow\alpha=1,\beta=2\Rightarrow$ $\Rightarrow f(x)=x+2$; 2) $f(X)=u,\ f(Y)=v\Rightarrow f(X+Y)=f(X)+f(Y)=u+v$, $f(X+Y)=$ $=f\left(\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}\right)=1+2i$. Deci $u+v=1+2i$. Din a doua ecuaţie $\Rightarrow u^3+v^3=-2+i\Rightarrow$ $(u,v)\in\{(1+i,i),(i,1+i)\}$. Sistemul dat are soluţiile $X_1=f^{-1}(1+i)=\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, Y_1=f^{-1}(i)=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ şi $X_2=f^{-1}(i), Y_2=f^{-1}(1+i)$; pentru ecuaţia $f(X)=u\Rightarrow u^3-(4-2i)u^2+(7-10i)u-6+12i=0\Rightarrow$ $u_1=2, u_2=2+i, u_3=-3i\Rightarrow X_1=f^{-1}(2), X_2=f^{-1}(2+i), X_3=f^{-1}(-3i)$; 7. $f:\mathcal{A}\to\mathcal{A}'$ 1) $f(x+y\sqrt{7})=\begin{pmatrix} x & y \\ 7y & x \end{pmatrix}$; 11) $\mathcal{A}=\{aI_3 \mid a\in\mathbb{C}\}, f:\mathbb{C}\to\mathcal{A}, f(a)=AI_3$; 8. a) $f((a,b))=\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$; 9. a) $f:H\to\mathcal{H}, f(a+bi+cj+dk)=\begin{pmatrix} a+bi & c+di \\ -(c-di) & a-bi \end{pmatrix}$; 10*. Matricea se scrie sub forma $aU+bI+cJ+dK$, unde $U=I_4, I=\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, J=\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, K=\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$, care verifică egalităţile: $I^2=J^2=K^2=I_4, IJ=-JI=K, JK=-KJ=I, KI=-IK=J; f:\mathcal{M}\to H$, $f(aU+bI+cJ+dK)=a+bi+cj+dk$ dă izomorfismul de corpuri; 12*. f este morfism de grupuri, $f:(\mathbb{Z},+)\to(\mathbb{Z}_n,+)$; $f(1)=\hat{a}\Rightarrow f(x)=\widehat{xa}, \hat{a}=f(1\cdot1)=f(1)f(1)=\hat{a}^2$, $f:\mathbb{Z}\to\mathbb{Z}_n, f(x)=\widehat{xa},\ \hat{a}^2=\hat{a}$ sunt morfismele căutate; $n=6$, $\hat{a}\in\{\hat{0},\hat{1},\hat{3},\hat{4}\}\Rightarrow$ patru morfisme; 13*. $f(\hat{1})=a\in\mathbb{Z}, 0=f(\hat{0})=f(\hat{n})=na\Rightarrow$ $\Rightarrow a=0\Rightarrow f\equiv0$; 14*. $f(\hat{1})=\hat{a}, \hat{a}=f(\hat{1}\cdot\hat{1})=f(\hat{1})f(\hat{1})=\hat{a}^2$; $f(\hat{k})=\widehat{ka},\ \hat{a}^2=\hat{a},\ f(\hat{1})=\hat{a}; n=6\Rightarrow$ $\Rightarrow\hat{a}\in\{\hat{0},\hat{1},\hat{3},\hat{4}\}$; 15*. $f(\hat{1})=\bar{a},\ f(\hat{x})=\overline{ax}, \bar{a}^2=\bar{a}$ şi $\overline{na}=\bar{0}$, $f_{\bar{0}}$ şi $f_{\bar{3}}$ pentru $n=4,\ m=6$; 16. $e=1, u=e, f(0)=1, f(1)=e\Rightarrow\alpha=\beta=1$; 17. $e=0, u=1; f(0)=0, f(1)=1\Rightarrow\alpha=1,\beta=0$; 19. $f:(\mathbb{Q},+,\cdot)\to(\mathbb{Q},\oplus,\odot), f(x)=\alpha x+\beta$; 20. $e=1, u=e^3\ f(0)=1, f(1)=e^3\Rightarrow n=0, m=3$; 22. 1) $f(a+b\sqrt{3})=\begin{pmatrix} a & b \\ 3b & a \end{pmatrix}$; 4) $g:\mathcal{K}'\to\mathbb{Q}, g(f_a)=a$; 6) $f:\mathcal{K}'\to\mathbb{R}, f(A_x)=2x$; 24. $f:\mathbb{C}\to M$, $f(z)=-\frac{1}{n}zA$; 25. $\varphi:A\to\mathbb{R}, \varphi(x)=f(x)$.

Inele de polinoame cu coeficienți într-un corp comutativ. **1.** 1) $a=10, b=7, c=5, d=2$; 2) $a=9, b=4$, $c=-3$; 3) $a=-2, b=3, c=0$; **3.** 1) $m=1 \Rightarrow f=6 \Rightarrow \text{grad}(f)=0$; $m=2 \Rightarrow \text{grad}(f)=2$; $m \in \mathbb{R}-\{1,2\} \Rightarrow \text{grad}(f)=3$; 2) $m=\pm i \Rightarrow f=iX \Rightarrow \text{grad}(f)=1$; $m \neq \pm i \Rightarrow \text{grad}(f)=4$; **4.** $m \in \mathbb{Q} \Rightarrow m^3 \neq 2 \Rightarrow \text{grad}(f)=3$; $\text{grad}(g)=3 \Rightarrow m=-1$; **5.** 0; **6.** a) $X^{2^{n+1}}-1$; b) $X^{2^{n+2}}+X^{2^{n+1}}+1$; **9.** $a=3, b=2$; **10.** $f=3X+5, g=-3X+4$; **11.** 1) $f=2X^2-3X-4$; **12.** $p=-12, q=9$; **13.** $(X+1)^3, (-2X+1)^3, (X-2)^3$; **14.** $f=3X^3-\frac{3}{2}X^2-\frac{1}{2}X+d, d \in \mathbb{R}$; **15.** 1) a) $f=\pm X^2$; b) $f_1=X^2, f_2=X^2-X, f_3=X^2+X+1, f_4=X^2-X+1$; **17.** $f=4X^3-6X^2+4X-1$; **19.** $f=\hat{2}X^2+\hat{2}X+\hat{3}$; **21.** Patru polinoame; **22.** $f=\hat{3}X^3+X^2+\hat{4}X+\hat{2}$; **24.** 1) $q=3X^2+X+6, r=1$; 2) $q=2X^4-3X^3+9X^2-4X+4, r=-7$; 4) $q=iX, r=(3-3i)X-i$; 5) $q=\hat{3}X^4+X^3+X^2, r=\hat{1}$; **25.** 1) $f(1)=0 \Rightarrow m=-\frac{1}{2}$; 5) $m=-40i$; 6) $m=\hat{3}$; **26.** 1) $f(2)=3 \Rightarrow m=3$; **27.** $f(1)=4$, $f(-2)=5 \Rightarrow m=-6, n=11$; **28.** $f(1)=1, f(-1)=-1, f(2)=41 \Rightarrow m=3, n=0, p=-3$; **31.** Se pune $x=0, x=-2$ în relație; **33.** 1) $m=0, n=-5$; 2) $n=0, m=0$ sau $n=0, m=-1$; 3) $m=-16, n=0$; **34.** 1) $f(-2)=0, f(i)=0 \Rightarrow m=n=3, p=2$; 2) $m=-3, n=1, p=2$; **37.** $f \in \mathbb{C}[X], \text{grad}(f)=n \Rightarrow$ $\Rightarrow (\exists) a_i \in \mathbb{C}, i=\overline{0,n}$ unici a.î. $f=a_0+a_1\frac{X}{1!}+a_2\frac{X(X-1)}{2!}+\ldots+a_n\frac{X(X-1)\ldots(X-n+1)}{n!}$; **39.** Prin reducere la absurd; **41.** 1) r^2; 2) 2; 3) $-6X+1$; **42.** Prin reducere la absurd; **43.** 1) $f=(X-2)(X^2+2X+4)$ (în $\mathbb{R}[X]$) $=(X-2)(X+1+i\sqrt{3})(X+1-i\sqrt{3})$ (în $\mathbb{C}[X]$); **44.** $f(\hat{0})=\hat{1} \neq \hat{0}, f(\hat{1})=\hat{3}, f(\hat{2})=\hat{1}, f(\hat{3})=\hat{1}, f(\hat{4})=\hat{4}$; $f=(X^2+\hat{4}X+\hat{1})(X^2+X+\hat{1})$; **45.** 1) $(X+\hat{1})(X+\hat{2})(X+\hat{3})$; 2) $\hat{3}(X+\hat{2})^2(X+\hat{3})(X+\hat{4})$; 3) ireductibil; **46.** Prin reducere la absurd; **47.** $m=\hat{1}, n=\hat{2}$ sau $m=\hat{2}, n=\hat{1}$; **48.** $X+\hat{1}, X^3+\hat{1}, 2X^3+\hat{2}X+\hat{1}$; **50.** $X^2+\hat{1}, X^2+X+\hat{1}, X^2+\hat{3}X+\hat{1}, X^2+\hat{2}, X^2+\hat{2}X+\hat{2}, X^2+X+\hat{3}, X^2+\hat{2}X+\hat{3}, X^2+\hat{3}X+\hat{3}$; **51.** 1) X^2+X-2; 2) X^2+X+1; 3) X^2-1; 4) X^2+X-1; **53.** $\alpha=2, \beta=-1$; $(f,g)=X^2-4X+3$; **54.** 1) $d=X^3+X-2=-\frac{1}{3}f+\frac{1}{3}(X+1)g$; **55.** 1) $x^2+1=0 \Rightarrow x=\pm i$; $f(i)=0 \Rightarrow f(-i)=\overline{f(i)}=0$; **56.** Fie α rădăcină a lui $g \Rightarrow \alpha^2+\alpha+1=0$ și $\alpha^3=1$; 1) $f(\alpha)=\alpha(\alpha^2+1)^{6n+1}+$ $+\alpha^{3n+2}=\alpha(-\alpha)^{6n+1}+\alpha^{3n}\cdot\alpha^2=\alpha(-\alpha)\left[(-\alpha)^2\right]^{3n}+\alpha^2=-\alpha^2(\alpha^3)^{2n}+\alpha^2=-\alpha^2+\alpha=0$; **57.** Fie α rădăcină a lui $g \Rightarrow \alpha^2-\alpha+1=0$ și $\alpha^3=-1$; 1) $f(\alpha)=(\alpha-1)^{n+3}+\alpha^{2n+3}=$ $(\alpha^2)^{n+3}+\alpha^{2n}\cdot\alpha^3=\alpha^{2n}\cdot\alpha^6+\alpha^{2n}(-1)=\alpha^{2n}-\alpha^{2n}=0$; **58.** α rădăcină a lui $g \Rightarrow \alpha^2+\alpha+1=0$, $\alpha^3=1$ și se discută cazurile $n \in \{6k, 6k \pm 1, 6k \pm 2, 6k+3\}$; 1) $n \in \{6k \pm 2\}, k \in \mathbb{N}$; **59.** Fie α rădăcină a lui $g \Rightarrow \alpha^2-\alpha+1=0, \alpha^3=-1$ și se ia $n \in \{6k, 6k \pm 1, 6k \pm 2, 6k+3\}, k \in \mathbb{N}$;

1) $n\in\{6k\pm 2; k\in\mathbb{N}\}$; 60. α rădăcină a lui $g\Rightarrow \alpha^3+\alpha^2+\alpha+1=0$ şi $\alpha^4=1\Rightarrow f(\alpha)=0$; 61. a) $p(\omega)=0\Leftrightarrow f(\omega^3)+\left(\frac{-1+i\sqrt{3}}{2}\right)^2 g(\omega^3)=0\Leftrightarrow f(1)+\omega^2 g(1)=0\Leftrightarrow 2f(1)-g(1)-i\sqrt{3}g(1)=0\Leftrightarrow$ $\Leftrightarrow\left(2f(1)-g(1)=0, \sqrt{3}g(1)=0\right)\Rightarrow f(1)=g(1)=0$; 62*. $x^3=y\Rightarrow y^2-6y+8=0\Rightarrow y_1=2, y_2=4\Rightarrow$ $\Rightarrow x_1=\sqrt[3]{2}, x_2=\sqrt[3]{4}$; $g(x_1)=0\Rightarrow f(2)+\sqrt[3]{2}g(2)+\sqrt[3]{4}h(2)=0\Rightarrow f(2)=h(2)=g(2)=0$ (deoarece $f(2), h(2), g(2)\in\mathbb{Q}$); 65. Inducţie matematică; 66. 1) α rădăcină pentru X^2+X+1; $f\,\vdots\left(X^2+X+1\right)^2\Leftrightarrow$ $\Leftrightarrow f(\alpha)=f'(\alpha)=0, f''(\alpha)\neq 0$; 2) Se ia $x\in\{0, 1, ..., 25\}, f=kX(X-1)...(X-25)$; 69. „$\Leftarrow$“ z_0 soluţie a ecuaţie $z^d=1; n=n_1d, m=m_1, d\Rightarrow z_0^n=\left(z_0^d\right)^{n_1}=1$, $z_0^m=\left(z_0^d\right)^{m_1}=1\Rightarrow z_0$ soluţie a ecuaţiei $z^d=1, n=n_1d, m=m_1d\Rightarrow z_0^n=\left(z_0^d\right)^{n_1}=1, z_0^m=\left(z_0^d\right)^{m_1}=1\Rightarrow z_0$ soluţie a ecuaţiilor $z^n=1, z^m=1$. „$\Rightarrow$“ Se ia $z_k=z_l$ rădăcină comună a ecuaţiilor $z^n=1, z^m=1$, etc.; 72. 1) $x–5=y$; 2) $x+4=y$; 3) $2x-4=y$; 4) $x=t+\frac{1}{t}$; 74. $t=x+\frac{1}{x}\Rightarrow f(t)=0$ ecuaţia rezolventă să aibă rădăcini reale $\Rightarrow \Delta_t\geq 0$ şi ecuaţiile $x+\frac{1}{x}=t_k, k=1,2$ să aibă rădăcinile reale $\Rightarrow \Delta_x\geq 0\Leftrightarrow t_k^2-4\geq 0\Rightarrow$ $\Rightarrow t_k\in(-\infty,-2]\cup[2,\infty)$; 1) $(-\infty,-8]$; 2) $[4,\infty)$; 3) $(-\infty,-16]$; 75. 1) $x+\frac{5}{x}=y$; 2) $x+\frac{2}{x}=y$; 3) $x+\frac{4}{x}=y$; 4) $x-\frac{2}{x}=y$; 5) $\frac{x}{3}-\frac{4}{x}=y$; 6) $2x-\frac{3}{x}=y$; 77. a) 1) $z^3+2z^2-15z+\left(-z^2-2z+15\right)i=0\overset{z\in\mathbb{R}}{\Rightarrow}$ $\Rightarrow\left(z^3+2z^2-15z=0 \text{ şi } -z^2-2z+15=0\right)\Rightarrow z_1=-5$ rădăcina comună; $\Rightarrow z^2-(3+i)z+3i=0\Rightarrow$ $\Rightarrow z_2=3, z_3=-i$; 2) $-3, -1, 1+i$; 2) $-2, 3, i-1$; b) $x^3-8x^2-6x+108+\left(x^2+x-48\right)\sqrt{3}=0,$ $x\in\mathbb{Q}\Rightarrow\left(x^3-8x^2-6x+108=0 \text{ şi } x^2+2x-48=0\right)\Rightarrow x_1=6$; $x_2=5-\sqrt{3}, x_3=-3-\sqrt{3}$; c) 1) $x^3+2x^2-5x-6+\left(x^2+x-6\right)m=0, (\forall)m\Rightarrow\left(x^3+2x^2-5x-6=0, x^2+x-6=0\right)\Rightarrow$ $\Rightarrow x_1=-3, x_2=2$ rădăcini comune; $x_3=-m+1$; 2) 3; 4; $\frac{m-1}{2}$; 3) -1; 2; $3m$; d) Verificare directă; e) 1) $x=\sqrt[3]{\sqrt{5}+2}-\sqrt[3]{\sqrt{5}-2}$ şi se ridică la cub $\Rightarrow x^3+3x-4=0$ cu unica soluţie reală $x=1$; 2) 4; 3) 3; f) 1) $x_1=a-1, x^2-x-2a=0$; 2) $x_1=a+1, x^2-x+a=0$; 79. 1) $m=-5, n=0$; 2) $m=-2, n=-3$; 3) $m=6, n=2$; 80. 1) $m=-2, n=-4$; 2) $m=1, n=3$; 81. 1) $m=\frac{1}{5}, n=\frac{26}{5}$; 2) $m=-1, n=1$; 3) $m=9, n=-1$; 82. 1) $m=27, n=40, p=-8$; 2) $m=-3, n=-1, p=1$; 83. 1) a)–b) – 2; c) 18; d) – 22; e) $-\frac{3}{4}$; f) $-\frac{7}{16}$; g) -1; h) -10; 2) a) 5; b) 27; c) 89; d) $\frac{1}{3}$; e) $-\frac{8}{9}$;

f) $\frac{8}{5}$; g) -360; 84. 1) 12; 2) $\frac{51}{4}$; 85. 1) $m=39; 1; 4; 7$; 2) $m=3, -2; 1; 4$; 86. 1) $m=-\frac{246}{5}$, $n=-\frac{362}{5}$; $2-3\sqrt{5}$; $2\pm\sqrt{5}$; 88. 1) $m=-6; -1; 3; 9$; 2) $m=-1; 1; -2; 4$; 89. I. 1) $m=-5, \frac{-3\pm\sqrt{5}}{2}$; $\frac{5}{2}$; $m=6, -3; 2; \frac{1}{2}$; 2) $m=\frac{1}{2}; 2; -2; \frac{1}{2}$; II. 1) $m=2; 1; 1; -2; -2$; $m=-2; -1; -1; 2; 2$; 2) $m=-7$; $x_{1,2}=\pm 2; -1; 3$; 90. I. 1) 1°) $\left(-1-\sqrt{2}, -1+\sqrt{2}\right)$; 2°) $\left[\frac{16}{11}, 2\right)$; II. 1) 1°) $\left[\frac{4-\sqrt{2}}{7}, \frac{4+\sqrt{2}}{7}\right]$; 2°) $\varnothing$;

91. 1) $x^3-3x^2-x+3=0$; 2) $x^3+x^2-2x=0$; 92. 1) $x^4-2x^3-x^2-2x=0$; 93. 1) $\{x,z,y\}=$ $=\{-1, 1, 2\}$; 2) $x=y=z=3$; 3) $\{x, y, z\}=\{-2, 1, 2\}$; 94. 1°) $x=-2-y$; $y^3+4y^2+7y+8=0$; 2°) $x=\frac{-2x}{1+y}, 4y^3+5y^2+6y+1=0$; 3°) $x=\frac{1}{y}, 2y^3-3y^2-2y-1=0$; 95. 1) $a^3=a+1 \Rightarrow y^2=5a^2-4$,

$y^3=2a^2+9a-5$; $y=2a^2-4$, $y^2=5a^2-4 \Rightarrow a^2=\frac{y^2+4}{5}, a=\frac{2y^2-5y+8}{5} \Rightarrow a^2=(a)^2 \Rightarrow$ $\Rightarrow y^3-4y^2+9y-11=0$; 2) $y^3-2y^2+y-1=0$; 96. 1) $a=-1, x=-1$; 2) $a=0, x=1$; 97. 1) $a_1=0, x_1=0$; $a_2=-6, x_2=1$; 98. $\alpha\in\mathbb{Z}$ rădăcina comună; 1) $\alpha=0 \Rightarrow a=b=0$; 2) $\alpha=2 \Rightarrow (\nexists)a,b\in\mathbb{Z}$; 3) $\alpha=-2 \Rightarrow a=-4, b=-8$; 4) $\alpha=4$, imposibil; 99. 1) $a=3, x_1=-1$, $x_2=2$; 2) $a=-3, x_1=1, x_2=-2$; 100. 1) $a=1, b=2, x^2-2x+6=0$; 101. α rădăcina dublă comună $\Rightarrow \left(\alpha^5+a\alpha^2+b\alpha+1\right)-\left(\alpha^5+m\alpha^2+n\alpha+1\right)=0 \Rightarrow \alpha^2(a-m)+\alpha(b-n)=0 \Rightarrow a=m, b=n$;

102. 1) $a=3, b=2, c=1$; 2) $a=1, b=0, c=-1$; 103. $x=1, a=4$; 105. $\sum x_1^2=-\left(a^2-a+1\right)<0$, $(\forall)a\in\mathbb{R}$; 106. $x_0=u+iv, |x_0|=1 \Rightarrow \overline{x_0}=u-iv$ este soluție $\Rightarrow f \vdots (x-x_0)(x-\bar{x}_0) \Rightarrow a=2, b=\frac{3}{2}$; 107. Se face $n=1, n=2$; 108. $\sum x_1x_2=0 \Rightarrow x_1+x_2, x_2+x_3, x_1+x_3>0 \Rightarrow a-x_1=x_2+x_3>0$, etc.; 109*. Se împarte prin a $\Rightarrow \frac{b}{a}=\frac{3x-x^3}{1-3x^2}$ şi se ia $x=\operatorname{tg} y$, $y\in\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$; 110. 1) $\sum(x_1-2)^2=1$; 2) din 1) $\Rightarrow (x_i-2)^2\le 1 \Rightarrow -1\le x_i-2\le 1$, etc.; 111. $|a|\le\sum|x_1|\le 3, |b|\le 3, |c|\le 1 \Rightarrow \sum|a|\le 7$;

Teste de evaluare. Testul 1. Varianta A. 1. $e_\perp=3, e_\top=4, x\top x'=4 \Rightarrow x'=3+\frac{1}{x-3}\in\mathbb{Z} \Rightarrow x\in\{2, 4\}$; 2. 1) $\perp$ comutativă $\Rightarrow a=b$; $\perp$ asociativă $\Rightarrow a=1$; $\top$ asociativă $\Rightarrow c=5$; $e_\perp=2, e_\top=3$; 2) $f(0)=2 \Rightarrow \beta=2$, $f(1)=3 \Rightarrow \alpha=1$; 3. a) $a=\hat{2}$; b) $(\hat{0}, \hat{4}), (\hat{1}, \hat{0}), (\hat{2}, \hat{1}), (\hat{3}, \hat{2}), (\hat{4}, \hat{3})$; 4. f cu grad$(f)\in\{1, 2\}$ nu există; $f=aX^3+bX^2+cX+d\in\mathbb{Z}_5[X] \Rightarrow f=\hat{3}X^3+X^2+\hat{4}X+\hat{2}$; 5. $a\le -6$; 6. a) $x=10, h=5$; b) $x\in(\infty, -4)\cup(2, 3)$; Varianta B. 1. $f(x)=1$ dacă $x<0$, $f(x)=0$ dacă $x\ge 0$, $g(x)=0$ dacă $x<0$, $g(x)=-1$, dacă $x\ge 0$, $f, g\ne 0 \Rightarrow fg=0$; 2. Prin reducere la absurd; $f: A\to B$, $f(x+y\sqrt{2})=x+y\sqrt{3}$, f bijectivă şi $f(u+v)=f(u)+f(v), (\forall)u,v\in A$, dar $f(uv)\ne f(u)f(v)$,

$(\forall)u,v\in A$; **3.** a) $\sum x_1^2=-3m^2-2<0$; b) $n=2k+1, k\in\mathbb{N}$; **4.** $y=\dfrac{x+i}{x-i}\Rightarrow y^n=-1$ etc.; b) $f(x_1)=16x_1^3-13x_1^2+7x_1+12\Rightarrow\sum f(x_1)=68$; **5.** a) Ecuația de gradul trei în t de soluții x, y, z este: $t^3+t^2-4t-4=0; (-2, 2, -1)$ și permutările; b) $(\hat{6}, \hat{3}, \hat{6})$; **6.** a) $n=30$ zile; b) $\sqrt[3]{x+1}=u$, $\sqrt{x-3}=v$, $x=7$;

Testul 2. Varianta A. **1.** Se construiesc tablele legilor; **2.** a) $f=X-1, g=X+1, f,g\neq 0$ și $f*g=0$; b) φ este bijectivă; $\varphi(f+g)=\varphi(f)+\varphi(g)$ dar $\varphi(f*g)\neq\varphi(f)\varphi(g)$; **3.** a) $f=(X+\hat{1})(X+\hat{2})(X+\hat{4})$; b) ireductibil; **4.** a) $\det(A)=\hat{3}$ inversabil în $\mathbb{Z}_8$, iar A^{-1} are liniile $(\hat{2}\ \hat{1}\ \hat{3}), (\hat{5}\ \hat{6}\ \hat{0}), (\hat{0}\ \hat{2}\ \hat{3})$; b) $AX=B$, $(\hat{3}\ \ \hat{0}\ \hat{3})$; **5.** $a\in\{1, 9\}$; **6.** a) $3^x+3^{-x}=y\geq 2$; b) $\left(-\dfrac{1}{3},0\right), \left(\dfrac{1}{2}, 0\right), (1,0)$; **Varianta B.** **1.** a) $a=b=1$; $e_0\Rightarrow n=m^2-m$; „$\circ$“ este distributivă față de „$*$“$\Rightarrow m=c$; c) $f(0)=-c, f(1)=1\Rightarrow$ $\alpha=1, \beta=-c$; **2.** $\alpha=-\dfrac{1}{2}, x_1=x_2=x_3=-\dfrac{1}{2}, x_4=\dfrac{1}{2}, a=-\dfrac{1}{4}, b=-\dfrac{1}{16}$; **3.** $a\in(-\infty,-1]\cup\left[-\dfrac{2}{3},\infty\right)$; **4.** a) $m=-2, n=p=-8$; **5.** $a=b=1, e=1, x'=2-x, c=3; f(x*y)=f(x)+f(y), f(x\circ y)=$ $=f(x)f(y)\Rightarrow p=q=2$; **6.** a) $x\in\{5, 6, 7\}$; b) $x\in\{1, 2, 3\}$.

Testul 3 (grilă). Varianta A. **1.** $a=b=1$; b) ; **2.** a); **3.** a); **4.** c); **5.** c); **6.** b); **7.** a); **8.** a); **9.** b); **10.** c); **Varianta B.** **1.** a); **2.** c); **3.** a); **4.** b); **5.** b); **6.** c); **7.** a); **8.** b); **9.** a); **10.** b).