ART
Grup Editorial

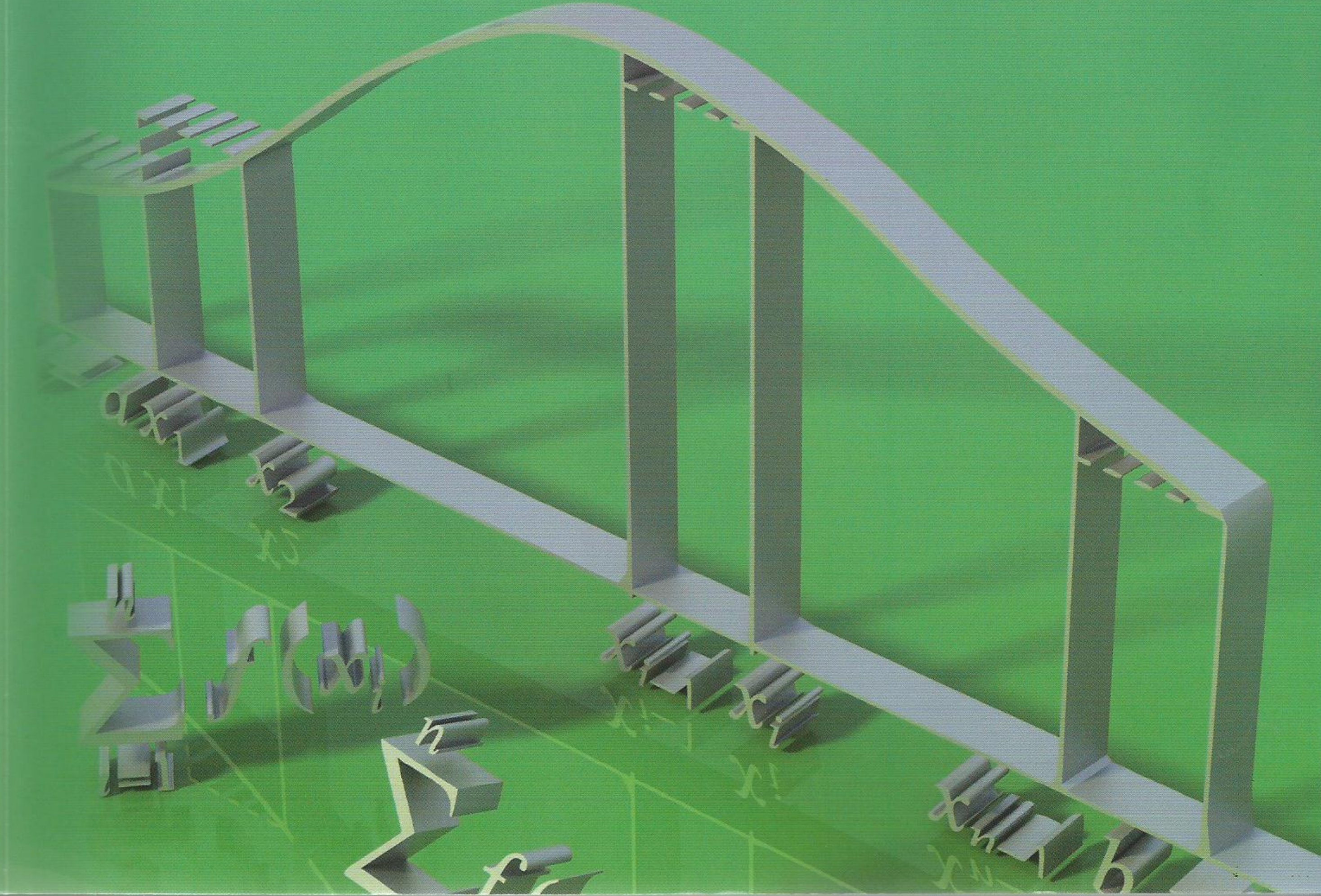
MINISTERUL EDUCAȚIEI, CERCETĂRII ŞI TINERETULUI

Matematică

Manual pentru clasa a XII-a

M1

Marcel Țena
Marian Andronache
Dinu Şerbănescu



MINISTERUL EDUCAȚIEI, CERCETĂRII ȘI TINERETULUI

Marcel ȚENA
Marian ANDRONACHE
Dinu ȘERBĂNESCU

MATEMATICĂ M1

Manual pentru clasa a XII-a

ART
Grup Editorial

Manualul a fost aprobat prin Ordinul ministrului Educației, Cercetării și Tineretului nr. 1342/29 din 19.06.2007, în urma evaluării calitative și este realizat în conformitate cu programa analitică aprobată prin Ordin al ministrului Educației și Cercetării nr. 5959 din 22.12.2006.

***Referenți*:**
Conf. univ. dr. Mircea BECHEANU
Prof. univ. dr. Radu GOLOGAN

***Tehnoredactare*:**
Ion ROȘU

Pentru **comenzi** vă puteți adresa:
Departamentului Difuzare
C.P. 78, O.P. 32, sector 1 – 012134, București
tel. 021.224.17.65
0721.213.576
0744.300.870

Descrierea CIP a Bibliotecii Naționale a României
ȚENA, MARCEL
Matematică M1: manual pentru clasa a XII-a / Marcel Țena, Marian Andronache, Dinu Șerbănescu. - București : Art, 2010
ISBN 978-973-124-549-2

I. Andronache, Marian
II. Șerbănescu, Dinu

51(075.35)

ELEMENTE DE ALGEBRĂ

GRUPURI

Lege de compoziție internă (operație algebrică), tabla operației, parte stabilă, proprietăți

În mod frecvent vorbim de *operații* pe anumite mulțimi. De exemplu, vorbim de operația de scădere a numerelor întregi, care este în definitiv un procedeu prin care cuplului de numere întregi $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ îi asociem numărul întreg $x - y \in \mathbb{Z}$. Este important să considerăm cuplul sau mulțimea ordonată (x, y) și nu mulțimea $\{x, y\}$, căci contează ordinea în care apar x și y; astfel, cuplului (y, x) îi corespunde prin această asociere numărul $y - x \in \mathbb{Z}$, care în general diferă de $x - y$.

Deoarece cuplurile de elemente ale unei mulțimi M sunt elementele produsului cartezian $M \times M$, iar procedeul prin care asociem fiecărui cuplu din $M \times M$ un element din M este o funcție de la $M \times M$ la M, suntem conduși la următoarea:

Definiție

Fie M o mulțime nevidă. Numim ***lege de compoziție internă*** (***operație algebrică***) pe mulțimea M orice funcție definită pe $M \times M$ cu valori în M:

$$* : M \times M \to M,\ (x, y) \mapsto x * y$$

care asociază fiecărui cuplu $(x, y) \in M \times M$ un unic element $x * y \in M$.

Elementul $x * y \in M$ se citește ***x compus cu y*** (sau ***x operat cu y***), în această ordine.

O operație algebrică va fi notată nu numai prin semnul $*$, ci și cu ajutorul altor simboluri cum sunt $+$, $-$, $\cdot$, $:$, $\circ$, $\oplus$, $\odot$, $\cup$, $\cap$, Δ etc.

Cel mai frecvent, în algebră se utilizează semnul $+$ (*notație aditivă*) și semnul $\cdot$ (*notație multiplicativă*). Cu toate acestea, pentru început preferăm notația din definiție, adică simbolul $*$.

Exemple de operații algebrice

1. Adunarea pe mulțimea $\mathbb{N}$, care este funcția:

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N},\ (x, y) \mapsto x + y.$$

2. Scăderea pe mulţimea $\mathbb{Z}$, care este funcţia:

$$- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \ (x, y) \mapsto x - y.$$

3. Înmulţirea pe mulţimea $\mathbb{R}$, adică funcţia:

$$\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \ (x, y) \mapsto xy.$$

4. Adunarea pe mulţimea de matrice $\mathcal{M}_n(\mathbb{C})$, care este funcţia:

$$+ : \mathcal{M}_n(\mathbb{C}) \times \mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_n(\mathbb{C}), \ (X, Y) \mapsto X + Y.$$

5. Reuniunea pe mulţimea $\mathcal{P}(M)$ a părţilor unei mulţimi M, adică:

$$\cup : \mathcal{P}(M) \times \mathcal{P}(M) \to \mathcal{P}(M), \ (X, Y) \mapsto X \cup Y.$$

În cazul unei mulţimi finite $M = \{x_1, x_2, \ldots, x_n\}$ o operaţie algebrică $*$ pe M poate fi definită prin ***tabla operaţiei***. Este vorba de un tablou de tipul:

$*$	x_1	x_2	$\ldots$	x_j	$\ldots$	x_n
x_1	$x_1 * x_1$	$x_1 * x_2$	$\ldots$	$x_1 * x_j$	$\ldots$	$x_1 * x_n$
x_2	$x_2 * x_1$	$x_2 * x_2$	$\ldots$	$x_2 * x_j$	$\ldots$	$x_2 * x_n$
$\vdots$						
x_i	$x_i * x_1$	$x_i * x_2$	$\ldots$	$x_i * x_j$	$\ldots$	$x_i * x_n$
$\vdots$						
x_n	$x_n * x_1$	$x_n * x_2$	$\ldots$	$x_n * x_j$	$\ldots$	$x_n * x_n$

în care, la intersecţia „liniei" i cu „coloana" j apare elementul $x_i * x_j$. De exemplu, înmulţirea pe mulţimea $M = \{-1, 0, 1\}$ este definită prin tabla:

$\cdot$	-1	0	1
-1	1	0	-1
0	0	0	0
1	-1	0	1

Definiţie

Fie M o mulţime nevidă şi $*$ o operaţie pe M. O submulţime nevidă $H \subseteq M$ se numeşte ***parte a lui M stabilă (închisă) faţă de operaţia*** $*$ dacă:

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

În acest caz restricţia operaţiei $*$ la submulţimea H, adică funcţia $* : H \times H \to H$, $(x, y) \mapsto x * y$ se numeşte ***operaţie pe H indusă de operaţia*** $*$ ***de pe M***.

(Pentru comoditate, am notat şi operaţia indusă tot cu $*$, deşi operaţia pe M şi operaţia pe H nu sunt egale, ca funcţii).

Exemple de părţi stabile

1. Submulţimea $\mathbb{Z}$ este o parte a lui $\mathbb{R}$ stabilă faţă de adunare, deci putem spune că adunarea pe $\mathbb{Z}$ este indusă de adunarea de pe $\mathbb{R}$.

2. Submulţimea $H = \{1, -1, i, -i\}$ este parte a lui $\mathbb{C}$ stabilă faţă de înmulţire. Într-adevăr, tabla înmulţirii pe H arată astfel:

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

şi observăm că produsele elementelor din H se menţin în H.

Observaţie

Dacă $*$ este o operaţie pe M şi $H \subseteq M$, exprimările:

1) H este o parte a lui M stabilă faţă de operaţia $*$

2) $*$ este o operaţie pe mulţimea H

sunt echivalente.

Definiţia care urmează pune în evidenţă proprietăţi importante ale unei operaţii, pe care le vom utiliza mai departe.

Definiţie

Fie M o mulţime nevidă şi $*$ o operaţie pe M. Spunem că:

1° Operaţia $*$ este ***asociativă*** dacă $(x * y) * z = x * (y * z)$, $\forall\, x, y, z \in M$.

2° Operaţia $*$ este ***comutativă*** dacă $x * y = y * x$, $\forall\, x, y \in M$.

3° Operaţia $*$ are ***elementul neutru e*** dacă $\exists\, e \in M$ astfel încât $x * e = e * x = x$, $\forall\, x \in M$.

4° Dacă operaţia $*$ are elementul neutru $e \in M$, spunem că un element $x \in M$ este ***simetrizabil*** faţă de operaţia $*$ dacă $\exists\, x' \in M$ astfel încât $x * x' = x' * x = e$ (x' se numeşte ***simetricul*** lui x).

Exemple 1) Adunarea pe mulţimea $\mathbb{Z}$ este asociativă, comutativă, are elementul neutru 0 şi orice $x \in \mathbb{Z}$ este simetrizabil faţă de adunare, având simetricul $-x$.

2) Înmulţirea pe mulţimea $\mathbb{Z}$ este asociativă, comutativă, are elementul neutru 1 şi singurele elemente simetrizabile faţă de înmulţire în $\mathbb{Z}$ sunt 1 (cu simetricul 1) şi -1 (cu simetricul -1).

Observaţie

Datorită asociativităţii unei operaţii, putem compune oricâte elemente (în număr finit) şi putem suprima parantezele; de exemplu, în loc de $(x * y) * z$ sau $x * (y * z)$ scriem $x * y * z$. Datorită comutativităţii unei operaţii putem compune elemente fără a ţine seama de ordinea în care apar.

Propoziție

Fie M o mulțime nevidă și „$*$" o operație pe M. Atunci:

1° Dacă operația $*$ are element neutru $e \in M$, acesta este unic determinat.

2° Dacă operația $*$ este asociativă și are elementul neutru e, iar $x \in M$ este un element simetrizabil, atunci simetricul $x' \in M$ al lui x este unic determinat.

Demonstrație. 1° Dacă $e' \in M$ ar fi un alt element neutru, atunci $e * e' = e$ (deoarece e' este element neutru) și $e * e' = e'$ (deoarece e este element neutru) prin urmare $e = e'$.
2° Dacă $x'' \in M$ ar fi un alt simetric al elementului $x \in M$, atunci
$x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''$, deci $x' = x''$ (am ținut seama că $x * x'' = e$ și $x' * x = e$).

Comentariu metodic

Deoarece în algebră cele mai frecvente notații sunt cea aditivă și cea multiplicativă, este bine să cunoaștem „*adaptarea*" terminologiei și scrierii la fiecare din aceste notații.

Astfel, în ***notație aditivă*** elementul neutru se notează cu 0 și se numește ***element nul***, iar simetricul unui element x se notează $-x$ și se numește ***opusul*** lui x.

În ***notație multiplicativă*** elementul neutru se notează cu 1 sau cu e și se numește ***element unitate***, iar simetricul unui element x se notează cu x^{-1} sau cu $\frac{1}{x}$ și se numește ***inversul*** lui x; elementul x care are invers se numește ***element inversabil***.

Exerciții rezolvate

1. Să se determine părțile finite ale mulțimii $\mathbb{C}$, care sunt stabile față de operația de înmulțire a numerelor complexe. Să se deducă părțile finite ale fiecăreia din mulțimile $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, stabile față de înmulțire.

Soluție. Fie $H = \{x_1, x_2, \ldots, x_n\}$ o submulțime a lui $\mathbb{C}$ cu n elemente, care este stabilă față de înmulțire. Tratăm două cazuri, după cum H nu îl conține pe 0, respectiv H îl conține pe 0.

Cazul $0 \notin H$. Să fixăm un $x \in H$ oarecare (deci $x = x_i$ pentru un anumit $i \in \{1, 2, \ldots, n\}$). Elementele $xx_1, xx_2, \ldots, xx_n$ aparțin lui H și sunt distincte două câte două (căci $i \neq j \Rightarrow x_i \neq x_j$ și cum $x \neq 0 \Rightarrow xx_i \neq xx_j$). Cum H are n elemente, înseamnă că $xx_1, xx_2, \ldots, xx_n$ sunt toate elementele lui H, aranjate eventual în altă ordine (permutate). Așadar:

$$H = \{x_1, x_2, \ldots, x_n\} = \{xx_1, xx_2, \ldots, xx_n\}.$$

Scriind produsul elementelor din H corespunzător celor două moduri în care gândim această mulțime, avem:

$$xx_1 \cdot xx_2 \cdot \ldots \cdot xx_n = x_1 x_2 \ldots x_n$$

şi simplificând cu $x_1x_2...x_n \neq 0$, obţinem $x^n = 1$.

Aceasta arată că x este o rădăcină de ordinul n a unităţii. Notând cu U_n mulţimea rădăcinilor de ordinul n ale unităţii, avem aşadar $x \in U_n$ şi cum $x \in H$ a fost arbitrar, desprindem concluzia că $H \subseteq U_n$. Însă ambele mulţimi H şi U_n au câte n elemente, prin urmare incluziunea precedentă este chiar o egalitate: $H = U_n$. Condiţia $H = U_n$, obţinută ca o condiţie necesară, este şi suficientă, în sensul că dacă $H = U_n$, atunci H este o parte a lui $\mathbb{C}$ stabilă faţă de înmulţire; într-adevăr, $\forall\, x,y \in U_n \Rightarrow x^n = 1$, $y^n = 1$ $\Rightarrow (xy)^n = x^n \cdot y^n = 1 \cdot 1 = 1 \Rightarrow xy \in U_n$.

<u>Cazul $0 \in H$</u>. Dacă $n = 1$, atunci $H = \{0\}$, care este parte a lui $\mathbb{C}$ stabilă faţă de înmulţire.

Dacă $n \geq 2$, fie $H' = H \setminus \{0\}$. Constatăm uşor că H' este parte finită a lui $\mathbb{C}$, stabilă faţă de înmulţire, care nu îl conţine pe 0. Cum H' are $n-1$ elemente, conform primului caz rezultă $H' = U_{n-1}$ şi atunci $H = \{0\} \cup U_{n-1}$. Observăm că această mulţime H este stabilă faţă de înmulţire.

În primul caz ($0 \notin H$) numărul $n \in \mathbb{N}^*$ este arbitrar, iar în al doilea caz ($0 \in H$) numărul $n \geq 2$ este arbitrar, deci $n - 1 \in \mathbb{N}^*$ este la rândul său arbitrar.

Concluzia este că părţile finite ale lui $\mathbb{C}$, stabile faţă de înmulţire sunt: $\{0\}$; U_n; $\{0\} \cup U_n$, unde U_n este mulţimea rădăcinilor de ordinul n ale unităţii, iar $n \in \mathbb{N}^*$ este arbitrar.

Pentru a obţine părţile finite ale lui $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, stabile faţă de înmulţire, intersectăm fiecare din aceste mulţimi cu părţile găsite pentru $\mathbb{C}$ şi obţinem de fiecare dată următoarele cinci mulţimi: $\{0\}$; $\{1\}$; $\{0, 1\}$; $\{-1, 1\}$; $\{-1, 0, 1\}$.

2. Pe mulţimea $\mathbb{Z}$ definim operaţia: $x * y = x + y + xy$.

Să se studieze asociativitatea, comutativitatea, existenţa elementului neutru şi a elementelor simetrizabile.

Soluţie. Pentru orice $x, y, z \in \mathbb{Z}$ avem: $(x * y) * z = x * y + z + (x * y)z = x + y + xy + z + (x + y + xy)z = x + y + z + xy + xz + yz + xyz$, iar $x * (y * z) = x + y * z + x(y * z) = x + y + z + yz + x(y + z + yz) = x + y + z + xy + xz + yz + xyz$, deci $(x * y) * z = x * (y * z)$, adică $*$ este asociativă. Pentru orice $x, y \in \mathbb{Z}$ avem $x * y = x + y + xy = y + x + yx = y * x$, deci $*$ este comutativă. Căutăm $e \in \mathbb{Z}$ astfel încât $x * e = e * x = x$, $\forall\, x \in \mathbb{Z}$, adică $e(1 + x) = 0$, $\forall\, x \in \mathbb{Z}$, deci $e = 0$ este elementul neutru. Dacă $x \in \mathbb{Z}$ este simetrizabil, $\exists\, x' \in \mathbb{Z}$ astfel încât $x * x' = x' * x = 0$ sau $x'(1 + x) = -x$. Trebuie ca $x \neq -1$ şi atunci $x' = -\dfrac{x}{1+x} = -1 + \dfrac{1}{1+x}$. Cum $x' \in \mathbb{Z}$ trebuie ca $1 + x \in \{-1, 1\}$ deci $x \in \{0, -2\}$, adică elementele simetrizabile sunt 0 şi -2.

EXERCIȚII PROPUSE

1. Pe mulțimea $M = \{0, 1, 2\}$ definim operația $*$ prin $x * y = |x - y|$. Scrieți tabla acestei operații.

2. Pe mulțimea $\mathbb{R}$ definim operația $*$ prin $x * y = xy - 2(x + y) + 6$. Arătați că intervalul $H = [2, \infty)$ este o parte a lui $\mathbb{R}$ stabilă față de operația $*$.

3. Se consideră numerele reale a, b și operația $*$ pe $\mathbb{R}$ definită prin
$$x * y = xy - a(x + y) + b.$$
Arătați că intervalul (a, ∞) este o parte a lui $\mathbb{R}$ stabilă față de operația $*$ dacă și numai dacă $b \geq a(a + 1)$.

4. Fie $d \in \mathbb{Z}$ un întreg care nu este pătrat perfect, iar $\sqrt{d}$ una din rădăcinile ecuației $x^2 = d$. Considerăm mulțimile:
$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$, $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$.
a) Arătați că $\mathbb{Z}[\sqrt{d}]$ și $\mathbb{Q}(\sqrt{d})$ sunt părți ale lui $\mathbb{C}$ (respectiv ale lui $\mathbb{R}$, când $d > 0$) stabile față de adunare și față de înmulțire.
b) Arătați că mulțimea $H = \{x + y\sqrt{d} \mid x, y \in \mathbb{Z}, x^2 - dy^2 = 1\}$ este o parte a lui $\mathbb{Z}[\sqrt{d}]$ stabilă față de înmulțire.

5. Fie $M = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$. Arătați că M este o parte a lui $\mathcal{M}_2(\mathbb{Z})$, stabilă față de înmulțire.

6. Să se demonstreze că mulțimile $H_1 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{R}, a + b = c + d \right\}$ și $H_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{R}, a + c = b + d \right\}$ sunt părți ale lui $\mathcal{M}_2(\mathbb{R})$, stabile față de înmulțire.

7. a) Demonstrați că $H_1 = \left\{ \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \middle| a, b, c \in \mathbb{Z} \right\}$ este o parte a lui $\mathcal{M}_3(\mathbb{Z})$, stabilă față de înmulțirea matricelor.
b) Deduceți că $H_2 = \{a^3 + b^3 + c^3 - 3abc \mid a, b, c \in \mathbb{Z}\}$ este o parte a lui $\mathbb{Z}$, stabilă față de înmulțirea numerelor întregi.

8. Fie A o mulțime nevidă. Considerăm mulțimile de funcții:
$A^A = \{f : A \to A\}$; $\mathfrak{I}(A) = \{f : A \to A \mid f \text{ injectivă}\}$; $\mathcal{S}(A) = \{f : A \to A \mid f \text{ surjectivă}\}$;

$\mathscr{B}(A)=\{f:A\to A \mid f \text{ bijectivă}\}$. Arătaţi că $\Im(A)$, $\mathscr{S}(A)$, $\mathscr{B}(A)$ sunt părţi ale lui A^A, stabile faţă de compunerea funcţiilor.

9. Pe mulţimea $\mathbb{Z}\times\mathbb{Z}$ definim operaţia $*$ prin $(a, b) * (c, d) = (ac, bc + d)$.

Să se arate că operaţia $*$ este asociativă, are element neutru şi să se determine elementele simetrizabile.

10. Fie M o mulţime cu cel puţin 2 elemente, pe care definim operaţiile:

$x * y = x,\ \forall\, x, y \in M$, respectiv $x \circ y = y,\ \forall\, x, y \in M$.

Să se arate că operaţiile $*$ şi $\circ$ sunt asociative, necomutative şi nu au element neutru.

11. Spunem că operaţia $*$ pe mulţimea M are *elementul neutru la stânga* e_s dacă $\exists\, e_s \in M$ astfel încât $e_s * x = x$, $\forall\, x \in M$; spunem că operaţia $*$ are *elementul neutru la dreapta* e_d dacă $\exists\, e_d \in M$ astfel încât $x * e_d = x$, $\forall\, x \in M$.

Arătaţi că dacă operaţia $*$ are elemente neutre la stânga şi la dreapta, atunci are element neutru.

12. Pe mulţimea M considerăm operaţia $*$ asociativă şi având elementul neutru e. Spunem că un element $x \in M$ este *simetrizabil la stânga* (respectiv *simetrizabil la dreapta*) dacă $\exists\, x'_s \in M$ (respectiv $\exists\, x'_d \in M$) astfel încât $x'_s * x = e$ (respectiv $x * x'_d = e$). Arătaţi că dacă $x \in M$ este simetrizabil la stânga şi la dreapta, atunci x este simetrizabil.

Grup, exemple

Comentariu metodic. Vom studia în continuare principalele structuri algebrice. În general prin „***structură algebrică***” vom înţelege o mulţime nevidă înzestrată cu una sau mai multe operaţii ce satisfac anumite axiome. Cu alte cuvinte, definiţia unei structuri algebrice este un sistem axiomatic.

Se poate arăta că un sistem axiomatic ce defineşte o structură algebrică verifică cerinţele logice pe care trebuie să le îndeplinească orice sistem axiomatic, dar cadrul manualului nu ne permite asemenea dezvoltări.

Structurile algebrice pe care le vom studia sunt: grupul (cu o singură operaţie), inelul, corpul (cu două operaţii).

Definiţie

Se numeşte ***grup*** un cuplu $(G, *)$ unde G este o mulţime nevidă, iar „$*$” este o operaţie pe mulţimea G, care satisface următoarele trei axiome (proprietăţi):

1° $(x * y) * z = x * (y * z)$, $\forall\, x,y,z \in G$ (adică operaţia $*$ este ***asociativă***);

2° $\exists\, e \in G$ astfel încât $x * e = e * x = x$, $\forall\, x \in G$ (adică operaţia $*$ ***are elementul neutru*** e);

3° $\forall\, x \in G$, $\exists\, x' \in G$ astfel încât $x * x' = x' * x = e$ (adică orice element $x \in G$ este ***simetrizabil***, deci are un ***element simetric*** $x' \in G$).

Dacă, în plus, este satisfăcută şi axioma a patra:

4° $x * y = y * x$, $\forall x,y \in G$ (adică operația $*$ este ***comutativă***), cuplul $(G, *)$ se numește ***grup comutativ (abelian)***.

Comentariu metodic. 1) Pentru simplitatea scrierii, vom nota cel mai adesea operația unui grup ca pe o înmulțire (notație multiplicativă), iar uneori ca pe o adunare (notație aditivă). Acest ***prim pas spre abstractizare***, ținând de notația operației grupului, trebuie bine înțeles: în expunerea părții teoretice, când lucrăm cu grupuri oarecare și nu cu exemple concrete, notația este neesențială, așa că o alegem pe cea mai simplă.
2) Când operația se subînțelege, nu o mai scriem. De exemplu, în loc de grupul $(G, *)$, scriem simplu, grupul G.

Exemple de grupuri numerice

Cele mai simple exemple de grupuri sunt cele determinate de operațiile uzuale (adunare, înmulțire) pe mulțimi remarcabile de numere și anume:

$(\mathbb{Z}, +)$; $(\mathbb{Q}, +)$; $(\mathbb{R}, +)$; $(\mathbb{C}, +)$;

$(\mathbb{Q}^*, \cdot)$; $(\mathbb{R}^*, \cdot)$; $(\mathbb{C}^*, \cdot)$; $(\mathbb{R}_+^*, \cdot)$,

unde am notat $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, $\mathbb{R}_+^* = (0, \infty)$.

Aceste grupuri se numesc ***grupul aditiv al numerelor întregi, grupul aditiv al numerelor raționale*** ș.a.m.d., respectiv ***grupul multiplicativ al numerelor raționale nenule, grupul multiplicativ al numerelor reale nenule*** ș.a.m.d.

Verificarea axiomelor grupului este imediată și poate avea un caracter oral. Aceste grupuri sunt comutative (abeliene).

Grupul rădăcinilor de ordin *n* ale unității

Un alt grup important, „*organizat*" pe o mulțime de numere este grupul rădăcinilor de ordinul n ale unității.

Reamintim că pentru fiecare $n \in \mathbb{N}^*$ submulțimea lui $\mathbb{C}$ definită prin

$$U_n = \{x \in \mathbb{C} \mid x^n = 1\} = \left\{\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \;\middle|\; k = 0, 1, 2, \ldots, n-1\right\}$$

se numește ***mulțimea rădăcinilor de ordinul n ale unității***.

Dacă $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, avem $\zeta^k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$, deci

$$U_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\} = \{\zeta^k \mid k \in \mathbb{Z}\}.$$

De exemplu, pentru $n = 1$ avem $\zeta = 1$, deci $U_1 = \{1\}$; pentru $n = 2$ avem $\zeta = -1$ și $U_2 = \{1, \zeta\} = \{1, -1\}$; pentru $n = 4$ avem $\zeta = i$ și $U_4 = \{1, \zeta, \zeta^2, \zeta^3\} = \{1, i, -1, -i\}$.

Propoziție

Mulțimea U_n este un grup abelian față de înmulțirea numerelor complexe, numit ***grupul rădăcinilor de ordinul n ale unității***.

Demonstrație. Mai întâi arătăm că înmulțirea este operație pe mulțimea U_n sau, echivalent, U_n este parte a lui $\mathbb{C}$, stabilă față de înmulțire.

Într-adevăr $\forall\, x,y \in U_n \Rightarrow x^n = y^n = 1 \Rightarrow (xy)^n = x^n y^n = 1 \cdot 1 = 1 \Rightarrow xy \in U_n$.

Verificăm axiomele grupului abelian.

1° Înmulțirea este asociativă pe mulțimea U_n, întrucât este asociativă pe mulțimea $\mathbb{C}$.

2° Deoarece $1 \in U_n$, rezultă că 1 este elementul – unitate pentru înmulțirea din U_n.

3° Orice $x \in U_n$ este inversabil în U_n, ceea ce se justifică astfel: $x \in U_n \Rightarrow x \neq 0 \Rightarrow \exists\, \frac{1}{x} \in \mathbb{C}$, dar $\frac{1}{x} \in U_n$, deoarece $\left(\frac{1}{x}\right)^n = \frac{1}{x^n} = \frac{1}{1} = 1$ și astfel inversul $\frac{1}{x}$ al lui x se menține în U_n.

4° Înmulțirea este comutativă pe mulțimea U_n, întrucât este comutativă pe mulțimea $\mathbb{C}$.

Terminologie. Dacă $(G, *)$ este un grup, numărul elementelor (cardinalul) mulțimii G se numește ***ordinul grupului G***. Ordinul unui grup poate fi finit sau infinit.

Exemplul anterior arată că grupul U_n are ordinul n.

Alte exemple de grupuri

Multe exemple de grupuri se obțin în strânsă legătură cu o altă structură algebrică și anume aceea de ***monoid***.

Definiție

Se numește ***monoid*** un cuplu $(M, *)$, unde M este o mulțime nevidă, iar „$*$" este o operație pe mulțimea M, care satisface următoarele două axiome:

1° $(x * y) * z = x * (y * z)$, $\forall\, x,y,z \in M$ (operația $*$ este asociativă);

2° $\exists\, e \in M$ astfel încât $x * e = e * x = x$, $\forall\, x \in M$ (operația $*$ are elementul neutru e).

Dacă, în plus, este satisfăcută și axioma a treia:

3° $x * y = y * x$, $\forall\, x,y \in M$ (operația $*$ este comutativă), atunci cuplul $(M, *)$ se numește ***monoid comutativ***.

Observație

Întrucât axiomele ce definesc monoidul se regăsesc și în definiția grupului (sunt primele două axiome ale grupului), deducem că orice grup este un monoid, deci structura de monoid este mai „*largă*" (mai „*generală*") decât aceea de grup.

Exemple imediate de monoizi sunt: $(\mathbb{N}, +)$; $(\mathbb{N}, \cdot)$; $(\mathbb{Z}, \cdot)$; $(\mathbb{Q}, \cdot)$; $(\mathbb{R}, \cdot)$; $(\mathbb{C}, \cdot)$; $(\mathcal{M}_n(\mathbb{C}), \cdot)$.

Notație

Dacă $(M, *)$ este un monoid având elementul neutru e, notăm cu $U(M)$ mulțimea elementelor simetrizabile din monoidul M, adică:

$$U(M) = \{x \in M \mid \exists\, x' \in M \text{ cu } x * x' = x' * x = e\}.$$

Rezultatul de mai jos arată că mulțimea $U(M)$ este chiar un grup.

Teoremă

Dacă $(M, *)$ este un monoid, mulțimea $U(M)$ a elementelor simetrizabile din monoidul M este un grup în raport cu operația monoidului, numit ***grupul elementelor inversabile*** sau ***grupul unităților*** din monoidul M.

Demonstrație. Mai întâi arătăm că „$*$" este o operație pe mulțimea $U(M)$, adică $\forall\, x,y \in U(M) \Rightarrow x * y \in U(M)$. Pentru aceasta, este suficient să arătăm că simetricul elementului $x * y$ este elementul

$$(x * y)' = y' * x' \qquad (1)$$

unde x', y' sunt simetricele lui x, respectiv y. Într-adevăr:

$$(x * y) * (y' * x') = x * (y * y') * x' = x * e * x' = x * x' = e;$$
$$(y' * x') * (x * y) = y' * (x' * x) * y = y' * e * y = y' * y = e.$$

Verificăm acum axiomele grupului.

1° Operația $*$ este asociativă pe mulțimea $U(M)$, întrucât este asociativă pe mulțimea M.

2° Elementul neutru $e \in M$ este simetrizabil, căci $e' = e$, deci $e \in U(M)$ și atunci e este element neutru și pentru operația indusă pe $U(M)$.

3° Orice element $x \in U(M)$ are un simetric $x' \in M$, dar atunci și x' este simetrizabil (având simetricul x), ceea ce înseamnă că $x' \in U(M)$. Așadar orice $x \in U(M)$ este simetrizabil în $U(M)$.

Observații

1) Reținem egalitatea (1) din demonstrația teoremei precedente:

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

care se transcrie în notație multiplicativă, respectiv aditivă prin:

$$(xy)^{-1} = y^{-1}x^{-1} \ \text{ respectiv } \ -(x + y) = -y - x, \ \forall\, x,y \in U(M).$$

2) De asemenea, faptul că x' are drept simetric pe x, se scrie:

$$(x')' = x, \ \forall\, x \in U(M),$$

iar în notație multiplicativă, respectiv aditivă, se transcrie:

$$(x^{-1})^{-1} = x, \text{ respectiv } -(-x) = x, \ \forall\, x \in U(M).$$

Exemple de grupuri de elemente inversabile ale unor monoizi

Pentru monoidul $(\mathbb{N}, \cdot)$ avem $U(\mathbb{N}) = \{1\} = U_1$.

Pentru monoidul $(\mathbb{Z}, \cdot)$ avem $U(\mathbb{Z}) = \{-1, 1\} = U_2$.

Pentru monoidul $(\mathbb{Q}, \cdot)$ avem $U(\mathbb{Q}) = \mathbb{Q}^*$.

Pentru monoidul $(\mathbb{R}, \cdot)$ avem $U(\mathbb{R}) = \mathbb{R}^*$.

Pentru monoidul $(\mathbb{C}, \cdot)$ avem $U(\mathbb{C}) = \mathbb{C}^*$.

Pentru monoidul $(\mathcal{M}_n(\mathbb{C}), \cdot)$ grupul elementelor inversabile este

$$GL_n(\mathbb{C}) = \{X \in \mathcal{M}_n(\mathbb{C}) \mid \det X \neq 0\},$$

iar acest grup este necomutativ pentru $n \geq 2$.

Pentru monoidul $(A^A, \circ)$, unde $A^A = \{f : A \to A\}$, iar „$\circ$" este compunerea funcţiilor, grupul elementelor inversabile este $U(A^A) = \{f : A \to A \mid f \text{ bijecţie}\}$.

Şi acest grup este necomutativ, dacă mulţimea A are cel puţin trei elemente.

Grupuri de matrice

Dacă $m,n \in \mathbb{N}^*$, atunci cuplul $(\mathcal{M}_{m,n}(\mathbb{C}), +)$ este un grup abelian numit *grupul aditiv al matricelor de tip (m, n) peste* $\mathbb{C}$.

Analog, putem vorbi de grupurile aditive abeliene $(\mathcal{M}_{m,n}(\mathbb{Z}), +)$, $(\mathcal{M}_{m,n}(\mathbb{Q}), +)$, $(\mathcal{M}_{m,n}(\mathbb{R}), +)$.

Verificările axiomelor grupului sunt imediate şi pot fi făcute oral.

Am văzut că grupul multiplicativ al elementelor inversabile din monoidul $(\mathcal{M}_{m,n}(\mathbb{C}), +)$ este $GL_n(\mathbb{C}) = \{X \in \mathcal{M}_n(\mathbb{C}) \mid \det X \neq 0\}$ care se numeşte *grupul liniar de ordin n peste* $\mathbb{C}$.

Analog, putem vorbi de grupurile multiplicative:

$$GL_n(\mathbb{R}) = \{X \in \mathcal{M}_n(\mathbb{R}) \mid \det X \neq 0\},$$

$$GL_n(\mathbb{Q}) = \{X \in \mathcal{M}_n(\mathbb{Q}) \mid \det X \neq 0\},$$

$$GL_n(\mathbb{Z}) = \{X \in \mathcal{M}_n(\mathbb{Z}) \mid \det X = \pm 1\}.$$

Aceste grupuri multiplicative de matrice pătratice sunt grupuri necomutative.

Grupul claselor de resturi modulo *n*

Fie $n \geq 2$ un număr natural. Resturile care se obţin la împărţirea cu n a diverselor numere întregi sunt $0, 1, 2, \ldots, n-1$.

Numerele întregi care dau la împărţirea cu n restul 0 sunt de forma nk, cu $k \in \mathbb{Z}$, iar mulţimea lor o notăm $n\mathbb{Z}$; caracteristica acestor numere este restul lor comun la împărţirea cu n şi anume 0, de aceea această mulţime se mai notează $\hat{0}$ şi se numeşte *clasa 0 modulo n*. Aşadar $\hat{0} = n\mathbb{Z}$.

Numerele întregi care dau la împărţirea cu n restul 1 sunt de forma $nk + 1$, cu $k \in \mathbb{Z}$, iar mulţimea lor o notăm $n\mathbb{Z} + 1$; caracteristica acestor numere este restul lor comun la împărţirea cu n şi anume 1, de aceea această mulţime se mai notează $\hat{1}$ şi se numeşte *clasa 1 modulo n*. Aşadar $\hat{1} = n\mathbb{Z} + 1$.

În mod asemănător construim mulţimile de numere întregi

$\hat{2} = n\mathbb{Z} + 2$, $\hat{3} = n\mathbb{Z} + 3$, ..., $\widehat{n-1} = n\mathbb{Z} + n - 1$, pe care le vom numi respectiv clasa 2 modulo n, clasa 3 modulo n, ..., clasa $n - 1$ modulo n.

Mulţimea $\mathbb{Z}_n = \{\hat{0}, \hat{1}, \hat{2}, ..., \widehat{n-1}\}$ se numeşte ***mulţimea claselor de resturi modulo n.***

Orice număr întreg a aparţine uneia şi numai uneia din clasele de resturi $\hat{0}$, $\hat{1}$, $\hat{2}$, ..., $\widehat{n-1}$, mai precis $a \in \hat{r}$, unde r este restul împărţirii numărului întreg a prin împărţitorul fixat n. Scriem atunci $\hat{a} = \hat{r}$, adică vom considera că fiecare număr întreg are o clasă modulo n, mai exact, clasa fiecărui număr este clasa restului său la împărţirea cu n. Aşadar, pentru două numere $a, b \in \mathbb{Z}$, avem echivalenţele:

$$\hat{a} = \hat{b} \Leftrightarrow a \text{ şi } b \text{ dau acelaşi rest la împărţirea cu } n \Leftrightarrow a - b = kn, \text{ cu } k \in \mathbb{Z}.$$

Putem scrie deci: $\mathbb{Z}_n = \{\hat{0}, \hat{1}, \hat{2}, ..., \widehat{n-1}\} = \{\hat{a} \mid a \in \mathbb{Z}\}$.

Pe mulţimea $\mathbb{Z}_n$ a claselor de resturi modulo n, introducem operaţiile:

– *adunarea* claselor de resturi, definită prin:

$$\hat{x} + \hat{y} = \widehat{x+y} \text{ (suma claselor este egală cu clasa sumei);}$$

– *înmulţirea* claselor de resturi, definită prin:

$$\hat{x} \cdot \hat{y} = \widehat{xy} \text{ (produsul claselor este egal cu clasa produsului).}$$

Aşadar, operaţiile cu clase de resturi sunt „inspirate" de operaţiile corespunzătoare cu numere întregi.

Comentariu metodic privind operaţiile cu clase de resturi

Apare aici o problemă şi anume dacă aceste operaţii sunt „bine definite" sau „consistente". Să explicăm ce înseamnă aceasta. În general, o corespondenţă $f : A \to B$ este „bine definită" ca funcţie dacă oricărui $x \in A$ îi corespunde un unic $f(x) \in B$, ceea ce se traduce sugestiv prin implicaţia:

$$x = x' \Rightarrow f(x) = f(x').$$

Deoarece o operaţie $*$ pe o mulţime M este o funcţie

$$* : M \times M \to M,$$

a spune că operaţia $*$ este „bine definită" revine, conform celor de mai sus, la a spune că $(x, y) = (x', y') \Rightarrow x * y = x' * y'$, adică, în definitiv:

$$x = x',\ y = y' \Rightarrow x * y = x' * y'.$$

Deoarece clasele de resturi se introduc prin „reprezentanţi" ai lor, adică numere întregi ce aparţin claselor respective, iar o clasă poate fi „reprezentată" de orice element al său, ne punem problema: dacă schimbăm reprezentanţii claselor, se schimbă cumva „rezultatul" operației? Vom vedea că nu, mai exact probăm implicațiile:

$$\hat{x}=\widehat{x'},\ \ \hat{y}=\widehat{y'} \Rightarrow \hat{x}+\hat{y}=\widehat{x'}+\widehat{y'};$$

$$\hat{x}=\widehat{x'},\ \ \hat{y}=\widehat{y'} \Rightarrow \hat{x}\cdot\hat{y}=\widehat{x'}\cdot\widehat{y'},$$

ceea ce va arăta că operațiile cu clase de resturi sunt bine definite.

Într-adevăr, $\hat{x}=\widehat{x'} \Rightarrow x - x' = k_1 n$, cu $k_1 \in \mathbb{Z}$, $\hat{y}=\widehat{y'} \Rightarrow y - y' = k_2 n$, cu $k_2 \in \mathbb{Z}$ şi atunci $(x + y) - (x' + y') = (x - x') + (y - y') = (k_1 + k_2)n$, ceea ce înseamnă că $\widehat{x+y}=\widehat{x'+y'}$, adică $\hat{x}+\hat{y}=\widehat{x'}+\widehat{y'}$; de asemenea $xy - x'y' = xy - xy' + xy' - x'y' =$ $= x(y - y') + y'(x - x') = xk_2 n + y'k_1 n = (xk_2 + y'k_1)n$, ceea ce înseamnă că $\widehat{xy}=\widehat{x'y'}$, adică $\hat{x}\cdot\hat{y}=\widehat{x'}\cdot\widehat{y'}$.

Ne preocupă să vedem ce structuri algebrice dau adunarea respectiv înmulțirea pe mulțimea $\mathbb{Z}_n$. Avem în acest sens următoarea:

Teoremă

Dacă $n \geq 2$ este un număr natural, atunci:

a) Cuplul $(\mathbb{Z}_n, +)$ este un grup abelian, numit ***grupul aditiv al claselor de resturi modulo n***.

b) Cuplul $(\mathbb{Z}_n, \cdot)$ este un monoid comutativ, în care grupul elementelor inversabile este:

$$U(\mathbb{Z}_n) = \{\hat{k} \in \mathbb{Z}_n \mid (k, n) = 1\}$$

numit ***grupul multiplicativ al claselor de resturi modulo n relativ prime cu n***.

Demonstrație. a) Verificăm axiomele grupului abelian.

1°. Adunarea claselor este asociativă; într-adevăr, dacă ținem seama de asociativitatea adunării pe $\mathbb{Z}$ şi de definiția adunării pe mulțimea $\mathbb{Z}_n$, avem pentru orice $\hat{x}, \hat{y}, \hat{z} \in \mathbb{Z}_n$:

$$(\hat{x}+\hat{y})+\hat{z} = \widehat{x+y}+\hat{z} = \widehat{(x+y)+z} = \widehat{x+(y+z)} = \hat{x}+\widehat{y+z} = \hat{x}+(\hat{y}+\hat{z}).$$

2°. Adunarea claselor are element neutru clasa nulă $\hat{0}$, deoarece:

$$\hat{x}+\hat{0} = \hat{0}+\hat{x} = \widehat{x+0} = \hat{x},\ \forall\, \hat{x} \in \mathbb{Z}_n.$$

3°. Orice clasă $\hat{x} \in \mathbb{Z}_n$ are drept clasă opusă clasa lui $-x$, adică $-\hat{x} = \widehat{(-x)}$, deoarece: $\hat{x} + \widehat{(-x)} = \widehat{(-x)} + \hat{x} = \widehat{x+(-x)} = \hat{0}$.

(De asemenea, pentru $k \in \{0, 1, 2, \ldots, n-1\}$ avem $-\hat{k} = \widehat{n-k}$, deoarece $\hat{k}+\widehat{n-k} =$ $=\hat{n} = \hat{0}$).

4°. Adunarea claselor este comutativă; într-adevăr:

$$\hat{x} + \hat{y} = \widehat{x+y} = \widehat{y+x} = \hat{y} + \hat{x},\ \forall\, \hat{x}, \hat{y} \in \mathbb{Z}_n.$$

b) Verificăm axiomele monoidului comutativ:

1°. Înmulțirea claselor este asociativă; într-adevăr:

$$(\hat{x}\,\hat{y})\,\hat{z} = \widehat{xy}\cdot\hat{z} = \widehat{(xy)z} = \widehat{x(yz)} = \hat{x}\cdot\widehat{yz} = \hat{x}(\hat{y}\,\hat{z}),\ \forall\, \hat{x}, \hat{y}, \hat{z} \in \mathbb{Z}_n.$$

2°. Cum $n \geq 2$ avem $\hat{1} \in \{\hat{0}, \hat{1}, ..., \widehat{n-1}\} = \mathbb{Z}_n$ și $\hat{1}$ este elementul–unitate, deoarece:

$$\hat{x}\cdot\hat{1} = \hat{1}\cdot\hat{x} = \widehat{x\cdot 1} = \hat{x},\ \forall\, \hat{x} \in \mathbb{Z}_n.$$

3°. Înmulțirea claselor este comutativă; într-adevăr:

$$\hat{x}\cdot\hat{y} = \widehat{xy} = \widehat{yx} = \hat{y}\cdot\hat{x},\ \forall\, \hat{x}, \hat{y} \in \mathbb{Z}_n.$$

Determinăm acum grupul elementelor inversabile (grupul unităților) din acest monoid. Pentru a proba egalitatea din enunț, arătăm echivalența:

$$\hat{k} \in U(\mathbb{Z}_n) \Leftrightarrow (k, n) = 1.$$

„$\Rightarrow$" Presupunem $\hat{k} \in U(\mathbb{Z}_n)$, deci există $\hat{p} \in \mathbb{Z}_n$ cu $\hat{k}\cdot\hat{p} = \hat{1}$. Aceasta se scrie succesiv $\widehat{kp} = \hat{1} \Leftrightarrow kp - 1 = nq$ cu $q \in \mathbb{Z}$.

Dacă $d = (k, n)$, $d \in \mathbb{N}^*$, rezultă $d \mid (kp - nq)$, adică $d \mid 1$, deci $d = 1$. Așadar $(k, n) = 1$.

„$\Leftarrow$" Presupunem $(k, n) = 1$. Atunci există $a, b \in \mathbb{Z}$ cu $ak + bn = 1$. (Justificare: numerele $k - 1$, $2k - 1$, $3k - 1$, ..., $nk - 1$ dau resturi distincte la împărțirea cu n, deci unul din ele este multiplu de n.) Deoarece două numere egale au clase de resturi egale, trecem la clase și obținem $\widehat{ak+bn} = \hat{1}$ care se scrie succesiv $\widehat{ak+bn} = \hat{1} \Leftrightarrow \hat{a}\cdot\hat{k} + \hat{b}\cdot\hat{n} = \hat{1} \Leftrightarrow \hat{a}\cdot\hat{k} + \hat{b}\cdot\hat{0} = \hat{1} \Leftrightarrow \hat{a}\cdot\hat{k} + \hat{0} = \hat{1} \Leftrightarrow$ $\Leftrightarrow \hat{a}\cdot\hat{k} = \hat{1}$, ceea ce arată că $\hat{k} \in U(\mathbb{Z}_n)$, inversa clasei $\hat{k}$ fiind clasa $\hat{a}$.

Observație

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

Exemplu

Pentru $n = 10$, grupul multiplicativ al elementelor inversabile din monoidul $(\mathbb{Z}_{10}, \cdot)$ este $U(\mathbb{Z}_{10}) = \{\hat{1}, \hat{3}, \hat{7}, \hat{9}\}$ care are ordinul $\varphi(10) = 4$.

Grupuri de permutări

Am văzut că dacă A este o mulțime nevidă, iar $(A^A, \circ)$ este monoidul funcțiilor definite pe A cu valori în A, operația „$\circ$" fiind aceea de compunere a funcțiilor, atunci grupul elementelor inversabile din acest monoid este:

$$U(A^A) = \{f : A \to A \mid f \text{ bijecție}\}.$$

În cazul când $A = \{1, 2, \ldots, n\}$, unde $n \in \mathbb{N}^*$ este fixat, grupul acesta al bijecțiilor mulțimii $\{1, 2, \ldots, n\}$ pe ea însăși se numește ***grupul permutărilor de grad n*** sau ***grupul simetric de grad n*** și se notează S_n. Acest grup este necomutativ dacă $n \geq 3$. Un studiu sistematic al permutărilor a fost întreprins în clasa a XI-a, de aceea vom reaminti pe scurt câteva chestiuni care privesc caracterul „grupal" al permutărilor.

Deoarece numărul permutărilor de grad n este egal cu $n!$, înseamnă că $(S_n, \circ)$ este un grup de ordin $n!$. Pentru o permutare scrisă ca un tablou:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix} \in S_n,$$

permutarea inversă σ^{-1} se obține „inversând" linia de sus cu cea de jos.

Cuplurile (i, j) cu $1 \leq i < j \leq n$, pentru care $\sigma(i) > \sigma(j)$ se numesc ***inversiuni*** ale permutării σ. Permutările cu un număr par de inversiuni se numesc ***permutări pare***, iar cele cu un număr impar de inversiuni se numesc ***permutări impare***. Numărul rațional $\varepsilon(\sigma)$ definit astfel:

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} = \begin{cases} +1, & \text{dacă } \sigma \text{ este permutare pară} \\ -1, & \text{dacă } \sigma \text{ este permutare impară} \end{cases}$$

se numește ***semnul*** (***signatura***) permutării σ.

Pentru orice două permutări $\sigma, \tau \in S_n$ există egalitățile:

1°. $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\, \varepsilon(\tau)$ (semnul produsului este produsul semnelor);

2°. $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$ (două permutări inverse au același semn).

În fine, dăm acum un rezultat care pune în evidență un alt grup de permutări de grad n, inclus în grupul simetric S_n.

Teoremă

Dacă A_n este mulțimea permutărilor pare din grupul simetric S_n, atunci A_n este la rândul său un grup relativ la produsul (compunerea) permutărilor.

Acest grup se numește ***grupul altern de grad n*** și are ordinul $\frac{n!}{2}$ pentru $n \geq 2$, respectiv 1 pentru $n = 1$.

Demonstrație. Dacă $\sigma, \tau \in A_n$, atunci $\varepsilon(\sigma) = 1$, $\varepsilon(\tau) = 1$ și rezultă $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\, \varepsilon(\tau) = 1 \cdot 1 = 1$, ceea ce arată că $\sigma\tau \in A_n$.

Prin urmare produsul permutărilor este operație algebrică pe mulțimea A_n.

Verificăm axiomele grupului.

1°. Produsul permutărilor este asociativ pe A_n, întrucât este asociativ pe S_n.

2°. Elementul neutru este permutarea identică $e \in A_n$ (este o permutare pară, întrucât are 0 inversiuni).

3°. Orice permutare $\sigma \in A_n$ este inversabilă în A_n, căci inversa sa $\sigma^{-1} \in S_n$ aparține chiar lui A_n (într-adevăr: $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma) = 1 \Rightarrow \sigma^{-1} \in A_n$).

Așadar A_n este un grup, necomutativ în general (mai precis, pentru $n \geq 4$).

Determinăm ordinul grupului A_n.

Dacă $n = 1$, avem $A_1 = S_1 = \{e\}$, deci ordinul lui A_1 este 1.

Dacă $n \geq 2$, fixăm o permutare impară $\alpha \in S_n$, de exemplu:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix} \text{ care are o singură inversiune.}$$

Definim funcţia $f : A \to S_n \setminus A_n$ prin $f(\sigma) = \alpha\sigma$ şi arătăm că este o bijecţie. Într-adevăr, mai întâi funcţia este bine definită, în sensul că ia valori în mulţimea permutărilor impare $S_n \setminus A_n$; aceasta, deoarece $\varepsilon(\alpha\sigma) = \varepsilon(\alpha)\,\varepsilon(\sigma) = -1 \cdot 1 = -1$, deci $\alpha\sigma$ este permutare impară.

Funcţia f este injectivă, căci $f(\sigma_1) = f(\sigma_2) \Rightarrow \alpha\sigma_1 = \alpha\sigma_2$ şi înmulţind la stânga cu α^{-1} rezultă $\sigma_1 = \sigma_2$.

Funcţia f este şi surjectivă, întrucât $\forall\, \tau \in S_n \setminus A_n$, $\exists\, \sigma = \alpha^{-1}\tau \in A_n$ astfel încât $f(\sigma) = \alpha\sigma = \alpha\,\alpha^{-1}\,\tau = \tau$ (am ţinut seama că dacă α este impară, atunci α^{-1} este impară, iar dacă α^{-1} şi τ sunt impare atunci produsul $\alpha^{-1}\,\tau$ este permutare pară, lucruri ce rezultă imediat din proprietăţile lui ε).

Aşadar f este bijecţie şi atunci mulţimile A_n şi $S_n \setminus A_n$ au acelaşi cardinal. Dar aceste mulţimi sunt disjuncte şi reuniunea lor este S_n, de cardinal $n!$, prin urmare fiecare din cele două mulţimi are cardinalul $\frac{n!}{2}$. În concluzie, ordinul grupului A_n este $\frac{n!}{2}$, când $n \geq 2$.

Comentariu metodic

Cronologic vorbind, grupurile de permutări sunt primele care au „apărut" în matematică. Mai bine zis, studiul permutărilor a permis degajarea conceptului general de grup.

Reguli de calcul într-un grup

Pentru uşurinţa scrierii, să adoptăm notaţia multiplicativă.

Dacă $(G, \cdot)$ este un grup, iar $x \in G$ un element fixat, definim ***puterile întregi*** ale lui x prin egalităţile:

$$\begin{cases} x^n = \underbrace{xxx\dots x}_{n \text{ ori}}, & \text{dacă } n \in \mathbb{N}^*; \\ x^0 = e & \text{(elementul neutru);} \\ x^{-n} = \left(x^n\right)^{-1}, & \text{dacă } n \in \mathbb{N}^*. \end{cases}$$

Putem stabili acum următorul rezultat:

Teoremă

Fie $(G, \cdot)$ un grup şi $x \in G$ fixat. Atunci:

1°. $x^n x^m = x^m x^n = x^{n+m}$, $\forall\, n,m \in \mathbb{Z}$;

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

Demonstraţie. 1°. Probăm egalitatea $x^n x^m = x^{n+m}$, tratând cazurile $n \geq 0$, $m \geq 0$; $n < 0$, $m < 0$; $n \geq 0$, $m < 0$; $n < 0$, $m \geq 0$.

Dacă $n \geq 0$, $m \geq 0$, atunci:

$$x^n x^m = \underbrace{xxx\ldots x}_{n \text{ ori}} \cdot \underbrace{xxx\ldots x}_{m \text{ ori}} = \underbrace{xxx\ldots x}_{n+m \text{ ori}} = x^{n+m}.$$

Dacă $n < 0$, $m < 0$, scriem $n = -n'$, $m = -m'$ cu $n' > 0$, $m' > 0$ şi avem:

$$x^n x^m = x^{-n'} x^{-m'} = (x^{n'})^{-1} (x^{m'})^{-1} = (x^{n'+m'})^{-1} = x^{-(n'+m')} = x^{n+m}.$$

Analog se tratează celelalte două cazuri.

Apoi, $x^m x^n = x^{m+n} = x^{n+m} = x^n x^m$ şi astfel punctul 1° este complet probat.

2°. Considerăm aceleaşi cazuri. Dacă $n \geq 0$, $m \geq 0$, atunci:

$$(x^n)^m = \underbrace{x^n x^n \ldots x^n}_{m \text{ ori}} = \underbrace{xxx\ldots x}_{nm \text{ ori}} = x^{nm}.$$

Dacă $n \geq 0$, $m < 0$ scriem $m = -m'$ cu $m' > 0$ şi avem:

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

Analog se tratează celelalte două cazuri.

Mai departe $(x^m)^n = x^{mn} = x^{nm} = (x^n)^m$ şi punctul 2° este probat.

Comentariu metodic

În scriere aditivă definim ***multiplii întregi*** ai unui element $x \in (G, +)$ prin egalităţile:

$$nx = \underbrace{x + x + \ldots + x}_{n \text{ ori}}, \text{ dacă } n \in \mathbb{N}^*;$$

$$0x = 0 \text{ (elementul neutru)};$$

$$(-n)x = -(nx), \text{ dacă } n \in \mathbb{N}^*.$$

Corespunzător, teorema precedentă se transcrie astfel:

1°. $nx + mx = mx + nx = (n + m)x$, $\forall\, n,m \in \mathbb{Z}$.

2°. $m(nx) = n(mx) = (nm)x$, $\forall\, n,m \in \mathbb{Z}$.

Rezultatul care urmează stabileşte o regulă de simplificare la stânga sau la dreapta într-un grup.

Teoremă

Fie $(G, \cdot)$ un grup şi $x,y,z \in G$ arbitrare. Avem echivalenţele:

1°. $zx = zy \Leftrightarrow x = y$ („simplificare" la stânga).

2°. $xz = yz \Leftrightarrow x = y$ („simplificare" la dreapta).

Demonstraţie. 1°. $(\Rightarrow)$ Presupunem $zx = zy$. Înmulţim la stânga cu z^{-1} şi avem succesiv:

$$z^{-1}(zx) = z^{-1}(zy) \Leftrightarrow (z^{-1}z)x = (z^{-1}z)y \Leftrightarrow ex = ey \Leftrightarrow x = y.$$

$(\Leftarrow)$ Presupunem $x = y$. Înmulţind la stânga cu z rezultă $zx = zy$.

2°. Analog.

Observaţie

Dacă grupul $(G, \cdot)$ este abelian putem simplifica printr-un element, fără a ţine seama că acesta este situat la stânga sau la dreapta. De exemplu:

$$xz = zy \Leftrightarrow x = y.$$

Comentariu metodic

Într-o scriere aditivă, teorema precedentă se transcrie astfel:

1°. $z + x = z + y \Leftrightarrow x = y$ („reducere" la stânga);

2°. $x + z = y + z \Leftrightarrow x = y$ („reducere la dreapta).

Să remarcăm că proprietatea elementară de a împărţi o egalitate (în particular, o ecuaţie) printr-un număr real nenul, decurge din teorema de mai sus aplicată în grupul $(\mathbb{R}^*, \cdot)$. De asemenea, posibilitatea de a reduce termeni egali situaţi în membri diferiţi ai unei egalităţi (în particular, ai unei ecuaţii) decurge din teorema de mai sus aplicată în grupul $(\mathbb{R}, +)$.

În fine, încheiem cu o „***teoremă de comutativitate***" adică o condiţie suficientă ca un grup să fie comutativ.

Teoremă

Dacă într-un grup $(G, \cdot)$ avem $x^2 = e$ pentru orice $x \in G$, atunci grupul este abelian.

Demonstraţie. Prin înmulţire cu x^{-1} ipoteza $x^2 = e$ se scrie echivalent:

$$x = x^{-1}, \ \forall x \in G.$$

Aşadar, în grupul G fiecare element este propriul său invers.

Atunci, pentru $x,y \in G$ arbitrare, avem:

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx,$$

deci grupul este abelian.

Exerciţii rezolvate

1. Să se arate că pe intervalul $G = (-1, 1)$ se poate defini operaţia algebrică:

$$x * y = \frac{x+y}{1+xy},$$

iar $(G, *)$ este un grup abelian.

Soluţie. Pentru a arăta că $*$ este operaţie algebrică pe $G = (-1, 1)$, arătăm că $\forall\ x,y \in$ $\in (-1, 1) \Rightarrow x * y \in (-1, 1)$.

E clar că $x,y \in (-1, 1) \Rightarrow |x| < 1$ şi $|y| < 1 \Rightarrow |xy| < 1 \Rightarrow xy \in (-1, 1) \Rightarrow$ $\Rightarrow 1 + xy > 0$. Atunci:

$$x * y - 1 = \frac{x+y}{1+xy} - 1 = \frac{x+y-1-xy}{1+xy} = \frac{(x-1)(1-y)}{1+xy} < 0,$$

deoarece $x - 1 < 0$, $1 - y > 0$ şi $1 + xy > 0$; rezultă că $x * y < 1$.

Analog se arată că $x * y > -1$.

Prin urmare $x * y \in (-1, 1)$, deci $*$ este operaţie pe $G = (-1, 1)$.

Verificăm acum axiomele grupului abelian.

1°. Operaţia $*$ este asociativă. Pentru $x,y,z \in G$ arbitrare, avem:

$$(x * y) * z = \frac{x+y}{1+xy} * z = \frac{\dfrac{x+y}{1+xy} + z}{1 + \dfrac{x+y}{1+xy} \cdot z} = \frac{x+y+z+xyz}{1+xy+xz+yz}, \text{ iar}$$

$$x * (y * z) = x * \frac{y+z}{1+yz} = \frac{x + \dfrac{y+z}{1+yz}}{1 + x \cdot \dfrac{y+z}{1+yz}} = \frac{x+y+z+xyz}{1+xy+xz+yz}.$$

Aşadar $(x * y) * z = x * (y * z)$, $\forall\ x,y,z \in G$, deci operaţia $*$ este asociativă.

2°. Operaţia $*$ are element neutru. Căutăm $e \in (-1, 1)$ astfel încât

$e * e = e * x = x$, $\forall\ x \in (-1, 1)$, ceea ce se scrie succesiv:

$$\frac{x+e}{1+xe} = x,\ \forall\ x \in (-1, 1) \Leftrightarrow x + e = x + x^2 e,\ \forall\ x \in (-1, 1) \Leftrightarrow$$

$$\Leftrightarrow e\left(1 - x^2\right) = 0,\ \forall\ x \in (-1, 1) \Leftrightarrow e = 0.$$

Aşadar $e = 0$ este element neutru pentru operaţia $*$.

3°. Orice element din G este simetrizabil faţă de operaţia $*$. Fie $x \in (-1, 1)$ arbitrar.

Căutăm $x' \in (-1, 1)$ astfel încât $x * x' = x' * x = 0$, ceea ce se scrie succesiv:

$$\frac{x+x'}{1+xx'} = 0 \Leftrightarrow x + x' = 0 \Leftrightarrow x' = -x \in (-1, 1).$$

Aşadar orice $x \in G$ este simetrizabil faţă de operaţia $*$, având simetricul $x' = -x$.

4°. Operaţia $*$ este comutativă. Pentru $x,y \in G$ arbitrare, avem:

$$x*y=\frac{x+y}{1+xy}=\frac{y+x}{1+yx}=y*x,$$

ceea ce înseamnă că operaţia $*$ este comutativă.

2. Fie $(G, \cdot)$ un cuplu format dintr-o mulţime nevidă şi o operaţie multiplicativă. Să se arate că $(G, \cdot)$ este grup dacă şi numai dacă sunt îndeplinite axiomele:

i) Operaţia este asociativă;

ii) Pentru fiecare $a,b \in G$ ecuaţiile $ax = b$ şi $xa = b$ au soluţie în G.

Soluţie. Dacă $(G, \cdot)$ este grup, atunci sunt îndeplinite axiomele i) şi ii). Într-adevăr operaţia grupului este asociativă, iar ecuaţiile $ax = b$ şi $xa = b$ au respectiv soluţiile $x_1 = a^{-1}b$, $x_2 = ba^{-1}$ care aparţin lui G.

Arătăm acum că dacă sunt verificate axiomele i) şi ii), atunci $(G, \cdot)$ este un grup. Trebuie să arătăm că există element neutru şi că orice element este inversabil.

Fixăm un element $a \in G$. Ecuaţia $xa = a$ are o soluţie $e_1 \in G$, deci $e_1a = a$. (1)

Ecuaţia $ax = a$ are de asemenea o soluţie $e_2 \in G$, deci $ae_2 = a$. (2)

Arătăm că e_1 este element neutru *„la stânga”* faţă de operaţia din G, adică:

$$e_1b = b, \ \forall\, b \in G. \qquad (3)$$

De asemenea, arătăm că e_2 este element neutru *„la dreapta”* faţă de operaţia din G, adică:

$$be_2 = b, \ \forall\, b \in G. \qquad (4)$$

Fie, într-adevăr, $b \in G$ oarecare. Ecuaţia $xa = b$ are o soluţie $x_1 \in G$, iar ecuaţia $ax = b$ are o soluţie $x_2 \in G$, prin urmare:

$$x_1a = b \quad (5) \quad \text{şi} \quad ax_2 = b. \quad (6)$$

Din (1), (2), (5), (6) avem:

$e_1b = e_1(ax_2) = (e_1a)x_2 = ax_2 = b$, adică (3), respectiv:

$be_2 = (x_1a)e_2 = x_1(ae_2) = x_1a = b$, adică (4).

Din faptul că operaţia are element neutru „la stânga” şi „la dreapta” vom arăta că are element neutru. Într-adevăr dacă luăm în (3) $b = e_2$ iar în (4) $b = e_1$ obţinem $e_1e_2 = e_2$, respectiv $e_1e_2 = e_1$, de unde $e_1 = e_2 \overset{\text{def.}}{=} e$. Atunci (3) şi (4) se scriu:

$$eb = be = b, \ \forall\, b \in G$$

şi arată că e este element neutru faţă de operaţia din G. Arătăm acum că orice element $b \in G$ este inversabil. Ecuaţia $xb = e$ are o soluţie $b_1 \in G$, iar ecuaţia $bx = e$ are o soluţie $b_2 \in G$, prin urmare:

$$b_1b = e \quad (7) \quad \text{şi} \quad bb_2 = e \quad (8).$$

Aşadar, b este inversabil „la stânga” şi „la dreapta”. Dar de aici rezultă că b este inversabil, întrucât:

$$b_1 = b_1e = b_1(bb_2) = (b_1b)b_2 = eb_2 = b_2,$$

deci $b_1 = b_2 \overset{\text{def.}}{=} b^{-1}$ şi atunci (7) şi (8) devin:

$$b^{-1}b = bb^{-1} = e,$$

ceea ce înseamnă că b este inversabil.

3. Fie $(G, \cdot)$ un cuplu format dintr-o mulțime nevidă și o operație multiplicativă. Să se arate că $(G, \cdot)$ este grup dacă și numai dacă sunt verificate axiomele:

I. Operația este asociativă.

II. Există $e \in G$ astfel încât $ex = x$, $\forall\, x \in G$ (există element neutru „la stânga").

III. Pentru orice $x \in G$, există $x' \in G$ cu $x'x = e$ (orice element este inversabil „la stânga").

Soluție. Desigur, dacă $(G, \cdot)$ este grup, axiomele I, II, III se verifică. Să presupunem acum că se verifică I, II, III și să dovedim că $(G, \cdot)$ este un grup. Trebuie să mai arătăm că există element neutru și că orice element este inversabil.

Mai întâi probăm că pentru fiecare $x \in G$ inversul său „la stânga" $x' \in G$, garantat de axioma III, este și invers „la dreapta" (față de același element neutru „la stânga" e). Fie x'' inversul la stânga al lui x', garantat de axioma III, deci $x''x' = e$. Atunci:

$$x' = ex' = (x'x)x' = x'(xx').$$

În egalitatea obținută $x' = x'(xx')$ înmulțim la stânga cu x'' și avem:

$$x''x' = (x''x')(xx') \Leftrightarrow e = e(xx') \Leftrightarrow e = xx',$$

adică x' este și invers „la dreapta" pentru x.

Mai rămâne să arătăm că e este și element neutru „la dreapta". Într-adevăr, pentru $x \in G$ oarecare, avem $xe = x(x'x) = (xx')x = ex = x$, deci $xe = x$, $\forall\, x \in G$. Așadar
$ex = xe = x$, $\forall\, x \in G$, ceea ce arată că e este elementul neutru al operației. Cum $x'x = xx' = e$, înseamnă că orice $x \in G$ este inversabil. Prin urmare $(G, \cdot)$ este un grup.

Comentariu metodic

Exercițiul rezolvat 2 arată o altă accepțiune a noțiunii de grup și anume aceea că grupul este o mulțime înzestrată cu o operație asociativă în care toate ecuațiile de gradul întâi au soluție. Exercițiul rezolvat 3 arată de asemenea o altă accepțiune a conceptului de grup, în care axiomele 2° și 3° pot fi „slăbite", în sensul că este suficient să fie verificate doar „la stânga"; bineînțeles, poate fi probat un rezultat analog, în care aceste axiome să fie verificate doar „la dreapta".

EXERCIȚII PROPUSE

1. Fie $a \in \mathbb{R}$ fixat. Pe mulțimea $\mathbb{R}$ definim operația $x * y = x + y + a$. Arătați că $(\mathbb{R}, *)$ este un grup abelian.

2. Pe mulțimea $\mathbb{R}$ definim operația $x * y = \sqrt[3]{x^3 + y^3}$. Arătați că $(\mathbb{R}, *)$ este un grup abelian.

3. Pe mulțimea $\mathbb{R}$ definim operația $x * y = x\sqrt{1+y^2} + y\sqrt{1+x^2}$. Arătați că $(\mathbb{R}, *)$ este un grup abelian.

4. Arătați că $x * y = xy - \sqrt{(x^2-1)(y^2-1)}$ este o operație pe mulțimea $G = (1, \infty)$, iar $(G, *)$ este un grup abelian.

5. Arătați că $x * y = \sqrt{1+(x^2-1)(y^2-1)}$ este o operație pe mulțimea $G = (1, \infty)$, iar $(G, *)$ este un grup abelian.

6. Fie $\mathbb{Z}[i] = \{a + bi \mid a,b \in \mathbb{Z}\}$ mulțimea întregilor lui Gauss ($i^2 = -1$). Să se arate că:

a) $(\mathbb{Z}[i], +)$ este un grup abelian;

b) $(\mathbb{Z}[i], \cdot)$ este un monoid comutativ;

c) Grupul elementelor inversabile din monoidul $(\mathbb{Z}[i], \cdot)$ este $U(\mathbb{Z}[i]) = U_4$.

7. Fie $M = \{u^2 + v^2 \mid u, v \in \mathbb{Z}[i]\}$. Arătați că M este un monoid comutativ, relativ la operația de înmulțire a numerelor complexe și determinați grupul elementelor inversabile din monoidul $(M, \cdot)$.

8. Fie $a,b,c \in \mathbb{Z}$, $b \neq 0$ și operația $*$ pe $\mathbb{Z}$ definită prin $x * y = axy + b(x+y) + c$. Demonstrați că:

1) $(\mathbb{Z}, *)$ este un monoid dacă și numai dacă $b^2 - b - ac = 0$ și b divide c.

2) În cazul $a = -1$, $b = 4$, $c = -12$, grupul elementelor simetrizabile din monoidul $(\mathbb{Z}, *)$ are 2 elemente.

9. Demonstrați că mulțimea $G = \{\cos \alpha\pi + i \sin \alpha\pi \mid \alpha \in \mathbb{Q}\}$ este un grup, relativ la înmulțirea numerelor complexe.

10. Pe mulțimea $M = (0, \infty)$ definim operația $x * y = x^{\ln y}$. Arătați că $(M, *)$ este un monoid comutativ și determinați grupul $(G, *)$ al elementelor simetrizabile din acest monoid.

11. Pe mulțimea $G = \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ definim operația $x * y = \operatorname{arctg}(\operatorname{tg} x + \operatorname{tg} y)$.

Arătați că $(G, *)$ este un grup abelian.

12. Pe mulțimea $G = (0, \pi)$ definim operația $x * y = \operatorname{arcctg}(\operatorname{ctg} x + \operatorname{ctg} y)$.
Arătați că $(G, *)$ este un grup abelian.

13. Arătaţi că $x * y = \arcsin\dfrac{\sin x + \sin y}{1 + \sin x \sin y}$ este o operaţie pe mulţimea $G = \left(-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right)$, iar $(G, *)$ este un grup abelian.

14. Arătaţi că $x * y = \arccos\dfrac{\cos x + \cos y}{1 + \cos x \cos y}$ este o operaţie pe mulţimea $G = (0, \pi)$, iar $(G, *)$ este un grup abelian.

15. Arătaţi că $x * y = \dfrac{xy}{2xy - x - y + 1}$ este operaţie algebrică pe mulţimea $G = (0, 1)$, iar $(G, *)$ este un grup abelian.

16. Fie $G = \left\{ \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \middle| \alpha \in \mathbb{R} \right\}$. Demonstraţi că $(G, \cdot)$ este grup abelian, unde „·" semnifică înmulţirea matricelor.

17. Fie $G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{Z} \right\}$. Demonstraţi că $(G, \cdot)$ este un grup abelian.

18. Fie $M = \left\{ \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \middle| a, b, c \in \mathbb{R}, a + b + c = 1 \right\}$. Demonstraţi că $(M, \cdot)$ este un monoid comutativ şi determinaţi grupul elementelor inversabile din acest monoid.

19. Arătaţi că mulţimea de matrice $G = \left\{ \begin{pmatrix} 1-x & 0 & x \\ 0 & 0 & 0 \\ x & 0 & 1-x \end{pmatrix} \middle| x \in \mathbb{R}, x \neq \dfrac{1}{2} \right\}$ este un grup, relativ la înmulţirea matricelor. Cum se explică făptul că, deşi sunt inversabile faţă de înmulţirea obişnuită în grupul G, matricele din G au determinantul nul?

20. Fie $M = \left\{ \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \middle| a, b, c \in \mathbb{R}, a + b + c = 0 \right\}$. Demonstraţi că $(M, \cdot)$ este un monoid comutativ şi determinaţi grupul $U(M)$ al elementelor inversabile din acest monoid. Explicaţi faptul că matricele din grupul $U(M)$ au determinantul nul, deşi sunt inversabile faţă de înmulţire.

21. Considerăm funcțiile $f_1, f_2, f_3, f_4 : \mathbb{R}^* \to \mathbb{R}^*$ unde $f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = -x$, $f_4(x) = -\frac{1}{x}$ și mulțimea $G = \{f_1, f_2, f_3, f_4\}$.
Arătați că mulțimea G este un grup abelian, relativ la operația de compunere a funcțiilor.

22. Pentru $n \in \mathbb{N}^*$ și $k \in \mathbb{Z}$ definim funcțiile $f_n, g_k : (0, \infty) \to (0, \infty)$, $f_n(x) = x^{\frac{1}{n}}$, $g_k(x) = x^k$.
a) Demonstrați că mulțimea $F = \{f_n \mid n \in \mathbb{N}^*\}$ este un monoid comutativ, relativ la compunerea funcțiilor și determinați grupul $U(F)$.
b) Demonstrați că mulțimea $G = \{g_k \mid k \in \mathbb{Z}\}$ este un monoid comutativ, relativ la compunerea funcțiilor și determinați grupul $U(G)$.

23. Pentru $a,b \in \mathbb{Z}$ definim funcția $f_{a,b} : \mathbb{R}^2 \to \mathbb{R}^2$ prin $f_{a,b}(x, y) = (ax, by)$. Arătați că mulțimea $M = \{f_{a,b} \mid a,b \in \mathbb{Z}\}$ este un monoid, relativ la compunerea funcțiilor și determinați grupul elementelor inversabile din acest inel.

24. Pentru $a \in \mathbb{R}^*$, $b \in \mathbb{R}$ definim funcțiile $f_{a,b} : \mathbb{C} \to \mathbb{C}$, $f_{a,b}(z) = az + b$ și $g_{a,b} : \mathbb{C} \to \mathbb{C}$, $g_{a,b}(z) = a\overline{z} + b$. Să se arate că mulțimea

$$G = \{f_{a,b} \mid a \in \mathbb{R}^*, b \in \mathbb{R}\} \cup \{g_{a,b} \mid a \in \mathbb{R}^*, b \in \mathbb{R}\}$$

este un grup, relativ la compunerea funcțiilor.

25. Pentru $a \in \mathbb{R}$, $b \in \mathbb{R}^*$ considerăm funcția $f_{a+bi} : \mathbb{C} \to \mathbb{C}$,

$$f_{a+bi}(x + yi) = x + (a + bi)y, \text{ pentru orice } x,y \in \mathbb{R}.$$

Demonstrați că mulțimea $G = \{f_{a+bi} \mid a \in \mathbb{R}, b \in \mathbb{R}^*\}$ este un grup, relativ la compunerea funcțiilor.

26. Pentru fiecare $a > 0$ definim funcția $f_a : \mathbb{R} \to \mathbb{R}$ prin $f_a(x) = \begin{cases} ax, & x > 0 \\ 0, & x \le 0 \end{cases}$.
Arătați că mulțimea $G = \{f_a \mid a > 0\}$ este un grup abelian, relativ la compunerea funcțiilor. Explicați faptul că, deși sunt inversabile față de compunere în grupul G, funcțiile din G nu sunt bijecții.

27. Considerăm unitatea imaginară $i \in \mathbb{C}$ și încă două „obiecte" matematice notate j, k între care introducem o „înmulțire" care „o prelungește" pe cea obișnuită din $\mathbb{C}$, în felul următor:

$$i^2 = j^2 = k^2 = -1;\ ij = -ji = k;\ jk = -kj = i;\ ki = -ik = j.$$

Arătaţi că mulţimea $\mathbb{C}_8 = \{1, i, j, k, -1, -i, -j, -k\}$ este un grup necomutativ faţă de înmulţire şi scrieţi tabla înmulţirii acestui grup. (Acest grup se numeşte ***grupul cuaternionilor de normă* 1**).

28. În planul raportat la reperul cartezian XOY considerăm următoarele transformări geometrice (funcţii definite pe mulţimea punctelor planului cu valori în ea însăşi): e = transformarea identică a planului; a = simetria faţă de axa OX; b = simetria faţă de axa OY; c = simetria faţă de originea O.
Să se arate că mulţimea $K = \{e, a, b, c\}$ este un grup abelian, relativ la compunerea funcţiilor (numit *grupul lui Klein*) şi să se întocmească tabla operaţiei.

29. Fie $ABCD$ un pătrat şi O centrul său de simetrie. Considerăm următoarele transformări geometrice ale planului pătratului: e = transformarea identică a planului;
a = rotaţia de centru O şi unghi orientat $\alpha = \frac{\pi}{2}$; b = simetria faţă de mediatoarea laturii AB. Notând multiplicativ compunerea transformărilor geometrice, arătaţi că:
a) $a^4 = e$ şi $b^2 = e$;
b) Mulţimea $G = \{e, a, a^2, a^3, b, ba, ba^2, ba^3\}$ este un grup necomutativ, relativ la compunere;
c) Funcţiile din grupul G transformă mulţimea $\{A, B, C, D\}$ în ea însăşi. (De aceea, acest grup se numeşte ***grupul izometriilor pătratului*** sau ***grupul diedral de ordin* 8**).

30. Fie $n \in \mathbb{N}$, $n \geq 2$ şi G_n mulţimea matricelor de ordin n cu proprietatea că pe fiecare linie şi pe fiecare coloană un element este egal cu 1 iar celelalte $n - 1$ elemente sunt egale cu 0. Demonstraţi că G_n este un grup, relativ la înmulţirea matricelor.

31. Fie $(G, *)$ un grup. Să se arate că există un monoid $(M, *)$ cu proprietăţile:
1) $(M, *)$ nu este grup;
2) $(G, *)$ este grupul elementelor simetrizabile din monoidul $(M, *)$.

Subgrupuri

Dacă privim grupul $(\mathbb{C}, +)$ şi grupurile $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$, constatăm că ultimele trei grupuri sunt incluse în primul, iar operaţia fiecăruia din aceste trei grupuri este indusă de adunarea din $(\mathbb{C}, +)$.

Suntem conduşi către următoarea:

Definiție

Fie $(G, *)$ un grup. O submulțime nevidă H a lui G care este parte stabilă față de operația $*$ și împreună cu operația indusă este un (nou) grup, se numește ***subgrup*** al grupului G.

Exemple

1. $(\mathbb{Z}, +)$ este subgrup al grupului $(\mathbb{Q}, +)$.

2. $(\mathbb{Q}, +)$ este subgrup al grupului $(\mathbb{R}, +)$.

3. $(\mathbb{R}, +)$ este subgrup al grupului $(\mathbb{C}, +)$.

4. $(\mathbb{Q}^*, \cdot)$ este subgrup al grupului $(\mathbb{R}^*, \cdot)$.

5. $(\mathbb{R}^*, \cdot)$ este subgrup al grupului $(\mathbb{C}^*, \cdot)$.

6. $(U_n, \cdot)$ este subgrup (finit) al grupului $(\mathbb{C}^*, \cdot)$.

7. Grupul altern $(A_n, \cdot)$ este un subgrup al grupului simetric $(S_n, \cdot)$.

8. Orice grup $(G, \cdot)$ de ordin cel puțin egal cu 2 are măcar două subgrupuri și anume $H_1 = \{e\}$, $H_2 = G$, numite ***subgrupuri improprii***; toate celelalte subgrupuri (dacă există) se numesc ***subgrupuri proprii***.

Următorul rezultat precizează condiții necesare și suficiente ca o submulțime a unui grup să fie subgrup. Înainte însă, vom stabili o lemă, care este interesantă și ca rezultat în sine.

Lemă

Fie $(G, \cdot)$ un grup și H un subgrup al său. Atunci:

1°. Elementul neutru al subgrupului H coincide cu elementul neutru al grupului G.

2°. Pentru orice element din H, inversul său în subgrupul H coincide cu inversul său în grupul G.

Demonstrație. 1°. Notăm cu e elementul neutru al grupului G și cu e' elementul neutru al grupului H. Gândind în G avem: $ee' = e'$ (1); gândind în H avem $e'e' = e'$ (2).

Din (1) și (2) rezultă $ee' = e'e'$ și dacă simplificăm la dreapta cu e' în grupul G obținem $e = e'$.

2°. Fie $x \in H$ arbitrar. Notăm cu x^{-1} inversul lui x în grupul G și cu x' inversul lui x în grupul H. Gândind în G avem $x^{-1}x = e$ (3); gândind în H avem $x'x = e$ (4).

Din (3) și (4) rezultă $x^{-1}x = x'x$ și simplificând la dreapta cu x în grupul G obținem $x^{-1} = x'$.

Teoremă

Fie $(G, \cdot)$ un grup și H o submulțime nevidă a lui G. Următoarele afirmații sunt echivalente:

1°. H este subgrup al grupului G.

2°. $\forall x,y \in H \Rightarrow xy^{-1} \in H$.

3°. $\forall x,y \in H \Rightarrow xy \in H$ şi $\forall x \in H \Rightarrow x^{-1} \in H$.

Demonstraţie. 1° $\Rightarrow$ 2°. Presupunem că H este subgrup al lui G, adică H este o parte stabilă faţă de operaţia grupului şi împreună cu operaţia indusă este un grup. Fie $x,y \in H$ arbitrar. Elementul $y \in H$ are un invers în subgrupul H. Conform lemei, acest invers al lui y în H coincide cu inversul y^{-1} al lui y în grupul G, deci $y^{-1} \in H$. Deoarece x, $y^{-1} \in H$ iar H este parte stabilă faţă de operaţia G, rezultă $x y^{-1} \in H$.

2° $\Rightarrow$ 3°. Luând un $x \in H$ avem $x, x^{-1} \in H \Rightarrow x x^{-1} \in H \Rightarrow e \in H$. Aceasta arată că submulţimea H conţine elementul neutru e din grupul G. Fie acum $x \in H$ arbitrar. Avem $e,x \in H \Rightarrow e x^{-1} \in H \Rightarrow x^{-1} \in H$. Aceasta înseamnă că submulţimea H conţine odată cu fiecare element şi inversul acestuia. În fine, dacă $x,y \in H$ sunt arbitrare, am văzut că $y^{-1} \in H$, deci x, $y^{-1} \in H \Rightarrow x\left(y^{-1}\right)^{-1} \in H \Rightarrow xy \in H$. Aşadar H conţine odată cu oricare două elemente şi produsul acestora.

3° $\Rightarrow$ 1°. Presupunem că $\forall x,y \in H \Rightarrow xy \in H$ şi $\forall x \in H \Rightarrow x^{-1} \in H$. Prima parte a acestei presupuneri arată că H este o parte a lui G, stabilă faţă de operaţia din G. Vom arăta că H cu operaţia indusă este un grup. Verificăm în acest sens axiomele grupului.

- Operaţia este asociativă pe H, întrucât este asociativă pe G.
- Alegând un $x \in H$, conform ipotezei în care lucrăm rezultă $x^{-1} \in H$ şi apoi $x x^{-1} \in H$, adică $e \in H$. Deoarece elementul neutru e din grupul G aparţine submulţimii H, rezultă că e rămâne element neutru şi pentru operaţia indusă pe H.
- Fie $x \in H$ arbitrar. Conform ipotezei în care lucrăm rezultă $x^{-1} \in H$, ceea ce înseamnă că x este inversabil în H.

Aşadar $(H, \cdot)$ este un grup, prin urmare este un subgrup al grupului $(G, \cdot)$.

Observaţie

Într-o notaţie aditivă condiţiile 2° şi 3° din teorema precedentă se transcriu astfel:

2°. $\forall x,y \in H \Rightarrow x - y \in H$;

3°. $\forall x,y \in H \Rightarrow x + y \in H$ şi $\forall x \in H \Rightarrow -x \in H$.

Exemple

1. Submulţimea $H = \{z \in \mathbb{C}^* \mid |z| = 1\}$ este un subgrup al grupului $(\mathbb{C}^*, \cdot)$. Într-adevăr se verifică 2° din teorema precedentă, căci putem scrie:

$$\forall x,y \in H \Rightarrow \left|xy^{-1}\right| = \left|\frac{x}{y}\right| = \frac{|x|}{|y|} = \frac{1}{1} = 1 \Rightarrow x y^{-1} \in H.$$

2. Fie $f : \mathbb{R} \to \mathbb{R}$ o funcţie periodică, adică pentru care există $T \in \mathbb{R}^*$ cu proprietatea $f(x + T) = f(x)$, $\forall x \in \mathbb{R}$ (un astfel de număr T se numeşte perioadă). Atunci mulţimea

$H = \{0\} \cup \{T \in \mathbb{R}^* \mid T = \text{perioadă}\}$ este un subgrup al grupului $(\mathbb{R}, +)$.

Pentru aceasta verificăm 3° din teorema precedentă, adică arătăm că $\forall\, T_1, T_2 \in H \Rightarrow T_1 + T_2 \in H$ şi $\forall\, T \in H \Rightarrow -T \in H$.

Desigur, e suficient să presupunem că $T_1, T_2, T \in \mathbb{R}^*$, adică T_1, T_2, T sunt perioade. Luând $x \in \mathbb{R}$ arbitrar, avem:

$$f(x + T_1 + T_2) = f((x + T_1) + T_2) = f(x + T_1) = f(x) \Rightarrow T_1 + T_2 \in H;$$
$$f(x - T) = f(x - T + T) = f(x) \Rightarrow -T \in H.$$

În cazul submulţimilor finite ale unui grup, teorema precedentă se simplifică şi arată în esenţă că *subgrupurile finite coincid cu părţile finite, stabile faţă de operaţia din grup*. Avem în acest sens următoarea:

Consecinţă

Fie $(G, \cdot)$ un grup şi H o submulţime *finită* a lui G. Următoarele afirmaţii sunt echivalente:

1°. H este subgrup al grupului G.

2°. H este parte stabilă faţă de operaţia din G.

Demonstraţie. 1° $\Rightarrow$ 2°. Evidentă.

2° $\Rightarrow$ 1°. Presupunem că H este parte stabilă faţă de operaţia din G, adică $\forall\, x, y \in H \Rightarrow xy \in H$. Conform condiţiei 3° din teorema precedentă, pentru a arăta că H este subgrup este suficient să mai arătăm că $\forall\, x \in H \Rightarrow x^{-1} \in H$.

Să zicem că $H = \{x_1, x_2, \ldots, x_n\}$ şi fie $x \in H$ fixat (deci $x = x_j$ pentru un anumit $j \in \{1, 2, \ldots, n\}$). Elementele $xx_1, xx_2, \ldots, xx_n$ sunt din H, căci H este parte stabilă. Ele sunt distincte două câte două (căci $xx_i = xx_k \Rightarrow x_i = x_k \Rightarrow i = k$). Atunci $H = \{xx_1, xx_2, \ldots, xx_n\}$, deci există $i \in \{1, 2, \ldots, n\}$ cu $xx_i = x$ de unde $x_i = e$ prin urmare $e \in H$. Atunci există $k \in \{1, 2, \ldots, n\}$ cu $xx_k = e$ de unde $x_k = x^{-1}$. Prin urmare $x^{-1} \in H$.

Exemplu

Subgrupurile finite ale grupului $(\mathbb{C}^*, \cdot)$ sunt grupurile de rădăcini ale unităţii U_n, unde $n \in \mathbb{N}^*$ şi numai acestea.

Într-adevăr, conform consecinţei precedente aceste subgrupuri coincid cu părţile finite ale lui $\mathbb{C}^*$, stabile faţă de înmulţire. Într-un exerciţiu rezolvat (pag. 6) am arătat că singurele părţi finite ale mulţimii $\mathbb{C}^*$, care sunt stabile faţă de înmulţire, sunt mulţimile U_n, unde $n \in \mathbb{N}^*$.

Comentariu metodic

Dacă $(G, \cdot)$ este un grup, iar H un subgrup al său, $H \neq G$ şi $x,y \in G$, ne punem problema căreia din mulţimile H şi $G \setminus H$ aparţin „produsele" xy şi yx în fiecare din cazurile:

a) $x \in H,\ y \in H$; b) $x \in H,\ y \in G \setminus H$; c) $x \in G \setminus H,\ y \in G \setminus H$.

În cazul a) este clar că $xy \in H$ şi $yx \in H$, deoarece subgrupul H este o parte stabilă faţă de operaţia grupului.

În cazul c) nu putem preciza nimic, după cum putem constata din exemplul grupului $(\mathbb{R}, +)$ cu subgrupul $(\mathbb{Q}, +)$: luând $x_1 = \sqrt{3} \in \mathbb{R} \setminus \mathbb{Q}$, $y_1 = \sqrt{3} \in \mathbb{R} \setminus \mathbb{Q} \Rightarrow x_1 + y_1 = 2\sqrt{3} \in \mathbb{R} \setminus \mathbb{Q}$, dar dacă luăm $x_2 = \sqrt{3} \in \mathbb{R} \setminus \mathbb{Q}$, $y_2 = -\sqrt{3} \in \mathbb{R} \setminus \mathbb{Q} \Rightarrow x_2 + y_2 = 0 \in \mathbb{Q}$.

În cazul b) răspunsul este precizat de rezultatul simplu de mai jos:

Dacă $x \in H$, $y \in G \setminus H$, atunci $xy \in G \setminus H$, $yx \in G \setminus H$.

Într-adevăr, să notăm $z = xy$ şi să presupunem prin absurd că $z \in H$. Rezultă $y = x^{-1}z$ şi cum $x,z \in H$ iar H este subgrup, deducem că $y \in H$, contradicţie. Analog se arată că $yx \in G \setminus H$.

Să dăm două exemple în acest sens. Luând grupul $(\mathbb{R}, +)$ şi subgrupul $(\mathbb{Q}, +)$, dacă $x \in \mathbb{Q}$, $y \in \mathbb{R} \setminus \mathbb{Q}$, rezultă $x+y \in \mathbb{R} \setminus \mathbb{Q}$, adică suma dintre un număr raţional şi un număr iraţional este un număr iraţional.

Luând grupul $(\mathbb{R}^*, \cdot)$ şi subgrupul $(\mathbb{Q}^*, \cdot)$, dacă $x \in \mathbb{Q}^*$, $y \in \mathbb{R}^* \setminus \mathbb{Q}^* = \mathbb{R} \setminus \mathbb{Q}$, atunci $xy \in \mathbb{R}^* \setminus \mathbb{Q}^* = \mathbb{R} \setminus \mathbb{Q}$, adică produsul dintre un număr raţional nenul şi un număr iraţional este un număr iraţional.

Grupuri finite, ordinul unui element, grupuri ciclice, aplicaţii

Dacă $(G, \cdot)$ este un grup finit, $G = \{x_1, x_2, \ldots, x_n\}$, operaţia din G poate fi redată sugestiv prin „tabla operaţiei". Aceasta arată astfel:

$\cdot$	x_1	x_2	$\ldots$	x_j	$\ldots$	x_n
x_1	x_1^2	$x_1 x_2$	$\ldots$	$x_1 x_i$	$\ldots$	$x_1 x_n$
x_2	$x_2 x_1$	x_2^2	$\ldots$	$x_2 x_j$	$\ldots$	$x_2 x_n$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
x_i	$x_i x_1$	$x_i x_2$	$\ldots$	$x_i x_j$	$\ldots$	$x_i x_n$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
x_n	$x_n x_1$	$x_n x_2$	$\ldots$	$x_n x_j$	$\ldots$	x_n^2

Deoarece pentru fiecare $x \in G$ elementele $x x_1, x x_2, \ldots, x x_n$ sunt distincte două câte două înseamnă că ele „epuizează" toate cele n elemente ale lui G. La fel, pentru $x \in G$ elementele $x_1 x, x_2 x, \ldots, x_n x$ sunt distincte două câte două, deci „epuizează" elementele din G. Rezultă că în tabla operației *pe fiecare linie și pe fiecare coloană apar toate elementele grupului și acestea sunt distincte două câte două.*

De exemplu, în grupul $U_4 = \{1, -1, i, -i\}$ tabla operației este redată mai jos și este instructiv să observăm că elementele grupului se reproduc pe fiecare linie și pe fiecare coloană:

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

Unul dintre cele mai frumoase și importante rezultate ce țin de grupurile finite este:

Teorema lui Lagrange

Ordinul oricărui subgrup al unui grup finit este un divizor al ordinului grupului.

Demonstrație. Fie $(G, \cdot)$ un grup finit de ordin n și $H = \{h_1, h_2, \ldots, h_k\}$ un subgrup al său de ordin k. Arătăm că numărul k divide n.

Pentru fiecare $x \in G$ considerăm submulțimea lui G definită astfel:

$$xH = \{x h_1, x h_2, \ldots, x h_k\} = \{xh \mid h \in H\}.$$

Submulțimile xH, $x \in G$, au următoarele proprietăți:

1°. Dacă $xH \neq yH$, atunci $xH \cap yH = \varnothing$.

2°. $\bigcup\limits_{x \in G} xH = G$.

Pentru a proba 1°, demonstrăm implicația echivalentă

$$xH \cap yH \neq \varnothing \Rightarrow xH = yH.$$

Într-adevăr, dacă $\exists\, z \in xH \cap yH$, atunci $z = xh_i = yh_j$, cu $1 \le i, j \le k$, deci $x = yh_j h_i^{-1}$. Luând un element arbitrar $t \in xH$, $t = xh_\ell$, cu $1 \le \ell \le k$ rezultă $t = y\left(h_j h_i^{-1} h_\ell\right) \in yH$, ceea ce arată incluziunea $xH \subseteq yH$; analog, se probează incluziunea $yH \subseteq xH$, deci avem egalitatea $xH = yH$.

Pentru a proba 2°, este clar mai întâi că $\bigcup\limits_{x \in G} xH \subseteq G$, întrucât toate mulțimile xH sunt incluse în G. Dar pentru orice $x \in G$ avem $x \in xH$ (căci $x = xe$ și $e \in H$), prin urmare avem și incluziunea $G \subseteq \bigcup\limits_{x \in G} xH$, adică, în fond, avem stabilită egalitatea 2°.

Deoarece G este mulțime finită, submulțimile xH, distincte două câte două, sunt în număr finit, fie acestea $x_1 H, x_2 H, \ldots, x_q H$. Din 1° rezultă că aceste mulțimi sunt chiar disjuncte două câte două, iar din 2° rezultă

$$G = x_1 H \cup x_2 H \cup \ldots \cup x_q H. \qquad (1)$$

Din definiția mulțimilor xH, vedem că fiecare mulțime xH are exact k elemente (ordinul subgrupului H). Trecând atunci la cardinale în egalitatea (1), rezultă:

$$n = \underbrace{k + k + \ldots + k}_{\text{de } q \text{ ori}} = kq \text{, deci } k \text{ divide } n.$$

Definiție

Fie $(G, \cdot)$ un grup și $x \in G$ un element fixat. Submulțimea lui G formată din toate puterile întregi ale lui x, adică:

$$< x > = \{x^k \mid k \in \mathbb{Z}\}$$

este evident un subgrup al lui G, numit ***subgrupul ciclic generat de elementul x***.

Dacă $(G, +)$ este un grup aditiv, atunci $< x > = \{kx \mid k \in \mathbb{Z}\}$.

Exemple

1. În grupul $(\mathbb{Q}^*, \cdot)$ subgrupul ciclic generat de -1 este $<-1> = \{(-1)^k \mid k \in \mathbb{Z}\} =$ $= \{-1, 1\} = U_2$.

2. În grupul $(\mathbb{C}^*, \cdot)$ subgrupul generat de i este $<i> = \{i^k \mid k \in \mathbb{Z}\} = \{1, -1, i, -i\} =$ $= U_4$.

3. În grupul $(\mathbb{R}, +)$ subgrupul ciclic generat de 1 este $<1> = \{k \cdot 1 \mid k \in \mathbb{Z}\} = \mathbb{Z}$.

4. În orice grup $(G, \cdot)$ subgrupul ciclic generat de elementul neutru este

$$< e > = \{e^k \mid k \in \mathbb{Z}\} = \{e\}.$$

Definiție

Fie $(G, \cdot)$ un grup și $x \in G$ un element fixat.

1°. Dacă există $n \in \mathbb{N}^*$ astfel încât $x^n = e$, cel mai mic $n \in \mathbb{N}^*$ cu această proprietate se numește ***ordinul elementului x în grupul G***.

2°. În caz contrar, adică dacă $x^n \neq e$ pentru orice $n \in \mathbb{N}^*$, spunem că x are ***ordinul*** ∞ în grupul G.

Exemple

Reluând exemplele precedente putem spune că:

1. În grupul $(\mathbb{Q}^*, \cdot)$ elementul -1 are ordinul 2.

2. În grupul $(\mathbb{C}^*, \cdot)$ elementul i are ordinul 4.

3. În grupul $(\mathbb{R}, +)$ elementul 1 are ordinul ∞.

4. În orice grup $(G, \cdot)$ elementul neutru e și numai acesta are ordinul 1.

Observație

În orice grup, ordinul unui element este egal cu ordinul inversului acestui element, lucru ce rezultă din echivalența:

$$x^k = e \Leftrightarrow x^{-k} = e.$$

Rezultatul următor arată că pentru un element de ordin finit, subgrupul ciclic generat de acest element este finit și are ordinul egal cu ordinul elementului. Avem următoarea:

Teoremă

Fie $(G, \cdot)$ un grup și $x \in G$ un element de ordin n. Atunci subgrupul ciclic generat de x are ordinul n și este dat de egalitatea:

$$< x > = \{e, x, x^2, \ldots, x^{n-1}\}.$$

Demonstrație. Incluziunea $\supseteq$ este clară, întrucât $< x > = \{x^k \mid k \in \mathbb{Z}\}$. Probăm acum incluziunea $\subseteq$.

Fie $x^k \in < x >$ un element arbitrar, unde $k \in \mathbb{Z}$. Conform teoremei împărțirii cu rest (k deîmpărțit, n împărțitor) avem $k = nq + r$ cu $q, r \in \mathbb{Z}$, $0 \leq r \leq n - 1$.

Atunci: $x^k = x^{nq+r} = (x^n)^q x^r = e^q x^r = ex^r = x^r \in \{e, x, x^2, \ldots, x^{n-1}\}$. În acest fel, egalitatea este demonstrată. Pentru a arăta că subgrupul ciclic $< x >$ are ordinul n, trebuie să arătăm că elementele $e, x, x^2, \ldots, x^{n-1}$ sunt distincte două câte două. Într-adevăr, dacă, prin absurd am avea $x^i = x^j$ cu $0 \leq i < j \leq n - 1$, ar rezulta $x^{j-i} = e$, ceea ce ar contrazice minimalitatea lui n din definiția ordinului unui element.

Consecința 1

Într-un grup finit, ordinul oricărui element este finit și este un divizor al ordinului grupului.

Demonstrație. Fie $(G, \cdot)$ un grup finit de ordin n și $x \in G$. Elementul x nu poate avea ordinul ∞, căci ar genera un subgrup ciclic infinit, absurd. Așadar x are un ordin finit k. Dar atunci subgrupul ciclic $< x >$ are ordinul k și conform teoremei lui Lagrange avem $k \mid n$.

Consecința 2

Într-un grup $(G, \cdot)$ de ordin n, avem: $x^n = e$, $\forall x \in G$.

Demonstrație. Fie $x \in G$ fixat. Cum G este finit, elementul x are un ordin finit k. Din consecința 1 avem $n = kq$ cu $q \in \mathbb{N}^*$ și atunci $x^n = (x^k)^q = e^q = e$.

Definiție

Un grup $(G, \cdot)$ se numește ***ciclic*** dacă există $x \in G$ astfel încât: $G = < x > =$ $= \{x^k \mid k \in \mathbb{Z}\}$ adică, mai sugestiv, dacă este generat de un anumit element al său.

Exemple

1. Pentru fiecare $n \in \mathbb{N}^*$, grupul $(U_n, \cdot)$ al rădăcinilor de ordin n ale unității este ciclic, întrucât:

$$U_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\} = \{\zeta^k \mid k \in \mathbb{Z}\} = < \zeta >, \text{ unde } \zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

2. Pentru fiecare $n \in \mathbb{N}$, $n \geq 2$, grupul claselor de resturi modulo n, adică $(\mathbb{Z}_n, +)$, este un grup ciclic, întrucât:

$$\mathbb{Z}_n = \{\hat{0}, \hat{1}, \hat{2}, \ldots, \widehat{n-1}\} = \{k \cdot \hat{1} \mid k \in \mathbb{Z}\} = < \hat{1} >.$$

3. Grupul $(\mathbb{Z}, +)$ este ciclic întrucât $\mathbb{Z} = \{k \cdot 1 \mid k \in \mathbb{Z}\} = < 1 >$.

Observație

Orice grup ciclic este abelian, întrucât puterile întregi ale aceluiași element comută între ele. Reciproc nu este adevărat: de exemplu, grupul $(\mathbb{Q}, +)$ este abelian, dar nu este ciclic.

Un exemplu de grup ciclic este dat de următoarea:

Propoziție

Orice grup de ordin număr prim este ciclic.

Demonstrație. Fie $(G, \cdot)$ un grup de ordin p, unde p este un număr prim. Cum $p \geq 2$ putem fixa un $x \in G$, $x \neq e$. Subgrupul ciclic $< x >$ are ordinul $k \geq 2$, căci conține pe e și x.

Conform teoremei lui Lagrange k divide p și cum p este prim iar $k > 1$, rezultă $k = p$. Dar atunci $< x > = G$, ceea ce arată că G este un grup ciclic.

Aplicații în teoria numerelor (extindere)

Dăm acum trei aplicații în teoria elementară a numerelor.

Teorema lui Euler

Fie $n \in \mathbb{N}$, $n \geq 2$ și $a \in \mathbb{Z}$, $(a, n) = 1$. Atunci $a^{\varphi(n)} - 1$ se divide cu n, unde φ este indicatorul lui Euler.

Demonstrație. Considerăm grupul multiplicativ $U(\mathbb{Z}_n)$ al elementelor inversabile din monoidul $(\mathbb{Z}_n, \cdot)$. Am văzut că acest grup are ordinul $\varphi(n)$ și este format din toate clasele $\hat{k}$ pentru care $(k, n) = 1$. Deoarece $(a, n) = 1$, înseamnă că $\hat{a} \in U(\mathbb{Z}_n)$. Conform consecinței 2 de la pag. 34 rezultă $\hat{a}^{\varphi(n)} = \hat{1}$, adică $\widehat{a^{\varphi(n)}} = \hat{1}$, ceea ce este echivalent cu $a^{\varphi(n)} - 1 = kn$, $k \in \mathbb{N}^*$.

Teorema lui Fermat („mica" teoremă a lui Fermat)

Fie $p > 0$ un număr prim și $a \in \mathbb{Z}$, a nedivizibil cu p. Atunci: $a^{p-1} - 1$ se divide cu p.

Demonstrație. Pentru p prim, afirmația a nu se divide cu p este echivalentă cu $(a, p) = 1$. De asemenea pentru p prim avem $\varphi(p) = p - 1$, căci toate numerele $1, 2, 3, \ldots, p - 1$ sunt relativ prime cu p. Conform teoremei lui Euler avem $a^{\varphi(p)} - 1 = kp$, $k \in \mathbb{N}^*$ adică $a^{p-1} - 1 = kp$.

Remarcăm că teorema lui Fermat este cazul particular din teorema lui Euler când $n = p$ = număr prim.

Înainte de a da un ultim rezultat de teoria numerelor, avem nevoie de o lemă.

Lemă

Într-un grup abelian finit $(G, \cdot)$ produsul tuturor elementelor grupului este egal cu produsul elementelor de ordin cel mult 2.

Demonstrație. Grupul fiind abelian, nu contează ordinea factorilor în produs, iar produsul elementelor grupului va fi egal cu produsul elementelor de ordin ≤ 2 înmulțit cu produsul elementelor de ordin ≥ 3 (dacă există elemente de ordin ≥ 3). Pentru a proba afirmația din enunț este suficient să arătăm că produsul elementelor de ordin ≥ 3 este egal cu elementul–unitate e.

Conform observației de la pag. 34 dacă $x \in G$ are ordinul ≥ 3, atunci x^{-1} are același ordin cu x, deci x^{-1} are tot un ordin ≥ 3. Mai mult, $x^{-1} \neq x$ (căci $x^{-1} = x \Rightarrow x^2 = e$, contrar faptului că x are ordin ≥ 3). Înseamnă că elementele de ordin ≥ 3 se pot grupa în submulțimi de tipul $\{x, x^{-1}\}$, fiecare submulțime având efectiv două elemente. Deoarece produsul elementelor dintr-o astfel de submulțime este egal cu e, rezultă că produsul elementelor de ordin ≥ 3 este egal cu e.

Teorema lui Wilson

Fie $p \in \mathbb{N}$, $p \geq 2$. Avem echivalența:

$$p \text{ este număr prim} \Leftrightarrow (p - 1)! + 1 \text{ se divide cu } p.$$

Demonstrație. ($\Rightarrow$). Presupunem că p este număr prim. Considerăm grupul $U(\mathbb{Z}_p)$ al elementelor inversabile din monoidul $(\mathbb{Z}_p, \cdot)$. Cum p este prim avem $(k, p) = 1$, $\forall\, k \in$ $\in \{1, 2, \ldots, p-1\}$, deci $U(\mathbb{Z}_p) = \mathbb{Z}_p^* = \{\hat{1}, \hat{2}, \ldots, \widehat{p-1}\}$. Conform lemei, produsul elementelor acestui grup abelian este egal cu produsul elementelor de ordin ≤ 2. Să găsim așadar elementele de ordin ≤ 2. Dacă $\hat{a} \in \mathbb{Z}_p^*$ este un astfel de element, avem $\hat{a}^2 = \hat{1}$, deci $(a^2 - 1) \,\vdots\, p$ sau $(a-1)(a+1) \,\vdots\, p$. Deoarece p este un număr prim înseamnă că $(a-1) \,\vdots\, p$ sau $(a+1) \,\vdots\, p$. Așadar $\hat{a} = \hat{1}$ sau $\hat{a} = -\hat{1}$. Produsul acestor elemente este $\hat{1} \cdot (-\hat{1}) = -\hat{1}$. Conform lemei avem așadar $\hat{1} \cdot \hat{2} \cdot \hat{3} \cdot \ldots \cdot \widehat{p-1} = -\hat{1}$, adică $\widehat{(p-1)!} = -\hat{1}$, ceea ce se mai scrie echivalent $(p-1)! + 1 = kp$, cu $k \in \mathbb{N}^*$.

($\Leftarrow$). Presupunem că $(p-1)! + 1$ se divide cu p și să admitem, prin absurd, că p nu este număr prim. Atunci există $k \in \{2, 3, \ldots, p-1\}$ cu $k \mid p$. Deoarece $(p-1)! + 1$ se divide cu p, cu atât mai mult $(p-1)! + 1$ se divide cu k. Dar $(p-1)!$ se divide cu k și atunci rezultă că 1 se divide cu k, contradicție. Contradicția obținută arată că presupunerea prin absurd este falsă, deci p este un număr prim.

Comentariu metodic

Teorema lui Wilson este o caracterizare a numerelor prime (un criteriu de „primalitate"), din nefericire însă aproape inutilizabilă, întrucât factorialele sunt numere foarte mari.

Exerciții rezolvate

1. Să se arate că subgrupurile grupului $(U_n, \cdot)$, cu $n \in \mathbb{N}^*$, sunt grupurile $(U_d, \cdot)$, unde d parcurge divizorii naturali ai lui n.

Soluție. Mai întâi observăm că dacă $d \in \mathbb{N}^*$, $d \mid n$, atunci U_d este subgrup al lui U_n. Într-adevăr, scriind $n = dq$, cu $q \in \mathbb{N}^*$, avem:

$$\forall\, x \in U_d \Rightarrow x^d = 1 \Rightarrow (x^d)^q = 1 \Rightarrow x^n = 1 \Rightarrow x \in U_n.$$

Așadar $U_d \subseteq U_n$ și cum $(U_d, \cdot)$ este un grup, înseamnă că U_d este subgrup al lui U_n. Reciproc, fie H un subgrup al grupului U_n. Deoarece $(U_n, \cdot)$ este un subgrup finit al grupului $(\mathbb{C}^*, \cdot)$, înseamnă că și $(H, \cdot)$ este un subgrup finit al grupului $(\mathbb{C}^*, \cdot)$. Dar am văzut că singurele subgrupuri finite ale lui $(\mathbb{C}^*, \cdot)$ sunt grupurile de rădăcini ale unității. Așadar există $d \in \mathbb{N}^*$ astfel încât $H = U_d$. Conform teoremei lui Lagrange $d \mid n$.

2. Să se arate că subgrupurile grupului $(\mathbb{Z}, +)$ sunt cele de forma $(n\mathbb{Z}, +)$, unde $n \in \mathbb{N}$.

Soluție. Reamintim că $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$.

Mai întâi e clar că orice submulțime de forma $n\mathbb{Z}$, $n \in \mathbb{N}$, este un subgrup al lui $(\mathbb{Z}, +)$, deoarece: $\forall\, x,y \in n\mathbb{Z} \Rightarrow x = nk_1,\ y = nk_2\ (k_1,k_2 \in \mathbb{Z}) \Rightarrow x - y = n(k_1 - k_2) \in n\mathbb{Z}$.

Reciproc, fie H un subgrup al lui $(\mathbb{Z}, +)$. Arătăm că $\exists\, n \in \mathbb{N}$ astfel încât $H = n\mathbb{Z}$.

Dacă $H = \{0\}$ luăm $n = 0$ și avem $H = 0 \cdot \mathbb{Z}$.

Să considerăm acum cazul când $H \neq \{0\}$. În acest caz H conține cel puțin un întreg nenul și fiind subgrup, va conține opusul acestui întreg. Dar dintre două numere întregi nenule opuse, unul este natural nenul. Prin urmare H conține cel puțin un număr natural nenul. Notăm cu n cel mai mic număr nenul care aparține lui H și arătăm egalitatea $H = n\mathbb{Z}$.

Deoarece $n \in H$, rezultă că toți multiplii întregi ai lui n sunt în H (căci H este un grup față de adunare), adică $n\mathbb{Z} \subseteq H$.

Să arătăm și incluziunea reciprocă $H \subseteq n\mathbb{Z}$. Fie $x \in H$ oarecare. Fiind vorba de numere întregi, putem aplica teorema împărțirii cu rest (x deîmpărțit, n împărțitor) și avem $x = nq + r$ cu $q,r \in \mathbb{Z}$, $0 \leq r < n$.

Cum $x \in H$, $nq \in n\mathbb{Z} \subseteq H$ iar $(H, +)$ este subgrup, rezultă că $r = x - nq \in H$. Numărul r este natural, aparține lui H și este mai mic decât n. Datorită minimalității lui n printre numerele naturale nenule din H, rezultă în mod necesar $r = 0$ și de aici $x = nq \in n\mathbb{Z}$. Deoarece $x \in H$ a fost arbitrar, rezultă $H \subseteq n\mathbb{Z}$, deci $H = n\mathbb{Z}$.

3. Fie $(G, \cdot)$ un grup finit cu proprietatea $x^2 = e$, pentru orice $x \in G$. Să se arate că ordinul grupului este de forma 2^k, cu $k \in \mathbb{N}$.

Soluție. Am văzut în teorema de la pag. 20 că un astfel de grup este abelian. Dacă $G = \{e\}$, atunci $|G| = 2^0$. Să presupunem că $G \neq \{e\}$, deci $\exists\, x_0 \in G$, $x_0 \neq e$. Deoarece $x_0^2 = e$, submulțimea $H_0 = \{e, x_0\}$ este un subgrup de ordin 2 al lui G. Așadar G conține subgrupuri de ordin 2^n, cu $n \in \mathbb{N}^*$. Fie $k \in \mathbb{N}^*$ cel mai mare număr natural cu proprietatea că există în G un subgrup H de ordin 2^k (există un asemenea k maxim, fiindcă G este finit). Arătăm că $G = H$ și vom avea $|G| = |H| = 2^k$. Presupunem prin absurd că $\exists\, x \in G \setminus H$. Cum $x^2 = e$, rezultă ușor că mulțimea finită $H' = H \cup xH$ este o parte stabilă față de operația din G, deci este un subgrup al lui G. Dar $H \cap xH = \varnothing$, $|H| = |xH| = 2^k$ și atunci $|H'| = 2^k + 2^k = 2^{k+1}$, ceea ce contrazice maximalitatea lui k.

4. Fie $(G, \cdot)$ un grup. Să se arate că:

a) Dacă elementul $x \in G$ are ordinul n, atunci pentru $k \in \mathbb{Z}$ avem echivalența:

$$x^k = e \Leftrightarrow n \mid k.$$

b) Dacă elementele $x, y \in G$ au respectiv ordinele n, m cu $(n, m) = 1$ şi aceste două elemente comută ($xy = yx$), atunci elementul xy are ordinul mn.

Soluţie. a) ($\Rightarrow$). Presupunem $x^k = e$. Conform teoremei împărţirii cu rest (k deîmpărţit, n împărţitor) avem $k = nq + r$ cu $q, r \in \mathbb{Z}$, $0 \le r \le n - 1$.

Ipoteza $x^k = e$ se scrie succesiv $x^{nq+r} = e \Leftrightarrow (x^n)^q \cdot x^r = e \Leftrightarrow x^r = e$. Datorită minimalităţii lui n din definiţia ordinului unui element, rezultă în mod necesar $r = 0$ şi atunci $k = nq$, deci $n \mid k$.

($\Leftarrow$). Presupunem că $n \mid k$, deci $k = nq$ cu $q \in \mathbb{Z}$. Atunci:

$$x^k = x^{nq} = (x^n)^q = e^q = e.$$

b) Notăm cu q ordinul elementului xy. Avem $(xy)^{mn} = (x^n)^m (y^m)^n = e$ şi conform cu a) rezultă $q \mid mn$ (am ţinut seama că dacă x şi y comută, atunci oricare două puteri întregi ale lui x şi y comută – ceea ce se arată astfel: $xy = yx \Leftrightarrow x^{-1}y = yx^{-1} \Leftrightarrow$ $\Leftrightarrow xy^{-1} = y^{-1}x \Leftrightarrow x^{-1}y^{-1} = y^{-1}x^{-1}$ şi atunci este suficient să arătăm că oricare două puteri naturale ale lui x şi y comută, adică $x^r y^s = y^s x^r$, $\forall\, r, s \in \mathbb{N}$, ceea ce se face fixând r şi făcând inducţie după s).

Pe de altă parte $e = (xy)^{qm} = x^{qm} y^{qm} = x^{qm}$ şi conform cu a) rezultă $n \mid qm$; cum $(n, m) = 1$, trebuie ca $n \mid q$. Analog $e = (xy)^{qn} = x^{qn} y^{qn} = y^{qn}$ şi conform cu a) vom avea $m \mid qn$, de unde $m \mid q$. Din $n \mid q$, $m \mid q$ şi $(n, m) = 1$ rezultă $mn \mid q$ şi cum $q \mid mn$ rezultă $q = mn$.

5. Fie $p > 1$ un număr întreg şi $a \in \mathbb{Z}$ cu proprietăţile:

1°. $a^{p-1} - 1$ se divide cu p.

2°. $a^d - 1$ nu se divide cu p, pentru orice divizor d al lui $p - 1$, $d < p - 1$.

Atunci p este un număr prim. (O reciprocă a micii teoreme a lui Fermat).

Soluţie. Din 1° rezultă că $(a, p) = 1$. Considerăm grupul $(U(\mathbb{Z}_p), \cdot)$ al elementelor inversabile din monoidul $(\mathbb{Z}_p, \cdot)$. Cum $(a, p) = 1$, înseamnă că $\hat{a} \in U(\mathbb{Z}_p)$ şi fie n ordinul lui $\hat{a}$ în grupul $U(\mathbb{Z}_p)$. Deoarece grupul $U(\mathbb{Z}_p)$ are ordinul $\varphi(p)$, iar ordinul unui element divide ordinul grupului, rezultă că $n \mid \varphi(p)$ (1).

Din 1° avem $\hat{a}^{p-1} = \hat{1}$ şi folosind punctul a) din exerciţiul precedent deducem că $n \mid (p - 1)$ (2). Din 2° avem $\hat{a}^d \neq \hat{1}$ dacă $d \mid (p - 1)$, $d < p - 1$ şi atunci (2) obligă la egalitatea $n = p - 1$. Atunci (1) devine $(p - 1) \mid \varphi(p)$, de unde $\varphi(p) \ge p - 1$. Dacă p nu ar fi prim, am avea $\varphi(p) < p - 1$ (căci printre numerele 1, 2, 3, …, $p - 1$ există unele care au divizori comuni cu p), ceea ce ar duce la o contradicţie.

Aşadar p este număr prim şi soluţia se încheie.

EXERCIȚII PROPUSE

1. Fie $(G, \cdot)$ un grup cu proprietatea că există $m,n \in \mathbb{Z}$, $(m, n) = 1$ astfel încât $(xy)^m = (yx)^m$ și $(xy)^n = (yx)^n$ pentru orice $x,y \in G$. Arătați că grupul G este abelian.

2. Fie $(G, \cdot)$ un grup cu proprietatea că există $a \in G$ astfel încât $x^3 = xax$ pentru orice $x \in G$. Arătați că grupul G este abelian.

3. Fie $(G, \cdot)$ un grup cu proprietatea că există $a \in G$ astfel încât $ax^3a = x$ pentru orice $x \in G$. Arătați că grupul G este abelian.

4. Fie $(G, \cdot)$ un grup și $x,y \in G$ astfel încât $x^2 = e$ și $xyx = y^3$, unde e este elementul neutru al grupului. Demonstrați că $y^8 = e$.

5. Fie $n \in \mathbb{N}^*$, $GL_n(\mathbb{C}) = \{X \in \mathcal{M}_n(\mathbb{C}) \mid \det X \neq 0\}$ și $SL_n(\mathbb{C}) = \{X \in \mathcal{M}_n(\mathbb{C}) \mid \det X = 1\}$. Arătați că $SL_n(\mathbb{C})$ este un subgrup al grupului multiplicativ $(GL_n(\mathbb{C}), \cdot)$.

6. Fie $n,m \in \mathbb{N}^*$ și să notăm $n\mathbb{Z} + m\mathbb{Z} = \{na + mb \mid a,b \in \mathbb{Z}\}$. Demonstrați că:

   1) $n\mathbb{Z} + m\mathbb{Z}$ este un subgrup al grupului aditiv $(\mathbb{Z}, +)$.

   2) $n\mathbb{Z} + m\mathbb{Z} = (n, m)\mathbb{Z}$, unde (n, m) este c.m.m.d.c. al numerelor n și m.

7. Determinați subgrupurile grupului lui Klein.

8. Determinați subgrupurile grupului simetric $(S_3, \cdot)$.

9. Arătați că $H = \{\cos \alpha\pi + i \sin \alpha\pi \mid \alpha \in \mathbb{Q}\}$ este un subgrup al grupului $(\mathbb{C}^*, \cdot)$.

10. Fie G un grup cu proprietatea că există $a \in G$ astfel încât $H = G \setminus \{a\}$ este un subgrup al lui G. Arătați că grupul G are ordinul 2.

11. Fie G un grup cu proprietatea că există $a,b \in G$, $a \neq b$, astfel încât $H = G \setminus \{a, b\}$ este un subgrup al lui G. Arătați că grupul G are ordinul 3 sau 4.

12. Arătați că un grup G de ordin cel puțin egal cu 2 nu poate fi scris ca reuniunea a două subgrupuri proprii ale sale.

13. Dacă $H_1, H_2, \ldots, H_n$ sunt subgrupuri ale unui grup G, arătați că
$$H = H_1 \cap H_2 \cap \ldots \cap H_n \text{ este de asemenea un subgrup al lui } G.$$

14. Considerăm subgrupurile $n\mathbb{Z}$ şi $m\mathbb{Z}$ $(n,m \in \mathbb{N}^*)$ ale grupului $(\mathbb{Z}, +)$. Arătaţi că $n\mathbb{Z} \cap m\mathbb{Z} = [n, m]\mathbb{Z}$, unde $[n, m]$ este c.m.m.m.c. al numerelor n şi m.

15. Considerăm subgrupurile U_n şi U_m $(n,m \in \mathbb{N}^*)$ ale grupului $(\mathbb{C}^*, \cdot)$. Arătaţi că $U_n \cap U_m = U_{(n, m)}$, unde (n, m) este c.m.m.d.c. al numerelor n şi m.

16. Fie $(G, \cdot)$ un grup. Arătaţi că:
a) Mulţimea $Z(G) = \{x \in G \mid xy = yx, \forall\, y \in G\}$ este un subgrup comutativ al grupului G. (Acest subgrup se numeşte ***centrul*** grupului G).
b) Grupul G este abelian dacă şi numai dacă $Z(G) = G$.

17. Determinaţi centrul grupului $\mathbb{C}_8$ din exerciţiul 27 pag. 26.

18. Arătaţi că pentru $n \geq 3$ centrul grupului simetric $(S_n, \cdot)$ este $Z(S_n) = \{e\}$.

19. Arătaţi că dacă într-un grup finit mai mult de jumătate din elementele grupului comută cu toate elementele, atunci acesta este abelian.

20. Arătaţi că orice subgrup al unui grup ciclic este ciclic.

21. Determinaţi subgrupurile grupului $(\mathbb{Z}_4, +)$.

22. Determinaţi subgrupurile grupului $(\mathbb{Z}_5, +)$.

23. Determinaţi subgrupurile grupului $(\mathbb{Z}_6, +)$.

24. Fie $p \geq 2$ un număr natural. Să se demonstreze că p este număr prim dacă şi numai dacă orice grup de ordin p are exact două subgrupuri.

25. Fie $(G, \cdot)$ un grup abelian şi H un subgrup al său. Notăm:

$$G_H = \{x \in G \mid \exists\, n \in \mathbb{N}^* \text{ cu } x^n \in H\}.$$

a) Arătaţi că G_H este un subgrup al lui G, iar H este un subgrup al lui G_H.
b) Dacă $G = (\mathbb{C}^*, \cdot)$ şi $H = U_k$, $k \in \mathbb{N}^*$, determinaţi subgrupul G_H.

26. Arătaţi că într-un grup G următoarele două afirmaţii sunt echivalente:
1°. Orice parte stabilă faţă de operaţia grupului este subgrup al lui G.
2°. Orice element din G are ordin finit.

27. Fie $(G, \cdot)$ un grup de ordin $n \geq 4$, astfel încât există $k \in \mathbb{N}$, $2 \leq k \leq n - 1$, cu proprietatea că toate submulţimile lui G cu k elemente, care conţin elementul neutru e, sunt subgrupuri ale lui G. Demonstraţi că:
a) $k = 2$; b) $x^2 = e$, $\forall\, x \in G$.

Morfisme şi izomorfisme de grupuri

Până aici ne-am referit mereu la un grup fixat. Acum vom încerca să corelăm între ele grupuri diferite.

Definiţie

1°. Fie $(G, *)$ şi $(G', \circ)$ două grupuri. O funcţie $f : G \to G'$ cu proprietatea $f(x * y) = f(x) \circ f(y)$, $\forall\, x,y \in G$, se numeşte ***morfism de grupuri***.

2°. Un morfism de grupuri de la un grup la el însuşi se numeşte ***endomorfism*** al acelui grup.

Exemple

1. Funcţia $f : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$, $f(x) = e^x$ este un morfism de grupuri, întrucât:

$$f(x + y) = e^{x+y} = e^x e^y = f(x)f(y),\ \forall\, x,y \in \mathbb{R}.$$

2. Funcţia $\varepsilon : (S_n, \cdot) \to (U_2, \cdot)$, $\varepsilon(\sigma) = \begin{cases} 1, & \text{dacă } \sigma \text{ este permutate pară} \\ -1, & \text{dacă } \sigma \text{ este permutare impară} \end{cases}$ este un morfism de grupuri, întrucât avem:

$$\varepsilon(\sigma_1\sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2),\ \forall\, \sigma_1, \sigma_2 \in S_n.$$

3. Funcţia $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$, $f(x) = nx$, cu $n \in \mathbb{Z}$ fixat, este un endomorfism al grupului $\mathbb{Z}$. Într-adevăr:

$$f(x + y) = n(x + y) = nx + ny = f(x) + f(y),\ \forall\, x,y \in \mathbb{Z}.$$

4. Funcţia $f : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$, $f(x) = \hat{x}$ este un morfism de grupuri, întrucât

$$f(x + y) = \widehat{x+y} = \hat{x} + \hat{y} = f(x) + f(y),\ \forall\, x,y \in \mathbb{Z}.$$

5. Pentru $(G, *)$, $(G', \circ)$ grupuri oarecare având elementele neutre e, respectiv e', funcţia $f : G \to G'$, $f(x) = e'$, $\forall\, x \in G$, este un morfism de grupuri, numit ***morfismul constant***. Într-adevăr: $f(x * y) = e' = e' \circ e' = f(x) \circ f(y)$, $\forall\, x,y \in G$.

Din motive pe care le-am mai menţionat şi care ţin de uşurinţa scrierii, revenim la notaţia multiplicativă în toate grupurile cu care lucrăm, atunci când expunem partea teoretică.

Un prim rezultat privind morfismele de grupuri este următoarea:

Propoziţie

Compunerea a două morfisme de grupuri este un morfism de grupuri.

Demonstrație. Să considerăm morfismele de grupuri: $(G, \cdot) \xrightarrow{g} (G', \cdot) \xrightarrow{f} (G'', \cdot)$ și fie u funcția compusă, adică $u = f \circ g$. Arătăm că u este de asemenea un morfism de grupuri. Într-adevăr:

$$u(xy) = (f\circ g)(xy) = f(g(xy)) = f(g(x)g(y)) = f(g(x))f(g(y)) =$$
$$= (f\circ g)(x)(f\circ g)(y) = u(x)u(y), \ \forall\, x,y \in G.$$

Următorul rezultat stabilește proprietățile unui morfism de grupuri.

Teoremă

Fie $f : (G, \cdot) \to (G', \cdot)$ un morfism de grupuri. Notând cu e, e' respectiv elementele neutre din grupurile G, G', avem:

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. 1°. Avem $f(e) = f(e \cdot e) = f(e)f(e)$ și simplificând în grupul $(G', \cdot)$ prin $f(e)$ se obține $e' = f(e)$.

2°. Putem scrie $e' = f(e) = f(x x^{-1}) = f(x)f(x^{-1})$ și înmulțind la stânga cu $(f(x))^{-1}$ în grupul $(G', \cdot)$, se obține $(f(x))^{-1} = f(x^{-1})$.

3°. Dacă $n = 0$ egalitatea devine $f(e) = e'$, adică punctul 1°.

Dacă $n \in \mathbb{N}^*$ avem $f(x^n) = f(\underbrace{xx\ldots x}_{n \text{ ori}}) = \underbrace{f(x)f(x)\ldots f(x)}_{n \text{ ori}} = (f(x))^n$.

Dacă $n < 0$, atunci $n = -n'$ cu $n' \in \mathbb{N}^*$ și avem:

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

Comentariu metodic

Transcrierea în notație aditivă a teoremei precedente este utilă și se face astfel:

1°. $f(0) = 0'$.

2°. $f(-x) = -f(x)$, $\forall\, x \in G$.

3°. $f(nx) = nf(x)$, $\forall\, x \in G$, $\forall\, n \in \mathbb{Z}$.

Definiție

Dacă $f : (G, \cdot) \to (G', \cdot)$ este un morfism de grupuri, submulțimea lui G definită prin:

$$\text{Ker}\, f = \{x \in G \mid f(x) = e'\}$$

se numește ***nucleul*** morfismului f.

Teoremă

Fie $(G, \cdot) \to (G', \cdot)$ un morfism de grupuri. Atunci:

1°. Ker f este un subgrup al grupului $(G, \cdot)$.

2°. Morfismul f este injectiv dacă şi numai dacă Ker $f = \{e\}$.

3°. Pentru orice subgrup $H \subseteq G$, mulţimea $f(H) = \{f(x) \mid x \in H\}$ este un subgrup al lui $(G', \cdot)$; în particular, mulţimea $Im\ f = f(G)$ este un subgrup al lui $(G', \cdot)$.

Demonstraţie. 1°. Arătăm că nucleul Ker f este un subgrup al lui G, adică $\forall\ x,y \in$ Ker f $\Rightarrow x y^{-1} \in$ Ker f. Într-adevăr $x,y \in$ Ker $f \Rightarrow f(x) = f(y) = e' \Rightarrow f(x y^{-1}) = f(x)f(y^{-1}) =$ $= e'(e')^{-1} = e' \Rightarrow x y^{-1} \in$ Ker f.

2°. Dovedim echivalenţa: f injectiv $\Leftrightarrow$ Ker $f = \{e\}$.

$(\Rightarrow)$. Presupunem că morfismul f este injectiv. Fie $x \in$ Ker f un element arbitrar. Atunci $f(x) = e' = f(e)$ şi cum f este funcţie injectivă, rezultă $x = e$. Prin urmare Ker $f \subseteq \{e\}$ şi cum incluziunea reciprocă este evidentă, rezultă egalitatea Ker $f = \{e\}$.

$(\Leftarrow)$. Presupunem Ker $f = \{e\}$. Pentru a dovedi că f este funcţie injectivă, arătăm că $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ $(x_1,x_2 \in G)$. Fie aşadar $x_1,x_2 \in G$ astfel încât $f(x_1) = f(x_2)$. Înmulţind la dreapta în grupul G' cu $(f(x_2))^{-1}$ obţinem succesiv: $f(x_1)\,(f(x_2))^{-1} = e'$ $\Leftrightarrow f(x_1)f(x_2^{-1}) = e' \Leftrightarrow f(x_1 x_2^{-1}) = e' \Leftrightarrow x_1 x_2^{-1} = e \Leftrightarrow x_1 = x_2$.

3°. Fie $y_1,y_2 \in f(H)$ şi să arătăm că $y_1 y_2^{-1} \in f(H)$. Într-adevăr, dacă scriem $y_1 = f(x_1)$, $y_2 = f(x_2)$ cu $x_1,x_2 \in H$, atunci: $y_1 y_2^{-1} = f(x_1)f(x_2^{-1}) = f(x_1 x_2^{-1}) \in H$, căci $x_1 x_2^{-1} \in H$, fiindcă H este subgrup al lui G. Aşadar, $f(H)$ este subgrup al lui G'. Luând în particular $H = G$, obţinem că $f(G) = Im\ f$ este un subgrup al grupului G'.

Observaţie

Punctul 2° din teorema precedentă constituie o metodă de a proba injectivitatea unui morfism, pe care o vom utiliza frecvent în cele ce urmează.

Definiţie

1) Fie $(G, *)$ şi $(G', \circ)$ două grupuri. O funcţie $f : G \to G'$ se numeşte ***izomorfism de grupuri*** dacă este un morfism de grupuri inversabil (adică un morfism care este funcţie inversabilă, iar funcţia inversă $f^{-1} : G' \to G$ este de asemenea morfism); funcţia f^{-1} este tot un izomorfism de grupuri, numit ***izomorfismul invers*** lui f.

2) Un izomorfism de la un grup la el însuşi se numeşte ***automorfism*** al acelui grup.

3) Dacă între grupurile G şi G' există cel puţin un izomorfism, spunem că ***grupurile sunt izomorfe*** şi scriem $G \approx G'$.

Exemple

1. Funcţia $f : (\mathbb{R}, +) \to (\mathbb{R}_+^*, \cdot)$, unde $\mathbb{R}_+^* = (0, \infty)$, $f(x) = e^x$ este un izomorfism de grupuri.

Într-adevăr, am văzut că funcţia este un morfism de grupuri, este inversabilă, iar inversa sa $f^{-1} : \mathbb{R}_+^* \to \mathbb{R}$, $f(x) = \ln x$ este de asemenea morfism de grupuri, întrucât $f^{-1}(xy) = \ln(xy) = \ln x + \ln y = f^{-1}(x) + f^{-1}(y)$, $\forall\, x,y \in \mathbb{R}_+^*$.

2. Funcţia $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$, $f(x) = -x$ este un automorfism al grupului $(\mathbb{Z}, +)$.

Într-adevăr: $f(x + y) = -(x + y) = (-x) + (-y) = f(x) + f(y)$, $\forall\, x,y \in \mathbb{Z}$, deci f este un morfism (un endomorfism), iar funcţia inversă este $f^{-1} = f$, care este un endomorfism al lui $(\mathbb{Z}, +)$.

3. Orice grup $(G, \cdot)$ are cel puţin un automorfism şi anume automorfismul identic $1_G : G \to G$, $1_G(x) = x$, $\forall\, x \in G$.

Comentariu metodic

În cazul grupurilor finite constatăm că două grupuri finite de acelaşi ordin sunt izomorfe dacă şi numai dacă tablele operaţiilor lor sunt la fel „organizate".

Într-adevăr, izomorfismul direct şi cel invers fac ca un element dintr-un grup şi imaginea sa prin izomorfismul respectiv în celălalt grup, să ocupe în cele două table aceleaşi poziţii.

De exemplu, grupul multiplicativ $U(\mathbb{Z}_{12})$ al claselor de resturi modulo 12 relativ prime cu 12 este izomorf cu grupul definit prin tabla din dreapta, numit *grupul lui Klein*. Acest lucru reiese dacă observăm tablele operaţiilor din cele două grupuri:

$U(\mathbb{Z}_{12}) = \{\hat{1}, \hat{5}, \hat{7}, \widehat{11}\}$

$\cdot$	$\hat{1}$	$\hat{5}$	$\hat{7}$	$\widehat{11}$
$\hat{1}$	$\hat{1}$	$\hat{5}$	$\hat{7}$	$\widehat{11}$
$\hat{5}$	$\hat{5}$	$\hat{1}$	$\widehat{11}$	$\hat{7}$
$\hat{7}$	$\hat{7}$	$\widehat{11}$	$\hat{1}$	$\hat{5}$
$\widehat{11}$	$\widehat{11}$	$\hat{7}$	$\hat{5}$	$\hat{1}$

$K = \{e, a, b, c\}$

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Două grupuri izomorfe sunt „identice" din punct de vedere al proprietăţilor algebrice. De exemplu, dacă unul este comutativ şi celălalt este comutativ, dacă unul conţine un element de un anumit ordin n, atunci şi celălalt conţine un element de ordin n etc.

Aceasta se explică prin aceea că izomorfismul direct şi cel invers „transportă" o structură în cealalaltă, transferând toate proprietăţile dintr-un grup în celălalt grup. De aceea în algebră „recunoaşterea" unui grup se face prin evidenţierea unui grup izomorf cu acesta, care să fie bine cunoscut. Se ajunge astfel la un ***pas de abstractizare*** de tipul următor: toate grupurile izomorfe între ele se comportă la fel, constituie aşadar un „tip" de grupuri, se pot asimila cu unul singur din ele, detaşându-ne de mulţimea şi operaţia fiecărui grup individual, deci nemaicontând „identitatea" lui concretă.

De exemplu, toate grupurile cu 4 elemente având tabla organizată ca în grupul lui Klein, constituie un tip de grupuri având ca reprezentant grupul lui Klein.

În concluzie, determinarea unui grup se face până la „un izomorfism", sau cum se mai spune, „abstracţie făcând de un izomorfism".

Rezultatul următor dă o caracterizare a morfismelor de grupuri care sunt izomorfisme, caracterizare ce ne va permite să arătăm mai simplu că anumite funcţii sunt izomorfisme de grupuri.

Teoremă

Un morfism de grupuri este izomorfism dacă şi numai dacă este bijectiv.

Demonstraţie. Fie $f : (G, \cdot) \to (G', \cdot)$ un morfism de grupuri. Arătăm echivalenţa:

$$f \text{ este izomorfism} \Leftrightarrow f \text{ este bijecţie.}$$

($\Rightarrow$). Presupunem că f este izomorfism de grupuri. Atunci f este o funcţie inversabilă, deci bijectivă.

($\Leftarrow$). Presupunem că f este o funcţie bijectivă. Atunci f este o funcţie inversabilă şi mai trebuie să dovedim că funcţia inversă $f^{-1} : G' \to G$ este tot un morfism de grupuri. Într-adevăr, pentru $y_1, y_2 \in G'$ arbitrare, să notăm $x_1 = f^{-1}(y_1) \in G$ şi $x_2 = f^{-1}(y_2) \in G$, ceea ce este echivalent cu $f(x_1) = y_1$ şi $f(x_2) = y_2$. Atunci:

$$f^{-1}(y_1y_2) = f(f(x_1)f(x_2)) = f^{-1}(f(x_1x_2)) = x_1x_2 = f^{-1}(y_1)\, f^{-1}(y_2),$$

adică f^{-1} este morfism de grupuri.

Un exemplu de utilizare a teoremei precedente îl constituie demonstraţia rezultatului care urmează şi care stabileşte „tipurile" de grupuri ciclice.

Teoremă

a) Orice grup ciclic finit de ordin n este izomorf cu grupul $(\mathbb{Z}_n, +)$.

b) Orice grup ciclic infinit este izomorf cu grupul $(\mathbb{Z}, +)$.

Demonstraţie. a) Fie $(G, \cdot)$ un grup ciclic de ordin n. Atunci există $x \in G$ astfel încât $G = \langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\} = \{x^k \mid k \in \mathbb{Z}\}$.

Definim funcţia $f : (G, \cdot) \to (\mathbb{Z}_n, +)$ prin $f(x^k) = \hat{k}$, $\forall\, k \in \mathbb{Z}$ şi arătăm că această funcţie este un izomorfism de grupuri. Vom arăta că f este un morfism bijectiv. Avem mai întâi:

$$f(x^k x^\ell) = f(x^{k+\ell}) = \widehat{k+\ell} = \hat{k} + \hat{\ell} = f(x^k) + f(x^\ell), \;\; \forall\, k, \ell \in \mathbb{Z},$$

ceea ce arată că f este morfism de grupuri. Nucleul acestui morfism este:

$$\text{Ker } f = \{x^k \in G \mid f(x^k) = \hat{0}\} = \{x^k \in G \mid \hat{k} = \hat{0}\} = \{x^k \in G \mid k \vdots n\} = \{e\}$$

(am ținut seama că x este un element de ordin n în grupul G), ceea ce arată că morfismul f este injectiv. Dar grupurile $(G, \cdot)$ și $(\mathbb{Z}_n, +)$ au același ordin n și atunci funcția injectivă f este chiar bijectivă. În concluzie, f este un morfism bijectiv de grupuri, deci un izomorfism de grupuri.

b) Fie $(G, \cdot)$ un grup ciclic infinit, $G = \langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$.

Funcția $f : (G, \cdot) \to (\mathbb{Z}, +)$, $f(x^k) = k$ este bine definită ca funcție (nu putem avea $x^k = x^\ell$ cu $k \neq \ell$, căci ar rezulta $x^{k-\ell} = e$, deci x ar avea ordin finit, fals) și este morfism de grupuri, întrucât:

$$f(x^k \cdot x^\ell) = f(x^{k+\ell}) = k + \ell = f(x^k) + f(x^\ell), \ \forall\, k,\ell \in \mathbb{Z}.$$

Nucleul acestui morfism este: $\text{Ker } f = \{x^k \in G \mid f(x^k) = 0\} = \{x^k \in G \mid k = 0\} = \{x^0\} = \{e\}$, ceea ce arată că morfismul f este injectiv. Dar f este și surjectiv, deoarece $\forall\, k \in \mathbb{Z}$, $\exists\, x^k \in G$ cu $f(x^k) = k$.

Prin urmare f este un morfism bijectiv, adică un izomorfism de grupuri.

Observație

În baza teoremei precedente, grupul ciclic $(U_n, \cdot)$ al rădăcinilor de ordinul n ale unității este izomorf cu grupul $(\mathbb{Z}_n, +)$ al claselor de resturi modulo n ($n \in \mathbb{N}$, $n \geq 2$).

Rezultatul de mai jos arată că un morfism injectiv de la un grup G la un grup G' permite „identificarea" lui G cu un subgrup al lui G' sau, cum se mai spune, arată că G se „scufundă" în G'.

Propoziție

Dacă $f : G \to G'$ este un morfism injectiv de grupuri, atunci grupul G este izomorf cu subgrupul $Im\ f$ al lui G'.

Demonstrație. Funcția $f_1 : G \to Im\ f$, $f_1(x) = f(x)$, $\forall\, x \in G$ este un morfism injectiv și surjectiv, deci bijectiv. Atunci f_1 este un izomorfism între grupul G și subgrupul $Im\ f$ al lui G'.

Legătura grupurilor finite cu grupurile de permutări, transport de structură (extindere)

Rezultatul următor este foarte important, căci arată în esență faptul că grupurile finite se scufundă în grupurile de permutări, deci studiul grupurilor finite se reduce la acela al subgrupurilor grupurilor de permutări.

Teoremă (Cayley)

Orice grup finit este izomorf cu un subgrup al unui grup de permutări.

Demonstrație. Fie $(G, \cdot)$ un grup finit de ordin n. Pentru fiecare $a \in G$ funcția $t_a : G \to G$, $t_a(x) = ax$ este o bijecție (permutare) a mulțimii G. Într-adevăr $t_a(x_1) = t_a(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$, deci funcția t_a este o injecție și deoarece G este mulțime finită, înseamnă că t_a este o bijecție. Să mai observăm că $t_a \circ t_b = t_{ab}$, $\forall\ a,b \in G$; într-adevăr: $(t_a \circ t_b)(x) = t_a(t_b(x)) = t_a(bx) = a(bx) = t_{ab}(x)$, $\forall\ x \in G$.

Fie $(\mathscr{B}(G), \circ)$ grupul tuturor bijecțiilor (permutărilor) mulțimii finite G, relativ la operația de compunere a funcțiilor. Acest grup este izomorf cu grupul simetric $(S_n, \cdot)$ al permutărilor de grad n, căci dacă $G = \{a_1, a_2, \ldots, a_n\}$, asocierea care „duce" o permutare $\sigma \in S_n$ în bijecția lui G definită prin tabloul $\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_{\sigma(1)} & a_{\sigma(2)} & \ldots & a_{\sigma(n)} \end{pmatrix}$ realizează un izomorfism între grupurile $(S_n, \cdot)$ și $(\mathscr{B}(G), \circ)$.

Definim acum funcția $f : (G, \cdot) \to (\mathscr{B}(G), \circ)$ prin $f(a) = t_a$ și arătăm că este un morfism injectiv de grupuri. Într-adevăr:

$$f(ab) = t_{ab} = t_a \circ t_b = f(a) \circ f(b),\ \forall\ a,b \in G,$$

ceea ce arată că f este morfism de grupuri. Nucleul acestui morfism este:

$$\operatorname{Ker} f = \{a \in G \mid f(a) = 1_G\} = \{a \in G \mid t_a = 1_G\} =$$
$$= \{a \in G \mid t_a(x) = x,\ \forall\ x \in G\} = \{a \in G \mid ax = x,\ \forall\ x \in G\} = \{e\},$$

ceea ce arată că f este injectiv. Conform propoziției anterioare, grupul G este izomorf cu subgrupul $Im\ f$ al grupului de permutări $(\mathscr{B}(G), \circ)$. Cum $(\mathscr{B}(G), \circ)$ este izomorf cu grupul simetric $(S_n, \cdot)$, înseamnă în ultimă instanță că G este izomorf cu un subgrup al lui $(S_n, \cdot)$.

În fine dăm acum un rezultat util în exerciții, care stabilește că o bijecție „transferă" o structură de grup dată, pe o mulțime „amorfă" (nestructurată) și reciproc că orice structură de grup poate fi gândită ca provenind dintr-un astfel de „transport" realizat de o bijecție.

Teoremă

a) Fie $(G, *)$ un grup, G' o mulţime şi $f : G \to G'$ o bijecţie. Pe mulţimea G' definim operaţia $\circ$ prin:

$$x \circ y = f\left(f^{-1}(x) * f^{-1}(y)\right),\ \forall x,y \in G'.$$

Atunci $(G', \circ)$ este un grup, iar $f : (G, *) \to (G', \circ)$ este un izomorfism de grupuri; se zice că $(G', \circ)$ este ***transportata*** structurii $(G, *)$ prin bijecţia f.

b) Dacă $(G, *)$ şi $(G', \circ)$ sunt două grupuri izomorfe, iar $f : G \to G'$ este un izomorfism de grupuri, atunci $(G', \circ)$ este transportata structurii $(G, *)$ prin bijecţia f şi invers, $(G, *)$ este transportata structurii $(G', \circ)$ prin bijecţia f^{-1}.

Demonstraţie. a) Verificăm axiomele grupului.

1°. Operaţia $\circ$ este asociativă, adică $(x \circ y) \circ z = x \circ (y \circ z)$, $\forall x,y,z \in G'$.

Într-adevăr: $(x \circ y) \circ z = \left(f\left(f^{-1}(x) * f^{-1}(y)\right)\right) \circ z = f\left(\left(f^{-1}(x) * f^{-1}(y)\right) * f^{-1}(z)\right) =$
$= f\left(f^{-1}(x) * f^{-1}(y) * f^{-1}(z)\right)$, iar $x \circ (y \circ z) = x \circ f\left(f^{-1}(y) * f^{-1}(z)\right) =$
$= f\left(f^{-1}(x) * \left(f^{-1}(y) * f^{-1}(z)\right)\right) = f\left(f^{-1}(x) * f^{-1}(y) * f^{-1}(z)\right)$, căci am ţinut seama de faptul că operaţia $*$ este asociativă.

2°. Operaţia $\circ$ are elementul neutru $e' = f(e)$, unde e este elementul neutru din grupul $(G, *)$. Într-adevăr:

$$x \circ e' = f\left(f^{-1}(x) * f^{-1}(e')\right) = f\left(f^{-1}(x) * e\right) = f\left(f^{-1}(x)\right) = x,\ \forall x \in G' \text{ şi}$$

$$e' \circ x = f\left(f^{-1}(e') * f^{-1}(x)\right) = f\left(e * f^{-1}(x)\right) = f\left(f^{-1}(x)\right) = x,\ \forall x \in G',$$

unde am ţinut seama de faptul că e este element neutru în grupul $(G, *)$.

3°. Orice element $x \in G'$ este simetrizabil faţă de operaţia $\circ$ şi are simetricul $f\left(\left(f^{-1}(x)\right)'\right)$, unde $\left(f^{-1}(x)\right)'$ reprezintă simetricul elementului $f^{-1}(x)$ în grupul $(G, *)$; într-adevăr:

$$x \circ f\left(\left(f^{-1}(x)\right)'\right) = f\left(f^{-1}(x) * \left(f^{-1}(x)\right)'\right) = f(e) = e' \text{ şi}$$

$$f\left(f^{-1}(x)'\right) \circ x = f\left(\left(f^{-1}(x)\right)' * f^{-1}(x)\right) = f(e) = e'.$$

Aşadar $(G', \circ)$ este un grup. Funcţia $f : (G, *) \to (G', \circ)$ este o bijecţie, dar şi un morfism de grupuri, deoarece:

$$f(x * y) = f\left(f^{-1}\left(f(x)\right) * f^{-1}\left(f(y)\right)\right) = f(x) \circ f(y),\ \forall x,y \in G.$$

Aşadar, grupurile $(G, *)$ şi $(G', \circ)$ sunt izomorfe prin izomorfismul f.

b) Deoarece f este un izomorfism de grupuri, avem pentru orice $x,y \in G'$:

$$x \circ y = f\left(f^{-1}(x)\right) \circ f\left(f^{-1}(y)\right) = f\left(f^{-1}(x) * f^{-1}(y)\right),$$

ceea ce este în conformitate cu operaţia introdusă la punctul a), deci $(G', \circ)$ este transportata structurii $(G, *)$ prin bijecţia f.

Analog rezultă că $(G, *)$ este transportata structurii $(G', \circ)$ prin bijecţia inversă f^{-1}.

Exerciţii rezolvate

1. Considerăm grupul $(G, *)$ studiat în exercițiul rezolvat 1 de la pag. 21, în care $G = (-1, 1)$, iar $x * y = \dfrac{x+y}{1+xy}$. Să se arate că funcția $f : (G, *)\to(\mathbb{R}, +)$, $f(x)=\ln\dfrac{1+x}{1-x}$ este un izomorfism de grupuri.

Soluție. Arătăm mai întâi că f este morfism de grupuri, adică:

$$f(x * y) = f(x) + f(y),\ \ \forall\, x,y \in (-1, 1).$$

Într-adevăr, putem scrie:

$$f(x * y) = f\left(\frac{x+y}{1+xy}\right) = \ln\frac{1+\dfrac{x+y}{1+xy}}{1-\dfrac{x+y}{1+xy}} = \ln\frac{1+x+y+xy}{1-x-y+xy} = \ln\frac{(1+x)(1+y)}{(1-x)(1-y)} =$$

$$= \ln\frac{1+x}{1-x} + \ln\frac{1+y}{1-y} = f(x) + f(y),\ \ \forall\, x,y \in (-1, 1).$$

Arătăm acum că f este bijectivă, ceea ce revine la a spune că $\forall\, y \in \mathbb{R}$, $\exists!\, x \in (-1, 1)$ astfel încât $y = f(x)$. Într-adevăr, avem succesiv:

$$f(x) = y \Leftrightarrow \ln\frac{1+x}{1-x} = y \Leftrightarrow \frac{1+x}{1-x} = e^y \Leftrightarrow 1+x = e^y - xe^y \Leftrightarrow x = \frac{e^y-1}{e^y+1};$$

este clar că x găsit este unic şi aparține intervalului $G = (-1, 1)$, fapt ce se verifică imediat, căci $x+1 = \dfrac{2e^y}{e^y+1} > 0$, iar $x-1 = -\dfrac{2}{e^y+1} < 0$. Fiind un morfism bijectiv, f este un izomorfism de grupuri.

2. Pentru $a \in \mathbb{R}^*$, $b \in \mathbb{R}$ definim funcția $f_{a,b}(x) = ax + b$.

Notăm $A = \{f_{a,b} \mid a \in \mathbb{R}^*,\ b \in \mathbb{R}\}$, $T = \{f_{1,b} \mid b \in \mathbb{R}\}$, $\Omega = \{f_{a,0} \mid a \in \mathbb{R}^*\}$ (funcțiile $f_{a,b}$ se numesc ***transformări afine*** ale dreptei reale, funcțiile $f_{1,b}$ se numesc ***translații*** ale dreptei reale, iar funcțiile $f_{a,0}$ se numesc ***omotetii*** ale dreptei reale).

Să se demonstreze că:

1) $(A, \circ)$ este un grup, unde $\circ$ desemnează compunerea funcțiilor.

2) $(T, \circ)$ este un subgrup abelian al lui $(A, \circ)$, izomorf cu grupul $(\mathbb{R}, +)$.

3) $(\Omega, \circ)$ este un subgrup abelian al lui $(A, \circ)$, izomorf cu grupul $(\mathbb{R}^*, \cdot)$.

Soluție. 1) Arătăm mai întâi că pe mulțimea A compunerea funcțiilor este o operație algebrică. Fie $f_{a,b}$ şi $f_{c,d}$ două funcții arbitrare din A. Pentru $x \in \mathbb{R}$ oarecare, avem:

$$(f_{a,b} \circ f_{c,d})(x) = f_{a,b}\left(f_{c,d}(x)\right) = f_{a,b}(cx+d) = a(cx+d)+b = acx+ad+b = f_{ac,ad+b}(x),$$

de unde desprindem „regula” de compunere:

$$f_{a,b} \circ f_{c,d} = f_{ac,\, ad+b} \qquad (1).$$

Cum $a \neq 0$, $c \neq 0$ rezultă $ac \neq 0$, deci $f_{ac,\, ad+b} \in A$ şi astfel am dovedit că pe mulţimea A compunerea funcţiilor este o operaţie algebrică.

Verificăm axiomele grupului.

1°. Compunerea este asociativă pe mulţimea A, întrucât este asociativă pe mulţimea $\mathbb{R}^{\mathbb{R}}$ a tuturor funcţiilor de la $\mathbb{R}$ la $\mathbb{R}$.

2°. Elementul neutru este funcţia identică $1_{\mathbb{R}} = f_{1,0} \in A$.

3°. Orice funcţie din A este inversabilă în A. Într-adevăr, dacă $f_{a,b} \in A$, căutăm $f_{c,d} \in A$ astfel încât $f_{a,b} \circ f_{c,d} = f_{c,d} \circ f_{a,b} = f_{1,0}$, ceea ce, ţinând seama de (1), se scrie succesiv:

$$f_{ac,\, ad+b} = f_{ac,\, bc+d} = f_{1,0} \Leftrightarrow \begin{cases} ac = 1 \\ ad + b = bc + d = 0 \end{cases} \Leftrightarrow \begin{cases} c = \dfrac{1}{a} \\ d = -\dfrac{b}{a} \end{cases}.$$

Prin urmare funcţia inversă a funcţiei $f_{a,b} \in A$ este $f_{a,b}^{-1} = f_{\frac{1}{a},\, -\frac{b}{a}} \in A$ (2).

2) Pentru a arăta că T este subgrup al lui A, verificăm că pentru oricare două funcţii $f_{1,\, b'}$ şi $f_{1,\, b''}$ din T, rezultă că $f_{1,\, b'} \circ (f_{1,\, b''})^{-1} \in T$. Într-adevăr, folosind egalităţile (1) şi (2), avem:

$$f_{1,\, b'} \circ (f_{1,\, b''})^{-1} = f_{1,\, b'} \circ f_{1,\, -b''} = f_{1,\, b'-b''} \in T.$$

Subgrupul T este abelian (deşi întregul grup A nu este abelian) întrucât:

$$f_{1,\, b'} \circ f_{1,\, b''} = f_{1,\, b''} \circ f_{1,\, b'} = f_{1,\, b'+b''}.$$

Definim funcţia $\varphi : (T, \circ) \to (\mathbb{R}, +)$ prin $\varphi(f_{1,\, b}) = b$ şi arătăm că este un izomorfism de grupuri. În primul rând φ este bine definită ca funcţie şi este un morfism de grupuri, deoarece:

$$\varphi(f_{1,\, b'} \circ f_{1,\, b''}) = \varphi(f_{1,\, b'+b''}) = b' + b'' = \varphi(f_{1,\, b'}) + \varphi(f_{1,\, b''}).$$

În al doilea rând φ este o bijecţie, întrucât $\forall\, b \in \mathbb{R}$, $\exists!\, f_{1,\, b} \in T$ astfel încât $\varphi(f_{1,\, b}) = b$. Rezultă că φ este un izomorfism de grupuri, deci $(T, \circ) \approx (\mathbb{R}, +)$.

3) Pentru a arăta că Ω este subgrup al lui A, probăm faptul că pentru oricare două funcţii $f_{a',\, 0}$ şi $f_{a'',\, 0}$ din Ω, rezultă $f_{a',\, 0} \circ (f_{a'',\, 0})^{-1} \in \Omega$.

Într-adevăr, folosind (1) şi (2) avem:

$$f_{a',\, 0} \circ (f_{a'',\, 0})^{-1} = f_{a',\, 0} \circ f_{\frac{1}{a''},\, 0} = f_{\frac{a'}{a''},\, 0} \in \Omega.$$

Subgrupul Ω este abelian, deoarece $f_{a',\, 0} \circ f_{a'',\, 0} = f_{a'',\, 0} \circ f_{a',\, 0} = f_{a'a'',\, 0}$.

Definim funcţia $\psi : (\Omega, \circ) \to (\mathbb{R}^*, \cdot)$ prin $\psi(f_{a,\, 0}) = a$ şi arătăm că este un izomorfism de grupuri. În primul rând ψ este bine definită şi este un morfism de grupuri, deoarece:

$$\psi(f_{a',0} \circ f_{a'',0}) = \psi(f_{a'a'',0}) = a'a'' = \psi(f_{a',0})\psi(f_{a'',0}) .$$

În al doilea rând ψ este bijecție, întrucât $\forall\ a \in \mathbb{R}^*$, $\exists!\ f_{a,0} \in \Omega$ astfel încât $\psi(f_{a,0}) = a$. Aşadar ψ este un izomorfism de grupuri, deci $(\Omega, \circ) \approx (\mathbb{R}^*, \cdot)$.

3. Fie $G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle|\, a,b \in \mathbb{R},\ a \neq 0 \text{ sau } b \neq 0 \right\}$. Să se arate că:

1) Mulțimea G este un grup abelian relativ la înmulțirea matricelor.

2) Pentru fiecare $n \in \mathbb{N}^*$, există un unic subgrup de ordin n al grupului G.

Soluție. 1) Verificăm mai întâi că înmulțirea matricelor este operație algebrică pe mulțimea G. Să notăm, pentru simplitate:

$$A_{a,b} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \text{ deci } G = \{ A_{a,b} \mid a,b \in \mathbb{R},\ a \neq 0 \text{ sau } b \neq 0\}.$$

Avem $A_{a,b} \cdot A_{c,d} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} = A_{ac-bd,\, ad+bc}$; de asemenea, să remarcăm că pentru $A_{a,b} \in G$ ipoteza $a \neq 0$ sau $b \neq 0$ este echivalentă cu $\det A_{a,b} \neq 0$; atunci dacă şi $A_{c,d} \in G$, avem $\det A_{c,d} \neq 0$, prin urmare $\det A_{ac-bd,\, ad+bc} =$ $= \det(A_{a,b} \cdot A_{c,d}) = \det A_{a,b} \cdot \det A_{c,d} \neq 0$ şi deci $A_{ac-bd,\, ad+bc} \in G$. Reținem „regula" de înmulțire:

$$A_{a,b} \cdot A_{c,d} = A_{ac-bd,\, ad+bc} \qquad (1).$$

Verificăm axiomele grupului abelian.

1°. Înmulțirea matricelor este asociativă pe mulțimea G, întrucât este asociativă pe mulțimea $\mathcal{M}_2(\mathbb{R})$.

2°. Elementul – unitate este matricea-unitate $I_2 = A_{1,0} \in G$.

3°. Orice matrice $A_{a,b} \in G$ este inversabilă în G, având inversa

$$A_{a,b}^{-1} = A_{\frac{a}{a^2+b^2},\, -\frac{b}{a^2+b^2}} \in G \qquad (2)$$

ceea ce rezultă uşor pe baza formulei (1); dacă vom căuta inversa lui $A_{a,b}$ de forma $A_{c,d}$, din condiția $A_{a,b} \cdot A_{c,d} = A_{c,d} \cdot A_{a,b} = A_{1,0}$, se obține $c = \dfrac{a}{a^2+b^2}$, $d = -\dfrac{b}{a^2+b^2}$.

4°. Înmulțirea matricelor este comutativă pe mulțimea G, întrucât:

$$A_{a,b} \cdot A_{c,d} = A_{c,d} \cdot A_{a,b} = A_{ac-bd,\, ad+bc}.$$

2) Arătăm că grupul $(\mathbb{C}^*, \cdot)$ este izomorf cu grupul $(G, \cdot)$. Pentru aceasta definim funcția $f : (\mathbb{C}^*, \cdot) \to (G, \cdot)$ prin $f(a + bi) = A_{a,b}$ şi arătăm că este un izomorfism de grupuri. Într-adevăr:

$$f\big((a+bi)(c+di)\big) = \big((ac-bd) + (ad+bc)i\big) = A_{ac-bd,\, ad+bc} =$$

$$= A_{a,b} \cdot A_{c,d} = f(a+bi)f(c+di)\,,\ \forall\, a+bi,\, c+di \in \mathbb{C}^*,$$

ceea ce arată că f este un morfism de grupuri. Acest morfism este bijectiv, întrucât $\forall\ A_{a,b} \in G$, $\exists!\ a + bi \in \mathbb{C}^*$ cu $f(a + bi) = A_{a,b}$. Prin urmare f este un izomorfism de grupuri, deci $(\mathbb{C}^*, \cdot) \approx (G, \cdot)$. Dar în grupul $(\mathbb{C}^*, \cdot)$ există un singur subgrup de ordin n şi anume grupul $(U_n, \cdot)$ al rădăcinilor de ordinul n ale unităţii (vezi exemplul de la pag. 30 în care se determină subgrupurile finite ale grupului $(\mathbb{C}^*, \cdot)$). Proprietatea se transmite atunci şi grupului izomorf $(G, \cdot)$ şi conchidem astfel că acest grup are un singur subgrup de ordinul n, pentru fiecare $n \in \mathbb{N}^*$.

4. Să se arate că orice grup de ordinul 4 este izomorf fie cu grupul ciclic $(\mathbb{Z}_4, +)$, fie cu grupul lui Klein $(\mathbb{K}, \cdot)$.

Soluţie. Fie $G = \{e, a, b, c\}$ un grup de ordin 4, cu operaţia notată multiplicativ, e fiind elementul neutru. Fiecare din elementele a, b, c au drept ordin un divizor al lui 4, diferit de 1, adică au ordinul 2 sau 4. Studiem două cazuri, complementare logic, după cum G conţine un element de ordin 4, respectiv G nu conţine un astfel de element.

Cazul I: G conţine un element de ordin 4, de exemplu a. Atunci subgrupul ciclic $\langle a \rangle$ are ordinul 4, deci $\langle a \rangle = G$.

Aceasta înseamnă că G este un grup ciclic de ordinul 4, deci este izomorf cu grupul $(\mathbb{Z}_4, +)$, conform teoremei de la pag. 46.

Cazul II: G nu conţine nici un element de ordinul 4. Înseamnă că toate elementele a, b, c au ordinul 2 deci $a^2 = b^2 = c^2 = e$. Să determinăm produsele ab, ba, ac, ca, bc, cb din G. Vom face raţionamentul doar pentru ab, pentru celelalte procedându-se analog.

Cum $ab \in G$, putem avea $ab = e$ sau $ab = a$ sau $ab = b$ sau $ab = c$.

Dacă $ab = e$, înmulţind la stânga cu a rezultă $a^2b = a$, adică $eb = a$, deci $b = a$, absurd.

Dacă $ab = a$, simplificând la stânga prin a, rezultă $b = e$, absurd.

Dacă $ab = b$ rezultă $a = e$, absurd. Prin urmare singura posibilitate este $ab = c$.

Toate celelalte produse sunt prezentate în tabla operaţiei care este redată mai jos:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Se vede că această tablă este „identică" cu tabla grupului lui Klein, mai exact, pătratul oricărui element este egal cu e, iar dintre elementele a, b, c, oricare două distincte, prin înmulţire îl dau pe al treilea.

Rezultă că grupul G este în acest caz izomorf cu grupul Klein. În concluzie, *abstracţie făcând de un izomorfism, există doar două grupuri de ordinul* 4*: grupul ciclic* $(\mathbb{Z}_4, +)$ *şi grupul lui Klein* $(\mathbb{K}, \cdot)$.

5. Fie $a \in \mathbb{R}$. Să se definească pe intervalul $G = (a, \infty)$ o structură de grup izomorfă cu grupul $(\mathbb{R}, +)$.

Soluție. Căutăm o bijecție $f : \mathbb{R} \to (a, \infty)$ și „transportăm" prin această bijecție structura $(\mathbb{R}, +)$ pe mulțimea $G = (a, \infty)$, conform teoremei de la pag. 49. Evident, avem bijecțiile imediate:

$$\mathbb{R} \xrightarrow{v} (0, \infty) \xrightarrow{u} (a, \infty),\quad v(x) = e^x,\ u(x) = x + a.$$

Atunci, compunerea acestora $f = u \circ v$, definită prin $f(x) = e^x + a$, este bijecția căutată de la $\mathbb{R}$ la $G = (a, \infty)$.

Operația $\circ$ pe mulțimea G se definește, în baza teoremei menționate, prin:

$$x \circ y = f\left(f^{-1}(x) + f^{-1}(y)\right),\ \forall x, y \in G, \qquad (1)$$

Observăm ușor că $f^{-1} : (a, \infty) \to \mathbb{R}$ este dată prin $f^{-1}(x) = \ln(x - a)$ și atunci (1) se scrie succesiv:

$$x \circ y = f\left(f^{-1}(x) + f^{-1}(y)\right) = f\left(\ln(x-a) + \ln(y-a)\right) = f\left(\ln(x-a)(y-a)\right) =$$
$$= e^{\ln(x-a)(y-a)} + a = (x-a)(y-a) + a = xy - ax - ay + a^2 + a.$$

Așadar, definind $x \circ y = xy - ax - ay + a^2 + a$, $\forall\ x, y \in G = (a, \infty)$, rezultă că $(G, \circ)$ este un grup izomorf cu grupul $(\mathbb{R}, +)$ prin izomorfismul $f : (\mathbb{R}, +) \to (G, \circ)$, $f(x) = e^x + a$.

EXERCIȚII PROPUSE

1. Arătați că funcția $f : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$, $f(x) = \cos 2\pi x + i \sin 2\pi x$ este un morfism de grupuri. Determinați nucleul și imaginea acestui morfism.

2. Arătați că funcția $f : (\mathbb{R}, +) \to (\mathbb{R}, *)$, $f(x) = x - a$, unde $(\mathbb{R}, *)$ este grupul cu operația $*$ definită prin $x * y = x + y + a$, cu $a \in \mathbb{R}$ fixat, este un izomorfism de grupuri.

3. Arătați că funcția $f : (\mathbb{R}, +) \to (\mathbb{R}, *)$, $f(x) = \sqrt[3]{x}$, unde $(\mathbb{R}, *)$ este grupul cu operația $x * y = \sqrt[3]{x^3 + y^3}$, este un izomorfism de grupuri.

4. Arătați că funcția $f : (G, *) \to (\mathbb{R}^*, \cdot)$, $f(x) = \ln x$, unde $G = \mathbb{R}_+^* \setminus \{1\}$ este grupul cu operația $x * y = x^{\ln y}$, este un izomorfism de grupuri.

5. Considerăm grupul $(\mathbb{R}, *)$ unde $x * y = x\sqrt{1+y^2} + y\sqrt{1+x^2}$. Arătați că funcția $f : (\mathbb{R}, +) \to (\mathbb{R}, *)$, $f(x) = \operatorname{sh} x = \dfrac{e^x - e^{-x}}{2}$, este un izomorfism de grupuri.

6. Fie $G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| \, a \in \mathbb{Z} \right\}$. Arătați că funcția $f : (\mathbb{Z}, +) \to (G, \cdot)$, $f(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ este un izomorfism de grupuri.

7. Fie $G_1 = \{z \in \mathbb{C} \mid |z| = 1\}$ și $G_2 = \left\{ \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \middle| \, \alpha \in \mathbb{R} \right\}$. Arătați că funcția $f : (G_1, \cdot) \to (G_2, \cdot)$, $f(\cos\alpha + i\sin\alpha) = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}$ este un izomorfism de grupuri.

8. Arătați că grupul $(G, *)$, unde $G = \left(-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right)$, iar operația $*$ este:

$x * y = \operatorname{arctg}(\operatorname{tg} x + \operatorname{tg} y)$, este izomorf cu grupul $(\mathbb{R}, +)$.

9. Arătați că grupul $(G, \circ)$, unde $G = \{f_1, f_2, f_3, f_4\}$, $f_1, f_2, f_3, f_4 : \mathbb{R}^* \to \mathbb{R}^*$, $f_1(x) = x$, $f_2(x) = \dfrac{1}{x}$, $f_3(x) = -x$, $f_4(x) = -\dfrac{1}{x}$, iar $\circ$ este operația de compunere a funcțiilor, este izomorf cu grupul lui Klein.

10. Arătați că grupul $(G, \circ)$, unde $G = \{f_a \mid a > 0\}$, $f_a : \mathbb{R} \to \mathbb{R}$, $f_a(x) = \begin{cases} ax, & x > 0 \\ 0, & x \le 0 \end{cases}$, pentru fiecare $a > 0$, iar $\circ$ este operația de compunere a funcțiilor, este izomorf cu grupul $(\mathbb{R}_+^*, \cdot)$, unde $\mathbb{R}_+^* = (0, \infty)$.

11. Arătați că orice grup de ordin 6 este izomorf fie cu grupul ciclic $(\mathbb{Z}_6, +)$, fie cu grupul simetric $(S_3, \cdot)$.

12. Determinați, abstracție făcând de izomorfisme, grupurile de ordin cel mult 7.

13. Fie $(G, +)$ un subgrup al grupului $(\mathbb{R}, +)$ astfel încât $G \cap (-a, a)$ este o mulțime finită, pentru orice $a > 0$. Să se arate că: $(G, \cdot) \approx (\mathbb{Z}, +)$.

14. Arătați că grupurile $(\mathbb{Z}, +)$ și $(\mathbb{Q}, +)$ nu sunt izomorfe.

15. Arătaţi că grupurile $(\mathbb{R}^*, \cdot)$ şi $(\mathbb{R}_+^*, \cdot)$ nu sunt izomorfe.

16. Arătaţi că grupurile $(\mathbb{R}^*, \cdot)$ şi $(\mathbb{C}^*, \cdot)$ nu sunt izomorfe.

17. Fie $(G, \cdot)$ un grup. Arătaţi că funcţia $f : G \to G$, $f(x) = x^{-1}$ este o bijecţie şi determinaţi structura grupului $(G, \circ)$ care este transportata prin bijecţia f a structurii de grup $(G, \cdot)$.

18. Fie $(G, +)$ un subgrup al grupului $(\mathbb{C}, +)$. Arătaţi că orice morfism de grupuri $f : (\mathbb{Q}, +) \to (G, +)$ este de forma $f(x) = ax$, unde $a \in G$.

19. Determinaţi endomorfismele şi automorfismele grupului $(\mathbb{Q}, +)$.

20. Determinaţi endomorfismele şi automorfismele grupului $(\mathbb{Z}, +)$.

21. Determinaţi morfismele de grup $f : (\mathbb{Q}, +) \to (\mathbb{Z}, +)$.

22. Arătaţi că grupul $(\mathbb{Z}, +)$ este izomorf cu orice subgrup propriu al său.

23. Arătaţi că grupul $(\mathbb{Q}, +)$ nu este izomorf cu nici un subgrup propriu al său.

24. Fie $(G, \cdot)$ un grup şi funcţia $f : G \to G$, $f(x) = x^{-1}$. Arătaţi că funcţia f este endomorfism dacă şi numai dacă grupul G este abelian.
Problemă analogă pentru funcţia $g : G \to G$, $g(x) = x^2$.

25. Fie $(G, \cdot)$ un grup cu proprietatea că există $k \in \mathbb{Z}$ astfel încât funcţiile $f, g : G \to G$, $f(x) = x^k$, $g(x) = x^{-k}$ sunt endomorfisme surjective. Arătaţi că G este un grup abelian.

26. Fie G un grup, H un subgrup propriu al lui G, iar f_1, f_2 endomorfisme ale grupului G. Arătaţi că dacă $f_1(x) = f_2(x)$, $\forall\, x \in G \setminus H$, atunci $f_1(x) = f_2(x)$, $\forall\, x \in G$.

27. Fie G un grup şi f un endomorfism al lui G. Arătaţi că mulţimea $H = \{x \in G \mid f(x) = x\}$ este un subgrup al lui G. În cazul $G = (\mathbb{C}, +)$ şi $f : \mathbb{C} \to \mathbb{C}$, $f(x) = \overline{x}$ (endomorfismul-conjugare), determinaţi subgrupul H.

TESTE DE EVALUARE

Testul 1

(timp de lucru - 30 minute; fiecare exercițiu se notează cu 3 puncte)

Indicați răspunsul corect.

1. Fie $a,b \in \mathbb{C}$, $a \neq 0$ și $H = \{z \in \mathbb{C} \mid az^{100} = b\}$. Să se determine $b(a - b)$ știind că $(H, \cdot)$ este grup, unde „$\cdot$" este înmulțirea numerelor complexe.

a) 1; b) 0; c) – 1; d) nu există a și b cu proprietatea din enunț.

2. Câte subgrupuri are grupul $(\mathbb{Z}_{100}, +)$?

a) 2; b) 9; c) 10; d) 100.

3. Câte automorfisme are grupul $(\mathbb{Q}, +)$?

a) 1; b) 2; c) 4; d) o infinitate.

Testul 2

(timp de lucru - 50 minute; fiecare exercițiu se notează cu 3 puncte)

Pentru următoarele probleme se cer soluții complete.

1. Fie $a \in \mathbb{R}^*$ și $G = \left\{ \begin{pmatrix} 1 & x & ax+ax^2 \\ 0 & 1 & 2ax \\ 0 & 0 & 1 \end{pmatrix} \middle| \, x \in \mathbb{R} \right\}$.

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

b) Să se arate că $(G, \cdot)$ este grup abelian.

c) Să se arate că $(\mathbb{R}, +)$ și $(G, \cdot)$ sunt izomorfe.

2. Pe $\mathbb{R}$ se definește legea de compoziție: $x \circ y = x\sqrt{1+y^2} + y\sqrt{1+x^2}$, $\forall\, x,y \in \mathbb{R}$.

a) Să se arate că $(\mathbb{R}, \circ)$ este grup abelian.

b) Să se arate că grupurile $(\mathbb{R}, \circ)$ și $(\mathbb{R}, +)$ sunt izomorfe.

c) Să se calculeze $\underbrace{x * x * x * \ldots * x}_{n \text{ ori}}$.

3. Pentru fiecare $a > 0$ se definește funcția $f_a : \mathbb{R} \to \mathbb{R}$, $f_a(x) = \begin{cases} ax, & x > 0 \\ 0, & x \leq 0 \end{cases}$ și se consideră mulțimea $G = \{f_a \mid a > 0\}$. Să se arate că:

a) G împreună cu operația „$\circ$" de compunere a funcțiilor este grup abelian.

b) Grupurile $(G, \circ)$ și $((0, \infty), \cdot)$ sunt izomorfe.

INELE ŞI CORPURI

Inele, exemple

Comentariu metodic

Spre a ne face o idee preliminară privind structurile de inel şi corp, să remarcăm mai întâi următorul fapt: într-un grup, pe care să-l notăm aditiv, există o „adunare" care este operaţia grupului, din care derivă şi o „scădere":

$$x - y = x + (-y).$$

După cum vom vedea, într-un inel avem două operaţii ale inelului, o „adunare" şi o „înmulţire", iar din adunare derivă şi o „scădere".

În fine, într-un corp avem două operaţii ale corpului şi anume o „adunare" şi o „înmulţire", iar din adunare derivă şi o „scădere" şi din înmulţire derivă şi o „împărţire" prin elemente nenule:

$$\frac{x}{y} = xy^{-1}.$$

Cu alte cuvinte, inelul este un „cadru" matematic în care ne putem desfăşura relativ la trei operaţii: adunare, înmulţire, scădere, în timp ce corpul este un „cadru" matematic în care ne putem desfăşura relativ la toate cele patru operaţii uzuale (aritmetice): adunare, înmulţire, scădere, împărţire prin elemente nenule.

Definiţie

Se numeşte ***inel*** un triplet $(A, +, \cdot)$ în care A este o mulţime nevidă, iar „+" şi „·" desemnează două operaţii pe A, numite prin extensie de limbaj „adunare" şi „înmulţire", care verifică următoarele trei axiome:

1°. Cuplul $(A, +)$ este un grup abelian.

2°. Cuplul $(A, \cdot)$ este un monoid.

3°. Înmulţirea este distributivă faţă de adunare, adică $\begin{cases} x(y+z) = xy + xz \\ (y+z)x = yx + zx \end{cases}$, $\forall x, y, z \in A$.

Dacă în plus, se verifică şi axioma a patra:

4°. Înmulţirea este comutativă (echivalent spus, în axioma 2° scriem „monoid comutativ"), atunci $(A, +, \cdot)$ se numeşte ***inel comutativ***.

Elementul neutru din grupul $(A, +)$ se notează cu 0 sau 0_A şi se numeşte ***elementul nul*** al inelului, iar elementul neutru din monoidul $(A, \cdot)$ se notează cu 1 sau 1_A şi se numeşte ***elementul unitate*** al inelului.

Comentariu metodic privind definiția inelului

Dacă în locul axiomei 2° se folosește axioma mai slabă:

2°°. Înmulțirea este asociativă,

spunem că $(A, +, \cdot)$ este un „inel fără element-unitate" (inel „neunitar").

Cazurile cele mai frecvente de inele presupun însă și existența elementului-unitate adică verificarea axiomei 2°. De aceea, din punct de vedere didactic, preferăm utilizarea în acest manual a acestei axiome, adică lucrăm cu „inele cu element-unitate" (inele „unitare"), fără a menționa în mod expres acest lucru.

Să mai remarcăm că în structura algebrică de inel „fuzionează" două structuri algebrice: ***una aditivă de grup abelian*** și ***una multiplicativă de monoid***. „Sudarea" acestor două structuri este realizată de ***axioma 3° de distributivitate*** a înmulțirii față de adunare.

Exemple de inele: inele numerice, inelul claselor de resturi modulo *n*, inele de matrice, inele de funcții reale

1. $(\mathbb{Z}, +, \cdot)$ este un inel comutativ, numit ***inelul numerelor întregi*** în care elementul nul este numărul întreg 0, iar elementul-unitate este numărul întreg 1.

2. Dacă $\mathbb{Z}[i] = \{a + bi \mid a,b \in \mathbb{Z}\}$, atunci $(\mathbb{Z}[i], +, \cdot)$ este un inel comutativ, cu elementul nul $0 = 0 + 0i$ și elementul unitate $1 = 1 + 0i$. (Aici i este unitatea imaginară, adică $i^2 = -1$). Inelul $(\mathbb{Z}[i], +, \cdot)$ se numește ***inelul întregilor lui Gauss***.

3. Dacă $d \in \mathbb{Z}$ este un număr întreg care nu este pătrat perfect, iar $\sqrt{d}$ este o soluție fixată în mulțimea $\mathbb{C}$ a ecuației $x^2 = d$, notăm: $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a,b \in \mathbb{Z}\}$.

Atunci $(\mathbb{Z}[\sqrt{d}], +, \cdot)$ este un inel comutativ cu elementul nul $0 = 0 + 0\sqrt{d}$ și elementul-unitate $1 = 1 + 0\sqrt{d}$, numit ***inel de întregi pătratici***.

Pentru $d = -1$ se obține inelul întregilor lui Gauss.

4. Pentru $n \in \mathbb{N}$, $n \geq 2$, tripletul $(\mathbb{Z}_n, +, \cdot)$ este un inel comutativ cu elementul nul $\hat{0}$ și elementul-unitate $\hat{1}$, numit ***inelul claselor de resturi modulo n***.

Faptul că $(\mathbb{Z}_n, +, \cdot)$ este inel comutativ rezultă astfel: știm deja că $(\mathbb{Z}_n, +)$ este un grup abelian (chiar ciclic), că $(\mathbb{Z}_n, \cdot)$ este un monoid comutativ și se arată ușor că înmulțirea este distributivă față de adunare.

5. Pentru $n \in \mathbb{N}^*$, tripletul $(\mathcal{M}_n(A), +, \cdot)$, unde $A \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, este un inel în care elementul nul este matricea nulă 0_n, iar elementul-unitate este matricea unitate I_n.

Acest inel se numeşte ***inelul matricelor pătratice de ordin n peste A*** şi este necomutativ dacă $n \geq 2$. Vom relua acest exemplu când vom vorbi de inele de matrice.

6. Fie $D \subseteq \mathbb{R}$ o mulţime nevidă şi $\mathbb{R}^D = \{f : D \to \mathbb{R}\}$ mulţimea funcţiilor reale definite pe D. Definim adunarea şi înmulţirea funcţiilor prin egalităţile $(f + g)(x) = f(x) + g(x)$; $(fg)(x) = f(x)g(x)$, $\forall\, x \in D$. Atunci, tripletul $(\mathbb{R}^D, +, \cdot)$ este un inel comutativ, în care elementul nul este funcţia constantă 0 (funcţia nulă), iar elementul-unitate este funcţia constantă 1. Acest inel se numeşte ***inel de funcţii reale***.

În cazul particular $D = \mathbb{N}$, obţinem inelul $(\mathbb{R}^{\mathbb{N}}, +, \cdot)$ al *şirurilor de numere reale*.

7. Ca exemplu de inel fără element-unitate, putem da inelul $(2\mathbb{Z}, +, \cdot)$.

Definiţie

Dacă $(A, +, \cdot)$ este un inel, grupul $(U(A), \cdot)$ al elementelor inversabile din monoidul $(A, \cdot)$ se numeşte ***grupul elementelor inversabile (grupul unităţilor)*** din inelul A.

Comentariu metodic

Atragem atenţia asupra faptului că într-un inel, relativ la adunare orice element este simetrizabil, deoarece $(A, +)$ este un grup. Relativ la înmulţire însă, numai anumite elemente sunt inversabile, deoarece $(A, \cdot)$ este doar un monoid şi aceste elemente inversabile constituie grupul $(U(A), \cdot)$.

Remarcă. Dacă operaţiile se subînţeleg, scriem simplu inelul A, în loc de inelul $(A, +, \cdot)$.

Exemple de grupuri de elemente inversabile ale unor inele

1. În inelul $\mathbb{Z}$ avem $U(\mathbb{Z}) = \{-1, 1\} = U_2$.

2. În inelul $\mathbb{Z}[i]$ avem $U(\mathbb{Z}[i]) = \{1, -1, i, -i\} = U_4$. Aceasta se arată în felul următor: dacă $z = a + bi \in U(\mathbb{Z}[i])$, atunci există $z^{-1} = c + di \in \mathbb{Z}[i]$ astfel încât $z z^{-1} = 1$, adică $(a + bi)(c + di) = 1$; trecem la module şi ridicăm la pătrat şi se obţine $|a + bi|^2 |c + di|^2 = 1$, adică $(a^2 + b^2)(c^2 + d^2) = 1$ şi cum $a, b, c, d \in \mathbb{Z}$, vom avea $a^2 + b^2 = c^2 + d^2 = 1$, de unde $a_1 = 1$, $b_1 = 0$; $a_2 = -1$, $b_2 = 0$; $a_3 = 0$, $b_3 = 1$; $a_4 = 0$, $b_4 = -1$. Corespunzător avem:

$$z_1 = 1 + 0i = 1;\quad z_2 = -1 + 0i = -1;\quad z_3 = 0 + 1i = i;\quad z_4 = 0 + (-1)i = -i.$$

3. În inelul $(\mathbb{Z}_n, +, \cdot)$ avem $U(\mathbb{Z}_n) = \left\{\hat{k} \in \mathbb{Z}_n \middle| (k, n) = 1\right\}$.

4. În inelul $\mathcal{M}_n(\mathbb{Z})$ avem $U(\mathcal{M}_n(\mathbb{Z})) = \{X \in \mathcal{M}_n(\mathbb{Z}) \mid \det X = \pm 1\}$.

5. În inelul $\mathcal{M}_n(K)$, unde $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ avem $U(\mathcal{M}_n(K)) = \{X \in \mathcal{M}_n(K) \mid \det X \neq 0\}$.

6. În inelul de funcții reale $\mathbb{R}^D$ avem $U(\mathbb{R}^D) = \{f : D \to \mathbb{R} \mid f(x) \neq 0, \forall\, x \in D\}$, iar „inversa" unei funcții $f \in U(\mathbb{R}^D)$ este funcția $\frac{1}{f}$, definită prin $\left(\frac{1}{f}\right)(x) = \frac{1}{f(x)}$, $\forall\, x \in D$.

Divizori ai lui zero. Reguli de calcul. Caracteristică

În inelul $\mathbb{Z}$ al numerelor întregi, avem proprietatea:

$$xy = 0 \Rightarrow x = 0 \text{ sau } y = 0.$$

În inelul $\mathbb{Z}_6$ al claselor de resturi modulo 6 o asemenea proprietate nu are loc, căci de exemplu $\hat{2} \cdot \hat{3} = \hat{0}$ deși $\hat{2} \neq \hat{0}$ și $\hat{3} \neq \hat{0}$.

Suntem conduși către următoarea:

Definiție

Fie $(A, +, \cdot)$ un inel.

1°. Un element $x \in A$, $x \neq 0$ se numește ***divizor al lui zero*** dacă există $y \in A$, $y \neq 0$ astfel încât $xy = 0$ sau $yx = 0$.

2°. Spunem că inelul A ***are divizori ai lui zero*** dacă A conține cel puțin un divizor al lui zero; în caz contrar, spunem că A ***nu are divizori ai lui zero*** sau că este un ***inel integru***.

3°. Un inel comutativ și fără divizori ai lui zero se numește ***domeniu de integritate***.

Observație

Dacă $x \in A$ este un divizor al lui zero, atunci un $y \in A$ corespunzător este tot divizor al lui zero. În cazul unui inel comutativ, definiția se simplifică: $x \in A$ este divizor al lui zero, dacă $x \neq 0$ și există $y \in A$, $y \neq 0$ astfel încât $xy = 0$.

Exemple

1. Inelul $(\mathbb{Z}_6, +, \cdot)$ are divizori ai lui zero, de exemplu $\hat{2}$ sau $\hat{3}$, întrucât $\hat{2} \cdot \hat{3} = \hat{0}$.

2. Mai general, inelul $(\mathbb{Z}_n, +, \cdot)$, cu $n \geq 2$ număr compus (neprim) are divizori ai lui zero. Într-adevăr, putem scrie $n = n_1 n_2$ cu $1 < n_1 < n$, $1 < n_2 < n$, $n_1, n_2 \in \mathbb{N}$. Atunci $\hat{0} = \hat{n} = \widehat{n_1} \cdot \widehat{n_2}$, deci $\widehat{n_1}$ şi $\widehat{n_2}$ sunt divizori ai lui zero.

3. Inelul $\mathcal{M}_n(A)$, $n \geq 2$, unde $A \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ are divizori ai lui zero, deoarece:

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix} = 0_n.$$

4. Inelele numerice $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}\left[\sqrt{d}\right]$ ($d \in \mathbb{Z}$, nepătrat perfect) sunt domenii de integritate.

Rezultatul următor caracterizează inelele integre, punând totodată în evidenţă metoda de a stabili că un inel este integru.

Propoziţie

Într-un inel A următoarele afirmaţii sunt echivalente:

1°. A este inel integru.

2°. $\forall\, x, y \in A,\ x \neq 0,\ y \neq 0 \Rightarrow xy \neq 0$.

3°. $\forall\, x, y \in A$ cu $xy = 0 \Rightarrow x = 0$ sau $y = 0$.

Demonstraţie. 1° $\Rightarrow$ 2°. Presupunem că A este inel integru. Dacă, prin absurd, există $x, y \in A$, $x \neq 0$, $y \neq 0$ cu $xy = 0$, înseamnă că x şi y sunt divizori ai lui zero, contradicţie cu presupunerea că A este inel integru.

2° $\Rightarrow$ 3°. Presupunem că $\forall\, x, y \in A$, $x \neq 0$, $y \neq 0 \Rightarrow xy \neq 0$. Deoarece implicaţia logică $p \Rightarrow q$ este echivalentă cu implicaţia $\overline{q} \Rightarrow \overline{p}$, rezultă că ipoteza 2° în care lucrăm este echivalentă cu: $\forall\, x, y \in A$, $xy = 0 \Rightarrow x = 0$ sau $y = 0$, adică 3°.

3° $\Rightarrow$ 1°. Presupunem că $\forall\, x, y \in A$, $xy = 0 \Rightarrow x = 0$ sau $y = 0$. Dacă, prin absurd, A ar conţine un divizor al lui zero x ($x \neq 0$), aceasta ar însemna că există $y \in A$, $y \neq 0$ cu $xy = 0$ sau $yx = 0$. Datorită presupunerii în care lucrăm, ar rezulta $x = 0$ sau $y = 0$, contradicţie cu faptul că x şi y sunt nenule.

Comentariu metodic

Afirmaţia 3° din propoziţia precedentă arată că un inel integru prezintă „avantajul" că dacă un produs este nul, atunci unul din factorii produsului este nul. Acest lucru este util în rezolvarea ecuaţiilor peste acel inel.

Rezultatul care urmează extinde la nivelul unui inel oarecare reguli de calcul cu care suntem familiarizaţi de la operaţiile cu numere reale sau complexe.

Teoremă

În orice inel A au loc egalitățile:

1°. $x \cdot 0 = 0 \cdot x = 0$, $\forall x \in A$ (se spune că 0 este un element „absorbant").

2°. $\begin{cases} x(-y) = (-x)y = -xy \\ (-x)(-y) = xy \end{cases}$, $\forall x, y \in A$ („regula semnelor" la înmulțire).

3°. $\begin{cases} x(y-z) = xy - xz \\ (y-z)x = yx - zx \end{cases}$, $\forall x, y, z \in A$ (înmulțirea este distributivă față de scădere).

Demonstrație. 1°. Avem $x \cdot 0 = x(0 + 0) = x \cdot 0 + x \cdot 0$. În grupul $(A, +)$ putem reduce în ambii membrii termenul $x \cdot 0$ și obținem $0 = x \cdot 0$. Analog se arată că $0 \cdot x = 0$.

2°. Avem $x(-y) + xy = x(-y + y) = x \cdot 0 = 0$ de unde rezultă că în grupul $(A, +)$ avem $x(-y) = -xy$. Analog se arată că $(-x)y = -xy$. În această egalitate înlocuind y cu $-y$ obținem $(-x)(-y) = -(x(-y)) = -(-xy) = xy$.

3°. Avem $x(y - z) = x(y + (-z)) = xy + x(-z) = xy + (-xz) = xy - xz$. Analog se arată că $(y - z)x = yx - zx$.

Un exemplu oarecum banal de inel îl constituie un inel cu un singur element. Într-un asemenea inel avem $0 = 1$. Vom vedea că o asemenea egalitate nu poate avea loc decât în acest caz banal, mai precis vom arăta că dacă un inel are cel puțin două elemente, atunci $0 \neq 1$. Avem în acest sens următoarea:

Propoziție

Într-un inel A următoarele afirmații sunt echivalente:

1°. Inelul A are cel puțin două elemente.

2°. $0 \neq 1$.

Demonstrație. 1° $\Rightarrow$ 2°. Presupunem că inelul A are cel puțin două elemente. Dacă prin absurd $0 = 1$ atunci $\forall x \in A \Rightarrow x \cdot 1 = x \cdot 0 = 0$, deci $A = \{0\}$, contrar faptului că A are cel puțin două elemente. Așadar $0 \neq 1$.

2° $\Rightarrow$ 1°. Evidentă.

O consecință simplă a teoremei precedente este următorul rezultat:

Propoziție

Fie A un inel cu $0 \neq 1$. Atunci:

1°. Elementul nul 0 nu este inversabil, adică $0 \notin U(A)$.

2°. Dacă $x \in U(A)$, atunci și $-x \in U(A)$.

Demonstrație. 1°. Presupunem prin absurd că 0 este inversabil, deci există $x = 0^{-1} \in A$ astfel încât $x \cdot 0 = 0 \cdot x = 1$. Cum însă $x \cdot 0 = 0 \cdot x = 0$, obținem $0 = 1$, contradicție cu ipoteza $0 \neq 1$.

2°. Dacă $x \in U(A)$, vom arăta că $-x \in U(A)$, arătând că $-x$ are drept invers pe $-x^{-1}$. Într-adevăr:

$$(-x)(-x^{-1}) = xx^{-1} = 1 \text{ şi } (-x^{-1})(-x) = x^{-1}x = 1.$$

În orice inel „statutul" de divizor al lui zero este incompatibil cu acela de element inversabil. Avem mai precis următoarea:

Propoziţie

Dacă în inelul A elementul x este inversabil, atunci x nu este divizor al lui zero (echivalent spus, dacă x este divizor al lui zero, atunci x este neinversabil).

Demonstraţie. Fie $x \in A$ inversabil, adică $x \in U(A)$. Dacă, prin absurd, x ar fi divizor al lui zero, ar exista $y \in A$, $y \neq 0$, astfel încât $xy = 0$ sau $yx = 0$. Dacă $xy = 0$, înmulţind la stânga cu x^{-1}, avem succesiv $x^{-1}(xy) = 0 \Leftrightarrow (x^{-1}x)y = 0 \Leftrightarrow 1y = 0 \Leftrightarrow y = 0$, contradicţie. Analog, dacă $yx = 0$, prin înmulţire la dreapta cu x^{-1} se obţine $y = 0$, contradicţie.

În inelele integre are loc şi o regulă de simplificare la stânga sau la dreapta, aşa cum reiese din următoarea:

Propoziţie

Fie A un inel integru. Pentru oricare trei elemente $a, x, y \in A$, cu $a \neq 0$, au loc echivalenţele:

1°. $ax = ay \Leftrightarrow x = y$.

2°. $xa = ya \Leftrightarrow x = y$.

Demonstraţie. 1°. ($\Rightarrow$). Avem succesiv: $ax = ay \Leftrightarrow ax - ay = 0 \Leftrightarrow a(x - y) = 0 \Leftrightarrow$ $a = 0$ sau $x - y = 0$. Dar $a \neq 0$ şi atunci $x - y = 0$, deci $x = y$.

($\Leftarrow$). Evidentă.

2°. Analog.

Definiţie

Fie A un inel.

1°. Dacă există $n \in \mathbb{N}^*$ cu $n \cdot 1 = 0$ (adică $\underbrace{1+1+\ldots+1}_{n \text{ ori}} = 0$), atunci cel mai mic n cu această proprietate se numeşte ***caracteristica*** inelului A; altfel spus, în acest caz caracteristica este ordinul elementului 1 în grupul $(A, +)$.

2°. În caz contrar, adică $n \cdot 1 \neq 0$. $\forall\, n \in \mathbb{N}^*$, spunem că inelul A ***are caracteristica zero***.

Exemple

1. Inelul $\mathbb{Z}_n$ are caracteristica n, căci grupul $(\mathbb{Z}_n, +)$ este ciclic generat de $\hat{1}$, prin urmare ordinul lui $\hat{1}$ în acest grup este n.

2. Inelul $\mathbb{Z}$ are caracteristica zero, căci $n \cdot 1 \neq 0$, $\forall\, n \in \mathbb{N}^*$.

Propoziție

Un inel integru are caracteristica zero sau un număr prim.

Demonstrație. Vom arăta că în cazul când caracteristica este nenulă, aceasta este un număr prim. Fie, așadar, A un inel integru a cărui caracteristică este $n \geq 1$. Presupunem prin absurd că n nu este număr prim, deci $n = n_1 n_2$, unde $n_1, n_2 \in \mathbb{N}$, $1 < n_1 < n$, $1 < n_2 < n$. Folosind distributivitatea înmulțirii față de adunare și definiția caracteristicii, avem succesiv:

$$n \cdot 1 = 0 \Leftrightarrow (n_1 n_2) \cdot 1 = 0 \Leftrightarrow \underbrace{1 + 1 + \ldots + 1}_{n_1 n_2 \text{ ori}} = 0 \Leftrightarrow$$

$$\Leftrightarrow \underbrace{(\underbrace{1+1+\ldots+1}_{n_1 \text{ ori}}) + (\underbrace{1+1+\ldots+1}_{n_1 \text{ ori}}) + \ldots + (\underbrace{1+1+\ldots+1}_{n_1 \text{ ori}})}_{n_2 \text{ grupări}} = 0 \Leftrightarrow$$

$$\Leftrightarrow (\underbrace{1+1+\ldots+1}_{n_1 \text{ ori}})(\underbrace{1+1+\ldots+1}_{n_2 \text{ ori}}) = 0 \Leftrightarrow (n_1 \cdot 1)(n_2 \cdot 1) = 0.$$

Cum A este inel integru, rezultă $n_1 \cdot 1 = 0$ sau $n_2 \cdot 1 = 0$, ceea ce contrazice faptul că $n \in \mathbb{N}^*$ este cel mai mic cu proprietatea $n \cdot 1 = 0$.

Corpuri

Definiție

Se numește ***corp*** un triplet $(K, +, \cdot)$ în care K este o mulțime cu cel puțin două elemente, iar $+$ și $\cdot$ două operații pe K (numite „adunare" respectiv „înmulțire") satisfăcând trei axiome:

1°. $(K, +)$ este un grup abelian cu elementul neutru notat 0.

2°. $(K \setminus \{0\}, \cdot)$ este un grup cu elementul neutru notat 1.

3°. Înmulțirea este distributivă față de adunare, adică

$$x(y+z) = xy + xz \quad \text{și} \quad (y+z)x = yx + zx,\ \forall\, x, y, z \in K.$$

Grupul $(K, +)$ se numește ***grupul aditiv*** al corpului, iar grupul $(K \setminus \{0\}, \cdot)$ se numește ***grupul multiplicativ al elementelor nenule*** ale corpului.

Dacă, în plus, este satisfăcută și axioma a patra:

4°. Înmulțirea este comutativă (echivalent spus, în axioma 2° scriem „grup abelian"), atunci tripletul $(K, +, \cdot)$ se numește ***corp comutativ***.

Comparând cu definiţia inelului şi ţinând seama că într-un inel cu cel puţin două elemente, avem $0 \neq 1$, putem da următoarea:

Definiţie echivalentă

Se numeşte ***corp*** un inel $(K, +, \cdot)$ cu $0 \neq 1$ (echivalent spus, având cel puţin două elemente) în care orice element nenul este inversabil (echivalent spus, $U(K) = K \setminus \{0\}$).

Remarcă. Dacă operaţiile se subînţeleg, scriem corpul K, în loc de corpul $(K, +, \cdot)$.

Exemple de corpuri: corpuri numerice, corpul claselor de resturi modulo *p*, corpul cuartenionilor, corpuri de matrice

1. $(\mathbb{Q}, +, \cdot)$ este un corp comutativ, numit ***corpul numerelor raţionale***.

2. $(\mathbb{R}, +, \cdot)$ este un corp comutativ, numit ***corpul numerelor reale***.

3. $(\mathbb{C}, +, \cdot)$ este un corp comutativ, numit ***corpul numerelor complexe***.

4. Dacă $d \in \mathbb{Z}$ este un întreg care nu este pătrat perfect şi notăm

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$

unde $\sqrt{d}$ este o soluţie fixată în mulţimea $\mathbb{C}$ a ecuaţiei $x^2 = d$, atunci $(\mathbb{Q}(\sqrt{d}), +, \cdot)$ este un corp comutativ numit ***corp pătratic***. Într-adevăr, $(\mathbb{Q}(\sqrt{d}), +, \cdot)$ este un inel comutativ cu $0 \neq 1$ (verificarea axiomelor inelului comutativ poate constitui o temă simplă) şi în care orice element este inversabil, căci dacă $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d}) \setminus \{0\}$, atunci există numărul complex $\frac{1}{z}$ şi avem:

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

Corpul claselor de resturi modulo p

Printre inelele de clase de resturi $\mathbb{Z}_n$, cu $n \in \mathbb{N}$, $n \geq 2$, există unele care sunt corpuri. Ele sunt precizate de următorul rezultat:

Propoziţie

Inelul $(\mathbb{Z}_n, +, \cdot)$ al claselor de resturi modulo n este corp dacă şi numai dacă n este prim.

Demonstrație. Avem echivalențele succesive:

$(\mathbb{Z}_n, +, \cdot)$ este corp $\Leftrightarrow U(\mathbb{Z}_n) = \mathbb{Z}_n \setminus \{\hat{0}\} \Leftrightarrow \{\hat{k} \in \mathbb{Z}_n \mid (k, n) = 1\} = \{\hat{1}, \hat{2}, \ldots, \widehat{n-1}\}$

$\Leftrightarrow (k, n) = 1,\ \forall k \in \{1, 2, \ldots, n-1\} \Leftrightarrow n$ este prim.

Pentru $n = p$ = număr prim, corpul $(\mathbb{Z}_p, +, \cdot)$ se numește *corpul claselor de resturi modulo p*. Acest corp este finit.

Corpul cuaternionilor

Toate exemplele de corpuri date până aici au fost de corpuri comutative. Dăm acum un exemplu de corp necomutativ datorat lui R. Hamilton (1854).

Notăm cu $i \in \mathbb{C}$ unitatea imaginară și definim două obiecte matematice notate j, k, între care introducem o înmulțire (ce prelungește înmulțirea din $\mathbb{C}$) în felul următor:

$$i^2 = j^2 = k^2 = -1,\ \ ij = -ji = k,\ jk = -kj = i,\ \ ki = -ik = j.$$

Expresiile formale de tipul $a + bi + cj + dk$ cu $a,b,c,d \in \mathbb{R}$ se numesc *cuaternioni*. Notăm cu $\mathbb{H}$ mulțimea cuaternionilor și remarcăm incluziunea $\mathbb{C} \subseteq \mathbb{H}$, întrucât:

$$\forall z \in \mathbb{C},\ z = a + bi\ (a,b \in \mathbb{R}) \Rightarrow z = a + bi + 0j + 0k \in \mathbb{H}.$$

Pe mulțimea $\mathbb{H}$ definim operațiile de adunare și înmulțire în felul următor: dacă $q_1, q_2 \in \mathbb{H}$, $q_1 = a_1 + b_1 i + c_1 j + d_1 k$, $q_2 = a_2 + b_2 i + c_2 j + d_2 k$, unde $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in \mathbb{R}$ atunci:

$$q_1 + q_2 = (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k$$

iar $q_1\, q_2$ se obține după regula de distributivitate a înmulțirii față de adunare și regula de înmulțire a lui i, j, k între ei, adică:

$$q_1 q_2 = (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + a_2 b_1 + c_1 d_2 - c_2 d_1)i +$$
$$+ (a_1 c_2 - b_1 d_2 + a_2 c_1 + b_2 d_1)j + (a_1 d_2 + b_1 c_2 - b_2 c_1 + a_2 d_1)k.$$

Dacă $q = a + bi + cj + dk \in \mathbb{H}$, atunci $\overline{q} = a - bi - cj - dk \in \mathbb{H}$ se numește *conjugatul* lui q, iar numărul real pozitiv $N(q) = q\,\overline{q} = a^2 + b^2 + c^2 + d^2$ se numește *norma* cuaternionului q.

Rezultatul care evidențiază corpul necomutativ de care vorbeam, este următoarea:

Propoziție

Tripletul $(\mathbb{H}, +, \cdot)$ este un corp necomutativ numit ***corpul cuaternionilor***.

Demonstrație. Verificarea axiomelor inelului, deşi destul de laborioasă, nu este dificilă şi din lipsă de spaţiu o trecem cu titlu de temă în seama cititorilor. Vom verifica doar faptul că orice $q \in \mathbb{H}$, $q \neq 0$ este inversabil.

Deoarece $q = a + bi + cj + dk \neq 0$, înseamnă că măcar unul din numerele reale a, b, c, d este nenul şi atunci $N(q) = a^2 + b^2 + c^2 + d^2 > 0$.

Egalităţile $q\,\overline{q} = \overline{q}\,q = N(q)$ se scriu echivalent:

$$q \cdot \frac{\overline{q}}{N(q)} = \frac{\overline{q}}{N(q)} \cdot q = 1$$

şi arată că elementul (cuaternionul) q este inversabil, având inversul:

$$q^{-1} = \frac{\overline{q}}{N(q)} = \frac{a}{a^2+b^2+c^2+d^2} - \frac{b}{a^2+b^2+c^2+d^2}i - \frac{c}{a^2+b^2+c^2+d^2}j -$$

$$- \frac{d}{a^2+b^2+c^2+d^2}k \in \mathbb{H}.$$

Corpuri de matrice

Vom pune în evidenţă patru exemple de corpuri formate din matrice pătratice de ordinul 2, în raport cu operaţiile uzuale de adunare şi înmulţire a matricelor.

1. Fie $d \in \mathbb{Z} \setminus \{1\}$ un întreg care nu este pătrat perfect şi să considerăm mulţimea:

$$K = \left\{ \begin{pmatrix} a & b \\ db & a \end{pmatrix} \middle| \, a, b \in \mathbb{Q} \right\} \subseteq \mathcal{M}_2(\mathbb{Q}).$$

Atunci, tripletul $(K, +, \cdot)$ este un corp comutativ.

Este uşor să dovedim că mulţimea K este o parte stabilă faţă de adunare şi de înmulţire a mulţimii $\mathcal{M}_2(\mathbb{Q})$, iar axiomele structurii de inel comutativ se verifică imediat. Rămâne să mai dovedim că orice matrice nenulă din K este inversabilă în K. Pentru aceasta dovedim în prealabil că pentru o matrice $X \in K$ avem echivalenţa:

$$X = 0_2 \Leftrightarrow \det X = 0.$$

Implicaţia ($\Leftarrow$) se probează în felul următor: dacă $X = \begin{pmatrix} a & b \\ db & a \end{pmatrix}$ şi $\det X = 0$, adică $a^2 = db^2$, dacă am presupune $b \neq 0$ ar rezulta $d = \left(\frac{a}{b}\right)^2$, adică d ar fi pătrat perfect în $\mathbb{Q}$ şi cum $d \in \mathbb{Z}$, ar însemna că d este pătrat perfect în $\mathbb{Z}$, absurd; aşadar $b = 0$ şi atunci $a^2 = 0$, deci $a = 0$, prin urmare $X = 0_2$.

Implicaţia ($\Rightarrow$) este evidentă.

Fie atunci o matrice $X \in K \setminus \{0_2\}$. Rezultă, conform celor de mai sus, că $\det X \neq 0$, ceea ce arată că X este inversabilă în inelul de matrice $\mathscr{M}_2(\mathbb{Q})$. Ţinând seama de procedeul de determinare a matricei inverse găsim că $X^{-1} = \frac{1}{\det X}\begin{pmatrix} a & -b \\ -db & a \end{pmatrix} \in K$, ceea ce arată că X este inversabilă chiar în K.

2. Considerăm mulţimea $K = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \, a, b \in \mathbb{R} \right\} \subseteq \mathscr{M}_2(\mathbb{R})$.

Atunci, tripletul $(K, +, \cdot)$ este un corp comutativ.

Faptul că adunarea şi înmulţirea sunt operaţii pe K (echivalent spus, K este o partea lui $\mathscr{M}_2(\mathbb{R})$, stabilă faţă de adunare şi înmulţire), precum şi axiomele structurii de inel comutativ se verifică uşor.

Arătăm acum că orice matrice nenulă din K este inversabilă în K. Observăm, ca şi în cazul exemplului precedent, că pentru $X \in K$ avem echivalenţa:

$$X = 0_2 \Leftrightarrow \det X = 0.$$

Fie $X \in K \setminus \{0_2\}$, $X = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Atunci $\det X = a^2 + b^2 \neq 0$, deci X este inversabilă în inelul $\mathscr{M}_2(\mathbb{R})$ şi calculând inversa lui X, obţinem:

$$X^{-1} = \frac{1}{a^2+b^2}\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in K,$$

ceea ce arată că X este inversabilă în K.

3. Fie p un număr prim cu proprietatea că $-\hat{1}$ nu este pătrat perfect în corpul $(\mathbb{Z}_p, +, \cdot)$. Considerăm mulţimea de matrice cu elemente din $\mathbb{Z}_p$:

$$K = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \, a, b \in \mathbb{Z}_p \right\} \subseteq \mathscr{M}_2(\mathbb{Z}_p).$$

Atunci, $(K, +, \cdot)$ este un corp comutativ cu p^2 elemente.

Faptul că adunarea şi înmulţirea sunt operaţii pe K, precum şi axiomele inelului comutativ, se verifică uşor.

Dovedim acum că orice matrice nenulă din K este inversabilă în K.

Mai întâi dovedim aceeaşi echivalenţă:

$$X = 0_2 \Leftrightarrow \det X = \hat{0}.$$

Pentru implicaţia netrivială ($\Leftarrow$) avem: $\det X = \hat{0} \Leftrightarrow a^2 + b^2 = \hat{0}$ şi dacă $b \neq \hat{0}$, înmulţind cu $b^{-2} = (b^{-1})^2$ (care există în corpul $\mathbb{Z}_p$), ar rezulta $(ab^{-1})^2 = -\hat{1}$, deci $-\hat{1}$ ar fi pătrat în corpul $\mathbb{Z}_p$, absurd; aşadar $b = \hat{0}$, ceea ce duce la $a = \hat{0}$, prin urmare $X = 0_2$.

Atunci, pentru $X \in K \setminus \{0_2\}$ avem $\det X \neq \hat{0}$, deci X este inversabilă în inelul $\mathscr{M}_2(\mathbb{Z}_p)$, iar inversa sa este:

$$X^{-1} = (\det X)^{-1}\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in K,$$

adică X este inversabilă în K. Aşadar K este un corp şi acest corp are p^2 elemente, întrucât a şi b parcurg independent cele p elemente ale corpului $\mathbb{Z}_p$. (De exemplu, numerele prime $p = 3$, $p = 7$, $p = 11$ satisfac ipoteza că $-\hat{1}$ nu este pătrat perfect în $\mathbb{Z}_p$).

4. Considerăm mulţimea $K = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \middle| \, a, b \in \mathbb{C} \right\} \subseteq \mathcal{M}_2(\mathbb{C})$.

Atunci, tripletul $(K, +, \cdot)$ este un corp necomutativ. (Prin $\overline{z}$ înţelegem conjugatul numărului complex z).

Faptul că mulţimea K este o parte stabilă faţă de adunare şi înmulţire a mulţimii $\mathcal{M}_2(\mathbb{C})$, precum şi axiomele inelului, se verifică uşor.

Rămâne să dovedim şi aici că orice matrice nenulă din K este inversabilă în K. Dacă $X = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in K$, observăm că $\det X = a\,\overline{a} + b\,\overline{b} = |a|^2 + |b|^2$, ceea ce duce imediat la echivalenţa:

$$X = 0_2 \Leftrightarrow \det X = 0.$$

Atunci, dacă $X \in K \setminus \{0_2\}$, rezultă $\det X \neq 0$, deci X este inversabilă în inelul $\mathcal{M}_2(\mathbb{C})$. Calculând matricea inversă, găsim:

$$X^{-1} = \frac{1}{\det X}\begin{pmatrix} \overline{a} & -b \\ \overline{b} & a \end{pmatrix} \in K,$$

deci X este inversabilă în K. Corpul K este necomutativ căci luând de exemplu $X = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $Y = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ se constată uşor că $XY \neq YX$.

Observaţie

În toate exemplele tratate, a fost esenţială echivalenţa

$$X = 0_2 \Leftrightarrow \det X = 0.$$

Inele de matrice pătratice peste un inel comutativ

Fie A un inel comutativ; în particular, A poate fi un corp comutativ K. Numim *matrice pătratică de ordin n peste A* un tablou cu n linii şi n coloane cu elemente din A. Notăm cu $\mathcal{M}_n(A)$ mulţimea matricelor de ordin n peste inelul A. Pe mulţimea $\mathcal{M}_n(A)$ definim două operaţii: adunarea matricelor (după regula „element cu element") şi înmulţirea matricelor (după regula „linii pe coloane"). Fiecărei matrice

$X \in \mathcal{M}_n(A)$ îi asociem un element din inelul A notat $\det X$ şi numit ***determinantul*** matricei X, care se defineşte în felul următor:

$$\text{dacă } X = \left(a_{ij}\right)_{1\le i,j\le n}, \text{ atunci } \det X = \sum_{\sigma\in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}.$$

Toate proprietăţile determinanţilor pe care le-am studiat în clasa a XI-a în contextul particular când $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ rămân valabile în acest context general când A este un inel comutativ.

Cu aceeaşi demonstraţie pe care am făcut-o când am stabilit proprietăţile operaţiilor cu matrice peste $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ stabilim următorul rezultat:

Teoremă

Dacă A este un inel comutativ iar $n \in \mathbb{N}^*$, atunci:

1°. Tripletul $(\mathcal{M}_n(A), +, \cdot)$ este un inel, numit inelul matricelor pătratice de ordin n peste inelul A.

2°. Pentru $n \ge 2$ inelul $\mathcal{M}_n(A)$ este necomutativ şi are divizori ai lui zero.

Rezultatul următor precizează elementele inversabile din inelul $\mathcal{M}_n(A)$, iar demonstraţia acestuia este identică cu cea efectuată în clasa a XI-a pentru cazul particular $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Teoremă

Dacă A este un inel comutativ şi $n \in \mathbb{N}^*$, grupul elementelor inversabile din inelul $\mathcal{M}_n(A)$, numit ***grupul liniar de ordin n peste inelul A*** şi notat $GL_n(A)$ este format din acele matrice care au determinantul inversabil în inelul A, adică:

$$GL_n(A) = \{X \in \mathcal{M}_n(A) \mid \det X \in U(A)\}.$$

Corolar

Dacă $n \in \mathbb{N}^*$ şi K este un corp comutativ, grupul elementelor inversabile din inelul $\mathcal{M}_n(K)$ este:

$$GL_n(K) = \{X \in \mathcal{M}_n(K) \mid \det X \neq 0\}.$$

Observaţie

Construcţia matricei inverse X^{-1} este exact aceeaşi pe care am văzut-o în clasa a XI-a şi care conţine trei paşi: mai întâi se construieşte matricea transpusă, apoi matricea adjunctă X^* şi în final matricea inversă $X^{-1} = (\det X)^{-1} \cdot X^*$.

Exemple

1. Matricea $X \in \mathcal{M}_n(\mathbb{Z})$ este inversabilă în inelul $\mathcal{M}_n(\mathbb{Z})$ dacă şi numai dacă $\det X \in \{-1, 1\}$, deoarece $U(\mathbb{Z}) = \{-1, 1\}$.

2. Matricea $X = \begin{pmatrix} \hat{2} & \hat{1} \\ \hat{1} & \hat{3} \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}_6)$ este inversabilă, întrucât $\det X = \hat{5} \in U(\mathbb{Z}_6)$.

3. Matricea $X = \begin{pmatrix} \hat{1} & \hat{2} \\ \hat{3} & \hat{4} \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}_5)$ este inversabilă, întrucât $\det X = -\hat{2} \neq \hat{0}$, iar $\mathbb{Z}_5$ este corp comutativ.

Comentariu metodic

Toată teoria sistemelor liniare, construită în clasa a XI-a peste $\mathbb{R}$ sau peste $\mathbb{C}$, rămâne valabilă (cu aceleaşi demonstraţii) peste un corp comutativ arbitrar K. De exemplu se menţine regula lui Cramer (cu menţiunea că în corpul K „împărţirea" $\frac{a}{b}$ înseamnă produsul ab^{-1}), sunt valabile teoremele de caracterizare a sistemelor compatibile (teorema Kronecker-Capelli, teorema Rouché) etc. Anumite adaptări se pot face şi în cazul cel mai general când se lucrează peste un inel comutativ A. De exemplu, regula lui Cramer se menţine dacă determinantul matricei sistemului este un element inversabil în inelul A.

Legătura dintre corpuri şi inele integre

Primul rezultat în acest sens este următoarea:

Propoziţie

Orice corp este un inel integru, adică fără divizori ai lui zero.

Demonstraţie. Orice element nenul din corpul respectiv este inversabil, deci nu poate fi divizor al lui zero. Aşadar, corpul nu are divizori ai lui zero.

Observaţie

Reciproca acestei afirmaţii este falsă, după cum rezultă din următorul contraexemplu: $\mathbb{Z}$ este inel integru, dar nu este corp.

Consecinţă

Caracteristica unui corp este zero sau un număr prim.

Demonstrație. Se ține seama de faptul că orice corp este inel integru, iar caracteristica unui inel integru este zero sau un număr prim.

Exemplu

Corpurile $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\sqrt{d})$, $\mathbb{H}$ au caracteristica zero, iar corpul $\mathbb{Z}_p$ (p prim) are caracteristica p.

În cazul inelelor finite este adevărată și reciproca ultimei propoziții. Avem așadar următoarea:

Propoziție

Fie A un inel finit cu $0 \neq 1$. Următoarele afirmații sunt echivalente:

1°. A este corp.

2°. A este inel integru.

Demonstrație. 1° $\Rightarrow$ 2°. Evidentă, conform propoziției precedente.

2° $\Rightarrow$ 1°. Presupunem că A este inel integru finit. Pentru a arăta că A este un corp, vom arăta că orice element nenul din A este inversabil în A.

Fie $a \in A$, $a \neq 0$, fixat. Considerăm funcția $f_a : A \to A$, $f_a(x) = ax$, care este injectivă. Într-adevăr: $f_a(x_1) = f_a(x_2) \Leftrightarrow ax_1 = ax_2 \Leftrightarrow x_1 = x_2$, deoarece într-un inel integru putem simplifica la stânga printr-un element nenul. Cum A este finit, rezultă că f_a este bijecție. Atunci $\exists\, b' \in A$ cu $f_a(b') = 1$, adică $ab' = 1$, deci a este inversabil „la dreapta". Analog funcția $g_a : A \to A$, $g_a(x) = xa$ este injectivă, deci bijectivă și atunci $\exists\, b'' \in A$ cu $g_a(b'') = 1$, adică $b''a = 1$, deci a este inversabil „la stânga". Dar atunci a este inversabil, căci inversul la stânga b'' este egal cu inversul la dreapta b', ceea ce se arată astfel:

$$b'' = b'' \cdot 1 = b''(ab') = (b''a)b' = 1b' = b'.$$

Comentariu metodic

Propoziția de mai înainte nu presupune neapărat comutativitatea inelului A. În realitate însă, lucrurile stau puțin altfel, mai precis, cadrul în care „funcționează" rezultatul precedent este cel al inelelor comutative. Aceasta, întrucât există un rezultat frumos, numit teorema lui Wedderburn, care afirmă că ***orice corp finit este comutativ***, dar care nu poate fi demonstrat în acest manual.

Exerciții rezolvate

1. Pe mulțimea $\mathbb{Z}$ definim operațiile:

$x \oplus y = x + y + a$; $x \odot y = (x + a)(y + a) - a$, unde $a \in \mathbb{Z}$ este un număr fixat.

Să se arate că tripletul $(\mathbb{Z}, \oplus, \odot)$ este un inel comutativ fără divizori ai lui zero (domeniu de integritate) şi să se determine grupul elementelor inversabile din acest inel.

Soluție. Verificăm axiomele inelului comutativ.

1°. $(\mathbb{Z}, \oplus)$ este grup abelian. Într-adevăr:

– operația $\oplus$ este asociativă, întrucât:

$(x \oplus y) \oplus z = (x+y+a) \oplus z = (x+y+a)+z+a = x+y+z+2a$,

$x \oplus (y \oplus z) = x \oplus (y+z+a) = x+(y+z+a)+a = x+y+z+2a$, deci

$(x \oplus y) \oplus z = x \oplus (y \oplus z)$, $\forall\, x,y,z \in \mathbb{Z}$.

– operația $\oplus$ este comutativă, întrucât:

$x \oplus y = x+y+a = y+x+a = y \oplus x$, $\forall\, x,y \in \mathbb{Z}$.

– operația $\oplus$ are un element neutru $\mathbf{0} \in \mathbb{Z}$, căci:

$x \oplus \mathbf{0} = x$, $\forall\, x \in \mathbb{Z} \Leftrightarrow x + \mathbf{0} + a = x$, $\forall\, x \in \mathbb{Z}$, deci $\mathbf{0} = -a \in \mathbb{Z}$.

– orice $x \in \mathbb{Z}$ este simetrizabil față de operația $\oplus$, deoarece:

$x \oplus x' = \mathbf{0} \Leftrightarrow x + x' + a = -a \Leftrightarrow x' = -x - 2a \in \mathbb{Z}$.

2°. $(\mathbb{Z}, \odot)$ este un monoid comutativ. Într-adevăr:

– operația $\odot$ este asociativă, întrucât:

$(x \odot y) \odot z = ((x+a)(y+a)-a) \odot z = ((x+a)(y+a)-a+a)(z+a)-a =$
$= (x+a)(y+a)(z+a)-a$, iar

$x \odot (y \odot z) = x \odot \big((y+a)(z+a)-a\big) = (x+a)\big((y+a)(z+a)-a+a\big)-a =$
$= (x+a)(y+a)(z+a)-a$, prin urmare

$(x \odot y) \odot z = x \odot (y \odot z)$, $\forall\, x,y,z \in \mathbb{Z}$.

– operația $\odot$ este comutativă, întrucât:

$x \odot y = (x+a)(y+a)-a = (y+a)(x+a)-a = y \odot x$, $\forall\, x,y \in \mathbb{Z}$.

– operația $\odot$ are element – unitate $\mathbf{1} \in \mathbb{Z}$, căci avem:

$x \odot \mathbf{1} = x$, $\forall\, x \in \mathbb{Z} \Leftrightarrow (x+a)(\mathbf{1}+a) - a = x$, $\forall\, x \in \mathbb{Z} \Leftrightarrow$

$\Leftrightarrow (x+a)(\mathbf{1}+a) = x+a$, $\forall\, x \in \mathbb{Z} \Leftrightarrow \mathbf{1}+a = 1 \Leftrightarrow \mathbf{1} = 1-a \in \mathbb{Z}$.

3°. „Înmulțirea” $\odot$ este distributivă față de „adunare” $\oplus$. Într-adevăr:

$x \odot (y \oplus z) = x \odot (y+z+a) = (x+a)(y+z+a+a)-a = (x+a)(y+z+2a)-a$

iar $(x \odot y) \oplus (x \odot z) = \big((x+a)(y+a)-a\big) \oplus \big((x+a)(z+a)-a\big) =$
$= (x+a)(y+a)-a+(x+a)(z+a)-a+a = (x+a)(y+z+2a)-a$,

prin urmare $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$, $\forall\, x,y,z \in \mathbb{Z}$.

Deoarece operația $\odot$ este comutativă, vom avea şi egalitatea:

$(y \oplus z) \odot x = (y \odot x) \oplus (z \odot x)$, $\forall\, x,y,z \in \mathbb{Z}$.

Rezultă că $\odot$ este distributivă față de $\oplus$.

Am arătat în acest fel că $(\mathbb{Z}, \oplus, \odot)$ este un inel comutativ.

Pentru a arăta că în acest inel nu există divizori ai lui zero, revine la a dovedi că

$$x \odot y = \mathbf{0} \Rightarrow x = \mathbf{0} \text{ sau } y = \mathbf{0}.$$

Într-adevăr $x \odot y = \mathbf{0} \Rightarrow (x+a)(y+a) - a = -a \Leftrightarrow (x+a)(y+a) = 0 \Leftrightarrow$

$$\Leftrightarrow x = -a = \mathbf{0} \text{ sau } y = -a = \mathbf{0}.$$

Aşadar, $(\mathbb{Z}, \oplus, \odot)$ este un domeniu de integritate.

Determinăm acum grupul $(U(\mathbb{Z}), \odot)$ al elementelor inversabile din acest inel. Avem succesiv:

$$x \in U(\mathbb{Z}) \Leftrightarrow \exists\ x^{-1} \in \mathbb{Z} \text{ cu } x \odot x^{-1} = \mathbf{1} \Leftrightarrow (x+a)(x^{-1}+a) - a = 1 - a \Leftrightarrow$$

$$\Leftrightarrow (x+a)(x^{-1}+a) = 1 \Leftrightarrow (x+a) \mid 1 \Leftrightarrow x + a \in \{-1, 1\} \Leftrightarrow x \in \{-1-a,\ 1-a = \mathbf{1}\}.$$

Aşadar $U(\mathbb{Z}) = \{-1-a,\ 1-a\}$, deci grupul unităţilor inelului $(\mathbb{Z}, \oplus, \odot)$ este un grup ciclic de ordinul 2.

Să remarcăm că pentru $a = 0$ inelul $(\mathbb{Z}, \oplus, \odot)$ coincide cu inelul obişnuit $(\mathbb{Z}, +, \cdot)$.

2. Fie A o mulţime nevidă, iar $+$ şi $\cdot$ două operaţii care verifică axiomele:

1°. $(A, +)$ este grup.

2°. $(A, \cdot)$ este monoid.

3°. „Înmulţirea" $\cdot$ este distributivă faţă de „adunarea" $+$.

Să se arate că adunarea este comutativă, deci tripletul $(A, +, \cdot)$ este un inel.

Soluţie. Fie $x, y \in A$ arbitrare. Utilizând distributivitatea înmulţirii faţă de adunare, vom calcula produsul $(1+1)(x+y)$ în două moduri. Avem:

$(1+1)(x+y) = (1+1)x + (1+1)y = x + x + y + y$, iar pe de altă parte

$(1+1)(x+y) = 1(x+y) + 1(x+y) = x + y + x + y$.

Rezultă $x+x+y+y = x+y+x+y$ şi dacă în grupul $(A, +)$ adunăm la stânga $-x$ şi la dreapta $-y$, egalitatea precedentă devine $x + y = y + x$, adică $+$ este comutativă.

Comentariu metodic

Exerciţiul precedent arată că în definiţia inelului axioma „$(A, +)$ este un grup abelian" se poate înlocui cu axioma mai slabă „$(A, +)$ este un grup". Riguros vorbind, aşa ar fi cazul să definim inelul, pentru că într-un sistem axiomatic axiomele trebuie să fie „minimale", să nu poată fi dedusă vreuna din ele pe baza altora.

Totuşi, din punct de vedere didactic, se preferă axioma mai tare conform căreia $(A, +)$ este un grup abelian.

EXERCIȚII PROPUSE

1. Pe mulțimea $\mathbb{Z}$ definim operațiile $x \oplus y = x + y + 1$, $x \odot y = xy + x + y$. Arătați că $(\mathbb{Z}, \oplus, \odot)$ este un inel comutativ fără divizori ai lui zero şi determinați grupul elementelor inversabile din acest inel.

2. Pe mulțimea $\mathbb{Z}$ definim operațiile $x \oplus y = x + y - 1$, $x \odot y = xy - x - y + 2$. Arătați că $(\mathbb{Z}, \oplus, \odot)$ este un inel comutativ fără divizori ai lui zero şi determinați grupul elementelor inversabile din acest inel.

3. Fie $\zeta = \dfrac{1+i\sqrt{3}}{2}$ şi $\mathbb{Z}[\zeta] = \{a + b\zeta \mid a,b \in \mathbb{Z}\}$. Arătați că:

   a) $\zeta^2 + \zeta + 1 = 0$.

   b) $\mathbb{Z}[\zeta]$ este o parte a lui $\mathbb{C}$ stabilă față de adunare şi înmulțire, iar $(\mathbb{Z}[\zeta], +, \cdot)$ este inel comutativ fără divizori ai lui zero.

   c) Grupul elementelor inversabile din inelul $\mathbb{Z}[\zeta]$ este $(U_6, \cdot)$.

4. Pe mulțimea $\mathbb{Z}[i] = \{a + bi \mid a,b \in \mathbb{Z}\}$ definim operația $*$ prin:

$$(a_1 + b_1 i) * (a_2 + b_2 i) = a_1 a_2 + (a_1 b_2 + a_2 b_1) i, \ \forall\ a_1, a_2, b_1, b_2 \in \mathbb{Z}.$$

   a) Arătați că $(\mathbb{Z}[i], +, *)$ este un inel comutativ cu divizori ai lui zero.

   b) Determinați grupul elementelor inversabile din inelul $(\mathbb{Z}[i], +, *)$.

5. Fie $A = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| \ a, b \in \mathbb{Z} \right\}$. Arătați că $(A, +, \cdot)$ este un inel comutativ cu divizori ai lui zero.

6. Fie $d \in \mathbb{Z}$ fixat şi mulțimea de matrice: $A = \left\{ \begin{pmatrix} a & b \\ db & a \end{pmatrix} \middle| \ a, b \in \mathbb{Z} \right\} \subseteq \mathcal{M}_2(\mathbb{Z})$.

   a) Demonstrați că tripletul $(A, +, \cdot)$ este un inel comutativ.

   b) Arătați că inelul $(A, +, \cdot)$ are divizori ai lui zero dacă şi numai dacă d este pătrat perfect.

   c) Determinați grupul $(U(A), \cdot)$ în fiecare din cazurile $d = 0$, $d = -1$, $d \leq -2$.

7. Fie $A = \left\{ \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \middle| \ a, b, c \in \mathbb{Z} \right\}$.

   a) Demonstrați că $(A, +, \cdot)$ este un inel comutativ.

b) Arătați că matricele $X=\begin{pmatrix}1&1&1\\1&1&1\\1&1&1\end{pmatrix}$, $Y=\begin{pmatrix}1&1&-2\\-2&1&1\\1&-2&1\end{pmatrix}$ sunt divizori ai lui zero în inelul A.

c) Demonstrați că grupul elementelor inversabile din acest inel este:

$$U(A)=\left\{\pm\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix};\pm\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix};\pm\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\right\}.$$

8. Fie $A=\left\{\begin{pmatrix}a&b&c\\0&a&d\\0&0&a\end{pmatrix}\,\middle|\, a,b,c,d\in\mathbb{R}\right\}$. Arătați că $(A, +, \cdot)$ este un inel necomutativ cu divizori ai lui zero.

9. Fie $A=\{f:\mathbb{R}\to\mathbb{R}\mid f \text{ continuă}\}$. Arătați că:

a) $(A, +, \cdot)$ este un inel comutativ.

b) Dacă $f\in A,\ f\neq 0$, există echivalența:

f este divizor al lui zero $\Leftrightarrow$ f se anulează pe un interval (neredus la un punct).

10. Pe mulțimea $K=(0,\infty)$ definim operațiile $\oplus$ și $\odot$ prin $x\oplus y=xy$ respectiv $x\odot y=x^{\ln y}$. Arătați că tripletul $(K, \oplus, \odot)$ este un corp comutativ.

11. Pe intervalul $K=\left(-\frac{\pi}{2},\frac{\pi}{2}\right)$ definim operațiile:

$$x\oplus y=\operatorname{arctg}(\operatorname{tg}x+\operatorname{tg}y),\quad x\odot y=\operatorname{arctg}(\operatorname{tg}x\cdot\operatorname{tg}y).$$

Demonstrați că tripletul $(K, \oplus, \odot)$ este un corp comutativ.

12. Pe mulțimea $K=\mathbb{Q}\times\mathbb{Q}$ definim „adunarea" și „înmulțirea" astfel:

$$(x_1, y_1)+(x_2, y_2)=(x_1+x_2, y_1+y_2),\quad (x_1, y_1)(x_2, y_2)=(x_1x_2-y_1y_2, x_1y_2+x_2y_1).$$

Demonstrați că tripletul $(K, +, \cdot)$ este un corp comutativ.

13. Pe mulțimea $K=\mathbb{Z}_3\times\mathbb{Z}_3$ definim „adunarea" și „înmulțirea" prin:

$$(x_1, y_1)+(x_2, y_2)=(x_1+x_2, y_1+y_2),\quad (x_1, y_1)(x_2, y_2)=(x_1x_2-y_1y_2, x_1y_2+x_2y_1).$$

Demonstrați că tripletul $(K, +, \cdot)$ este un corp comutativ cu 9 elemente.

14. Fie $K=\left\{\begin{pmatrix}a+b&b\\b&a-b\end{pmatrix}\,\middle|\, a,b\in\mathbb{Q}\right\}$. Demonstrați că tripletul $(K, +, \cdot)$ este un corp comutativ.

15. Fie $K=\{0_2, I_2, X, Y\}\subseteq \mathcal{M}_2(\mathbb{Z}_2)$, unde

$$0_2=\begin{pmatrix}\hat{0} & \hat{0}\\ \hat{0} & \hat{0}\end{pmatrix},\ I_2=\begin{pmatrix}\hat{1} & \hat{0}\\ \hat{0} & \hat{1}\end{pmatrix},\ X=\begin{pmatrix}\hat{0} & \hat{1}\\ \hat{1} & \hat{1}\end{pmatrix},\ Y=\begin{pmatrix}\hat{1} & \hat{1}\\ \hat{1} & \hat{0}\end{pmatrix}.$$

Scrieţi tabla adunării şi înmulţirii pe mulţimea K şi demonstraţi că tripletul $(K, +, \cdot)$ este un corp comutativ cu 4 elemente.

16. Pentru fiecare $a \in \mathbb{Q}$ definim funcţia $f_a : \mathbb{Q} \to \mathbb{Q}$, $f_a(x) = ax$ şi considerăm mulţimea $K = \{f_a \mid a \in \mathbb{Q}\}$. Arătaţi că tripletul $(K, +, \circ)$ este un corp comutativ. (Prin $\circ$ am notat compunerea funcţiilor).

17. Pentru fiecare $a \in \mathbb{Q}$ definim funcţia $f_a : \mathbb{R} \to \mathbb{R}$ prin $f_a(x)=\begin{cases} ax, & \text{dacă } x\in\mathbb{Q}\\ 0, & \text{dacă } x\in\mathbb{R}\setminus\mathbb{Q}\end{cases}$

şi considerăm mulţimea $K = \{f_a \mid a \in \mathbb{Q}\}$. Arătaţi că tripletul $(K, +, \circ)$ este un corp comutativ. (Prin $\circ$ am notat compunerea funcţiilor).

18. Fie $K=\left\{\begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix} \middle|\ a\in\mathbb{Q}\right\}$.

a) Arătaţi că tripletul $(K, +, \cdot)$ este un corp comutativ.

b) Explicaţi faptul că, deşi matricele din K sunt inversabile faţă de înmulţire în corpul K, ele au determinantul nul.

19. Considerăm următoarele matrice din $\mathcal{M}_2(\mathbb{C})$:

$$e_0=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix};\ e_1=\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix};\ e_2=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix};\ e_3=\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$$

şi mulţimea $K=\{\lambda_0 e_0+\lambda_1 e_1+\lambda_2 e_2+\lambda_3 e_3 \mid \lambda_0,\lambda_1,\lambda_2,\lambda_3\in\mathbb{R}\}$. De asemenea pentru $x \in K$, $x=\lambda_0 e_0+\lambda_1 e_1+\lambda_2 e_2+\lambda_3 e_3$, notăm $x^*=\lambda_0 e_0-\lambda_1 e_1-\lambda_2 e_2-\lambda_3 e_3$ şi $|x|=\sqrt{\lambda_0^2+\lambda_1^2+\lambda_2^2+\lambda_3^2}$. Arătaţi că:

a) $xx^*=x^*x=|x|^2 e_0$, $\forall x \in K$.

b) $(K, +, \cdot)$ este un corp necomutativ.

c) Ce legătură există între acest corp şi corpul din exemplul 4 de la pg. 70?

Subinele. Subcorpuri (extindere)

Dacă privim inelele $(\mathbb{Z}, +, \cdot)$ şi $(\mathbb{Z}[i], +, \cdot)$, constatăm că primul inel este inclus în al doilea, iar operaţiile din $\mathbb{Z}$ sunt induse de operaţiile din $\mathbb{Z}[i]$. Mai mult, elementul–unitate din cele două inele este acelaşi şi anume $1 = 1 + 0i$.

De asemenea, dacă observăm corpurile $(\mathbb{Q}, +, \cdot)$ şi $(\mathbb{R}, +, \cdot)$, constatăm că primul corp este inclus în al doilea, operaţiile din $\mathbb{Q}$ sunt induse de cele din $\mathbb{R}$, iar elementul–unitate este acelaşi.

Suntem conduşi la următoarea:

Definiţie

Fie $(A, +, \cdot)$ un inel şi B o submulţime nevidă a lui A.

Spunem că B este un ***subinel*** al lui A dacă B este parte stabilă faţă de operaţiile din A, mulţimea B împreună cu operaţiile induse este un (nou) inel, iar elementul–unitate din B coincide cu elementul–unitate din A.

Exemple

1. $(\mathbb{Z}, +, \cdot)$ este un subinel al lui $(\mathbb{Z}[i], +, \cdot)$.

2. $(\mathbb{Z}, +, \cdot)$ este un subinel al lui $(\mathbb{Q}, +, \cdot)$.

3. $(\mathcal{M}_n(\mathbb{Z}), +, \cdot)$ este un subinel al lui $(\mathcal{M}_n(\mathbb{Q}), +, \cdot)$.

4. Mulţimea $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| \, a \in \mathbb{Z} \right\} \subseteq \mathcal{M}_2(\mathbb{Z})$ este o parte stabilă faţă de adunarea şi înmulţirea din $\mathcal{M}_2(\mathbb{Z})$, deoarece:

$$\begin{pmatrix} a_1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a_2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & 0 \\ 0 & 0 \end{pmatrix}; \quad \begin{pmatrix} a_1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a_2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & 0 \\ 0 & 0 \end{pmatrix}.$$

De asemenea, $(A, +, \cdot)$ este un inel (ceea ce se poate verifica uşor ca temă) în care elementul–unitate este $1_A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

Totuşi $(A, +, \cdot)$ nu este subinel al inelului $(\mathcal{M}_2(\mathbb{Z}), +, \cdot)$, întrucât elementul–unitate din $\mathcal{M}_2(\mathbb{Z})$ este $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \neq 1_A$.

Observaţie

Dacă B este un subinel al inelului A, rezultă că grupul $(B, +)$ este subgrup al grupului $(A, +)$ şi de aici rezultă (conform lemei de la pag. 28) că elementul nul al inelului B coincide cu elementul nul al inelului A.

Rezultatul care urmează precizează o condiție necesară și suficientă ca o submulțime a unui inel să fie subinel.

Teoremă

Fie $(A, +, \cdot)$ un inel cu element–unitate 1_A iar B o submulțime nevidă a lui A. Următoarele afirmații sunt echivalente:

$1°$. B este un subinel al lui A.

$2°$. $1_A \in B$ și $\forall\, x,y \in B \Rightarrow x - y \in B$ și $xy \in B$.

Demonstrație. $1° \Rightarrow 2°$. Presupunem că B este un subinel al lui A. Atunci B este o parte stabilă față de operațiile lui A, iar tripletul $(B, +, \cdot)$ este un inel care are drept element–unitate pe 1_A. Rezultă că $1_A \in B$, iar din faptul că $(B, +)$ este un subgrup rezultă că $\forall\, x,y \in B \Rightarrow x - y \in B$.

În fine, cum B este parte stabilă față de înmulțire avem:

$$\forall\, x,y \in B \Rightarrow xy \in B.$$

$2° \Rightarrow 1°$. Presupunem că $1_A \in B$ și $\forall\, x,y \in B \Rightarrow x - y \in B$ și $xy \in B$.

Cum $1_A \in B$, rezultă 1_A este element–unitate și pentru înmulțirea din B. Deoarece $\forall\, x,y \in B \Rightarrow x - y \in B$, înseamnă că $(B, +)$ este un subgrup al grupului abelian
$(A, +)$, deci $(B, +)$ este un grup abelian. Deoarece $\forall\, x,y \in B \Rightarrow xy \in B$, înseamnă că $(B, \cdot)$ este un monoid cu elementul–unitate 1_A.

În fine, înmulțirea este distributivă față de adunare pe mulțimea B și aceasta arată că $(B, +, \cdot)$ este un inel, adică în fond, B este un subinel al lui A.

Definiție

Fie $(K, +, \cdot)$ un corp și L o submulțime nevidă a lui K.

Spunem că L este un ***subcorp*** al lui K dacă L este o parte stabilă față de operațiile din K și împreună cu operațiile induse este un corp.

Exemple

1. $(\mathbb{Q}, +, \cdot)$ este un subcorp al lui $(\mathbb{R}, +, \cdot)$.

2. $(\mathbb{R}, +, \cdot)$ este un subcorp al lui $(\mathbb{C}, +, \cdot)$.

3. Corpul pătratic $\left(\mathbb{Q}(\sqrt{d}), +, \cdot\right)$ cu $d \in \mathbb{Z}$, nepătrat perfect, este un subcorp al lui $(\mathbb{C}, +, \cdot)$, iar când $d > 0$ este un subcorp al lui $(\mathbb{R}, +, \cdot)$.

Observații

1. Remarcăm că $(L, +, \cdot)$ este un subcorp al unui corp $(K, +, \cdot)$ dacă și numai dacă $(L, +)$ este un subgrup al grupului $(K, +)$, iar $(L^*, \cdot)$ este un subgrup al grupului $(K^*, \cdot)$, unde am notat $L^* = L \setminus \{0_L\}$, $K^* = K \setminus \{0_K\}$. Rezultă, în particular, că elementele nule din L și K coincid și, de asemenea elementele unitate din L și K

coincid, adică $0_L = 0_K$ şi $1_L = 1_K$.

2. Dacă L este un subcorp al corpului K, atunci L este un subinel al lui K. Reciproca nu este adevărată, conform cu următorul contraexemplu: $\mathbb{Z}$ este subinel al *lui $\mathbb{Q}$, dar nu este subcorp, căci $\mathbb{Z}$ nu este un corp.*

Următorul rezultat precizează o condiţie necesară şi suficientă ca o submulţime a unui corp să fie subcorp.

Teoremă

Fie $(K, +, \cdot)$ un corp şi L o submulţime nevidă a lui K. Următoarele afirmaţii sunt echivalente:

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

2°. $\forall\, x,y \in L \Rightarrow x - y \in L$ şi $\forall\, x,y \in L^* \Rightarrow xy^{-1} \in L^*$.

Demonstraţie. Se ţine seama de observaţia precedentă 1 şi de teorema de caracterizare a subgrupurilor unui grup, adică de condiţia necesară şi suficientă ca o submulţime a unui grup să fie subgrup.

Exerciţii rezolvate

1. Fie $d \in \mathbb{Z} \setminus \{1\}$ un întreg nepătrat perfect şi mulţimea:

$$A = \left\{ \begin{pmatrix} a & b \\ db & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{Z} \right\} \subseteq \mathcal{M}_2(\mathbb{Z}).$$

Să se arate că $(A, +, \cdot)$ este un subinel comutativ al inelului $(\mathcal{M}_2(\mathbb{Z}), +, \cdot)$.

Soluţie. Arătăm că $\forall\ X_1, X_2 \in A \Rightarrow X_1 - X_2 \in A,\ X_1X_2 \in A$ şi $I_2 \in A$.

Fie într-adevăr $X_1 = \begin{pmatrix} a_1 & b_1 \\ db_1 & a_1 \end{pmatrix}$, $X_2 = \begin{pmatrix} a_2 & b_2 \\ db_2 & a_2 \end{pmatrix}$ două matrice arbitrare, unde $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Avem:

$$X_1 - X_2 = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ d(b_1 - b_2) & a_1 - a_2 \end{pmatrix} \in A \text{ şi } X_1X_2 = \begin{pmatrix} a_1a_2 + db_1b_2 & a_1b_2 + a_2b_1 \\ d(a_1b_2 + a_2b_1) & a_1a_2 + db_1b_2 \end{pmatrix} \in A.$$

De asemenea, $I_2 \in A$, căci matricea – unitate se obţine pentru $a = 1,\ b = 0$.

Rezultă că $(A, +, \cdot)$ este un subinel al inelului $(\mathcal{M}_2(\mathbb{Z}), +, \cdot)$.

Constatăm cu uşurinţă că $X_1X_2 = X_2X_1$, deci A este un subinel comutativ al lui $\mathcal{M}_2(\mathbb{Z})$.

2. Fie $K = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \,\middle|\, a \in \mathbb{R} \right\} \subseteq \mathcal{M}_2(\mathbb{R})$.

a) Să se arate că tripletul $(K, +, \cdot)$ este un corp comutativ.

b) Deşi matricele nenule din K sunt inversabile, ele au determinantul nul.

Cum se explică aceasta?

Soluție. a) Observăm ușor „regulile" de adunare și înmulțire în K:

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+b & 0 \\ 0 & 0 \end{pmatrix}; \quad \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}.$$

Verificarea axiomelor corpului comutativ este simplă și poate trece drept temă.

Atragem atenția doar asupra unor aspecte și anume: elementul nul este matricea $0_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, elementul–unitate este matricea $E = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, iar inversa unei matrice nenule $X = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in K$ este $X^{-1} = \begin{pmatrix} \frac{1}{a} & 0 \\ 0 & 0 \end{pmatrix} \in K.$

b) Corpul K și inelul $\mathcal{M}_2(\mathbb{R})$ au elementele–unitate distincte și anume E, respectiv I_2. Prin urmare K nu este subinel al lui $\mathcal{M}_2(\mathbb{R})$, ca atare inversabilitatea din K nu are nici o legătură cu inversabilitatea din $\mathcal{M}_2(\mathbb{R})$. Așa se face că matricele inversabile din K (și anume cele nenule) au determinantul nul, deci nu sunt inversabile în $\mathcal{M}_2(\mathbb{R})$.

Comentariu metodic

Exercițiul precedent arată că atunci când vorbim de „elemente inversabile" trebuie precizată structura algebrică în care gândim inversabilitatea acestor elemente.

Când spunem în mod obișnuit *o matrice X este inversabilă dacă și numai dacă* $\det X \neq 0$, gândim (subînțelegem) inversabilitatea în inelul $\mathcal{M}_n(\mathbb{C})$. Dacă schimbăm inelul (ca în exercițiul precedent) un astfel de enunț poate să-și piardă valabilitatea.

Morfisme și izomorfisme de inele și de corpuri

Ca și la grupuri, ne propunem să studiem legături între diferite inele sau corpuri.

Definiție

Fie $(A, +, \cdot)$ și $(A', +, \cdot)$ două inele. O funcție $f : A \to A'$ cu proprietățile:

1°. $f(x + y) = f(x) + f(y),\ \forall\, x,y \in A$

2°. $f(xy) = f(x)f(y),\ \forall\, x,y \in A$

3°. $f(1_A) = 1_{A'}$

se numește ***morfism de inele***.

Un morfism de la un inel la el însuși se numește ***endomorfism*** al inelului respectiv.

Comentariu metodic

Dacă din definiția precedentă excludem condiția 3°, spunem că avem un morfism de inele *„**neunitar**”*. Totuşi, pentru comoditatea tratării nu ne vom întâlni pe parcursul acestui manual cu astfel de morfisme, aşa că *din punct de vedere didactic preferăm definiția cu toate cele trei condiții.*

De asemenea este cazul să remarcăm că, pentru uşurința scrierii, am notat în definiția de mai sus ambele „adunări” cu + şi ambele „înmulțiri” cu $\cdot$, deşi este limpede că în general operațiile din cele două inele sunt distincte. În egalitățile 1° şi 2° din definiția precedentă operațiile $x + y$ şi xy se efectuează în inelul A, în timp ce operațiile $f(x) + f(y)$ şi $f(x)f(y)$ se efectuează în inelul A'.

Observație

Dacă $f : (A, +, \cdot) \to (A', +, \cdot)$ este un morfism de inele, atunci $f : (A, +) \to (A', +)$ este morfism de grupuri abeliene. În particular, rezultă $f(0_A) = 0_{A'}$, $f(-x) = -f(x)$, $\forall\, x \in A$ şi $f(nx) = nf(x)$, $\forall\, x \in A$, $\forall\, n \in \mathbb{Z}$.

Exemple

1. Funcția $f : (\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_n, +, \cdot)$, $f(x) = \hat{x}$ este un morfism de inele, numit ***morfismul canonic*** ($n \in \mathbb{N}$, $n \geq 2$).

2. Funcția $f : (\mathbb{Z}, +, \cdot) \to (A, +, \cdot)$, $f(x) = n \cdot 1_A$ este un morfism de inele (A fiind un inel oarecare).

3. Dacă B este un subinel al inelului A, funcția $f : B \to A$, $f(x) = x$ este un morfism de inele, numit ***morfismul–incluziune***.

4. Dacă A şi A' sunt două inele oarecare, cu $0_A \neq 1_A$ şi $0_{A'} \neq 1_{A'}$, funcția $f : A \to A'$, $f(x) = 0_{A'}$ este un morfism de inele, numit ***morfismul nul***; acest morfism este unul „neunitar”.

Verificările sunt imediate şi pot fi privite drept teme pentru elevi.

Un alt rezultat, întrucâtva analog celui de la pag. 44, este dat de următoarea:

Teoremă

Fie $f : (A, +, \cdot) \to (A', +, \cdot)$ un morfism de inele. Atunci:

1°. Mulțimea $\text{Ker } f = \{x \in A \mid f(x) = 0_A\}$ este un subgrup al grupului $(A, +)$ (numit ***nucleul*** morfismului f) care are proprietatea:

$$\forall\, x \in \text{Ker } f,\ \forall\, a \in A \Rightarrow ax,\ xa \in \text{Ker } f.$$

2°. Morfismul f este injectiv dacă şi numai dacă $\text{Ker } f = \{0_A\}$.

Demonstrație. 1°. Deoarece f este un morfism de inele, rezultă că $f : (A, +) \to (A', +)$

este şi un morfism de grupuri abeliene. Atunci, după cum ştim de la grupuri, rezultă că mulţimea Ker f este un subgrup al grupului $(A, +)$.

Fie acum $x \in \operatorname{Ker} f$, $a \in A$ arbitrare şi să arătăm că $ax, xa \in \operatorname{Ker} f$.

Într-adevăr: $f(ax) = f(a)f(x) = f(a)0_{A'} = 0_{A'}$ şi $f(xa) = f(x)f(a) = 0_{A'}f(a) = 0_{A'}$.

2°. Se utilizează rezultatul corespunzător de la morfismele de grupuri.

Comentariu metodic

O submulţime I a unui inel A, cu proprietatea că I este subgrup al grupului $(A, +)$ şi $\forall\, x \in I$, $\forall\, a \in A \Rightarrow ax, xa \in I$ se numeşte ***ideal bilateral*** al inelului A. Prin urmare, punctul 1° din teoremă afirmă că nucleul unui morfism de inele este un ideal bilateral al inelului domeniu de definiţie. În cadrul inelelor comutative fără divizori ai lui zero se poate dezvolta o teorie aritmetică a idealelor.

Definiţie

1) Fie $(K, +, \cdot)$ şi $(K', +, \cdot)$ două corpuri. Un morfism de inele $f : K \to K'$ se numeşte ***morfism de corpuri*** (atenţie: este vorba de un morfism unitar de inele!).

2) Un morfism de corpuri de la un corp la el însuşi se numeşte ***endomorfism*** al acelui corp.

Exemple

1. Funcţia $f : \mathbb{Q} \to \mathbb{C}$, $f(x) = x$ este un morfism de corpuri, numit ***morfismul-incluziune***.

2. Funcţia $f : \mathbb{C} \to \mathbb{C}$, $f(z) = \overline{z}$ este un endomorfism al corpului $\mathbb{C}$, ceea ce rezultă uşor din proprietăţile conjugării complexe.

Putem demonstra foarte uşor următorul rezultat:

Propoziţie

Compunerea a două morfisme de inele (respectiv de corpuri) este un morfism de inele (respectiv de corpuri).

Demonstraţie. Fie morfismele de inele $(A, +, \cdot) \xrightarrow{g} (A', +, \cdot) \xrightarrow{f} (A'', +, \cdot)$. Să considerăm funcţia $h = f \circ g$. Avem, pentru orice $x, y \in A$:

$$h(x+y) = (f \circ g)(x+y) = f\left(g(x+y)\right) = f\left(g(x)+g(y)\right) = f\left(g(x)\right) + f\left(g(y)\right) = h(x)+h(y);$$

$$h(xy) = (f \circ g)(xy) = f\left(g(xy)\right) = f\left(g(x)g(y)\right) = f\left(g(x)\right) f\left(g(y)\right) = h(x)h(y);$$

$$h(1_A) = (f \circ g)(1_A) = f\left(g(1_A)\right) = f(1_{A'}) = 1_{A''},$$

ceea ce arată că h este un morfism de inele.

În fine, un rezultat specific morfismelor de corpuri este următoarea:

Propoziție

Orice morfism de corpuri este injectiv.

Demonstrație. Fie $f : K \to K'$ un morfism de corpuri. Vom arăta că $\text{Ker } f = \{0\}$.

Presupunem prin absurd că există $x \in \text{Ker } f$, $x \neq 0_K$. Atunci elementul nenul x este inversabil în corpul K, deci există $x^{-1} \in K$ astfel încât $x x^{-1} = x^{-1} x = 1_K$.

Conform cu teorema precedentă punctul 1°, deoarece $x \in \text{Ker } f$ și $x^{-1} \in K$ rezultă că $x x^{-1} \in \text{Ker } f$, adică $1_K \in \text{Ker } f$. Atunci $f(1_K) = 0_{K'}$ și cum $f(1_K) = 1_{K'}$, rezultă $0_{K'} = 1_{K'}$, contradicție.

Definiție

1) Fie $(A, +, \cdot)$ și $(A', +, \cdot)$ două inele. O funcție $f : A \to A'$ se numește ***izomorfism de inele*** dacă este un morfism de inele inversabil (adică este funcție inversabilă și funcția inversă $f^{-1} : A' \to A$ este de asemenea morfism de inele); funcția inversă f^{-1} este tot un izomorfism de inele, numit ***izomorfismul invers*** lui f.

2) Un izomorfism de inele de la un inel la el însuși se numește ***automorfism*** al acelui inel.

3) Dacă între două inele A și A' există (cel puțin) un izomorfism de inele, spunem că inelele sunt izomorfe și scriem $A \approx A'$.

Exemple

1. $f : \mathbb{Z}[i] \to \mathbb{Z}[i]$, $f(z) = \bar{z}$ este un automorfism al inelului $\mathbb{Z}[i]$.

2. Pentru $d \in \mathbb{Z}$ nepătrat perfect, considerăm inelele $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ și $A = \left\{ \begin{pmatrix} a & b \\ db & a \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$; primul inel este gândit ca subinel al corpului $\mathbb{C}$, iar al doilea inel este gândit ca subinel al inelului $\mathcal{M}_2(\mathbb{Z})$ (vezi exercițiul rezolvat 1 pag. 73).

Funcția $f : \mathbb{Z}[\sqrt{d}] \to A$, $f(a + b\sqrt{d}) = \begin{pmatrix} a & b \\ db & a \end{pmatrix}$ este un izomorfism de inele.

Într-adevăr, funcția f este morfism de inele deoarece $\forall\ z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$, $z_1 = a_1 + b_1\sqrt{d}$, $z_2 = a_2 + b_2\sqrt{d}$, avem:

1°. $f(z_1 + z_2) = f\left((a_1 + a_2) + (b_1 + b_2)\sqrt{d}\right) =$

$$= \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ d(b_1 + b_2) & a_1 + a_2 \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ db_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ db_2 & a_2 \end{pmatrix} = f(z_1) + f(z_2);$$

2°. $f(z_1 z_2) = f\left((a_1 a_2 + d b_1 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{d}\right) =$

$$=\begin{pmatrix} a_1a_2+db_1b_2 & a_1b_2+a_2b_1 \\ d(a_1b_2+a_2b_1) & a_1a_2+db_1b_2 \end{pmatrix}=\begin{pmatrix} a_1 & b_1 \\ db_1 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ db_2 & a_2 \end{pmatrix}=f(z_1)f(z_2);$$

3°. $f(1)=f\left(1+0\cdot\sqrt{d}\right)=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=I_2$.

Funcţia f este inversabilă având inversa $f^{-1}: A\to\mathbb{Z}[\sqrt{d}]$, $f^{-1}\left(\begin{pmatrix} a & b \\ db & a \end{pmatrix}\right)=$ $=a+b\sqrt{d}$, iar funcţia inversă f^{-1} este morfism de inele deoarece $\forall\ X_1, X_2\in A$, $X_1=\begin{pmatrix} a_1 & b_1 \\ db_1 & a_1 \end{pmatrix}$, $X_2=\begin{pmatrix} a_2 & b_2 \\ db_2 & a_2 \end{pmatrix}$, avem:

1°. $f^{-1}(X_1+X_2)=f^{-1}\left(\begin{pmatrix} a_1+a_2 & b_1+b_2 \\ d(b_1+b_2) & a_1+a_2 \end{pmatrix}\right)=(a_1+a_2)+(b_1+b_2)\sqrt{d}=$

$$=\left(a_1+b_1\sqrt{d}\right)+\left(a_2+b_2\sqrt{d}\right)=f^{-1}(X_1)+f^{-1}(X_2);$$

2°. $f^{-1}(X_1X_2)=f^{-1}\left(\begin{pmatrix} a_1a_2+db_1b_2 & a_1b_2+a_2b_1 \\ d(a_1b_2+a_2b_1) & a_1a_2+db_1b_2 \end{pmatrix}\right)=(a_1a_2+db_1b_2)+(a_1b_2+a_2b_1)\sqrt{d}=$

$$=\left(a_1+b_1\sqrt{d}\right)\left(a_2+b_2\sqrt{d}\right)=f^{-1}(X_1)f^{-1}(X_2);$$

3°. $f^{-1}(I_2)=f^{-1}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=1+0\sqrt{d}=1$.

Prin urmare avem izomorfismul de inele $\left(\mathbb{Z}[\sqrt{d}], +, \cdot\right)\approx(A, +, \cdot)$.

Observaţie

Dacă două inele $(A, +, \cdot)$ şi $(A', +, \cdot)$ sunt izomorfe, atunci grupurile $(A, +)$ şi $(A', +)$ sunt izomorfe. Reciproc nu este adevărat.

Definiţie

1) Fie K şi K' două corpuri. Un izomorfism de inele $f: K\to K'$ se numeşte *izomorfism de corpuri*.

2) Un izomorfism de la un corp la el însuşi se numeşte ***automorfism*** al acelui corp.

3) Dacă între două corpuri K şi K' există un izomorfism spunem că ele sunt *corpuri izomorfe* şi scriem $K\approx K'$.

Observaţie

Funcţia $f: K\to K'$ este un izomorfism de corpuri dacă şi numai dacă funcţiile $f: (K, +)\to(K', +)$ şi $f: (K^*, \cdot)\to(K'^*, \cdot)$ sunt izomorfisme de grupuri.

Comentariu metodic

În legătură cu observația anterioară, remarcăm că dacă avem corpurile izomorfe K şi K', atunci grupurile aditive $(K, +)$ şi $(K', +)$ sunt izomorfe şi la fel, grupurile multiplicative $(K^*, \cdot)$ şi $(K'^*, \cdot)$ sunt izomorfe. Reciproc nu este adevărat, mai precis este posibil să avem izomorfismele de grupuri $(K, +) \approx (K', +)$ şi $(K^*, \cdot) \approx (K'^*, \cdot)$ şi totuşi corpurile K şi K' să nu fie izomorfe.

Contraexemplele depăşesc însă scopurile acestui manual.

Rezultatul următor caracterizează morfismele de inele sau de corpuri care sunt izomorfisme, degajând în acelaşi timp o metodă mai simplă de a proba că anumite funcții sunt izomorfisme de inele sau de corpuri.

Teoremă

Fie $f : A \to A'$ un morfism de inele (respectiv de corpuri, dacă A şi A' sunt corpuri). Următoarele afirmații sunt echivalente:

1°. f este izomorfism de inele (respectiv de corpuri).

2°. f este bijectiv.

Demonstrație. 1° $\Rightarrow$ 2°. Dacă f este izomorfism de inele, înseamnă că f este un morfism inversabil. Deoarece funcția f este inversabilă, rezultă că f este bijectivă.

2° $\Rightarrow$ 1°. Presupunem că f este un morfism bijectiv de inele. Deoarece funcția f este bijectivă, rezultă că f este inversabilă. Mai rămâne să dovedim că funcția inversă $f^{-1} : A' \to A$ este un morfism de inele.

Într-adevăr, pentru $y_1, y_2 \in A'$ arbitrare, notând $x_1 = f^{-1}(y_1)$, $x_2 = f^{-1}(y_2)$, avem $x_1, x_2 \in A$ şi putem scrie:

1°. $f^{-1}(y_1 + y_2) = f^{-1}(f(x_1) + f(x_2)) = f^{-1}(f(x_1 + x_2)) = x_1 + x_2 = f^{-1}(y_1) + f^{-1}(y_2)$;

2°. $f^{-1}(y_1 y_2) = f^{-1}(f(x_1) f(x_2)) = f^{-1}(f(x_1 x_2)) = x_1 x_2 = f^{-1}(y_1) f^{-1}(y_2)$;

3°. $f^{-1}(1_{A'}) = f^{-1}(f(1_A)) = 1_A$.

Aşadar funcția f este un izomorfism de inele.

Încheiem considerațiunile privitoare la morfisme şi izomorfisme de inele sau corpuri cu următorul rezultat:

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 un subinel (respectiv subcorp) al lui A'; în particular mulțimea $Im\ f = f(A)$ este un subinel (respectiv subcorp) al lui A'.

2°. Dacă f este un morfism injectiv, A este izomorf cu un subinel (respectiv subcorp) al lui A'.

Demonstrație. 1°. Dacă A, A' sunt inele, revine la arăta că pentru orice $y_1, y_2 \in B'$ avem $y_1 - y_2 \in B'$, $y_1 y_2 \in B'$ și $1_{A'} \in B'$.

Într-adevăr, fie $y_1 = f(x_1)$, $y_2 = f(x_2)$ unde $x_1, x_2 \in B$; atunci:

$y_1 - y_2 = f(x_1) - f(x_2) = f(x_1 - x_2) \in f(B) = B'$, deoarece $x_1 - x_2 \in B$;

$y_1 y_2 = f(x_1) f(x_2) = f(x_1 x_2) \in f(B) = B'$, deoarece $x_1 x_2 \in B$;

$1_{A'} = f(1_A) = f(1_B) \in f(B) = B'$, deoarece $1_A = 1_B$.

Dacă A, A' sunt corpuri, doar condiția a doua trebuie „modificată" astfel:

$$\forall\ y_1, y_2 \in B'^* \Rightarrow y_1 y_2^{-1} \in B'^*.$$

Într-adevăr: $y_1 y_2^{-1} = f(x_1)\left(f(x_2)\right)^{-1} = f(x_1) f(x_2^{-1}) = f(x_1 x_2^{-1}) \in f(B^*) = B'^*$, deoarece din aceea că $x_1, x_2 \in B^*$ rezultă $x_1 x_2^{-1} \in B^*$, fiindcă $(B^*, \cdot)$ este un subgrup al grupului $(A^*, \cdot)$.

2°. Dacă f este morfism injectiv de inele, avem $A \approx Im\ f$, iar $Im\ f$ este un subinel (respectiv subcorp) al lui A'.

Corolar

Dacă $f : K \to K'$ este un morfism de corpuri, atunci corpul K este izomorf cu un subcorp al corpului K'.

Demonstrație. Se ține seama că orice morfism de corpuri este injectiv și se aplică punctul 2° din teorema precedentă.

Exercițiu rezolvat

Pe mulțimea $\mathbb{R} \times \mathbb{R}$ definim operațiile de adunare și înmulțire astfel:

$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ și $(x_1, y_2)(x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)$.

Să se arate că:

a) $(\mathbb{R} \times \mathbb{R})$, +, ·) este un corp comutativ.

b) Corpul $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ este izomorf cu corpul $(\mathbb{C}, +, \cdot)$ al numerelor complexe.

(Reamintim că $\mathbb{C} = \{x + yi \mid x, y \in \mathbb{R},\ i^2 = -1\}$).

Soluție. a) Axiomele inelului comutativ se verifică relativ ușor, deși apar câteva calcule mai complicate. De aceea le vom lăsa cu titlul de temă.

Vom semnala faptul că elementul nul al inelului este (0, 0) iar elementul–unitate este (1, 0).

Să arătăm ultima axiomă din structura de corp și anume faptul că orice element nenul este inversabil. Fie așadar $(x, y) \in \mathbb{R} \times \mathbb{R}$, cu $x \neq 0$ sau $y \neq 0$. Căutăm un element

$(u, v) \in \mathbb{R} \times \mathbb{R}$ astfel încât $(x, y)(u, v) = (1, 0)$, adică $(xu - yv,\ xv + yu) = (1, 0)$, de unde:

$$\begin{cases} xu - yv = 1 \\ yu + xv = 0 \end{cases}$$

Rezolvând acest sistem în u şi v, obţinem:

$$u = \frac{x}{x^2 + y^2},\quad v = -\frac{y}{x^2 + y^2},$$

ceea ce arată că inversul lui $(x, y) \in \mathbb{R} \times \mathbb{R} \setminus \{(0, 0)\}$ este $\left(\frac{x}{x^2+y^2}, -\frac{y}{x^2+y^2}\right) \in \mathbb{R}\times\mathbb{R}$.

Aşadar $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ este corp comutativ.

b) Arătăm că funcţia $f : \mathbb{C} \to \mathbb{R} \times \mathbb{R}$, $f(x + yi) = (x, y)$ este un izomorfism de corpuri.

Într-adevăr, pentru orice $z_1, z_2 \in \mathbb{C}$, $z_1 = x_1 + y_1 i$, $z_2 = x_2 + y_2 i$, putem scrie:

1°. $f(z_1 + z_2) = f\left((x_1 + x_2) + (y_1 + y_2)i\right) = (x_1 + x_2,\ y_1 + y_2) =$
$= (x_1, y_1) + (x_2, y_2) = f(z_1) + f(z_2)$;

2°. $f(z_1 z_2) = f\left((x_1x_2 - y_1y_2) + (x_1y_2 + x_2y_1)i\right) = (x_1x_2 - y_1y_2,\ x_1y_2 + x_2y_1) =$
$= (x_1, y_1)(x_2, y_2) = f(z_1)f(z_2)$;

3°. $f(1) = f(1 + 0i) = (1, 0)$.

Până aici am dovedit că f este un morfism de corpuri. Dar f este şi o bijecţie, deoarece $\forall\ (x, y) \in \mathbb{R} \times \mathbb{R}$, $\exists!\ z = x + yi \in \mathbb{C}$ astfel încât $f(z) = (x, y)$. Aşadar f este un izomorfism de corpuri.

Comentariu metodic

Datorită izomorfismului de corpuri de mai sus, unii autori preferă să accepte drept corp al numerelor complexe tocmai corpul izomorf cu acesta $(\mathbb{R} \times \mathbb{R}, +, \cdot)$. Desigur, nu este eronat, deoarece două corpuri izomorfe au acelaşi comportament algebric, este doar discutabil un astfel de punct de vedere. Opinia noastră este că în rolul corpului numerelor complexe „originalul” îl constituie tripletul:

$$(\mathbb{C} = \{x + yi \mid x,y \in \mathbb{R},\ i^2 = -1),\ +,\ \cdot)$$

în timp ce $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ este doar o „copie” izomorfă.

EXERCIŢII PROPUSE

1. Fie A un inel comutativ de caracteristică p număr prim. Arătaţi că:

a) Funcţia $f : A \to A$, $f(x) = x^p$ este un endomorfism al inelului A (numit ***endomorfismul lui Frobenius***).

b) Pentru orice $n \in \mathbb{N}^*$ şi orice $a,b \in A$ avem egalitatea: $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

2. Arătaţi că funcţia $f : (\mathbb{Z}, +, \cdot) \to (\mathbb{Z}, \oplus, \odot)$, $f(x) = x - 1$, este un izomorfism între inelul numerelor întregi şi inelul din ex. 1 pag. 76.

3. Arătaţi că funcţia $f : (\mathbb{Z}, +, \cdot) \to (\mathbb{Z}, \oplus, \odot)$, $f(x) = x + 1$ este un izomorfism între inelul numerelor întregi şi inelul din exerciţiul 2 pag. 76.

4. Arătaţi că funcţia $f : \mathbb{Z}[i] \to A$, $f(a + bi) = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ este un izomorfism de inele între inelele care apar în exerciţiile 4 şi 5 de la pag. 76.

5. Arătaţi că acel corp care apare în exerciţiul 10 de la pag. 77 este izomorf cu corpul numerelor reale.

6. Arătaţi că acel corp care apare în ex. 11 de la pag 77 este izomorf cu corpul numerelor reale.

7. Arătaţi că acel corp care apare în ex. 12 de la pag. 77 este izomorf cu corpul pătratic $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$.

8. Arătaţi că acel corp care apare în exerciţiul 16 de la pag. 78 este izomorf cu corpul numerelor raţionale.

9. Arătaţi că acel corp care apare în exerciţiul 17 de la pag. 78 este izomorf cu corpul numerelor raţionale.

10. Arătaţi că acel corp care apare în exerciţiul 18 de la pag. 78 este izomorf cu corpul numerelor raţionale.

11. Arătaţi că acel corp care apare în exerciţiul 19 de la pag. 78 este izomorf cu corpul cuaternionilor (definit la pag. 67).

12. Fie $(A, +, \cdot)$ un inel, A' o mulţime şi $f : A \to A'$ o bijecţie. Pe mulţimea A' definim operaţiile $\oplus$ şi $\odot$ în felul următor: $x \oplus y = f\left(f^{-1}(x) + f^{-1}(y)\right)$, respectiv $x \odot y = f\left(f^{-1}(x)f^{-1}(y)\right)$, $\forall\, x,y \in A'$. Arătaţi că $(A', \oplus, \odot)$ este un inel, iar funcţia f este un izomorfism de inele. (Se spune că structura $(A', \oplus, \odot)$ este ***transportata*** structurii $(A, +, \cdot)$ prin bijecţia f).

13. Fie $(A, +, \cdot)$ şi $(A', +, \cdot)$ două inele izomorfe şi $f : A \to A'$ un izomorfism între aceste inele. Arătaţi că structura $(A', +, \cdot)$ este transportata structurii $(A, +, \cdot)$ prin bijecţia f, iar $(A, +, \cdot)$ este transportata structurii $(A', +, \cdot)$ prin bijecţia inversă f^{-1}.

14. Considerăm bijecţia $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x - a$, unde $a \in \mathbb{Z}$ este fixat. Să se descrie structura $(\mathbb{Z}, \oplus, \odot)$, care este transportata structurii $(\mathbb{Z}, +, \cdot)$ prin bijecţia f.

15. Considerăm bijecţia $f : \mathbb{R} \to K = (0, \infty)$, $f(x) = e^{x}$. Să se descrie structura $(K, \oplus, \odot)$, care este transportata structurii $(\mathbb{R}, +, \cdot)$ prin bijecţia f.

16. Considerăm bijecţia $f : \mathbb{R} \to K = \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$, $f(x) = \operatorname{tg} x$. Să se descrie structura $(K, \oplus, \odot)$, transportata structurii $(\mathbb{R}, +, \cdot)$ prin bijecţia f.

17. Determinaţi endomorfismele inelului $(\mathbb{Z}, +, \cdot)$.

18. Determinaţi endomorfismele corpului pătratic $\left(\mathbb{Q}(\sqrt{d}), +, \cdot\right)$, unde $d \in \mathbb{Z}$ este un număr care nu este pătrat perfect.

19. Determinaţi endomorfismele corpului $(\mathbb{R}, +, \cdot)$.

20. Determinaţi endomorfismele $f : \mathbb{C} \to \mathbb{C}$ ale corpului $(\mathbb{C}, +, \cdot)$, având proprietatea că $f(x) = x$, pentru orice $x \in \mathbb{R}$.

21. Fie K, K' două corpuri astfel încât există un morfism de corpuri $f : K \to K'$. Arătaţi că ambele corpuri au aceeaşi caracteristică. (Se mai spune că un morfism de corpuri „păstrează" caracteristica).

22. Arătaţi că un corp de caracteristică zero conţine un subcorp izomorf cu $\mathbb{Q}$, iar un corp de caracteristică p (număr prim) conţine un subcorp izomorf cu $\mathbb{Z}_p$.

23. Fie $(G, +)$ un grup abelian şi $\operatorname{End}(G) = \{f : G \to G \mid f \text{ endomorfism de grup}\}$. Pe mulţimea $\operatorname{End}(G)$ definim adunarea şi compunerea endomorfismelor astfel:

$$(f + g)(x) = f(x) + g(x); \quad (f \circ g)(x) = f(g(x)), \ \forall\, x \in G.$$

a) Arătaţi că $(\operatorname{End}(G), +, \circ)$ este un inel (numit ***inelul endomorfismelor grupului abelian*** G).

b) Arătaţi că inelul endomorfismelor grupului abelian $(\mathbb{Q}, +)$ este corpul din exerciţiul 16, pag. 78.

TESTE DE EVALUARE

Testul 1

(timp de lucru - 30 minute; fiecare exercițiu se notează cu 3 puncte)

Indicați răspunsul corect.

1. În inelul $(\mathbb{Z}, *, \circ)$ unde $x * y = x + y + 3$ și $x \circ y = xy + 3x + 3y + 6$ notăm cu a numărul elementelor inversabile și cu b numărul divizorilor lui zero. Atunci $a + b$ este:

a) 2; b) 3; c) 4; d) 1.

2. Inelul A are 25 de elemente și nu este corp. Dacă a este numărul divizorilor lui zero, atunci:

a) $a = 1$; b) $a = 2$; c) $a = 3$; d) $a \geq 4$.

3. Câte automorfisme are corpul $\left(\mathbb{Q}(\sqrt{2}), +, \cdot\right)$?

a) 1; b= 2; c) 3; d) o infinitate.

Testul 2

(timp de lucru - 50 minute; fiecare exercițiu se notează cu 3 puncte)

Pentru următoarele probleme se cer soluții complete.

1. Fie $K = \left\{a + b\sqrt[3]{3} + c\sqrt[3]{9} \mid a, b, c \in \mathbb{Q}\right\}$.

a) Să se arate că operațiile de adunare și înmulțire a numerelor reale sunt legi pe K.

b) Să se arate că tripletul $(K, +, \cdot)$ este corp comutativ.

c) Câte automorfisme are corpul K?

2. Fie $K = \left\{\begin{pmatrix} x & y \\ \hat{3}y & x \end{pmatrix} \middle| x, y \in \mathbb{Z}_5\right\}$.

a) Să se arate că dacă $x, y \in \mathbb{Z}_5$ și $x^2 - \hat{3}y^2 = \hat{0}$ atunci $x = y = \hat{0}$.

b) Să se arate că $(K, +, \cdot)$ este corp comutativ.

c) Câte elemente are corpul K?

3. Fie $A = \{f : [0, 1] \to \mathbb{R} \mid f$ continuă pe $[0, 1]\}$.

a) Să se arate că A împreună cu operațiile de adunare și înmulțire a funcțiilor este inel comutativ.

b) Să se arate că inelul A are o infinitate de divizori ai lui zero.

INELE DE POLINOAME CU COEFICIENȚI ÎNTR-UN INEL SAU CORP COMUTATIV

Forma algebrică a unui polinom, operații cu polinoame, funcția polinomială

Fie A un inel comutativ şi X o ***nedeterminată***, adică un obiect matematic neprecizat. Expresiile formale de tipul:

$$f = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n = \sum_i a_iX^i \text{ (sumă finită)},$$

unde $n \in \mathbb{N}$, iar $a_0, a_1, \ldots, a_n \in A$, se numesc ***polinoame (în nedeterminata X) cu coeficienți în A*** sau, mai scurt, ***polinoame peste A***.

Scrierea anterioară a polinomului f se mai numeşte ***forma algebrică*** a polinomului f.

Mulțimea polinoamelor cu coeficienți în inelul A se notează $A[X]$.

Dacă în polinomul $f = \sum_i a_iX^i$ cel puțin un coeficient a_i este nenul, atunci cel mai mare $n \in \mathbb{N}$ pentru care $a_n \neq 0$, se numeşte ***gradul*** polinomul f; dacă însă toți $a_i = 0$, polinomul $f = 0$ se numeşte ***polinomul nul*** şi considerăm că are gradul $-\infty$.

Dacă $f = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$ este un polinom de grad n ($a_n \neq 0$), spunem că a_n este ***coeficientul dominant***, iar în cazul când $a_n = 1$ spunem că polinomul este ***monic*** (***unitar***).

Elementele inelului A sunt polinoame peste A, mai precis 0 este polinomul nul, iar elementele $a \in A \setminus \{0\}$ sunt polinoamele de grad zero. Aşadar $A \subseteq A[X]$.

Pe mulțimea $A[X]$ se definesc două operații: ***adunarea polinoamelor*** şi ***înmulțirea polinoamelor***. Dacă $f, g \in A[X]$, $f = \sum_i a_iX^i$, $g = \sum_i b_iX^i$ (sumele sunt finite) atunci: $f + g = \sum_i (a_i + b_i)X^i$, iar $fg = \sum_{i,j} a_ib_jX^{i+j} = \sum_i c_iX^i$, unde $c_i = a_0b_i + a_1b_{i-1} + \ldots + a_ib_0 = \sum_{k+\ell=i} a_kb_\ell$. (În cuvinte: când adunăm două polinoame, adunăm între ei termenii cu puteri egale ale lui X, iar când înmulțim două polinoame respectăm distributivitatea înmulțirii față de adunare, adică înmulțim fiecare termen dintr-un polinom cu fiecare termen din celălalt polinom, după care „reducem" între ei termenii cu puteri egale ale lui X).

În cazul particular când $g = \lambda \in A$, înmulțirea $\lambda f = \sum_i (\lambda a_i) X^i$ poate fi interpretată ca fiind *produsul unui polinom cu un „scalar"*.

Exemplu

Dacă $f,\ g \in \mathbb{Z}[X]$, $f = 1 + 2X + 4X^2$, $g = 5 - X + X^3$, atunci $f + g = 6 + X + 4X^2 + X^3$, iar $fg = (1 + 2X + 4X^2)(5 - X + X^3) = 5 - X + X^3 + 10X - 2X^2 + 2X^4 + 20X^2 - 4X^3 + 4X^5 = 5 + 9X + 18X^2 - 3X^3 + 2X^4 + 4X^5$.

Relativ la gradul sumei și produsului avem următoarea:

Observație

Pentru orice $f,g \in A[X]$ există inegalitățile:

1°. grad $(f + g) \le \max$ (grad f, grad g);

2°. grad $(fg) \le$ grad f + grad g.

În inegalitățile de mai sus se poate atinge egalitatea sau se poate să avem inegalități stricte.

Exemple

1. $f,g \in \mathbb{Z}_4[X]$, $f = X^2 + \hat{1}$, $g = \hat{3}X \Rightarrow f + g = X^2 + \hat{3}X + \hat{1}$, $fg = \hat{3}X^3 + \hat{3}X$, deci grad $(f + g) = \max$(grad f, grad g) și grad (fg) = grad f + grad g.
2. $f,g \in \mathbb{Z}_4[X]$, $f = \hat{2}X + \hat{1}$, $g = \hat{2}X + \hat{2} \Rightarrow f + g = \hat{3}$, $fg = \hat{2}X + \hat{2}$, deci grad $(f + g) < \max$(grad f, grad g) și grad $(fg) <$ grad f + grad g.

Proprietățile adunării și înmulțirii polinoamelor se probează relativ ușor și permit degajarea următorului rezultat:

Teoremă

Tripletul $(A[X], +, \cdot)$ este un inel comutativ, numit ***inelul polinoamelor peste A***, iar A este un subinel al lui $A[X]$.

Demonstrație. Vom arăta doar asociativitatea înmulțirii și distributivitatea înmulțirii față de adunare în $A[X]$.

Dacă $f,g,h \in A[X]$, $f = \sum_i a_i X^i$, $g = \sum_j b_j X^j$, $h = \sum_k c_k X^k$ (sumele sunt finite) atunci:

$$(fg)h = \left(\sum_{i,j} a_i b_j X^{i+j}\right)\left(\sum_k c_k X^k\right) = \sum_{i,j,k} a_i b_j c_k X^{i+j+k}, \text{ iar}$$

$$f(gh) = \left(\sum_i a_i X^i\right)\left(\sum_{j,k} b_j c_k X^{j+k}\right) = \sum_{i,j,k} a_i b_j c_k X^{i+j+k}, \text{ deci } (fg)h = f(gh).$$

De asemenea:

$$fg + fh = \sum_{i,j} a_i b_j X^{i+j} + \sum_{i,j} a_i c_j X^{i+j} = \sum_{i,j} a_i (b_j + c_j) X^{i+j}\text{, iar}$$

$$f(g+h) = \left(\sum_i a_i X^i\right)\left(\sum_j (b_j + c_j) X^j\right) = \sum_{i,j} a_i (b_j + c_j) X^{i+j}\text{, deci}$$

$f(g + h) = fg + fh$.

În acest inel elementul nul este polinomul nul 0, iar elementul–unitate este polinomul 1. Faptul că A este subinel al lui $A[X]$ rezultă din definiția subinelului.

Rezultatul următor arată în ce caz inelul de polinoame $A[X]$ este un domeniu de integritate.

Teoremă

Inelul $A[X]$ este domeniu de integritate dacă şi numai dacă inelul A este domeniu de integritate, caz în care avem relația gradelor:

$$\text{grad }(fg) = \text{grad } f + \text{grad } g.$$

Demonstrație. Dacă $A[X]$ este domeniu de integritate, cum A este un subinel al lui $A[X]$ rezultă că şi A este domeniu de integritate. Reciproc, să presupunem că A este un domeniu de integritate şi să dovedim că $A[X]$ este domeniu de integritate. Pentru aceasta, arătăm că

$\forall\ f,g \in A[X],\ f \neq 0,\ g \neq 0 \Rightarrow fg \neq 0$. Într-adevăr, dacă $f = \sum_{i=0}^{n} a_i X^i$, $a_n \neq 0$ şi

$g = \sum_{j=0}^{m} b_j X^j$, $b_m \neq 0$, atunci $fg = a_0 b_0 + (a_0 b_1 + a_1 b_0)X + \ldots + a_n b_m X^{n+m}$.

Deoarece A este domeniu de integritate, din $a_n \neq 0$, $b_m \neq 0$ rezultă $a_n b_m \neq 0$, deci $fg \neq 0$. Mai mult, rezultă că grad$(fg) = n + m =$ grad f + grad g, $\forall\ f,g \in A[X]$, $f \neq 0$, $g \neq 0$. Dacă $f = 0$ sau $g = 0$, relația gradelor este de asemenea verificată, datorită convențiilor de calcul $-\infty + n = -\infty$, $\forall\ n \in \mathbb{N}$ şi $-\infty - \infty = -\infty$.

Pentru inelele de polinoame care sunt domenii de integritate, grupul elementelor inversabile este precizat de următoarea:

Teoremă

1) Dacă A este un domeniu de integritate, avem

$$U(A[X]) = U(A)$$

adică polinoamele inversabile din inelul $A[X]$ sunt exact elementele inversabile ale inelului A.

2) În particular, când $A = K =$ corp comutativ, avem

$$U(K[X]) = K^*$$

adică elementele inversabile din inelul $K[X]$ sunt elementele nenule din K (polinoamele de gradul zero).

Demonstrație. 1) Dacă $a \in U(A)$, $\exists\, b \in A$ cu $ab = 1$ și gândind această egalitate în $A[X]$ rezultă că $a \in U(A[X])$. Așadar, avem incluziunea:

$$U(A) \subseteq U(A[X]).$$

Fie acum $f \in U(A[X])$, deci $\exists\, g \in A[X]$ cu $fg = 1$. Trecând la grade și ținând seama de relația gradelor avem grad f + grad $g = 0$.

Cum $f \neq 0$, $g \neq 0$ avem grad f, grad $g \in \mathbb{N}$ și rezultă în mod necesar că grad f = = grad $g = 0$, deci $f,g \in A^* = A \setminus \{0\}$. Atunci egalitatea $fg = 1$ are loc în inelul A și arată că $f \in U(A)$. Avem așadar și incluziunea: $U(A[X]) \subseteq U(A)$.

Din cele două incluziuni, rezultă egalitatea din enunț.

2) Se aplică 1) și ținem cont că $U(K) = K^*$.

Exemple

1. $U(\mathbb{Z}[X]) = U(\mathbb{Z}) = \{-1, 1\}$;

2. $U(\mathbb{C}[X]) = U(\mathbb{C}) = \mathbb{C}^*$.

Definiție

1) Fie A un inel comutativ și $f \in A[X]$, $f = a_0 + a_1X + \ldots + a_nX^n$. Funcția $\tilde{f} : A \to A$ care asociază fiecărui $x \in A$ valoarea polinomului f în punctul x, adică elementul $f(x) = a_0 + a_1x + \ldots + a_nx^n \in A$, se numește ***funcția polinomială*** asociată polinomului.

Dacă nu este pericol de confuzie, putem nota funcția polinomială tot cu f, ca și polinomul căruia i se asociază.

2) Dacă $f(x_0) = 0$ pentru un $x_0 \in A$, spunem că x_0 este ***rădăcină*** a polinomului f în inelul A.

Observație

Dacă două polinoame sunt egale, atunci și funcțiile polinomiale care corespund sunt egale. Altfel spus:

$$f = g \Rightarrow \tilde{f} = \tilde{g}.$$

Reciproca acestei implicații este în general, falsă. Contraexemplu: $f,g \in \mathbb{Z}_3[X]$, $f = X^3$, $g = X$. Într-adevăr, $f \neq g$, dar $\tilde{f} = \tilde{g}$ deoarece funcțiile $\tilde{f}$, $\tilde{g}$ au același domeniu de definiție $\mathbb{Z}_3$, același codomeniu $\mathbb{Z}_3$ și același mod de corespondență căci $\tilde{f}(\hat{0}) = \tilde{g}(\hat{0}) = \hat{0}$, $\tilde{f}(\hat{1}) = \tilde{g}(\hat{1}) = \hat{1}$, $\tilde{f}(\hat{2}) = \tilde{g}(\hat{2}) = \hat{2}$.

Rezultatul următor arată că în anumite condiții este valabilă și reciproca implicației din observația anterioară. Avem nevoie în prealabil de următoarea:

Lemă

Fie K un corp comutativ şi $f \in K[X]$ un polinom de grad cel mult egal cu n. Dacă polinomul f are (cel puţin) $n+1$ rădăcini în corpul K, atunci f este polinomul nul.

Demonstraţie. Deoarece grad $f \leq n$, avem $f = a_0 + a_1X + \ldots + a_nX^n$ cu $a_i \in K$, $i = 0, 1, \ldots, n$. Vom arăta că $a_0 = a_1 = \ldots = a_n = 0$ şi atunci $f = 0$, ceea ce va încheia demonstraţia.

Fie $x_0, x_1, \ldots, x_n$ cele $n+1$ rădăcini ale polinomului f în corpul K. Scriind că $f(x_0) = 0$, $f(x_1) = 0$, ..., $f(x_n) = 0$ avem:

$$\begin{cases} a_0 + x_0a_1 + x_0^2a_2 + \ldots + x_0^na_n = 0 \\ a_0 + x_1a_1 + x_1^2a_2 + \ldots + x_1^na_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_0 + x_na_1 + x_n^2a_2 + \ldots + x_n^na_n = 0 \end{cases}$$

Interpretăm aceste egalităţi ca un sistem liniar omogen cu necunoscutele a_0, a_1, ..., a_n.

Determinantul sistemului este un determinant Vandermonde de ordinul $n+1$ şi are valoarea $\Delta = \prod_{0 \leq j < i \leq n} (x_i - x_j) \neq 0$. Dar un sistem liniar omogen, peste un corp comutativ, care are determinantul nenul, admite doar soluţia nulă. Aşadar $a_0 = a_1 = \ldots = a_n = 0$, adică $f = 0$.

Teoremă

Fie $f, g \in K[X]$ două polinoame de grade cel mult egale cu n, astfel încât $\widetilde{f} = \widetilde{g}$. Dacă K este un corp comutativ cu mai mult de n elemente (în particular, K poate fi infinit), atunci $f = g$.

Demonstraţie. Considerăm $h = f - g$. Din ipoteză avem $h(x) = 0$, $\forall\, x \in K$. Aşadar h este un polinom de grad cel mult n care se anulează în (cel puţin) $n+1$ puncte distincte din corpul K. Conform lemei rezultă $h = 0$ şi de aici $f = g$.

Comentariu metodic

Corpurile numerice $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sunt infinite şi de aceea pentru polinoamele peste aceste corpuri, există echivalenţa:

$$f = g \Leftrightarrow \widetilde{f} = \widetilde{g}.$$

Exercițiu rezolvat

Să se determine polinoamele de gradul întâi $f \in \mathbb{R}[X]$ cu proprietatea $f(x^2) = (f(x))^2$ pentru orice $x \in \mathbb{R}$.

Soluție. Fie $f = aX + b$ cu $a \in \mathbb{R}^*$, $b \in \mathbb{R}$, un polinom căutat. Ipoteza se scrie echivalent:

$$ax^2 + b = a^2x^2 + 2abx + b^2, \ \forall\, x \in \mathbb{R}.$$

Aceasta înseamnă că funcțiile polinomiale asociate polinoamelor $aX^2 + b \in \mathbb{R}[X]$ și $a^2X^2 + 2abX + b^2 \in \mathbb{R}[X]$ sunt egale. Conform teoremei de la pag. 97, polinoamele respective sunt egale, de unde, identificând coeficienții termenilor cu puteri egale ale lui X, obținem:

$$\begin{cases} a = a^2 \\ 0 = 2ab \\ b = b^2 \end{cases}$$

de unde $a = 1$ și $b = 0$, deci polinomul căutat este unic și anume $f = X$.

Comentariu metodic

Atunci când din egalitatea a două funcții polinomiale deducem egalitatea polinoamelor, ceea ce ne permite să identificăm coeficienții puterilor egale ale lui X, spunem că folosim „metoda coeficienților nedeterminați”. Astfel, putem spune că sistemul în a și b din acest exercițiu se obține prin metoda coeficienților nedeterminați.

EXERCIȚII PROPUSE

1. Determinați, în funcție de valorile parametrului m, gradul fiecăruia din polinoamele de mai jos:
   a) $(2m^3 + m^2 - m)X^2 + (m+1)X + m \in \mathbb{Z}[X]$;
   b) $(9m^2 - 4)X^4 + (3m+2)X^3 - X^2 + 2mX + 1 \in \mathbb{Q}[X]$;
   c) $(m^4 - 5m^2 + 6)X^3 + (m^2 - 2)X^2 + (m^2 - 3)X + m\sqrt{5} \in \mathbb{R}[X]$:
   d) $(m^4 - 1)X^5 + (m^2 + 1)X^4 + (m^4 - 2m^2 + 1)X^2 + mi \in \mathbb{C}[X]$.

2. Efectuați suma $f + g$ și diferența $f - g$, în fiecare din cazurile:
   a) $f = X^3 + 5X^2 - 2X + 1 \in \mathbb{Z}[X]$, $g = X^2 + X + 1 \in \mathbb{Z}[X]$;

b) $f=\frac{1}{2}X^2-\frac{3}{2}X+1 \in \mathbb{Q}[X]$, $g=3X^4-8X^3+\frac{1}{2}X^2-\frac{5}{2}X+6 \in \mathbb{Q}[X]$;

c) $f=\sqrt{3}\,X^4+X^2-\sqrt{2} \in \mathbb{R}[X]$, $g=-\sqrt{3}\,X^4+X^3-X^2+\sqrt{2} \in \mathbb{R}[X]$;

d) $f=iX^4+(1+i)X^3+(2+i)X^2-iX+10 \in \mathbb{C}[X]$,

$g=-iX^4+(1-i)X^3+(2-i)X^2+iX+10 \in \mathbb{C}[X]$;

e) $f=\hat{2}X^3+X^2+\hat{1} \in \mathbb{Z}_3[X]$, $g=X^2+\hat{2}X+\hat{2} \in \mathbb{Z}_3[X]$.

3. Efectuați produsul fg în fiecare din cazurile:

a) $f=X+1 \in \mathbb{Z}[X]$, $g=X^2-X+1 \in \mathbb{Z}[X]$;

b) $f=X^2-\frac{1}{3}X+\frac{1}{2} \in \mathbb{Q}[X]$, $g=2X^2+X+\frac{1}{3} \in \mathbb{Q}[X]$;

c) $f=\sqrt{2}\,X^2-\sqrt{3}\,X+\sqrt{5} \in \mathbb{R}[X]$, $g=\sqrt{2}\,X^2+\sqrt{3}\,X-\sqrt{5} \in \mathbb{R}[X]$;

d) $f=X+\frac{1}{2}-\frac{i\sqrt{3}}{2} \in \mathbb{C}[X]$, $g=X^2+\left(-\frac{1}{2}+\frac{i\sqrt{3}}{2}\right)X-\frac{1}{2}-\frac{i\sqrt{3}}{2} \in \mathbb{C}[X]$;

e) $f=\hat{2}X^2+X+\hat{3} \in \mathbb{Z}_5[X]$, $g=\hat{3}X+\hat{4} \in \mathbb{Z}_5[X]$;

f) $f=\hat{3}X^2+\hat{2} \in \mathbb{Z}_6[X]$, $g=\hat{2}X^2+\hat{3} \in \mathbb{Z}_6[X]$.

4. Demonstrați că pentru orice două polinoame $f,g \in A[X]$ sunt adevărate egalitățile:

a) $(f+g)^2=f^2+2fg+g^2$; b) $(f-g)^2=f^2-2fg+g^2$;

c) $(f+g)^3=f^3+3f^2g+3fg^2+g^3$; d) $(f-g)^3=f^3-3f^2g+3fg^2-g^3$;

e) $(f+g)(f-g)=f^2-g^2$; f) $(f+g)(f^2-fg+g^2)=f^3+g^3$;

g) $(f-g)(f^2+fg+g^2)=f^3-g^3$;

h) $(f-g)(f^{n-1}+f^{n-2}g+f^{n-3}g^2+\ldots+fg^{n-2}+g^{n-1})=f^n-g^n$, unde $n \in \mathbb{N}$, $n \geq 2$.

5. Fie K un corp comutativ de caracteristică 0. Determinați polinoamele $f \in K[X]$ având proprietatea: $f(x+y)=f(x)+f(y)$, $\forall\, x,y \in K$.

6. Fie K un corp comutativ infinit și $f=a_0+a_1X+a_2X^2+\ldots+a_nX^n \in K[X]$ un polinom de grad $n \in \mathbb{N}$. Spunem că polinomul f este ***reciproc de speța I*** dacă $a_{n-i}=a_i$, $i=0, 1, \ldots, n$ și spunem că polinomul f este ***reciproc de speța a II-a*** dacă $a_{n-i}=-a_i$, $i=0, 1, \ldots, n$. Să se demonstreze că:

a) Polinomul f este reciproc de speța I dacă și numai dacă

$$f\left(\frac{1}{x}\right)=\frac{1}{x^n}f(x),\ \forall\, x \in K^*.$$

b) Polinomul f este reciproc de speța a II-a dacă și numai dacă

$$f\left(\frac{1}{x}\right)=-\frac{1}{x^n}f(x),\ \forall\, x\in K^*.$$

7. Fie K un corp comutativ infinit și $f,g \in K[X]$ două polinoame nenule. Demonstrați că:
a) Dacă f, g sunt reciproce de speța I, atunci produsul fg este un polinom reciproc de speța I.
b) Dacă f, g sunt reciproce de speța a II-a, atunci produsul fg este un polinom reciproc de speța I.
c) Dacă f este reciproc de speța I și g este reciproc de speța a II-a, atunci produsul fg este un polinom reciproc de speța a II-a.

8. Fie K un corp comutativ infinit și f, g, $h \in K[X]$ polinoame nenule astfel încât $f = gh$. Demonstrați că:
a) Dacă f, g sunt reciproce de speța I, atunci h este reciproc de speța I;
b) Dacă f, g sunt reciproce de speța II, atunci h este reciproc de speța I;
c) Dacă f este reciproc de speța I, iar g este reciproc de speța a II-a (sau invers), atunci h este reciproc de speța a II-a.

9. Fie K un corp comutativ infinit și $f \in K[X]$. Demonstrați echivalența afirmațiilor:
1°. Funcția polinomială asociată polinomului f este pară.
2°. Există $g \in K[X]$ astfel încât $f(x)=g(x^2)$, $\forall\, x\in K$.

10. Fie K un corp comutativ infinit și $f \in K[X]$. Demonstrați echivalența afirmațiilor:
1°. Funcția polinomială asociată polinomului f este impară.
2°. Există $g \in K[X]$ astfel încât $f(x)=xg(x^2)$, $\forall\, x\in K$.

11. Dacă A este un inel comutativ, iar $f,g \in A[X]$, $f=a_nX^n+\ldots+a_1X+a_0$ definim polinomul $f\circ g=f(g)\in A[X]$ prin $f\circ g=a_ng^n+\ldots+a_1g+a_0$. Arătați că:
1°. $f=f(X)=X(f)$, $\forall\, f\in A[X]$.
2°. $(f\circ g)\circ h=f\circ(g\circ h)$, $\forall\, f,g,h\in A[X]$.

12. Fie A un inel comutativ și $A^{(\mathbb{N})}$ mulțimea șirurilor cu elemente din A, care au doar un număr finit de termeni nenuli. Definim suma și produsul a două șiruri din $A^{(\mathbb{N})}$ prin egalitățile $(a_n)_{n\ge 0}+(b_n)_{n\ge 0}=(a_n+b_n)_{n\ge 0}$ respectiv $(a_n)_{n\ge 0}\cdot(b_n)_{n\ge 0}=(c_n)_{n\ge 0}$, unde $c_n=\sum\limits_{i+j=n}a_ib_j$, $\forall\, n\in\mathbb{N}$.

Să se arate că tripletul $(A^{(\mathbb{N})}, +, \cdot)$ este un inel comutativ, izomorf cu inelul de polinoame $A[X]$.

Teorema împărțirii cu rest, împărțirea polinoamelor, împărțirea prin $X - a$, schema lui Horner

Vom pătrunde acum în *aritmetica inelelor de polinoame* $K[X]$ (K = corp comutativ) și vom constata că aceasta este foarte asemănătoare cu aritmetica inelului $\mathbb{Z}$ al numerelor întregi. Două rezultate fundamentale realizează această „apropiere" și anume teorema împărțirii cu rest și teorema de descompunere unică în factori ireductibili (primi). De acum încolo majoritatea considerațiunilor se referă la inelele de polinoame $K[X]$, iar acolo unde va fi cazul vom preciza că ele rămân adevărate și în cazul inelelor $A[X]$ (A = inel comutativ).

Teorema împărțirii cu rest

Fie $f,g \in K[X]$ două polinoame, cu $g \neq 0$. Există atunci alte două polinoame $q,r \in K[X]$ care verifică proprietățile:

1°. $f = qg + r$;

2°. $\text{grad}(r) < \text{grad}(g)$.

Polinoamele f, g, q, r se numesc ***deîmpărțit, împărțitor*** (care este nenul!), ***cât***, respectiv ***rest***.

Demonstrație. Tratăm două cazuri:

I) $\text{grad}(f) < \text{grad}(g)$.

Scriem $f = 0 \cdot g + f$, deci putem lua $q = 0$, $r = f$ și concluzia teoremei este satisfăcută.

II) $\text{grad}(f) \geq \text{grad}(g)$.

Fie $\text{grad}(f) = n$, $\text{grad}(g) = m$, $n \geq m$. Procedăm prin inducție după n, adică după gradul deîmpărțitului, împărțitorul fiind fixat.

Dacă $n = m$, putem scrie $f = a_m X^m + \ldots + a_1 X + a_0$, $g = b_m X^m + \ldots + b_1 X + b_0$ cu $a_i \in K$, $b_j \in K$, $i = 0, 1, \ldots, m$, $j = 0, 1, \ldots, m$ și $a_m \neq 0$, $b_m \neq 0$. Luăm atunci $q = \dfrac{a_m}{b_m} \in K$ (am notat mai sugestiv $b_m^{-1} = \dfrac{1}{b_m}$ și observăm că toate „fracțiile" cu numitor nenul din K și numărător din K sunt elemente din K) și $r = f - \dfrac{a_m}{b_m} g = f - gq$. Rezultă $f = gq + r$ și evident $\text{grad}(r) < \text{grad}(g)$, adică teorema este valabilă pentru aceste polinoame f și g.

Să presupunem că teorema este valabilă pentru toate polinoamele-deîmpărțit de grad n, cu $m \leq n < k$, și să arătăm că rămâne valabilă și în cazul când polinomul-deîmpărțit are gradul k.

Fie aşadar $f = a_k X^k + \ldots + a_1 X + a_0 \in K[X]$ un polinom-deîmpărţit de grad k. Considerăm polinomul $f_1 = f - \frac{a_k}{b_m} X^{k-m} \cdot g \in K[X]$, despre care este clar că grad(f_1) < < grad(f) = k (remarcăm iarăşi că $\frac{a_k}{b_m} \in K$). Atunci, cu f_1 în rol de deîmpărţit, teorema este valabilă, deci există q_1, $r_1 \in K[X]$ astfel încât $f_1 = gq_1 + r_1$ şi grad(r_1) < grad(g). Egalitatea precedentă devine:

$$f - \frac{a_k}{b_m} X^{k-m} \cdot g = gq_1 + r_1 \quad \text{sau} \quad f = \left(\frac{a_k}{b_m} X^{k-m} + q_1 \right) \cdot g + r_1 .$$

Luând atunci $q = \frac{a_k}{b_m} X^{k-m} + q_1 \in K[X]$ şi $r = r_1 \in K[X]$, avem $f = gq + r$ şi grad(r) < grad(g). Aceasta arată că teorema este valabilă şi pentru polinomul-deîmpărţit f având gradul k şi demonstraţia prin inducţie se încheie.

Observaţii

1. În teorema împărţirii cu rest câtul şi restul sunt unic determinate (ca şi în teorema corespunzătoare de la numere întregi), pentru un deîmpărţit şi un împărţitor date. Totuşi, unicitatea câtului şi restului nu foloseşte în mod esenţial în consideraţiunile teoretice despre polinoame.

2. Teorema împărţirii cu rest are loc şi în inele $A[X]$ în anumite cazuri particulare. De exemplu dacă polinomul-împărţitor g are coeficientul dominant $b_m = \pm 1$, urmărind demonstraţia teoremei constatăm că aceasta rămâne valabilă, deoarece:

$$\frac{a_m}{b_m} \in A \quad \text{şi} \quad \frac{a_k}{b_m} \in A.$$

Exemple

Să arătăm pe două exemple concrete „algoritmul" efectuării împărţirii cu rest a două polinoame.

1. Să considerăm polinoamele $f, g \in \mathbb{Q}[X]$, $f = 2X^4 + X^2 + 3X - 1$, $g = 3X^2 + X$. Împărţirea lui f prin g se face astfel:

$$
\begin{array}{l|l}
2X^4 \qquad\qquad + X^2 + 3X - 1 & 3X^2 + X \\ \cline{2-2}
-2X^4 - \dfrac{2}{3}X^3 & \dfrac{2}{3}X^2 - \dfrac{2}{9}X + \dfrac{11}{27} \\ \cline{1-1}
/ \quad -\dfrac{2}{3}X^3 + X^2 + 3X - 1 & \\
\qquad \dfrac{2}{3}X^3 + \dfrac{2}{9}X^2 & \\ \cline{1-1}
\qquad / \quad \dfrac{11}{9}X^2 + 3X - 1 & \\
\qquad\quad -\dfrac{11}{9}X^2 - \dfrac{11}{27}X & \\ \cline{1-1}
\qquad\qquad / \quad \dfrac{70}{27}X - 1 &
\end{array}
$$

Se obțin câtul și restul $q, r \in \mathbb{Q}[X]$, $q = \dfrac{2}{3}X^2 - \dfrac{2}{9}X + \dfrac{11}{27}$, $r = \dfrac{70}{27}X - 1$.

Dacă aceleași polinoame f, g din exemplul dat, le gândim în $\mathbb{Z}[X]$, constatăm că $q, r \notin \mathbb{Z}[X]$. Aceasta arată nevalabilitatea teoremei împărțirii cu rest în inelul de polinoame $\mathbb{Z}[X]$.

2. Să se determine câtul și restul împărțirii lui f prin g, unde $f, g \in \mathbb{Z}_5[X]$,

$$f = \hat{2}X^3 + X + \hat{4}, \quad g = \hat{3}X^2 + X.$$

Ținând seama că într-un corp comutativ K notăm $\dfrac{a}{b} = ab^{-1}$ și că în corpul $K = \mathbb{Z}_5$ avem $\hat{3}^{-1} = \hat{2}$, împărțirea se efectuează astfel:

$$
\begin{array}{l|l}
\hat{2}X^3 \qquad + X + \hat{4} & \hat{3}X^2 + X \\ \cline{2-2}
-\hat{2}X^3 - \hat{4}X^2 & \hat{4}X + \hat{2} \\ \cline{1-1}
/ \quad X^2 + X + \hat{4} & \\
\quad -X^2 - \hat{2}X & \\ \cline{1-1}
\qquad / \quad \hat{4}X + \hat{4} &
\end{array}
$$

Așadar câtul este $q = \hat{4}X + \hat{2} \in \mathbb{Z}_5[X]$, restul este $r = \hat{4}X + \hat{4} \in \mathbb{Z}_5[X]$.

Un caz particular cu o semnificație deosebită îl constituie acela când în teorema împărțirii cu rest polinomul-împărțitor este de forma $X - a$. Rezultatul cel mai important în acest sens îl constituie următoarea:

Teoremă (Bézout)

Restul împărţirii polinomului $f \in K[X]$ prin polinomul $X - a \in K[X]$ este $f(a)$, adică valoarea polinomului f în punctul a (aici, K este un corp comutativ).

Demonstrație. Aplicăm teorema împărţirii cu rest. Există deci $q,r \in K[X]$ cu proprietăţile:

$$f = (X - a)q + r, \qquad (1)$$

$$\text{grad}(r) < \text{grad}(X - a). \qquad (2)$$

Din (2) rezultă că grad(r) = 0 sau grad(r) = $-\infty$, adică $r \in K$ (r este un polinom constant).

Trecem în (1) la valoarea numerică în punctul a şi obţinem $f(a) = (a - a)q(a) + r = r$, adică $r = f(a)$.

Un procedeu rapid de a efectua împărţirea unui polinom $f \in K[X]$ prin $X - a \in K[X]$ este aşa-numita *schemă a lui Horner*. Aceasta se obţine pe baza algoritmului împărţirii şi o vom descrie mai jos. Să presupunem că vrem să împărţim polinomul $f = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n \in K[X]$ la polinomul $g = X - a \in K[X]$. Pentru a scrie mai uşor, am indexat crescător coeficienţii puterilor descrescătoare ale lui X din polinomul f.

Facem următorul tabel (schema lui Horner):

	a_0	a_1	a_2	...	a_{i-1}	a_i	...	a_n
a	b_0	b_1	b_2	...	b_{i-1}	b_i	...	b_n

Pe prima linie scriem coeficienţii polinomului f, după puterile descrescătoare ale lui X, adică $a_0, a_1, a_2, \ldots, a_n$. Pe linia a doua, în stânga îl scriem pe a, iar apoi scriem numerele $b_0, b_1, b_2, \ldots, b_n$, obţinute recursiv după „regula”:

$$b_0 = a_0; \; b_i = ab_{i-1} + a_i, \; \forall\, i \in \{1, 2, \ldots, n\}.$$

Coeficienţii câtului, după puterile descrescătoare ale lui X, sunt $b_0, b_1, b_2, \ldots, b_{n-1}$, iar restul împărţirii este b_n.

Exemplu

Să împărţim polinomul $f = 2X^5 - 8X^4 - 3X^3 + 6X + 1$ la polinomul $g = X - 4$, unde $f,g \in \mathbb{Q}[X]$.

Avem schema lui Horner:

	2	−8	−3	0	6	1
4	2	4·2−8 = 0	4·0−3 = −3	4·(−3)+0 = −12	4·(−12)+6 = −42	4·(−42)+1 = −167

Câtul obţinut este polinomul $q = 2X^4 - 3X^2 - 12X - 42$, iar restul este polinomul $r = -167$, unde $q,r \in \mathbb{Q}[X]$. Conform teoremei lui Bézout, restul coincide cu valoarea polinomului f în punctul 4, adică $f(4) = -167$.

Divizibilitatea polinoamelor, cel mai mare divizor comun, descompunerea în factori ireductibili

Noțiunile din acest paragraf extind la polinoame noțiuni similare întâlnite la numere întregi.

Definiție

Fixăm un inel de polinoame $K[X]$. Dacă f, $g \in K[X]$ spunem că g ***divide*** f în $K[X]$ (echivalent, f ***se divide*** cu g) dacă există $h \in K[X]$ astfel încât $f = gh$. Se mai spune că g este ***divizor*** al lui f. Scriem $g \mid f$ (echivalent, $f \,\vdots\, g$).

Avem următoarea:

Observație

Dacă $f,g \in K[X]$, $g \neq 0$, există echivalența:

$$f \,\vdots\, g \Leftrightarrow \text{restul împărțirii lui } f \text{ prin } g \text{ este } 0 \text{ (polinomul nul).}$$

Rezultă ușor următoarea caracterizare a rădăcinilor unui polinom, exprimată în termeni de divizibilitate, care este o variantă a teoremei lui Bézout:

Teoremă (Bézout)

Fie $f \in K[X]$ și $a \in K$. Atunci:

$$a \text{ este rădăcină pentru } f \text{ în } K \text{ dacă și numai dacă } f \,\vdots\, (X-a) \text{ în } K[X].$$

Demonstrație. Fie $r \in K[X]$ restul împărțirii lui f prin $X - a$, deci $r = f(a)$. Avem echivalențele succesive: a este rădăcină pentru $f \Leftrightarrow f(a) = 0 \Leftrightarrow r = 0 \Leftrightarrow f \,\vdots\, (X-a)$.

Definiție

Polinoamele f, $g \in K[X]$ se numesc ***asociate în divizibilitate*** (mai scurt, ***asociate***) dacă $f \mid g$ și $g \mid f$. Scriem $f \sim g$.

Două polinoame asociate au aceleași proprietăți aritmetice.

Rezultatul următor caracterizează polinoamele asociate în divizibilitate într-un inel $K[X]$.

Propoziție

Polinoamele nenule f, $g \in K[X]$ sunt asociate în divizibilitate dacă și numai dacă $f = \lambda g$, unde $\lambda \in K^*$.

Demonstrație. Să presupunem că $f \sim g$, deci $f \mid g$ și $g \mid f$ în $K[X]$. Atunci $f = \lambda g$ și

$g = \mu f$, cu $\lambda, \mu \in K[X]$. Rezultă $f = \lambda\mu f$ şi împărţind prin $f \neq 0$ obţinem $\lambda\mu = 1$. Trecând la grade rezultă grad(λ) + grad(μ) = 0, de unde grad(λ) = grad(μ) = 0, ceea ce înseamnă că $\lambda, \mu \in K^*$. Rezultă $f = \lambda g$, cu $\lambda \in K^*$.
Reciproc, dacă $f = \lambda g$, cu $\lambda \in K^*$ avem $g = \lambda^{-1} f$, deci $f \mid g$ şi $g \mid f$, adică $f \sim g$.

De exemplu, în $\mathbb{Q}[X]$ polinoamele $3X + 5$ şi $X + \frac{5}{3}$ sunt asociate deoarece $3X + 5 = 3\left(X + \frac{5}{3}\right)$ şi $3 \in \mathbb{Q}^*$.

Definiţie

Spunem că polinoamele $f, g \in K[X]$ ***au un cel mai mare divizor comun*** dacă există polinomul $d \in K[X]$ cu proprietăţile:

1°. $d \mid f$ şi $d \mid g$ (adică d este un divizor comun pentru f şi g).

2°. $\forall\, d' \in K[X]$, $d' \mid f$, $d' \mid g \Rightarrow d' \mid d$ (orice alt divizor comun îl divide pe d).

Polinomul d se numeşte ***cel mai mare divizor comun*** (pe scurt, c.m.m.d.c.) al polinoamelor f şi g şi se notează $d = (f, g)$.

Următorul rezultat arată că definiţia precedentă are obiect, mai exact, există cel mai mare divizor comun pentru oricare două polinoame din $K[X]$.

Teoremă

Fie $f, g \in K[X]$ două polinoame oarecare. Atunci:

1°. Există un cel mai mare divizor comun $d \in K[X]$ al polinoamelor f şi g.

2°. C.m.m.d.c. este determinat până la o asociere în divizibilitate, în sensul că dacă $\delta \in K[X]$ este un alt c.m.m.d.c. pentru f şi g atunci $d \sim \delta$.

Demonstraţie. 1°. Dacă unul din polinoame este nul, de exemplu $g = 0$, atunci $(f, 0) = f$, deoarece $f \mid 0$.

Să presupunem că ambele polinoame sunt nenule, deci $f \neq 0$, $g \neq 0$. Considerăm mulţimea $D \subseteq K[X]$, unde

$$D = \{uf + vg \mid u, v \in K[X],\ uf + vg \neq 0\}.$$

Mulţimea D este nevidă, căci $f, g \in D$. Polinoamele din mulţimea D se numesc „***combinaţii liniare***" (nenule) de polinoamele f şi g cu „coeficienţi" din $K[X]$. Fie $d \in D$ un polinom de grad minim; există un asemenea polinom, deoarece mulţimea gradelor polinoamelor din D este o submulţime nevidă a lui $\mathbb{N}$, deci are un minim.

Arătăm că $d = (f, g)$. Deoarece $d \in D$, există $u_0, v_0 \in K[X]$ astfel încât $d = u_0 f + v_0 g$. Polinomul d divide polinomul f, căci din teorema împărţirii cu rest avem $f = dq + r$, cu $q, r \in K[X]$ şi grad(r) < grad(d); dar atunci $r = f - dq = f - (u_0 f + v_0 g)q = (1 - u_0)f - (v_0 q)g$ şi dacă am avea $r \neq 0$ ar rezulta $r \in D$, adică r ar fi un polinom din D de grad mai mic decât grad(g), contradicţie. Aşadar $r = 0$, deci $f = dq$, adică $d \mid f$.

Analog se arată că $d \mid g$.

Fie acum $d' \in K[X]$ astfel încât $d' \mid f$ şi $d' \mid g$. Atunci $d' \mid (u_0 f + v_0 g)$, adică $d' \mid d$. Prin urmare $d = (f, g)$.

2°. C.m.m.d.c. este determinat până la o asociere în divizibilitate, căci dacă $\delta \in K[X]$ este un alt cel mai mare divizor comun pentru polinoamele f şi g, avem $\delta \mid f$, $\delta \mid g$, deci $\delta \mid d$; dar şi $d \mid f$, $d \mid g$, deci $d \mid \delta$. Prin urmare $d \sim \delta$.

Din demonstraţia dată teoremei precedente rezultă următorul:

Corolar. Dacă $f, g \in K[X]$ şi $d = (f, g)$, atunci există $u, v \in K[X]$ astfel încât avem scrierea:

$$d = uf + vg.$$

Este bine să remarcăm un fapt: existenţa c.m.m.d.c. a două polinoame a fost dovedită pentru polinoamele din $K[X]$ şi în demonstraţie am utilizat teorema împărţirii cu rest, valabilă în $K[X]$.

Definiţie

1°. Un polinom $p \in K[X]$, neasociat cu 0 şi 1 (echivalent spus, de grad ≥ 1), se numeşte ***ireductibil*** în $K[X]$ (sau ***ireductibil peste K***) dacă, abstracţie făcând de asocieri, singurii săi divizori în $K[X]$ sunt 1 şi p.

2°. Un polinom din $K[X]$, neasociat cu 0 sau 1, care nu este ireductibil în $K[X]$, se numeşte ***reductibil*** în $K[X]$.

După cum observăm cu uşurinţă, noţiunea de ***polinom ireductibil*** este analoagă celei de ***număr prim***.

Evident, pe baza definiţiei avem următoarea:

Observaţie

Pentru un polinom $p \in K[X]$, neasociat cu 0 sau 1, următoarele afirmaţii sunt echivalente:

1°. p este ireductibil în $K[X]$.

2°. $\forall\, q \in K[X]$, $q \mid p \Rightarrow q \sim 1$ sau $q \sim p$.

3°. p nu se poate scrie ca produsul a două polinoame din $K[X]$, ambele de grade mai mici decât grad(p).

Exemple de polinoame ireductibile

1. Orice polinom de gradul întâi $p \in K[X]$ este ireductibil în $K[X]$, căci nu poate fi scris ca un produs de două polinoame de grad mai mic ca 1.
2. Polinomul $p = X^2 + 1 \in \mathbb{R}[X]$ este ireductibil peste $\mathbb{R}$.

Într-adevăr, dacă p s-ar scrie ca un produs de două polinoame din $\mathbb{R}[X]$ de grade mai mici ca 2, acestea ar trebui să fie de grad 1 şi ar avea (fiecare din ele) o rădăcină în $\mathbb{R}$; ar rezulta că p are rădăcini reale, contradicţie.

3. Polinomul $p = X^3 - 2 \in \mathbb{Q}[X]$ este ireductibil peste $\mathbb{Q}$.

   Într-adevăr, dacă p s-ar scrie ca produsul a două polinoame din $\mathbb{Q}[X]$ de grade mai mici ca 3, unul din acestea ar avea gradul 1 şi deci ar avea o rădăcină în $\mathbb{Q}$, deci p ar avea o rădăcină în $\mathbb{Q}$, contradicţie.

4. Orice polinom p de grad 2 sau 3 din $K[X]$ care nu are rădăcini în K este ireductibil în $K[X]$.
   Într-adevăr, dacă p s-ar scrie ca un produs de două polinoame din $K[X]$, de grade mai mici decât grad(p), atunci unul din aceste polinoame are gradul 1, prin urmare are o rădăcină în K, deci p ar avea o rădăcină în K, absurd.

Exemplele anterioare 2 şi 3 sunt cazuri particulare din exemplul 4.

Pentru a demonstra un rezultat important care urmează, avem nevoie de trei rezultate pregătitoare.

Lema 1. Fie $p \in K[X]$ un polinom ireductibil şi $f \in K[X]$ un polinom oarecare. Dacă p nu divide f, atunci $(p, f) = 1$
Demonstraţie. Fie $d = (p, f)$. Cum $d \mid p$ avem $d \sim 1$ sau $d \sim p$. Dacă am avea $d \sim p$, cum $d \mid f$ ar rezulta că $p \mid f$, contrar ipotezei. Deci $d \sim 1$, adică $(p, f) = 1$.

Lema 2. Fie $f, g \in K[X]$ astfel încât $f \mid gh$ şi $(f, g) = 1$. Atunci $f \mid h$.
Demonstraţie. Deoarece $(f, g) = 1$, conform colorarului de la pag. 97 există $u, v \in$ $\in K[X]$ astfel încât $uf + vg = 1$. Prin înmulţire cu h obţinem $ufh + vgh = h$. Deoarece $f \mid gh$, există $s \in K[X]$ astfel încât $gh = fs$. Egalitatea obţinută se scrie $ufh + vfs = h$ sau $f(uh + vs) = h$ şi arată că $f \mid h$.

Lema 3. Fie $p \in K[X]$, neasociat cu 0 sau 1. Următoarele afirmaţii sunt echivalente:
1°. p este ireductibil în $K[X]$.
2°. $\forall f, g \in K[X],\ p \mid fg \Rightarrow p \mid f$ sau $p \mid g$.
Demonstraţie. 1° $\Rightarrow$ 2°. Presupunem p ireductibil şi fie $f, g \in K[X]$ astfel încât $p \mid fg$. Pentru a arăta că $p \mid f$ sau $p \mid g$, procedăm astfel: admitem de exemplu că p nu divide f şi demonstrăm că p divide g. Într-adevăr, cum p nu divide f, conform lemei 1 avem $(p, f) = 1$. Aşadar $p \mid fg$ şi $(p, f) = 1$, ceea ce, în baza lemei 2, duce la $p \mid g$.
2° $\Rightarrow$ 1°. Presupunem că $\forall f, g \in K[X],\ p \mid fg \Rightarrow p \mid f$ sau $p \mid g$. Pentru a arăta că p este ireductibil, considerăm un divizor arbitrar $q \in K[X]$ al lui p şi demonstrăm că $q \sim 1$ sau $q \sim p$. Avem $p = qs$, cu $s \in K[X]$, deci $p \mid qs$ şi atunci, pe baza ipotezei în care lucrăm, avem $p \mid q$ sau $p \mid s$. Dacă $p \mid q$, cum şi $q \mid p$, avem $q \sim p$. Dacă $p \mid s$, cum $s \mid p$,

avem $s \sim p$ şi atunci $q \sim 1$.

Rezultatul care urmează, extrem de important, este analogul la nivelul inelelor de polinoame $K[X]$ al teoremei fundamentale a aritmeticii din inelul $\mathbb{Z}$ (adică teorema de descompunere în factori primi). Demonstraţia acestei teoreme este o bună ilustrare a metodei inducţiei matematice.

Teoremă (de descompunere în factori ireductibili)

Orice polinom din $K[X]$, neasociat cu 0 sau 1, se descompune în mod unic într-un produs de polinoame ireductibile din $K[X]$.

Unicitatea trebuie înţeleasă abstracţie făcând de asocieri şi de ordinea factorilor.

Demonstraţie. a) *Existenţa descompunerii.* Fie $f \in K[X]$, neasociat cu 0 sau 1, şi să notăm $\ell = \text{grad}(f) \geq 1$. Procedăm prin inducţie după ℓ. Pentru $\ell = 1$ polinomul f este ireductibil în $K[X]$ şi descompunerea este asigurată, mai precis f are un singur factor ireductibil în descompunerea sa.

Să presupunem că toate polinoamele de grad mai mic decât ℓ se descompun în factori ireductibili şi să dovedim că şi polinomul f de grad ℓ se descompune.

Dacă f este ireductibil, descompunerea este asigurată.

Dacă f este reductibil, avem $f = gh$, cu $g, h \in K[X]$ şi $\text{grad}(g) < \ell$, $\text{grad}(h) < \ell$.

Conform ipotezei de inducţie $g = p_1p_2 \dots p_s$, $h = p_{s+1}p_{s+2} \dots p_t$, unde $t > s$ şi unde $p_1, \dots, p_s, p_{s+1}, \dots, p_t \in K[X]$ sunt polinoame ireductibile, nu neapărat distincte. Atunci $f = gh = p_1p_2 \dots p_sp_{s+1} \dots p_t$, deci f se descompune în factori ireductibili.

b) *Unicitatea descompunerii.* Presupunem că f are două descompuneri: $f = p_1p_2 \dots p_n = q_1q_2 \dots q_m$, unde $p_1, \dots, p_n, q_1, \dots, q_m$ sunt polinoame ireductibile din $K[X]$. Vom arăta că $m = n$ şi, după o eventuală renotare, avem $p_1 \sim q_1$, $p_2 \sim q_2$, $\dots$, $p_n \sim q_n$. Procedăm prin inducţie după n, adică după numărul factorilor ireductibili ai primei descompuneri. Dacă $n = 1$ avem

$$p_1 = q_1 q_2 \dots q_m. \tag{1}$$

Atunci $p_1 \mid q_1 q_2 \dots q_m$ şi, conform lemei 3, p_1 divide unul din factorii q_1, q_2, $\dots$, q_m. După o eventuală renotare, putem presupune $p_1 \mid q_1$. Din (1) avem însă $q_1 \mid p_1$ şi astfel $p_1 \sim q_1$. Dacă am avea $m \geq 2$, din (1) ar rezulta că $q_2, q_3, \dots, q_m$ ar fi asociate cu 1, contrar faptului că ele sunt polinoame ireductibile. Aşadar $m = n = 1$ şi astfel unicitatea descompunerii este probată în cazul $n = 1$. Presupunem că unicitatea descompunerii are loc pentru $n - 1$ şi arătăm că este adevărată şi pentru n. Din egalitatea

$$p_1 p_2 \dots p_n = q_1 q_2 \dots q_m \tag{2}$$

rezultă $p_n \mid q_1 q_2 \dots q_m$. Conform lemei 3, p_n divide unul din factorii $q_1, q_2, \dots, q_m$.

După o eventuală renotare, putem presupune că $p_n \mid q_m$. Cum q_m este ireductibil şi p_n nu este asociat cu 1, rezultă $p_n \sim q_m$, deci $q_m = \lambda p_n$, cu $\lambda \in K^*$. Înlocuind în (2) şi simplificând prin $p_n \neq 0$, obţinem:

$$p_1 p_2 \dots p_{n-1} = (\lambda q_1) q_2 \dots q_{m-1}; \tag{3}$$

unde λq_1 este un polinom ireductibil, căci este asociat cu q_1. Conform ipotezei de inducţie, din (3) rezultă $n - 1 = m - 1$, adică $n = m$ şi după o eventuală renotare, avem: $p_1 \sim \lambda q_1 \sim q_1$, $p_2 \sim q_2$, …, $p_{n-1} \sim q_{m-1}$. Cum şi $p_n \sim q_m = q_n$, teorema este demonstrată.

Observaţii

1. Dacă în descompunerea în factori ireductibili grupăm factorii asociaţi şi utilizăm scrierea cu puteri, obţinem că orice polinom $f \in K[X]$ de grad ≥ 1 se scrie sub forma:

$$f = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

unde $p_1, p_2, \dots, p_k \in K[X]$ sunt polinoame ireductibile, neasociate două câte două, iar $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{N}^*$.

2. Dacă $f, g \in K[X]$, neasociate cu 0 sau 1, au descompunerile în factori ireductibili:

$$f = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \quad g = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k},$$

unde $p_1, p_2, \dots, p_k$ sunt polinoame ireductibile, iar $\alpha_1, \alpha_2, \dots, \alpha_k, \beta_1, \beta_2, \dots, \beta_k \in \mathbb{N}$ (unele din aceste numere pot fi egale cu zero), atunci c.m.m.d.c. al polinoamelor f şi g este dat de egalitatea:

$$(f, g) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdot \ldots \cdot p_k^{\min(\alpha_k, \beta_k)}.$$

Rezultatele din cele două observaţii anterioare sunt în deplină concordanţă cu cele similare de la numere întregi.

Definiţie

Dacă $f, g \in K[X]$, spunem că polinomul $m = [f, g] \in K[X]$ este un ***cel mai mic multiplu comun*** (c.m.m.m.c.) al polinoamelor f şi g dacă verifică:

1°. $f \mid m$ şi $g \mid m$;

2°. $\forall\, m' \in K[X]$ cu $f \mid m'$ şi $g \mid m' \Rightarrow m \mid m'$.

Observaţie

C.m.m.m.c. a două polinoame $f, g \in K[X]$ este determinat până la o asociere în divizibilitate, iar dacă $f = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $g = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$, atunci

$$[f, g] = p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdot \ldots \cdot p_k^{\max(\alpha_k, \beta_k)}.$$

Remarcăm, de asemenea, egalitatea: $[f, g] = \dfrac{fg}{(f, g)}$.

EXERCIȚII PROPUSE

1. Să se determine câtul și restul împărțirii polinomului f prin polinomul g, în fiecare din cazurile:
   a) $f = 2X^5 + 6X^4 - 3X^3 + 8X^2 - X + 1 \in \mathbb{Z}[X]$, $g = X^2 + X + 2 \in \mathbb{Z}[X]$;
   b) $f = \frac{3}{4}X^6 + \frac{1}{2}X^5 - X^4 + \frac{3}{2}X^3 + X^2 + X + \frac{1}{2} \in \mathbb{Q}[X]$, $g = 2X^2 - X + \frac{1}{2} \in \mathbb{Q}[X]$;
   c) $f = X^3 + 2X^2 - X + \sqrt{5} \in \mathbb{R}[X]$, $g = X^2 - 1 \in \mathbb{R}[X]$;
   d) $f = iX^4 + (1+i)X^3 + 2X^2 - X + 1 \in \mathbb{C}[X]$, $g = (1+i)X^2 + iX + 1 \in \mathbb{C}[X]$;
   e) $f = \hat{3}X^4 + X^3 + \hat{4}X^2 + \hat{1} \in \mathbb{Z}_5[X]$, $g = \hat{4}X^2 + X + \hat{2} \in \mathbb{Z}_5[X]$.

2. Utilizând schema lui Horner, determinați câtul și restul împărțirii polinomului f prin polinomul g, în fiecare din cazurile:
   a) $f = 2X^3 + 4X^2 + 10X + 5 \in \mathbb{Z}[X]$, $g = X - 1 \in \mathbb{Z}[X]$;
   b) $f = 3X^4 + 10X^3 + 11X^2 - 12X + \frac{1}{3} \in \mathbb{Q}[X]$, $g = X - \frac{1}{2} \in \mathbb{Q}[X]$;
   c) $f = \pi X^3 + 2X^2 - (\pi + 1)X + 1 \in \mathbb{R}[X]$, $g = X + \pi \in \mathbb{R}[X]$;
   d) $f = (2+3i)X^5 - (1+i)X^4 + iX^2 + X - 1 \in \mathbb{C}[X]$, $g = X + i \in \mathbb{C}[X]$;
   e) $f = \hat{5}X^4 + \hat{3}X^3 + \hat{6}X^2 + \hat{2}X + \hat{1} \in \mathbb{Z}_7[X]$, $g = X + \hat{5} \in \mathbb{Z}_7[X]$.

3. Pentru ce valori ale lui m, restul împărțirii polinomului
   $m^4X^4 + 16X^3 - 32X^2 + 16mX - 32m \in \mathbb{R}[X]$ prin $X - 2$ este egal cu 1?

4. Fie K un corp comutativ și $f \in K[X]$ un polinom, iar $a, b \in K$, $a \neq b$. Demonstrați că restul împărțirii polinomului f prin $(X-a)(X-b)$ este
$$r = \frac{f(a) - f(b)}{a - b} \cdot X + \frac{af(b) - bf(a)}{a - b}.$$

5. Să se determine parametrii $m, n \in \mathbb{Q}$ astfel ca polinomul
   $f = X^4 + mX^3 + 7X^2 + nX + 10$ să se dividă cu polinomul $g = X^2 - 3X + 2$.

6. Fie K un corp comutativ și $f, g \in K[X]$. Demonstrați echivalența:
$$(f, g) = 1 \Leftrightarrow \exists\, u, v \in K[X] \text{ cu } uf + vg = 1.$$

7. Fie K un corp comutativ și $f, g \in K[X]$, $g \neq 0$, iar q și r câtul, respectiv restul împărțirii lui f prin g. Demonstrați egalitatea: $(f, g) = (g, r)$.

8. Fie K un corp comutativ şi $f, g \in K[X]$, $g \neq 0$. Considerăm următoarele împărţiri cu rest:

1) f se împarte la g, dând câtul q_1 şi restul r_1;

2) dacă $r_1 \neq 0$, g se împarte la r_1, dând câtul q_2 şi restul r_2;

3) dacă $r_2 \neq 0$, r_1 se împarte la r_2, dând câtul q_3 şi restul r_3;

....

Demonstraţi că:

a) Şirul acestor împărţiri este finit, adică există un $k \geq 1$ pentru care $r_k = 0$.

b) Avem egalitatea $(f, g) = \begin{cases} g, & \text{pentru } k = 1 \\ r_{k-1}, & \text{pentru } k \geq 2 \end{cases}$

adică c.m.m.d.c. al polinoamelor f şi g este ultimul rest nenul din şirul de împărţiri considerat. (Această metodă se numeşte ***algoritmul lui Euclid***).

9. Să se determine c.m.m.d.c. al polinoamelor:

a) $f, g \in \mathbb{Q}[X]$, $f = X^5 + 3X^4 + 3X^3 + 6X^2 + 4X + 4$, $g = X^4 + X^3 + 3X^2 + 2X + 2$.

b) $f, g \in \mathbb{R}[X]$, $f = X^4 - 1$, $g = X^6 - 1$.

c) $f, g \in \mathbb{C}[X]$, $f = X^3 + 3X^2 + X + 3$, $g = X^3 + (6-i)X^2 + (9-6i)X - 9i$.

10. Arătaţi că polinomul $f = X^2 + 4$ este ireductibil în $\mathbb{R}[X]$, dar este reductibil în $\mathbb{C}[X]$.

11. Arătaţi că polinoamele $f = X^2 + X + \hat{1}$, $g = X^3 + X^2 + \hat{1}$, $h = X^3 + X + \hat{1}$ sunt ireductibile în inelul $\mathbb{Z}_2[X]$.

12. Arătaţi că polinomul $f = X^4 + X^3 + X^2 + X + 1$ este ireductibil în $\mathbb{Q}[X]$.

13. Să se determine c.m.m.d.c. şi c.m.m.m.c. al polinoamelor:

a) $f, g \in \mathbb{Q}[X]$, $f = (X^3 - 1)^{2000}(X^3 - 8)^{1999}$, $g = (X^2 - 3X + 2)^{500}(X^6 - 1)^{1000}$.

b) $f, g \in \mathbb{R}[X]$, $f = (X^2 + 1)^{10}(X^2 - 1)^{20}$, $g = (X^3 - X^2 + X - 1)^{25}(X + 1)^{30}$.

14. Descompuneţi în factori ireductibili în fiecare din inelele de polinoame $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ polinoamele: $f = X^3 - 1$, $g = X^4 - 1$, $h = X^4 + 4$.

15. Descompuneţi în factori ireductibili polinomul $f = X^3 + \hat{2}$ în inelul $\mathbb{Z}_5[X]$.

16. Dacă $p > 0$ este un număr prim şi $a \in \mathbb{Z}_p$, descompuneţi în factori ireductibili polinomul $f = X^p + a$ în inelul $\mathbb{Z}_p[X]$.

17. Descompuneți în factori ireductibili în $\mathbb{C}[X]$ polinomul: $f = X^n - 1$, $n \in \mathbb{N}^*$.

18. Descompuneți în factori ireductibili în $\mathbb{R}[X]$ fiecare din polinoamele:

a) $f = X^{2n} - 1$, $n \in \mathbb{N}^*$; b) $f = X^{2n+1} - 1$, $n \in \mathbb{N}^*$.

Rădăcini ale polinoamelor, descompunerea în factori liniari, ecuații algebrice, formulele lui Viète

Am văzut că dacă $f \in A[X]$, o ***rădăcină în inelul A*** a polinomului f este un element $x_0 \in A$ pentru care $f(x_0) = 0$.

Studiem în special cazul polinoamelor cu coeficienți numerici.

Notăm cu A unul din inelele $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Evident, pentru fiecare din aceste inele avem incluziunile de subinele $A \subseteq \mathbb{C}$ și $A[X] \subseteq \mathbb{C}[X]$. Rezultă că orice polinom $f \in A[X]$ poate fi gândit ca un polinom în $\mathbb{C}[X]$.

Gândind polinomul f în $\mathbb{C}[X]$, putem vorbi de ***rădăcinile lui f în corpul C*** pe care le vom numi – simplu – ***rădăcinile lui f***. Avem așadar următoarea:

Definiție

Pentru orice polinom $f \in A[X]$ numim ***rădăcină*** a lui f numărul $x_0 \in \mathbb{C}$ cu proprietatea $f(x_0) = 0$. (Aici, A este unul din inelele numerice $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$).

Polinomul nul din $\mathbb{C}[X]$ are ca rădăcini toate numerele din $\mathbb{C}$. Polinoamele de grad zero din $\mathbb{C}[X]$ nu au rădăcini, căci sunt constante nenule.

Lăsând aceste cazuri banale la o parte, ne va interesa studiul rădăcinilor polinoamelor de grad ≥ 1. În acest sens, un prim rezultat fundamental – pe care îl acceptăm fără demonstrație – îl constituie:

Teorema fundamentală a algebrei (d'Alembert-Gauss).

Orice polinom $f \in \mathbb{C}[X]$ de grad ≥ 1 are cel puțin o rădăcină în $\mathbb{C}$.

Din teorema fundamentală a algebrei rezultă imediat care sunt polinoamele ireductibile din $\mathbb{C}[X]$. Avem în acest sens următoarea:

Propoziție

Singurele polinoame ireductibile din $\mathbb{C}[X]$ sunt polinoamele de gradul întâi.

Demonstrație. Fie $p \in \mathbb{C}[X]$ un polinom ireductibil. Cum grad(p) ≥ 1, conform teoremei fundamentale a algebrei polinomul f admite o rădăcină $x_0 \in \mathbb{C}$. Conform teoremei lui Bézout, vom avea $p = (X - x_0)q$, unde $q \in \mathbb{C}[X]$. Cum $q \mid p$ și p este ireductibil, avem $q \sim 1$ sau $q \sim p$. Nu este posibil ca $q \sim p$, căci ar rezulta ca $X - x_0 \sim 1$, adică $X - x_0$ ar fi de gradul zero, absurd. Rezultă $q \sim 1$, deci $p \sim X - x_0$ și de aici rezultă grad(p) = 1. Pe de altă parte, am văzut că toate polinoamele de grad 1 sunt ireductibile, ceea ce încheie demonstrația.

De aici decurge mai departe următorul rezultat important, care dă descompunerea unui polinom din $\mathbb{C}[X]$ în factori ireductibili.

Teoremă (de descompunere în factori liniari)

Orice polinom $f \in \mathbb{C}[X]$ de grad $n \geq 1$ are în $\mathbb{C}$ exact n rădăcini (nu neapărat distincte) $x_1, x_2, \ldots, x_n$. În plus, polinomul f se descompune în $\mathbb{C}[X]$ în n factori liniari astfel:

$$f = a_n(X - x_1)(X - x_2)\ldots(X - x_n),$$

unde a_n este coeficientul dominant al lui f.

Demonstrație. Polinomul f se descompune într-un produs de polinoame ireductibile în $\mathbb{C}[X]$, adică într-un produs de polinoame de gradul întâi. Din motive de grade, numărul acestor factori liniari este egal cu n. Fie

$$f = p_1 p_2 \ldots p_n \tag{1}$$

descompunerea de care vorbim, unde $p_i = \alpha_i X + \beta_i$ cu $\alpha_i \in \mathbb{C}^*$, $\beta_i \in \mathbb{C}$, $i = 1, 2, \ldots, n$.

Notând cu $x_i = -\dfrac{\beta_i}{\alpha_i} \in \mathbb{C}$ unica rădăcină a polinomului p_i, rezultă că $p_i = \alpha_i(X - x_i)$, adică $p_i \sim X - x_i$, $i = 1, 2, \ldots, n$. Atunci rădăcinile lui f sunt $x_1, x_2, \ldots, x_n \in \mathbb{C}$ (nu neapărat distincte, căci factorii $p_1, \ldots, p_n$ nu sunt neapărat neasociați). Obținem din (1) că $f \sim (X - x_1)(X - x_2)\ldots(X - x_n)$, prin urmare există $\lambda \in \mathbb{C}^*$ astfel încât

$$f = \lambda(X - x_1)(X - x_2)\ldots(X - x_n); \tag{2}$$

identificând coeficienții dominanți din scrierea (2) rezultă $\lambda = a_n$ și astfel (2) devine

$$f = a_n(X - x_1)(X - x_2)\ldots(X - x_n).$$

Să remarcăm că în cazul particular $n = 2$ obținem cunoscuta descompunere a trinomului de gradul doi în factori liniari.

Așa cum am văzut, rădăcinile $x_1, x_2, \ldots, x_n \in \mathbb{C}$ ale unui polinom $f \in \mathbb{C}[X]$ de grad n nu sunt neapărat distincte. Să presupunem că, după o eventuală renotare, rădăcinile distincte două câte două sunt $x_1, x_2, \ldots, x_k$ şi ele se repetă de $\alpha_1, \alpha_2, \ldots$, respectiv α_k ori, unde $\alpha_1 + \alpha_2 + \ldots + \alpha_k = n$. Spunem atunci că x_1 este ***rădăcină multiplă de ordin*** α_1, x_2 este ***rădăcină multiplă de ordin*** $\alpha_2, \ldots, x_k$ este ***rădăcină multiplă de ordin*** α_k.

Aşadar, dacă $x_0 \in \mathbb{C}$ este o rădăcină a polinomului $f \in \mathbb{C}[X]$, ***ordinul de multiplicitate*** al rădăcinii x_0 este cel mai mare număr $\alpha \in \mathbb{N}^*$ pentru care $(X - x_0)^{\alpha} \mid f$.

Rădăcinile multiple de ordin 1 se mai numesc ***rădăcini simple***, cele multiple de ordin 2 se numesc ***rădăcini duble***, cele multiple de ordin 3 se numesc ***rădăcini triple*** ş.a.m.d.

Atunci avem următoarea:

Propoziţie

Fie $f \in \mathbb{C}[X]$ un polinom de grad $n \geq 1$, având rădăcinile $x_1, x_2, \ldots, x_k$ multiple de ordine $\alpha_1, \alpha_2, \ldots$, respectiv α_k, cu $\alpha_1 + \alpha_2 + \ldots + \alpha_k = n$.

Atunci descompunerea lui f în factori liniari este:

$$f = a_n(X - x_1)^{\alpha_1}(X - x_2)^{\alpha_2} \ldots (X - x_k)^{\alpha_k},$$

unde a_n este coeficientul dominant al polinomului f.

Demonstraţie. Se aplică teorema precedentă şi se ţine seama de definiţia rădăcinilor multiple.

Din această propoziţie decurge imediat următorul rezultat de divizibilitate:

Consecinţă

Fie $f, g \in \mathbb{C}[X]$ două polinoame de grade ≥ 1. Polinomul g divide polinomul f dacă şi numai dacă rădăcinile lui g se află printre rădăcinile lui f, iar ordinele de multiplicitate cu care apar în g sunt cel mult egale cu ordinele de multiplicitate cu care apar în f.

De exemplu, polinomul $g = (X - 1)^2(X + 3)^5$ divide polinomul $f = (X - 1)^{100}(X + 3)^{10}(X + i)^{100}$, dar polinomul $h = (X - 1)^{2000}(X + 3)^{50}$ nu divide polinomul f.

Vom vedea acum care sunt polinoamele ireductibile din $\mathbb{R}[X]$, pentru ca apoi să arătăm descompunerea unui polinom în factori ireductibili în $\mathbb{R}[X]$.

Propoziţie

Polinoamele ireductibile din $\mathbb{R}[X]$ sunt polinoamele de gradul întâi şi polinoamele de gradul doi fără rădăcini reale.

Demonstrație. Am văzut că orice polinom de gradul întâi este ireductibil. De asemenea, orice polinom $p \in \mathbb{R}[X]$ care are gradul doi și nu are rădăcini în $\mathbb{R}$ este ireductibil; într-adevăr, o descompunere a lui p într-un produs de două polinoame de grade mai mici ca 2 ar însemna o descompunere în factori de gradul întâi și aceștia au rădăcini în $\mathbb{R}$, contrar presupunerii asupra polinomului p.

Fie acum $p \in \mathbb{R}[X]$ un polinom ireductibil cu grad(p) ≥ 2. Conform teoremei fundamentale a algebrei polinomul p are o rădăcină $x_0 \in \mathbb{C}$. Nu se poate ca $x_0 \in \mathbb{R}$, căci dacă ar fi așa, din teorema lui Bézout ar rezulta că $p \,\vdots\, (X - x_0)$ în $\mathbb{R}[X]$, deci p ar fi reductibil în $\mathbb{R}[X]$, absurd. Deci $x_0 \in \mathbb{C} \setminus \mathbb{R}$.

Dacă $p = a_n X^n + \ldots + a_1 X + a_0$, din $p(x_0) = 0$ rezultă $a_n x_0^n + \ldots + a_1 x_0 + a_0 = 0$. Trecând la conjugate complexe, rezultă imediat că $a_n\left(\overline{x}_0\right)^n + \ldots + a\overline{x}_0 + a_0 = 0$, adică $p\left(\overline{x}_0\right) = 0$. Așadar, polinomul p are rădăcinile conjugate x_0 și $\overline{x}_0$, deci se divide în $\mathbb{C}[X]$ cu polinomul $q = (X - x_0)(X - \overline{x}_0)$. Dar $q = X^2 - (x_0 + \overline{x}_0)X + x_0\overline{x}_0 \in \mathbb{R}[X]$ și astfel p se divide cu q în $\mathbb{R}[X]$. Există așadar $h \in \mathbb{R}[X]$ astfel încât $p = qh$. Deoarece p este ireductibil e necesar să avem $h \sim 1$ și atunci $p \sim q$. Aceasta înseamnă că p este un polinom de gradul doi, având rădăcinile complexe nereale x_0 și $\overline{x}_0$.

Din această propoziție și din teorema de descompunere în factori ireductibili rezultă ușor următorul rezultat privind descompunerea unui polinom din $\mathbb{R}[X]$ în factori ireductibili:

Corolar. Orice polinom $f \in \mathbb{R}[X]$ de grad ≥ 1 se descompune în $\mathbb{R}[X]$ în mod unic într-un produs de polinoame de gradul întâi sau polinoame de gradul doi fără rădăcini reale. Unicitatea trebuie înțeleasă abstracție făcând de asocieri și de ordinea factorilor.

De exemplu, dacă $f = X^3 + 1 \in \mathbb{R}[X]$, scrierile:

$$f = (X+1)(X^2 - X + 1), \text{ respectiv } f = \left(\frac{1}{3}X^2 - \frac{1}{3}X + \frac{1}{3}\right)(3X+3)$$

reprezintă aceeași descompunere, întrucât

$$X + 1 \sim 3X + 3, \quad X^2 - X + 1 \sim \frac{1}{3}X^2 - \frac{1}{3}X + \frac{1}{3}$$

și este schimbată ordinea factorilor.
Să revenim acum la problema rădăcinilor unui polinom.

Definiție

Dacă $f \in \mathbb{C}[X]$ este un polinom de grad ≥ 1, ecuația

$$f(x) = 0$$

se numeşte ***ecuaţie polinomială*** sau ***ecuaţie algebrică*** asociată polinomului f.

A rezolva această ecuaţie înseamnă a determina toate rădăcinile din corpul $\mathbb{C}$ ale polinomului f.

Uneori, pentru mai multă precizie, spunem că *rezolvăm în corpul* $\mathbb{C}$ ecuaţia respectivă.

Ecuaţiile de gradul întâi sunt ecuaţii algebrice asociate polinoamelor de gradul întâi, iar ecuaţiile de gradul doi sunt ecuaţii algebrice asociate polinoamelor de gradul doi.

Deşi am văzut că orice polinom de grad n are n rădăcini în corpul $\mathbb{C}$ al numerelor complexe, problema aflării acestor rădăcini, deci a rezolvării unei ecuaţii algebrice, este în general o problemă dificilă pentru $n \geq 3$. Există formule de rezolvare pentru ecuaţiile de gradul 3 şi de gradul 4 (aşa cum există pentru ecuaţia de gradul 2), dar acestea sunt greoaie şi practic inaplicabile. Există un rezultat calitativ (teorema Abel-Ruffini) care arată că pentru $n \geq 5$ nici măcar nu se pot obţine astfel de formule generale de rezolvare. Totuşi în scopul rezolvării unei ecuaţii algebrice – atunci când cunoaştem unele informaţii suplimentare privind rădăcinile – sunt utile aşa-zisele relaţii între rădăcini şi coeficienţi sau, cum se mai numesc, formulele lui Viète. În acest sens există următoarea:

Teoremă (Viète)

Fie $f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \in \mathbb{C}[X]$ un polinom de grad n având rădăcinile $x_1, x_2, \ldots, x_n \in \mathbb{C}$, nu neapărat distincte. Atunci au loc egalităţile numite ***formulele lui Viète***:

$$\begin{cases} \sum\limits_{1 \leq i \leq n} x_i = -\dfrac{a_{n-1}}{a_n} \\ \sum\limits_{1 \leq i < j \leq n} x_i x_j = \dfrac{a_{n-2}}{a_n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \sum\limits_{1 \leq i_1 < i_2 < \ldots < i_p \leq n} x_{i_1} x_{i_2} \ldots x_{i_p} = (-1)^p \dfrac{a_{n-p}}{a_n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \prod\limits_{1 \leq i \leq n} x_i = (-1)^n \dfrac{a_0}{a_n} \end{cases}$$

Demonstraţie. Reamintim că prin scrierea $\sum\limits_{1 \leq i_1 < i_2 < \ldots < i_p \leq n}$ înţelegem că suma se face după toate alegerile posibile de sisteme $(i_1, i_2, \ldots, i_p)$ cu $i_1, i_2, \ldots, i_p \in \{1, 2, \ldots, n\}$ şi $i_1 < i_2 < \ldots < i_p$.

Folosim teorema de descompunere în factori liniari:

$$f = a_n(X - x_1)(X - x_2)\dots(X - x_n) =$$

$$= a_n\left[X^n - \left(\sum_{1\le i\le n} x_i\right)X^{n-1} + \left(\sum_{1\le i<j\le n} x_i x_j\right)X^{n-2} - \dots + (-1)^n \prod_{1\le i\le n} x_i\right].$$

Pe de altă parte avem $f = a_n X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0$. Identificăm coeficienții termenilor cu puteri egale ale lui X din cele două scrieri ale polinomului f şi obținem egalitățile din enunțul teoremei.

Rezultatul rămâne valabil în general, conform cu prima din următoarele două:

Observații

1. Dacă un polinom $f \in K[X]$ (K fiind un corp comutativ oarecare), cu grad $f = n$, are în corpul K exact n rădăcini $x_1, x_2, \dots, x_n$, atunci are loc teorema de descompunere în factori liniari şi rămân valabile formulele lui Viète, cu aceleaşi demonstrații ca în cazul $K = \mathbb{C}$.

2. Dacă $x_1, x_2, \dots, x_n \in \mathbb{C}$ şi $S_1 = \sum_{1\le i\le n} x_i$, $S_2 = \sum_{1\le i<j\le n} x_i x_j$, ..., $S_n = \prod_{1\le i\le n} x_i$, atunci polinomul de grad n şi monic $f \in \mathbb{C}[X]$, având rădăcinile $x_1, x_2, \dots, x_n$, este

$$f = (X - x_1)(X - x_2)\dots(X - x_n) = X^n - S_1 X^{n-1} + S_2 X^{n-2} - \dots + (-1)^n S_n.$$

Să ne oprim puțin asupra cazurilor particulare uzuale $n = 2$, $n = 3$, $n = 4$, şi să vedem cum se scriu formulele lui Viète în fiecare din aceste cazuri.

Pentru $n = 2$, formulele lui Viète pentru polinomul $f = aX^2 + bX + c \in \mathbb{C}[X]$ sunt binecunoscute deja:

$$\begin{cases} x_1 + x_2 = -\dfrac{b}{a} \\ x_1 x_2 = \dfrac{c}{a} \end{cases}$$

Pentru $n = 3$ avem $f = aX^3 + bX^2 + cX + d \in \mathbb{C}[X]$, iar formulele lui Viète pentru f se scriu:

$$\begin{cases} x_1 + x_2 + x_3 = -\dfrac{b}{a} \\ x_1 x_2 + x_1 x_3 + x_2 x_3 = \dfrac{c}{a} \\ x_1 x_2 x_3 = -\dfrac{d}{a} \end{cases}$$

Pentru $n = 4$ avem $f = aX^4 + bX^3 + cX^2 + dX + e \in \mathbb{C}[X]$, iar formulele lui Viète se scriu:

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = -\dfrac{b}{a} \\ x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 = \dfrac{c}{a} \\ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = -\dfrac{d}{a} \\ x_1x_2x_3x_4 = \dfrac{e}{a} \end{cases}$$

În acest caz, dacă notăm $s_1 = x_1 + x_2$, $s_2 = x_3 + x_4$, $p_1 = x_1x_2$, $p_2 = x_3x_4$, formulele lui Viète se pot scrie astfel:

$$\begin{cases} s_1 + s_2 = -\dfrac{b}{a} \\ s_1s_2 + p_1 + p_2 = \dfrac{c}{a} \\ s_1p_2 + s_2p_1 = -\dfrac{d}{a} \\ p_1p_2 = \dfrac{e}{a} \end{cases}$$

Uneori, în aplicații, această ultimă scriere se dovedește utilă.

Ca tipuri speciale de ecuații algebrice, pentru care dispunem de metode de rezolvare, menționăm ecuațiile binome și ecuațiile reciproce, dar și ecuațiile bipătrate, bicubice etc.

O ***ecuație binomă*** este o ecuație de forma

$$x^n = u,$$

unde $n \in \mathbb{N}^*$ și $u \in \mathbb{C}$.

A rezolva această ecuație revine la a determina rădăcinile de ordinul n din numărul complex u, ceea ce se cunoaște din clasa a X-a.

O ***ecuație reciprocă*** este o ecuație de forma

$$a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$$

unde coeficienții $a_i \in \mathbb{C}$ satisfac egalitățile

$$a_{n-1} = a_i,\ i = 0, 1, 2, \ldots, n.$$

În rezolvarea unei asemenea ecuații distingem două cazuri:

I. n par. Deoarece $a_0 = a_n \neq 0$ ecuația nu admite rădăcina $x = 0$. Prin urmare putem împărți ecuația cu $x^{\frac{n}{2}}$ și apoi folosim substituția $y = x + \dfrac{1}{x}$. Se obține o ecuație în y de grad $\dfrac{n}{2}$. Dacă putem rezolva această ecuație, determinându-i rădăcinile $y_1, y_2, \ldots, y_{\frac{n}{2}}$, avem de rezolvat după aceea $\frac{n}{2}$ ecuaţii de gradul doi de forma $x+\frac{1}{x}=y_i$, $i = 1, 2, \ldots, \frac{n}{2}$.

II. n impar. Se observă uşor că $x = -1$ este o rădăcină a ecuaţiei, după care, împărţind prin $x + 1$, rămâne de rezolvat o ecuaţie reciprocă de gradul $n - 1$ (conform cu exerciţiul 8 punctul a), pag. 100) adică problema se reduce la cazul precedent.

O ***ecuaţie bipătrată*** este de forma

$$ax^4 + bx^2 + c = 0$$

şi prin substituţia $y = x^2$ devine o ecuaţie de gradul 2 în y.

O ***ecuaţie bicubică*** are forma

$$ax^6 + bx^3 + c = 0$$

şi prin substituţia $y = x^3$ devine o ecuaţie de gradul 2 în y.

Exerciţii rezolvate

1. Să se arate că pentru orice $n \in \mathbb{N}$ polinomul $X^{12n+2} - X^{6n+1} + 1$ se divide cu polinomul $X^2 - X + 1$.

Soluţie. Fie $f = X^{12n+2} - X^{6n+1} + 1$ şi $g = X^2 - X + 1$. Este suficient să dovedim că rădăcinile polinomului g sunt rădăcini ale polinomului f; într-adevăr, rădăcinile lui g sunt simple (discriminantul fiind nenul) şi se aplică atunci consecinţa de la pag. 115. Să notăm cu $x \in \mathbb{C}$ o rădăcină oarecare a polinomului g, deci $g(x) = 0$, adică $x^2 - x + 1 = 0$. Înmulţind această egalitate cu $x + 1$ obţinem $x^3 + 1 = 0$, de unde $x^3 = -1$. Ridicând la pătrat rezultă $x^6 = 1$. Atunci:

$$f(x) = x^{12n+2} - x^{6n+1} + 1 = \left(x^6\right)^{2n} \cdot x^2 - \left(x^6\right)^n \cdot x + 1 = x^2 - x + 1 = 0,$$

ceea ce înseamnă că x este rădăcină şi pentru polinomul f.

2. Să se determine parametrul $m \in \mathbb{C}$ şi să se rezolve ecuaţia

$$x^4 + 10x^3 + mx^2 + 50x + 24 = 0$$

ştiind că suma a două rădăcini este egală cu suma celorlalte două rădăcini.

Soluţie. Fie $x_1, x_2, x_3, x_4 \in \mathbb{C}$ rădăcinile ecuaţiei considerate.

Notând $s_1 = x_1 + x_2$, $s_2 = x_3 + x_4$, $p_1 = x_1 x_2$, $p_2 = x_3 x_4$, formulele lui Viète se scriu:

$$\begin{cases} s_1 + s_2 = -10 & (1) \\ s_1 s_2 + p_1 + p_2 = m & (2) \\ s_1 p_2 + s_2 p_1 = -50 & (3) \\ p_1 p_2 = 24 & (4) \end{cases}$$

iar ipoteza în care lucrăm se scrie:

$$s_1 = s_2 \qquad (5)$$

Din (1) şi (5) rezultă $s_1 = s_2 = -5$ şi introducând în (3) şi (4) obţinem:

$$\begin{cases} -5p_1 - 5p_1 = -50 \\ p_1 p_2 = 24 \end{cases} \text{ sau } \begin{cases} p_1 + p_2 = 10 \\ p_1 p_2 = 24 \end{cases}$$

Ecuaţia în p cu rădăcinile p_1, p_2 este atunci $p^2 - 10p + 24 = 0$, de unde obţinem $p_1 = 4$, $p_2 = 6$.

Înlocuind în (2) avem $(-5)(-5) + 4 + 6 = m$, adică $m = 35$.

Deoarece $s_1 = x_1 + x_2 = -5$, $p_1 = x_1 x_2 = 6$, rezultă că ecuaţia în x cu rădăcinile x_1, x_2 este $x^2 + 5x + 4 = 0$, de unde obţinem $x_1 = -4$, $x_2 = -1$.

Deoarece $s_2 = x_3 + x_4 = -5$, $p_2 = x_3 x_4 = 6$, rezultă că ecuaţia în x cu rădăcinile x_3, x_4 este $x^2 + 5x + 6 = 0$, de unde obţinem $x_3 = -3$, $x_4 = -2$.

Aşadar ecuaţia are rădăcinile $x_1 = -4$, $x_2 = -1$, $x_3 = -3$, $x_4 = -2$.

3. Să se rezolve în corpul $\mathbb{C}$ ecuaţia $6x^5 - 23x^4 + 13x^3 + 13x^2 - 23x + 6 = 0$.

Soluţie. Ecuaţia este reciprocă de grad impar, deci admite rădăcina $x_1 = -1$. Conform teoremei lui Bézout, polinomul $f = 6X^5 - 23X^4 + 13X^3 + 13X^2 - 23X + 6$ se divide prin polinomul $g = X + 1$. Câtul împărţirii se obţine uşor cu schema lui Horner:

	6	−23	13	13	−23	6
−1	6	−29	42	−29	6	0

Acest cât este polinomul $q = 6X^4 - 29X^3 + 42X^2 - 29X + 6$.

Rămâne de rezolvat ecuaţia $6x^4 - 29x^2 + 42x^2 - 29x + 6 = 0$. Fiind o ecuaţie reciprocă de grad par $n = 4$, o împărţim prin $x^{\frac{n}{2}} = x^2$ şi obţinem:

$$6\left(x^2 + \frac{1}{x^2}\right) - 29\left(x + \frac{1}{x}\right) + 42 = 0.$$

Notând $y = x + \frac{1}{x}$, rezultă $x^2 + \frac{1}{x^2} = y^2 - 2$ şi obţinem o ecuaţie în y:

$$6(y^2 - 1) - 29y + 42 = 0 \text{ sau } 6y^2 - 29y + 30 = 0,$$

de unde $y_1 = \frac{3}{2}$, $y_2 = \frac{10}{3}$. Rezultă ecuaţiile $x + \frac{1}{x} = \frac{3}{2}$, $x + \frac{1}{x} = \frac{10}{3}$.

Prima ecuaţie are rădăcinile $x_2 = \frac{3 - i\sqrt{7}}{4}$, $x_3 = \frac{3 + i\sqrt{7}}{4}$, iar a doua ecuaţie are rădăcinile $x_4 = \frac{1}{3}$, $x_5 = 3$. Rădăcinile ecuaţiei iniţiale sunt:

$$x_1 = -1,\ x_2 = \frac{3 - i\sqrt{7}}{4},\ x_3 = \frac{3 + i\sqrt{7}}{4},\ x_4 = \frac{1}{3},\ x_5 = 3.$$

4. Dacă $f = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{C}[X]$, polinomul

$f' = a_1 + 2a_2X + \ldots + na_nX^{n-1} \in \mathbb{C}[X]$ se numeşte ***derivata*** lui f, polinomul $f'' = (f')'$ se numeşte ***derivata de ordin* 2** a lui f şi, în general, polinomul $f^{(k)} = \left(f^{(k-1)}\right)'$ se numeşte ***derivata de ordinul k*** a lui f. Să se arate că:

a) dacă $f, g \in \mathbb{C}[X]$, atunci au loc egalităţile:

$$(f+g)' = f' + g';\ (fg)' = f'g + fg';\ \left(f^{\alpha}\right)' = \alpha f^{\alpha-1}\cdot f' \quad (\alpha \in \mathbb{N}^*);$$

b) dacă $f \in \mathbb{C}[X]$, $x_0 \in \mathbb{C}$ este o rădăcină a lui f şi $\alpha \in \mathbb{N}$, $\alpha \geq 2$, avem echivalenţa:

$$\begin{cases} x_0 \text{ este rădăcină multiplă de} \\ \quad \text{ordin } \alpha \text{ pentru } f \end{cases} \Leftrightarrow \begin{cases} x_0 \text{ este rădăcină multiplă de} \\ \quad \text{ordin } \alpha - 1 \text{ pentru } f' \end{cases}$$

c) dacă $f \in \mathbb{C}[X]$, $x_0 \in \mathbb{C}$ şi $\alpha \in \mathbb{N}$, $\alpha \geq 2$, avem echivalenţa:

$$\begin{cases} x_0 \text{ este rădăcină multiplă de} \\ \quad \text{ordin } \alpha \text{ pentru } f \end{cases} \Leftrightarrow \begin{cases} f(x_0) = f'(x_0) = f''(x_0) = \ldots = f^{(\alpha-1)}(x_0) = 0 \\ \text{şi } f^{(\alpha)}(x_0) \neq 0 \end{cases}$$

Soluţie. a) Fie $f = \sum_i a_iX^i$, $g = \sum_j b_jX^j$, sumele fiind finite. Atunci $f + g = \sum_k (a_k + b_k)X^k$. Rezultă conform definiţiei derivatei:

$$(f+g)' = \sum_k k(a_k + b_k)X^{k-1} = \sum_k ka_kX^{k-1} = \sum_k kb_kX^{k-1} = f' + g'.$$

De asemenea

$$fg = \sum_{i,j} a_ib_jX^{i+j}, \text{ deci } (fg)' = \sum_{i,j}(i+j)a_ib_jX^{i+j-1}. \tag{1}$$

Pe de altă parte:

$$f'g + fg' = \left(\sum_i ia_iX^{i-1}\right)\left(\sum_j b_jX^j\right) + \left(\sum_i a_iX^i\right)\left(\sum_j jb_jX^{j-1}\right) =$$

$$= \sum_{i,j} ia_ib_jX^{i+j-1} + \sum_{i,j} ja_ib_jX^{i+j-1} = \sum_{i,j}(i+j)a_ib_jX^{i+j-1}. \tag{2}$$

Din (1) şi (2) rezultă egalitatea $(fg)' = f'g + fg'$.

În fine, ultima egalitate se demonstrează prin inducţie după α. Pentru $\alpha = 1$ egalitatea se scrie $f' = f'$ şi este evidentă. Dacă o presupunem adevărată pentru α, atunci

$$\left(f^{\alpha+1}\right)' = \left(f^{\alpha}\cdot f\right)' = \left(f^{\alpha}\right)' f + f^{\alpha}\cdot f' = \alpha f^{\alpha-1} f'f + f^{\alpha}\cdot f' = \alpha f^{\alpha} f' + f^{\alpha} f' = (\alpha+1) f^{\alpha} f',$$

adică egalitatea este adevărată şi pentru $\alpha + 1$.

b) „$\Rightarrow$”. Presupunem că x_0 este rădăcină de ordin α pentru f, adică $f = (X - x_0)^{\alpha} g$, unde $g \in \mathbb{C}[X]$ şi $g(x_0) \neq 0$.

Atunci

$$f' = \alpha(X-x_0)^{\alpha-1}(X-x_0)'g + (X-x_0)^{\alpha}g' = (X-x_0)^{\alpha-1}\left[\alpha g + (X-x_0)g'\right] = (X-x_0)^{\alpha-1}h$$

unde am notat $h = \alpha g + (X-x_0)g' \in \mathbb{C}[X]$. Cum $h(x_0) = \alpha g(x_0) \neq 0$, înseamnă că x_0 este rădăcină de ordin $\alpha - 1$ pentru f'.

„$\Leftarrow$". Presupunem că x_0 este rădăcină de ordin $\alpha - 1$ pentru f'. Dacă $\beta \in \mathbb{N}^*$ este ordinul de multiplicitate al rădăcinii x_0 în polinomul f (atenție, știm că x_0 este rădăcină a lui f), conform cu implicația precedentă, deja probată, rezultă că x_0 este rădăcină de ordin $\beta - 1$ pentru f'.

Așadar $\beta - 1 = \alpha - 1$, deci $\beta = \alpha$, adică x_0 este rădăcină multiplă de ordin α a lui f.

c) „$\Rightarrow$". Presupunem că x_0 este rădăcină de ordin α pentru f. Aplicând repetat punctul b) deducem că x_0 este rădăcină de ordin $\alpha - 1$ pentru f', de ordin $\alpha - 2$ pentru f'', ..., de ordin 1 pentru $f^{(\alpha-1)}$.

Așadar $f(x_0) = f'(x_0) = f''(x_0) = \ldots = f^{(\alpha-1)}(x_0) = 0$ și $f^{(\alpha)}(x_0) \neq 0$.

„$\Leftarrow$". Presupunem că $f(x_0) = f'(x_0) = f''(x_0) = \ldots = f^{(\alpha-1)}(x_0) = 0$ și $f^{(\alpha)}(x_0) \neq 0$. Din $f^{(\alpha-1)}(x_0) = 0$ și $f^{(\alpha)}(x_0) \neq 0$ rezultă că x_0 este rădăcină de ordin 1 pentru $f^{(\alpha-1)}$. Pe baza lui b) rezultă că x_0 este rădăcină de ordin 2 pentru $f^{(\alpha-2)}$, ..., de ordin α pentru f.

Caracterizarea rădăcinilor multiple cu ajutorul derivatelor, pe care am obținut-o la punctul c) din acest exercițiu, este foarte utilă. Să mai observăm că derivatele polinoamelor se obțin prin niște derivări „formale", care sunt însă inspirate de regulile de derivare pe care le cunoaștem de la funcții reale.

5. Fie $K = \{a_1 = 0, a_2 = 1, a_3, \ldots, a_q\}$ un corp finit cu q elemente.

a) Să se descompună în factori ireductibili polinomului $f = X^q - X \in K[X]$.

b) Să se demonstreze teorema lui Wilson, utilizând formulele lui Viète pentru polinomul $g = X^{p-1} - \hat{1} \in \mathbb{Z}_p[X]$, unde $p > 0$ este un număr prim.

Soluție. a) Observăm că pentru orice $a \in K$ avem $a^q = a$; într-adevăr, pentru $a = 0$ este evident, iar pentru $a \neq 0$, în grupul $(K^*, \cdot)$ care are ordinul $q - 1$, avem $a^{q-1} = 1$, de unde $a^q = a$. Înseamnă că orice $a \in K$ este o rădăcină a polinomului $f = X^q - X \in K[X]$. Atunci, acest polinom se descompune în inelul $K[X]$ în factori liniari, adică:

$$f = X^q - X = \prod_{a \in K}(X-a) = X(X-1)(X-a_3)\ldots(X-a_q).$$

b) Polinomul $g = X^{p-1} - \hat{1} \in \mathbb{Z}_p[X]$ are ca rădăcini elementele nenule din corpul $\mathbb{Z}_p$, deci clasele $\hat{1}, \hat{2}, \ldots, (\widehat{p-1})$. Din ultima formulă Viète avem:

$$\hat{1}\cdot\hat{2}\cdot\ldots\cdot(\widehat{p-1}) = (-1)^{p-1}(-\hat{1}) = -\hat{1} \text{ pentru } p \text{ impar,}$$

de unde: $(p-1)!+1$ se divide cu p, adică teorema lui Wilson.

Pentru $p = 2$, teorema este evidentă.

6. Fie K un subcorp al corpului comutativ Ω şi $\alpha \in \Omega$ un ***element algebric*** peste K, adică rădăcină a unui polinom nenul din $K[X]$. Să se demonstreze că:

1°. Există un unic polinom monic de grad minim $f \in K[X]$ cu proprietatea că $f(\alpha) = 0$ (f se numeşte ***polinomul minimal*** al lui α).

2°. Pentru $g \in K[X]$ avem echivalenţa $g(\alpha) = 0 \Leftrightarrow g \,\vdots\, f$.

3°. Polinomul f este ireductibil în inelul $K[X]$.

4°. Dacă $g \in K[X]$ este ireductibil şi $g(\alpha) = 0$, atunci $g \sim f$.

5°. Dacă $\mathrm{grad}(f) = n$, atunci $K(\alpha) = \{ a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in K\}$ este un subcorp al lui Ω şi este cel mai mic subcorp al lui Ω ce conţine pe K şi pe α (acest corp $K(\alpha)$ se numeşte ***corpul obţinut din K prin adjuncţionarea lui*** α).

Soluţie. 1°. Mulţimea $A = \{g \in K[X] \mid g \neq 0,\ g(\alpha) = 0\}$ este nevidă, deoarece α este algebric peste K. Mulţimea gradelor polinoamelor din A este o submulţime nevidă a mulţimii $\mathbb{N}^*$, deci are un minim $n \in \mathbb{N}^*$. Aşadar există un polinom nenul $f \in K[X]$, de grad minim n, astfel încât $f(\alpha) = 0$. În plus, abstracţie făcând de o asociere, polinomul f poate fi gândit ca un polinom monic şi atunci este unic determinat.

2°. ($\Rightarrow$). Fie $g \in K[X]$ cu $g(\alpha) = 0$. Din teorema împărţirii cu rest, avem $g = fq + r$, unde $q, r \in K[X]$ şi $\mathrm{grad}(r) < \mathrm{grad}(f) = n$. Atunci $g(\alpha) = f(\alpha)q(\alpha) + r(\alpha)$ şi cum $g(\alpha) = 0$, $f(\alpha) = 0$ rezultă $r(\alpha) = 0$.

Deoarece gradul minim al polinoamelor nenule din $K[X]$ care îl au pe α ca rădăcină este n, iar $\mathrm{grad}(r) < n$, rezultă în mod necesar $r = 0$. Atunci $g = fq$, deci $g \,\vdots\, f$.
($\Leftarrow$). Dacă $g \,\vdots\, f$, avem $g = fq$ cu $q \in K[X]$ şi atunci $g(\alpha) = f(\alpha)q(\alpha) = 0q(\alpha) = 0$.

3°. Polinomul f se descompune în inelul $K[X]$ în factori ireductibili. Cum $f(\alpha) = 0$, există un factor ireductibil h al lui f astfel încât $h(\alpha) = 0$. Conform cu 2° avem $f \mid h$ şi cum ştim deja că $h \mid f$, rezultă $f \sim h$. Cum h este ireductibil în $K[X]$, înseamnă că şi f este ireductibil în $K[X]$.

4°. Dacă $g \in K[X]$ este ireductibil şi $g(\alpha) = 0$, conform cu 2° avem $g \,\vdots\, f$, dar g fiind ireductibil, orice divizor al său de grad ≥ 1 este asociat cu g. Aşadar $f \sim g$.

5°. Demonstrăm mai întâi egalitatea de mulţimi:

$$K(\alpha) = \{h(\alpha) \mid h \in K[X]\}. \tag{1}$$

($\subseteq$). Fie $x \in K(\alpha)$ arbitrar, $x = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ unde $a_0, a_1, \ldots, a_{n-1} \in K$. Atunci $x = h(\alpha)$ unde $h = a_0 + a_1X + \ldots + a_{n-1}X^{n-1} \in K[X]$.

($\supseteq$). Fie $h \in K[X]$ arbitrar. Conform teoremei împărţirii cu rest avem $h = fq + r$, cu $q, r \in K[X]$, $\mathrm{grad}(r) < \mathrm{grad}(f) = n$. Atunci $r = a_0 + a_1X + \ldots + a_{n-1}X^{n-1}$ unde $a_0, a_1, \ldots, a_{n-1} \in K$. Rezultă $h(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha) = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \in K(\alpha)$. Dubla incluziune probată arată că egalitatea (1) este adevărată. Din (1) rezultă imediat că mulţimea $K(\alpha)$ este un subinel al corpului Ω. Într-adevăr dacă $x,y \in K(\alpha)$, există

$h_1, h_2 \in K[X]$ cu $x = h_1(\alpha)$, $y = h_2(\alpha)$. Atunci: $x - y = h_1(\alpha) - h_2(\alpha) = (h_1 - h_2)(\alpha) \in$ $\in K(\alpha)$, $xy = h_1(\alpha) h_2(\alpha) = (h_1 h_2)(\alpha) \in K(\alpha)$, iar $1 \in K \subseteq K(\alpha)$. Rămâne să mai arătăm că orice element nenul din $K(\alpha)$ este inversabil în $K(\alpha)$.

Fie $x = h(\alpha) \in K(\alpha) \setminus \{0\}$. Conform cu 2° rezultă că h nu se divide cu f şi cum f este ireductibil, înseamnă că $(h, f) = 1$. Atunci există $u, v \in K[X]$ astfel încât $uh + vf =$ $= 1$. Trecând la valoarea în punctul α avem $u(\alpha)h(\alpha) = 1$, ceea ce arată că inversul lui $h(\alpha)$ este $u(\alpha) \in K(\alpha)$. Aşadar $K(\alpha)$ este un corp comutativ, mai precis un subcorp al corpului Ω. Arătăm acum că dacă $L \subseteq \Omega$ este un alt subcorp al lui Ω ce conţine pe K şi α, atunci $K(\alpha) \subseteq L$. Într-adevăr, cum $K \subseteq L$ şi $\alpha \in L$, iar L este un corp, rezultă că toate elementele de forma $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ cu $a_0, a_1, \ldots, a_{n-1} \in K$ aparţin lui L, adică în definitiv $K(\alpha) \subseteq L$. Aceasta arată că dintre subcorpurile lui Ω ce conţin pe K şi α, subcorpul $K(\alpha)$ este cel mai mic.

EXERCIŢII PROPUSE

1. Să se arate că polinomul f se divide cu polinomul g în fiecare din cazurile de mai jos:

a) $f, g \in \mathbb{Q}[X]$, $f = (X-2)^{1000} + \left(X^2 - X - 1\right)^{999}$, $g = X - 1$.

b) $f, g \in \mathbb{Q}[X]$, $f = X^{6n+5} + X^{3n+1} + 1$, $g = X^2 + X + 1$, $n \in \mathbb{N}$.

c) $f, g \in \mathbb{R}[X]$, $f = \sqrt{2}\left(X^2 + X - 1\right)^{2n+1} - \sqrt{2}X$, $g = \pi(X^2 - 1)$, $n \in \mathbb{N}$.

d) $f, g \in \mathbb{C}[X]$, $f = i(X^{4m} + X^{4n+1} + X^{4p+2} + X^{4q+3})$,

$$g = X^3 + X^2 + X + 1,\ m, n, p, q \in \mathbb{N}.$$

2. Fie $f \in \mathbb{C}[X]$ cu proprietatea că $f(x+1) = f(x)$, $\forall\, x \in \mathbb{C}$.
Arătaţi că f este un polinom constant.

3. Să se determine polinomul $f \in \mathbb{C}[X]$ cu proprietatea

$$xf(x) = (x+1)f(x+1),\ \forall\, x \in \mathbb{C}.$$

4. Să se determine polinoamele $f \in \mathbb{C}[X]$ cu proprietatea:

$$xf(x) = (x-1)f(x+1),\ \forall\, x \in \mathbb{C}.$$

5. Descompuneţi în factori liniari polinomul:

$$f = 1 + \frac{X}{1!} + \frac{X(X+1)}{2!} + \ldots + \frac{X(X+1)\ldots(X+n-1)}{n!} \in \mathbb{C}[X],\ n \in \mathbb{N}^*.$$

6. Să se determine $a, b, c \in \mathbb{C}$ şi apoi să se afle rădăcinile polinoamelor

$$f = X^4 + aX^2 + bX + 2, \quad g = X^3 - 3X + c$$

ştiind că au o rădăcină dublă comună.

7. Să se arate că polinomul

$$f = 1 + \frac{X}{1!} + \frac{X^2}{2!} + \ldots + \frac{X^n}{n!} \in \mathbb{C}[X], \ n \in \mathbb{N}^*,$$

are numai rădăcini simple.

8. Dacă x_1, x_2, x_3 sunt rădăcinile ecuaţiei $x^3 + ix + 1 = 0$, să se calculeze:

a) $x_1 + x_2 + x_3$;
b) $x_1^2 + x_2^2 + x_3^2$;
c) $x_1^3 + x_2^3 + x_3^3$;
d) $x_1^4 + x_2^4 + x_3^4$.

9. Să se arate că polinomul:

$$f = X^4 + (a+1)X^3 + \left(a^2 + \frac{a}{2} + 1\right)X^2 + bX + c \in \mathbb{R}[X]$$

are cel mult două rădăcini reale.

10. Fie x_1, x_2, x_3 rădăcinile ecuaţiei $x^3 + ax^2 + bx + 1 = 0$, $a, b \in \mathbb{C}$. Să se formeze ecuaţia de gradul trei în y care are rădăcinile:

$$y_1 = 1 + \frac{1}{x_1}, \quad y_2 = 1 + \frac{1}{x_2}, \quad y_3 = 1 + \frac{1}{x_3}.$$

11. Să se determine $m \in \mathbb{R}^*$ astfel încât ecuaţia $x^3 - (m+1)x^2 + (m-2)x + 2m = 0$ să aibă o rădăcină dublă, apoi să se rezolve ecuaţia.

12. Să se determine $m, n \in \mathbb{R}$ şi să se rezolve ecuaţia $x^5 - 2x^4 + x^3 - x^2 + mx + n = 0$ ştiind că are o rădăcină reală triplă.

13. Să se determine $m \in \mathbb{C}$ şi să se rezolve ecuaţia $x^3 - 5x^2 - 2x + m = 0$ ştiind că $x_1 + x_2 = 7$.

14. Să se determine $m \in \mathbb{C}$ şi să se rezolve ecuaţia $x^4 - 20x^3 + mx^2 - 240x + 144 = 0$ ştiind că între rădăcinile sale există relaţia $x_1 - x_2 = x_3 - x_4$.

15. Să se rezolve ecuaţia $x^4 + x^3 - 19x^2 + 11x + m = 0$, $m \in \mathbb{R}$ ştiind că suma a două rădăcini este egală cu -3.

16. Fie $f \in \mathbb{R}[X]$ un polinom de gradul 4 având rădăcinile în progresie aritmetică. Să se arate că polinomul derivat f' are de asemenea rădăcinile în progresie aritmetică.

17. Să se rezolve în corpul $\mathbb{C}$ ecuațiile binome:

a) $x^3 = 2$; b) $x^4 = i$; c) $x^5 = 1+i$; d) $x^6 = -1$;
e) $x^5 = -1+i\sqrt{3}$; f) $x^{100} + x = 0$; g) $2x^{101} - x = 0$.

18. Să se rezolve în corpul $\mathbb{C}$ ecuațiile:

a) $x^{2000} - 5x^{1000} + 6 = 0$; b) $x^{20} + x^{10} + 1 = 0$;
c) $x^6 - 35ix^3 - 216 = 0$; d) $x^8 - 17a^4x^4 + 16a^8 = 0$, $a \in \mathbb{R}$.

19. Să se rezolve în corpul $\mathbb{C}$ ecuațiile reciproce:

a) $x^3 + 6x^2 + 6x + 1 = 0$; b) $2x^3 + 7x^2 + 7x + 2 = 0$;
c) $6x^4 + 35x^3 + 62x^2 + 35x + 6 = 0$; d) $2x^4 + 7x^3 + 9x^2 + 7x + 2 = 0$;
e) $15x^5 - 113x^4 + 162x^3 + 162x^2 - 113x + 15 = 0$.

20. Două localități A și B sunt la o distanță de 240 km. Un tren pleacă din A spre B, iar peste o jumătate de oră alt tren pleacă din B spre A. Știind că trenul ce pleacă din B are o viteză cu 12 km/h mai mare decât a celui ce pleacă din A și că ele se întâlnesc la mijlocul distanței dintre cele două localități, să se afle vitezele celor două trenuri.

21. Să se arate că:

a) Numărul $2\cos\dfrac{2\pi}{5}$ este rădăcină a ecuației $x^2 + x - 1 = 0$ și să se determine $\cos\dfrac{2\pi}{5}$;

b) Numărul $2\cos\dfrac{2\pi}{7}$ este rădăcină a ecuației $x^3 + x^2 - 2x - 1 = 0$.

22. Un trapez isoscel circumscris unui cerc are perimetrul de 20 cm, iar aria de 20 cm^2. Să se afle lungimile laturilor trapezului.

23. Să se demonstreze egalitățile:

$$\cos n\alpha = P_n(\cos\alpha),\quad \sin n\alpha = \sin\alpha\, Q_{n-1}(\cos\alpha),$$

unde P_n, Q_{n-1} sunt anumite polinoame cu coeficienți întregi, având gradele n, respectiv $n-1$ ($n \in \mathbb{N}^*$, $\alpha \in \mathbb{R}$).

Rezolvarea ecuațiilor algebrice cu coeficienți în $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$

În această lecție studiem câteva proprietăți speciale pe care le întâlnim la rădăcinile polinoamelor din inelele $\mathbb{R}[X]$, $\mathbb{Q}[X]$, $\mathbb{Z}[X]$. Primul rezultat se referă la rădăcinile polinoamelor cu coeficienți reali.

Teoremă

Dacă un polinom $f \in \mathbb{R}[X]$ admite o rădăcină $x_0 \in \mathbb{C} \setminus \mathbb{R}$, atunci admite și rădăcina conjugată $\overline{x}_0$, cu același ordin de multiplicitate.

Demonstrație. Fie $f = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{R}[X]$. Deoarece $f(x_0) = 0$ avem $a_0 + a_1x_0 + a_2x_0^2 + \ldots + a_nx_0^n = 0$. Trecând la conjugatele complexe în ultima egalitate și ținând seama de proprietățile conjugării, obținem $a_0 + a_1\overline{x}_0 + a_2(\overline{x}_0)^2 + \ldots + a_n(\overline{x}_0)^n = 0$, adică $f(\overline{x}_0) = 0$. Așadar, dacă x_0 este rădăcină, rezultă că și $\overline{x}_0$ este rădăcină.

Fie α ordinul de multiplicitate al rădăcinii x_0 și β ordinul de multiplicitate al rădăcinii $\overline{x}_0$. Vom arăta că $\alpha = \beta$.

Să presupunem prin absurd că $\alpha \neq \beta$, de exemplu $\alpha > \beta$.

Ținând seama de descompunerea în factori liniari, rezultă că polinomul f se divide cu $(X - x_0)^\alpha(X - \overline{x}_0)^\beta$ în $\mathbb{C}[X]$, deci $f = (X - x_0)^\alpha(X - \overline{x}_0)^\beta g$, unde $g \in \mathbb{C}[X]$ nu are rădăcini pe x_0 sau $\overline{x}_0$. Cum $\alpha > \beta$, ultima egalitate se scrie:

$$f = [(X - x_0)(X - \overline{x}_0)]^\beta \cdot (X - x_0)^{\alpha-\beta} \cdot g = [X^2 - (x_0 - \overline{x}_0)X + x_0\overline{x}_0]^\beta \cdot (X - x_0)^{\alpha-\beta} \cdot g.$$

Dar polinomul $X^2 - (x_0 - \overline{x}_0)X + x_0\overline{x}_0 \in \mathbb{R}[X]$ și atunci din egalitatea

$$f = [X^2 - (x_0 - \overline{x}_0)X + x_0\overline{x}_0]^\beta \cdot (X - x_0)^{\alpha-\beta} \cdot g$$

rezultă că polinomul $(X - x_0)^{\alpha-\beta} g \in \mathbb{R}[X]$ are rădăcina $x_0 \in \mathbb{C} \setminus \mathbb{R}$ și nu mai admite rădăcina conjugată $\overline{x}_0$, contradicție cu ce am demonstrat deja.

Înainte de a pune în evidență o proprietate de același tip pentru polinoamele cu coeficienți raționali, facem o mică pregătire.

Fie $d \in \mathbb{Z}$ un întreg care nu este pătrat perfect. Notăm cu $\sqrt{d}$ una din cele două rădăcini din corpul $\mathbb{C}$ ale ecuației

$$x^2 = d.$$

De obicei, când $d > 0$ prin $\sqrt{d}$ înțelegem rădăcina pătrată „aritmetică", adică numărul real pozitiv al cărui pătrat este egal cu d; când $d < 0$, prin $\sqrt{d}$ înțelegem numărul complex $i\sqrt{-d}$.

De exemplu: $\sqrt{-8} = i\sqrt{8}$.

Considerăm corpul pătratic $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$, introdus în exemplul 4 pag. 66. În general, avem incluziunea de subcorpuri $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$, iar când $d > 0$ avem $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}$. Cum $d \in \mathbb{Z}$ nu este pătrat perfect, rezultă uşor că $\sqrt{d} \notin \mathbb{Q}$, iar scrierea unui număr sub forma $a + b\sqrt{d}$, cu $a, b \in \mathbb{Q}$, este unică.

Pentru fiecare $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, considerăm numărul

$$z^* = a - b\sqrt{d} \in \mathbb{Q}(\sqrt{d}),$$

care se numeşte ***conjugatul pătratic*** al lui z. Dacă $d < 0$, conjugatul pătratic al lui z coincide cu conjugatul complex al lui z. De exemplu. pentru $d = -8$, avem:

$$z = 5 + \sqrt{-8} = 5 + i\sqrt{8} \Rightarrow z^* = 5 - \sqrt{-8} = 5 - i\sqrt{8} = \overline{z}.$$

Dacă $d > 0$, conjugatul pătratic al lui z diferă de conjugatul complex al lui z.
De exemplu pentru $d = 2$ avem:

$$z = 3 + 10\sqrt{2} \Rightarrow z^* = 3 - 10\sqrt{2}, \text{ în timp ce } \overline{z} = 3 + 10\sqrt{2}, \text{ căci } z \in \mathbb{R}.$$

Conjugarea pătratică are proprietăţi asemănătoare conjugării complexe şi acestea sunt puse în evidenţă de următoarea:

Propoziţie

Fie $d \in \mathbb{Z}$ un întreg care nu este pătrat perfect. Atunci, pentru orice z_1, z_2, $z \in \mathbb{Q}(\sqrt{d})$ avem:

1°. $(z_1 \pm z_2)^* = z_1^* \pm z_2^*$;

2°. $(z_1 z_2)^* = z_1^* z_2^*$;

3°. $\left(\dfrac{z_1}{z_2}\right)^* = \dfrac{z_1^*}{z_2^*}$, cu $z_2 \neq 0$;

4°. $z^* = z \Leftrightarrow z \in \mathbb{Q}$.

Considerăm că demonstraţia este foarte simplă, încât poate rămâne drept temă.
Suntem acum în măsură să enunţăm proprietatea de care vorbeam.

Teoremă

Dacă un polinom $f \in \mathbb{Q}[X]$ admite o rădăcină pătratică $x_0 \in \mathbb{Q}(\sqrt{d}) \setminus \mathbb{Q}$, atunci admite şi rădăcina conjugată pătratică x_0^*, cu acelaşi ordin de multiplicitate.

Demonstraţia este practic aceeaşi cu a teoremei precedente, doar că se înlocuieşte $\mathbb{R}$ cu $\mathbb{Q}$, conjugarea complexă cu conjugarea pătratică şi se folosesc proprietăţile conjugării pătratice, întrutotul analoage proprietăţilor conjugării complexe. De aceea, considerăm că şi această demonstraţie reprezintă o temă utilă.

În fine, prezentăm un rezultat care priveşte polinoamele cu coeficienţi întregi şi care reprezintă o condiţie necesară pentru ca un număr raţional (în particular, un număr întreg) să fie rădăcină a unui polinom din $\mathbb{Z}[X]$.

Teoremă (Newton)

Fie $f = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{Z}[X]$.

1°. Dacă $x_0 \in \mathbb{Q}$, cu $x_0 = \frac{p}{q}$, $p,q \in \mathbb{Z}$ şi $(p, q) = 1$, este o rădăcină a polinomului f, atunci p divide a_0 şi q divide a_n.

2°. Dacă $x_0 \in \mathbb{Z}$ este o rădăcină a polinomului f, atunci x_0 divide a_0.

Demonstraţie. 1°. Avem echivalenţele succesive:

$$f(x_0) = 0 \Leftrightarrow f\left(\frac{p}{q}\right) = 0 \Leftrightarrow a_n \cdot \left(\frac{p}{q}\right)^n + a_{n-1} \cdot \left(\frac{p}{q}\right)^{n-1} + \ldots + a_1 \cdot \frac{p}{q} + a_0 = 0 \Leftrightarrow$$

$$\Leftrightarrow a_n \cdot \frac{p^n}{q^n} + a_{n-1} \cdot \frac{p^{n-1}}{q^{n-1}} + \ldots + a_1 \cdot \frac{p}{q} + a_0 = 0 \Leftrightarrow$$

$$\Leftrightarrow a_np^n + a_{n-1}p^{n-1}q + \ldots + a_1pq^{n-1} + a_0q^n = 0. \qquad (1)$$

Scriem (1) sub forma:

$$p(a_np^{n-1} + a_{n-1}qp^{n-2} + \ldots + a_1q^{n-1}) = -a_0q^n$$

şi rezultă că $p \mid a_0q^n$. Cum $(p, q) = 1$, rezultă $p \mid a_0$.

Scriem acum (1) sub forma

$$q(a_{n-1}p^{n-1} + \ldots + a_1pq^{n-2} + a_0q^{n-1}) = -a_np^n$$

şi rezultă că $q \mid a_np^n$. Cum $(p, q) = 1$, deducem că $q \mid a_n$.

2°. Se obţine din 1° luând $q = 1$, $x_0 = p$.

În cuvinte acest rezultat se exprimă astfel:

1°. Rădăcinile raţionale ale unui polinom cu coeficienţi întregi sunt printre fracţiile ireductibile $\frac{p}{q}$, unde p divide termenul liber iar q divide coeficientul dominant.

2°. Rădăcinile întregi ale unui polinom cu coeficienţi întregi sunt printre divizorii termenului liber.

EXERCIŢII PROPUSE

1. Să se rezolve ecuaţia $x^4 + 4x^3 - 17x^2 + 26x - 14 = 0$ ştiind că admite rădăcina $x_1 = 1 + i$.

2. Să se determine parametrii $m,n \in \mathbb{R}$ şi să se rezolve ecuaţia

$$x^4 - 7x^3 + 19x^2 + mx + n = 0$$

ştiind că admite rădăcina $x_1 = 2 + i$.

3. Să se determine parametrii reali m, n şi să se rezolve ecuaţia
$$5x^5+2x^4+10x^3+4x^2+mx+n=0$$
ştiind că admite rădăcina dublă $x_1=x_2=i$.

4. Să se rezolve ecuaţia $x^4+x^3-19x^2-20x-20=0$ ştiind că admite rădăcina $x_1=2\sqrt{5}$.

5. Să se determine parametrii $m,n\in\mathbb{Q}$ şi să se rezolve ecuaţia

$x^4+mx^3+12x^2+nx-4=0$ ştiind că admite rădăcina $x_1=-2+\sqrt{6}$.

6. Să se rezolve ecuaţia $3x^5+x^4-6x^3-2x^2-9x-3=0$ ştiind că admite rădăcinile $x_1=\sqrt{3}$, $x_2=i$.

7. Să se afle rădăcinile întregi ale ecuaţiei $x^4-2x^3+x^2-4=0$ şi apoi să se rezolve ecuaţia.

8. Să se determine rădăcinile raţionale ale ecuaţiei $6x^6+17x^5-x^4+4x^3-10x^2-13x-3=0$ şi apoi să se rezolve ecuaţia.

9. Demonstraţi că un polinom de grad impar cu coeficienţi reali are cel puţin o rădăcină reală.

10. Demonstraţi că un polinom de grad par având coeficienţii numere întregi impare nu poate avea rădăcini raţionale.

11. Fie $p>0$ un număr prim. Demonstraţi că polinomul $f=X^3+pX^2+pX+p$ este ireductibil în inelul $\mathbb{Q}[X]$.

Descompunerea fracţiilor raţionale peste un corp comutativ în sume de fracţii simple (extindere)

O aplicaţie a teoremei împărţirii cu rest şi a teoremei de descompunere în factori ireductibili o constituie descompunerea fracţiilor raţionale peste un corp comutativ K în sume de fracţii simple.

Ca de obicei, K desemnează un corp comutativ, iar $K[X]$ inelul de polinoame asociat. Expresiile formale de tipul $\frac{f}{g}$ unde $f,\ g\in K[X]$, $g\neq 0$ se numesc ***fracţii raţionale*** peste K, iar mulţimea lor o notăm $K(X)$. Definim ***adunarea*** şi ***înmulţirea*** fracțiilor raționale prin $\frac{f}{g}+\frac{f_1}{g_1}=\frac{fg_1+f_1g}{gg_1}$, $\frac{f}{g}\cdot\frac{f_1}{g_1}=\frac{ff_1}{gg_1}$ și în felul acesta tripletul $(K(X), +, \cdot)$ devine un corp comutativ, numit ***corpul fracțiilor raționale peste K.***

Evident, $K[X]$ este un subinel al corpului $K(X)$.

Definiție

1) Fracțiile raționale de forma $\frac{u}{p^k} \in K(X)$ unde $p \in K[X]$ este un polinom ireductibil, iar $u \in K[X]$ este un polinom cu grad$(u) <$ grad(p), k fiind un număr natural nenul oarecare, se numesc ***fracții raționale simple.***

2) Fracțiile raționale $\frac{u}{v} \in K(X)$ cu $(u, v) = 1$ se numesc ***fracții ireductibile.***

Vom arăta că orice fracție rațională din corpul $K(X)$ se scrie în mod unic ca o sumă dintre un polinom și niște fracții raționale simple. Vom parcurge pentru aceasta câteva etape pregătitoare.

Lema 1

Fie $p \in K[X]$ un polinom nenul și $u \in K[X]$ un polinom oarecare. Atunci, pentru fiecare $n \in \mathbb{N}^*$ fixat, există și sunt unice polinoamele $u_0, u_1, \ldots, u_{n-1}, v \in K[X]$ cu grad$(u_i) <$ grad(p), $i=\overline{0, n-1}$, astfel încât:

$$u = u_0 + u_1 p + \ldots + u_{n-1}p^{n-1} + vp^n .$$

Demonstrație. Existența scrierii. Procedăm prin inducție după n. Pentru $n = 1$, deoarece în $K[X]$ este valabilă teorema împărțirii cu rest, putem scrie $u = u_0 + vp$ cu grad$(u_0) <$ grad(p).

Să presupunem că scrierea este valabilă pentru n, adică:

$$u = u_0 + u_1 p + \ldots + u_{n-1}p^{n-1} + vp^n \text{ cu grad}(u_i) < \text{grad}(p),\ i=\overline{0, n-1}.$$

Conform teoremei împărțirii cu rest, avem $v = u_n + wp$ cu grad$(u_n) <$ grad(p) și atunci scrierea anterioară devine:

$$u = u_0 + u_1 p + \ldots + u_{n-1}p^{n-1} + u_n p^n + wp^{n+1} \text{ cu grad}(u_i) < \text{grad}(p),\ i=\overline{0, n}.$$

Aceasta înseamnă că scrierea are loc și pentru $n + 1$ și demonstrația prin inducție se încheie.

Unicitatea scrierii. Să presupunem că pentru un număr $n \in \mathbb{N}^*$ avem două scrieri:

$$u = u_0 + u_1 p + \ldots + u_{n-1}p^{n-1} + vp^n = \overline{u}_0 + \overline{u}_1 p + \ldots + \overline{u}_{n-1}p^{n-1} + \overline{v}p^n$$

cu grad$(u_i) <$ grad(p), grad$(\overline{u}_i) <$ grad(p), $i=\overline{0, n-1}$.

Vom arăta că $u_i = \overline{u}_i$, $i=\overline{0, n-1}$ și $v = \overline{v}$. Din ipoteză rezultă:

$$(u_0 - \overline{u}_0) + (u_1 - \overline{u}_1)p + \ldots + (u_{n-1} - \overline{u}_{n-1})p^{n-1} + (v - \overline{v})p^n = 0 . \quad (1)$$

Din (1) rezultă că $u_0 - \overline{u}_0$ se divide cu p şi cum grad($u_0 - \overline{u}_0$) < grad(p), vom avea în mod necesar $u_0 - \overline{u}_0 = 0$, adică $u_0 = \overline{u}_0$. Reducând atunci termenii corespunzători în (1) şi, „împărţind" apoi în corpul $K(X)$ prin polinomul nenul p, obţinem:

$$(u_1 - \overline{u}_1) + (u_2 - \overline{u}_2)p + \ldots + (u_{n-1} - \overline{u}_{n-1})p^{n-1} + (v - \overline{v})p^{n-1} = 0. \qquad (2)$$

Din (2) rezultă ca şi mai înainte că $u_1 = \overline{u}_1$. Continuând raţionamentul obţinem $u_2 = \overline{u}_2, \ldots, u_{n-1} = \overline{u}_{n-1}$ şi în final $v = \overline{v}$.

Lema 2

Dacă $\dfrac{u}{v_1 v_2 \ldots v_n} \in K[X]$ este o fracţie ireductibilă, unde $n \geq 2$ şi $(v_i, v_j) = 1$ pentru $i \neq j$, există $h_1, h_2, \ldots, h_n \in K[X]$ cu $(h_i, v_i) = 1$, $i = \overline{1, n}$, astfel încât să avem scrierea (nu neapărat unică):

$$\frac{u}{v_1 v_2 \ldots v_n} = \frac{h_1}{v_1} + \frac{h_2}{v_2} + \ldots + \frac{h_n}{v_n}.$$

Demonstraţie. Procedăm prin inducţie după n. Pentru $n = 2$, întrucât $(v_1, v_2) = 1$, există $\ell_1, \ell_2 \in K[X]$ astfel încât $\ell_2 v_1 + \ell_1 v_2 = 1$ (1). Înmulţim cu fracţia $\dfrac{u}{v_1 v_2}$ şi obţinem $\dfrac{u\ell_2}{v_2} + \dfrac{u\ell_1}{v_1} = \dfrac{u}{v_1 v_2}$, adică $\dfrac{u}{v_1 v_2} = \dfrac{h_1}{v_1} + \dfrac{h_2}{v_2}$ unde $h_1 = u\ell_1$, $h_2 = u\ell_2$. Fracţia iniţială $\dfrac{u}{v_1 v_2}$ fiind ireductibilă avem $(u, v_1) = (u, v_2) = 1$.

De asemenea, din (1) se vede că $(v_1, \ell_1) = (v_2, \ell_2) = 1$. Deoarece $(v_1, u) = 1$ şi $(v_1, \ell_1) = 1$ rezultă $(v_1, u\ell_1) = 1$, adică $(v_1, h_1) = 1$; analog obţinem $(v_2, h_2) = 1$ şi astfel cazul $n = 2$ este complet tratat. Să presupunem proprietatea adevărată pentru n şi să o demonstrăm pentru $n + 1$. Considerând fracţia $\dfrac{u}{v_1 v_2 \ldots v_n v_{n+1}}$ cu $(v_i, v_j) = 1$ pentru $i \neq j$, vom avea $(v_1 v_2 \ldots v_n, v_{n+1}) = 1$ şi atunci conform cazului $n = 2$ putem scrie:

$$\frac{u}{v_1 v_2 \ldots v_n v_{n+1}} = \frac{h}{v_1 v_2 \ldots v_n} + \frac{h_{n+1}}{v_{n+1}}$$

unde $h, h_{n+1} \in K[X]$ şi $(h, v_1 v_2 \ldots v_n) = 1$, $(h_{n+1}, v_{n+1}) = 1$.

Dar proprietatea fiind valabilă pentru n, avem $\dfrac{h}{v_1 v_2 \ldots v_n} = \dfrac{h_1}{v_1} + \dfrac{h_2}{v_2} + \ldots + \dfrac{h_n}{v_n}$ cu $(h_i, v_i) = 1$ pentru $i = \overline{1, n}$. Atunci, vom avea:

$$\frac{h}{v_1 v_2 \ldots v_n v_{n+1}} = \frac{h_1}{v_1} + \frac{h_2}{v_2} + \ldots + \frac{h_n}{v_n} + \frac{h_{n+1}}{v_{n+1}}$$

cu $(h_i, v_i) = 1$ pentru $i = \overline{1, n+1}$ şi astfel scrierea are loc şi pentru $n + 1$.

Lema 3

Fie $\frac{u}{v} \in K[X]$ o fracţie raţională (respectiv o fracţie raţională ireductibilă) şi fie $v = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ descompunerea lui v în factori ireductibili în inelul $K[X]$. Atunci are loc o descompunere în sumă de fracţii raţionale (respectiv în sumă de fracţii raţionale ireductibile) de tipul:

$$\frac{u}{v} = \frac{h_1}{p_1^{k_1}} + \frac{h_2}{p_2^{k_2}} + \dots + \frac{h_n}{p_n^{k_n}}.$$

În plus dacă mai avem şi scrierea:

$$\frac{u}{v} = \frac{\ell_1}{p_1^{k_1}} + \frac{\ell_2}{p_2^{k_2}} + \dots + \frac{\ell_n}{p_n^{k_n}}$$

atunci $(h_i - \ell_i) \vdots p_i^{k_i}$, $i = \overline{1, n}$.

Demonstraţie. Notăm $v_i = p_i^{k_i}$, $i = \overline{1, n}$ şi suntem în condiţiile lemei 2, care asigură existenţa scrierii. Pentru partea de „unicitate", să presupunem că avem două scrieri:

$$\frac{u}{v} = \frac{h_1}{p_1^{k_1}} + \frac{h_2}{p_2^{k_2}} + \dots + \frac{h_n}{p_n^{k_n}} = \frac{\ell_1}{p_1^{k_1}} + \frac{\ell_2}{p_2^{k_2}} + \dots + \frac{\ell_n}{p_n^{k_n}}.$$

Scriem această egalitate sub forma $\frac{h_1 - \ell_1}{p_1^{k_1}} = \sum_{i=2}^{n} \frac{\ell_i - h_i}{p_i^{k_i}}$ şi o înmulţim cu $p_2^{k_2} \cdot p_3^{k_3} \cdot \dots \cdot p_n^{k_n}$. Se obţine $\frac{p_2^{k_2} \cdot p_3^{k_3} \cdot \dots \cdot p_n^{k_n} (h_1 - \ell_1)}{p_1^{k_1}} = w \in K[X]$ ceea ce înseamnă că polinomul $p_1^{k_1}$ divide polinomul $p_2^{k_2} \cdot p_3^{k_3} \cdot \dots \cdot p_n^{k_n} (h_1 - \ell_1)$.

Deoarece $(p_1^{k_1}, p_2^{k_2} p_3^{k_3} \dots p_n^{k_n}) = 1$, rezultă că $(h_1 - \ell_1) \vdots p_i^{k_i}$.

Analog se arată că $(h_i - \ell_i) \vdots p_i^{k_i}$, $i = \overline{2, n}$.

Observaţie

Lema 3 rămâne valabilă şi pentru $k_1 = k_2 = \dots = k_n = 0$, adică atunci când fracţia raţională considerată este chiar un polinom.

Lema 4

Fie $p \in K[X]$ un polinom ireductibil, $u \in K[X]$ şi $n \in \mathbb{N}^*$. Atunci fracţia $\frac{u}{p^n}$ se descompune în mod unic într-o sumă de fracţii simple şi un polinom, adică:

$$\frac{u}{p^n} = u_0 + \frac{u_1}{p} + \frac{u_2}{p^2} + \dots + \frac{u_n}{p^n}$$

cu $u_0, u_1, \dots, u_n \in K[X]$, iar $\text{grad}(u_i) < \text{grad}(p)$, $i = \overline{1, n}$.

Demonstrație. Conform lemei 1 avem o scriere unică de tipul:

$$u = u_n + u_{n-1}p + u_{n-2}p^2 + \ldots + u_1 p^{n-1} + u_0 p^n$$

unde $u_0, u_1, \ldots, u_n \in K[X]$ și grad(u_i) < grad(p), $i = \overline{1, n}$.

Împărțind în corpul $K(X)$ prin p^n se obține:

$$\frac{u}{p^n} = u_0 + \frac{u_1}{p} + \frac{u_2}{p^2} + \ldots + \frac{u_n}{p^n},$$

adică scrierea din enunț.

Dacă mai avem o altă scriere $\frac{u}{p^n} = v_0 + \frac{v_1}{p} + \frac{v_2}{p^2} + \ldots + \frac{v_n}{p^n}$ cu $v_0, v_1, \ldots, v_n \in K[X]$ și grad(v_i) < grad(p), $i = \overline{1, n}$, atunci:

$$u = u_n + u_{n-1}p + u_{n-2}p^2 + \ldots + u_1 p^{n-1} + u_0 p^n = v_n + v_{n-1}p + v_{n-2}p^2 + \ldots + v_1 p^{n-1} + v_0 p^n$$

și folosind unicitatea scrierii dată de lema 1 rezultă $u_i = v_i$, $i = \overline{1, n}$.

În fine, putem da rezultatul important.

Teoremă (de descompunere în fracții simple)

Fie $\frac{u}{v} \in K[X]$ o fracție rațională. Presupunem că în inelul $K[X]$ polinomul v are următoarea descompunere în factori ireductibili.

$$v = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}.$$

Atunci fracția $\frac{u}{v}$ se scrie în mod unic drept sumă dintre un polinom și niște fracții simple, în felul următor:

$$\frac{u}{v} = u_0 + \sum_{i=1}^{n} \sum_{j=1}^{k_i} \frac{u_{ij}}{p_i^j}$$

unde u_0, $u_{ij} \in K[X]$, grad(u_{ij}) < grad(p_i), $j = \overline{1, k_i}$, $i = \overline{1, n}$.

Demonstrație. *Existența scrierii*. Conform lemei 3 putem scrie:

$$\frac{u}{v} = \sum_{i=1}^{n} \frac{h_i}{p_i^{k_i}}.$$

Aplicând apoi lema 4 pentru fiecare $i = 1, 2, \ldots, n$ putem scrie:

$$\frac{h_i}{p_i^{k_i}} = \ell_i + \sum_{j=1}^{k_i} \frac{u_{ij}}{p_i^j}$$

cu ℓ_i, $u_{ij} \in K[X]$ și grad(u_{ij}) < grad(p_i), $j = \overline{1, k_i}$.

Notând $\sum_{i=1}^{n} \ell_i = u_0$, din cele două egalități precedente rezultă:

$$\frac{u}{v} = u_0 + \sum_{i=1}^{n} \sum_{j=1}^{k_i} \frac{u_{ij}}{p_i^j}.$$

Unicitatea scrierii. Dacă mai avem şi scrierea:

$$\frac{u}{v}=\bar{u}_0+\sum_{i=1}^{n}\sum_{j=1}^{k_i}\frac{\bar{u}_{ij}}{p_i^j}$$

cu $\bar{u}_0,\bar{u}_{ij}\in K[X]$ şi grad($\bar{u}_{ij}$) < grad(p_i), $j=\overline{1,k_i}$, $i=\overline{1,n}$, atunci putem scrie:

$$(u_0-\bar{u}_0)+\sum_{i=1}^{n}\sum_{j=1}^{k_i}\frac{u_{ij}-\bar{u}_{ij}}{p_i^j}=0. \tag{1}$$

Să scriem (1) în forma următoare, în care fixăm i = 1 şi explicităm suma corespunzătoare după j, adică:

$$(u_0-\bar{u}_0)+\frac{u_{11}-\bar{u}_{11}}{p_1}+\frac{u_{12}-\bar{u}_{12}}{p_1^2}+\ldots+\frac{u_{1k_1}-\bar{u}_{1k_1}}{p_1^{k_1}}+\sum_{i=2}^{n}\sum_{j=1}^{k_i}\frac{u_{ij}-\bar{u}_{ij}}{p_i^j}=0. \tag{2}$$

Înmulţind (2) cu $p_1^{k_1-1}p_2^{k_2}\ldots p_n^{k_n}$ rezultă o egalitate de forma:

$$p_2^{k_2}\ldots p_n^{k}\cdot\frac{u_{1k_1}-\bar{u}_{1k_1}}{p_1}+w=0$$

cu $w\in K[X]$, ceea ce înseamnă că $p_1 \mid (u_{1k_1}-\bar{u}_{1k_1})$.

Deoarece grad $(u_{1k_1}-\bar{u}_{1k_1})$ < grad(p_1), rezultă în mod necesar $u_{1k_1}-\bar{u}_{1k_1}=0$, adică $u_{1k_1}=\bar{u}_{1k_1}$. Reducând termenii corespunzători în (1) şi înmulţind apoi cu $p_1^{k_1-2}p_2^{k_2}\ldots p_n^{k_n}$ vom obţine în mod asemănător $u_{1k_1-1}=\bar{u}_{1k_1-1}$ şi aşa mai departe, până ce vom obţine $u_{11}=\bar{u}_{11}$. Fixând apoi în (1) i = 2 vom găsi analog $u_{2k_2}=\bar{u}_{2k_2}$, ..., $u_{21}=\bar{u}_{21}$. Continuând raţionamentul pentru i = 3, 4, ..., n obţinem respectiv $u_{3k_3}=\bar{u}_{3k_3}$, ..., $u_{31}=\bar{u}_{31}$, ..., $u_{nk_n}=\bar{u}_{nk_n}$, ..., $u_{n1}=\bar{u}_{n1}$.

După toate acestea, egalitatea (1) devine $u_0-\bar{u}_0=0$, adică $u_0=\bar{u}_0$. Teorema este demonstrată.

Dat fiind că în inelele $\mathbb{C}[X]$ şi $\mathbb{R}[X]$ cunoaştem exact polinoamele ireductibile, rezultă că teorema de descompunere în fracţii simple se transcrie în corpurile de fracţii raţionale $\mathbb{C}(X)$ şi $\mathbb{R}(X)$ sub forma următoarelor două teoreme:

Teoremă

Dacă $\frac{u}{v}\in\mathbb{C}(X)$, unde $v=\prod_{i=1}^{n}(a_iX+b_j)^{k_i}$, atunci avem scrierea unică:

$$\frac{u}{v}=u_0+\sum_{i=1}^{n}\sum_{j=1}^{k_i}\frac{A_{ij}}{(a_iX+b_i)^j}$$

unde $u_0\in\mathbb{C}[X]$, $A_{ij}\in\mathbb{C}$, $j=\overline{1,k_i}$, $i=\overline{1,n}$.

Teoremă

Dacă $\frac{u}{v} \in \mathbb{R}(X)$, iar v are în inelul $\mathbb{R}[X]$ următoarea descompunere în factori ireductibili:

$$v = \prod_{i=1}^{n} (a_i X + b_j)^{k_i} \cdot \prod_{i=1}^{m} \left(\alpha_i X^2 + \beta_i X + \gamma_i\right)^{\ell_i}$$

unde $\beta_i^2 - 4\alpha_i\gamma_i < 0$, $i = \overline{1, m}$, atunci avem scrierea unică:

$$\frac{u}{v} = u_0 + \sum_{i=1}^{n}\sum_{j=1}^{k_i} \frac{A_{ij}}{(a_i X + b_i)^j} + \sum_{i=1}^{m}\sum_{j=1}^{\ell_i} \frac{B_{ij}X + C_{ij}}{(\alpha_i X^2 + \beta_i X + \gamma_i)^j}$$

unde $u_0 \in \mathbb{R}[X]$, $A_{ij} \in \mathbb{R}$, $j = \overline{1, k_i}$, $i = \overline{1, n}$ şi $B_{ij}, C_{ij} \in \mathbb{R}$, $j = \overline{1, \ell_i}$, $i = \overline{1, m}$.

Comentariu metodic

De obicei, pentru determinarea efectivă a unei descompuneri în fracţii simple se procedează astfel: polinomul care apare în membrul drept este tocmai câtul împărţirii numărătorului la numitor, după care rămâne de efectuat descompunerea unei fracţii raţionale în care numărătorul (restul împărţirii anterioare) are gradul mai mic decât numitorul.

Această ultimă descompunere se face determinând coeficienţii polinoamelor de la numărătorii din membrul drept, fapt ce se realizează eliminând numitorii şi identificând coeficienţii în egalitatea polinomială obţinută (metoda coeficienţilor nedeterminaţi), ajungându-se la rezolvarea unui sistem liniar.

Să mai remarcăm că, întrucât scrierea unui polinom ca produs de factori ireductibili este relativă la inelul de polinoame în care gândim polinomul, tot astfel, descompunerea unei fracţii raţionale în sumă de fracţii raţionale simple este relativă la corpul de fracţii în care gândim fracţia raţională respectivă. Aşa de exemplu, fracţia raţională $\frac{1}{X^4 - 1}$ se scrie în corpul $\mathbb{R}(X)$ sub forma $\frac{1}{X^4-1} = \frac{A}{X-1} + \frac{B}{X+1} + \frac{CX+D}{X^2+1}$ cu $A, B, C, D \in \mathbb{R}$, iar în corpul $\mathbb{C}(X)$ sub forma $\frac{1}{X^4-1} = \frac{A}{X-1} + \frac{B}{X+1} + \frac{C}{X-i} + \frac{D}{X+i}$, cu $A, B, C, D \in \mathbb{C}$.

Determinarea coeficienţilor A, B, C, D în fiecare din cele două cazuri este o problemă simplă ce duce la un sistem liniar în A, B, C, D şi nu mai insistăm.

Exerciţiu rezolvat

Fie K un corp comutativ, $v \in K[X]$ un polinom de grad n având în corpul K rădăcinile simple $x_1, x_2, \ldots, x_n$ iar $u \in K[X]$ un polinom de grad mai mic decât n. Să se arate că fracţia raţională $\frac{u}{v} \in K[X]$ are următoarea descompunere în fracţii simple:

$$\frac{u}{v}=\sum_{i=1}^{n}\frac{u(x_i)}{v'(x_i)(X-x_i)}$$

unde v' este derivata polinomului v. Cazuri particulare: $u = 1$, $u = v'$.

(Egalitatea de mai sus se numeşte *identitatea lui Euler*).

Soluţie. Deoarece v are toate cele n rădăcini în K, el se va descompune în inelul $K[X]$ în factori ireductibili liniari, adică: $v=a(X-x_1)(X-x_2)\ldots(X-x_n)$, cu $a \in K^*$.

Ţinând seama că regulile de derivare (formală) coincid cu cele ce se demonstrează în analiza matematică, rezultă:

$$v'=a(X-x_2)(X-x_3)\ldots(X-x_n)+a(X-x_1)(X-x_3)\ldots(X-x_n)+\ldots+$$
$$+\,a(X-x_1)(X-x_2)\ldots(X-x_{n-1}) \text{ şi de aici}$$
$$v'(x_i)=a(x_i-x_1)(x_i-x_2)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_n),\quad i=\overline{1,n}.$$

Deoarece $a \neq 0$ şi $x_i \neq x_j$ pentru $i \neq j$ (rădăcinile fiind simple), rezultă

$$v'(x_i) \neq 0,\quad i=\overline{1,n}.$$

Considerăm polinomul $w \in K[X]$, $w=u-v\cdot\sum_{j=1}^{n}\frac{u(x_j)}{v'(x_j)(X-x_j)}$; deoarece grad($u$) < n, iar $\text{grad}\left(v\cdot\sum_{j=1}^{n}\frac{u(x_j)}{v'(x_j)(X-x_j)}\right)\leq n-1$, rezultă grad $w \leq n - 1$. Ţinând seama de descompunerea lui v în factori liniari, rezultă că polinomul w are forma:

$$w=u-a\cdot\sum_{j=1}^{n}\frac{u(x_j)(X-x_1)(X-x_2)\ldots(X-x_{j-1})(X-x_{j+1})\ldots(X-x_n)}{v'(x_j)}$$

şi dacă ţinem seama şi de valoarea $v'(x_i)$ obţinută mai sus, rezultă:

$$w(x_i)=u(x_i)-u(x_i)\cdot\frac{v'(x_i)}{v'(x_i)}=0,\quad i=\overline{1,n}.$$

Aşadar, polinomul $w \in K(X)$, de grad cel mult $n - 1$, are în corpul K rădăcinile distincte $x_1, x_2, \ldots, x_n$ şi atunci conform lemei de la pag. 87 rezultă că $w = 0$. Aşadar

$$u-v\cdot\sum_{j=1}^{n}\frac{u(x_j)}{v'(x_j)(X-x_j)}=0$$

şi împărţind în corpul $K(X)$ prin $v \neq 0$ se obţine:

$$\frac{u}{v}=\sum_{j=1}^{n}\frac{u(x_j)}{v'(x_j)(X-x_j)},$$ adică identitatea din enunţ.

În cazul particular $u = 1$, identitatea lui Euler devine:

$$\frac{1}{v}=\sum_{i=1}^{n}\frac{1}{v'(x_i)(X-x_i)}$$

iar în cazul particular $u = v'$, identitatea lui Euler devine:

$$\frac{v'}{v}=\sum_{i=1}^{n}\frac{1}{X-x_i}.$$

TESTE DE EVALUARE

Testul 1

(timp de lucru - 30 minute; fiecare exercițiu se notează cu 3 puncte)

Indicați răspunsul corect.

1. Cât este restul împărțirii polinomului $X^{2007}+X^2+X+2$ la $X^4+X^3+X^2+X+1$?
a) X^2-X+2; b) $2X^2+X+1$; c) $2X^2+X+2$; d) $2X^2+X+3$.

2. Câte rădăcini raționale are polinomul $f=X^{100}+3X^{81}+X^2+X+1$?
a) 0; b) 1; c) 2; d) 100.

3. Polinomul $f=X^4+4X^3+6X^2+aX+b$, are toate rădăcinile x_1, x_2, x_3, x_4 reale. Cât este $x_1^{100}+x_2^{100}+x_3^{100}+x_4^{100}$?
a) 0; b) 1; c) 100; d) 4.

Testul 2

(timp de lucru - 50 minute; fiecare exercițiu se notează cu 3 puncte)

Pentru următoarele probleme se cer soluții complete.

1. Să se determine $n \in \mathbb{N}$, $3 \le n \le 10$ astfel încât polinomul $f=X^n+X^2+X+1$ să se dividă cu polinomul $g=(X+1)(X^2+1)$.

2. Fie $f=X^4+aX^3+aX^2+bX+c \in \mathbb{R}[X]$ și x_1, x_2, x_3, $x_4 \in \mathbb{C}$ rădăcinile lui.
a) Să se calculeze $x_1^2+x_2^2+x_3^2+x_4^2$.
b) Să se arate că dacă $a \in (0, 2)$ atunci f nu are toate rădăcinile reale.
c) Rămâne concluzia de la punctul b) adevărată dacă $a \in \left[2, \frac{8}{3}\right)$?

3. Fie $f \in \mathbb{R}[X]$ cu $f(1)=0$ și $f(2)=1$. Să se determine f știind că gradul lui f este 5 și $f(x^3)=\left(f(x)\right)^3$, $\forall x \in \mathbb{Z}$.

PROBLEME RECAPITULATIVE

1. Fie $(G, \cdot)$ un grup şi H o submulţime nevidă a lui G, $H \neq G$, astfel încât $\forall\ x \in H$, $\forall\ y \in G \setminus H \Rightarrow xy \in G \setminus H$. Să se demonstreze că H este un subgrup al grupului G. Comparaţi rezultatul cu cel din comentariul metodic de la pag. 31.

2. Fie $(G, \cdot)$ un grup abelian finit de ordin n. Arătaţi că:

a) Pentru fiecare $k \in \mathbb{Z}$ cu $(k, n) = 1$, funcţia $f_k : G \to G$, $f_k(x) = x^k$ este un automorfism al lui G.

b) Mulţimea $\Gamma = \{f_k \mid k \in \mathbb{Z},\ (k, n) = 1\}$ este un grup abelian finit, faţă de compunerea funcţiilor. Care este ordinul lui Γ în cazurile $G = \mathbb{K}$ (grupul lui Klein) respectiv $G = U_n$?

3. Demonstraţi că grupul $(G_n, \cdot)$ de matrice care apare în ex. 30 pag. 27 este izomorf cu grupul simetric $(S_n, \cdot)$.

4. Fie $(G, \cdot)$ un grup. Arătaţi că mulţimea $\mathrm{Aut}(G)$ a automorfismelor lui G este un grup, relativ la compunerea funcţiilor (numit *grupul automorfismelor lui G*).

5. Fie $(G, \cdot)$ un grup. Pentru fiecare $a \in G$ definim funcţia $i_a : G \to G$, $i_a(x) = axa^{-1}$. Arătaţi că:

a) Funcţia i_a este un automorfism al grupului G (numit *automorfismul interior determinat de a*).

b) Mulţimea $I(G) = \{i_a \mid a \in G\}$ este un grup, relativ la compunerea funcţiilor (numit *grupul automorfismelor interioare*).

c) G este abelian dacă şi numai dacă $I(G) = \{i_e\}$.

6. Demonstraţi că pentru orice $n, m \in \mathbb{N}^*$ avem proprietăţile:

a) $U_n \subseteq U_m \Leftrightarrow n \mid m$. b) $U_n \cap U_m = U_{(n,\, m)}$. c) $U_nU_m = U_{[n,\, m]}$.

(Reamintim că $U_n = \{x \in \mathbb{C} \mid x^n = 1\}$; $U_nU_m = \{xy \mid x \in U_n,\ y \in U_m\}$; (n, m) respectiv $[n, m]$ desemnează c.m.m.d.c., respectiv c.m.m.m.c. al numerelor n şi m).

7. Dacă $(G_1, \cdot)$, $(G_2, \cdot)$ sunt două grupuri, definim pe mulţimea produs cartezian $G_1 \times G_2$ operaţia $(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2)$. Arătaţi că $(G_1 \times G_2, \cdot)$ este un grup (numit *produsul direct* al grupurilor G_1 şi G_2, în această ordine).

8. Arătaţi că pentru $n, m \in \mathbb{N}^*$, $(n, m) = 1$, avem izomorfismul de grupuri:

$$\mathbb{Z}_n \times \mathbb{Z}_m \approx \mathbb{Z}_{nm}.$$

9. Arătaţi că avem izomorfismul de grupuri: $\mathbb{Z}_2 \times \mathbb{Z}_2 \approx \mathbb{K}$.

10. a) Considerăm grupul $(\mathbb{R}, +)$ şi bijecţiile $f, g : \mathbb{R} \to \mathbb{R}$, $f(x) = x - a$ ($a \in \mathbb{R}$ fixat), $g(x) = \sqrt[3]{x}$. Să se definească structurile de grup $(\mathbb{R}, *)$ şi $(\mathbb{R}, \circ)$ care sunt transportatele structurii $(\mathbb{R}, +)$ prin bijecţiile f respectiv g.

b) Arătaţi că structura de grup din exerciţiul 15 pag. 25 provine din structura de grup din exerciţiul rezolvat 1, pag. 21, prin transportul dat de o bijecţie.

11. Fie $(A, +, \cdot)$ un inel şi $a,b \in A$ două elemente care „comută" adică $ab = ba$. Demonstraţi următoarele „formule de calcul":

a) $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-1} + b^{n-1})$, $\forall n \in \mathbb{N}$, $n \geq 2$.

b) $a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \ldots - ab^{n-1} + b^{n-1})$, $\forall n \in \mathbb{N}$, $n \geq 3$, n impar.

c) $(a+b)^n = a^n + C_n^1 a^{n-1}b + C_n^2 a^{n-1}b^2 + \ldots + C_n^{n-1} ab^{n-1} + b^n$, $\forall n \in \mathbb{N}^*$,
(formula binomului lui Newton).

12. Fie A un inel cu proprietatea că $x^2 = x$ pentru orice $x \in A$ (un astfel de inel se numeşte *inel boolean*). Arătaţi că:
a) $1 + 1 = 0$.
b) A este un inel comutativ.

13. Fie A un inel cu $0 \neq 1$ şi cu proprietatea că $x^2 = 0$ sau $x^2 = 1$ pentru orice $x \in A$. Arătaţi că:

a) Grupul elementelor inversabile este $U(A) = \{x \in A \mid x^2 = 1\}$;
b) $x \notin U(A) \Rightarrow 1 + x \in U(A)$;
c) A este inel comutativ.

14. Fie A un inel cu $0 \neq 1$ în care grupul $U(A)$ al elementelor inversabile are ordin impar. Arătaţi că inelul A are caracteristica 2.

15. Fie A un inel cu proprietatea că $x^3 = x$, pentru orice $x \in A$. Arătaţi că inelul A este comutativ.

16. Fie A un inel, cu $0 \neq 1$, care nu are divizori ai lui zero. Arătaţi că grupurile $(A, +)$ şi $(U(A), \cdot)$ nu sunt izomorfe.

17. Fie A un inel, cu $0 \neq 1$, având $2^n - 1$ elemente inversabile şi cel mult tot atâtea elemente neinversabile. Arătaţi că inelul A este un corp cu 2^n elemente.

18. Dacă A este un inel, considerăm mulţimea $Z(A) = \{x \in A \mid xy = yx,\ \forall y \in A\}$ pe care o numim *centrul lui A*. Arătaţi că:
a) $Z(A)$ este un subinel comutativ al lui A;
b) A este un inel comutativ dacă şi numai dacă $Z(A) = A$;
c) A este inel comutativ dacă şi numai dacă $x^2 - x \in Z(A)$, pentru orice $x \in A$.

19. Fie A un inel comutativ şi $a_1, a_2, \ldots, a_n \in A$ $(n \geq 2)$ elemente ale inelului, nu neapărat distincte. Considerăm sumele: $\sigma_1 = \sum a_1 \left(= \sum_{i=1}^{n} a_i\right)$; $\sigma_2 = \sum a_1 a_2 \left(= \sum_{1 \leq i < j \leq n} a_i a_j\right)$;

$\sigma_3 = \sum a_1 a_2 a_3 \left(= \sum_{1 \leq i < j < k \leq n} a_i a_j a_k\right)$; ...; $\sigma_n = a_1 a_2 \ldots a_n$; $s_p = \sum a_1^p \left(= \sum_{i=1}^{n} a_i^p\right)$,

pentru fiecare $p \in \mathbb{N}^*$. Arătaţi că au loc formulele (numite *formulele lui Newton*):

a) $s_p - s_{p-1}\sigma_1 + s_{p-2}\sigma_2 - \ldots + (-1)^{p-1} s_1\sigma_{p-1} + (-1)^p p\sigma_p = 0$, pentru $1 \le p \le n$;

b) $s_p - s_{p-1}\sigma_1 + s_{p-2}\sigma_2 - \ldots + (-1)^n s_{p-n}\sigma_n = 0$, pentru $p \ge n + 1$.

20. Fie A un inel cu $0 \ne 1$, având proprietatea că $x^2 = 1$, pentru orice $x \in A \setminus \{0\}$. Arătați că A este izomorf cu unul din corpurile $\mathbb{Z}_2$ sau $\mathbb{Z}_3$.

21. Fie A un inel cu $0 \ne 1$, având proprietatea că $x^4 = 1$, pentru orice $x \in A \setminus \{0\}$. Arătați că A este izomorf cu unul din corpurile $\mathbb{Z}_2$ sau $\mathbb{Z}_3$ sau $\mathbb{Z}_5$.

22. Fie A un inel cu $0 \ne 1$, având exact 2 elemente neinversabile. Arătați că:

a) Inelul A are 4 elemente.

b) Abstracție făcând de un izomorfism de inele, există doar două inele cu proprietatea din enunț.

23. Fie $\alpha \in \mathbb{C} \setminus \mathbb{Q}$ cu proprietatea că mulțimea $A = \{a + b\alpha \mid a,b \in \mathbb{Z}\}$ este inel față de operațiile uzuale din $\mathbb{C}$ (adică A este un subinel al corpului $\mathbb{C}$). Ştiind că inelul A are exact 4 elemente inversabile, să se arate că $A = \mathbb{Z}[i]$.

24. Dați exemplu de un inel cu divizori ai lui zero A şi un polinom $f \in A[X]$ de grad $n \ge 1$, cu proprietatea că f are în A mai mult de n rădăcini.

25. Fie K un corp finit. Arătați că orice funcție $f : K \to K$ este polinomială, adică există un polinom $P \in K[X]$ astfel încât $f = \widetilde{P}$.

26. Fie $f = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{Z}[X]$ un polinom cu proprietatea că există un număr prim p astfel încât $p \mid a_k$, $k = \overline{0, n-1}$, p nu divide a_n, iar p^2 nu divide a_0. Arătați că polinomul f este ireductibil în inelul $\mathbb{Q}[X]$. (*Criteriul de ireductibilitate al lui Eisenstein*).

27. Pentru $p > 0$ număr prim, considerăm polinomul $\Phi_p = X^{p-1} + X^{p-2} + \ldots + X + 1$ (numit *al p-lea polinom ciclotomic*). Arătați că:

a) Polinomul $f(X) = \Phi_p(X + 1)$ este ireductibil în $\mathbb{Q}[X]$.

b) Polinomul Φ_p este ireductibil în $\mathbb{Q}[X]$.

28. Fie K un corp finit astfel încât polinomul $X^2 - 5$ este ireductibil în inelul $K[X]$. Demonstrați că orice polinom de forma $X^5 + a$, unde $a \in K$, este reductibil în inelul $K[X]$.

29. Fie K un corp cu 2^n elemente, $n \in \mathbb{N}^*$. Demonstrați că polinomul $X^4 + X + 1$ este ireductibil în inelul $K[X]$ dacă şi numai dacă n este impar.

30. Fie $f \in \mathbb{C}[X]$ un polinom de grad $n \ge 2$ având rădăcinile simple $x_1, x_2, \ldots, x_n \in \mathbb{C}$.

Arătați că $\displaystyle\sum_{i=1}^{n} \frac{1}{f'(x_i)} = 0$.

31. Fie polinomul $f \in \mathbb{C}[X]$ definit prin $f = X^{n-1} + X^{n-2} + \ldots + X + 1$, unde $n \in \mathbb{N}$, $n \geq 2$.

a) Descompuneți polinomul f în factori liniari în $\mathbb{C}[X]$;

b) Deduceți identitatea: $\sin\frac{\pi}{n} \cdot \sin\frac{2\pi}{n} \cdot \ldots \cdot \sin\frac{(n-1)\pi}{n} = \frac{n}{2^{n-1}}$.

32. Fie $f \in \mathbb{C}[X]$. Demonstrați că următoarele afirmații sunt echivalente:

1°. $f(x) = f(-x)$, $\forall\, x \in \mathbb{C}$.

2°. $\exists\, g \in \mathbb{C}[X]$ astfel încât $f(x) = g(x)g(-x)$, $\forall\, x \in \mathbb{C}$.

33. Fie $P, Q \in \mathbb{C}[X]$ polinoame nenule. Demonstrați că următoarele afirmații sunt echivalente:

1°. $\exists\, \lambda \in \mathbb{C}^*$ astfel încât $P = \lambda Q$ (adică P, Q sunt asociate).

2°. Funcția $f : \mathbb{C} \to \mathbb{R}$, $f(x) = |P(x)| - |Q(x)|$ nu își schimbă semnul.

34. Fie $f = a_0 + a_1 X + \ldots + a_n X^n \in \mathbb{R}[X]$ un polinom cu proprietatea că toate rădăcinile sale au modulul 1. Să se arate că:

$$a_i = (-1)^{\alpha_0} a_{n-1},\ i = 0, 1, 2, \ldots, n$$

unde $\alpha_0 \in \mathbb{N}$ este ordinul de multiplicitate ale rădăcinii $x_0 = 1$.

35. Fie $f = a_0 + a_1 X + \ldots + a_n X^n \in \mathbb{R}[X]$ un polinom cu proprietatea că toate rădăcinile sale au modulul $r > 0$. Să se arate că:

$$a_i = (-1)^{\alpha_0} r^{n-2i} a_{n-i},\ i = 0, 1, 2, \ldots, n$$

unde $\alpha_0 \in \mathbb{N}$ este ordinul de multiplicitate ale rădăcinii $x_0 = r$.

36. Fie inelele $(A_1, +, \cdot)$ și $(A_2, +, \cdot)$. Pe mulțimea produs-cartezian $A_1 \times A_2$ definim operațiile $(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$ și $(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_2)$. Arătați că:

a) $(A_1 \times A_2, +, \cdot)$ este un inel (numit *produsul direct* al inelelor A_1 și A_2 în această ordine).

b) Grupul elementelor inversabile din inelul $A_1 \times A_2$ este dat de egalitatea

$$U(A_1 \times A_2) = U(A_1) \times U(A_2).$$

37. Dacă $n, m \in \mathbb{N}$, $n \geq 2$, $m \geq 2$, $(n, m) = 1$, arătați că avem izomorfismul de inele:

$\mathbb{Z}_n \times \mathbb{Z}_m \approx \mathbb{Z}_{nm}$ și izomorfismul de grupuri multiplicative $U(\mathbb{Z}_n) \times U(\mathbb{Z}_m) \approx U(\mathbb{Z}_{nm})$.

38. Reamintim că dacă $n \in \mathbb{N}^*$ notăm cu $\varphi(n)$ indicatorul lui Euler, adică numărul numerelor naturale k, cu proprietatea $1 \leq k \leq n$ și $(k, n) = 1$. Să se arate că:

a) Dacă p este număr prim și $\alpha \in \mathbb{N}^*$ atunci $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$;

b) Dacă $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ cu $p_1 < p_2 < \ldots < p_k$ numere prime, iar $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{N}^*$, atunci $\varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_k^{\alpha_k - 1}(p_1 - 1)(p_2 - 1)\ldots(p_k - 1)$.

ELEMENTE DE ANALIZĂ MATEMATICĂ

Introducere: probleme care conduc la noţiunea de integrală

În clasa a XI-a am studiat un concept extrem de important care intervine în analiza matematică şi anume noţiunea de ***derivată*** a unei funcţii.

Partea din analiza matematică, care studiază derivatele, se mai numeşte şi ***calcul diferenţial***.

În acest an studiem un alt concept important şi anume acela de ***integrală***, concept care apare într-o dublă ipostază: ***integrala definită*** (acesta este propriu-zis conceptul de integrală), dar şi ***integrala nedefinită*** (în strânsă legătură cu o altă noţiune, aceea de primitivă a unei funcţii).

Partea din analiza matematică, care studiază integralele, se mai numeşte şi ***calcul integral***.

Fondatorii calculului diferenţial şi integral sunt *G. W. Leibniz* (1646 – 1716) în Germania şi *I. Newton* (1643 – 1727) în Anglia.

Am văzut că problemele care au condus la degajarea conceptului de ***derivată a unei funcţii într-un punct*** au fost: problema tangentei într-un punct la graficul unei funcţii (*Leibniz*), respectiv problema vitezei instantanee a unui mobil într-o mişcare neuniformă (*Newton*).

Vom vedea acum care sunt problemele ce conduc la degajarea conceptului de ***integrală*** şi de ***primitivă***.

1. Evaluarea ariei unui trapez curbiliniu

Să considerăm o funcţie continuă $f : [a, b] \to \mathbb{R}$ şi pozitivă, adică $f(x) \geq 0$, $\forall\, x \in [a, b]$. Suprafaţa plană delimitată de axa OX, graficul funcţiei f şi dreptele verticale de ecuaţii $x = a$, $x = b$ se numeşte „***trapez curbiliniu***" sau „***subgrafic***" asociat funcţiei f.

Problema care se pune este aceea a ***evaluării ariei*** acestui trapez curbiliniu. Desigur, aici trebuie să facem unele precizări. Noi ştim deocamdată să definim aria unei suprafeţe poligonale (care este, în ultimă instanţă, suma ariilor unor triunghiuri), dar nu ştim încă să definim aria unei suprafeţe plane oarecare. Fundamentarea conceptului de arie va fi făcută abia în ultimul capitol al acestui manual.

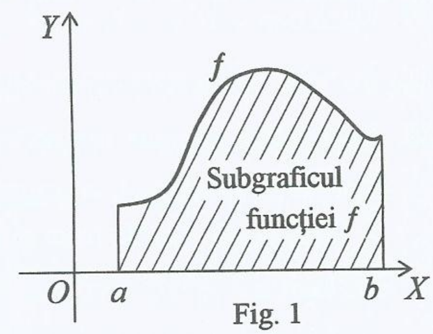


Fig. 1

Totuşi, *acceptăm intuitiv* că un astfel de trapez curbiliniu are o arie. Ideea de calcul a unei astfel de arii este foarte veche (datând de la Arhimede) şi constă în aproximarea ariei trapezului curbiliniu cu suma ariilor unor dreptunghiuri.

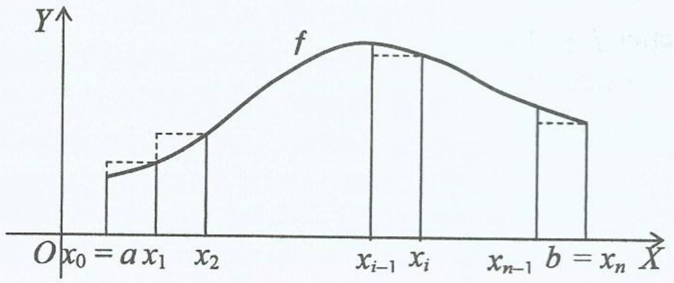


Fig. 2

Pentru aceasta, împărţim intervalul $[a, b]$ în n intervale mai mici prin „punctele de diviziune" $a = x_0 < x_1 < x_2 < \ldots < x_n = b$. Considerăm dreptunghiurile care au drept baze intervalele $[x_{i-1}, x_i]$ şi înălţimi $f(x_i)$, pentru fiecare $i = 1, 2, \ldots, n$ (fig. 2)

Suma ariilor acestor dreptunghiuri este:

$$\sum_{i=1}^{n} f(x_i)(x_i - x_{i-1}) = \sum_{i=1}^{n} f(x_i)dx_i,$$

unde am notat $dx_i = x_i - x_{i-1}$, $i = 1, 2, \ldots, n$.

Această sumă a ariilor dreptunghiurilor puse în evidenţă aproximează aria trapezului curbiliniu considerat.

Cu cât n este mai mare, iar lungimile bazelor dx_i mai mici, aproximarea este mai bună.

De aici ideea, aparţinând lui *Leibniz*, că aria trapezului curbiliniu este egală cu *limita* sumelor:

$$\sum_{i=1}^{n} f(x_i)dx_i \qquad (1)$$

când $n \to \infty$ şi $\max\limits_{1 \le i \le n} dx_i \to 0$.

Acceptând că această limită există, *Leibniz* o notează prin simbolul

$$\int_a^b f(x)dx$$

care se citeşte „integrală de la a la b din $f(x)dx$".

Semnul $\int$ este un S alungit şi marchează o sumă trecută la limită, în timp ce expresia $f(x)dx$ sugerează termenii sumei (1).

2. Funcţia – arie

Ca şi în problema precedentă, să considerăm o funcţie continuă şi pozitivă $f : [a, b] \to \mathbb{R}$. Pentru fiecare $t \in [a, b]$, notăm cu $F(t)$ aria „trapezului curbiliniu" delimitat de axa OX, graficul funcţiei f şi dreptele de ecuaţii $x = a$, $x = t$ (fig. 3). Funcţia $F : [a, b] \to \mathbb{R}$, care asociază fiecărui $t \in [a, b]$ numărul $F(t)$ definit mai sus, se numeşte „***funcţia - arie***" asociată funcţiei f.

Teoremă

Cu notaţiile şi ipotezele de mai sus, funcţia F este derivabilă, iar derivata sa este tocmai funcţia f, adică $F' = f$.

Pentru *a justifica* acest rezultat, vom arăta că $F'(t) = f(t)$, $\forall\ t \in [a, b]$. Fixăm aşadar un $t \in [a, b]$. Mai întâi, să admitem că $t \in (a, b)$. Alegem un $h > 0$ arbitrar, astfel încât $t + h < b$ (fig. 4).

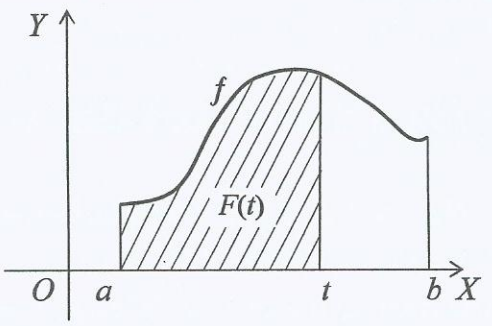


Fig. 3

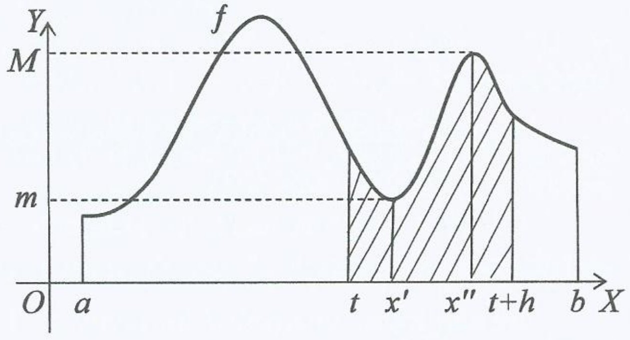


Fig. 4

Diferenţa $F(t + h) - F(t)$ este tocmai aria haşurată din fig. 4.

Conform teoremei de mărginire a lui Weierstrass, pe intervalul compact $[t, t + h]$ funcţia continuă f îşi atinge marginile. Aşadar, există $x', x'' \in [t, t + h]$ astfel încât $m = \inf\limits_{x\in[t,\, t+h]} f(x) = f(x')$, $M = \sup\limits_{x\in[t,\, t+h]} f(x) = f(x'')$. Deducem că aria haşurată este cuprinsă între aria dreptunghiului având ca bază intervalul $[t, t + h]$ iar înălţime m şi aria dreptunghiului de bază acelaşi interval $[t, t + h]$, dar înălţime M. Aşadar:
$hf(x') \le F(t + h) - F(t) \le hf(x'')$ sau, împărţind prin $h > 0$:

$$f(x') \le \frac{F(t+h) - F(t)}{h} \le f(x'') \qquad (1).$$

Când $h \searrow 0$, rezultă $x' \searrow t$, $x'' \searrow t$ şi cum f este continuă, vom avea

$\lim\limits_{h\searrow 0} f(x') = f(t)$ şi $\lim\limits_{h\searrow 0} f(x'') = f(t)$.

Trecând aşadar la limită când $h \searrow 0$ în inegalitatea (1) şi utilizând criteriul cleştelui, obţinem:

$$\lim_{h \searrow 0} \frac{F(t+h)-F(t)}{h} = f(t),$$

ceea ce înseamnă că $F_d'(t) = f(t)$. Analog se arată că $F_s'(t) = f(t)$, prin urmare $F'(t) = f(t)$.

Dacă $t = a$ sau $t = b$, raţionamentul este acelaşi, cu menţiunea că vom calcula doar o singură derivată laterală.

Cu aceasta, teorema enunţată este *justificată*.

Funcţia F având proprietatea că este derivabilă şi $F' = f$ se numeşte „***primitivă***" a funcţiei f.

Întrucât aria $F(t)$ a fost notată în prima problemă prin

$$\int_a^t f(x)dx,$$

ţinând seama că $F'(t) = f(t)$, putem scrie:

$$\frac{d}{dt}\left(\int_a^t f(x)dx\right) = f(t) \qquad (2),$$

unde $\frac{d}{dt}$ semnifică „***derivarea***" în raport cu variabila t.

În capitolele următoare vom studia riguros conceptele de integrală, primitivă, egalitatea (2) care stabileşte o legătură între integrală şi primitivă etc.

PRIMITIVE

Primitivele unei funcţii, integrala nedefinită

Peste tot de acum încolo I semnifică un interval (neredus la un punct) al dreptei reale. Una dintre problemele importante care se pun în analiza matematică este următoarea:

Fiind dată o funcţie $f : I \to \mathbb{R}$, există o funcţie $F : I \to \mathbb{R}$, derivabilă pe I, astfel încât $F' = f$?

Vom arăta că în anumite ipoteze (de exemplu, atunci când funcţia f este continuă) răspunsul la această problemă este afirmativ.

Mai mult, vom căuta procedee pentru determinarea funcţiei F când cunoaştem funcţia f.

Definiţie

Spunem că funcţia $f : I \to \mathbb{R}$ ***are (admite) primitive*** dacă există o funcţie derivabilă $F : I \to \mathbb{R}$ astfel încât $F' = f$, ceea ce înseamnă că $F'(x) = f(x)$ pentru orice $x \in I$.

Funcţia F se numeşte ***primitivă (antiderivată)*** a funcţiei f.

Dacă funcţia $f : I \to \mathbb{R}$ are primitive se mai spune că funcţia f este ***primitivabilă*** sau, totuna, că funcţia f este o ***derivată***.

De exemplu, funcţia $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ are primitive, o primitivă a sa fiind funcţia $F : \mathbb{R} \to \mathbb{R}$, $F(x) = \frac{x^3}{3}$, deoarece

$$\left(\frac{x^3}{3}\right)' = x^2, \ \forall x \in \mathbb{R}.$$

Un prim rezultat este dat de următoarea:

Propoziţie

Dacă funcţia $f : I \to \mathbb{R}$ are primitive, atunci:

1°. Oricare două primitive ale sale diferă printr-o constantă aditivă.

2°. Dacă F este o primitivă fixată a funcţiei f, atunci toate primitivele lui f sunt de forma $F + C$, unde C este o constantă reală arbitrară.

Demonstrație. 1°. Dacă F_1, $F_2 : I \to \mathbb{R}$ sunt două primitive ale funcției f, atunci: $F_1' = F_2' = f$. Deoarece ***două funcții care au derivate egale pe un interval diferă printr-o constantă***, rezultă că $F_2 = F_1 + C$, unde $C \in \mathbb{R}$.

2°. Din 1° rezultă că orice primitivă a lui f este de forma $F + C$, cu $C \in \mathbb{R}$.

Comentariu metodic

Ținând seama de modul în care se definesc operațiile „aritmetice" cu funcții (adunarea, scăderea, înmulțirea etc.) și de definiția egalității a două funcții, egalitatea $F_2 = F_1 + C$ care apare în demonstrația propoziției precedente, trebuie înțeleasă sub forma $F_2(x) = F_1(x) + C$, $\forall\, x \in I$.

Teoria funcțiilor care au primitive *se face pentru funcții definite pe un interval,* tocmai pentru faptul că funcțiile definite pe același interval și având derivate egale diferă printr-o constantă, ceea ce dă valabilitate propoziției precedente, care stabilește mulțimea primitivelor unei funcții date.

Definiția care urmează este extrem de importantă.

Definiție

Dacă funcția $f : I \to \mathbb{R}$ are primitive, mulțimea primitivelor sale se numește ***integrala nedefinită a funcției f*** și se notează

$$\int f(x)dx \qquad (1),$$

care se citește „***integrală din f(x)dx***".

Observație.

Cu notația introdusă pentru integrala nedefinită, utilizând și propoziția anterioară, deducem că dacă F este o primitivă fixată a funcției f, atunci:

$$\int f(x)dx = \{F + C \mid C \in \mathbb{R}\}.$$

De obicei, pentru simplitate, ***mulțimea funcțiilor constante definite pe I*** se notează cu $\mathscr{C}$, iar mulțimea $\{F + C \mid C \in \mathbb{R}\}$ se notează $F + \mathscr{C}$ sau $F(x) + \mathscr{C}$, în acest fel ultima egalitate scriindu-se sub forma:

$$\int f(x)dx = F(x) + \mathscr{C} \qquad (2).$$

De exemplu, scriem:

$$\int x^2 dx = \frac{x^3}{3} + \mathscr{C}.$$

Comentariu metodic privind notația integralei nedefinite

Notația $\int f(x)dx$ își are cumva explicația în proprietatea (2) de la pag. 147, care arată în definitiv că funcția – arie F definită prin $F(t)=\int_a^t f(x)dx$ este o primitivă a funcției continue f. De altfel, istoricește vorbind, multă vreme prin ***integrala nedefinită*** a funcției f s-a înțeles tocmai $\int_a^t f(x)dx$, spre deosebire de ***integrala definită*** care este $\int_a^b f(x)dx$ (diferența constă în aceea că t este variabil, „***nedefinit***", pe când b este fixat, „***definit***", ca și a).

Întrucât $\int_a^t f(x)dx$ este o primitivă a funcției continue f, denumirea s-a extins asupra tuturor primitivelor, ajungându-se la sensul actual: ***integrala nedefinită*** este mulțimea tuturor primitivelor.

Totodată, scrierea $\int f(x)dx$ marchează faptul că ***argumentul funcției f este notat cu x*** și atunci ***la fel va fi notat*** și ***argumentul oricărei primitive*** a lui f.

Dacă $u : I \to \mathbb{R}$ este o funcție derivabilă, expresia: $du = u'(x)dx$ se numește ***diferențiala formală a funcției u***.

În cazul particular al funcției identice $u(x)=x$, diferențiala formală este $du = dx$ și se numește ***diferențiala formală a argumentului***.

Dacă $f : I \to \mathbb{R}$ are primitiva F, atunci diferențiala formală a primitivei este $dF = F'(x)dx = f(x)dx$, adică ***exact expresia care se scrie sub semnul „integrală"***.

În acest fel egalitatea (2) se scrie sub forma „diferențială":

$$\int dF = F + \mathscr{C} \qquad (3)$$

și arată că ***integrala nedefinită*** (***trecerea la primitive***) ***și diferențierea formală sunt oarecum inverse una alteia***.

Această notație diferențială, rămasă tot de la *Leibniz*, se va dovedi foarte inspirată când vom studia metoda schimbării de variabilă.

Pornind de la formulele cunoscute de derivare, putem obține, prin „inversarea" acestora, formule „imediate" de integrare. De exemplu:

$$(\sin x)' = \cos x,\ x \in \mathbb{R} \Rightarrow \int \cos x\, dx = \sin x + \mathscr{C},\ x \in \mathbb{R}.$$

Redăm acum tabloul ***integralelor nedefinite imediate*** și ***intervalele de lungime maximă*** pe care aceste formule de integrare sunt adevărate; totodată, vom evidenția în acest tablou și unele cazuri particulare ale anumitor formule de integrare, demne de a fi reținute ca formule în sine.

Să remarcăm că funcțiile corespunzătoare „cazurile particulare" pot avea domeniul de definiție mai „larg" decât cele corespunzătoare „cazului general". Așa de exemplu funcția putere $f(x)=x^\alpha$ cu $\alpha \in \mathbb{R}$ este definită pe $(0, \infty)$, pe când funcția putere $f(x)=x^n$ cu $n \in \mathbb{N}^*$ este definită pe $\mathbb{R}$.

Tabelul primitivelor (integralelor nedefinite) imediate

Nr. crt.	Formula de integrare	Un interval maximal pe care este adevărată	Nr. crt.	Cazuri particulare	Un interval maximal pentru cazurile particulare
1.	$\int x^{\alpha} dx = \frac{x^{\alpha+1}}{\alpha+1}+\mathscr{C}$, $(\alpha \in \mathbb{R},\ \alpha \neq -1)$	$(0, \infty)$	1′	$\int dx = x+\mathscr{C}$	$\mathbb{R}$
			1″	$\int x^n dx = \frac{x^{n+1}}{n+1}+\mathscr{C}\ (n \in \mathbb{N}^*)$	$\mathbb{R}$
			1‴	$\int \frac{dx}{\sqrt{x}} = 2\sqrt{x}+\mathscr{C}$	$(0, \infty)$
2.	$\int \frac{dx}{x} = \ln\lvert x\rvert+\mathscr{C}$	$(-\infty, 0)$ sau $(0, \infty)$			
3.	$\int a^x dx = \frac{a^x}{\ln a}+\mathscr{C}$, $(a>0,\ a\neq 1)$	$\mathbb{R}$	3′	$\int e^x dx = e^x+\mathscr{C}$	$\mathbb{R}$
4.	$\int \sin x\, dx = -\cos x+\mathscr{C}$	$\mathbb{R}$			
5.	$\int \cos x\, dx = \sin x+\mathscr{C}$	$\mathbb{R}$			
6.	$\int \frac{dx}{\cos^2 x} = \int (1+\operatorname{tg}^2 x)dx = \operatorname{tg} x+\mathscr{C}$	$\left((2k-1)\frac{\pi}{2},\ (2k+1)\frac{\pi}{2}\right)$, $k \in \mathbb{Z}$			
7.	$\int \frac{dx}{\sin^2 x} = \int (1+\operatorname{ctg}^2 x)dx = -\operatorname{ctg} x+\mathscr{C}$	$(k\pi,\ (k+1)\pi)$, $k \in \mathbb{Z}$			
8.	$\int \frac{dx}{\sqrt{a^2-x^2}} = \arcsin\frac{x}{a}+\mathscr{C}$, $(a>0)$	$(-a, a)$	8′	$\int \frac{dx}{\sqrt{1-x^2}} = \arcsin x+\mathscr{C}$	$(-1, 1)$
9.	$\int \frac{dx}{x^2+a^2} = \frac{1}{a}\operatorname{arctg}\frac{x}{a}+\mathscr{C}$, $(a \in \mathbb{R},\ a \neq 0)$	$\mathbb{R}$	9′	$\int \frac{dx}{x^2+1} = \operatorname{arctg} x+\mathscr{C}$	$\mathbb{R}$
10.	$\int \frac{dx}{\sqrt{x^2+\alpha}} = \ln\left\lvert x+\sqrt{x^2+\alpha}\right\rvert+\mathscr{C}$, $(\alpha \in \mathbb{R},\ \alpha \neq 0)$	$\mathbb{R}$ dacă $\alpha>0$, $(-\infty, -\sqrt{-\alpha})$ sau $(\sqrt{-\alpha}, \infty)$ dacă $\alpha<0$	10′	$\int \frac{dx}{\sqrt{x^2+a^2}} = \ln\left(x+\sqrt{x^2+a^2}\right)+\mathscr{C}$ $(a \in \mathbb{R},\ a \neq 0)$	$\mathbb{R}$
			10″	$\int \frac{dx}{\sqrt{x^2-a^2}} = \ln\left\lvert x+\sqrt{x^2-a^2}\right\rvert+\mathscr{C}$ $(a \in \mathbb{R},\ a \neq 0)$	$(-\infty, -\lvert a\rvert)$ sau $(\lvert a\rvert, \infty)$
11.	$\int \frac{dx}{x^2-a^2} = \frac{1}{2a}\ln\left\lvert\frac{x-a}{x+a}\right\rvert+\mathscr{C}$, $(a \in \mathbb{R},\ a \neq 0)$	$(-\infty, -\lvert a\rvert)$ sau $(\lvert a\rvert, \infty)$ sau $(-\lvert a\rvert, \lvert a\rvert)$			

Faptul că funcția din membrul drept al fiecărei formule este o primitivă pentru funcția de sub integrală se verifică ușor prin derivare, dar este bine să fie făcut ca temă de către elevi. Totodată este bine să se rețină intervalele pe care sunt definite funcțiile respective și pe care „funcționează” deci, aceste formule de integrare.

Operații cu integrale nedefinite, liniaritatea integralei nedefinite

Vom defini în cele ce urmează ***suma*** a două integrale nedefinite, corespunzătoare unor funcții definite pe un același interval, precum și ***produsul*** dintre o integrală nedefinită și un scalar real.

Fie așadar $f, g : I \to \mathbb{R}$ două funcții care au primitive, deci pentru care putem vorbi de integralele lor nedefinite, iar λ un număr real.

Este ușor să remarcăm că funcțiile $f + g$ și λf, definite tot pe intervalul I, au primitive, deci au integrale nedefinite. Definim ***suma*** integralelor nedefinite asociate funcțiilor f și g prin egalitatea:

$$\int f(x)dx + \int g(x)dx \overset{\text{def.}}{=} \int (f+g)(x)dx = \int \left(f(x)+g(x)\right)dx. \qquad (1)$$

De asemenea, definim ***produsul*** dintre integrala nedefinită asociată funcției f și scalarul λ prin egalitatea:

$$\lambda \int f(x)dx \overset{\text{def.}}{=} \int (\lambda f)(x)dx = \int \lambda f(x)dx \qquad (2)$$

cu mențiunea că dacă $\lambda = 0$, ambii membri din (2) se consideră egali cu $\mathscr{C}$ (familia funcțiilor constante).

Comentariu metodic privind definițiile (1) și (2)

Definițiile (1) și (2) au o anumită explicație logică. Am văzut că

$$\int f(x)dx = F + \mathscr{C}$$

unde F este o primitivă (oarecare) a funcției f, iar $\mathscr{C}$ familia funcțiilor constante. Deoarece pentru orice $C \in \mathscr{C}$ avem $(F + C)' = f$, ***putem defini derivata formală a unei integrale nedefinite*** prin egalitatea:

$$\left(\int f(x)dx\right)' = f.$$

Această egalitate marchează cumva faptul că ***integrarea și derivarea sunt inverse una alteia***. Căutând atunci ca ***suma a două integrale nedefinite să fie tot o integrală nedefinită***, adică:

$$\int f(x)dx + \int g(x)dx = \int h(x)dx$$

cu $h : I \to \mathbb{R}$ funcție primitivabilă, trecând la derivate formale după regula „derivata sumei este egală cu suma derivatelor”, vom avea $f + g = h$.

Prin urmare, definiția pe care o dăm sumei a două integrale nedefinite trebuie să fie de tipul:

$$\int f(x)dx + \int g(x)dx = \int (f+g)(x)dx$$

adică tocmai definiția (1).

Analog, folosind regula „derivata produsului dintre un scalar şi o funcţie este egală cu produsul dintre acest scalar şi derivata funcţiei", se justifică definiţia (2).

Prin urmare, putem spune că *definiţiile* (1) şi (2) *„prelungesc" regulile de calcul de la derivate la integrale nedefinite*.

Totodată, definiţiile (1) şi (2) arată că operaţiile cu integrale nedefinite (deci, operaţii cu mulţimi de funcţii) sunt naturale, sunt „inspirate" de operaţiile corespunzătoare cu funcţii (suma, respectiv produsul cu un scalar).

O situaţie asemănătoare întâlnim când definim operaţiile cu clase de resturi (deci, operaţii cu mulţimi de numere întregi), care sunt „inspirate" de operaţiile corespunzătoare cu numere întregi (suma, respectiv produsul).

Să mai remarcăm că *nu putem defini produsul sau câtul a două integrale nedefinite* tocmai pentru faptul că *nu există* o regulă de tipul „derivata produsului (câtului) este egală cu produsul (câtul) derivatelor", pe care să o prelungim apoi la integrale nedefinite.

Observaţie

De obicei, definiţiile (1) şi (2) se citesc „invers", adică de la dreapta spre stânga şi se interpretează ca „proprietăţi" ale integralei nedefinite. Aşadar, avem egalităţile:

$$\int (f(x)+g(x))\,dx=\int f(x)dx+\int g(x)dx \qquad (3)$$

$$\int \lambda f(x)dx=\lambda\int f(x)dx \qquad (4)$$

cu aceeaşi menţiune, că pentru $\lambda = 0$, ambii membri din (4) se consideră egali cu $\mathscr{C}$.

Egalitatea (3) arată că *integrala sumei este egală cu suma integralelor* şi se exprimă concis prin aceea că *integrala este aditivă*.

Egalitatea (4) arată că *o constantă multiplicativă iese în faţa integralei* şi se exprimă concis prin aceea că *integrala este omogenă*.

Proprietăţile (3) şi (4) se exprimă laolaltă prin aceea că *integrala (nedefinită) este liniară*.

Consecinţă

Dacă $f, g : I \to \mathbb{R}$ sunt funcţii cu primitive, atunci:

1°. $\int (-f(x))\,dx=-\int f(x)dx$.

2°. $\int (g(x)-f(x))\,dx=\int g(x)dx-\int f(x)dx$.

Demonstraţie. 1°. Rezultă din egalitatea (4) în care luăm $\lambda = -1$.

2°. Avem $\int (g(x)-f(x))\,dx=\int [g(x)+(-f(x))]\,dx\overset{(3)}{=}\int g(x)dx+\int (-f(x))\,dx\overset{1°}{=}$

$=\int g(x)dx-\int f(x)dx$.

Observație

Liniaritatea integralei nedefinite se poate extinde (prin inducție) pentru oricâte funcții, în număr finit. Mai precis, dacă avem date funcțiile $f_1, f_2, \ldots, f_n : I \to \mathbb{R}$, având primitive şi scalarii $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{R}$, atunci există egalitatea:

$$\int \left(\lambda_1 f_1(x) + \lambda_2 f_2(x) + \ldots + \lambda_n f_n(x)\right) dx = \lambda_1 \int f_1(x)dx + \lambda_2 \int f_2(x)dx + \ldots + \lambda_n \int f_n(x)dx.$$

Exercițiu rezolvat

Să se calculeze integralele nedefinite:

a) $\displaystyle\int \left(x^4 + \frac{3}{x} - 8\sqrt[3]{x} + 2^x \right) dx$, $x \in (0, \infty)$;

b) $\displaystyle\int \left(\sin x + \cos x + \operatorname{tg}^2 x - \operatorname{ctg}^2 x\right) dx$, $x \in \left(0, \frac{\pi}{2}\right)$;

c) $\displaystyle\int \left(\frac{1}{\sqrt{9-x^2}} + \frac{1}{\sqrt{9+x^2}} + \frac{3}{9+x^2} + \frac{6}{9-x^2} \right) dx$, $x \in (-3; 3)$.

Soluție. Utilizăm tabloul integralelor uzuale, precum şi liniaritatea integralei. Avem:

a) $\displaystyle\int \left(x^4 + \frac{3}{x} - 8\sqrt[3]{x} + 2^x \right) dx = \int x^4 dx + 3\int \frac{dx}{x} - 8\int x^{\frac{1}{3}} dx + \int 2^x dx =$

$$= \frac{x^5}{5} + 3\ln|x| - 8 \cdot \frac{x^{\frac{1}{3}+1}}{\frac{1}{3}+1} + \frac{2^x}{\ln 2} + \mathscr{C} = \frac{x^5}{5} + 3\ln x - 6\sqrt[3]{x^4} + \frac{2^x}{\ln 2} + \mathscr{C}.$$

b) $\displaystyle\int \left(\sin x + \cos x + \operatorname{tg}^2 x - \operatorname{ctg}^2 x\right) dx = \int \left(\sin x + \cos x + (1 + \operatorname{tg}^2 x) - (1 + \operatorname{ctg}^2 x)\right) dx =$

$$= \int \sin x dx + \int \cos x \, dx + \int (1 + \operatorname{tg}^2 x) dx - \int (1 + \operatorname{ctg}^2 x) dx =$$

$$= -\cos x + \sin x + \operatorname{tg} x - (-\operatorname{ctg} x) + \mathscr{C} = \sin x - \cos x + \operatorname{tg} x + \operatorname{ctg} x + \mathscr{C}.$$

c) $\displaystyle\int \left(\frac{1}{\sqrt{9-x^2}} + \frac{1}{\sqrt{9+x^2}} + \frac{3}{9+x^2} + \frac{6}{9-x^2} \right) dx = \int \frac{dx}{\sqrt{9-x^2}} + \int \frac{dx}{\sqrt{9+x^2}} + 3\int \frac{dx}{9+x^2} - 6\int \frac{dx}{x^2-9} =$

$$= \arcsin \frac{x}{3} + \ln\left|x + \sqrt{9+x^2}\right| + 3 \cdot \frac{1}{3} \operatorname{arctg} \frac{x}{3} - 6 \cdot \frac{1}{6} \ln\left|\frac{x-3}{x+3}\right| + \mathscr{C} =$$

$= \arcsin \dfrac{x}{3} + \ln\left(x + \sqrt{9+x^2}\right) + \operatorname{arctg} \dfrac{x}{3} - \ln \dfrac{3-x}{3+x} + \mathscr{C}$, unde am ținut seama că $x + \sqrt{9+x^2} > x + \sqrt{x^2} = x + |x| \geq 0$, deci $\left|x + \sqrt{9+x^2}\right| = x + \sqrt{9+x^2}$, iar $\left|\dfrac{x-3}{x+3}\right| = \dfrac{3-x}{3+x}$ pentru $x \in (-3, 3)$.

Primitive uzuale

Pentru calculul primitivelor (integralelor nedefinite) uzuale, utilizăm tabloul primitivelor imediate, liniaritatea integralei nedefinite, dar şi două metode foarte simple şi anume schimbarea de variabilă şi integrarea prin părţi.

Schimbarea de variabilă (integrala unei funcţii compuse)

Cadrul teoretic al metodei este dat de următoarea:

Teoremă

Dacă avem funcţiile $I \xrightarrow{u} J \xrightarrow{f} \mathbb{R}$ (I, J intervale) cu proprietatea că u este derivabilă, iar f are primitiva F, atunci:

$$\int f(u(x))u'(x)dx = F(u(x)) + \mathscr{C}.$$

Demonstraţie. Este suficient să observăm că funcţia $F \circ u$ este o primitivă pentru funcţia de sub integrală $(f \circ u)u'$. Acest lucru rezultă imediat, ţinând seama de formula de derivare a unei funcţii compuse şi de faptul că $F' = f$. Avem, într-adevăr:

$$(F \circ u)' = (F' \circ u)u' = (f \circ u)u'.$$

Comentariu metodic

Practic, când vrem să calculăm o integrală de tipul $\int f(u(x))u'(x)dx$, efectuăm următorii paşi:

1°. facem substituţia (notaţia) $t = u(x)$;

2°. diferenţiem formal, adică $dt = u'(x)\,dx$;

3°. înlocuim în integrala de calculat şi obţinem succesiv:

$$\int f(u(x))u'(x)dx \overset{(1)}{=} \int f(t)dt = F(t) + \mathscr{C} \overset{(2)}{=} F(u(x)) + \mathscr{C}.$$

Egalităţile (1) şi (2) *sunt formale*, întrucât ele stabilesc „egalitatea" unor mulţimi de funcţii cu domenii de definiţie diferite. Totuşi, ***prin tradiţie s-a încetăţenit scrierea lor*** în succesiunea de egalităţi de la punctul 3°, întrucât lasă calculele „să curgă".

Metoda se numeşte „*schimbare de variabilă*", întrucât de la variabila iniţială x se trece la variabila t, se calculează integrala funcţiei în t, după care se revine la variabila x. Datorită substituţiei $t = u(x)$, acest mod de a calcula integrale nedefinite, se numeşte şi *metoda substituţiei*.

Exerciții rezolvate

1. Să se calculeze integralele:

a) $\int x\left(x^2-1\right)^{99} dx$, $x \in \mathbb{R}$; **b)** $\int \frac{\ln x}{x} dx$, $x \in (0, \infty)$;

c) $\int \frac{x}{100+x^4} dx$, $x \in \mathbb{R}$.

Soluție. **a)** Facem substituția $t = x^2 - 1$, de unde $dt = 2x\, dx$. Atunci:

$$\int x\left(x^2-1\right)^{99} dx = \frac{1}{2} \cdot \int \left(x^2-1\right)^{99} \cdot 2x\, dx = \frac{1}{2}\int t^{99} dt = \frac{1}{2} \cdot \frac{t^{100}}{100} + \mathscr{C} = \frac{\left(x^2-1\right)^{100}}{200} + \mathscr{C}.$$

b) Facem substituția $t = \ln x$, de unde $dt = \frac{dx}{x}$. Atunci:

$$\int \frac{\ln x}{x} dx = \int t\, dt = \frac{t^2}{2} + \mathscr{C} = \frac{\ln^2 x}{2} + \mathscr{C}.$$

c) Facem substituția $t = x^2$, de unde $dt = 2x\, dx$. Atunci:

$$\int \frac{x}{100+x^4} dx = \frac{1}{2} \cdot \int \frac{2x\, dx}{x^4+100} = \frac{1}{2}\int \frac{dt}{t^2+100} = \frac{1}{2} \cdot \frac{1}{10} \operatorname{arctg} \frac{t}{10} + \mathscr{C} = \frac{1}{20} \operatorname{arctg} \frac{x^2}{10} + \mathscr{C}.$$

2. Să se calculeze integralele:

a) $\int \frac{x^2-1}{x^2} \cos \frac{x^2+1}{x} dx$, $x \in (0, \infty)$; **b)** $\int \operatorname{tg} x\, dx$, $x \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$;

c) $\int \operatorname{ctg} x\, dx$, $x \in (0, \pi)$.

Soluție. **a)** Notăm $t = \frac{x^2+1}{x}$, de unde $dt = \frac{x^2-1}{x^2} dx$ și avem:

$$\int \frac{x^2-1}{x^2} \cos \frac{x^2+1}{x} dx = \int \cos t\, dt = \sin t + \mathscr{C} = \sin \frac{x^2+1}{x} + \mathscr{C}.$$

b) Facem substituția $t = \cos x$, de unde $dt = -\sin x\, dx$ și avem:

$$\int \operatorname{tg} x\, dx = -\int \frac{-\sin x\, dx}{\cos x} = -\int \frac{dt}{t} = -\ln|t| + \mathscr{C} = -\ln|\cos x| + \mathscr{C} = -\ln(\cos x) + \mathscr{C},$$

deoarece $\cos x > 0$ pentru $x \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$.

c) Facem substituția $t = \sin x$, de unde $dt = \cos x\, dx$ și avem:

$$\int \operatorname{ctg} x\, dx = \int \frac{\cos x\, dx}{\sin x} = \int \frac{dt}{t} = \ln|t| + \mathscr{C} = \ln|\sin x| + \mathscr{C} = \ln(\sin x) + \mathscr{C},$$

deoarece $\sin x > 0$ pentru $x \in (0, \pi)$.

Formula integrării prin părţi (integrala unui produs)

Se pune problema cum calculăm integrala produsului a două funcţii, mai ales că – aşa cum am văzut – nu are sens să definim produsul a două integrale. Un răspuns parţial este dat de metoda integrării prin părţi. Cadrul teoretic este dat de următoarea:

Teoremă

Dacă $u, v : I \to \mathbb{R}$ sunt funcţii derivabile, iar funcţia $u'v$ are primitive, atunci şi funcţia uv' are primitive şi există egalitatea:

$$\int u(x)v'(x)dx = u(x)v(x) - \int u'(x)v(x)dx$$

sau, în notaţie diferenţială:

$$\int u\, dv = uv - \int v\, du .$$

Oricare din aceste egalităţi se numeşte *formula de integrare prin părţi*.

Demonstraţie. Funcţia produs este derivabilă şi avem:

$$(uv)' = u'v + uv' .$$

Rezultă $uv' = (uv)' - u'v$ şi atunci funcţia uv' are primitive, deoarece este diferenţa a două funcţii cu primitive. Integrând, obţinem:

$$\int u(x)v'(x)dx = \int \left[u(x)v(x)\right]' dx - \int u'(x)v(x)dx = u(x)v(x) - \int u'(x)v(x)dx .$$

Observaţie

De regulă – deşi există şi excepţii – în alegerea funcţiilor u şi v' se ia în rolul lui u o funcţie mai „dificilă”.

Exerciţii rezolvate

1. Să se calculeze integralele:

a) $\int x \ln x\, dx$, $x \in (0, \infty)$; **b)** $\int x \sin x\, dx$, $x \in \mathbb{R}$; **c)** $\int \operatorname{arctg} x\, dx$, $x \in \mathbb{R}$.

Soluţie. **a)** Notăm $u = \ln x$, $dv = x\, dx$, de unde $du = \dfrac{dx}{x}$, $v = \dfrac{x^2}{2}$.

Aplicând formula $\int u\, dv = uv - \int v\, du$, obţinem:

$$\int x \ln x\, dx = \frac{x^2}{2}\ln x - \int \frac{x^2}{2}\cdot\frac{dx}{x} = \frac{x^2}{2}\ln x - \frac{1}{2}\int x\, dx = \frac{x^2}{2}\ln x - \frac{x^2}{4} + \mathscr{C} .$$

b) Luăm $u = x$, $dv = \sin x\, dx$, de unde $du = dx$, $v = -\cos x$, deci:

$$\int x \sin x\, dx = -x\cos x - \int(-\cos x)dx = -x\cos x + \sin x + \mathscr{C} .$$

c) Luăm $u = \text{arctg}\, x$, $dv = dx$, de unde $du = \dfrac{dx}{x^2+1}$, $v = x$, deci:

$$\int \text{arctg}\, x\, dx = x\, \text{arctg}\, x - \int \frac{x\, dx}{x^2+1} \quad (1).$$

Integrala la care am ajuns se calculează prin substituția $t = x^2 + 1$ de unde $dt = 2x\, dx$, prin urmare:

$$\int \frac{x\, dx}{x^2+1} = \frac{1}{2}\int \frac{2x\, dx}{x^2+1} = \frac{1}{2}\int \frac{dt}{t} = \frac{1}{2}\ln|t| + \mathscr{C} = \frac{1}{2}\ln(x^2+1) + \mathscr{C}.$$

Continuând în (1) obținem:

$$\int \text{arctg}\, x\, dx = x\, \text{arctg}\, x - \frac{1}{2}\ln(x^2+1) + \mathscr{C}.$$

2. Să se calculeze integralele:

a) $\int x^2 \sin x\, dx$, $x \in \mathbb{R}$; **b)** $\int e^x \sin x\, dx$, $x \in \mathbb{R}$; **c)** $\int \sin(\ln x) dx$, $x \in (0, \infty)$.

Soluție. **a)** Luăm $u = x^2$, $dv = \sin x\, dx$, de unde $du = 2x\, dx$, $v = -\cos x$, deci:

$$\int x^2 \sin x\, dx = -x^2 \cos x - \int 2x(-\cos x) dx = -x^2 \cos x + 2\int x \cos x\, dx \quad (1).$$

Integrala la care am ajuns se calculează tot prin părți, luând $u_1 = x$, $dv_1 = \cos x\, dx$, de unde $du_1 = dx$, $v_1 = \sin x$ și atunci:

$$\int x \cos x\, dx = x \sin x - \int \sin x\, dx = x \sin x + \cos x + \mathscr{C}.$$

Înlocuind în (1) obținem:

$$\int x^2 \sin x\, dx = -x^2 \cos x + 2x \sin x + 2\cos x + \mathscr{C}.$$

b) Luăm $u = \sin x$, $dv = e^x dx$, de unde $du = \cos x\, dx$, $v = e^x$, prin urmare:

$$\int e^x \sin x\, dx = e^x \sin x - \int e^x \cos x\, dx, \quad (1).$$

Integrala la care am ajuns se calculează tot prin părți, luând $u_1 = \cos x$, $dv_1 = e^x dx$, de unde $du_1 = -\sin x\, dx$, $v_1 = e^x$ și atunci:

$$\int e^x \cos x\, dx = e^x \cos x - \int e^x(-\sin x)\, dx = e^x \cos x + \int e^x \sin x\, dx.$$

Înlocuind în (1) rezultă:

$$\int e^x \sin x\, dx = e^x \sin x - e^x \cos x - \int e^x \sin x\, dx,$$

adică, notând $I(x) = \int e^x \sin x\, dx$, am obținut: $I(x) = e^x(\sin x - \cos x) - I(x)$.

Rezolvând această ecuație cu necunoscuta $I(x)$, obținem:

$$I(x) = \frac{e^x(\sin x - \cos x)}{2} + \mathscr{C}.$$

c) Luăm $u = \sin(\ln x)$, $dv = dx$, de unde $du = \dfrac{\cos(\ln x)}{x}dx$, $v = x$, deci:

$$\int \sin(\ln x)dx = x\sin(\ln x) - \int x \cdot \frac{\cos(\ln x)}{x}dx = x\sin(\ln x) - \int \cos(\ln x)dx \quad (1).$$

Integrala la care am ajuns se calculează luând $u_1 = \cos(\ln x)$, $dv_1 = dx$, de unde $du_1 = -\frac{\sin(\ln x)}{x}dx$, $v_1 = x$, deci:

$$\int \cos(\ln x)dx = x\cos(\ln x) - \int x\left(-\frac{\sin(\ln x)}{x}\right)dx = x\cos(\ln x) + \int \sin(\ln x)dx.$$

Înlocuind în (1) se obține:

$$\int \sin(\ln x)dx = x\sin(\ln x) - x\cos(\ln x) - \int \sin(\ln x)dx.$$

Notând $I(x) = \int \sin(\ln x)dx$, am obținut ecuația:

$$I(x) = x\left(\sin(\ln x) - \cos(\ln x)\right) - I(x), \text{ de unde}$$

$$I(x) = \frac{x\left(\sin(\ln x) - \cos(\ln x)\right)}{2} + \mathscr{C}.$$

3. Să se calculeze integralele: $\int \sqrt{x^2+\alpha}\ dx$, $\int \sqrt{a^2-x^2}\ dx$ ($\alpha \in \mathbb{R}^*$, $a > 0$) definite pe câte un interval pentru care $x^2+\alpha > 0$, respectiv $a^2-x^2 > 0$.

Soluție. Notăm $I(x) = \int \sqrt{x^2+\alpha}\ dx$, $J(x) = \int \sqrt{a^2-x^2}\ dx$. Pentru calculul lui $I(x)$ avem succesiv:

$$I(x) = \int \frac{x^2+\alpha}{\sqrt{x^2+\alpha}}dx = \alpha\int \frac{dx}{\sqrt{x^2+\alpha}} + \int x \cdot \frac{x}{\sqrt{x^2+\alpha}}dx = \alpha\ln\left|x+\sqrt{x^2+\alpha}\right| + \int x\left(\sqrt{x^2+\alpha}\right)' dx =$$

$$= \alpha\ln\left|x+\sqrt{x^2+\alpha}\right| + x\sqrt{x^2+\alpha} - \int \left(\sqrt{x^2+\alpha}\right)x'dx = \alpha\ln\left|x+\sqrt{x^2+\alpha}\right| + x\sqrt{x^2+\alpha} - I(x),$$

de unde

$$I(x) = \frac{x\sqrt{x^2+\alpha}}{2} + \frac{\alpha}{2}\ln\left|x+\sqrt{x^2+\alpha}\right| + \mathscr{C}.$$

Asemănător găsim:

$$J(x) = \frac{x\sqrt{a^2-x^2}}{2} + \frac{a^2}{2}\arcsin\frac{x}{a} + \mathscr{C}.$$

Formulele găsite pot fi chiar reținute, întrucât integralele nedefinite de acest tip apar frecvent.

EXERCIȚII PROPUSE

I. Calculați integralele nedefinite de mai jos:

1. $\int dx$, $x \in \mathbb{R}$;

2. $\int 5\,dx$, $x \in \mathbb{R}$;

3. $\int x^3 dx$, $x \in \mathbb{R}$;

4. $\int x^{-2} dx$, $x \in (0, \infty)$;

5. $\int \sqrt{x}\,dx$, $x \in [0, \infty)$;

6. $\int \sqrt[3]{x}\,dx$, $x \in \mathbb{R}$;

7. $\int \frac{dx}{\sqrt[5]{x}}$, $x \in (-\infty, 0)$;

8. $\int (4x^3 - 6x^2 - 4x + 3)dx$, $x \in \mathbb{R}$;

9. $\int \left(\frac{4}{3}x^3 - \frac{3}{4}x^2 + 5\right)dx$, $x \in \mathbb{R}$;

10. $\int 3(2x^2 - 1)^2\,dx$, $x \in \mathbb{R}$;

11. $\int x^3(1 + 5x)dx$, $x \in \mathbb{R}$;

12. $\int x^4(x - 1)dx$, $x \in \mathbb{R}$;

13. $\int \frac{x^2 - x + 1}{3x}dx$, $x \in (0, \infty)$;

14. $\int (3x^{-4} + 8x^{-5})dx$, $x \in (-\infty, 0)$;

15. $\int \left(5x^{\frac{3}{2}} - 7x^{\frac{3}{4}}\right)dx$, $x \in [0, \infty)$;

16. $\int \frac{x^{\frac{1}{2}} - x^{\frac{1}{3}} + x^{\frac{1}{4}}}{x^2}dx$, $x \in (0, \infty)$;

17. $\int \frac{x^{\frac{3}{4}} + x^{\frac{2}{3}} + x^{\frac{1}{2}}}{x}dx$, $x \in (0, \infty)$;

18. $\int \left(\frac{3}{x^2} - \frac{2}{\sqrt{x}} + \frac{4\sqrt[3]{x^2}}{x}\right)dx$, $x \in (0, \infty)$;

19. $\int 5^x dx$, $x \in \mathbb{R}$;

20. $\int 3^{2x} dx$, $x \in \mathbb{R}$;

21. $\int (e^x + 2x)dx$, $x \in \mathbb{R}$;

22. $\int \frac{(x^2 + 1)(x^2 - 2)}{\sqrt[3]{x^2}}dx$, $x \in (0, \infty)$;

23. $\int \frac{dx}{\sqrt{8 - x^2}}$, $x \in \left(-2\sqrt{2}, 2\sqrt{2}\right)$;

24. $\int \frac{\left(\sqrt{a} - \sqrt{x}\right)^4}{\sqrt{ax}}dx$, $x \in (0, \infty)$, $a > 0$;

25. $\int \frac{dx}{\sqrt{4 + x^2}}$, $x \in \mathbb{R}$;

26. $\int \frac{\sqrt{3 + x^2} - \sqrt{3 - x^2}}{\sqrt{9 - x^4}}dx$, $x \in \left(-\sqrt{3}, \sqrt{3}\right)$;

27. $\int (\sin x - 5\cos x)dx$, $x \in \mathbb{R}$;

28. $\int \frac{\sin 2x}{\cos x}dx$, $x \in \left(0, \frac{\pi}{2}\right)$;

29. $\int 3^x e^x dx$, $x \in \mathbb{R}$;

30. $\int \frac{dx}{2\cos^2 x}$, $x \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$;

31. $\int \frac{3\,dx}{\sin^2 x}$, $x \in (0, \pi)$;

32. $\int \frac{dx}{x^2 - 9}$, $x \in (3, \infty)$;

33. $\int \frac{dx}{x^2 - 25}$, $x \in (-5, 5)$;

34. $\int \frac{dx}{x^2 + 25}$, $x \in \mathbb{R}$;

35. $\int \frac{dx}{\sqrt{x^2 - 16}}$, $x \in (-\infty, -4)$;

36. $\int \frac{dx}{\sqrt{16 - x^2}}$, $x \in (-4, 4)$;

37. $\int \frac{dx}{\sqrt{16 - 9x^2}}$, $x \in \left(-\frac{4}{3}, \frac{4}{3}\right)$;

38. $\int \frac{dx}{16 + 25x^2}$, $x \in \mathbb{R}$;

39. $\int \mathrm{tg}^2 x\, dx$, $x \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$;

40. $\int \mathrm{ctg}^2 x\, dx$, $x \in (0, \pi)$.

II. Utilizând metoda schimbării de variabilă, calculați integralele:

1. $\int (3x+2)^5 dx$, $x \in \mathbb{R}$;

2. $\int \frac{dx}{(4x+1)^4}$, $x \in \left(-\frac{1}{4}, \infty\right)$;

3. $\int (2x^3+1)^4 x^2 dx$, $x \in \mathbb{R}$;

4. $\int \frac{x\,dx}{(x^2+1)^3}$, $x \in \mathbb{R}$;

5. $\int \frac{x^2 dx}{5x^3+1}$, $x \in \left(-\frac{1}{\sqrt[3]{5}}, \infty\right)$;

6. $\int \frac{dx}{(5x+1)^3}$, $x \in \left(-\infty, -\frac{1}{5}\right)$;

7. $\int \sqrt[3]{(3x+1)^2}\, dx$, $x \in \mathbb{R}$;

8. $\int \sqrt{2x-1}\, dx$, $x \in \left[\frac{1}{2}, \infty\right)$;

9. $\int \sqrt[3]{(3x+1)^2}\, dx$, $x \in \mathbb{R}$;

10. $\int \frac{dx}{\sqrt{(3x-1)^2}}$, $x \in \left(\infty, \frac{1}{3}\right)$;

11. $\int \frac{dx}{\sqrt[3]{(3x-5)^2}}$, $x \in \left(\frac{5}{3}, \infty\right)$;

12. $\int (x^2+3)^5 x\, dx$, $x \in \mathbb{R}$;

13. $\int (x^4-1)^2 x^3 dx$, $x \in \mathbb{R}$;

14. $\int \frac{6x^2 dx}{(1-2x^3)^4}$, $x \in \left(\frac{1}{\sqrt[3]{2}}, \infty\right)$;

15. $\int \frac{x^3 dx}{(5x^4+3)^5}$, $x \in \mathbb{R}$;

16. $\int x^2\sqrt{4x^3+1}\, dx$, $x \in \left[-\frac{1}{\sqrt[4]{3}}, \infty\right)$;

17. $\int x^3\sqrt{(x^4-1)^3}\, dx$, $x \in \mathbb{R}$;

18. $\int x \cdot 3^{5x^2} dx$, $x \in \mathbb{R}$;

19. $\int x \cdot e^{-3x^2+1}\, dx$, $x \in \mathbb{R}$;

20. $\int \mathrm{tg}\, x\, dx$, $x \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$;

21. $\int \operatorname{ctg} x\, dx$, $x \in (0, \pi)$;

22. $\int e^x\sqrt{e^x+1}\, dx$, $x \in \mathbb{R}$;

23. $\int \cos x\sqrt{2\sin x - 1}\, dx$, $x \in \left[\frac{\pi}{6}, \frac{\pi}{2}\right]$;

24. $\int x^3\sqrt{(3x^4+2)^3}\, dx$, $x \in \mathbb{R}$;

25. $\int x\sqrt[3]{(1-3x^2)^4}\, dx$, $x \in \mathbb{R}$;

26. $\int \frac{x\, dx}{\sqrt{x^2+1}}$, $x \in \mathbb{R}$;

27. $\int \frac{x^3 dx}{\sqrt[3]{(5x^4+2)^3}}$, $x \in \mathbb{R}$;

28. $\int \frac{x^2 dx}{\sqrt{(x^3-1)^3}}$, $x \in (1, \infty)$;

29. $\int \frac{e^x dx}{(e^x+1)^3}$, $x \in \mathbb{R}$;

30. $\int \frac{\cos x\, dx}{\sqrt{1-\sin x}}$, $x \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$:

31. $\int \frac{dx}{x(1+\ln x)}$, $x \in \left(0, \frac{1}{e}\right)$;

32. $\int \frac{e^{\sqrt{x}}}{\sqrt{x}}dx$, $x \in 0, \infty)$;

33. $\int \frac{\cos\sqrt{x}\, dx}{\sqrt{x}}$, $x \in (0, \infty)$;

34. $\int \frac{x^2 dx}{1+x^6}$, $x \in \mathbb{R}$;

35. $\int xe^{-x^2} dx$, $x \in \mathbb{R}$;

36. $\int xe^{-x^2} dx$, $x \in \mathbb{R}$;

37. $\int \sin x \cdot e^{\cos x}\, dx$, $x \in \mathbb{R}$;

38. $\int \cos x \cdot e^{\sin x}\, dx$, $x \in \mathbb{R}$;

39. $\int \frac{dx}{\sqrt{x}\cos^2\sqrt{x}}$, $x \in \left(0, \frac{\pi^2}{4}\right)$;

40. $\int \frac{dx}{x^2\sin^2\frac{1}{x}}$, $x \in \left(\frac{1}{\pi}, \infty\right)$;

41. $\int \frac{dx}{x\sin^2(\ln x)}$, $x \in \left(1, e^{\pi}\right)$;

42. $\int \frac{e^x dx}{\sqrt{1-e^{2x}}}$, $x \in (-\infty, 0)$;

43. $\int \frac{dx}{x\sqrt{1-\ln^2 x}}$, $x \in \left(\frac{1}{e}, e\right)$;

44. $\int \frac{e^x dx}{1+e^{2x}}$, $x \in \mathbb{R}$;

45. $\int \frac{dx}{x(1+\ln^2 x)}$, $x \in (0, \infty)$;

46. $\int \frac{e^{\frac{1}{x}}}{x^2}dx$, $x \in (-\infty, 0)$;

47. $\int \frac{x^2}{\sqrt{x^6-1}}dx$, $x \in (1, \infty)$;

48. $\int \frac{\operatorname{arctg} x}{1+x^2}dx$, $x \in \mathbb{R}$;

49. $\int \sqrt{\frac{\arcsin x}{1-x^2}}dx$, $x \in [0, 1)$;

50. $\int \frac{1-\sin x}{x+\cos x}dx$, $x \in \left[0, \frac{\pi}{2}\right]$;

51. $\int \frac{dx}{x\ln^2 x}$, $x \in (1, \infty)$;

52. $\int \frac{x\,dx}{\sqrt{1-x^4}}$, $x \in (-1, 1)$;

53. $\int \frac{\sqrt[3]{1+\ln x}}{x}dx$, $x \in (0, \infty)$;

54. $\int \frac{\sin 2x}{\sqrt{1-\sin^4 x}}dx$, $x \in \left[0, \frac{\pi}{2}\right)$;

55. $\int \frac{dx}{\sin^2 x\cos^2 x}$, $x \in \left(0, \frac{\pi}{2}\right)$;

56. $\int \sqrt{\frac{\ln\left(x+\sqrt{x^2+1}\right)}{1+x^2}}dx$, $x \in [0, \infty)$.

III. Utilizând metoda integrării prin părți, calculați integralele:

1. $\int x\sin x\,dx$, $x \in \mathbb{R}$;

2. $\int x\cos x\,dx$, $x \in \mathbb{R}$;

3. $\int \frac{\ln x}{x}dx$, $x \in (0, \infty)$;

4. $\int \frac{\ln x}{x^2}dx$, $x \in (0, \infty)$;

5. $\int \ln x\,dx$, $x \in (0, \infty)$;

6. $\int xe^x dx$, $x \in \mathbb{R}$;

7. $\int \frac{x}{e^x}dx$, $x \in \mathbb{R}$;

8. $\int \frac{x\,dx}{\sin^2 x}$, $x \in (0, \pi)$;

9. $\int \frac{x\,dx}{\cos^2 x}$, $x \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$;

10. $\int \operatorname{arctg} x\,dx$, $x \in \mathbb{R}$;

11. $\int \arcsin x\,dx$, $x \in (-1, 1)$;

12. $\int \arcsin x\,dx$, $x \in [-1, 1]$;

13. $\int e^x \cdot \sin x\,dx$, $x \in \mathbb{R}$;

14. $\int e^x \cdot \cos x\,dx$, $x \in \mathbb{R}$;

15. $\int x\arcsin x\,dx$, $x \in [-1, 1]$;

16. $\int x\operatorname{arctg} x\,dx$, $x \in \mathbb{R}$;

17. $\int \ln^2 x\,dx$, $x \in (0, \infty)$;

18. $\int \frac{\ln x}{\sqrt{x}}dx$, $x \in (0, \infty)$;

19. $\int \ln\left(x+\sqrt{1+x^2}\right)dx$, $x \in (0, \infty)$;

20. $\int \cos(\ln x)dx$, $x \in (0, \infty)$;

21. $\int x\sin^2 x\,dx$, $x \in \mathbb{R}$;

22. $\int x\cos^2 x\,dx$, $x \in \mathbb{R}$;

23. $\int x^2 \sin x\,dx$, $x \in \mathbb{R}$;

24. $\int x^2 \cos x\,dx$, $x \in \mathbb{R}$;

25. $\int x^2\operatorname{arctg} x\,dx$, $x \in \mathbb{R}$;

26. $\int x(\operatorname{arctg} x)^2 dx$, $x \in \mathbb{R}$;

27. $\int \sqrt{a^2+x^2}dx$, $x \in \mathbb{R}^*$;

28. $\int \sqrt{a^2-x^2}dx$, $x \in (-a, a)$, $a > 0$;

29. $\int \frac{x^2}{\sqrt{a^2+x^2}}dx$, $x \in \mathbb{R}^*$;

30. $\int \frac{x^2}{\sqrt{a^2-x^2}}dx$, $x \in (-a, a)$, $a > 0$.

TESTE DE EVALUARE

Testul 1

(timp de lucru - 40 minute; fiecare exercițiu se notează cu 2,25 puncte)

Indicați răspunsul corect.

1. Fie $F : \mathbb{R} \to \mathbb{R}$ o primitivă a funcției $f(x) = \sin x \cdot \cos^2 x$, $x \in \mathbb{R}$.

   Atunci $F(\pi) - F(0)$ este:

   a) π; b) 2π; c) 0; d) 1.

2. Integrala nedefinită a funcției $f : (-\infty; -1) \to \mathbb{R}$, $f(x) = \dfrac{1}{x\sqrt{x^2-1}}$ este:

   a) $\arcsin\dfrac{1}{x} + \mathscr{C}$; b) $\arccos\dfrac{1}{x} + \mathscr{C}$; c) $\ln\sqrt{x^2-1} + \mathscr{C}$; d) $\operatorname{arctg}\sqrt{x^2-1} + \mathscr{C}$.

3. Dacă $\int (ax+b) \cdot e^{-x} dx = (2x+3) \cdot e^{-x} + \mathscr{C}$, atunci $3a + 4b$ este:

   a) 8; b) 2; c) -10; d) 4.

4. Dacă $F : [-1, 1] \to \mathbb{R}$ este o primitivă a funcției $f(x) = \arcsin x$, atunci $F(1) - F(-1)$ este:

   a) 0; b) -1; c) 1; d) π.

Testul 2

(timp de lucru - 60 minute; fiecare exercițiu se notează cu 2,25 puncte)

Pentru următoarele probleme se cer soluții complete.

1. Să se calculeze integralele:

   a) $\int \dfrac{\ln^4 x}{x} dx$, $x \in (0, \infty)$; b) $\int (x^2 + x + 1)e^x dx$, $x \in \mathbb{R}$.

2. Considerăm funcțiile continue f, g : $\left(0, \dfrac{\pi}{2}\right) \to \mathbb{R}$, $f(x) = \dfrac{\sin x}{\sin x + \cos x}$ și $g(x) = \dfrac{\cos x}{\sin x + \cos x}$. Notăm $I = \int f(x)dx$ și $J = \int g(x)dx$. Să se calculeze $I + J$ și $I - J$ și apoi să se afle I și J.

3. Fie $f : \mathbb{R} \to (0, \infty)$ o funcție derivabilă cu derivata continuă.

   Să se calculeze: $\int \dfrac{f(x) + f'(x)}{f(x) + e^{-x}} dx$.

4. Să se determine o funcție polinomială $f : \mathbb{R} \to \mathbb{R}$, de gradul 3, știind că -1 și 2 sunt puncte de extrem și $f(0) = 4$, $f(1) = 1$.

INTEGRALA DEFINITĂ

Diviziuni, sisteme de puncte intermediare, sume Riemann, funcţii integrabile

În introducerea la partea a doua a acestui manual am văzut că în problema *determinării ariei trapezului curbiliniu* delimitat de graficul funcţiei continue şi pozitive $f : [a, b] \to \mathbb{R}$, axa OX şi dreptele de ecuaţii $x = a$, $x = b$, suntem conduşi la a considera suma:

$$\sigma = \sum_{i=1}^{n} f(x_i)(x_i - x_{i-1}) = \sum_{i=1}^{n} f(x_i)dx_i ,$$

unde $a = x_0 < x_1 < \ldots < x_n = b$, $dx_i = x_i - x_{i-1}$, $i = 1, 2, \ldots, n$, apoi limita acestei sume când $\max\limits_{1\le i\le n} dx_i \xrightarrow{n\to\infty} 0$.

Vom dezvolta acum riguros şi vom aprofunda această problematică. Înainte însă, reamintim *definiţia limitei* unei funcţii într-un punct, precum şi o *caracterizare* a limitei.

Definiţie

Spunem că funcţia $f : D\ (\subseteq \mathbb{R}) \to \mathbb{R}$ ***are limita ℓ când x tinde la x_0*** şi scriem $\lim\limits_{x\to x_0} f(x) = \ell$ dacă pentru orice şir $(a_n)_{n\ge1} \subseteq D \setminus \{ x_0 \}$ cu $\lim\limits_{n\to\infty} a_n = x_0$ rezultă $\lim\limits_{n\to\infty} f(a_n) = \ell$.

În definiţia anterioară $\ell \in \overline{\mathbb{R}}$, iar $x_0 \in \overline{\mathbb{R}}$ este un punct de acumulare pentru mulţimea D.

Teoremă (de caracterizare a limitei cu ε şi δ)

Pentru o funcţie $f : D \to \mathbb{R}$ următoarele afirmaţii sunt echivalente:

1°. $\lim\limits_{x\to x_0} f(x) = \ell$;

2°. $\forall\ \varepsilon > 0$, $\exists\ \delta_\varepsilon > 0$ astfel încât $\forall\ x \in D, x \neq x_0$, $|x - x_0| < \delta_\varepsilon \Rightarrow |f(x) - \ell| < \varepsilon$.

În teorema anterioară x_0 este un ***punct de acumulare finit*** pentru D, iar numărul ℓ este de asemenea ***finit***.

Introducem acum câteva concepte importante, culminând cu acela de ***integrală***. În tot ceea ce facem, lucrăm cu funcţii reale definite pe un *interval compact* (adică închis şi mărginit).

Definiție

Dacă $[a, b] \subseteq \mathbb{R}$ este un interval compact, numim ***diviziune*** a intervalului $[a, b]$ un sistem finit de puncte $\Delta = (a = x_0, x_1, x_2, \ldots, x_n = b)$ cu $x_{i-1} < x_i$, $i = 1, 2, \ldots, n$. Punctele x_i, $i = 0, 1, \ldots, n$ se numesc ***puncte de diviziune***, iar intervalele $[x_{i-1}, x_i]$, $i = 1, 2, \ldots, n$ se numesc ***intervale de diviziune***. Numărul pozitiv $dx_i = x_i - x_{i-1}$ este ***lungimea*** intervalului $[x_{i-1}, x_i]$, iar numărul pozitiv $\| \Delta \| = \max\limits_{1 \le i \le n} dx_i$ se numește ***norma*** diviziunii Δ.

Notație. Notăm cu $\mathscr{D}([a, b])$ mulțimea diviziunilor intervalului $[a, b]$.

Definiție

Dacă $\Delta = (a = x_0 < x_1 < x_2 < \ldots < x_n = b)$ este o diviziune a intervalului $[a, b]$, un sistem finit de puncte $\xi = (\xi_1, \xi_2, \ldots, \xi_n)$ cu proprietatea că $\xi_i \in [x_{i-1}, x_i]$, $i = 1, 2, \ldots, n$ se numește ***sistem de puncte intermediare*** asociat diviziunii Δ.

Definiție

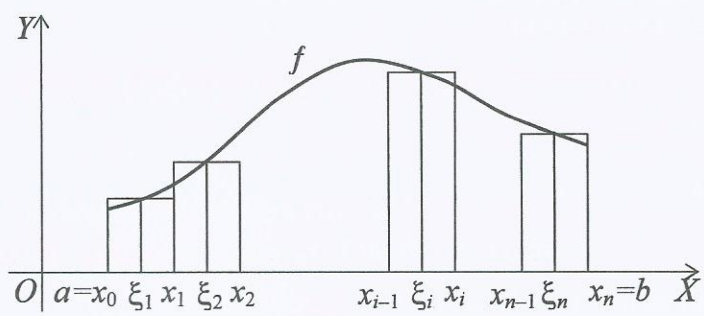
Fie $f : [a, b] \to \mathbb{R}$ o funcție, $\Delta = (a = x_0 < x_1 < x_2 < \ldots < x_n = b)$ o diviziune a intervalului $[a, b]$, iar $\xi = (\xi_1, \xi_2, \ldots, \xi_n)$ un sistem de puncte intermediare asociat diviziunii Δ. Numărul real definit prin:

$$\sigma(f, \Delta, \xi) = \sum_{i=1}^{n} f(\xi_i)(x_i - x_{i-1}) = \sum_{i=1}^{n} f(\xi_i) dx_i$$

se numește ***suma Riemann*** asociată funcției f, diviziunii Δ și sistemului de puncte intermediare ξ.

Interpretare geometrică

În cazul unei funcții continue și pozitive $f : [a, b] \to \mathbb{R}$ suma Riemann $\sigma(f, \Delta, \xi)$ este ***suma ariilor dreptunghiurilor*** având ca baze intervalele de diviziune $[x_{i-1}, x_i]$, iar ca înălțimi valorile $f(\xi_i)$, pentru $i = 1, 2, \ldots, n$.



Așadar suma Riemann $\sigma(f, \Delta, \xi)$ ***aproximează aria trapezului curbiliniu*** delimitat de graficul funcției f, axa OX și dreptele de ecuații $x = a$, $x = b$.

Observație importantă.

Pentru o funcție fixată f, suma Riemann $\sigma(f, \Delta, \xi)$ depinde de diviziunea Δ, deci implicit de norma $\| \Delta \|$ a acestei diviziuni, precum și de sistemul de puncte intermediare ξ. Totuși, în toate considerațiile care urmează, ***punctele intermediare pot fi alese oricum*** în intervalele de diviziune, ceea ce înseamnă că nu ne interesează cum depinde suma Riemann de sistemul de puncte intermediare ξ. Așadar, ***ne interesează cum depinde suma Riemann*** $\sigma(f, \Delta, \xi)$ ***doar de numărul pozitiv*** $\| \Delta \|$, adică, pe scurt gândim ca și cum $\sigma(f, \Delta, \xi)$ ***este o funcție de variabila*** $\| \Delta \|$.

Totuși, pentru a reliefa acest fapt vom adăuga în exprimări formularea „indiferent de alegerea sistemului de puncte intermediare".

Definiție importantă

Spunem că funcția $f : [a, b] \to \mathbb{R}$ este ***integrabilă Riemann*** (pe scurt, ***integrabilă***) pe intervalul $[a, b]$, dacă există și este finită limita:

$$I = \lim_{\|\Delta\| \to 0} \sigma(f, \Delta, \xi)$$

indiferent de alegerea sistemului de puncte intermediare ξ.

Această limită se numește ***integrala Riemann (integrala definită)*** a funcției f pe intervalul $[a, b]$ și se notează:

$$I = \int_a^b f(x)dx$$

(citim „integrală de la a la b din $f(x)dx$").

Ținând seama de definiția anterioară și cele două accepțiuni ale limitei unei funcții într-un punct pe care le-am reamintit, putem desprinde următoarele caracterizări ale funcțiilor integrabile:

Teoremă (de caracterizare a funcțiilor integrabile)

Pentru o funcție $f : [a, b] \to \mathbb{R}$, următoarele afirmații sunt echivalente:

1°. Funcția f este integrabilă și $\int_a^b f(x)dx = I$.

2°. $\forall \ (\Delta_n)_{n\geq 1} \subseteq \mathcal{D}(a, b])$ cu $\lim\limits_{n\to\infty} \|\Delta_n\| = 0$, rezultă $\lim\limits_{n\to\infty} \sigma(f, \Delta_n, \xi_n) = I$, indiferent de alegerea șirului de sisteme de puncte intermediare $(\xi_n)_{n\geq 1}$.

3°. $\forall \ \varepsilon > 0, \exists \ \delta_\varepsilon > 0$ astfel încât $\forall \ \Delta \in \mathcal{D}([a, b])$ cu $\| \Delta \| < \delta_\varepsilon$ rezultă $|\sigma(f, \Delta, \xi) - I| < \varepsilon$, indiferent de alegerea sistemului de puncte intermediare ξ.

Terminologie. Când scriem $\int_a^b f(x)dx$, numărul a se numește ***limita inferioară de integrare***, iar numărul b se numește ***limita superioară de integrare***.

Comentariu metodic

Numărul $\int_a^b f(x)dx$ este unic determinat pentru o funcţie integrabilă $f : [a, b] \to \mathbb{R}$, întrucât limita este unică. Acest număr depinde doar de funcţia f şi limitele de integrare a şi b şi nu depinde de variabila x. De aceea în loc de $\int_a^b f(x)dx$ putem scrie $\int_a^b f(t)dt$ sau $\int_a^b f(u)du$ etc.

Atragem atenţia asupra semnificaţiei conceptelor introduse: ***integrala definită*** (a unei funcţii integrabile pe un interval compact) este un ***număr real***, în timp ce ***integrala nedefinită*** (a unei funcţii cu primitive pe un interval oarecare) este o ***mulţime de funcţii*** (mulţimea primitivelor acestei funcţii). Aşadar, notaţiile asemănătoare $\int_a^b f(x)dx$ şi $\int f(x)dx$ au semnificaţii destul de „îndepărtate". Cu toate acestea, vom vedea că între conceptul de integrală definită şi noţiunea de primitivă există legături importante.

Mai remarcăm, de asemenea, că atunci când am studiat funcţiile care au primitive (primitivabile) a fost foarte uşor să dăm exemple de astfel de funcţii (e suficient să privim tabloul primitivelor imediate), în timp ce, definiţia mult mai complexă a noţiunii de funcţie integrabilă nu ne permite să dăm uşor exemple de astfel de funcţii.

De aceea, în secţiunea imediat următoare vom da un criteriu de integrabilitate (în fond, tot o caracterizare a funcţiilor integrabile) cu ajutorul căruia vom „găsi" clase întregi de funcţii integrabile (de exemplu, funcţiile continue şi funcţiile monotone).

Totuşi, un prim exemplu de funcţie integrabilă, obţinut doar pe baza definiţiei, este următorul:

Exemplu (de funcţie integrabilă)

Funcţia constantă $f : [a, b] \to \mathbb{R}$, $f(x) = \lambda$ este integrabilă Riemann şi integrala sa este:

$$\int_a^b \lambda \, dx = \lambda(b-a).$$

Într-adevăr, să considerăm o diviziune oarecare $\Delta = (a = x_0, x_1, x_2, \ldots, x_n = b)$ a intervalului $[a, b]$ şi un sistem arbitrar de puncte intermediare asociat $\xi = (\xi_1, \xi_2, \ldots, \xi_n)$ cu $\xi_i \in [x_{i-1}, x_i]$, $i = \overline{1, n}$. Suma Riemann corespunzătoare este:

$$\sigma(f, \Delta, \xi) = \sum_{i=1}^{n} f(\xi_i)(x_i - x_{i-1}) = \sum_{i=1}^{n} \lambda(x_i - x_{i-1}) = \lambda \sum_{i=1}^{n} (x_i - x_{i-1}) = \lambda(x_n - x_0) = \lambda(b-a),$$

ceea ce arată că această sumă este constantă (în sensul că nu depinde de diviziunea Δ şi nici de sistemul de puncte intermediare ξ). Prin urmare $\lim\limits_{\|\Delta\| \to 0} \sigma(f, \Delta, \xi) = \lambda(b-a)$, adică funcţia f este integrabilă, având integrala $\lambda(b-a)$.

Tot pe baza definiției putem face o constatare importantă, prin următoarea:

Propoziție

Modificarea valorilor unei funcții integrabile într-un număr finit de puncte, nu afectează integrabilitatea acesteia și nici valoarea integralei.

Demonstrație. Fie $f : [a, b] \to \mathbb{R}$ integrabilă și $g : [a, b] \to \mathbb{R}$, care diferă de f în punctele $\alpha_1, \ldots, \alpha_k \in [a, b]$. Notăm $M = \max\limits_{1 \le i \le k} |f(\alpha_i) - g(\alpha_i)|$. Atunci $\forall\, \Delta \in \mathscr{D}([a, b])$ și $\forall\, \xi$ un sistem de puncte intermediare asociat, vedem imediat că:

$$|\sigma(f, \Delta, \xi) - \sigma(g, \Delta, \xi)| \le \sum_{i=1}^{n} |f(\alpha_i) - g(\alpha_i)|\, dx_i \le kM\, \|\Delta\| \xrightarrow{\|\Delta\| \to 0} 0 .$$

Conform criteriului majorării, rezultă $\lim\limits_{\|\Delta\| \to 0} (\sigma(f, \Delta, \xi) - \sigma(g, \Delta, \xi)) = 0$, deci

$$\lim_{\|\Delta\| \to 0} \sigma(g, \Delta, \xi) = \lim_{\|\Delta\| \to 0} \sigma(f, \Delta, \xi) = \int_a^b f(x)dx .$$

Rezultă că funcția g este integrabilă și $\int_a^b g(x)dx = \int_a^b f(x)dx$.

Criteriul de integrabilitate al lui Darboux (extindere)

Vom demonstra acum o condiție necesară și suficientă ca o funcție mărginită să fie integrabilă. Cu ajutorul acesteia vom obține apoi suficiente exemple de funcții integrabile.

Avem nevoie mai întâi de o anumită pregătire.

Definiție

Dacă $f : [a, b] \to \mathbb{R}$ este o funcție mărginită, iar $\Delta = (a = x_0, x_1, x_2, \ldots, x_n = b)$ o diviziune a intervalului $[a, b]$ și dacă $m_i = \inf\limits_{x \in [x_{i-1}, x_i]} f(x)$, $M_i = \sup\limits_{x \in [x_{i-1}, x_i]} f(x)$, $i = \overline{1, n}$, atunci numerele reale definite prin:

$$s(f, \Delta) = \sum_{i=1}^{n} m_i (x_i - x_{i-1}) = \sum_{i=1}^{n} m_i dx_i , \quad S(f, \Delta) = \sum_{i=1}^{n} M_i (x_i - x_{i-1}) = \sum_{i=1}^{n} M_i dx_i$$

se numesc ***suma Darboux inferioară*** respectiv ***suma Darboux superioară*** asociate funcției f și diviziunii Δ.

Sunt imediate următoarele:

Observații

1) Cu notațiile din definiția precedentă, pentru orice sumă Riemann corespunzătoare diviziunii Δ şi unui sistem arbitrar ξ de puncte intermediare, avem inegalitățile:

$$s(f, \Delta) \leq \sigma(f, \Delta, \xi) \leq S(f, \Delta).$$

2) În cazul particular când f este o funcție continuă, conform teoremei lui Weierstrass avem $m_i = f(\xi_i')$, $M_i = f(\xi_i'')$ cu $\xi_i', \xi_i'' \in [x_{i-1}, x_i]$, $i = \overline{1, n}$, prin urmare $s(f, \Delta) = \sigma(f, \Delta, \xi')$ şi $S(f, \Delta) = \sigma(f, \Delta, \xi'')$ (aşadar, în cazul unei funcții continue, cele două sume Darboux sunt nişte sume Riemann).

Rezultatul de mai jos stabileşte proprietățile sumelor Darboux şi o legătură mai profundă a acestora cu sumele Riemann.

Lemă

1) Avem $s(f, \Delta) = \inf \{\sigma(f, \Delta, \xi)\}$, $S(f, \Delta) = \sup \{\sigma(f, \Delta, \xi)\}$, unde $\{\sigma(f, \Delta, \xi)\}$ este mulțimea tuturor sumelor Riemann corespunzătoare diviziunii Δ, când ξ parcurge toate sistemele de puncte intermediare asociate acestei diviziuni.

2) Pentru orice două diviziuni $\Delta, \Delta' \in \mathscr{D}([a, b])$ cu $\Delta \subseteq \Delta'$, avem: $s(f, \Delta) \leq$ $\leq s(f, \Delta')$ iar $S(f, \Delta) \geq S(f, \Delta')$ (aşadar, prin trecere de la o diviziune la una care o conține, sumele Darboux inferioare cresc, iar sumele Darboux superioare descresc).

3) Pentru orice două diviziuni $\Delta, \Delta' \in \mathscr{D}([a, b])$ avem $s(f, \Delta) \leq S(f, \Delta')$ (orice sumă Darboux inferioară este mai mică sau egală cu orice sumă Darboux superioară).

Demonstrație. 1) E clar că $s(f, \Delta)$ este un minorant pentru mulțimea $\{\sigma(f, \Delta, \xi)\}$, după cum rezultă din observația precedentă 1).

Dacă $\varepsilon > 0$ este oarecare, cum $m_i = \inf\limits_{x \in [x_{i-1}, x_i]} f(x)$ = cel mai mare minorant pentru mulțimea $f([x_{i-1}, x_i])$, înseamnă că $m_i + \dfrac{\varepsilon}{b-a}$ nu mai este minorant pentru această mulțime, prin urmare există $\xi_i \in [x_{i-1}, x_i]$ cu $f(\xi_i) < m_i + \dfrac{\varepsilon}{b-a}$, $i = \overline{1, n}$. Atunci pentru sistemul $\xi = (\xi_1, \xi_2, \ldots, \xi_n)$ avem:

$$\sigma(f, \Delta, \xi) = \sum_{i=1}^{n} f(\xi_i) dx_i < \sum_{i=1}^{n} \left(m_i + \frac{\varepsilon}{b-a} \right) dx_i =$$

$$= \sum_{i=1}^{n} m_i dx_i + \frac{\varepsilon}{b-a} \sum_{i=1}^{n} dx_i = s(f, \Delta) + \frac{\varepsilon}{b-a} \cdot (b-a) = s(f, \Delta) + \varepsilon.$$

Aceasta arată că numărul $s(f, \Delta) + \varepsilon$ nu mai este minorant pentru mulțimea $\{\sigma(f, \Delta, \xi)\}$, prin urmare $s(f, \Delta)$ este cel mai mare minorant pentru această mulțime, adică $s(f, \Delta) = \inf \{\sigma(f, \Delta, \xi)\}$. Analog se arată că $S(f, \Delta) = \sup \{\sigma(f, \Delta, \xi)\}$.

2) Este suficient să tratăm cazul când Δ' are în plus un singur punct de diviziune față de Δ (căci dacă Δ' are p puncte în plus față de Δ, aplicăm de p ori consecutiv cazul de mai înainte). Să presupunem aşadar că: $\Delta = (a = x_0, x_1, x_2, \ldots, x_{k-1}, x_k, \ldots, x_n = b)$,

$\Delta' = (a = x_0, x_1, x_2, \ldots, x_{k-1}, y, x_k, \ldots, x_n = b)$, unde $x_{k-1} < y < x_k$.

Fie $m_k' = \inf\limits_{x\in[x_{k-1}, y]} f(x)$, $m_k'' = \inf\limits_{x\in[y, x_k]} f(x)$. Avem evident $m_k' \geq \inf\limits_{x\in[x_{k-1}, x_k]} f(x) = m_k$ şi de asemenea $m_k'' \geq m_k$. Atunci $(y - x_{k-1})m_k' + (x_k - y)m_k'' \geq (y - x_{k-1})m_k + (x_k - y)m_k =$ $= (x_k - x_{k-1})m_k$. Prin urmare, putem scrie:

$$s(f, \Delta') = \sum_{\substack{i=1\\ i\neq k}}^{n} (x_i - x_{i-1})m_i + (y - x_{k-1})m_k' + (x_k - y)m_k'' \geq$$

$$\geq \sum_{\substack{i=1\\ i\neq k}}^{n} (x_i - x_{i-1})m_i + (x_k - x_{k-1})m_k = \sum_{i=1}^{n} (x_i - x_{i-1})m_i = s(f, \Delta).$$

Analog se arată că $S(f, \Delta') \leq S(f, \Delta)$.

3) Notând $\Delta'' = \Delta \cup \Delta'$, avem $\Delta \subseteq \Delta''$, $\Delta' \subseteq \Delta''$, deci conform cu cele deja stabilite, avem:

$$s(f, \Delta) \leq s(f, \Delta'') \leq S(f, \Delta'') \leq S(f, \Delta').$$

Să considerăm acum mulţimile de sume Darboux $\{s(f, \Delta) \mid \Delta \in \mathscr{D}([a, b])\}$ şi $\{S(f, \Delta) \mid \Delta \in \mathscr{D}([a, b])\}$. Prima mulţime are majoranţi, căci orice sumă Darboux superioară este un majorant pentru aceasta, iar a doua mulţime are minoranţi căci orice sumă Darboux inferioară este un minorant (am ţinut seama de punctul 3) din lemă). Putem vorbi atunci de două numere reale care sunt marginea superioară, respectiv marginea inferioară pentru cele două mulţimi de sume Darboux puse în evidenţă. Mai precis, avem următoarea:

Definiţie

Numerele reale definite prin:

$$I_* = \sup\{s(f, \Delta) \mid \Delta \in \mathscr{D}([a, b])\}$$
$$I^* = \inf\{S(f, \Delta) \mid \Delta \in \mathscr{D}([a, b])\}$$

se numesc ***integrala Darboux inferioară*** respectiv ***integrala Darboux superioară*** ale funcţiei f.

O proprietate simplă a celor două integrale Darboux este pusă în evidenţă de următoarea:

Lemă

Pentru fiecare diviziune $\Delta \in \mathscr{D}([a, b])$ avem inegalităţile:

$$s(f, \Delta) \leq I_* \leq I^* \leq S(f, \Delta).$$

Demonstraţie. Inegalităţile $s(f, \Delta) \leq I_*$ şi $I^* \leq S(f, \Delta)$ sunt evidente, în baza definiţiei celor două integrale Darboux. Să probăm inegalitatea $I_* \leq I^*$. Conform lemei precedente, fiecare sumă $s(f, \Delta)$ este un minorant pentru mulţimea $\{S(f, \Delta) \mid \Delta \in \mathscr{D}([a, b])\}$ şi cum I_* este cel mai mare minorant pentru această mulţime, deducem că

$s(f, \Delta) \le I^*$. Dar aceasta arată că numărul I^* este un majorant pentru mulţimea $\{s(f, \Delta) \mid \Delta \in \mathscr{D}([a, b])\}$ şi cum I_* este cel mic majorant pentru această mulţime, rezultă că $I_* \le I^*$.

După această pregătire, suntem în măsură să caracterizăm integrabilitatea funcţiilor mărginite prin următoarea:

Teoremă (Criteriul de integrabilitate Darboux)

Pentru o funcţie mărginită $f : [a, b] \to \mathbb{R}$, următoarele afirmaţii sunt echivalente:

1°. Funcţia f este integrabilă Riemann.

2°. $\forall\, \varepsilon > 0$, $\exists\, \delta_\varepsilon > 0$ astfel încât $\forall\, \Delta \in \mathscr{D}([a, b])$ cu $\| \Delta \| < \delta_\varepsilon$ rezultă $S(f, \Delta) - s(f, \Delta) < \varepsilon$ (echivalent spus, $\lim\limits_{\|\Delta\| \to 0} (S(f, \Delta) - s(f, \Delta)) = 0$).

Demonstraţie. 1° $\Rightarrow$ 2°. Presupunem că funcţia f este integrabilă şi fie $I = \int_a^b f(x)dx$. Fie $\varepsilon > 0$ ales arbitrar. Conform teoremei de caracterizare a funcţiilor integrabile, există $\delta_\varepsilon > 0$ astfel încât $\forall\, \Delta \in \mathscr{D}([a, b])$ cu $\| \Delta \| < \delta_\varepsilon$ avem $|\sigma(f, \Delta, \xi) - I| < \dfrac{\varepsilon}{2}$, indiferent de alegerea sistemului de puncte intermediare ξ. Pentru o asemenea diviziune Δ fixată, vom avea aşadar $I - \dfrac{\varepsilon}{2} < \sigma(f, \Delta, \xi) < I + \dfrac{\varepsilon}{2}$, pentru orice sistem de puncte intermediare ξ asociat diviziunii Δ. Rezultă că $I + \dfrac{\varepsilon}{2}$ este un majorant pentru mulţimea $\{\sigma(f, \Delta, \xi)\}$ când ξ parcurge toate sistemele de puncte intermediare. Cum $S(f, \Delta)$ este cel mai mic majorant pentru această mulţime (lema de la pag. 170, punctul 1), înseamnă că $S(f, \Delta) \le I + \dfrac{\varepsilon}{2}$, (1).

Analog, $I - \dfrac{\varepsilon}{2}$ este un minorant pentru mulţimea $\{\sigma(f, \Delta, \xi)\}$ şi cum $s(f, \Delta)$ este cel mai mare minorant pentru această mulţime, obţinem $I - \dfrac{\varepsilon}{2} \le s(f, \Delta)$, (2).

Atunci, pe baza lui (1) şi (2) avem: $S(f, \Delta) - s(f, \Delta) \le I + \dfrac{\varepsilon}{2} - \left(I - \dfrac{\varepsilon}{2}\right) = \varepsilon$.

2° $\Rightarrow$ 1°. Presupunem că $\forall\, \varepsilon > 0$, $\exists\, \delta_\varepsilon > 0$ astfel încât $\forall\, \Delta \in \mathscr{D}([a, b])$ cu $\| \Delta \| < \delta_\varepsilon$ rezultă $S(f, \Delta) - s(f, \Delta) < \varepsilon$. Conform ultimei leme, avem inegalitatea:

$$s(f, \Delta) \le I_* \le I^* \le S(f, \Delta) \tag{3}$$

de unde $0 \le I_* - I^* < \varepsilon$, pentru orice $\varepsilon > 0$. Rezultă în mod necesar $I_* = I^*$ şi fie I valoarea comună a celor două integrale Darboux, adică $I = I_* = I^*$. Inegalitatea (3) devine:

$$s(f, \Delta) \le I \le S(f, \Delta) \tag{4}$$

Conform cu observaţia 1 de la pag. 170 avem, pentru orice sistem ξ asociat lui Δ:

$$s(f, \Delta) \leq \sigma(f, \Delta, \xi) \leq S(f, \Delta). \tag{5}$$

Din (4) şi (5), folosind ipoteza în care lucrăm, rezultă:

$$\underline{|\sigma(f, \Delta, \xi) - I|} \leq S(f, \Delta) - s(f, \Delta) < \underline{\varepsilon}.$$

Textul subliniat arată, pe baza teoremei de caracterizare a funcţiilor integrabile, că funcţia f este integrabilă şi are integrala I.

Observaţie

Spre deosebire de teorema de la pag. 167, criteriul de integrabilitate al lui Darboux dă o caracterizare „intrinsecă" a funcţiilor integrabile, care nu face apel la valoarea integralei.

Integrabilitatea funcţiilor monotone şi a funcţiilor continue

Pe baza criteriului de integrabilitate al lui Darboux, vom arăta că funcţiile monotone şi funcţiile continue (definite pe un interval compact) sunt integrabile.

Teoremă

Dacă $f : [a, b] \to \mathbb{R}$ este o funcţie monotonă, atunci f este integrabilă pe $[a, b]$.

Demonstraţie. Fixând ideile, să zicem că f este crescătoare. Atunci $f(a) \leq f(x) \leq f(b)$, $\forall\, x \in [a, b]$, deci funcţia f este mărginită.

Dacă $f(a) = f(b)$, funcţia f este constantă şi am văzut că orice funcţie constantă este integrabilă. Să presupunem aşadar că $f(a) < f(b)$. Atunci, pentru orice $\varepsilon > 0$, luând, $\delta_\varepsilon = \dfrac{\varepsilon}{f(b) - f(a)} > 0$, avem pentru o diviziune oarecare $\Delta = (a = x_0, x_1, \ldots, x_n = b)$ cu $\| \Delta \| < \delta_\varepsilon$:

$$\underline{S(f, \Delta) - s(f, \Delta)} = \sum_{i=1}^{n} M_i \cdot dx_i - \sum_{i=1}^{n} m_i \cdot dx_i = \sum_{i=1}^{n} f(x_i) dx_i - \sum_{i=1}^{n} f(x_{i-1}) dx_i =$$

$$= \sum_{i=1}^{n} \left(f(x_i) - f(x_{i-1}) \right) dx_i < \| \Delta \| \sum_{i=1}^{n} \left(f(x_i) - f(x_{i-1}) \right) \leq \frac{\varepsilon}{f(b) - f(a)} \cdot \left(f(b) - f(a) \right) = \underline{\varepsilon}.$$

(Am ţinut seama şi de faptul că, deoarece funcţia f este crescătoare, avem $m_i = f(x_{i-1})$, $M_i = f(x_i)$, $i = \overline{1, n}$).

Textul subliniat arată că funcţia f satisface criteriul de integrabilitate al lui Darboux, prin urmare este o funcţie integrabilă.

Pentru a arăta că funcţiile continue sunt integrabile, probăm în prealabil următoarea:

Lemă

Dacă $f : [a, b] \to \mathbb{R}$ este o funcție continuă, atunci:
$\forall \varepsilon > 0, \exists \delta_\varepsilon > 0$ astfel încât $\forall x', x'' \in [a, b]$ cu $|x' - x''| < \delta_\varepsilon$ rezultă $|f(x') - f(x'')| < \varepsilon$.
(Se spune că funcția f este ***uniform continuă*** pe intervalul $[a, b]$).
Demonstrație. Presupunem prin absurd că $\exists\ \varepsilon_0 > 0$ astfel încât $\forall\ \delta > 0, \exists\ x'_\delta, x''_\delta \in [a,b]$ cu $|x'_\delta - x''_\delta| < \delta$, dar $|f(x'_\delta) - f(x''_\delta)| \geq \varepsilon_0$.

Să luăm $\delta_n = \frac{1}{n}$, pentru orice $n \in \mathbb{N}^*$. Atunci, $\forall\ n \in \mathbb{N}^*, \exists\ x'_n, x''_n \in [a, b]$ cu $|x'_n - x''_n| < \frac{1}{n}$, dar $|f(x'_n) - f(x''_n)| \geq \varepsilon_0$. Șirul mărginit $(x'_n)_{n\geq 1}$ conține un subșir convergent (lema lui Cesaro) și, pentru a nu complica notația, vom admite că însuși șirul $(x'_n)_{n\geq 1}$ este convergent. Notând $x = \lim\limits_{n\to\infty} x'_n$, rezultă că $x \in [a, b]$.

Din $|x'_n - x''_n| < \frac{1}{n}, \forall\ n \in \mathbb{N}^*$ rezultă că $\lim\limits_{n\to\infty}(x'_n - x''_n) = 0$ și de aici, rezultă mai departe că $\lim\limits_{n\to\infty} x''_n = x$. Deoarece funcția f este continuă în punctul $x \in [a, b]$, rezultă $\lim\limits_{n\to\infty} f(x'_n) = f(x)$ și $\lim\limits_{n\to\infty} f(x''_n) = f(x)$. De aici: $\lim\limits_{n\to\infty}\left(f(x'_n) - f(x''_n)\right) = f(x) - f(x) = 0$, în contradicție cu faptul că $|f(x'_n) - f(x''_n)| \geq \varepsilon_0, \forall\ n \in \mathbb{N}^*$.

Teoremă

Dacă $f : [a, b] \to \mathbb{R}$ este funcție continuă, atunci f este integrabilă pe $[a, b]$.

Demonstrație. Conform teoremei lui Weierstrass, funcția f este mărginită.
Arătăm că f satisface criteriul de integrabilitate al lui Darboux.
Fie $\varepsilon > 0$ oarecare. Conform ultimei leme, $\exists\ \delta_\varepsilon > 0$ astfel încât $\forall\ x', x'' \in [a, b]$ cu $|x' - x''| < \delta_\varepsilon$, rezultă $|f(x') - f(x'')| < \frac{\varepsilon}{b - a}$.
Fie $\Delta = (a = x_0, x_1, x_2, \ldots, x_n = b)$ o diviziune oarecare cu $\| \Delta \| < \delta_\varepsilon$.
Tot din teorema lui Weierstrass, avem:

$$m_i = \inf_{x\in[x_{i-1}, x_i]} f(x) = f(\xi'_i),\quad M_i = \sup_{x\in[x_{i-1}, x_i]} f(x) = f(\xi''_i),$$

unde $\xi'_i, \xi''_i \in [x_{i-1}, x_i]$, $i = \overline{1, n}$.

Atunci $|\xi'_i - \xi''_i| \leq x_i - x_{i-1} = dx_i \leq \| \Delta \| < \delta_\varepsilon$, deci $|f(\xi'_i) - f(\xi''_i)| < \frac{\varepsilon}{b - a}$, adică $M_i - m_i < \frac{\varepsilon}{b - a}$, $i = \overline{1, n}$. Prin urmare:

$$\underline{S(f, \Delta) - s(f, \Delta)} = \sum_{i=1}^{n} M_i \cdot dx_i - \sum_{i=1}^{n} m_i \cdot dx_i = \sum_{i=1}^{n} (M_i - m_i) dx_i <$$

$$< \frac{\varepsilon}{b-a} \cdot \sum_{i=1}^{n} dx_i = \frac{\varepsilon}{b-a} \cdot (b-a) = \underline{\varepsilon}.$$

Textul subliniat arată că funcţia f satisface criteriul de integrabilitate al lui Darboux, prin urmare este o funcţie integrabilă.

Formula Leibniz – Newton (formula fundamentală din calculul integral)

După ce am constatat că există „suficient de multe" funcţii integrabile, vom arăta o metodă foarte simplă pentru calculul integralei. Această metodă este valabilă pentru o clasă largă de funcţii şi stabileşte o legătură între integrala Riemann (integrala definită) şi noţiunea de primitivă a unei funcţii.

Teoremă

Dacă $f : [a, b] \to \mathbb{R}$ este o funcţie integrabilă care are primitive, integrala sa este dată de egalitatea:

$$\int_a^b f(x)dx = F(b) - F(a)$$

unde F este o primitivă fixată a funcţiei f.

Această egalitate se numeşte ***formula Leibniz – Newton***.

Demonstraţie. Considerăm o diviziune oarecare $\Delta = (a = x_0, x_1, x_2, \ldots, x_n = b)$ a intervalului $[a, b]$. Aplicăm teorema lui Lagrange (teorema creşterilor finite) primitivei F pe fiecare din intervalele de diviziune $[x_{i-1}, x_i]$, $i = \overline{1, n}$. Prin urmare $\exists \xi_i \in (x_{i-1}, x_i)$ cu proprietatea

$$F(x_i) - F(x_{i-1}) = F'(\xi_i)(x_i - x_{i-1}), \text{ adică } F(x_i) - F(x_{i-1}) = f(\xi_i)(x_i - x_{i-1}). \qquad (1)$$

Pentru sistemul de puncte intermediare pus în evidenţă $\xi = (\xi_1, \xi_2, \ldots, \xi_n)$, suma Riemann corespunzătoare este:

$$\sigma(f, \Delta, \xi) = \sum_{i=1}^{n} f(\xi_i)(x_i - x_{i-1}) \overset{(1)}{=} \sum_{i=1}^{n} (F(x_i) - F(x_{i-1})) = F(x_n) - F(x_0) = F(b) - F(a)$$

deci este constantă (nu depinde de diviziunea Δ).

Deoarece funcţia f este integrabilă, avem $\lim\limits_{\|\Delta\| \to 0} \sigma(f, \Delta, \xi) = \int_a^b f(x)dx$.

Atunci, trecând la limită când $\|\Delta\| \to 0$ în egalitatea $\sigma(f, \Delta, \xi) = F(b) - F(a)$, obținem $\int_a^b f(x)dx = F(b) - F(a)$.

Observație.

De obicei se notează $F(b) - F(a) = F(x)\Big|_a^b$ (se citește „$F(x)$ luat de la a la b") și atunci formula Leibniz – Newton se mai poate scrie sub forma:

$$\int_a^b f(x)dx = F(x)\Big|_a^b.$$

Exercițiu rezolvat

Să se calculeze integralele:

a) $\int_0^1 x^3 dx$; **b)** $\int_2^{2\sqrt{3}} \frac{dx}{x^2+4}$.

Soluție. **a)** Aplicăm formula Leibniz – Newton și avem: $\int_0^1 x^3 dx = \frac{x^4}{4}\Big|_0^1 = \frac{1}{4}$.

b) La fel, aplicăm formula Leibniz – Newton:

$$\int_2^{2\sqrt{3}} \frac{dx}{x^2+4} = \frac{1}{2}\operatorname{arctg}\frac{x}{2}\Big|_2^{2\sqrt{3}} = \frac{1}{2}\operatorname{arctg}\sqrt{3} - \frac{1}{2}\operatorname{arctg} 1 = \frac{1}{2}\left(\frac{\pi}{3} - \frac{\pi}{4}\right) = \frac{\pi}{24}.$$

EXERCIȚII PROPUSE

I. Considerăm o funcție $f : [0, 1] \to \mathbb{R}$ și notăm cu Δ_n diviziunea care împarte intervalul $[0, 1]$ în n părți egale, iar cu ξ_n sistemul de puncte intermediare format cu extremitățile din dreapta ale intervalelor diviziunii Δ_n, $n \in \mathbb{N}^*$. Calculați:

1. $\|\Delta_n\|$ și $\lim\limits_{n\to\infty} \|\Delta_n\|$.

2. $\sigma(f, \Delta_n, \xi_n)$ și $\lim\limits_{n\to\infty} \sigma(f, \Delta_n, \xi_n)$ pentru fiecare din funcțiile:

a) $f(x) = x$;
b) $f(x) = e^x$.

II. Utilizând formula Leibniz – Newton, calculați integralele:

1. $\int_0^1 x\,dx$ (comparați cu ex. 2,a) din setul I);

2. $\int_2^3 x^2dx$;

3. $\int_{-1}^2 (x^2+2x+1)dx$;

4. $\int_0^1 e^x dx$ (comparați cu ex.2 b) din setul I);

5. $\int_1^e \frac{dx}{x}$;

6. $\int_{\frac{\pi}{6}}^{\frac{\pi}{2}} \cos x\,dx$;

7. $\int_{\frac{\pi}{4}}^{\frac{\pi}{3}} \frac{dx}{\sin^2 x}$;

8. $\int_{-1}^{\frac{\sqrt{3}}{2}} \frac{dx}{\sqrt{1-x^2}}$;

9. $\int_0^1 \frac{dx}{1+x^2}$;

10. $\int_1^3 x^4dx$;

11. $\int_{\frac{1}{2}}^1 \frac{dx}{x^3}$;

12. $\int_1^8 \sqrt[3]{x}\,dx$;

13. $\int_1^9 \frac{x-1}{\sqrt{x}}dx$;

14. $\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} (\cos x - \sin x)dx$;

15. $\int_{\frac{\pi}{6}}^{\frac{\pi}{3}} \left(\frac{1}{\cos^2 x} - \frac{1}{\sin^2 x}\right)dx$;

16. $\int_{\sqrt{2}}^{\sqrt{3}} \frac{dx}{\sqrt{4-x^2}}$;

17. $\int_5^{5\sqrt{3}} \frac{dx}{25+x^2}$;

18. $\int_0^{\sqrt{2}} \frac{dx}{\sqrt{2+x^2}}$;

19. $\int_2^3 \frac{1}{x^2-1}$;

20. $\int_0^{\frac{1}{2}} \frac{dx}{4x^2+1}$.

Liniaritatea integralei, aditivitatea integralei în raport cu intervalul de integrare

Studiem în continuare două proprietăți importante ale integralei, care vor fi deosebit de utile în calculul efectiv al integralelor definite.

Prima dintre ele este analoagă proprietății din observația de la pag. 153, care se referea la integrala nedefinită. Este vorba de următoarea:

Teoremă

Fie $f, g : [a, b] \to \mathbb{R}$, funcții integrabile și $\lambda \in \mathbb{R}$. Atunci:

1) Funcția $f + g$ este integrabilă și $\int_a^b \big(f(x)+g(x)\big)dx = \int_a^b f(x)dx + \int_a^b g(x)dx$

(integrala sumei este egală cu suma integralelor).

2) Funcţia λf este integrabilă şi $\int_a^b \lambda f(x)dx = \lambda\int_a^b f(x)dx$

(o constantă multiplicativă iese în faţa integralei).

Demonstraţie. **1)** Pentru o diviziune arbitrară $\Delta = (a = x_0, x_1, \ldots, x_n = b)$ a intervalului $[a, b]$ şi un sistem de puncte intermediare arbitrar $\xi = (\xi_1, \xi_2, \ldots, \xi_n)$ asociat diviziunii Δ, suma Riemann corespunzătoare funcţiei $f + g$ este:

$$\sigma(f+g, \Delta, \xi) = \sum_{i=1}^{n}(f+g)(\xi_i)dx_i = \sum_{i=1}^{n}\left(f(\xi_i)+g(\xi_i)\right)dx_i =$$

$$= \sum_{i=1}^{n} f(\xi_i)dx_i + \sum_{i=1}^{n} g(\xi_i)dx_i = \sigma(f, \Delta, \xi) + \sigma(g, \Delta, \xi).$$

Rezultă că:

$$\lim_{\|\Delta\|\to 0}\sigma(f+g, \Delta, \xi) = \lim_{\|\Delta\|\to 0}\sigma(f, \Delta, \xi) + \lim_{\|\Delta\|\to 0}\sigma(g, \Delta, \xi),$$

adică integrala funcţiei $f + g$ pe intervalul $[a, b]$ există şi este dată de egalitatea:

$$\int_a^b \left(f(x)+g(x)\right)dx = \int_a^b f(x)dx + \int_a^b g(x)dx.$$

2) Analog.

Observaţie. Proprietatea **1)** din teorema precedentă se exprimă în cuvinte prin aceea că integrala este ***aditivă*** (în raport cu „integrandul", adică funcţia de sub integrală) proprietatea **2)** prin aceea că integrala este ***omogenă***, iar împreună **1)** şi **2)** se exprimă prin aceea că integrala este ***liniară***.

Cea de-a doua proprietate la care facem referinţă este dată de următoarea:

Teoremă

Fie $f : [a, b] \to \mathbb{R}$ o funcţie şi $c \in (a, b)$. Funcţia f este integrabilă pe $[a, b]$ dacă şi numai dacă este integrabilă pe $[a, c]$ şi pe $[c, b]$, caz în care avem egalitatea:

$$\int_a^b f(x)dx = \int_a^c f(x)dx + \int_c^b f(x)dx.$$

Demonstraţie. Presupunem că funcţia f este integrabilă pe $[a, b]$. Vom arăta un rezultat mai general şi anume că f este integrabilă pe orice interval $[\alpha, \beta] \subseteq [a, b]$, de unde va rezulta că este integrabilă pe $[a, c]$ şi pe $[c, b]$.

Conform criteriului de integrabilitate al lui Darboux, avem:

$$\forall\ \varepsilon > 0,\ \exists\ \delta_\varepsilon > 0 \text{ astfel încât } \forall\ \Delta \in \mathscr{D}([a, b]) \text{ cu } \|\Delta\| < \delta_\varepsilon \Rightarrow S(f, \Delta) - s(f, \Delta) < \varepsilon.$$

Pentru $\varepsilon > 0$ oarecare, fie $\Delta' \in \mathscr{D}([\alpha, \beta])$ o diviziune arbitrară a intervalului $[\alpha, \beta]$ cu $\|\Delta'\| < \delta_\varepsilon$, unde δ_ε este cel din criteriul lui Darboux.

Completăm diviziunea Δ' până la o diviziune Δ a intervalului $[a, b]$ în care α şi β sunt puncte de diviziune şi astfel încât $\| \Delta \| \le \| \Delta' \| < \delta_\varepsilon$.

Să zicem că $\Delta = (a = x_0, x_1, x_2, \ldots, x_k = \alpha, x_{k+1}, \ldots, x_p = \beta, x_{p+1}, \ldots, x_n = b)$.

Cu notaţiile cunoscute avem:

$$S(f, \Delta') - s(f, \Delta') = \sum_{i=k+1}^{p} (M_i - m_i)dx_i \le \sum_{i=1}^{n} (M_i - m_i)dx_i = S(f, \Delta) - s(f, \Delta) < \varepsilon.$$

Conform criteriului lui Darboux, funcţia f este integrabilă pe $[\alpha, \beta]$.

Invers, să presupunem că funcţia f este integrabilă pe $[a, c]$ şi $[c, b]$ şi să arătăm că este integrabilă pe $[a, b]$. Conform criteriului lui Darboux, $\forall\ \varepsilon > 0$, $\exists\ \delta'_\varepsilon > 0$, $\delta''_\varepsilon > 0$ astfel încât $\forall\ \Delta' \in \mathscr{D}([a, c])$ cu $\| \Delta' \| < \delta'_\varepsilon$ şi $\forall\ \Delta'' \in \mathscr{D}([c, b])$ cu $\| \Delta'' \| < \delta''_\varepsilon$ avem $S(f, \Delta') - s(f, \Delta') < \dfrac{\varepsilon}{2}$ şi $S(f, \Delta'') - s(f, \Delta'') < \dfrac{\varepsilon}{2}$.

Luăm $\delta_\varepsilon = \min(\delta'_\varepsilon, \delta''_\varepsilon)$ şi fie $\Delta = \mathscr{D}([a, b])$ cu $\| \Delta \| < \delta_\varepsilon$. Notăm cu Δ' diviziunea formată din toate punctele lui Δ situate în $[a, c]$ la care adăugăm punctul c şi cu Δ'' diviziunea formată din toate punctele lui Δ situate în $[c, b]$ la care adăugăm de asemenea punctul c. În felul acesta $\Delta' \in \mathscr{D}([a, c])$, iar $\Delta'' \in \mathscr{D}([c, b])$ şi avem $\Delta \subseteq \Delta' \cup \Delta''$, $\| \Delta' \| \le \| \Delta \| < \delta_\varepsilon \le \delta'_\varepsilon$, $\| \Delta'' \| \le \| \Delta \| < \delta_\varepsilon \le \delta''_\varepsilon$. Cum termenii de forma $(M_i - m_i)dx_i$ sunt pozitivi, putem scrie:

$$S(f, \Delta) - s(f, \Delta) \le S(f, \Delta' \cup \Delta'') - s(f, \Delta' \cup \Delta'') =$$

$$= [S(f, \Delta') - s(f, \Delta')] + [S(f, \Delta'') - s(f, \Delta'')] < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Conform criteriului lui Darboux, funcţia f este integrabilă pe $[a, b]$.

Probăm în fine, egalitatea din enunţ. Fie Δ' o diviziune oarecare a lui $[a, c]$, Δ'' o diviziune oarecare a lui $[b, c]$, iar $\Delta = \Delta' \cup \Delta''$ care este o diviziune a lui $[a, b]$. Dacă ξ' este un sistem de puncte intermediare pentru Δ', ξ'' un sistem de puncte intermediare pentru Δ'', atunci $\xi = \xi' \cup \xi''$ este un sistem de puncte intermediare pentru Δ şi avem evident:

$$\sigma(f, \Delta', \xi') + \sigma(f, \Delta'', \xi'') = \sigma(f, \Delta, \xi). \qquad (1)$$

Când $\| \Delta' \| \to 0$ şi $\| \Delta'' \| \to 0$, cum $\| \Delta \| = \max(\| \Delta' \|, \| \Delta'' \|)$ rezultă că $\| \Delta \| \to 0$; prin urmare, trecând la limită în (1) când $\| \Delta' \| \to 0$ şi $\| \Delta'' \| \to 0$, obţinem:

$$\lim_{\|\Delta'\|\to 0} \sigma(f, \Delta', \xi') + \lim_{\|\Delta''\|\to 0} \sigma(f, \Delta'', \xi'') = \lim_{\|\Delta\|\to 0} \sigma(f, \Delta, \xi),$$

adică

$$\int_a^c f(x)dx + \int_c^b f(x)dx = \int_a^b f(x)dx.$$

Observaţie. Egalitatea din teorema precedentă se exprimă în cuvinte prin aceea că integrala este ***aditivă*** în raport cu intervalul de integrare.

Vom vedea acum că „ordonarea" $a < c < b$ din teorema precedentă nu este esenţială. Pentru aceasta, dăm mai întâi următoarea:

Convenție: Fie $f : I \to \mathbb{R}$ (I interval) o funcție care este integrabilă pe orice subinterval compact al lui I. Pentru orice $a,b \in I$, $a < b$, definim:

$$\int_a^a f(x)dx = 0 \quad (1) \quad \text{şi} \int_b^a f(x)dx = -\int_a^b f(x)dx \quad (2).$$

Avem atunci următoarea:

Consecință

Fie $f : I \to \mathbb{R}$ (I interval) o funcție care este integrabilă pe orice subinterval compact al lui I. Atunci, pentru orice $a,b,c \in I$ avem:

$$\int_a^b f(x)dx = \int_a^c f(x)dx + \int_c^b f(x)dx.$$

Demonstrație. Ordonarea $a < c < b$ a fost tratată în teoremă. Să considerăm acum o altă ordonare, de exemplu $b < a < c$. Conform teoremei avem:

$$\int_b^c f(x)dx = \int_b^a f(x)dx + \int_a^c f(x)dx.$$

Folosind (2) din convenția făcută, această egalitate se mai scrie:

$$-\int_c^b f(x)dx = -\int_a^b f(x)dx + \int_a^c f(x)dx \text{ sau } \int_a^b f(x)dx = \int_a^c f(x)dx + \int_c^b f(x)dx.$$

Orice altă ordonare a numerelor a, b, c (inclusiv cazurile când cel puțin două din aceste numere sunt egale) se tratează analog.

Exercițiu rezolvat

Să se calculeze: $\int_{-1}^{1} |x|\, dx$.

Soluție. Utilizăm aditivitatea integralei față de interval și avem:

$$\int_{-1}^{1} |x|\, dx = \int_{-1}^{0} (-x)dx + \int_0^1 x\, dx = -\frac{x^2}{2}\bigg|_{-1}^{0} + \frac{x^2}{2}\bigg|_0^1 = 0 - \left(-\frac{1}{2}\right) + \frac{1}{2} - 0 = 1.$$

Monotonia integralei, teorema de medie, primitivabilitatea funcțiilor continue

Demonstrăm mai întâi următorul rezultat preliminar, care reprezintă o condiție necesară de integrabilitate.

Teoremă

Dacă funcţia $f : [a, b] \to \mathbb{R}$ este integrabilă, atunci f este mărginită.

Demonstraţie. Presupunem prin absurd că f este nemărginită. Arătăm că în această ipoteză, dacă fixăm un $M > 0$, atunci pentru orice diviziune $\Delta \in \mathscr{D}([a, b])$, există un sistem de puncte intermediare ξ, astfel încât $|\sigma(f, \Delta, \xi)| > M$. Fie, într-adevăr, $\Delta = (a = x_0, x_1, \ldots, x_n = b)$; deoarece f este nemărginită pe $[a, b]$, rezultă că f este nemărginită pe cel puţin unul din intervalele de diviziune, să zicem $[x_{j-1}, x_j]$.

Atunci, notând $S = \sum_{\substack{i=1 \\ i \neq j}}^{n} f(x_i) dx_i$, există un $\xi_j \in [x_{j-1}, x_j]$ astfel încât

$$|f(\xi_j)| > \frac{M + |S|}{dx_j} \tag{1}$$

Considerăm sistemul de puncte intermediare $\xi = (x_1, x_2 \ldots, x_{j-1}, \xi_j, x_{j+1} \ldots, x_n)$, pentru care suma Riemann corespunzătoare este $\sigma(f, \Delta, \xi) = f(\xi_j) dx_j + S$.

Trecând la module şi ţinând seama de inegalitatea $|a - b| \geq |a| - |b|$ şi de (1) obţinem:

$$|\sigma(f, \Delta, \xi)| \geq |f(\xi_j)|\, dx_j - |S| > M, \text{ adică } |\sigma(f, \Delta, \xi)| > M. \tag{2}$$

Fixăm un $M > |I|$, unde I este integrala funcţiei f şi trecem la limită în (2) când $\|\Delta\| \to 0$. Obţinem:

$$|I| = \left| \lim_{\|\Delta\| \to 0} \sigma(f, \Delta, \xi) \right| = \lim_{\|\Delta\| \to 0} |\sigma(f, \Delta, \xi)| \geq M > |I|, \text{ contradicţie.}$$

Observaţie. Rezultă imediat că orice funcţie nemărginită (definită pe un interval compact) nu este integrabilă Riemann.

Comentariu metodic

Deoarece toate funcţiile integrabile sunt mărginite, deducem că ipoteza de mărginire, care figurează în criteriul de integrabilitate al lui Darboux, nu este deloc restrictivă. Mai precis, funcţiile integrabile mărginite (caracterizate prin criteriul lui Darboux) epuizează *toate* funcţiile integrabile.

Rezultatul de mai jos arată că într-o inegalitate „se poate integra", adică altfel spus, „integrala este monoton crescătoare".

Propoziţie

Dacă $f, g : [a, b] \to \mathbb{R}$ sunt funcţii integrabile, astfel încât $f(x) \leq g(x)$, $\forall x \in [a, b]$, atunci $\int_a^b f(x)dx \leq \int_a^b g(x)dx$.

Demonstrație. Pentru orice diviziune $\Delta \in \mathscr{D}([a, b])$ și orice sistem de puncte intermediare asociat ξ, avem $\sigma(f, \Delta, \xi) = \sum_{i=1}^{n} f(\xi_i)dx_i \leq \sum_{i=1}^{n} g(\xi_i)dx_i = \sigma(g, \Delta, \xi)$.

Trecând la limită, când $\| \Delta \| \to 0$, obținem:

$$\lim_{\|\Delta\|\to 0} \sigma(f, \Delta, \xi) \leq \lim_{\|\Delta\|\to 0} \sigma(g, \Delta, \xi), \text{ adică } \int_a^b f(x)dx \leq \int_a^b g(x)dx.$$

Consecință

Dacă $f : [a, b] \to \mathbb{R}$ este o funcție integrabilă și considerăm numerele reale $m = \inf_{x\in[a, b]} f(x)$, $M = \sup_{x\in[a, b]} f(x)$, atunci:

$$m(b-a) \leq \int_a^b f(x)dx \leq M(b-a).$$

Demonstrație. Avem $m \leq f(x) \leq M$, pentru orice $x \in [a, b]$. Integrând obținem:

$$\int_a^b m\, dx \leq \int_a^b f(x)dx \leq \int_a^b M\, dx \quad \text{adică} \quad mx\Big|_a^b \leq \int_a^b f(x)dx \leq Mx\Big|_a^b$$

sau, în definitiv:

$$m(b-a) \leq \int_a^b f(x)dx \leq M(b-a).$$

Înainte de a demonstra un rezultat important, definim noțiunea de medie a unei funcții integrabile pe un interval compact. Avem în acest sens următoarea:

Definiție

Dacă $f : [a, b] \to \mathbb{R}$ este o funcție integrabilă, numărul real:

$$M(f) = \frac{1}{b-a}\int_a^b f(x)dx$$

se numește ***media integrală*** (pe scurt, ***media***) funcției f pe intervalul $[a, b]$.

Teoremă (de medie)

Fie $f : [a, b] \to \mathbb{R}$ o funcție integrabilă și $m = \inf_{x\in[a, b]} f(x)$, $M = \sup_{x\in[a, b]} f(x)$.

Atunci:

1°. Există $\mu \in [m, M]$ astfel încât $\int_a^b f(x)dx = (b-a)\mu$, adică $M(f) = \mu \in [m, M]$.

2°. Dacă, în plus, f este continuă, există $c \in [a, b]$ astfel încât
$\int_a^b f(x)dx = (b-a)f(c)$, adică $M(f) = f(c)$, cu $c \in [a, b]$.

Demonstrație. 1°. Conform consecinței precedente avem $m(b-a) \leq \int_a^b f(x)dx \leq M(b-a)$

și notând $\frac{1}{b-a}\int_a^b f(x)dx = \mu$, rezultă $\mu \in [m, M]$.

2°. Dacă f este continuă, conform teoremei lui Weierstrass, marginile m și M ale funcției f sunt valori ale acesteia în anumite puncte. Deoarece $f([a, b])$ este un interval, rezultă imediat egalitatea $[m, M] = f([a, b])$ și prin urmare $\mu \in [m, M]$ este de forma $\mu = f(c)$, cu $c \in [a, b]$. Obținem:

$$\int_a^b f(x)dx = (b-a)\mu = (b-a)f(c).$$

În ultimul capitol vom da o *interpretare geometrică pentru punctul 2° din teorema de medie*.

Revenim acum la funcția numită ***funcția – arie***.

Relativ la această funcție, am probat – pe baza unor considerente intuitive – că este primitiva unei funcții continue date.

Vom arăta acum în mod riguros că funcțiile continue au primitive.

Avem în acest sens următorul rezultat important:

Teoremă

Fie $I \subseteq \mathbb{R}$ un interval și $f : I \to \mathbb{R}$ o funcție integrabilă pe orice interval compact inclus în I. Fixăm un $a \in I$ și definim funcția:

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

Atunci:

1°. Funcția F este continuă pe I.

2°. Dacă în plus, f este continuă, rezultă că funcția F este derivabilă pe I și $F' = f$ (așadar, ***funcția continuă f are primitive*** și o primitivă a sa este funcția F).

Demonstrație. 1°. Fixăm un $t_0 \in I$ și fie $[\alpha, \beta]$ un interval compact, fixat, inclus în I și care conține punctul t_0. Atunci, pentru orice $t \in [\alpha, \beta]$, utilizând aditivitatea integralei în raport cu intervalul și punctul 1° din teorema de medie, avem:

$$F(t) - F(t_0) = \int_a^t f(x)dx - \int_a^{t_0} f(x)dx = \int_{t_0}^t f(x)dx = (t-t_0)\mu_t \qquad (1)$$

unde μ_t este cuprins între marginile funcției f pe intervalul de capete t_0 și t. Atunci μ_t este, cu atât mai mult, cuprins între marginile funcției f pe intervalul $[\alpha, \beta]$, deci există $M > 0$ astfel ca $|\mu_t| \leq M$, pentru orice $t \in [\alpha, \beta]$.

Trecând la module în (1), obținem: $|F(t) - F(t_0)| = |t - t_0| \cdot |\mu_t| \leq M|t - t_0|$ de unde, conform criteriului majorării, $\lim\limits_{t \to t_0} F(t) = F(t_0)$.

Aşadar funcţia F este continuă în punctul t_0 şi cum $t_0 \in I$ este arbitrar, deducem că F este continuă pe I.

2°. Fixăm un $t_0 \in I$. Pentru orice $t \in I$, $t \neq t_0$, conform cu punctul 2° din teorema de medie, avem:

$$\frac{F(t)-F(t_0)}{t-t_0}=\frac{\int_a^t f(x)dx-\int_a^{t_0} f(x)dx}{t-t_0}=\frac{\int_{t_0}^t f(x)dx}{t-t_0}=f(c_t) \qquad (2)$$

unde c_t este cuprins între t_0 şi t. Când $t \to t_0$, rezultă $c_t \to t_0$ şi deoarece f este continuă, rezultă $f(c_t) \to f(t_0)$.

Prin urmare, trecând în (2) la limită când $t \to t_0$, obţinem:

$$\lim_{t\to t_0}\frac{F(t)-F(t_0)}{t-t_0}=f(t_0),\text{ adică } F'(t_0)=f(t_0).$$

Cum $t_0 \in I$ este arbitrar, deducem că $F' = f$.

Observaţie

Deoarece funcţiile continue sunt integrabile şi primitivabile, deducem că formula Leibniz–Newton este valabilă pentru orice funcţie continuă $f : [a, b] \to \mathbb{R}$.

Comentariu metodic

Punctul 2° al teoremei precedente, arată că pentru o funcţie continuă $f : I \to \mathbb{R}$, avem egalitatea:

$$\frac{d}{dt}\left(\int_a^t f(x)dx\right)=f(t)$$

care se traduce în cuvinte astfel: dacă derivăm o integrală (cu limita inferioară de integrare constantă, iar limita superioară de integrare variabilă) în raport cu limita superioară de integrare, obţinem valoarea funcţiei de sub integrală calculată în această limită superioară de integrare.

Mult timp, aşa cum am mai spus, integrala $\int_a^t f(x)dx$ s-a numit ***integrala nedefinită*** a funcţiei continue f, tocmai pentru faptul că limita superioară de integrare este variabilă (nedefinită). Întrucât această integrală este o primitivă a funcţiei continue f, denumirea s-a extins asupra tuturor primitivelor, ajungându-se la sensul actual al termenului: ***integrala nedefinită*** este mulţimea tuturor primitivelor.

De asemenea, să remarcăm faptul că, acum, când ştim că funcţiile continue au primitive, putem „regăsi" punctul 2° din teorema de medie, aplicând teorema lui Lagrange unei primitive a funcţiei continue f şi utilizând apoi formula Leibniz-Newton. Într-adevăr, dacă $F : [a, b] \to \mathbb{R}$ este o primitivă a funcţiei continue $f : [a, b] \to \mathbb{R}$, din teorema lui Lagrange există $c \in (a, b)$ astfel încât $F(b) - F(a) = (b - a)f(c)$, adică, datorită formulei Leibniz-Newton: $\int_a^b f(x)dx = (b-a)f(c)$. Această „demonstrație scurtă" a teoremei de medie nu putea fi dată la început, căci nu știam că funcțiile continue au primitive (în demonstrația faptului că o funcție continuă are primitive se folosește tocmai teorema de medie!).

Exercițiu rezolvat

Fie $f : [0, \infty) \to [m, M]$ o funcție continuă, unde $0 < m < M$. Să se calculeze limita:

$$\lim_{t\to\infty} \frac{1}{t^2}\int_0^t f(x)dx$$

prin două metode și anume:

a) folosind teorema de medie; **b)** folosind regula lui l'Hospital.

Soluție

a) Din teorema de medie avem:

$\int_0^t f(x)dx = tf(c_t)$ cu $c_t \in [0, t]$. Din $m \le f(c_t) \le M$ și $t > 0$ rezultă $mt \le tf(c_t) \le Mt$ și mai departe $\frac{m}{t} \le \frac{1}{t^2}\cdot tf(c_t) \le \frac{M}{t}$, adică $\frac{m}{t} \le \frac{1}{t^2}\int_0^t f(x)dx \le \frac{M}{t}$.

Deoarece $\lim_{t\to\infty}\frac{m}{t} = \lim_{t\to\infty}\frac{M}{t} = 0$, conform criteriului cleștelui obținem că $\lim_{t\to\infty}\frac{1}{t^2}\int_0^t f(x)dx = 0$.

b) Din $f(x) \ge m$ rezultă $\int_0^t f(x)dx \ge \int_0^t m\,dx = mt$ și cum $\lim_{t\to\infty} mt = +\infty$ (fiindcă $m > 0$), înseamnă că și $\lim_{t\to\infty}\int_0^t f(x)dx = +\infty$.

Prin urmare suntem în ipotezele regulii lui l'Hospital, cazul $\frac{\infty}{\infty}$.

Aplicând regula lui l'Hospital, avem:

$$\lim_{t\to\infty}\frac{\int_0^t f(x)dx}{t^2} = \lim_{t\to\infty}\frac{\frac{d}{dt}\left(\int_0^t f(x)dx\right)}{2t} = \lim_{t\to\infty}\frac{f(t)}{2t} = 0.$$

Ultima egalitate rezultă din criteriul cleștelui și faptul că

$$\frac{m}{2t} \le \frac{f(t)}{2t} \le \frac{M}{2t}.$$

Metode de calcul al integralelor definite: schimbarea de variabilă şi integrarea prin părţi

1. Metoda schimbării de variabilă (a substituţiei)

Prima formulă a schimbării de variabilă: substituţia $t = u(x)$

Cadrul teoretic este fixat prin următoarea:

Teoremă

Considerăm funcţiile $I \xrightarrow{u} J \xrightarrow{f} \mathbb{R}$ (I, J intervale), funcţia u având argumentul x, iar funcţia f având argumentul t.

Dacă u este de clasă C^1 (derivabilă, cu derivata continuă) iar f este continuă, atunci pentru $a, b \in I$ arbitrare există egalitatea:

$$\int_a^b f(u(x))u'(x)dx = \int_{u(a)}^{u(b)} f(t)dt.$$

Demonstraţie. Funcţia $(f \circ u)u'$ este continuă, deci integrabilă, prin urmare integrala din membrul stâng are sens. De asemenea, funcţia f fiind continuă, este integrabilă, prin urmare integrala din membrul drept are sens. Funcţia continuă f are primitive şi fie $F : J \to \mathbb{R}$ o primitivă a sa. Atunci funcţia $F \circ u : I \to \mathbb{R}$ este o primitivă pentru funcţia $(f \circ u)u' : I \to \mathbb{R}$, fapt care se constată imediat. Folosind formula Leibniz – Newton, avem:

$$\int_a^b f(u(x))u'(x)dx = F(u(x))\Big|_a^b = F(u(a)) - F(u(b)) = F(t)\Big|_{u(a)}^{u(b)} = \int_{u(a)}^{u(b)} f(t)dt.$$

Comentariu metodic

Din teorema precedentă desprindem *modul practic de a proceda* atunci când vrem să calculăm o integrală de forma $\int_a^b f(u(x))u'(x)dx$. Pentru aceasta efectuăm următorii paşi:

1°. Facem substituţia $t = u(x)$.

2°. Diferenţiem formal, adică $dt = u'(x)\,dx$. (1)

3°. Schimbăm limitele de integrare conform substituţiei efectuate, adică $x_1 = a \Rightarrow t_1 = u(a)$, $x_2 = b \Rightarrow t_2 = u(b)$ şi înlocuim în integrala pe care vrem să o calculăm, obţinând:

$$\int_a^b f(u(x))u'(x)dx = \int_{t_1}^{t_2} f(t)dt \quad \left(= \int_{u(a)}^{u(b)} f(t)dt\right).$$

Atragem atenţia că egalitatea (1) este formală, totuşi e bine să fie utilizată, întrucât lasă calculul să decurgă de la sine. De asemenea, dacă facem comparaţie cu metoda schimbării de variabilă utilizată în cazul integralei nedefinite, constatăm că există o mare asemănare. Există însă şi o deosebire: în cazul integralei definite apare „în plus" schimbarea limitelor de integrare, care însă „se compensează" cu aceea că nu ne mai întoarcem la vechea variabilă de integrare.

Exerciţiu rezolvat

Să se calculeze integralele:

a) $\int_0^1 \frac{x^3}{1+x^8}dx$; **b)** $\int_{e^2}^{e^3} \frac{dx}{x\ln x}$; **c)** $\int_0^{\frac{\pi}{2}} \sin^4 x \cos x \, dx$.

Soluţie. **a)** Facem substituţia $t = x^4$. Diferenţiem formal şi obţinem $dt = 4x^3dx$. Schimbăm limitele de integrare: $x_1 = 0 \Rightarrow t_1 = 0^4 = 0$; $x_2 = 1 \Rightarrow t_2 = 1^4 = 1$. Integrala devine: $\int_0^1 \frac{x^3}{1+x^8}dx = \frac{1}{4}\int_0^1 \frac{4x^3dx}{1+x^8} = \frac{1}{4}\int_0^1 \frac{dt}{1+t^2} = \frac{1}{4} \operatorname{arctg} t \Big|_0^1 = \frac{1}{4}\left(\frac{\pi}{4} - 0\right) = \frac{\pi}{16}$.

b) Facem substituţia $t = \ln x$, de unde $dt = \frac{dx}{x}$. Schimbăm limitele de integrare: $x_1 = e^2 \Rightarrow t_1 = \ln e^2 = 2$; $x_2 = e^3 \Rightarrow t_2 = \ln e^3 = 3$. Integrala se scrie:

$$\int_{e^2}^{e^3} \frac{dx}{x\ln x} = \int_2^3 \frac{dt}{t} = \ln t \Big|_2^3 = \ln 3 - \ln 2.$$

c) Facem substituţia $t = \sin x$. Rezultă $dt = \cos x \, dx$. Schimbăm limitele de integrare: $x_1 = 0 \Rightarrow t_1 = \sin 0 = 0$; $x_2 = \frac{\pi}{2} \Rightarrow t_2 = \sin\frac{\pi}{2} = 1$. Integrala devine succesiv:

$$\int_0^{\frac{\pi}{2}} \sin^4 x \cos x \, dx = \int_0^1 t^4 dt = \frac{t^5}{5}\Big|_0^1 = \frac{1}{5}.$$

A doua formulă a schimbării de variabilă: substituţia $x = u(t)$

Cadrul teoretic al metodei este fixat prin următoarea:

Teoremă

Considerăm funcţiile $I \xrightarrow{u} J \xrightarrow{f} \mathbb{R}$ (*I*, *J* intervale), funcţia u având argumentul t, iar funcţia f având argumentul x. Dacă u este de clasă C^1 şi inversabilă iar f este continuă, atunci pentru $a, b \in I$ puncte arbitrare, avem egalitatea:

$$\int_a^b f(x)dx = \int_{u^{-1}(a)}^{u^{-1}(b)} f(u(t))u'(t)dt.$$

Demonstrație. Funcțiile f și $(f \circ u)u'$ sunt continue, deci integrabile, prin urmare ambele integrale considerate în enunț au sens. Funcția f fiind continuă, are primitive și fie $F : J \to \mathbb{R}$ o primitivă a sa. Atunci funcția $F \circ u : I \to \mathbb{R}$ este o primitivă pentru funcția $(f \circ u)u'$. Folosind formula Leiniz – Newton, putem scrie atunci:

$$\int_a^b f(x)dx = F(x)\Big|_a^b = F(b) - F(a) = F\left(u\left(u^{-1}(b)\right)\right) - F\left(u\left(u^{-1}(a)\right)\right) =$$

$$= (F \circ u)\left(u^{-1}(b)\right) - (F \circ u)\left(u^{-1}(a)\right) = (F \circ u)(t)\Big|_{u^{-1}(a)}^{u^{-1}(b)} = \int_{u^{-1}(a)}^{u^{-1}(b)} f\left(u(t)\right)u'(t)dt\,.$$

Comentariu metodic

Din teorema precedentă *desprindem modul practic de a proceda*. De multe ori, dacă vrem să calculăm o integrală definită, $\int_a^b f(x)dx$, efectuăm următorii pași:

1°. Facem substituția $x = u(t)$ (echivalent, $t = u^{-1}(x)$), cu u funcție inversabilă de clasă C^1.

2°. Diferențiem formal, adică $dx = u'(t)\, dt$. (1)

3°. Schimbăm limitele de integrare, adică $x_1 = a = u(t_1) \Rightarrow t_1 = u^{-1}(a)$; $x_2 = b = u(t_2) \Rightarrow t_2 = u^{-1}(b)$ și înlocuim în integrala de calculat, obținând:

$$\int_a^b f(x)dx = \int_{t_1}^{t_2} f\left(u(t)\right)u'(t)dt \quad \left(= \int_{u^{-1}(a)}^{u^{-1}(b)} f\left(u(t)\right)u'(t)dt\right).$$

Atragem și aici atenția că egalitatea (1) este una formală, totuși prin tradiție aceasta e bine să fie utilizată, întrucât permite calculelor să decurgă în mod firesc.

De multe ori, cele două variante ale schimbării de variabilă se aplică „în tandem”.

Exercițiu rezolvat

Să se calculeze: a) $\int_{\frac{1}{\sqrt{2}}}^{1} \frac{\sqrt{1-x^2}}{x^2}dx$; b) $\int_0^{\frac{\pi}{2}} \frac{dx}{2+\sin x}$; c) $\int_0^9 \frac{dx}{2+\sqrt{x}}$.

Soluție. a) Facem substituția $x = \sin t$, $t \in \left(0, \frac{\pi}{2}\right]$ (funcția $u : \left(0, \frac{\pi}{2}\right] \to (0,1]$, $u(t) = \sin t$ este inversabilă și de clasă C^1 iar funcția $f : (0, 1] \to \mathbb{R}$, $f(x) = \frac{\sqrt{1-x^2}}{x^2}$ este continuă).

Diferențiem formal și rezultă $dx = \cos t\, dt$. Schimbăm limitele de integrare: $x_1 = \frac{1}{\sqrt{2}}$ $\Rightarrow \sin t_1 = \frac{1}{\sqrt{2}} \Rightarrow t_1 = \arcsin\frac{1}{\sqrt{2}} = \frac{\pi}{4}$; $x_2 = 1 \Rightarrow \sin t_2 = 1 \Rightarrow t_2 = \arcsin 1 = \frac{\pi}{2}$.

Integrala devine:

$$\int_{\frac{1}{\sqrt{2}}}^{1}\frac{\sqrt{1-x^2}}{x^2}dx=\int_{\frac{\pi}{4}}^{\frac{\pi}{2}}\frac{\sqrt{1-\sin^2 t}}{\sin^2 t}\cdot\cos t\,dt=\int_{\frac{\pi}{4}}^{\frac{\pi}{2}}\frac{\cos^2 t}{\sin^2 t}dt=\int_{\frac{\pi}{4}}^{\frac{\pi}{2}}\frac{1-\sin^2 t}{\sin^2 t}dt=$$

$$=\int_{\frac{\pi}{4}}^{\frac{\pi}{2}}\left(\frac{1}{\sin^2 t}-1\right)dt=-(\operatorname{ctg} t+t)\Big|_{\frac{\pi}{4}}^{\frac{\pi}{2}}=-\frac{\pi}{2}+\left(1+\frac{\pi}{4}\right)=1-\frac{\pi}{4}.$$

b) Notăm $t=\operatorname{tg}\frac{x}{2}$ (prima formulă a schimbării de variabilă!). Dar $\frac{x}{2}\in\left[0,\frac{\pi}{4}\right]\subseteq\left(-\frac{\pi}{2},\frac{\pi}{2}\right)$ şi deoarece funcţia tg este inversabilă pe $\left(-\frac{\pi}{2},\frac{\pi}{2}\right)$, obţinem $\frac{x}{2}=\operatorname{arctg} t$, adică $x = 2\operatorname{arctg} t$ (a doua formulă a schimbării de variabilă!). Rezultă $dx=\frac{2\,dt}{1+t^2}$, apoi $x = 0 \Rightarrow t = \operatorname{tg} 0 = 0$, $x=\frac{\pi}{2}\Rightarrow t=\operatorname{tg}\frac{\pi}{4}=1$. Deoarece $\sin x=\frac{2t}{1+t^2}$,

integrala devine: $I=\int_0^{\frac{\pi}{2}}\frac{dx}{2+\sin x}=\int_0^1\frac{\frac{2\,dt}{1+t^2}}{2+\frac{2t}{1+t^2}}=\int_0^1\frac{dt}{t^2+t+1}=\int_0^1\frac{dt}{\left(t+\frac{1}{2}\right)^2+\frac{3}{4}}$.

Cu substituţia $u=t+\frac{1}{2}$, deci $du = dt$, $t = 0\Rightarrow u=\frac{1}{2}$, $t = 1\Rightarrow u=\frac{3}{2}$, obţinem:

$$I=\int_{\frac{1}{2}}^{\frac{3}{2}}\frac{du}{u^2+\left(\frac{\sqrt{3}}{2}\right)^2}=\frac{2}{\sqrt{3}}\operatorname{arctg}\frac{2u}{\sqrt{3}}\Big|_{\frac{1}{2}}^{\frac{3}{2}}=\frac{2}{\sqrt{3}}\left(\operatorname{arctg}\sqrt{3}-\operatorname{arctg}\frac{1}{\sqrt{3}}\right)=\frac{2}{\sqrt{3}}\left(\frac{\pi}{3}-\frac{\pi}{6}\right)=\frac{\pi}{3\sqrt{3}}.$$

c) Notăm $t=2+\sqrt{x}$ (prima formulă a schimbării de variabilă!). Rezultă $\sqrt{x}=t-2$, deci $x=(t-2)^2$ (a doua formulă a schimbării de variabilă!) şi apoi $dx=2(t-2)dt$. Schimbăm limitele de integrare: $x = 0\Rightarrow t = 2$, $x = 9 \Rightarrow t = 5$.

Integrala se scrie: $\int_0^9\frac{dx}{2+\sqrt{x}}=\int_2^5\frac{2(t-2)dt}{t}=2\int_2^5\left(1-\frac{2}{t}\right)dt=2(t-2\ln t)\Big|_2^5=$
$=2(5-2\ln 5-2+2\ln 2)=2(3+2\ln 2-2\ln 5)$.

La punctele b) şi c) verificarea condiţiilor din teoremă privind funcţiile u şi f rămâne ca o temă cu caracter oral.

2. Metoda integrării prin părţi

Cadrul teoretic al metodei este dat de următoarea:

Teoremă

Fie $u, v : [a, b] \to \mathbb{R}$ două funcţii de clasă C^1. Atunci are loc egalitatea următoare, numită formula integrării prin părţi:

$$\int_a^b u(x)v'(x)dx = u(x)v(x)\Big|_a^b - \int_a^b u'(x)v(x)dx,$$

sau, în notație diferențială:

$$\int_a^b u\,dv = uv\Big|_a^b - \int_a^b v\,du.$$

Demonstrație. Mai întâi e clar că integralele scrise au sens, întrucât funcțiile care se integrează sunt continue, deci integrabile. În egalitatea $(uv)' = u'v + uv'$ integrăm și obținem:

$$\int_a^b \big(u(x)v(x)\big)'\,dx = \int_a^b u'(x)v(x)dx + \int_a^b u(x)v'(x)dx,$$

adică

$$u(x)v(x)\Big|_a^b = \int_a^b u'(x)v(x)dx + \int_a^b u(x)v'(x)dx,$$

de unde

$$\int_a^b u(x)v'(x)dx = u(x)v(x)\Big|_a^b - \int_a^b u'(x)v(x)dx.$$

Observație

Se vede ușor că această formulă este analoagă celei de integrare prin părți de la integralele nedefinite, doar că aici totul *se ia* între limitele de integrare a și b.

Următorul exercițiu rezolvat vine să ilustreze aplicabilitatea metodei.

Exercițiu rezolvat

Să se calculeze integralele:

a) $\int_1^e x\ln x\,dx$; **c)** $\int_0^{\frac{\pi}{2}} \sin^n x\,dx$, unde $n \in \mathbb{N}$;

b) $\int_0^{\pi} e^x \sin x\,dx$; **d)** $\int_0^{\frac{\pi}{2}} \cos^n x\,dx$, unde $n \in \mathbb{N}$.

Soluție. **a)** Luăm $u = \ln x$, $dv = x\,dx$, de unde $du = \frac{dx}{x}$, $v = \frac{x^2}{2}$. Aplicând formula integrării prin părți obținem:

$$\int_1^e x\ln x\,dx = \frac{x^2}{2}\ln x\Big|_1^e - \int_1^e \frac{x^2}{2}\cdot\frac{dx}{x} = \frac{e^2}{2} - \frac{1}{2}\int_1^e x\,dx =$$

$$= \frac{e^2}{2} - \frac{1}{2}\cdot\frac{x^2}{2}\Big|_1^e = \frac{e^2}{2} - \left(\frac{e^2}{4} - \frac{1}{4}\right) = \frac{e^2+1}{4}.$$

b) Luăm $u = \sin x$, $dv = e^x dx$, de unde $du = \cos x\,dx$, $v = e^x$ și avem:

$$\int_0^{\pi} e^x \sin x\, dx = e^x \sin x \Big|_0^{\pi} - \int_0^{\pi} e^x \cos x\, dx. \quad (1)$$

Integrala la care am ajuns se calculează tot prin părţi luând $u_1 = \cos x$, $dv_1 = e^x dx$, de unde $du_1 = -\sin x\, dx$, $v_1 = e^x$ şi atunci:

$$\int_0^{\pi} e^x \cos x\, dx = e^x \cos x \Big|_0^{\pi} + \int_0^{\pi} e^x \sin x\, dx. \quad (2)$$

Notând $I = \int_0^{\pi} e^x \sin x\, dx$, din (1) şi (2) obţinem: $I = (e^x \sin x - e^x \cos x)\Big|_0^{\pi} - I$, de unde $I = \frac{1}{2}(e^x \sin x - e^x \cos x)\Big|_0^{\pi} = \frac{1}{2}e^{\pi} + \frac{1}{2} = \frac{e^{\pi}+1}{2}$.

c) Să notăm $I_n = \int_0^{\frac{\pi}{2}} \sin^n x\, dx$, $n \in \mathbb{N}$. Pentru $n \geq 2$ luăm $u = \sin^{n-1} x$, $dv = \sin x\, dx$, de unde $du = (n-1)\sin^{n-2} x \cos x\, dx$, $v = -\cos x$. Integrăm prin părţi şi avem succesiv:

$$I_n = -\sin^{n-1} x \cos x \Big|_0^{\pi} - \int_0^{\pi} (n-1)\sin^{n-2} x \cos x(-\cos x)dx =$$

$$= (n-1)\int_0^{\pi} \sin^{n-2} x \cos^2 x\, dx = (n-1)\int_0^{\pi} \sin^{n-2} x(1-\sin^2 x)dx =$$

$$= (n-1)\int_0^{\pi} \sin^{n-2} x\, dx - (n-1)\int_0^{\pi} \sin^n x\, dx = (n-1)I_{n-2} - (n-1)I_n.$$

Rezultă $nI_n = (n-1)I_{n-2}$ şi de aici obţinem recurenţa de ordinul doi $I_n = \frac{n-1}{n} \cdot I_{n-2}$ (3), valabilă pentru $n \in \mathbb{N}$, $n \geq 2$.

Să mai observăm că $I_0 = \int_0^{\frac{\pi}{2}} dx = x\Big|_0^{\frac{\pi}{2}} = \frac{\pi}{2}$ şi $I_1 = \int_0^{\frac{\pi}{2}} \sin x\, dx = -\cos x\Big|_0^{\frac{\pi}{2}} = 1$.

Din (3) şi valorile I_0, I_1 rezultă imediat că $I_n \neq 0$, $\forall\, n \in \mathbb{N}$. Dacă în (3) luăm pe rând $n = 2$, $n = 4$, $n = 6$, …, $n = 2k$, obţinem: $I_2 = \frac{1}{2} \cdot I_0$, $I_4 = \frac{3}{4} \cdot I_2$, $I_6 = \frac{5}{6} \cdot I_4$, …, $I_{2k} = \frac{2k-1}{2k} \cdot I_{2k-2}$. Înmulţim toate aceste egalităţi şi obţinem:

$$I_2 I_4 I_6 \ldots I_{2k} = \frac{1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2k-1)}{2 \cdot 4 \cdot 6 \cdot \ldots \cdot (2k)} \cdot I_0 I_2 I_4 \ldots I_{2k-2}.$$

Simplificând prin $I_2 I_4 I_6 \ldots I_{2k-2} \neq 0$ şi ţinând seama că $I_0 = \frac{\pi}{2}$ rezultă:

$$I_{2k} = \frac{1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2k-1)}{2 \cdot 4 \cdot 6 \cdot \ldots \cdot (2k)} \cdot \frac{\pi}{2} = \frac{(2k-1)!!}{(2k)!!} \cdot \frac{\pi}{2}. \quad (4)$$

Dacă în (3) luăm pe rând $n = 3$, $n = 5$, $n = 7$, …, $n = 2k + 1$, obţinem:

$$I_3=\frac{2}{3}\cdot I_1,\ \ I_5=\frac{4}{5}\cdot I_3,\ \ I_7=\frac{6}{7}\cdot I_5,\ \ldots,\ I_{2k+1}=\frac{2k}{2k+1}\cdot I_{2k-1}.$$

Înmulţind aceste egalităţi rezultă: $I_3 I_5 I_7 \ldots I_{2k+1}=\dfrac{2\cdot 4\cdot 6\cdot\ldots\cdot(2k)}{3\cdot 5\cdot 7\cdot\ldots\cdot(2k+1)}\cdot I_1 I_3 I_5\ldots I_{2k-1}$.

Simplificând prin $I_3 I_5 I_7\ldots I_{2k-1}\neq 0$ şi ţinând seama că $I_1=1$ obţinem:

$$I_{2k+1}=\frac{2\cdot 4\cdot 6\cdot\ldots\cdot(2k)}{3\cdot 5\cdot 7\cdot\ldots\cdot(2k+1)}=\frac{(2k)!!}{(2k+1)!!}. \qquad (5)$$

d) Să notăm $J_n=\int_0^{\frac{\pi}{2}}\cos^n x\,dx$. Efectuăm schimbarea de variabilă $x=\dfrac{\pi}{2}-t$, de unde $dx=-dt$, $x_1=0\Rightarrow t_1=\dfrac{\pi}{2}$, $x_2=\dfrac{\pi}{2}\Rightarrow t_2=0$ şi integrala devine:

$$J_n=\int_0^{\frac{\pi}{2}}\cos^n x\,dx=\int_{\frac{\pi}{2}}^{0}\cos^n\left(\frac{\pi}{2}-t\right)(-dt)=\int_0^{\frac{\pi}{2}}\sin^n t\,dt=I_n,$$

unde I_n este integrala calculată la punctul c).

Prin urmare valorile integralei J_n sunt date de formulele (4) şi (5) de la punctul c), care corespund cazurilor n par, respectiv n impar.

EXERCIŢII PROPUSE

I. Utilizând metoda schimbării de variabilă, calculaţi integralele:

1. $\int_1^3 e^{2x}dx$; **2.** $\int_0^1\dfrac{dx}{x+2}$; **3.** $\int_0^{\frac{\pi}{4}}\cos 2x\,dx$;

4. $\int_0^{\frac{\pi}{4}}\sin 4x\,dx$; **5.** $\int_2^3(2x-1)^3dx$; **6.** $\int_1^2\dfrac{dx}{\sqrt{5x-1}}$;

7. $\int_4^5(4-x)^3dx$; **8.** $\int_0^1\dfrac{dx}{(3x+1)^4}$: **9.** $\int_0^3\sqrt[3]{3x-1}\,dx$;

10. $\int_1^5\sqrt{(2x-1)^3}\,dx$; **11.** $\int_{-2}^5\dfrac{dx}{\sqrt[3]{(x+3)^2}}$; **12.** $\int_{-1}^2 x\left(x^2-1\right)^2dx$;

13. $\int_0^2\dfrac{4x\,dx}{\left(x^2-1\right)^3}$; **14.** $\int_0^2 9x^2\sqrt{x^3+1}\,dx$; **15.** $\int_0^{\frac{\pi}{2}}\cos x\cdot\sqrt{3\sin x+1}\,dx$;

16. $\int_{\frac{3\pi}{2}}^{2\pi}\sin x\cdot\sqrt{1-\cos x}\,dx$; **17.** $\int_0^{\frac{\pi}{3}}\dfrac{\sin x\,dx}{3-\cos x}$; **18.** $\int_0^{\frac{\pi}{2}}\dfrac{\cos x\,dx}{2+\sin x}$;

19. $\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \frac{\sin x\, dx}{1+\cos x}$; 20. $\int_0^{\frac{\pi}{6}} \cos x \cdot e^{\sin x} dx$; 21. $\int_0^1 x e^{x^2} dx$;

22. $\int_0^{\sqrt[3]{2}} 3x^2 e^{x^3} dx$; 23. $\int_0^{\pi} \sin\frac{x}{3} dx$; 24. $\int_{\frac{2\pi}{9}}^{\frac{\pi}{3}} \sin\left(3x - \frac{\pi}{2}\right) dx$;

25. $\int_{\frac{\pi}{6}}^{\frac{\pi}{4}} \cos\left(2x - \frac{\pi}{6}\right) dx$; 26. $\int_{\frac{2\pi}{3}}^{\frac{4\pi}{3}} \cos\frac{x}{4} dx$; 27. $\int_{\frac{\pi}{8}}^{\frac{\pi}{6}} \frac{dx}{\cos^2 2x}$;

28. $\int_{\frac{\pi}{18}}^{\frac{\pi}{9}} \frac{dx}{\sin^2 3x}$; 29. $\int_{\frac{3}{2}}^{\frac{3\sqrt{2}}{2}} \frac{\sqrt{2}\, dx}{\sqrt{9-2x^2}}$; 30. $\int_{\frac{1}{2}}^{\frac{3}{2}} \frac{dx}{3+4x^2}$;

31. $\int_0^1 \frac{dx}{1+\sqrt{x}}$; 32. $\int_0^{\ln 2} \sqrt{e^x - 1}\, dx$; 33. $\int_0^1 \sqrt{1-x^2}\, dx$;

34. $\int_1^2 \frac{\sqrt{x^2-1}}{x} dx$; 35. $\int_0^{\frac{\pi}{2}} \frac{dx}{3+2\cos x}$; 36. $\int_0^{2\pi} \frac{dx}{3+2\cos x}$.

II. Utilizând metoda integrării prin părți, calculați integralele:

1. $\int_1^e \ln x\, dx$; 2. $\int_e^4 x \ln x\, dx$; 3. $\int_0^1 x e^{-e} dx$;

4. $\int_0^{\frac{\pi}{2}} x \sin x\, dx$; 5. $\int_0^{\frac{\pi}{2}} x \cos x\, dx$; 6. $\int_0^1 \operatorname{arctg} x\, dx$;

7. $\int_0^1 x \operatorname{arctg} x\, dx$; 8. $\int_0^1 \arcsin x\, dx$; 9. $\int_0^{\pi} e^x \sin x\, dx$;

10. $\int_{\frac{1}{e}}^{e} |\ln x|\, dx$.

III. Notăm $I_n = \int_{-1}^{1} (1-x^2)^n dx$, unde $n \in \mathbb{N}$. Arătați că:

a) $I_n = \frac{2n}{2n+1} \cdot I_{n-1}$ pentru orice $n \in \mathbb{N}^*$;

b) $I_n = 2 \cdot \frac{(2n)!!}{(2n+1)!!}$ pentru orice $n \in \mathbb{N}^*$;

c) $\sum_{k=0}^{n} \frac{(-1)^k C_n^k}{2k+1} = \frac{(2n)!!}{(2n+1)!!}$.

TESTE DE EVALUARE

Testul 1

(timp de lucru - 40 minute; fiecare exercițiu se notează cu 2,25 puncte)

Indicați răspunsul corect.

1. $\lim\limits_{n\to\infty}\int_1^e \ln^n x\,dx =$

a) 1; b) e; c) 0; d) $+\infty$.

2. $\int_0^{\pi/4}\ln(1+\operatorname{tg} x)dx =$

a) $\frac{\pi}{4}+\ln 2$; b) $\pi\ln 2$; c) $\frac{\pi}{4}\ln 3$; d) $\frac{\pi}{8}\ln 2$.

3. $\lim\limits_{x\to 0}\dfrac{\int_0^x \ln(1+t^2)dt}{\sin^3 x} =$

a) $\frac{1}{2}$; b) 0; c) $\frac{1}{3}$; d) 1.

4. Dacă $m\int_0^1 e^{mx^2+\ln x}dx = 1$, atunci $m =$

a) ln 3; b) 2; c) e; d) ln 2.

Testul 2

(timp de lucru - 60 minute; fiecare exercițiu se notează cu 2,25 puncte)

Pentru următoarele probleme se cer soluții complete.

1. Calculați $\lim\limits_{x\to\infty}\frac{1}{n}\int_0^1 [nx]dx$.

2. Să se arate că $2\sqrt{e}\le\int_0^1 e^{x^2}dx+\int_0^1 e^{1-x^2}dx\le 1+e$.

3. Fie $f:[0,1]\to\mathbb{R}$ o funcție continuă cu $\int_0^1 f(x)dx=\frac{1}{2}$. Să se arate că există $c\in(0,1)$ cu $f(c)=c$.

4. a) Fie $f:[0,1]\to\mathbb{R}$ o funcție continuă. Să se arate că $\lim\limits_{x\to\infty}\int_0^1 x^n f(x)dx = 0$.

b) Fie $f:[0,1]\to\mathbb{R}$ o funcție derivabilă cu derivata continuă.

Să se arate că $\lim\limits_{x\to\infty} n\int_0^1 x^n f(x)dx = f(1)$.

Integralele funcţiilor raţionale

Prin ***funcţie raţională*** înţelegem o funcţie asociată unei fracţii raţionale cu coeficienţi reali, definită pe un interval care nu conţine nici o rădăcină reală a polinomului de la numitor.

Mai precis, dacă $\frac{u}{v}=\frac{u(X)}{v(X)} \in \mathbb{R}(X)$ este o fracţie raţională, iar $I \subseteq \mathbb{R}$ un interval astfel încât $v(x) \neq 0$, $\forall\, x \in I$, funcţia raţională asociată este $f : I \to \mathbb{R}$, $f(x) = \frac{u(x)}{v(x)}$.

Funcţiile raţionale asociate fracţiilor raţionale simple le vom numi ***funcţii raţionale simple***. La sfârşitul capitolului „Inele de polinoame" am demonstrat teorema de descompunere unică în fracţii raţionale simple a unei fracţii raţionale cu coeficienţi reali.

Reamintim enunţul acestei teoreme:

Teoremă

Dacă $\frac{u(X)}{v(X)}$ este o fracţie raţională cu coeficienţi reali, iar polinomul $v(X)$ are în $\mathbb{R}[X]$ descompunerea în factori ireductibili $v(X)=\prod_{i=1}^{n}(a_iX+b_i)^{k_i}\cdot\prod_{i=1}^{m}\left(\alpha_iX^2+\beta_iX+\gamma_i\right)^{\ell_i}$, cu $\beta_i^2-4\alpha_i\gamma_i<0$, $i=\overline{1,m}$, atunci avem scrierea unică:

$$\frac{u(X)}{v(X)}=u_0(X)+\sum_{i=1}^{n}\sum_{j=1}^{k_i}\frac{A_{ij}}{(a_iX+b_i)^j}+\sum_{i=1}^{m}\sum_{j=1}^{\ell_i}\frac{B_{ij}X+C_{ij}}{\left(\alpha_iX^2+\beta_iX+\gamma_i\right)^j},$$

unde $u_0(X) \in \mathbb{R}[X]$, iar $A_{ij} \in \mathbb{R}$, $i=\overline{1,n}$, $j=\overline{1,k_i}$, $B_{ij}, C_{ij} \in \mathbb{R}$, $i=\overline{1,m}$, $j=\overline{1,\ell_i}$.

Determinarea efectivă a polinomului $u_0(X)$ şi a coeficienţilor A_{ij}, B_{ij}, C_{ij} se poate face prin metoda coeficienţilor nedeterminaţi.

Corespunzător, orice funcţie raţională se scrie în mod unic ca o sumă dintre o funcţie polinomială şi nişte funcţii raţionale simple.

Deoarece integrala unei sume este egală cu suma integralelor, iar integrala unei funcţii polinomiale se face foarte uşor, deducem că ***pentru a calcula integrala unei funcţii raţionale este suficient să ştim să calculăm integralele funcţiilor raţionale simple.***

Bineînţeles, integrala Riemann a unei funcţii raţionale $f : [a, b] \to \mathbb{R}$ se poate calcula uşor cu ajutorul formulei Leibniz – Newton, dacă ştim să calculăm primitivele (integrala nedefinită) funcţiei f. De aceea *vom face calculul pentru integrale nedefinite*, acest calcul fiind totodată mai relevant pentru însuşirea metodei.

Aşadar, în cele ce urmează vom calcula integrale nedefinite de forma:

I) $\int \frac{A}{(ax+b)^n}dx$ sau **II)** $\int \frac{Bx+C}{\left(\alpha x^2+\beta x+\gamma\right)^n}dx$ cu $\beta^2-4\alpha\gamma<0$,

n fiind un număr natural nenul.

În exercițiile din acest manual ***vom întâlni valori mici ale lui n***, în ideea de a nu obține calcule complicate.

Vom lucra, de regulă, cu fracții raționale în care *gradul numitorului este mai mic sau egal cu* 4.

Pentru o integrală de forma I) avem:

$$\int \frac{A}{(ax+b)^n}dx = A\int \frac{dx}{(ax+b)^n}.$$

Facem substituția $t=ax+b$, de unde $dt=a\,dx$ şi atunci:

$$\int \frac{dx}{(ax+b)^n}dx=\frac{1}{a}\int \frac{a\,dx}{(ax+b)^n}=\frac{1}{a}\int \frac{dt}{t^n}=\frac{1}{a}\int t^{-n}dt.$$

Dacă $n=1$, avem $\int t^{-1}dt=\ln|t|+\mathscr{C}$, iar pentru $n\geq 2$ avem:

$$\int t^{-n}dt=\frac{t^{-n+1}}{-n+1}+\mathscr{C}=-\frac{1}{(n-1)t^{n-1}}+\mathscr{C}.$$

În concluzie:

$$\int \frac{A}{(ax+b)^n}dx=\begin{cases}\dfrac{A}{a}\ln|ax+b|+\mathscr{C}, & \text{dacă } n=1\\ -\dfrac{A}{(n-1)a(ax+b)^{n-1}}+\mathscr{C}, & \text{dacă } n\geq 2\end{cases}$$

(Atenție, prezența lui a la numitor este posibilă, căci $a\neq 0$, din moment ce $aX+b$ este un polinom de gradul întâi).

Ne ocupăm în continuare de integralele de forma II).

Mai întâi, când $B\neq 0$, încercăm să organizăm la numărător derivata trinomului de gradul doi de la numitor, adică $\left(\alpha x^2+\beta x+\gamma\right)'=2\alpha x+\beta$.

Pentru aceasta amplificăm integrala cu 2α (posibil, căci $\alpha\neq 0$), apoi forțăm factorul comun B la numărător şi, în fine, adunăm şi scădem β la numărător. Avem aşadar:

$$\int \frac{Bx+C}{\left(\alpha x^2+\beta x+\gamma\right)^n}dx=\frac{1}{2\alpha}\int \frac{2\alpha Bx+2\alpha C}{\left(\alpha x^2+\beta x+\gamma\right)^n}dx=\frac{B}{2\alpha}\int \frac{2\alpha x+\dfrac{2\alpha C}{B}}{\left(\alpha x^2+\beta x+\gamma\right)^n}dx=$$

$$=\frac{B}{2\alpha}\int \frac{(2\alpha x+\beta)+\left(\dfrac{2\alpha C}{B}-\beta\right)}{\left(\alpha x^2+\beta x+\gamma\right)^n}dx=\frac{B}{2\alpha}\int \frac{2\alpha x+\beta}{\left(\alpha x^2+\beta x+\gamma\right)^n}dx+\frac{2\alpha C-\beta B}{2\alpha}\int \frac{dx}{\left(\alpha x^2+\beta x+\gamma\right)^n}.$$

Prima integrală se calculează prin substituţia $t = \alpha x^2 + \beta x + \gamma$, deci $dt = (2\alpha x + \beta)dx$, obţinând:

$$\int \frac{2\alpha x + \beta}{\left(\alpha x^2 + \beta x + \gamma\right)^n} dx = \int \frac{dt}{t^n} = \int t^{-n} dt = \begin{cases} \ln|t| + \mathscr{C}, & \text{dacă } n = 1 \\ \dfrac{t^{-n+1}}{-n+1} + \mathscr{C}, & \text{dacă } n \geq 2 \end{cases} =$$

$$= \begin{cases} \ln|\alpha x^2 + \beta x + \gamma| + \mathscr{C}, & \text{dacă } n = 1 \\ -\dfrac{1}{(n-1)\left(\alpha x^2 + \beta x + \gamma\right)^{n-1}} + \mathscr{C}, & \text{dacă } n \geq 2 \end{cases}$$

Pentru a doua integrală, utilizăm scrierea cu pătrat restrâns a trinomului de gradul doi şi anume:

$$\alpha x^2 + \beta x + \gamma = \alpha\left(\left(x + \frac{\beta}{2\alpha}\right)^2 - \frac{\Delta}{4\alpha^2}\right), \text{ unde } \Delta = \beta^2 - 4\alpha\gamma < 0.$$

Notând $\delta^2 = -\dfrac{\Delta}{4\alpha^2}$, unde $\delta \in \mathbb{R}^*$, obţinem $\alpha x^2 + \beta x + \gamma = \alpha\left(\left(x + \dfrac{\beta}{2\alpha}\right)^2 + \delta^2\right)$.

Rezultă:

$$\int \frac{dx}{\left(\alpha x^2 + \beta x + \gamma\right)^n} = \frac{1}{\alpha^n} \cdot \int \frac{dx}{\left(\left(x + \dfrac{\beta}{2\alpha}\right)^2 + \delta^2\right)^n}.$$

Integrala la care am ajuns se transformă prin substituţia $t = x + \dfrac{\beta}{2\alpha}$ în integrala:

$$I_n(t) = \int \frac{dt}{(t^2 + \delta^2)^n},$$

care pentru $n = 1$ este imediată, iar pentru $n \geq 2$ se calculează stabilind o relaţie de recurenţă în şirul $(I_n(t))_{n \geq 1}$. Pentru aceasta amplificăm cu δ^2 şi apoi adunăm şi scădem la numărător t^2. Obţinem, pentru $n \geq 2$:

$$I_n(t) = \frac{1}{\delta^2} \int \frac{\delta^2}{(t^2 + \delta^2)^n} dt = \frac{1}{\delta^2} \int \frac{(t^2 + \delta^2) - t^2}{(t^2 + \delta^2)^n} dt =$$

$$= \frac{1}{\delta^2} \int \frac{dt}{(t^2 + \delta^2)^{n-1}} - \frac{1}{\delta^2} \int \frac{t^2}{(t^2 + \delta^2)^n} dt = \frac{1}{\delta^2} \cdot I_{n-1}(t) - \frac{1}{\delta^2} \int t \cdot \frac{t}{(t^2 + \delta^2)^n} dt. \quad (1)$$

Ultima integrală se calculează prin părţi luând $u = t$, $dv = \dfrac{t\,dt}{\left(t^2+\delta^2\right)^n}$.

Obţinem $du = dt$, $v \in \displaystyle\int \frac{t\,dt}{\left(t^2+\delta^2\right)^n} = \frac{1}{2}\int \frac{2t\,dt}{\left(t^2+\delta^2\right)^n}$.

Cu substituţia $\tau = t^2 + \delta^2$, deci $d\tau = 2t\,dt$, avem:

$$\int \frac{2t\,dt}{\left(t^2+\delta^2\right)^n} = \int \frac{d\tau}{\tau^n} = \frac{\tau^{-n+1}}{-n+1} + \mathscr{C} = -\frac{1}{(n-1)\tau^{n-1}} + \mathscr{C} = -\frac{1}{(n-1)\left(t^2+\delta^2\right)^{n-1}} + \mathscr{C},$$

aşa că putem lua $v = -\dfrac{1}{2(n-1)\left(t^2+\delta^2\right)^{n-1}}$.

Calculând integrala prin părţi, de care am vorbit, obţinem:

$$\int t \cdot \frac{t}{\left(t^2+\delta^2\right)^n}\,dt = -\frac{t}{2(n-1)\left(t^2+\delta^2\right)^n} - \int\left(-\frac{1}{2(n-1)\left(t^2+\delta^2\right)^{n-1}}\right)dt =$$

$$= -\frac{t}{2(n-1)\left(t^2+\delta^2\right)^{n-1}} + \frac{1}{2(n-1)} \cdot I_{n-1}(t).$$

Înlocuind în (1) rezultă:

$$I_n(t) = \frac{1}{\delta^2} I_{n-1}(t) - \frac{1}{\delta^2}\left(-\frac{t}{2(n-1)\left(t^2+\delta^2\right)^{n-1}} + \frac{1}{2(n-1)} I_{n-1}(t)\right),$$

adică o recurenţă de ordinul întâi care arată astfel:

$$I_n(t) = \frac{t}{2(n-1)\delta^2\left(t^2+\delta^2\right)^{n-1}} + \frac{2n-3}{2(n-1)\delta^2} \cdot I_{n-1}(t),\ \forall\, n \geq 2.$$

Acestei relaţii de recurenţă îi adăugăm primul termen din şirul $\left(I_n(t)\right)_{n\geq 1}$:

$$I_1(t) = \int \frac{dt}{t^2+\delta^2} = \frac{1}{\delta}\ \mathrm{arctg}\,\frac{t}{\delta} + \mathscr{C}.$$

În acest fel şirul $\left(I_n(t)\right)_{n\geq 1}$ este perfect determinat şi revenind la variabila iniţială x, calculul integralei se încheie.

Observație

Mai sus am expus un *calcul în principiu al integralelor din funcții raționale simple*. Nu trebuie reținute formulele care privesc acest calcul, ci doar ideile mari, care permit refacerea calculelor în fiecare caz concret. Deoarece, așa cum am mai menționat, valorile lui n vor fi mici, calculele pe care le vom întâlni nu vor fi foarte anevoioase.

Exercițiu rezolvat

Să se calculeze integralele:

a) $\displaystyle\int \frac{10x^3-4x^2-34x+12}{x^4-10x^2+9}\,dx$, $x \in (3, \infty)$;

b) $\displaystyle\int \frac{x^5+2x^4+x^3-3x^2-4x+1}{x^4+2x^3+2x^2+2x+1}\,dx$, $x \in (-\infty, -1)$;

c) $\displaystyle\int_0^1 \frac{x^3+x^2+3x+2}{(x^2+x+1)^2}\,dx$.

Soluție. **a)** Numitorul se descompune în factori ireductibili cu coeficienți reali astfel:

$$x^4-10x^2+9=(x-1)(x+1)(x-3)(x+3).$$

Deoarece gradul numărătorului este mai mic decât gradul numitorului, nu avem „parte polinomială", deci descompunerea în fracții raționale simple este de forma:

$$\frac{10x^3-4x^2-34x+12}{(x-1)(x+1)(x-3)(x+3)}=\frac{A}{x-1}+\frac{B}{x+1}+\frac{C}{x-3}+\frac{D}{x+3}, \qquad (*)$$

fiind valabilă pentru orice $x \in \mathbb{R} \setminus \{-3, -1, 1, 3\}$.

Pentru determinarea constantelor A, B, C, D putem să eliminăm numitorii și apoi să folosim metoda coeficienților nedeterminați în egalitatea polinomială care se obține. Totuși, în situația în care numitorul are în descompunerea sa doar factori liniari (ca în cazul de față), se poate proceda astfel: se înmulțește egalitatea (*) cu $x - 1$, obținându-se:

$$\frac{10x^3-4x^2-34x+12}{(x+1)(x-3)(x+3)}=A+(x-1)\left(\frac{B}{x+1}+\frac{C}{x-3}+\frac{D}{x+3}\right),$$

după care trecem la limită când $x \to 1$ și găsim $A = 1$; apoi se înmulțește egalitatea (*) cu $x + 1$, obținându-se:

$$\frac{10x^3-4x^2-34x+12}{(x-1)(x-3)(x+3)}=B+(x+1)\left(\frac{A}{x-1}+\frac{C}{x-3}+\frac{D}{x+3}\right),$$

după care trecem la limită când $x \to -1$ și găsim $B = 2$.

Analog obținem $C = 3$, $D = 4$, prin urmare, descompunerea în fracții raționale simple este:

$$\frac{10x^3-4x^2-34x+12}{(x-1)(x+1)(x-3)(x+3)}=\frac{1}{x-1}+\frac{2}{x+1}+\frac{3}{x-3}+\frac{4}{x+3}.$$

Integrând obținem:

$$\int\frac{10x^3-4x^2-34x+12}{x^4-10x^2+9}dx=\int\frac{dx}{x-1}+2\int\frac{dx}{x+1}+3\int\frac{dx}{x-3}+4\int\frac{dx}{x+3}=$$
$$=\ln(x-1)+2\ln(x+1)+3\ln(x-3)+4\ln(x+3)+\mathscr{C},$$

unde am ținut seama că $x>3$, deci modulele sub semnul ln nu mai apar efectiv.

b) Deoarece gradul numărătorului este mai mare ca gradul numitorului, împărțim numărătorul la numitor şi obținem câtul x şi restul $-x^3-5x^2-5x+1$. Din teorema împărțirii cu rest avem:

$$x^5+2x^4+x^3-3x^2-4x+1=x(x^4+2x^3+2x^2+2x+1)-(x^3+5x^2+5x-1),$$

de unde: $\dfrac{x^5+2x^4+x^3-3x^2-4x+1}{x^4+2x^3+2x^2+2x+1}=x-\dfrac{x^3+5x^2+5x-1}{x^4+2x^3+2x^2+2x+1}$.

Rămânem să descompunem în fracții raționale simple fracția rațională:

$\dfrac{x^3+5x^2+5x-1}{x^4+2x^3+2x^2+2x+1}$. Mai întâi descompunem numitorul în factori ireductibili cu coeficienți reali. Observăm că $x=-1$ este rădăcină dublă pentru polinomul de la numitor, întrucât verifică acest polinom şi derivata sa. Rezultă că polinomul de la numitor se divide cu $(x+1)^2$, iar câtul împărțirii este x^2+1, care este un polinom ireductibil cu coeficienți reali. Prin urmare descompunerea numitorului este:

$$x^4+2x^3+2x^2+2x+1=(x+1)^2(x^2+1).$$

Conform teoremei de descompunere în fracții simple, vom avea:

$$\frac{x^3+5x^2+5x-1}{(x+1)^2(x^2+1)}=\frac{A}{x+1}+\frac{B}{(x+1)^2}+\frac{Cx+D}{x^2+1}.$$

Eliminând numitorii, obținem:

$$x^3+5x^2+5x-1=A(x+1)(x^2+1)+B(x^2+1)+(Cx+D)(x+1)^2,$$

sau, după calcule:

$$x^3+5x^2+5x-1=(A+C)x^3+(A+B+2C+D)x^2+(A+C+2D)x+(A+B+D).$$

Aplicăm metoda coeficienților nedeterminați (identificăm coeficienții termenilor cu puteri egale ale lui x) şi obținem sistemul liniar:

$$\begin{cases}A+C=1\\A+B+2C+D=5\\A+C+2D=5\\A+B+D=-1\end{cases}$$

Rezultă uşor $A=-2$, $B=-1$, $C=3$, $D=2$. Prin urmare descompunerea în fracții simple este:

$$\frac{x^3+5x^2+5x-1}{(x+1)^2(x^2+1)}=-\frac{2}{x+1}-\frac{1}{(x+1)^2}+\frac{3x+2}{x^2+1}.$$

În final, funcția de integrat se va scrie:

$$\frac{x^5+2x^4+x^3-3x^2-4x+1}{x^4+2x^3+2x^2+2x+1}=x+\frac{2}{x+1}+\frac{1}{(x+1)^2}-\frac{3x+2}{x^2+1}.$$

Integrând, obținem:

$$\int\frac{x^5+2x^4+x^3-3x^2-4x+1}{x^4+2x^3+2x^2+2x+1}dx=\int x\,dx-2\int\frac{dx}{x+1}+\int\frac{dx}{(x+1)^2}-\frac{3}{2}\int\frac{2x}{x^2+1}dx-$$

$$-2\int\frac{dx}{x^2+1}=\frac{x^2}{2}-2\ln|x+1|-\frac{1}{x+1}-\frac{3}{2}\ln(x^2+1)-2\text{ arctg }x+\mathscr{C}=$$

$$=\frac{x^2}{2}-\frac{1}{x+1}-2\ln(-x-1)-\frac{3}{2}\ln(x^2+1)-2\text{ arctg }x+\mathscr{C}.$$

Am ținut seama că $x\in(-\infty,-1)$, deci $|x+1|=-x-1$.

c) Gradul numărătorului fiind mai mic decât cel al numitorului, iar numitorul fiind deja descompus în factori ireductibili cu coeficienți reali, trecem direct la descompunerea în fracții raționale simple. Avem:

$$\frac{x^3+x^2+3x+2}{(x^2+x+1)^2}=\frac{Ax+B}{x^2+x+1}+\frac{Cx+D}{(x^2+x+1)^2}.$$

Eliminând numitorii, obținem $x^3+x^2+3x+2=(Ax+B)(x^2+x+1)+Cx+D$ sau după calcule: $x^3+x^2+3x+2=Ax^3+(A+B)x^2+(A+B+C)x+(B+D)$.

Identificând coeficienții, obținem sistemul:

$$\begin{cases}A=1\\A+B=1\\A+B+C=3\\B+D=2\end{cases},\text{ de unde } A=1,\ B=0,\ C=2,\ D=2.$$

Prin urmare funcția rațională de integrat se scrie:

$$\frac{x^3+x^2+3x+2}{(x^2+x+1)^2}=\frac{x}{x^2+x+1}+\frac{2x+2}{(x^2+x+1)^2}.$$

Preferăm să calculăm integrala nedefinită (primitivele) și în final să aplicăm formula Leibniz – Newton. Avem:

$$\int\frac{x^3+x^2+3x+2}{(x^2+x+1)^2}dx=\frac{1}{2}\int\frac{(2x+1)-1}{x^2+x+1}dx+\int\frac{(2x+1)dx}{(x^2+x+1)^2}+\int\frac{dx}{(x^2+x+1)^2}=$$

$$=\frac{1}{2}\int\frac{(2x+1)dx}{x^2+x+1}+\int\frac{(2x+1)dx}{(x^2+x+1)^2}-\frac{1}{2}\int\frac{dx}{x^2+x+1}+\int\frac{dx}{(x^2+x+1)^2}.$$

Primele două integrale se calculează prin substituția $t=x^2+x+1$, de unde $dt=(2x+1)dx$, prin urmare:

$$\int\frac{(2x+1)dx}{x^2+x+1}=\int\frac{dt}{t}=\ln|t|+\mathscr{C}=\ln(x^2+x+1)+\mathscr{C},$$

$$\int \frac{(2x+1)dx}{(x^2+x+1)^2} = \int \frac{dt}{t^2} = -\frac{1}{t} + \mathscr{C} = -\frac{1}{x^2+x+1} + \mathscr{C}.$$

Pentru a treia şi a patra integrală, scriem forma cu pătrat restrâns $x^2+x+1 = \left(x+\frac{1}{2}\right)^2 + \frac{3}{4}$ şi facem substituţia $t = x + \frac{1}{2}$, de unde $dt = dx$. Obţinem:

$$I_1(t) = \int \frac{dt}{t^2 + \frac{3}{4}} = \frac{2}{\sqrt{3}} \text{ arctg } \frac{2t}{\sqrt{3}} + \mathscr{C};$$

$$I_2(t) = \int \frac{dt}{\left(t^2+\frac{3}{4}\right)^2} = \frac{4}{3}\int \frac{\frac{3}{4}}{\left(t^2+\frac{3}{4}\right)^2}dt = \frac{4}{3}\int \frac{\left(\frac{3}{4}+t^2\right)-t^2}{\left(t^2+\frac{3}{4}\right)^2}dt =$$

$$= \frac{4}{3}\cdot I_1(t) - \frac{4}{3}\int \frac{t^2}{\left(t^2+\frac{3}{4}\right)^2}dt = \frac{4}{3}\cdot\frac{2}{\sqrt{3}} \text{ arctg}\frac{2t}{\sqrt{3}} - \frac{4}{3}\int t\cdot\frac{t}{\left(t^2+\frac{3}{4}\right)^2}dt.$$

Ultima integrală la care am ajuns se calculează prin părţi, cu alegerea $u = t$, $dv = \frac{t\,dt}{\left(t^2+\frac{3}{4}\right)^2}$, de unde $du = dt$, $v = -\frac{1}{2\left(t^2+\frac{3}{4}\right)}$ şi avem:

$$\int t\cdot\frac{t}{\left(t^2+\frac{3}{4}\right)^2}dt = -\frac{t}{2\left(t^2+\frac{3}{4}\right)} + \frac{1}{2}\int\frac{dt}{t^2+\frac{3}{4}} = -\frac{t}{2\left(t^2+\frac{3}{4}\right)} + \frac{1}{2}\cdot I_1(t) =$$

$$= -\frac{1}{2\left(t^2+\frac{3}{4}\right)} + \frac{1}{\sqrt{3}} \text{ arctg}\frac{2t}{\sqrt{3}} + \mathscr{C}.$$

Revenind în variabila x, obţinem:

$$\int \frac{dx}{x^2+x+1} = \frac{2}{\sqrt{3}} \text{ arctg}\frac{2x+1}{\sqrt{3}} + \mathscr{C};$$

$$\int \frac{dx}{(x^2+x+1)^2} = \frac{8}{3\sqrt{3}} \text{ arctg}\frac{2x+1}{\sqrt{3}} - \frac{4}{3}\left(-\frac{2x+1}{4(x^2+x+1)} + \frac{1}{\sqrt{3}} \text{ arctg}\frac{2x+1}{\sqrt{3}}\right) + \mathscr{C} =$$

$$= \frac{2x+1}{3(x^2+x+1)} + \frac{4}{3\sqrt{3}} \text{ arctg}\frac{2x+1}{\sqrt{3}} + \mathscr{C}.$$

În final, integrala iniţială devine:

$$\int \frac{x^3+x^2+3x+2}{(x^2+x+1)^2}dx = \frac{1}{2}\ln(x^2+x+1) - \frac{1}{x^2+x+1} - \frac{1}{\sqrt{3}} \text{ arctg}\frac{2x+1}{\sqrt{3}} +$$

$$+\frac{2x+1}{3(x^2+x+1)}+\frac{4}{3\sqrt{3}}\operatorname{arctg}\frac{2x+1}{\sqrt{3}}+\mathscr{C}=$$

$$=\frac{2x-2}{3(x^2+x+1)}+\frac{1}{2}\ln(x^2+x+1)+\frac{1}{3\sqrt{3}}\operatorname{arctg}\frac{2x+1}{\sqrt{3}}+\mathscr{C}.$$

Aplicând acum formula Leibniz – Newton, rezultă:

$$\int_0^1\frac{x^3+x^2+3x+2}{\left(x^2+x+1\right)^2}dx=\left(\frac{2x-2}{3(x^2+x+1)}+\frac{1}{2}\ln(x^2+x+1)+\frac{1}{3\sqrt{3}}\operatorname{arctg}\frac{2x+1}{\sqrt{3}}\right)\Bigg|_0^1=$$

$$=\left(\frac{1}{2}\ln 3+\frac{1}{3\sqrt{3}}\cdot\frac{\pi}{3}\right)-\left(-\frac{2}{3}+\frac{1}{3\sqrt{3}}\cdot\frac{\pi}{6}\right)=\frac{2}{3}+\frac{1}{2}\ln 3+\frac{\pi}{18\sqrt{3}}.$$

EXERCIȚII PROPUSE

I. Calculați următoarele integrale de funcții raționale:

1. $\int\frac{dx}{x(x+1)}$, $x\in(0,\infty)$;

2. $\int_1^2\frac{dx}{x^2(x+1)}$;

3. $\int\frac{dx}{x(x+1)^2}$, $x\in(0,\infty)$;

4. $\int_1^3\frac{dx}{\left(x^2+x\right)^2}$;

5. $\int\frac{dx}{x(x^2-1)}$, $x\in(0,1)$;

6. $\int_2^3\frac{5x^3+2}{x^3-5x^2+4x}dx$;

7. $\int\frac{x^2-8x+7}{\left(x^2-3x-10\right)^2}dx$, $x\in(5,\infty)$;

8. $\int_1^2\frac{x^3-1}{4x^3-x}dx$;

9. $\int\frac{dx}{x(x^2+1)}$, $x\in(-\infty,0)$;

10. $\int_3^5\frac{x^4}{x^4-1}dx$;

11. $\int\frac{dx}{x^3+1}$, $x\in(-1,\infty)$;

12. $\int_{-1}^0\frac{dx}{x^3-1}$;

13. $\int\frac{dx}{x^4+x^2+1}$, $x\in\mathbb{R}$;

14. $\int_0^1\frac{dx}{x^4+1}$;

15. $\int\frac{dx}{x^4+4}$, $x\in\mathbb{R}$;

16. $\int_0^1\frac{dx}{\left(x^2+1\right)^2}$;

17. $\int \frac{dx}{(x+1)(x^2+x+1)^2}$, $x \in (-1, \infty)$;

18. $\int_1^2 \frac{dx}{(x^2+4x+3)(x^2+4x+5)}$;

19. $\int \frac{dx}{(x+1)^2(x^2+1)^2}$, $x \in (-1, \infty)$;

20. $\int_0^2 \frac{x^5}{(x^3+1)(x^3+8)}dx$;

21. $\int \frac{dx}{x^4(x^3+1)^2}$, $x \in (0, \infty)$;

22. $\int_{-1}^0 \frac{x^2dx}{(x-1)^{10}}$;

23. $\int \frac{dx}{x(x^7+1)}$, $x \in (0, \infty)$;

24. $\int_1^2 \frac{dx}{x(x^5+1)^2}$;

25. $\int \frac{dx}{x^8+x^6}$, $x \in (0, \infty)$.

II. Calculați integralele următoare, utilizând substituții care să le aducă la integrale din funcții raționale:

1. $\int \frac{dx}{2+\sin x}$, $x = (-\pi, \pi)$;

2. $\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \frac{dx}{2+\cos x}$;

3. $\int \frac{\cos x}{1+\cos x}dx$, $x \in (-\pi, \pi)$;

4. $\int_0^{\frac{\pi}{2}} \frac{dx}{3+\cos x+2\sin x}$;

5. $\int \frac{1+\operatorname{tg} x}{1-\operatorname{tg} x}dx$, $x \in \left(-\frac{\pi}{2}, \frac{\pi}{4}\right)$;

6. $\int_{-\frac{\pi}{4}}^{\frac{\pi}{4}} \frac{3\sin x+2\cos x}{2\sin x+3\cos x}dx$;

7. $\int_2^3 \frac{dx}{(1-x^2)\sqrt{1+x^2}}$;

8. $\int \frac{dx}{x\sqrt{x^2+x+1}}$, $x \in (0, \infty)$;

9. $\int_0^1 x\sqrt{x^2+2x+2}\, dx$;

TESTE DE EVALUARE

Testul 1

(timp de lucru - 30 minute; fiecare exercițiu se notează cu 3 puncte)

Indicați răspunsul corect.

1. $\int_1^2 \frac{dx}{x+3x^3} =$

a) $\ln 4$; b) 1; c) $\frac{1}{3}\ln 12$; d) $\frac{1}{2}\ln\frac{16}{13}$.

2. $\int_0^1 \frac{x+\sqrt{x}}{\sqrt[4]{x}+\sqrt{x}+1}dx =$

a) $3+\frac{2\pi}{\sqrt{3}}$; b) $\frac{3}{2}+\frac{\pi}{6}$; c) $3-\frac{4\pi}{3\sqrt{3}}$; d) $\ln 2-\frac{2\pi}{\sqrt{3}}$.

3. $\int_0^{\pi/4} \frac{\sin 2x}{\sin^4 x+\cos^4 x}dx =$

a) $\frac{\pi}{2}$; b) 1; c) $\frac{\pi}{4}$; d) 0.

Testul 2

(timp de lucru - 60 minute; fiecare exercițiu se notează cu 2,25 puncte)

Pentru următoarele probleme se cer soluții complete.

Calculați următoarele integrale:

1. $\int \frac{1}{x(x^{12}+1)}dx$, $x \in (0, \infty)$.

2. $\int \ln(x^2+x+1)dx$, $x \in \mathbb{R}$.

3. $\int_0^1 \frac{x^4+1}{x^6+1}dx$.

4. $\int_0^1 \frac{2x+3}{x(x+1)(x+2)(x+3)+1}dx$.

Legătura dintre unele clase remarcabile de funcții (extindere)

Dacă I este un interval arbitrar al dreptei reale, am studiat în acest manual ***clasa (mulțimea) funcțiilor care au primitive (primitivabile) pe I***, iar în cazul în care I este un interval compact, am studiat ***clasa funcțiilor integrabile*** pe intervalul I.

În clasa a XI-a ne-am ocupat de ***funcțiile continue*** pe intervalul I, precum și de ***funcțiile cu proprietatea lui Darboux*** definite pe intervalul I. Reamintim că funcțiile cu proprietatea lui Darboux sunt acele funcții care transformă orice subinterval al lui I într-un interval (eventual redus la un punct).

Reamintim câteva rezultate pe care le-am stabilit relativ la aceste clase de funcții.

Teoremă (Bolzano)

Dacă $f : I \to \mathbb{R}$ este continuă, atunci f are proprietatea lui Darboux.

Teoremă (Darboux)

Dacă $f : I \to \mathbb{R}$ este derivabilă, atunci derivata f' are proprietatea lui Darboux.

Teoremă

Dacă $f : I \to \mathbb{R}$ este continuă, atunci f are primitive.

Teoremă

Dacă $f : I \to \mathbb{R}$ este continuă, atunci f este integrabilă.

Rezultatul care urmează arată că o condiție ***necesară ca o funcție să aibă primitive este să aibă proprietatea lui Darboux.***

Propoziție

Dacă $f : I \to \mathbb{R}$ are primitive, atunci f are proprietatea lui Darboux.

Demonstrație. Fie $F : I \to \mathbb{R}$ o primitivă pentru f, adică $f = F'$. Conform teoremei lui Darboux, funcția F' are proprietatea lui Darboux. Rezultă că $f = F'$ are această proprietate.

Observaţie

O exprimare echivalentă a propoziţiei precedente este următoarea:
Dacă $f : I \to \mathbb{R}$ nu are proprietatea lui Darboux, atunci f nu are primitive.

Aşadar, ***absenţa proprietăţii lui Darboux este o condiţie suficientă pentru ca o funcţie să nu aibă primitive***.

Mai reamintim că ***o funcţie $f : I \to \mathbb{R}$ care are o discontinuitate de speţa întâi nu are proprietatea lui Darboux*** şi prin urmare ***o astfel de funcţie nu are primitive***.

Un rezultat simplu, util în cele ce urmează, este următoarea:

Propoziţie

Dacă $f : I \to \mathbb{R}$ are primitive, iar $g : I \to \mathbb{R}$ nu are primitive, atunci suma $f + g : I \to \mathbb{R}$ nu are primitive.

(Altfel spus: suma dintre o funcţie cu primitive şi o funcţie fără primitive este o funcţie fără primitive).

Demonstraţie. Să notăm $h = f + g$. Dacă, prin absurd, h ar avea primitive, ar însemna că $g = h - f$ are primitive, contradicţie.

Din cele relatate, rezultă că pentru o funcţie $f : I \to \mathbb{R}$, I fiind un interval arbitrar, sunt adevărate implicaţiile:

$$f \text{ continuă} \Rightarrow f \text{ are primitive} \Rightarrow f \text{ are proprietatea lui Darboux.}$$

Dacă notăm cu $\mathscr{C}(I)$ mulţimea funcţiilor continue pe I, cu $\mathscr{P}(I)$ mulţimea funcţiilor primitivabile pe I şi cu $\mathscr{D}a(I)$ mulţimea funcţiilor cu proprietatea lui Darboux pe I, implicaţiilor de mai sus le corespund incluziunile:

$$\mathscr{C}(I) \subseteq \mathscr{P}(I) \subseteq \mathscr{D}a(I).$$

Vom arăta că incluziunile respective sunt stricte, adică vom da exemple de funcţii care aparţin diferenţelor $\mathscr{P}(I) \setminus \mathscr{C}(I)$ şi $\mathscr{D}a(I) \setminus \mathscr{P}(I)$.

Exemplu de funcţie cu primitive care nu e continuă

Să considerăm funcţia:

$$f : \mathbb{R} \to \mathbb{R},\ f(x) = \begin{cases} \sin\dfrac{1}{x}, & x \neq 0 \\ 0, & x = 0 \end{cases}$$

Vom arăta că această funcţie are primitive, dar nu e continuă. Mai întâi este limpede că funcţia f nu este continuă în origine, întrucât nu are limită în zero,

Pentru a arăta că f are primitive, procedăm în trei „paşi":

Pasul 1. Considerăm funcția $G : \mathbb{R} \to \mathbb{R}$, $G(x) = \begin{cases} x^2 \cos\frac{1}{x}, & x \neq 0 \\ 0, & x = 0 \end{cases}$

Această funcție este derivabilă pe $\mathbb{R}$, căci pe $\mathbb{R} \setminus \{0\}$ e clar, iar în punctul 0 avem:

$$G'(0) = \lim_{x\to 0} \frac{G(x) - G(0)}{x - 0} = \lim_{x\to 0} \frac{x^2 \cos\frac{1}{x}}{x} = \lim_{x\to 0} x\cos\frac{1}{x} = 0$$

(ultima limită se poate justifica astfel: $\left|x\cos\frac{1}{x}\right| \leq |x| \xrightarrow{x\to 0} 0$ și se aplică criteriul majorării).

Pasul 2. Considerăm funcția $g : \mathbb{R} \to \mathbb{R}$, $g = G'$, adică:

$$g(x) = \begin{cases} \left(x^2 \cos\frac{1}{x}\right)', & x \neq 0 \\ G'(0), & x = 0 \end{cases} = \begin{cases} 2x\cos\frac{1}{x} + x^2\left(-\sin\frac{1}{x}\right)\left(-\frac{1}{x^2}\right), & x \neq 0 \\ 0, & x = 0 \end{cases} =$$

$$= \begin{cases} 2x\cos\frac{1}{x} + \sin\frac{1}{x}, & x \neq 0 \\ 0, & x = 0 \end{cases} = \begin{cases} 2x\cos\frac{1}{x}, & x \neq 0 \\ 0, & x = 0 \end{cases} + \begin{cases} \sin\frac{1}{x}, & x \neq 0 \\ 0, & x = 0 \end{cases} = h(x) + f(x),$$

unde $h : \mathbb{R} \to \mathbb{R}$, $h(x) = \begin{cases} 2x\cos\frac{1}{x}, & x \neq 0 \\ 0, & x = 0 \end{cases}$.

Observăm ușor că funcția h e continuă pe $\mathbb{R}$, căci pe $\mathbb{R} \setminus \{0\}$ e clar, iar în punctul 0 avem $\lim_{x\to 0} h(x) = \lim_{x\to 0} 2x\cos\frac{1}{x} = 0 = h(0)$.

Pasul 3. Din egalitatea de la pasul 2, obținem $f = g - h$. Funcția g are primitive (de exemplu, G este primitivă a funcției g) și funcția h are primitive (deoarece este continuă). Deducem că funcția – diferență $f = g - h$ are primitive.

Comentariu metodic

Ideea considerării funcției G de la pasul 1 din exemplul precedent și a derivatei acesteia $g = G'$ de la pasul 2, vine din aceea că atunci când vrem să calculăm $\int \sin\frac{1}{x}dx$ pe un interval $I \subseteq \mathbb{R}^*$, putem integra prin părți, astfel:

$$\int f(x)dx = \int \sin\frac{1}{x}dx = \int x^2 \cdot \frac{1}{x^2}\sin\frac{1}{x}dx = \int x^2 d\left(\cos\frac{1}{x}\right) =$$

$$= x^2\cos\frac{1}{x} - \int \cos\frac{1}{x}d(x^2) = x^2\cos\frac{1}{x} - \int 2x\cos\frac{1}{x}dx = G(x) - \int h(x)dx,$$

de unde, prin derivare, $f = g - h$.

Dacă intervalul I conține și originea, atunci vom prelungi în origine aceste funcții cu valoarea zero.

Complet analog rezultă că funcția:

$$f : \mathbb{R} \to \mathbb{R},\ f(x) = \begin{cases} \cos\frac{1}{x}, & x \neq 0 \\ 0, & x = 0 \end{cases}$$

are primitive și nu este continuă.

Exemplu de funcție cu proprietatea lui Darboux care nu are primitive

Să considerăm funcția $f : \mathbb{R} \to \mathbb{R},\ f(x) = \begin{cases} \sin\frac{1}{x}, & x \neq 0 \\ \alpha, & x = 0 \end{cases}$ cu $\alpha \in [-1, 1] \setminus \{0\}$.

Această funcție are proprietatea lui Darboux întrucât transformă orice interval $I \subseteq \mathbb{R}^*$ într-un interval (deoarece restricțiile lui f la $(-\infty, 0)$ și $(0, \infty)$ sunt funcții continue) și transformă orice interval I care conține pe 0 în $[-1, 1]$. Arătăm că funcția f nu are primitive. Într-adevăr:

$$f(x) = \begin{cases} \sin\frac{1}{x}, & x \neq 0 \\ 0, & x = 0 \end{cases} + \begin{cases} 0, & x \neq 0 \\ \alpha, & x = 0 \end{cases}$$

și în această sumă prima funcție are primitive, iar a doua funcție nu are primitive (neavând proprietatea lui Darboux). Deoarece suma dintre o funcție cu primitive și una fără primitive este o funcție fără primitive, deducem că f nu are primitive.

Dacă intervalul I este un interval compact, adică $I = [a, b]$, putem lua în considerare și clasa funcțiilor integrabile pe acest interval, pe care o vom nota $\mathscr{I}([a, b])$.

Dacă $f : [a, b] \to \mathbb{R}$, am văzut că este adevărată implicația:

$$f \text{ continuă} \Rightarrow f \text{ integrabilă}.$$

care se traduce corespunzător prin incluziunea:

$$\mathscr{C}([a. b]) \subseteq \mathscr{I}([a, b]).$$

Și această incluziune este strictă, întrucât există funcții discontinue care sunt integrabile, de exemplu funcțiile mărginite cu un număr finit de discontinuități.

Dacă facem comparație între clasele de funcții $\mathscr{I}([a, b])$ și $\mathscr{P}([a, b])$, respectiv $\mathscr{I}([a\ b])$ și $\mathscr{D}a([a\ ,b])$, lucrurile se prezintă astfel:

$\mathscr{I}([a\ b]) \cap \mathscr{P}([a, b]) \neq \varnothing$, $\mathscr{I}([a\ b]) \not\subseteq \mathscr{P}([a, b])$, $\mathscr{P}([a, b]) \not\subseteq \mathscr{I}([a\ b])$,

$\mathscr{I}([a\ b]) \cap \mathscr{D}a([a\ ,b]) \neq \varnothing$, $\mathscr{I}([a\ b]) \not\subseteq \mathscr{D}a([a\ ,b])$, $\mathscr{D}a([a\ ,b]) \not\subseteq \mathscr{I}([a\ b])$.

Dăm acum exemple de funcții aparținând diferențelor de mulțimi în care apare $\mathscr{I}([a\ b])$.

Exemplu de funcție integrabilă care nu are primitive

Funcția $f : [0, 1] \to \mathbb{R}$, $f(x) = [x]$ este integrabilă şi nu are primitive.

Într-adevăr, funcția dată diferă într-un singur punct ($x = 1$) de funcția constantă nulă, prin urmare este integrabilă în baza propoziției de la pag. 169. Dar, putem scrie:

$$f(x)=\begin{cases}0, & x\in[0,1)\\ 1, & x=1\end{cases}$$

ceea ce arată că $f([0, 1]) = \{0, 1\}$, deci $f([0, 1])$ nu este un interval; înseamnă că f nu are proprietatea lui Darboux şi în consecință nu are primitive.

Totodată, acesta este un exemplu de *funcție integrabilă care nu are proprietatea lui Darboux.*

Mai general, orice funcție $f : [a, b] \to \mathbb{R}$ care este mărginită şi are un număr finit de discontinuități, toate de speța întâi, este integrabilă şi nu are primitive.

Exemplu de funcție cu primitive care nu este integrabilă

Să considerăm funcția $F : [0, 1] \to \mathbb{R}$, $F(x)=\begin{cases}x^2\sin\dfrac{1}{x^2}, & x\in(0,1]\\ 0, & x=0\end{cases}$.

Este uşor de văzut că funcția F este derivabilă şi are derivata $f : [0, 1] \to \mathbb{R}$, $f(x)=\begin{cases}2x\sin\dfrac{1}{x^2}-\dfrac{2}{x}\cos\dfrac{1}{x^2}, & x\in(0,1]\\ 0, & x=0\end{cases}$. E clar că $\lim\limits_{n\to\infty} f\left(\dfrac{1}{\sqrt{2n\pi}}\right)=\lim\limits_{n\to\infty}\left(-2\sqrt{2n\pi}\right)=-\infty$, ceea ce înseamnă că funcția f este nemărginită. Aşadar funcția f are primitive (de exemplu, pe F), dar nu este integrabilă (fiind nemărginită).

Totodată, acesta este un exemplu de *funcție cu proprietatea lui Darboux care nu este integrabilă.*

Exerciții rezolvate

1. Care din următoarele funcții $f : \mathbb{R} \to \mathbb{R}$ au primitive?

a) $f(x)=\begin{cases}\dfrac{\sin x}{x}, & x\neq 0\\ 1, & x=0\end{cases}$;

c) $f(x)=\begin{cases}\sin\dfrac{1}{x}, & x\neq 0\\ \dfrac{\pi}{4}, & x=0\end{cases}$;

b) $f(x)=\begin{cases}\dfrac{\sin x}{x}, & x\neq 0\\ 0, & x=0\end{cases}$;

d) $f(x)=\begin{cases}x, & x\in\mathbb{Q}\\ x^2, & x\in\mathbb{R}\setminus\mathbb{Q}\end{cases}$.

Soluție. **a)** Funcția f este continuă pe $\mathbb{R}$, deci are primitive.

b) Avem $f(x)=\begin{cases}\dfrac{\sin x}{x}, & x\neq 0\\ 1, & x=0\end{cases}+\begin{cases}0, & x\neq 0\\ -1, & x=0\end{cases}$ și în această sumă prima funcție are primitive (fiind continuă), în timp ce a doua funcție nu are primitive (neavând proprietatea lui Darboux). Deducem că suma nu are primitive, deci funcția f nu are primitive. Putem argumenta și astfel: $\lim\limits_{x\to 0} f(x) = 1 \neq f(0)$, deci f are o discontinuitate de speța întâi, prin urmare nu are proprietatea lui Darboux și deci nu are primitive.

c) Avem $f(x)=\begin{cases}\sin\dfrac{1}{x}, & x\neq 0\\ 0, & x=0\end{cases}+\begin{cases}0, & x\neq 0\\ \dfrac{\pi}{4}, & x=0\end{cases}$ și în această sumă prima funcție are primitive, în timp ce a doua funcție nu are primitive (neavând proprietatea lui Darboux). Deducem că funcția – sumă f nu are primitive.

d) Să considerăm intervalul $I = [2, 3]$. Dacă $x \in I \cap \mathbb{Q}$, avem $f(x) = x \in [2, 3]$, iar dacă $x \in I \cap (\mathbb{R} \setminus \mathbb{Q})$ avem $f(x)=x^2 \in [4, 9]$. Prin urmare $f(I) \subseteq [2, 3] \cup [4, 9]$ și $f(I) \cap [2, 3] \neq \emptyset$, $f(I) \cap [4, 9] \neq \emptyset$, ceea ce înseamnă că $f(I)$ nu este un interval.

Deducem că funcția f nu are proprietatea lui Darboux, deci nu are primitive.

2. Care din următoarele funcții $f : [0, 1] \to \mathbb{R}$ sunt integrabile?

a) $f(x)=\begin{cases}\dfrac{\operatorname{tg} x}{x}, & x\in(0, 1]\\ 1, & x=0\end{cases}$; **b)** $f(x)=\begin{cases}\dfrac{1}{x}, & x\in(0, 1]\\ 1, & x=0\end{cases}$;

c) $f(x)=\begin{cases}1, & x\in[0, 1]\cap\mathbb{Q}\\ 0, & x\in[0, 1]\cap(\mathbb{R}\setminus\mathbb{Q})\end{cases}$.

Soluție. **a)** Funcția f este continuă pe $[0, 1]$, deci este integrabilă.

b) Deoarece $\lim\limits_{x\searrow 0} f(x) = \lim\limits_{x\searrow 0} \dfrac{1}{x} = +\infty$, deducem că funcția f este nemărginită, prin urmare nu este integrabilă.

c) Fie $\Delta = (0 = x_0, x_1, x_2, \dots, x_n = 1)$ o diviziune oarecare a intervalului $[0, 1]$, iar ξ un sistem de puncte intermediare asociat. Dacă ξ conține doar puncte raționale, suma Riemann corespunzătoare este:

$$\sigma(f, \Delta, \xi) = \sum_{i=1}^{n} f(\xi_i)(x_i - x_{i-1}) = \sum_{i=1}^{n}(x_i - x_{i-1}) = x_n - x_0 = 1.$$

Dacă ξ conține doar puncte iraționale, suma Riemann corespunzătoare este:

$$\sigma(f, \Delta, \xi) = \sum_{i=1}^{n} f(\xi_i)(x_i - x_{i-1}) = 0.$$

În concluzie, nu există limita $\lim\limits_{\|\Delta\|\to 0} \sigma(f, \Delta, \xi)$, prin urmare funcția f nu este integrabilă.

EXERCIȚII PROPUSE

I. Arătați că funcțiile următoare au primitive:

1. $f:\mathbb{R}\to\mathbb{R},\ f(x)=\begin{cases}|x|\sin\frac{1}{x}, & x\neq 0\\ 0, & x=0\end{cases}$; **2.** $f:\mathbb{R}\to\mathbb{R},\ f(x)=\begin{cases}|x|\cos\frac{1}{x}, & x\neq 0\\ 0, & x=0\end{cases}$

3. $f:\mathbb{R}\to\mathbb{R},\ f(x)=\begin{cases}\sin\frac{\alpha}{x}, & x\neq 0\\ 0, & x=0\end{cases}$, unde $\alpha\in\mathbb{R}$ este fixat.

4. $f:\mathbb{R}\to\mathbb{R},\ f(x)=\begin{cases}\cos\frac{\alpha}{x}, & x\neq 0\\ 0, & x=0\end{cases}$, unde $\alpha\in\mathbb{R}\setminus\{0\}$ este fixat.

5. $f:\mathbb{R}\to\mathbb{R},\ f(x)=\begin{cases}\sin\frac{\alpha}{x}\sin\frac{\beta}{x}, & x\neq 0\\ 0, & x=0\end{cases}$, unde $\alpha,\beta\in\mathbb{R}$ sunt fixate, $|\alpha|\neq|\beta|$.

6. $f:\mathbb{R}\to\mathbb{R},\ f(x)=\begin{cases}\cos\frac{\alpha}{x}\cos\frac{\beta}{x}, & x\neq 0\\ 0, & x=0\end{cases}$, unde $\alpha,\beta\in\mathbb{R}\setminus\{0\}$ sunt fixate, $|\alpha|\neq|\beta|$.

7. $f:\mathbb{R}\to\mathbb{R},\ f(x)=\begin{cases}\sin\frac{\alpha}{x}\cos\frac{\beta}{x}, & x\neq 0\\ 0, & x=0\end{cases}$, unde $\alpha\in\mathbb{R}$, $\beta\in\mathbb{R}\setminus\{0\}$ sunt fixate.

II. Arătați că funcțiile următoare nu au primitive:

1. $f:\mathbb{R}\to\mathbb{R}$, $f(x)=[x]$ (funcția „parte întreagă”).

2. $f:\mathbb{R}\to\mathbb{R}$, $f(x)=\{x\}$ (funcția „parte fracționară”).

3. $f:\mathbb{R}\to\mathbb{R},\ f(x)=\begin{cases}\sin\frac{1}{x}, & x\neq 0\\ \lambda, & x=0\end{cases}$, unde $\lambda\in\mathbb{R}\setminus\{0\}$.

4. $f:\mathbb{R}\to\mathbb{R},\ f(x)=\begin{cases}\cos\frac{1}{x}, & x\neq 0\\ \lambda, & x=0\end{cases}$, unde $\lambda\in\mathbb{R}\setminus\{0\}$.

5. $f:\mathbb{R}\to\mathbb{R},\ f(x)=\begin{cases}\sin^2\frac{1}{x}, & x\neq 0\\ 0, & x=0\end{cases}$

6. $f:\mathbb{R}\to\mathbb{R},\ f(x)=\begin{cases}\cos^2\frac{1}{x}, & x\neq 0\\ 0, & x=0\end{cases}$

APLICAȚII ALE INTEGRALEI DEFINITE

Aria unei suprafețe plane

Vom defini conceptul de *arie* pentru o suprafață plană în general, după care *vom arăta cum se calculează aria* în anumite situații, *utilizând conceptul de integrală*.

În geometria elementară am văzut cum se calculează aria pentru unele suprafețe plane asociate unor poligoane convexe: triunghi, paralelogram, trapez. În general, putem calcula aria unei suprafețe asociate unui poligon convex ca sumă a ariilor unor triunghiuri în care se descompune acel poligon.

Această idee se extinde imediat prin următoarea:

Definiție

1) Numim *suprafață poligonală* regiunea din plan cuprinsă între laturile unui poligon oarecare (inclusiv linia poligonală) sau o reuniune finită de asemenea regiuni.

2) Dacă P este o suprafață poligonală, aria sa $\mathscr{A}(P)$ este suma ariilor triunghiurilor în care se descompune suprafața poligonală P (care nu depinde de descompunerea aleasă).

Observație

Dacă P și Q sunt suprafețe poligonale astfel încât $P \subseteq Q$, atunci $\mathscr{A}(P) \leq \mathscr{A}(Q)$.

Acest lucru rezultă din aceea că există o descompunere în triunghiuri a suprafeței Q care conține toate triunghiurile din descompunerea suprafeței P (și pe lângă aceasta, mai poate conține eventual și altele).

Să fixăm acum o suprafață plană arbitrară S, care este *mărginită*, adică poate fi inclusă într-un anumit pătrat.

Considerăm mulțimea tuturor suprafețelor poligonale incluse în S, adică:

$$\mathscr{P} = \{P \mid P = \text{suprafață poligonală, } P \subseteq S\}$$

precum și mulțimea tuturor suprafețelor poligonale care includ pe S, adică

$$\mathscr{Q} = \{Q \mid Q = \text{suprafață poligonală, } Q \supseteq S\}.$$

Evident, pentru orice suprafață poligonală $P \in \mathscr{P}$ și oricare suprafață poligonală $Q \in \mathscr{Q}$ avem $P \subseteq Q$, deci $\mathscr{A}(P) \leq \mathscr{A}(Q)$.

Rezultă că mulțimea $\{\mathscr{A}(P) \mid P \in \mathscr{P}\}$ este mărginită superior, căci orice $\mathscr{A}(Q)$ cu $Q \in \mathscr{Q}$ este un majorant pentru această mulțime.

Analog, mulțimea $\{\mathscr{A}(Q) \mid Q \in \mathscr{Q}\}$ este mărginită inferior, căci orice $\mathscr{A}(P)$ cu $P \in \mathscr{P}$ este un minorant pentru această mulțime.

Putem atunci considera numerele reale:

$$\mathscr{A}_*(S) = \sup\{\mathscr{A}(P) \mid P \in \mathscr{P}\}; \quad \mathscr{A}^*(S) = \inf\{\mathscr{A}(Q) \mid Q \in \mathscr{Q}\}$$

numite ***aria interioară***, respectiv ***aria exterioară*** ale suprafeței S.

Avem imediat următoarea:

Propoziție

Cu notațiile anterioare, avem: $\mathscr{A}_*(S) \le \mathscr{A}^*(S)$.

Demonstrație. Fie $P \in \mathscr{P}$. Deoarece $\mathscr{A}(P) \le \mathscr{A}(Q)$, $\forall\, Q \in \mathscr{Q}$, rezultă că $\mathscr{A}(P)$ este un minorant pentru mulțimea $\{\mathscr{A}(Q) \mid Q \in \mathscr{Q}\}$; însă $\mathscr{A}^*(S)$ este cel mai mare minorant pentru această mulțime, prin urmare $\mathscr{A}(P) \le \mathscr{A}^*(S)$. Cum $P \in \mathscr{P}$ a fort arbitrar, deducem că $\mathscr{A}^*(S)$ este un majorant pentru mulțimea $\{\mathscr{A}(P) \mid P \in \mathscr{P}\}$; însă $\mathscr{A}_*(S)$ este cel mai mic majorant pentru această mulțime prin urmare $\mathscr{A}_*(S) \le \mathscr{A}^*(S)$.

Introducem acum conceptul general de arie prin următoarea:

Definiție

Spunem că o suprafață plană mărginită S ***are arie*** dacă aria interioară și aria exterioară ale suprafeței S sunt egale, iar în acest caz ***aria*** lui S este prin definiție valoarea comună a celor două arii, adică:

$$\mathscr{A}(S) = \mathscr{A}_*(S) = \mathscr{A}^*(S).$$

Următorul rezultat stabilește o caracterizare a mulțimilor care au arie și totodată un mod de a calcula aria ca limită a unui șir de arii de suprafețe poligonale.

Teoremă

Fie S o suprafață plană mărginită. Următoarele afirmații sunt echivalente:

1°. Suprafața S are arie.

2°. Există un șir $(P_n)_{n\ge1}$ de suprafețe poligoanele incluse în S și un șir $(Q_n)_{n\ge1}$ de suprafețe poligonale care includ pe S, astfel încât:

$$\lim_{n\to\infty} \mathscr{A}(P_n) = \lim_{n\to\infty} \mathscr{A}(Q_n).$$

Valoarea comună a acestor limite este tocmai aria suprafeței S.

Demonstrație. 1° $\Rightarrow$ 2°. Presupunem că suprafața S are arie, adică:

$$\mathscr{A}(S) = \mathscr{A}_*(S) = \mathscr{A}^*(S).$$

Din aceea că $\mathscr{A}(S) = \mathscr{A}_*(S) =$ cel mai mic majorant pentru $\{\mathscr{A}(P) \mid P \in \mathscr{P}\}$, înseamnă că pentru orice $n \in \mathbb{N}^*$, numărul $\mathscr{A}(S) - \dfrac{1}{n}$ nu mai este majorant pentru mulțimea în cauză, deci există $P_n \in \mathscr{P}$ cu $\mathscr{A}(S) - \dfrac{1}{n} < \mathscr{A}(P_n)$.

Din aceea că $\mathscr{A}(S) = \mathscr{A}^*(S)$ = cel mai mare minorant pentru $\{\mathscr{A}(Q) \mid Q \in \mathscr{Q}\}$, înseamnă că pentru orice $n \in \mathbb{N}^*$, numărul $\mathscr{A}(S) + \frac{1}{n}$ nu mai este minorant, deci există $Q_n \in \mathscr{Q}$ cu $\mathscr{A}(S) + \frac{1}{n} > \mathscr{A}(Q_n)$. Aşadar:

$$\mathscr{A}(S) - \frac{1}{n} < \mathscr{A}(P_n) \le \mathscr{A}(Q_n) < \mathscr{A}(S) + \frac{1}{n},\ \forall\, n \in \mathbb{N}^*.$$

Aplicând criteriul cleştelui, rezultă $\lim\limits_{n\to\infty} \mathscr{A}(P_n) = \lim\limits_{n\to\infty} \mathscr{A}(Q_n) = \mathscr{A}(S)$.

$2° \Rightarrow 1°$. Presupunem că există două şiruri $(P_n)_{n\ge1} \subseteq \mathscr{P}$ şi $(Q_n)_{n\ge1} \subseteq \mathscr{Q}$ astfel încât $\lim\limits_{n\to\infty} \mathscr{A}(P_n) = \lim\limits_{n\to\infty} \mathscr{A}(Q_n)$ şi fie L valoarea comună a acestor două limite. Arătăm că $L = \mathscr{A}_*(S)$ şi $L = \mathscr{A}^*(S)$, de unde va rezulta că $\mathscr{A}_*(S) = \mathscr{A}^*(S)$, adică suprafaţa S are arie.

Deoarece pentru $P \in \mathscr{P}$ avem $\mathscr{A}(P) \le \mathscr{A}(Q_n)$, $\forall\, n \in \mathbb{N}^*$, rezultă $\mathscr{A}(P) \le \le \lim\limits_{n\to\infty} \mathscr{A}(Q_n)$, adică $\mathscr{A}(P) \le L$. Aşadar, L este un majorant pentru mulţimea $\{\mathscr{A}(P) \mid P \in \mathscr{P}\}$.

Să dovedim acum că L este cel mai mic majorant pentru această mulţime, adică $L - \varepsilon$ nu mai este majorant, pentru orice $\varepsilon > 0$. Într-adevăr, deoarece $\lim\limits_{n\to\infty} \mathscr{A}(P_n) = L$, înseamnă că $\forall\, \varepsilon > 0$, $\exists\, n \in \mathbb{N}^*$ astfel încât $\forall\, n \ge n_\varepsilon \Rightarrow |\mathscr{A}(P_n) - L| < \varepsilon$, adică $L - \mathscr{A}(P_n) < \varepsilon$ sau $L - \varepsilon < \mathscr{A}(P_n)$, ceea ce arată că $L - \varepsilon$ nu mai este majorant. Cele probate arată că

$$L = \sup\{\mathscr{A}(P) \mid P \in \mathscr{P}\} = \mathscr{A}_*(S).$$

Analog se arată că $L = \mathscr{A}^*(S)$.

Reţinem în final egalităţile:

$$L = \mathscr{A}_*(S) = \mathscr{A}^*(S), \text{ deci } L = \mathscr{A}(S),$$

adică aria suprafeţei S este egală cu valoarea comună a limitelor celor două şiruri de arii de suprafeţe poligonale.

Observaţie

Rezultă imediat că aria este „aditivă”, mai precis: dacă S_1, S_2 sunt suprafeţe plane mărginite care nu au puncte interioare comune, iar $S = S_1 \cup S_2$, atunci din aceea că două din suprafeţele S_1, S_2, S au arie rezultă că şi cea de-a treia are arie şi avem egalitatea $\mathscr{A}(S) = \mathscr{A}(S_1) + \mathscr{A}(S_2)$.

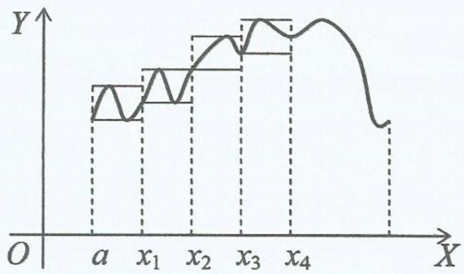
După această fundamentare a conceptului de arie, să ne întoarcem acum la problema cu care am început partea de analiză a acestui manual, adică problema determinării ariei unui trapez curbiliniu.

Vom vedea că această arie se exprimă printr-o integrală. Avem în acest sens următorul rezultat important:

Teoremă

Fie $f : [a, b] \to \mathbb{R}$ o funcție continuă și pozitivă. Trapezul curbiliniu S delimitat de graficul funcției f, axa OX și dreptele de ecuații $x = a$, $x = b$, are arie și aceasta este dată de formula:

$$\mathscr{A}(S) = \int_a^b f(x)dx.$$



Demonstrație. Pentru fiecare $n \in \mathbb{N}^*$ considerăm diviziunea Δ_n a intervalului $[a, b]$ care împarte acest interval în n intervale de lungimi egale, prin punctele de diviziune.

$$x_i^{(n)} = a + \frac{i(b-a)}{n}, \quad i = \overline{0, n}.$$

Notăm cu $m_i^{(n)}$, $M_i^{(n)}$ minimul, respectiv maximul funcției f pe intervalul de diviziune $\left[x_{i-1}^{(n)}, x_i^{(n)}\right]$, $i = \overline{1, n}$.

Reuniunea dreptunghiurilor de baze segmentele $\left[x_{i-1}^{(n)}, x_i^{(n)}\right]$ și înălțimi $m_i^{(n)}$, $i = \overline{1, n}$ este o suprafață poligonală P_n inclusă în S, care are aria:

$$\mathscr{A}(P_n) = \sum_{i=1}^{n} m_i^{(n)}\left(x_i^{(n)} - x_{i-1}^{(n)}\right) = s(f, \Delta_n),$$

adică suma Darboux inferioară corespunzătoare funcției f și diviziunii Δ_n.

Reuniunea dreptunghiurilor de baze segmentele $\left[x_{i-1}^{(n)}, x_i^{(n)}\right]$ și înălțimi $M_i^{(n)}$, $i = \overline{1, n}$ este o suprafață poligonală Q_n care include S și are aria:

$$\mathscr{A}(Q_n) = \sum_{i=1}^{n} M_i^{(n)}\left(x_i^{(n)} - x_{i-1}^{(n)}\right) = S(f, \Delta_n),$$

adică suma Darboux superioară corespunzătoare funcției f și diviziunii Δ_n.

Dar $\| \Delta_n \| = \dfrac{b-a}{n} \to 0$ și cum sumele Darboux sunt niște sume Riemann (căci funcția f este continuă) rezultă:

$$\lim_{n\to\infty} \mathscr{A}(P_n) = \lim_{n\to\infty} s(f, \Delta_n) = \int_a^b f(x)dx;$$

$$\lim_{n\to\infty} \mathscr{A}(Q_n) = \lim_{n\to\infty} S(f, \Delta_n) = \int_a^b f(x)dx.$$

Conform teoremei precedente, rezultă că suprafața S are arie și aceasta este:

$$\mathscr{A}(S) = \lim_{n\to\infty} \mathscr{A}(P_n) = \lim_{n\to\infty} \mathscr{A}(Q_n) = \int_a^b f(x)dx.$$

Observație (interpretarea geometrică a teoremei de medie)

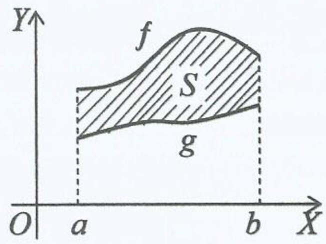
Din teorema anterioară și teorema de medie, care afirmă egalitatea $\int_a^b f(x)dx =$ $= (b - a)f(c)$ pentru un $c \in [a, b]$, deducem că aria trapezului curbiliniu considerat este egală cu aria unui dreptunghi cu baza intervalul $[a, b]$ și înălțime $f(c)$.

Consecință

Fie $f, g : [a, b] \to \mathbb{R}$ două funcții continue cu proprietatea că $f(x) \geq g(x)$ pentru orice $x \in [a, b]$. Suprafața plană S delimitată de graficele celor două funcții și dreptele de ecuații $x = a$, $x = b$, are arie și aceasta este dată de formula:

$$\mathscr{A}(S) = \int_a^b (f(x) - g(x))\,dx.$$

Demonstrație. Tratăm două cazuri, complementare logic.



I. $g(x) \geq 0$, $\forall\, x \in [a, b]$. Atunci funcțiile f și g sunt pozitive, mai precis $f(x) \geq g(x) \geq 0$, $\forall\, x \in [a, b]$. Rezultă că aria suprafeței S este diferența dintre ariile a două trapeze curbilinii: cel corespunzător graficului lui f și cel corespunzător graficului lui g (am folosit aditivitatea ariei). Aplicând teorema, rezultă:

$$\mathscr{A}(S) = \int_a^b f(x)dx - \int_a^b g(x)dx = \int_a^b (f(x) - g(x))\,dx.$$

II. $\exists\, x_0 \in [a, b]$ cu $g(x_0) < 0$. Funcția g fiind continuă pe intervalul compact $[a, b]$, este mărginită. Deci există $\lambda \in \mathbb{R}$ astfel încât $g(x) \geq \lambda$, $\forall\, x \in [a, b]$. Considerăm atunci funcțiile $f_1, g_1 : [a, b] \to \mathbb{R}$, $f_1(x) = f(x) - \lambda$, $g_1(x) = g(x) - \lambda$ și avem $f_1(x) \geq$ $\geq g_1(x) \geq 0$, $\forall\, x \in [a, b]$. Deoarece graficele lui f_1 și g_1 se obțin din cele ale lui f, respectiv g printr-o translație de direcția axei OY, rezultă că suprafața S_1 delimitată de graficele lui f_1, g_1 și dreptele $x = a$, $x = b$ este echivalentă (are aceeași arie) cu suprafața S.

Dar aria lui S_1 se calculează conform cazului I). Așadar:

$$\mathscr{A}(S) = \mathscr{A}(S_1) = \int_a^b (f_1(x) - g_1(x))\,dx = \int_a^b (f(x) - \lambda - g(x) + \lambda)\,dx = \int_a^b (f(x) - g(x))\,dx.$$

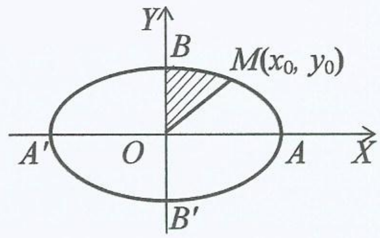
Exercițiu rezolvat

Considerăm elipsa de ecuație $\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$ având axa mare $AA'=2a$ şi axa mică $BB'=2b$ $(a>0, b>0)$.

a) Dacă $M(x_0, y_0)$ este un punct al elipsei $(x_0 > 0,\ y_0 \geq 0)$, să se afle aria suprafeței plane delimitate de curbele de ecuații $x=0,\ xy_0=x_0y,\ y=\frac{b}{a}\sqrt{a^2-x^2}$.

b) Să se deducă aria elipsei şi în particular, aria cercului.

Soluție. **a)** Din ecuația elipsei deducem $y=\pm\frac{b}{a}\sqrt{a^2-x^2}$, ceea ce arată că elipsa este reuniunea graficelor a două funcții opuse şi anume $f: [-a, a] \to \mathbb{R},\ f(x)=\frac{b}{a}\sqrt{a^2-x^2}$ şi $-f: [-a, a] \to \mathbb{R},\ (-f)(x)=-\frac{b}{a}\sqrt{a^2-x^2}$. Arcul mic al elipsei BM este inclus în graficul funcției pozitive f, iar segmentul OM este inclus în dreapta de ecuație $xy_0=x_0y$. Prin urmare suprafața în cauză este triunghiul curbiliniu OBM şi are aria:



$$\mathcal{A}_{(OBM)}=\int_0^{x_0}\left(f(x)-\frac{y_0}{x_0}x\right)dx=\frac{b}{a}\int_0^{x_0}\sqrt{a^2-x^2}dx-\frac{x_0y_0}{2}.$$

Calculăm integrala rămasă cu substituția $x=a\sin t,\ t\in\left[-\frac{\pi}{2},\frac{\pi}{2}\right]$. Avem $dx=a\cos t\,dt,\ x=0\Rightarrow t=0,\ \ x=x_0\Rightarrow t_0=\arcsin\frac{x_0}{a}$. Rezultă:

$$\int_0^{x_0}\sqrt{a^2-x^2}\,dx=\int_0^{t_0}\sqrt{a^2(1-\sin^2 t)}\cdot a\cos t\,dt=a^2\int_0^{t_0}\cos^2 t\,dt=\frac{a^2}{2}\int_0^{t_0}(1+\cos 2t)dt=$$

$$=\frac{a^2}{2}\left(t+\frac{1}{2}\sin 2t\right)\Bigg|_0^{t_0}=\frac{a^2}{2}(t_0+\sin t_0\cos t_0)=\frac{a^2}{2}\left(\arcsin\frac{x_0}{a}+\frac{x_0}{a}\cdot\sqrt{1-\frac{x_0^2}{a^2}}\right)=$$

$$=\frac{a^2}{2}\arcsin\frac{x_0}{a}+\frac{ax_0y_0}{2b}.$$ Atunci $\mathcal{A}_{(OBM)}=\frac{ab}{2}\arcsin\frac{x_0}{a}+\frac{x_0y_0}{2}-\frac{x_0y_0}{2}=\frac{ab}{2}\arcsin\frac{x_0}{a}$.

(Pentru calculul integralei putem folosi şi rezultatul din exercițiul rezolvat 3 de la pag. 159 care dă o primitivă a funcției $x\mapsto\sqrt{a^2-x^2}$).

b) Pentru $x_0=a,\ y_0=0$ punctul M devine A şi obținem că aria „sfertului de elipsă" OAB este: $\mathcal{A}_{(OAB)}=\frac{ab}{2}\arcsin 1=\frac{\pi ab}{4}$.

Deducem că aria elipsei este πab.

În cazul particular $a=b=r$, obținem că aria cercului de rază r este πr^2.

EXERCIȚII PROPUSE

I. Calculați aria suprafeței plane delimitate de curbele de ecuații date, după ce în prealabil reprezentați grafic aceste curbe:

1. $y=x^2$; $x=-4$; $y=0$; **2.** $y=-3x^2-2$; $x=1$; $y=-1$;

3. $y=x^2-6x+5$; $x+y=11$; **4.** $y=x^2$; $|y|=x$;

5. $y=\frac{8}{x^2}$; $y=x$; $x=4$; **6.** $y=\sqrt{x-1}$; $x+y=3$; $y=0$;

7. $y=-x^2+6x-2$; $y=x^2-2x+4$; **8.** $y=-16x$; $y=-x^3$; $y=1$;

9. $y=3^x$; $x=\log_3 4$; $x=\log_3 5$; $y=0$; **10.** $y=\sin x$; $y=\frac{2\sqrt{2}}{3}$; $x=0$; $x=\arcsin\frac{2\sqrt{2}}{3}$.

II. Determinați valorile lui $a\in\mathbb{R}$ astfel încât aria suprafeței delimitate de curbele de ecuații $y=3x^3+2x$, $x=a$, $y=0$ să fie egală cu 1.

Volumul unui corp de rotație

Fundamentarea noțiunii de volum este aproape „paralelă" cu aceea a noțiunii de arie.

Din geometria elementară știm să calculăm volumele unor poliedre: prisma, piramida, trunchiul de piramidă. În general, pentru a calcula volumul unui poliedru oarecare, îl descompunem în tetraedre (piramide triunghiulare) și facem suma volumelor acestor tetraedre.

Extindem ideea prin următoarea:

Definiție

1) Numim ***corp poliedral*** o reuniune finită de poliedre, care este același lucru cu o reuniune finită de tetraedre.

2) Dacă P este un corp poliedral, volumul său $\mathcal{V}(P)$ este suma volumelor tetraedrelor în care se descompune corpul P (care nu depinde de descompunerea aleasă).

Observație

Dacă P, Q sunt corpuri poliedrale şi $P \subseteq Q$, atunci $\mathcal{V}(P) \leq \mathcal{V}(Q)$.

Să fixăm acum un corp geometric C, care este ***mărginit***, adică poate fi inclus într-un anumit cub.

Considerăm mulţimea tuturor corpurilor poliedrale incluse în C, adică:

$$\mathcal{P} = \{P \mid P = \text{corp poliedral}, P \subseteq C\}$$

şi mulţimea tuturor corpurilor poliedrale care includ pe C, adică

$$\mathcal{Q} = \{Q \mid Q = \text{corp poliedral}, Q \supseteq C\}.$$

Ca şi în consideraţiunile similare pe care le-am făcut când am vorbit despre arii, putem considera numerele reale:

$$\mathcal{V}_*(C) = \sup\{\mathcal{V}(P) \mid P \in \mathcal{P}\}$$
$$\mathcal{V}^*(C) = \inf\{\mathcal{V}(P) \mid P \in \mathcal{P}\}$$

numite ***volumul interior***, respectiv, ***volumul exterior*** ale corpului C.

Rezultă uşor că $\mathcal{V}_*(C) \leq \mathcal{V}^*(C)$.

Conceptul general de volum se introduce prin următoarea:

Definiţie

Spunem că un corp geometric mărginit C ***are volum*** dacă volumul său interior este egal cu volumul său exterior, iar în acest caz ***volumul*** lui C este prin definiţie valoarea comună a celor două volume, adică:

$$\mathcal{V}(C) = \mathcal{V}_*(C) = \mathcal{V}^*(C).$$

Ca şi în geometria plană, putem demonstra următoarea teoremă de caracterizare a corpurilor care au volum:

Teoremă

Fie C un corp geometric mărginit. Următoarele afirmaţii sunt echivalente:

1°. Corpul C are volum.

2°. Există un şir $(P_n)_{n\geq 1}$ de corpuri poliedrale incluse în C şi un şir $(Q_n)_{n\geq 1}$ de corpuri poliedrale care includ pe C, astfel încât:

$$\lim_{n\to\infty} \mathcal{V}(P_n) = \lim_{n\to\infty} \mathcal{V}(Q_n).$$

Valoarea comună a acestor limite este tocmai volumul corpului C.

Demonstraţia este aceeaşi cu a teoremei corespunzătoare de la arii, doar că în loc de aria $\mathcal{A}$ se consideră volumul $\mathcal{V}$.

Cu exact aceeaşi tehnică de demonstraţie, utilizată în teorema precedentă pentru implicaţia 2° $\Rightarrow$ 1°, putem stabili următorul rezultat mai general:

Teoremă

Fie C un corp geometric mărginit. Presupunem că există un şir de corpuri $(C_n)_{n\geq 1}$ care au volum şi sunt incluse în C, precum şi un şir de corpuri (mărginite) $(D_n)_{n\geq 1}$ care au volum şi includ pe C, astfel încât:

$$\lim_{n\to\infty} \mathscr{V}(C_n) = \lim_{n\to\infty} \mathscr{V}(D_n).$$

Atunci, corpul C are volum şi $\mathscr{V}(C)$ este valoarea comună a celor două limite.

Demonstraţia poate trece drept temă în seama cititorului.

Ca în geometria plană, se poate stabili imediat proprietatea de „aditivitate" a volumului. Avem în acest sens următoarea:

Observaţie

Dacă C_1, C_2 sunt corpuri geometrice mărginite care nu au puncte interioare comune, iar $C = C_1 \cup C_2$, atunci din aceea că două din corpurile C_1, C_2, C au volum rezultă că şi cel de-al treilea are volum şi avem egalitatea:

$$\mathscr{V}(C) = \mathscr{V}(C_1) + \mathscr{V}(C_2).$$

Următorul exemplu este ilustrativ pentru partea teoretică expusă.

Exemplu: volumul unui cilindru circular drept

Dacă C este un cilindru circular drept cu raza r şi înălţimea h, atunci C are volum şi acesta este dat de egalitatea:

$$\mathscr{V}(C) = \pi r^2 h.$$

Într-adevăr, pentru fiecare $n \in \mathbb{N}$, $n \geq 3$, să notăm cu P_n prisma „înscrisă" în cilindrul C, având drept bază poligonul regulat cu n laturi înscris în cercul de bază al cilindrului, iar cu Q_n prisma „circumscrisă" cilindrului C, având ca bază poligonul regulat cu n laturi circumscris cercului de bază al cilindrului. Notăm aria bazei prismei P_n cu S'_n, iar aria bazei prismei Q_n cu S''_n. Avem, conform teoremei de la arii:

$$\lim_{n\to\infty} S'_n = \lim_{n\to\infty} S''_n = \pi r^2.$$

Volumul prismei P_n este $\mathscr{V}(P_n) = hS'_n$, iar volumul prismei Q_n este $\mathscr{V}(Q_n) = hS''_n$, prin urmare $\lim\limits_{n\to\infty} \mathscr{V}(P_n) = \lim\limits_{n\to\infty} hS'_n = \pi r^2 h$ şi $\lim\limits_{n\to\infty} \mathscr{V}(Q_n) = \lim\limits_{n\to\infty} hS''_n = \pi r^2 h$.

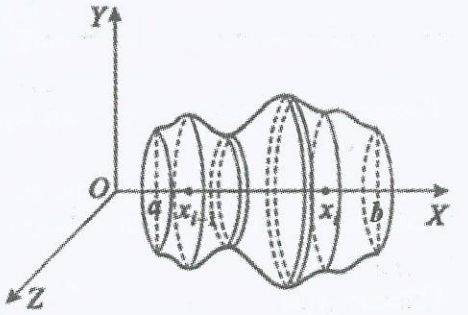
Conform teoremei de caracterizare a corpurilor care au volum, deducem că cilindrul C are volum şi acesta este $\mathscr{V}(C) = \pi r^2 h$.

Rezultatul care urmează este important şi arată cum se exprimă volumul unui anumit corp de rotaţie printr-o integrală.

Teoremă

Fie $f : [a, b] \to \mathbb{R}$ o funcție continuă și pozitivă. Rotim în jurul axei OX trapezul curbiliniu delimitat de grafic, axa OX și dreptele $x = a$, $x = b$. Corpul de rotație obținut C are volum și acesta este dat de formula:

$$\mathcal{V}(C) = \pi\int_a^b f^2(x)dx.$$



Demonstrație. Pentru fiecare $n \in \mathbb{N}^*$, fie Δ_n diviziunea care împarte intervalul $[a, b]$ în n părți egale, prin punctele de diviziune

$$x_i^{(n)} = a + \frac{i(b-a)}{n}, \quad i = \overline{1, n}.$$

Fie $m_i^{(n)}$, $M_i^{(n)}$ minimul, respectiv maximul funcției f pe intervalul de diviziune $\left[x_{i-1}^{(n)}, x_i^{(n)}\right]$, $i = \overline{1, n}$.

Reuniunea cilindrilor de raze $m_i^{(n)}$ și înălțimi $x_i^{(n)} - x_{i-1}^{(n)}$, $i = \overline{1, n}$ este un corp geometric C_n inclus în C, al cărui volum (utilizând aditivitatea volumului) este:

$$\mathcal{V}(C_n) = \sum_{i=1}^{n} \pi\left(m_i^{(n)}\right)^2\left(x_i^{(n)} - x_{i-1}^{(n)}\right) = \pi\sum_{i=1}^{n}\left(m_i^{(n)}\right)^2\left(x_i^{(n)} - x_{i-1}^{(n)}\right) = \pi s(f^2, \Delta_n),$$

adică este suma Darboux inferioară asociată funcției f^2 și diviziunii Δ_n, înmulțită cu π.

Reuniunea cilindrilor de raze $M_i^{(n)}$ și înălțimi $x_i^{(n)} - x_{i-1}^{(n)}$, $i = \overline{1, n}$ este un corp geometric D_n care include C, al cărui volum este:

$$\mathcal{V}(D_n) = \sum_{i=1}^{n} \pi\left(M_i^{(n)}\right)^2\left(x_i^{(n)} - x_{i-1}^{(n)}\right) = \pi\sum_{i=1}^{n}\left(M_i^{(n)}\right)^2\left(x_i^{(n)} - x_{i-1}^{(n)}\right) = \pi S(f^2, \Delta_n),$$

adică este suma Darboux superioară asociată funcției f^2 și diviziunii Δ_n, înmulțită cu π.

Dar $\|\Delta_n\| = \dfrac{b-a}{n} \to 0$ și cum sumele Darboux sunt niște sume Riemann (căci funcția f^2 este continuă), rezultă:

$$\lim_{n\to\infty}\mathcal{V}(C_n) = \pi\lim_{n\to\infty} s(f^2, \Delta_n) = \pi\int_a^b f^2(x)dx;$$

$$\lim_{n\to\infty}\mathcal{V}(D_n) = \pi\lim_{n\to\infty} S(f^2, \Delta_n) = \pi\int_a^b f^2(x)dx.$$

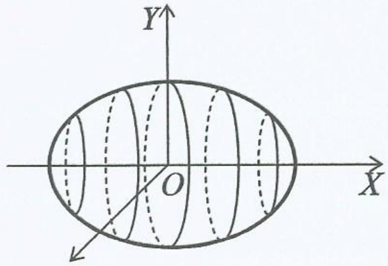
Conform teoremei de la pag. 221, rezultă că acest corp C din enunțul teoremei are volum și acesta este:

$$\mathcal{V}(C) = \lim_{n\to\infty}\mathcal{V}(C_n) = \lim_{n\to\infty}\mathcal{V}(D_n) = \pi\int_a^b f^2(x)dx.$$

Exerciții rezolvate

1. Să se determine volumul elipsoidului de rotație obținut prin rotația în jurul axei OX a elipsei de ecuație $\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$, apoi să se deducă volumul sferei.

Soluție. În fond este suficient să rotim în jurul axei OX trapezul curbiliniu delimitat de graficul funcției $f:[a, b]\to\mathbb{R}$, $f(x)=\frac{b}{a}\sqrt{a^2-x^2}$, axa OX și dreptele de ecuații $x=a,\ x=b$. Rezultă că volumul elipsoidului este:



$$\mathcal{V}=\pi\int_a^b\frac{b^2}{a^2}(a^2-x^2)dx=\frac{\pi b^2}{a^2}\left(a^2x-\frac{x^3}{3}\right)\Bigg|_{-a}^{a}=$$

$$=\frac{\pi b^2}{a^2}\left(a^3-\frac{a^3}{3}\right)-\frac{\pi b^2}{a^2}\left(-a^3-\frac{a^3}{3}\right)=\frac{4\pi ab^2}{3}.$$

În cazul când $a=b=r$, obținem că volumul sferei de rază r este: $\mathcal{V}=\frac{4\pi r^3}{3}$.

2. Să se afle aria suprafeței plane delimitate de curbele de ecuații $y=\cos x,\ \ y=0,\ \ x=0,\ \ x=\pi/2$, precum și volumul corpului obținut prin rotația în jurul axei OX a acestei suprafețe.

Soluție. Suprafața este tocmai subgraficul funcției $f:\left[0,\frac{\pi}{2}\right]\to\mathbb{R},\ f(x)=\cos x,$ deci are aria: $S=\int_0^{\frac{\pi}{2}}\cos x dx=\sin x\Big|_0^{\frac{\pi}{2}}=1.$

Volumul căutat este $V=\pi\int_0^{\frac{\pi}{2}}\cos^2 x dx=\frac{\pi}{2}\int_0^{\frac{\pi}{2}}(1+\cos 2x)dx=\frac{\pi}{2}\left(x+\frac{1}{2}\sin 2x\right)\Bigg|_0^{\frac{\pi}{2}}=\frac{\pi^2}{4}.$

EXERCIȚII PROPUSE

Calculați volumul corpului obținut prin rotația în jurul axei OX a suprafeței plane delimitate de curbele de ecuații:

1. $y=\sqrt{x}$; $y=0$; $x=1$;

2. $y^2=x^2$; $y=0$; $x=1$;

3. $y=x^2$; $y=\sqrt{x}$;

4. $x^2-y^2=a^2$; $x=2a$, unde $a>0$;

5. $y=xe^x$; $y=0$; $x=1$;

6. $y=\sin x$; $y=0$; $x=0$; $x=\pi$;

7. $y=\sqrt{\cos x}$, $y=0$; $x=0$; $x=\frac{\pi}{2}$;

8. $y=\sqrt{1-x^2}$; $y=0$; $x=-1$; $x=1$;

9. $y=|x|$; $y=0$; $x=-3$; $x=-1$;

10. $y^2=2px$; $x=p$ (unde $p>0$).

Calculul unor limite de şiruri folosind integrala definită

Un prim rezultat, cu o largă arie de aplicabilitate, îl constituie următoarea:

Teoremă

Dacă $f : [0, 1] \to \mathbb{R}$ este o funcţie integrabilă, atunci:

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n} f\left(\frac{i}{n}\right)=\int_0^1 f(x)dx.$$

Demonstraţie. Considerăm diviziunea $\Delta = \left(0, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{i}{n}, \ldots, 1\right)$ care împarte intervalul $[0, 1]$ în n intervale de lungimi egale, prin punctele de diviziune $x_i = \frac{i}{n}$, $i=\overline{1, n}$; norma acestei diviziuni este $\| \Delta \| = \frac{1}{n}$ şi când $n \to \infty$, avem $\| \Delta \| \to 0$.

Asociem acestei diviziuni sistemul de puncte intermediare ξ dat de capetele din dreapta ale intervalelor de diviziune $\xi_i = \frac{i}{n}$, $i=\overline{1, n}$, deci $\xi = \left(\frac{1}{n}, \frac{2}{n}, \ldots, \frac{i}{n}, \ldots, 1\right)$.

Suma Riemann corespunzătoare este:

$$\sigma(f, \Delta, \xi) = \sum_{i=1}^{n} f(\xi_i)(x_i - x_{i-1}) = \sum_{i=1}^{n} f\left(\frac{i}{n}\right)\left(\frac{i}{n}-\frac{i-1}{n}\right)=\frac{1}{n}\sum_{i=1}^{n} f\left(\frac{i}{n}\right),$$

adică tocmai suma din enunţ. Dar când $n \to \infty$, $\| \Delta \| \to 0$, iar $\sigma(f, \Delta, \xi) \to \int_0^1 f(x)dx$, prin urmare:

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n} f\left(\frac{i}{n}\right)=\int_0^1 f(x)dx.$$

Alte două rezultate spectaculoase sunt date de următoarea:

Teoremă

Există egalităţile:

a) $\lim\limits_{n\to\infty}\left(\frac{(2n)!!}{(2n-1)!!}\right)^2 \cdot \frac{1}{2n+1} = \frac{\pi}{2}$ (formula lui Wallis);

b) $\lim\limits_{n\to\infty}\frac{n!}{\sqrt{2\pi}\cdot n^{n+\frac{1}{2}}\cdot e^{-n}} = 1$ (formula lui Stirling).

Demonstrație. **a)** Pentru orice $x \in \left[0, \frac{\pi}{2}\right]$ şi $n \in \mathbb{N}^*$, avem inegalitățile:

$$\sin^{2n+1} x \le \sin^{2n} x \le \sin^{2n-1} x$$

de unde, prin integrare:

$$\int_0^{\frac{\pi}{2}} \sin^{2n+1} x \, dx \le \int_0^{\frac{\pi}{2}} \sin^{2n} x \, dx \le \int_0^{\frac{\pi}{2}} \sin^{2n-1} x \, dx .$$

Ținând seama de exercițiul rezolvat de la pag. 190, punctul c), ultima inegalitate se scrie (cu inegalități stricte, deoarece π este irațional):

$$\frac{(2n)!!}{(2n+1)!!} < \frac{(2n-1)!!}{(2n)!!} \cdot \frac{\pi}{2} < \frac{(2n-2)!!}{(2n-1)!!}.$$

Împărțind prin $\frac{(2n-1)!!}{(2n)!!}$, obținem:

$$\left(\frac{(2n)!!}{(2n-1)!!}\right)^2 \cdot \frac{1}{2n+1} < \frac{\pi}{2} < \left(\frac{(2n)!!}{(2n-1)!!}\right)^2 \cdot \frac{1}{2n}. \tag{1}$$

Diferența dintre şirurile ce-l încadrează pe $\frac{\pi}{2}$ în (1) este:

$$\alpha_n = \left(\frac{(2n)!!}{(2n-1)!!}\right)^2 \cdot \frac{1}{2n} - \left(\frac{(2n)!!}{(2n-1)!!}\right)^2 \cdot \frac{1}{2n+1} = \left(\frac{(2n)!!}{(2n+1)!!}\right)^2 \cdot \left(\frac{1}{2n} - \frac{1}{2n+1}\right) =$$

$$= \left(\frac{(2n)!!}{(2n-1)!!}\right)^2 \cdot \frac{1}{2n(2n+1)} \overset{(1)}{<} \frac{\pi}{2} \cdot \frac{1}{2n}, \text{ deci } \alpha_n \to 0.$$

Scriem atunci (1) sub forma:

$$\frac{\pi}{2} - \alpha_n < \left(\frac{(2n)!!}{(2n-1)!!}\right)^2 \cdot \frac{1}{2n+1} < \frac{\pi}{2}. \tag{2}$$

Utilizând (2) şi criteriul cleştelui, deducem că:

$$\lim_{n\to\infty} \left(\frac{(2n)!!}{(2n-1)!!}\right)^2 \cdot \frac{1}{2n+1} = \frac{\pi}{2}.$$

b) Mai întâi, să observăm că dacă „extragem radicalul", formula lui Wallis poate fi scris sub forma:

$$\lim_{n\to\infty} \frac{(2n)!!}{(2n-1)!!} \cdot \frac{1}{\sqrt{2n+1}} = \sqrt{\frac{\pi}{2}}, \text{ sau,}$$

ținând seama că $(2n)!! = 2^n \cdot n!$ şi $(2n-1)!! = \frac{(2n)!}{(2n)!!} = \frac{(2n)!}{2^n \cdot n!}$, se poate scrie echivalent:

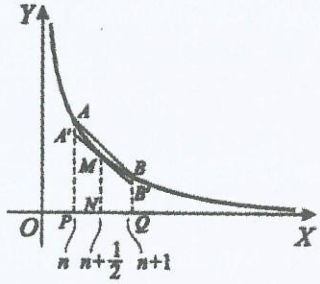
$$\lim_{n\to\infty} \frac{2^{2n} \cdot (n!)^2}{(2n)!\sqrt{2n+1}} = \sqrt{\frac{\pi}{2}}. \tag{3}$$

Să notăm cu a_n partea care depinde efectiv de n din şirul care apare în enunțul formulei lui Stirling, adică:

$$a_n = \frac{n!}{n^{n+\frac{1}{2}} \cdot e^{-n}}, \ n \in \mathbb{N}^*. \tag{4}$$

Rezultă uşor că $\dfrac{a_n}{a_{n+1}} = e^{-1}\left(1+\dfrac{1}{n}\right)^{n+\frac{1}{2}}$ de unde, logaritmând:

$$\ln \frac{a_n}{a_{n+1}} = -1 + \left(n+\frac{1}{2}\right)\ln\left(1+\frac{1}{n}\right). \tag{5}$$



Considerăm funcţia $f : (0, \infty) \to \mathbb{R}$, $f(x) = \dfrac{1}{x}$.

Notăm cu A, M, B punctele de pe grafic de abscise n, $n+\dfrac{1}{2}$, $n + 1$ (pentru $n \in \mathbb{N}^*$ fixat), cu P, N, Q punctele de pe axa OX de abscise n, $n+\dfrac{1}{2}$, $n + 1$, iar cu A', B' intersecţiile tangentei în M la grafic cu dreptele AP, BQ (adică dreptele de ecuaţii $x = n$, $x = n + 1$).

Funcţia f fiind convexă are graficul situat deasupra tangentei $A'B'$ şi sub coarda AB. Rezultă că aria trapezului curbiliniu determinat de graficul funcţiei, axa OX şi dreptele de ecuaţii $x = n$, $x = n + 1$ este cuprins între ariile trapezelor $PQB'A'$ şi $PQBA$.

Aria trapezului curbiliniu de care vorbim este $\displaystyle\int_n^{n+1} f(x)\,dx = \int_n^{n+1} \frac{dx}{x}$.

Aria trapezului $PQB'A'$ este $\dfrac{PQ(PA'+QB')}{2} = PQ \cdot MN = f\left(n+\dfrac{1}{2}\right) = \dfrac{1}{n+\frac{1}{2}}$,

iar aria trapezului $PQBA$ este $\dfrac{PQ(PA+PB)}{2} = \dfrac{1}{2}\big(f(n)+f(n+1)\big) = \dfrac{1}{2}\left(\dfrac{1}{n}+\dfrac{1}{n+1}\right)$.

Aşadar, avem inegalitatea:

$$\frac{1}{n+\frac{1}{2}} < \int_n^{n+1} \frac{dx}{x} < \frac{1}{2}\left(\frac{1}{n}+\frac{1}{n+1}\right)$$

care se mai scrie:

$$\frac{1}{n+\frac{1}{2}} < \ln\left(1+\frac{1}{n}\right) < \frac{1}{2}\left(\frac{1}{n}+\frac{1}{n+1}\right) = \frac{2n+1}{2n(n+1)}.$$

Înmulţind cu $n+\dfrac{1}{2}$ şi scăzând 1 peste tot, rezultă:

$$0 < \left(n+\frac{1}{2}\right)\ln\left(1+\frac{1}{n}\right) - 1 < \frac{(2n+1)^2}{4n(n+1)} - 1 = \frac{1}{4n(n+1)} = \frac{1}{4}\left(\frac{1}{n}-\frac{1}{n+1}\right). \tag{6}$$

Combinând (5) cu (6) obţinem:

$$0<\ln\frac{a_n}{a_{n+1}}<\frac{1}{4}\left(\frac{1}{n}-\frac{1}{n+1}\right)$$

şi de aici mai departe:

$$1<\frac{a_n}{a_{n+1}}<e^{\frac{1}{4}\left(\frac{1}{n}-\frac{1}{n+1}\right)}. \tag{7}$$

Dacă în (7) înlocuim pe n pe rând cu valorile 1, 2, 3, ..., $n-1$ şi înmulţind inegalităţile obţinute, rezultă:

$$1<\frac{a_1}{a_n}<e^{\frac{1}{4}\left(1-\frac{1}{n}\right)}. \tag{8}$$

Din (7) avem $a_n>a_{n+1}$, deci şirul $(a_n)_{n\geq 1}$ este descrescător şi având termenii pozitivi este mărginit, deci are limita $\ell=\lim\limits_{n\to\infty}a_n\geq 0$. Atunci, în (8) putem trece la limită şi obţinem:

$$1\leq\frac{a_1}{\ell}\leq e^{\frac{1}{4}}. \tag{9}$$

Din (9) rezultă cu nu putem avea $\ell=0$, deci neapărat $\ell>0$. Să calculăm acum raportul $\frac{a_n^2}{a_{2n}}$. Avem, folosind (4):

$$\frac{a_n^2}{a_{2n}}=\frac{(n!)^2}{n^{2n+1}\cdot e^{-2n}}\cdot\frac{(2n)^{2n+\frac{1}{2}}\cdot e^{-2n}}{(2n)!}=\frac{2^{2n}\cdot(n!)^2}{(2n)!\sqrt{n}}\cdot\sqrt{2},$$

adică:

$$\frac{a_n^2}{a_{2n}}=\frac{2^{2n}\cdot(n!)^2}{(2n)!\sqrt{2n+1}}\cdot\sqrt{\frac{2n+1}{n}}\cdot\sqrt{2}. \tag{10}$$

Trecând la limită în (10) şi folosind formula lui Wallis scrisă sub forma (3) obţinem:

$$\frac{\ell^2}{\ell}=\sqrt{\frac{\pi}{2}}\cdot\sqrt{2}\cdot\sqrt{2},\ \text{adică}\ \ell=\sqrt{2\pi}.$$

Aşadar $\ell=\lim\limits_{n\to\infty}\frac{n!}{n^{n+\frac{1}{2}}\cdot e^{-n}}=\sqrt{2\pi}$, care se mai scrie echivalent:

$$\lim_{n\to\infty}\frac{n!}{\sqrt{2\pi}\cdot n^{n+\frac{1}{2}}\cdot e^{-n}}=1.$$

Exerciţiu rezolvat

Să se calculeze limitele:

a) $\lim\limits_{n\to\infty}\left(\frac{1}{n+1}+\frac{1}{n+2}+\ldots+\frac{1}{n+n}\right)$;

b) $\lim\limits_{n\to\infty}\left(\frac{n^2}{(n+1)^3}+\frac{n^2}{(n+2)^3}+\ldots+\frac{n^2}{(n+n)^3}\right)$;

c) $\lim\limits_{n\to\infty}\frac{1}{n}\left(\sin\frac{\pi}{n}+\sin\frac{2\pi}{n}+\ldots+\sin\frac{(n-1)\pi}{n}\right)$.

Soluţie. **a)** Limita se scrie: $\lim\limits_{n\to\infty}\sum\limits_{i=1}^{n}\frac{1}{n+i}=\lim\limits_{n\to\infty}\sum\limits_{i=1}^{n}\frac{1}{n\left(1+\frac{i}{n}\right)}=\lim\limits_{n\to\infty}\frac{1}{n}\sum\limits_{i=1}^{n}f\left(\frac{i}{n}\right)$,

unde $f:[0,1]\to\mathbb{R}$, $f(x)=\frac{1}{1+x}$.

Conform teoremei, valoarea limitei este $\int_0^1\frac{1}{1+x}dx=\ln(1+x)\Big|_0^1=\ln 2$.

b) Avem: $\lim\limits_{n\to\infty}\sum\limits_{i=1}^{n}\frac{n^2}{(n+i)^3}=\lim\limits_{n\to\infty}\sum\limits_{i=1}^{n}\frac{n^2}{n^3\left(1+\frac{i}{n}\right)^3}=\lim\limits_{n\to\infty}\frac{1}{n}\sum\limits_{i=1}^{n}\frac{1}{\left(1+\frac{i}{n}\right)^3}=\lim\limits_{n\to\infty}\frac{1}{n}\sum\limits_{i=1}^{n}f\left(\frac{i}{n}\right)$,

unde $f:[0,1]\to\mathbb{R}$, $f(x)=\frac{1}{(1+x)^3}$. Conform teoremei, valoarea limitei este:

$$\int_0^1\frac{1}{(1+x)^3}dx\overset{t=1+x}{=}\int_1^2\frac{1}{t^3}dt=-\frac{1}{2t^2}\Big|_1^2=-\frac{1}{8}+\frac{1}{2}=\frac{3}{8}.$$

c) Avem: $\lim\limits_{n\to\infty}\frac{1}{n}\sum\limits_{i=1}^{n-1}\sin\frac{i\pi}{n}=\lim\limits_{n\to\infty}\frac{1}{n}\sum\limits_{i=1}^{n}\sin\frac{i\pi}{n}=\lim\limits_{n\to\infty}\frac{1}{n}\sum\limits_{i=1}^{n}f\left(\frac{i}{n}\right)$, unde $f:[0,1]\to\mathbb{R}$,

$f(x)=\sin\pi x$. Conform teoremei, limita şirului este integrala:

$$\int_0^1\sin\pi x\,dx\overset{t=\pi x}{=}\frac{1}{\pi}\int_0^\pi\sin t\,dt=-\frac{1}{\pi}\cos t\Big|_0^\pi=\frac{1}{\pi}-\left(-\frac{1}{\pi}\right)=\frac{2}{\pi}.$$

EXERCIŢII PROPUSE

Calculaţi limitele următoarelor şiruri $(a_n)_{n\geq 1}$:

1. $a_n = \dfrac{1^p + 2^p + 3^p + \ldots + n^p}{n^{p+1}}$, unde $p > 0$ este fixat;

2. $a_n = n\left(\dfrac{1}{n^2+1^2} + \dfrac{1}{n^2+2^2} + \ldots + \dfrac{1}{n^2+n^2}\right)$;

3. $a_n = \dfrac{1}{\sqrt{n^2+1^2}} + \dfrac{1}{\sqrt{n^2+2^2}} + \ldots + \dfrac{1}{\sqrt{n^2+n^2}}$;

4. $a_n = \dfrac{n+1}{n^2+1^2} + \dfrac{n+2}{n^2+2^2} + \ldots + \dfrac{n+n}{n^2+n^2}$;

5. $a_n = \dfrac{1}{n}\left(\cos\dfrac{\pi}{n} + \cos\dfrac{2\pi}{n} + \ldots + \cos\dfrac{n\pi}{n}\right)$;

6. $a_n = \dfrac{1}{n}\left(\sin\dfrac{\pi}{n} + \sin\dfrac{2\pi}{n} + \ldots + \sin\dfrac{n\pi}{n}\right)$;

7. $a_n = \dfrac{\sqrt{n+1} + \sqrt{n+2} + \ldots + \sqrt{n+n}}{n\sqrt{n}}$;

8. $a_n = \dfrac{1}{n}\left(\sin^2\dfrac{1}{n} + \sin^2\dfrac{2}{n} + \ldots + \sin^2\dfrac{n}{n}\right)$.

TESTE DE EVALUARE

Testul 1

(timp de lucru - 40 minute; fiecare exerciţiu se notează cu 2,25 puncte)

Indicaţi răspunsul corect.

1. $\lim\limits_{n\to\infty}\sum\limits_{k=1}^{n}\dfrac{1}{n+2k-1} =$

   a) $\dfrac{\ln 2}{2}$; b) $\ln 3$; c) 1; d) $\dfrac{1}{2}$.

2. Aria suprafeței delimitată de graficele funcțiilor $f(x)=\sqrt{1-x^2}$, $g(x)=\sqrt{2x-x^2}$ şi axa OX este:

a) $\frac{\pi}{3}-\frac{\sqrt{3}}{4}$; b) $\frac{\pi}{3}-1$; c) $\pi-\sqrt{3}$; d) $\frac{\pi-2\sqrt{3}}{4}$.

3. Graficul funcției $f(x) = \arcsin x$, $x \in [0, 1]$ se roteşte în jurul axei OY. Volumul corpului de rotație obținut este:

a) 1; b) $\frac{20}{3}$; c) $\frac{\pi^2}{4}$; d) $\frac{\pi \ln 2}{2}$.

4. Aria suprafeței cuprinsă între parabolele de ecuații $y=x^2$ şi $y=a-x^2$ este egală cu $\frac{2\sqrt{2}}{3}$. Atunci a este:

a) 1; b) 2; c) $\sqrt{2}$; d) $2\sqrt{2}$.

Testul 2

(timp de lucru - 60 minute; fiecare exercițiu se notează cu 2,25 puncte)

Pentru problemele următoare se cer soluții complete.

1. Să se afle aria suprafeței din plan cuprinsă între dreapta de ecuație $y = 2x - 1$ şi parabola de ecuație $x = y^2$.

2. Calculați volumul corpului obținut prin rotația în jurul axei OX a domeniului plan mărginit de graficul funcției $f(x) = x \cdot \ln x$, $x \in [1, e]$ şi axa OX.

3. Fie $f : [0, 1] \to [1, \infty]$ o funcție continuă.

Să se arate că $\lim\limits_{n\to\infty} \sqrt[n]{f\left(\frac{1}{n}\right)\cdot f\left(\frac{2}{n}\right)\cdot\ldots\cdot f\left(\frac{n}{n}\right)} = e^{\int_0^1 f(x)dx}$.

4. Se consideră funcția $f : [0, 2] \to \mathbb{R}$, $f(x)=2x-x^2$. Să se afle $m \in \mathbb{R}$ ştiind că dreapta de ecuație $y = mx$ împarte subgraficul funcției f în două suprafețe de arii egale.

PROBLEME RECAPITULATIVE

I. În ipotezele indicate, demonstrați următoarele identități:

1. Dacă $f : [-a, a] \to \mathbb{R}$ este o funcție continuă impară, atunci: $\int_{-a}^{a} f(x)dx = 0$.

2. Dacă $f : [-a, a] \to \mathbb{R}$ este o funcție continuă pară, atunci: $\int_{-a}^{a} f(x)dx = 2\int_{0}^{a} f(x)dx$.

3. Dacă $f : [-a, a] \to \mathbb{R}$ este o funcție continuă, atunci: $\int_{a}^{b} f(x)dx = \int_{a}^{b} f(a+b-x)dx$.

4. Dacă $f : [-a, a] \to \mathbb{R}$ este o funcție continuă, atunci:

a) $\int_{0}^{\frac{\pi}{2}} f(\sin x)dx = \int_{0}^{\frac{\pi}{2}} f(\cos x)dx$;

b) $\int_{0}^{\pi} xf(\sin x)dx = \frac{\pi}{2}\int_{0}^{\pi} f(\sin x)dx = \int_{0}^{\frac{\pi}{2}} f(\sin x)dx$.

5. Dacă $f : [a, b] \to [c, d]$ este bijecție crescătoare și derivabilă, atunci:

$\int_{a}^{b} f(x)dx + \int_{c}^{d} f^{-1}(y)dy = bd - ac$ (identitatea lui Young).

II. Utilizând convenabil exercițiile din setul I, calculați:

1. $\int_{-\pi}^{\pi} x^{2001} \sin^{2002} x \, dx$.

2. $\int_{-1}^{1} x^3 e^{-x^2} dx$.

3. $\int_{0}^{1} |x| dx$ și $\int_{-1}^{1} |x| dx$.

4. $\int_{0}^{2} \sqrt{4-x^2}\, dx$ și $\int_{-2}^{2} \sqrt{4-x^2}\, dx$.

5. $\int_{0}^{\frac{\pi}{2}} \sin^2 x \, dx$ și $\int_{0}^{\frac{\pi}{2}} \cos^2 x \, dx$.

6. $\int_{0}^{\pi} x\sin^2 x \, dx$ și $\int_{0}^{\pi} x\cos^2 x \, dx$.

7. $\int_{0}^{\frac{\pi}{4}} \ln(1 + \operatorname{tg} x)dx$.

8. $\int_{0}^{1} e^{x^2} dx + \int_{1}^{e} \sqrt{\ln x}\, dx$.

9. $\int_{0}^{\frac{\pi}{2}} \operatorname{arctg}(\sin x)dx + \int_{0}^{\frac{\pi}{2}} \arcsin(\operatorname{tg} x)dx$.

III. În ipotezele indicate, demonstrați următoarele inegalități:

1. Dacă $f : [a, b] \to \mathbb{R}$ este o funcție continuă, atunci: $\left|\int_a^b f(x)dx\right| \le \int_a^b |f(x)|dx$.

2. Dacă $f, g : [a, b] \to \mathbb{R}$ sunt funcții continue, atunci:

a) $\lambda^2 \int_a^b f^2(x)dx - 2\lambda \int_a^b f(x)g(x)dx + \int_a^b g^2(x)dx \ge 0$, $\forall \lambda \in \mathbb{R}$.

b) $\left(\int_a^b f(x)g(x)dx\right)^2 \le \int_a^b f^2(x)dx \cdot \int_a^b g^2(x)dx$.

(forma integrală a inegalității Cauchy-Buniakowski-Schwarz)

3. Dacă $[a, b] \xrightarrow{g} I \xrightarrow{f} \mathbb{R}$ sunt funcții continue, f fiind convexă, iar $\Delta \in \mathscr{D}([a, b])$, $\Delta = (a = x_0, x_1, x_2, \ldots, x_n = b)$ și $\xi = (\xi_1, \xi_2, \ldots, \xi_n)$ este un sistem de puncte intermediare asociat, atunci:

a) $f\left(\frac{1}{b-a} \cdot \sum_{i=1}^{n} f(\xi_i)dx_i\right) \le \frac{1}{b-a} \cdot \sum_{i=1}^{n} f\left(g(\xi_i)\right)dx_i$.

b) $f\left(\frac{1}{b-1} \cdot \int_a^b g(x)dx\right) \le \frac{1}{b-a} \cdot \int_a^b f\left(g(x)\right)dx$ (forma integrală a inegalității Jensen).

c) În cazul când f este o funcție concavă, există o inegalitate analoagă celei de la b), dar cu sensul schimbat.

IV. Fie $a_1, a_2, \ldots, a_n$ numere reale. Aplicând teorema de medie funcției polinomiale $f : [0, 1] \to \mathbb{R}$, $f(x) = a_1x + a_2x^2 + \ldots + a_nx^n$, arătați că există $c \in [0, 1]$ cu proprietatea: $a_1\left(\frac{1}{2} - c\right) + a_2\left(\frac{1}{3} - c^2\right) + \ldots + a_n\left(\frac{1}{n+1} - c^n\right) = 0$.

V. Calculați derivatele funcțiilor:

1. $f : (0, \infty) \to \mathbb{R}$, $f(t) = \int_\pi^t \frac{\sin x}{x} dx$.

2. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \int_t^{2t} e^{x^2} dx$.

VI. Notăm $B(p, q) = \int_0^1 x^{p-1}(1-x)^{q-1}dx$, unde $p, q \in \mathbb{N}^*$ (integrala lui Euler de speța întâi). Arătați că:

a) $B(p, q) = B(q, p)$, $\forall\, p, q \in \mathbb{N}^*$ fără a calcula efectiv integrala.

b) $B(p, q)=\frac{q-1}{p}\cdot B(p+1, q-1)$, $\forall\, p,q \in \mathbb{N}^*$, $q \geq 2$.

c) $B(p, q)=\frac{(p-1)!(q-1)!}{(p+q+2)!}\cdot B(p+q-1, 1)$, $\forall\, p,q \in \mathbb{N}^*$.

d) $B(p, q)=\frac{(p-1)!(q-1)!}{(p+q-1)!}$, $\forall\, p,q \in \mathbb{N}^*$.

VII. Notăm $I_{m,n}=\int_0^{\frac{\pi}{2}}\sin^{2m+1} x\cos^{2n+1} x\, dx$, unde $m,n \in \mathbb{N}$. Arătați că:

a) $I_{m,n}=\frac{1}{2}B(m+1, n+1)$, $\forall$ m,n $\in$ $\mathbb{N}$, unde $B(p,\ q)$ are semnificația din exercițiul precedent.

b) $I_{m,n}=\frac{1}{2}\cdot\frac{m!n!}{(m+n+1)!}$, $\forall\, m,n \in \mathbb{N}$.

VIII. Integrând pe intervalul [0, 1] egalitatea $C_n^0+C_n^1x+C_n^2x^2+\ldots+C_n^nx^n=(1+x)^n$, deduceți valoarea expresiei:

$$C_n^0+\frac{C_n^1}{2}+\frac{C_n^2}{3}+\ldots+\frac{C_n^n}{n+1}.$$

IX. Determinați funcțiile continue $f : \mathbb{R} \to (0, \infty)$ cu proprietatea că există $\lambda > 0$ astfel încât: $\int f(x)dx=\frac{xf(x)}{2}+\lambda\int\frac{1}{f(x)}dx$.

Comparați rezultatul cu acela din exercițiul rezolvat 3 pag. 159.

X. Fie $f : \mathbb{R} \to \mathbb{R}$ o funcție cu proprietatea că funcțiile „produs" $f \cdot \sin$ și $f \cdot \cos$ au primitive. Arătați că f are primitive.

XI. Fie $f : \mathbb{R} \to \mathbb{R}$ o funcție continuă având perioada $T > 0$. Arătați că funcția $g:\mathbb{R}\to\mathbb{R},\ g(x)=\begin{cases} f\left(\frac{1}{x}\right), & x\neq 0\\ \lambda, & x=0\end{cases}$ are primitive dacă și numai dacă $\lambda=\frac{\int_0^T f(x)dx}{T}$.

XII. Pentru fiecare $n \in \mathbb{N}^*$ considerăm funcția $f_n : \mathbb{R} \to \mathbb{R}$, $f_n(x)=\begin{cases}\sin^n\frac{1}{x}, & x\neq 0\\ \lambda_n, & x=0\end{cases}$

unde $\lambda_n \in \mathbb{R}$. Arătați că:

a) Pentru n impar, funcția f_n are primitive dacă și numai dacă $\lambda_n = 0$.

b) Pentru n par, funcția f_n are primitive dacă și numai dacă $\lambda_n = \dfrac{(2n-1)!!}{(2n)!!}$.

c) Formulați și rezolvați un exercițiu analog pentru funcția:

$$g_n : \mathbb{R} \to \mathbb{R},\ g_n(x) = \begin{cases} \cos^n \dfrac{1}{x}, & x \neq 0 \\ \lambda_n, & x = 0 \end{cases}.$$

XIII. Fie $I \subseteq \mathbb{R}$ un interval și $f,g \in \mathbb{R}$ două funcții. Arătați că:

a) Dacă f are primitive și nu se anulează, iar g este continuă, atunci funcția produs fg are primitive.

b) Dacă f are primitive și este mărginită, iar g este continuă, atunci funcția produs fg are primitive (teorema lui Wilkosz).

XIV. Fie $I \subseteq \mathbb{R}$ un interval și $f,\ g : I \to \mathbb{R}$ două funcții care au primitive. Arătați că dacă g nu se anulează pe I, atunci funcția $\dfrac{f}{g}$ are proprietatea lui Darboux (teorema lui Jarnik).

XV. Arătați că funcția $f : \mathbb{R} \to \mathbb{R},\ f(x) = \begin{cases} |x-1|\sin\dfrac{1}{x}, & x \neq 0 \\ 0, & x = 0 \end{cases}$ are primitive.

XVI. Arătați că dacă funcția $f : [a, b] \to \mathbb{R}$ este integrabilă, atunci funcția $|f|$ este integrabilă.

XVII. Arătați că dacă funcțiile $f, g : [a, b] \to \mathbb{R}$ sunt integrabile, atunci funcția-produs fg este integrabilă.

XVIII. Dacă $f : [a, b] \to \mathbb{R}$ este o funcție de clasă C^1, arătați că:

$$\lim_{n\to\infty} n\left(\int_0^1 f(x)dx - \frac{1}{n}\sum_{i=1}^{n} f\left(\frac{i}{n}\right)\right) = \frac{f(0)-f(1)}{2}.$$

XIX. Dacă $f : [a, b] \to \mathbb{R}$ este o funcție continuă pozitivă, arătați că:

$$\lim_{n\to\infty}\left(\int_a^b f^n(x)dx\right)^{\frac{1}{n}} = \sup_{x\in[a,\,b]} f(x),$$

știind că limita din membrul stâng există.

PROBLEME PENTRU EXAMENUL DE BACALAUREAT ȘI ADMITERE ÎN FACULTĂȚI

1. Fie p un număr prim și $G = \left\{ \begin{pmatrix} \hat{1} & \hat{0} & \hat{0} \\ \hat{a} & \hat{1} & \hat{0} \\ \hat{b} & \hat{c} & \hat{1} \end{pmatrix} \middle| \ \hat{a}, \hat{b}, \hat{c} \in \mathbb{Z}_p \right\}$.

a) Să se arate că G este parte stabilă a lui $\mathcal{M}_3(\mathbb{Z}_p)$ în raport cu operația de înmulțire a matricelor.

b) Să se arate că $(G, \cdot)$ este grup necomutativ cu p^3 elemente.

Bacalaureat

2. Se consideră în mulțimea $\mathbb{C}$ sistemul de ecuații: $\begin{cases} 3x - y - z = 4 \\ x + y - z = 1 + i\sqrt{3} \\ x + 2y + 2z = -1 \end{cases}$

a) Să se arate că sistemul este compatibil determinat.

b) Dacă $G = \{x_0, y_0, z_0\}$ unde (x_0, y_0, z_0) este soluția sistemului dat, să se arate că G împreună cu înmulțirea numerelor complexe este grup abelian.

Bacalaureat

3. Fie matricea $A = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$.

a) Să se calculeze A^{2007}.

b) Să se arate că mulțimea $G = \{I_2, A, A^2\}$ împreună cu înmulțirea matricelor este grup abelian.

Bacalaureat

4. Fie $G = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \middle| \ a, b \in \mathbb{C} \right\}$ unde $\overline{z}$ este conjugatul lui z.

a) Să se arate că $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \in G$.

b) Să se arate că G împreună cu operația de adunare a matricelor este grup abelian.

c) Să se arate că G împreună cu operațiile de adunare și înmulțire a matricelor este corp necomutativ.

Bacalaureat

5. Pe mulțimea $G = (0, \infty) \times \mathbb{R}$ se definește legea de compoziție „$\circ$" prin

$$(a, x) \circ (b, y) = (ab, ay + x), \ \forall\, a, b \in (0, \infty) \text{ și } x, y \in \mathbb{R}.$$

a) Să se arate că $(G, \circ)$ este grup necomutativ.

b) Să se arate că pentru orice $(a, x) \in G$ şi orice $n \in \mathbb{N}^*$, există $(b, y) \in G$ astfel încât $\underbrace{(b, y) \circ (b, y) \circ \ldots \circ (b, y)}_{n \text{ ori}} = (a, x)$.

Bacalaureat

6. Fie $A = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$ şi $B = \begin{pmatrix} 2 & -3 \\ 1 & -2 \end{pmatrix}$.

a) Să se calculeze A^2 şi B^2.

b) Să se arate că $AB \neq BA$.

c) Să se arate că $(BA)^n \neq I_2$, $\forall\, n \in \mathbb{N}^*$.

d) Să se dea exemplu de grup în care există două elemente de ordin finit al căror produs nu are ordin finit.

Bacalaureat

7. Pentru fiecare $n \in \mathbb{N}^*$ se consideră mulţimea $H_n = \left\{ \frac{k}{n!} \,\middle|\, k \in \mathbb{Z} \right\} \subset \mathbb{Q}$.

a) Să se arate că H_n este subgrup al grupului $(\mathbb{Q}, +)$.

b) Să se arate că grupul $(\mathbb{Q}, +)$ nu se poate scrie ca reuniune finită de subgrupuri proprii.

Bacalaureat

8. Se consideră grupul S_4 şi H o submulţime cu 13 elemente a lui S_4.

a) Să se arate că dacă G este un subgrup al lui S_4, $G \neq S_4$ atunci G are cel mult 12 elemente.

b) Să se arate că există $\sigma, \tau \in H$ astfel încât $\sigma\tau \neq \tau\sigma$.

Bacalaureat

9. Fie $G = \left\{ \begin{pmatrix} \hat{x} & \hat{y} \\ \hat{2}\hat{y} & \hat{x} \end{pmatrix} \,\middle|\, \hat{x}, \hat{y} \in \mathbb{Z}_3 \right\}$.

a) Să se arate că G împreună cu operaţiile de adunare şi înmulţire a matricelor este corp comutativ cu 9 elemente.

b) Să se dea exemplu de corp cu 25 de elemente.

Bacalaureat

10. Se consideră polinomul $f = X^3 - aX^2 + bX - c \in \mathbb{R}[X]$ şi $x_1, x_2, x_3 \in \mathbb{C}$ rădăcinile lui. Notăm $S_k = x_1^k + x_2^k + x_3^k$, $k \geq 1$, $A = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \\ x_3 & x_1 & x_2 \end{pmatrix}$ şi $\Delta = \det(A)$.

a) Să se calculeze S_3 şi S_4 în funcţie de a, b şi c.

b) Să se calculeze Δ în funcţie de a, b şi c.

c) Să se arate că dacă x_1, x_2, x_3 sunt în progresie aritmetică, atunci $2a^3 - 9ab + 27 = 0$.

d) Să se arate că dacă $b^2 - 2ac < 0$, atunci f are o singură rădăcină reală.

Bacalaureat

c) Să se arate că $\Delta \geq 0$ dacă şi numai dacă $x_1, x_2, x_3 \in \mathbb{R}$.

Bacalaureat

15. Fie $n \geq 3$ şi polinomul $f = X^{n-1} + X^{n-2} + \ldots + X + 1$ cu rădăcinile $x_1, x_2, \ldots, x_{n-1} \in \mathbb{C}$.

a) Să se arate că $f(x) = \dfrac{x^n - 1}{x - 1}$, $\forall\, x \in \mathbb{C} \setminus \{1\}$.

b) Să se determine rădăcinile lui f.

c) Să se arate că $(1 - x_1)(1 - x_2)\ldots(1 - x_n) = n$.

d) Să se arate că $\sin\dfrac{\pi}{n} \cdot \sin\dfrac{2\pi}{n} \cdot \ldots \cdot \sin\dfrac{(n-1)\pi}{n} = \dfrac{n}{2^{n-1}}$, $\forall\, n \geq 3$.

e) Să se arate că $\sin\dfrac{\pi}{2n} \cdot \sin\dfrac{2\pi}{2n} \cdot \ldots \cdot \sin\dfrac{(n-1)\pi}{2n} = \dfrac{\sqrt{n}}{2^{n-1}}$, $\forall\, n \geq 3$.

Bacalaureat

16. Fie inelul $(\mathbb{Z}, *, \circ)$ unde $x * y = x + y - 3$ şi $x \circ y = xy - 3x - 3y + 12$. Să se determine polinomul de grad minim care are coeficientul dominant 1 şi rădăcini elementele inversabile ale inelului $(\mathbb{Z}, *. \circ)$.

Admitere A.S.E. Bucureşri

17. Pe $\mathbb{R}$ se defineşte legea de compoziţie „$*$" astfel: $a * b = ab - 2(a + b) + 6$, $\forall\, a, b \in \mathbb{R}$. Să se determine suma elementelor din $\mathbb{R}$ care coincid cu simetricele lor.

Admitere A.S.E. Bucureşti

18. Se consideră sistemul de ecuaţii $\begin{cases} \hat{a}x + \hat{3}y + \hat{3}z = \hat{2} \\ \hat{6}x + \hat{4}y + \hat{2}z = \hat{6} \\ \hat{3}x + \hat{2}y + \hat{4}z = \hat{3} \end{cases}$ în $\mathbb{Z}_7$.

Să se determine mulţimea valorilor lui $\hat{a}$ pentru care sistemul este compatibil.

Admitere A.S.E. Bucureşti

19. Pe mulţimea $E = \{1, 2, 3, 4\}$ se defineşte legea de compoziţie „$*$" prin
$x * y =$ restul împărţirii lui x^y la 5.
Să se rezolve în E ecuaţiile: $4 * x = 1$ şi $x * 4 = 3$.

Admitere A.S.E. Bucureşti

20. Pe mulţimea $\mathbb{Q}_+^*$ a numerelor raţionale pozitive se defineşte legea „$*$" care are următoarele proprietăţi:

a) $(x * y) \cdot (z * t) = (x \cdot y) * (y \cdot t)$, $\forall\, x, y, z, t \in \mathbb{Q}_+^*$.

b) $x * x = 1$, $\forall\, x \in \mathbb{Q}_+^*$.

c) $x * 1 = x$, $\forall\, x \in \mathbb{Q}_+^*$.

Să se calculeze $18 * 12$.

Admitere A.S.E. Bucureşti

21. Să se determine restul împărţirii polinomului $P = X^{20} + X^{10} + X^5 + 1$ la $Q = X^2 - 1$.

Admitere Politehnică, Bucureşti

22. Fie $f, g \in \mathbb{R}[X]$ nenule, care au rădăcina comună $2 + 3i$. Dacă $d \in \mathbb{R}[X]$ este un cel mai mare divizor al lui f şi g să se determine gradul minim al lui d.

Admitere Politehnică, Bucureşti

23. Să se determine $m \in \mathbb{Z}_5$ astfel încât polinomul $f = X^4 + X^2 + mX + \hat{3} \in \mathbb{Z}_5[X]$ să aibă cel puţin două rădăcini distincte în $\mathbb{Z}_5$.

Admitere A.S.E. Bucureşti

24. Polinomul $f = X^6 + 5X^5 + 8X^4 + aX^3 + bX^2 + cX + d \in \mathbb{R}[X]$ are toate rădăcinile reale. Dacă $f(1) = f(-2) = 0$, să se calculeze $\sum_{k=1}^{6}(x_k + 1)^2$.

Admitere A.S.E. Bucureşti

25. Se consideră polinomul $f = (a+1)X^3 + 2(a+1)X^2 - (a^2 - 6a)X - a^2 + 5a - 1$, $a \in \mathbb{R} \setminus \{-1\}$. Să se determine a, ştiind că f are o rădăcină dublă.

Admitere A.S.E. Bucureşti

26. Să se precizeze valoarea integralei $\int_1^3 \frac{dx}{1+|x-a|}$ pentru $a \in (1, 3)$:

a) $\ln\frac{4-a}{2+a}$; b) $\ln\big(a(4-a)\big)$; c) $\ln\frac{a}{a+2}$; d) $\ln\frac{4-a}{a}$.

Admitere Facultatea de Ştiinţe Economice, Braşov

27. Se dă integrala $I_n = \int_0^n \frac{dt}{(t+2)\left(\sqrt{t+1}+1\right)}$, $n \in \mathbb{N}$.

a) Calculaţi I_n.

b) Calculaţi limita şirului $\left(I_n\right)_{n\in\mathbb{N}}$.

Admitere Universitatea din Piteşti

28. Se consideră $I_n = \int_0^n e^{-bx} \cdot \sin ax\, dx$, $n \in \mathbb{N}^*$, $a \neq 0$, $b > 0$. Fie $L = \lim_{n\to\infty} I_n$. Dacă I este valoarea integralei I_n pentru $n = 1$ şi $a = b = \frac{\pi}{2}$, atunci:

a) $L = 0$; b) $L = \frac{a+b}{a^2+b^2}$; c) $L = \frac{a}{a^2+b^2}$; d) $L = \frac{b}{a^2}$; e) $L = \frac{b}{a}$.

a) $I = \frac{1-e^{-\frac{\pi}{2}}}{\pi}$; b) $I = \frac{e^{-\frac{\pi}{2}}}{\pi}$; c) $I = \frac{1-e}{\pi}$; d) $I = \frac{\pi^2}{4}e^{-\frac{\pi}{2}}$; e) $I = \frac{4e^{\pi}}{\pi}$.

Admitere A.S.E. Bucureşti

29. Să se calculeze $I = \int \frac{e^{\operatorname{arctg} x}}{(1+x^2)^{\frac{3}{2}}} dx$.

Admitere Universitatea de Vest, Timişoara

30. Dacă $I = \int_{-1}^{1} \frac{x^2}{e^x+1} dx$, atunci:

a) $I = e$; b) $I = \frac{1}{3}$; c) $I = \frac{1}{6}$; d) $I = \frac{1}{2}$; e) $I = 1$.

Admitere A.S.E. Bucureşti

31. Se consideră funcţia $F : \mathbb{R} \to \mathbb{R}$, $F(x) = \int_0^x e^t \ln(1 - t + t^2)dt$. Dacă p este numărul punctelor de extrem local ale lui F, atunci:

a) $p = 0$; b) $p = 4$; c) $p = 3$; d) $p = 2$; e) $p = 1$.

Admitere A.S.E. Bucureşti

32. Se consideră funcţia $f : \mathbb{R}^* \to \mathbb{R}$ care satisface relaţia $f(x) + 2f\left(\frac{1}{x}\right) = x^2$, $\forall x \in \mathbb{R}^*$. Dacă $I = \int_1^2 f(x)dx$, atunci:

a) $I = -\frac{4}{9}$; b) $I = -\frac{4}{3}$; c) $I = \frac{5}{9}$; d) $I = -\frac{7}{3}$; e) $I = \frac{2}{3}$.

Admitere A.S.E. Bucureşti

33. Dacă $I_n = \int\limits_{\frac{1}{n+1}}^{\frac{1}{n}} \operatorname{arctg}(nx)dx$ şi $L = \lim\limits_{n\to\infty} n(n+1)I_n$, atunci:

a) $L = 0$; b) $L = 1$; c) $L = \frac{\pi}{4}$; d) $L = \frac{\pi}{2}$; e) $L = \frac{\sqrt{2}}{2}$.

Admitere A.S.E. Bucureşti

34. Integrala $\int_0^2 \frac{(2-x)^{2n-1}}{(2+x)^{2n+1}}dx$, $n \geq 1$ este:

a) $\frac{1}{8n}$; b) $\frac{1}{4n}$; c) $\frac{1}{2n}$; d) $\frac{3}{8n}$; e) alt răspuns.

Admitere Universitatea Tehnică, Cluj Napoca

35. Să se determine $m \in \mathbb{R}$ astfel încât funcţia

$f_m : \mathbb{R} \to \mathbb{R}$, $f_m(x) = \begin{cases} (2x-1)\cdot \sin\frac{1}{x^2 - x}, & x \in \mathbb{R} - \{0, 1\} \\ m, & x \in \{0, 1\} \end{cases}$ să admită primitive.

Admitere Universitatea de Vest, Timişoara

36. Se consideră funcţia $f : \left[0, \frac{1}{\sqrt{2}}\right] \to \mathbb{R}$, $f(x) = \int_{\frac{\pi}{4}}^{\arcsin x} \ln(1 + \sin^2 t)dt$. Să se arate că:

(i) f este derivabilă şi să se calculeze $f\,'(x)$;

(ii) f este integrabilă şi să se calculeze $\int_0^{\frac{1}{\sqrt{2}}} f(x)dx$.

Admitere Universitatea de Vest, Timişoara

37. Se consideră funcţia $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \frac{2x^3 + x}{x^2 + 1}$.

a) Să se calculeze $\int_0^1 f(x)dx$.

b) Să se arate că funcţia f este bijectivă.

c) Să se calculeze $\int_0^{\frac{3}{2}} f^{-1}(x)dx$.

Bacalaureat

38. Se consideră funcţiile $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 3 + \{x\}(1 - \{x\})$ şi $F : \mathbb{R} \to \mathbb{R}$, $F(x) = \int_0^x f(t)dt$.

a) Să se arate că $f(x + 1) = f(x)$, $\forall\, x \in \mathbb{R}$.

b) Să se arate că f este continuă în punctul $x = 1$.

c) Să se verifice că $F(x) = 3x + \frac{x^2}{2} - \frac{x^3}{3}$, $\forall\, x \in [0, 1)$.

d) Să se arate că $3 \le f(x) \le 4$, $\forall\, x \in \mathbb{R}$.

e) Să se calculeze $\lim\limits_{x\to\infty} F(x)$.

f) Să se arate că există $a \in \mathbb{R}$, astfel încât funcţia $G : \mathbb{R} \to \mathbb{R}$, $G(x) = F(x) - ax$ să fie periodică, având perioada egală cu 1.

Bacalaureat

39. Se consideră şirul $(a_n)_{n\ge1}$, $a_n = 1 - \frac{1}{3} + \frac{1}{5} - \ldots + \frac{(-1)^n}{2n+1}$, $\forall\, n \in \mathbb{N}^*$.

a) Să se arate că $\frac{1}{1+x^2} = 1 - x^2 + x^4 - \ldots + (-1)^{2n} x^{2n} + (-1)^{n+1} \frac{x^{2n+2}}{1+x^2}$, $\forall\, x \in [0, 1]$, $\forall\, n \in \mathbb{N}^*$.

b) Să se arate că $0 \le \frac{x^{2n+2}}{1+x^n} \le x^{2n+2}$, $\forall\, x \in [0, 1]$, $\forall\, n \in \mathbb{N}^*$.

c) Să se arate că $\lim\limits_{n\to\infty} \int_0^1 \frac{x^{2n+2}}{1+x^2} dx = 0$.

d) Să se calculeze $\int_0^1 \frac{1}{1+x^2} dx$.

e) Să se arate că $\lim\limits_{n\to\infty} a_n = \frac{\pi}{4}$.

f) Să se calculeze $\lim\limits_{n\to\infty} n\left(a_{2n} - \frac{\pi}{4}\right)$.

Bacalaureat

40. Se consideră $n \in \mathbb{N}^*$ şi funcţiile $f : [0, \infty) \to \mathbb{R}$, $f(x) = e^{-x} \cdot x^n$, $g : [0, \infty) \to \mathbb{R}$, $g(x) = 1 - e^{-x}\left(1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!}\right)$ şi $h : [0, \infty) \to \mathbb{R}$, $h(x) = \frac{1}{n!}\int_0^x f(t)dt$.

a) Să se arate că $g'(x) = h'(x)$ şi $g(x) = h(x)$, $\forall\, x \geq 0$.

b) Să se arate că $0 \leq g(x) \leq \dfrac{e^{-x} \cdot x^{n+1}}{n!}$, $\forall\, x \in [0, n]$.

c) Să se arate că dacă $x \geq 0$, atunci $\lim\limits_{n\to\infty} \dfrac{x^n}{n!} = 0$.

d) Să se demonstreze că: $\lim\limits_{n\to\infty}\left(1+\dfrac{x}{1!}+\dfrac{x^2}{2!}+\ldots+\dfrac{x^n}{n!}\right)=e^x$, $\forall\, x \geq 0$.

Bacalaureat

41. Pentru $n \in \mathbb{N}$ se consideră funcţiile: $f_n : \left(0, \dfrac{\pi}{2}\right) \to \mathbb{R}$, $f_n(x) = \dfrac{\operatorname{tg}^n x}{\operatorname{tg}^n x + \operatorname{ctg}^n x}$,

$g_n : \left(0, \dfrac{\pi}{2}\right) \to \mathbb{R}$, $g_n(x) = \dfrac{\operatorname{ctg}^n x}{\operatorname{tg}^n x + \operatorname{ctg}^n x}$, $x \in \left(0, \dfrac{\pi}{2}\right)$.

a) Să se arate că $f_n\left(\dfrac{\pi}{2} - x\right) = g_n(x)$, $x \in \left(0, \dfrac{\pi}{2}\right)$.

b) Să se calculeze $\int_{\frac{\pi}{6}}^{\frac{\pi}{4}} f_1(x)dx$.

c) Să se arate că $\int_{\frac{\pi}{4}-a}^{\frac{\pi}{4}+a} f_n(x)dx = \int_{\frac{\pi}{4}-a}^{\frac{\pi}{4}+a} g_n(x)dx = a$, oricare ar fi $a \in \left(0, \dfrac{\pi}{4}\right)$.

d) Să se determine $\lim\limits_{n\to\infty} \int_a^b f_n(x)dx$, unde $0 < a < b < \dfrac{\pi}{4}$.

e) Să se determine $\lim\limits_{n\to\infty} \int_{\frac{\pi}{10}}^{\frac{\pi}{3}} f_n(x)dx$.

Bacalaureat

Soluții

Elemente de algebră

Legi de compoziție

7. b) Ținem seama că dacă $X = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \in H_1$, atunci $\det X = a^3 + b^3 + c^3 - 3abc$ $\in H_2$ și folosim $\det(XY) = \det X \cdot \det Y$. **9.** Elementul neutru este $(1, 0)$ iar elementele simetrizabile sunt $(1, b)$ și $(-1, b)$, unde $b \in \mathbb{Z}$. **10.** Dacă $*$ ar avea elementul neutru e, atunci $x * e = x$, $\forall\, x \in M$ și $e * x = e$, $\forall\, x \in M$ deci $x = e$, $\forall\, x \in M$, adică $M = \{e\}$ contrar ipotezei că M are cel puțin 2 elemente. **11.** $e_s * e_d = e_d$ (deoarece e_s este element neutru la stânga) și $e_s * e_d = e_s$ (deoarece e_d este element neutru la dreapta). Deci $e_s = e_d = e$ și atunci $x * e = e * x = x$, $\forall\, x \in M$, adică e este element neutru. **12.** $x_s' =$ $= x_s' * e = x_s' * (x * x_d') = (x_s' * x) * x_d' = e * x_d' = x_d'$. Așadar $x_s' = = x_d' = x'$ și atunci $x' * x = x * x' = e$, adică x este simetrizabil.

Grupuri

6. c) Dacă $a + bi \in U(\mathbb{Z}[i]) \Rightarrow \exists\, c + di \in \mathbb{Z}[i]$ cu $(a + bi)(c + di) = 1 \Rightarrow |\, a + bi\,|^2 \cdot$ $\cdot\, |\, c + di\,|^2 = 1 \Rightarrow (a^2 + b^2)(c^2 + d^2) = 1 \Rightarrow a^2 + b^2 = 1$ etc. **7.** Ținem seama că $(u_1^2 + v_1^2)(u_2^2 + v_2^2) = (u_1u_2 + v_1v_2)^2 + (u_1v_2 - u_2v_1)^2$, deci înmulțirea este operație algebrică pe M. Pentru determinarea $U(M)$, observăm că $U(M) \subseteq U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$. Se constată că $1, -1 \in M$, iar $i, -i \notin M$. Rezultă că $U(M) = \{-1, 1\} = U_2$. **8.** 1) Elementul neutru este $e = -\dfrac{c}{b}$; 2) $U(\mathbb{Z}) = \{3, 5\}$. **18.** Elementul neutru este I_3, iar $U(M) =$ $= M \setminus \{X\}$, unde $X = \dfrac{1}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$. **19.** Elementul-unitate este matricea $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, care nu este I_3. De aceea inversabilitatea în G nu are legătură cu inversabilitatea în monoidul $(\mathcal{M}_3(\mathbb{R}), \cdot)$ sau în grupul $(GL_3(\mathbb{R}), \cdot)$. **20.** Elementul neutru este $E = \dfrac{1}{3}\begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix}$, iar $U(M) = M \setminus \{0_3\}$. **22.** a) $U(F) = \{f_1\}$; b) $U(G) = \{g_1, g_{-1}\}$. **23.** $U(M) = \{f_{1,1}; f_{1,-1}; f_{-1,1}; f_{-1,-1}\}$. **30.** O matrice aparține lui G_n dacă și numai dacă

elementele sale sunt numere naturale şi suma elementelor pe fiecare linie şi pe fiecare coloană este egală cu 1. Dacă $A = (a_{ij})$, $B = (b_{ij}) \in G_n$, iar $AB = (c_{ij})$, atunci $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$. Suma elementelor pe linia i în matricea AB este: $\sum_{j=1}^{n} c_{ij} = \sum_{j=1}^{n}\left(\sum_{k=1}^{n} a_{ik}b_{kj}\right) =$
$= \sum_{k=1}^{n}\left(\sum_{j=1}^{n} a_{ik}b_{kj}\right) = \sum_{k=1}^{n}\left(a_{ik}\sum_{j=1}^{n} b_{kj}\right) = \sum_{k=1}^{n} a_{ik} = 1$ şi analog suma elementelor pe coloana j în matricea AB este $\sum_{i=1}^{n} c_{ij} = 1$. Rezultă că $AB \in G_n$, deci înmulţirea este operaţie pe G_n. Elementul neutru este I_n, iar inversa unei matrice $A \in G_n$ este tocmai matricea transpusă $A^t \in G_n$. Într-adevăr, dacă $A = (a_{ij})$, atunci $A^t = (b_{ij})$ unde $b_{ij} = a_{ji}$ şi notând $AA^t = (c_{ij})$, avem $c_{ii} = \sum_{k=1}^{n} a_{ik}b_{ki} = \sum_{k=1}^{n} a_{ik}^2 = 1$, iar pentru $i \neq j$ avem $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=1}^{n} a_{ik}a_{jk} =$
$= \sum_{k=1}^{n} 0 = 0$. În consecinţă $AA^t = I_n$ şi analog $A^tA = I_n$. Aşadar $(G_n, \cdot)$ este un grup.
31. Fie a un element care nu aparţine mulţimii G. Luăm $M = G \cup \{a\}$ şi „prelungim" operaţia $*$ de pe G pe M astfel: $a * x = x * a = a$, $\forall\, x \in G$ şi $a * a = a$ (adică a este un element „absorbant"). Se arată că $(M, *)$ este un monoid care nu e grup (a este neinversabil), iar $G = U(M)$.

Reguli de calcul, subgrupuri

1. $(m, n) = 1 \Rightarrow \exists\, a,b \in \mathbb{Z}$ cu $am + bn = 1 \Rightarrow xy = (xy)^{am+bn} = \left((xy)^m\right)^a \left((xy)^n\right)^b =$
$= \left((yx)^m\right)^a \left((yx)^n\right)^b = (yx)^{am+bn} = yx$, $\forall\, x,y \in G$. **2.** Înlocuim x cu ax şi obţinem $(ax)^3 = aaxa$, adică $axaxax = aaxa$. Simplificăm la stânga cu a şi rezultă $x(axa)x =$ $= axa$ sau, folosind ipoteza, $xx^3x = x^3$. Aşadar $x^5 = x^3$ sau $x^2 = e$, $\forall\, x \in G$ şi atunci grupul este abelian. **4.** Se arată prin inducţie că $y^{3^n} = xy^nx$, $\forall\, n \in \mathbb{N}^*$. Atunci, pentru $n = 3$, avem $y^9 = xy^3x = x(xyx)x = (x^2)y(x^2) = y$ adică $y^9 = y$, de unde $y^8 = e$. **7.** $\{e\}$; $\{e, a\}$; $\{e, b\}$; $\{e, c\}$; $\mathbb{K} = \{e, a, b, c\}$. **10.** $e \in H = G \setminus \{a\} \Rightarrow a \neq e$. Arătăm că $G = \{e, a\}$. Fie $x \in H$ oarecare; cum $a \notin H \Rightarrow ax \notin H \Rightarrow ax = a \Rightarrow x = e \Rightarrow$ $H = \{e\} \Rightarrow G \setminus \{a\} = \{e\} \Rightarrow G = \{e, a\}$. **11.** Din enunţ, rezultă $|G| \geq 3$. Este suficient să arătăm că $|G| > 3 \Rightarrow |G| = 4$. Într-adevăr, dacă G are mai mult de 3 elemente, fie $x \in G \setminus \{e, a, b\}$ arbitrar. Ecuaţia $xu = a$ cu necunoscuta u are soluţie unică în G. Cum $x \in H$ şi $a \in G \setminus H$, rezultă $u \in G \setminus H$, adică $u \in \{a, b\}$. Dacă $u = a$, rezultă $x = e$, absurd. Aşadar $u = b$, deci $x = au^{-1} = ab^{-1}$, adică x este unic determinat. În concluzie $G = \{e, a, b, ab^{-1}\}$, adică $|G| = 4$. **12.** Presupunem prin absurd $G = H_1 \cup H_2$, cu H_1, H_2 subgrupuri proprii. Atunci $\exists\, x \in G \setminus H_1$ şi $\exists\, y \in G \setminus H_2$, de unde rezultă că $x \in H_2$ şi $y \in H_1$. Cum $y \in H_1$ şi $x \in G \setminus H_1 \Rightarrow xy \in G \setminus H_1$. Analog $x \in H_2$, $y \in G \setminus H_2 \Rightarrow$

$xy \in G \setminus H_2$. Dar $xy \in G = H_1 \cup H_2$, deci $xy \in H_1$ sau $xy \in H_2$, contradicție. **17.** $Z(\mathbb{C}_8) = \{-1, 1\}$. **18.** Presupunem prin absurd că $\exists\ \sigma \in Z(S_n)$, $\sigma \neq e$. Atunci $\exists\ i \in \{1, 2, \dots, n\}$ cu $\sigma(i) = j, j \neq i$. Cum $n \geq 3$, $\exists\ k \in \{1, 2, \dots, n\}$, $k \neq i$, $k \neq j$. Notăm cu τ permutarea care duce pe j în k, pe k în j și invariază toate celelalte elemente (τ este transpoziția (jk)). Cum $\sigma \in Z(S_n)$ avem $\sigma\tau = \tau\sigma$ și atunci $(\sigma\tau)(i) = (\tau\sigma)(i) \Rightarrow \sigma(\tau(i)) = \tau(\sigma(i)) \Rightarrow \sigma(i) = \tau(j) \Rightarrow i = k$, contradicție. **19.** Din ipoteză avem $|Z(G)| > \frac{1}{2}|G|$ și cum $|Z(G)|$ divide $|G|$ (teorema lui Lagrange), rezultă $|Z(G)| = |G|$, deci $Z(G) = G$ și atunci G este abelian. **20.** E suficient să demonstrăm afirmația pentru grupul $(U_n, \cdot)$ și pentru grupul $(\mathbb{Z}, +)$. **21.** $\{\hat{0}\}$; $\{\hat{0}, \hat{2}\} = <\hat{2}>$; $\mathbb{Z}_4$. **22.** $\{\hat{0}\}$; $\mathbb{Z}_5$. **23.** $\{\hat{0}\}$; $\{\hat{0}, \hat{2}, \hat{4}\} = <\hat{2}>$; $\{\hat{0}, \hat{3}\} = <\hat{3}>$; $\mathbb{Z}_6$. **24.** Se aplică teorema lui Lagrange. **25.** b) Când $G = \mathbb{C}^*$, $H = U_k$ avem $G_H = \{z \in \mathbb{C}^* \mid \exists\ n \in \mathbb{N}^* \text{ cu } z^n = 1\}$ = subgrupul elementelor de ordin finit (toate rădăcinile unității) din grupul $\mathbb{C}^*$. **26.** $1° \Rightarrow 2°$. Presupunem că orice parte stabilă este subgrup și fie $x \in G$. Atunci $H = \{x, x^2, x^3, \dots, x^n, \dots\}$ este parte stabilă, deci subgrup și atunci $e \in H$. Deci $\exists\ n \in \mathbb{N}^*$ cu $x^n = e$, ceea ce arată că x are ordin finit. $2° \Rightarrow 1°$. Presupunem că orice element din G are ordin finit. Fie $H \subseteq G$ o parte stabilă. Arătăm că $\forall\ x \in H \Rightarrow x^{-1} \in H$ și va rezulta că H este subgrup. Fie așadar $x \in H$ și n ordinul lui x. Atunci $x^n = e$ sau $x^{n-1}x = xx^{n-1} = e$, adică $x^{-1} = x^{n-1}$. Dar $x^{n-1} \in H$, căci H este parte stabilă. Rezultă că $x^{-1} \in H$, deci H este subgrup al lui G. **27.** a) Presupunem prin absurd $k > 2$. Luăm $x,y \in G$, $x \neq e$, $y \neq e$, $x \neq y$. Cum $n-3 \geq k-2$ putem alege elementele distincte $a_1, a_2, \dots, a_{k-2} \in G \setminus \{e, x, y\}$. Atunci, conform ipotezei, submulțimile $H_1 = \{e, x, a_1, a_2, \dots, a_{k-2}\}$ și $H_2 = \{e, y, a_1, a_2, \dots, a_{k-2}\}$ sunt subgrupuri ale lui G. Cum $xa_1 \in H_1$ și $xa_1 \neq a_1$, $xa_1 \neq x$ rezultă $xa_1 \in \{e, a_2, a_3, \dots, a_{k-2}\}$, deci $x \in \{a_1^{-1}, a_2a_1^{-1}, a_3a_1^{-1}, \dots, a_{k-2}a_1^{-1}\} \subseteq H_2$ (căci H_2 este subgrup), deci $x \in H_2$, absurd. Așadar $k = 2$. b) Dacă $x \in G$, $x \neq e$, deoarece $k = 2$, conform ipotezei submulțimea $\{e, x\}$ este un subgrup al lui G de ordin 2, prin urmare $x^2 = e$.

Morfisme și izomorfisme de grupuri

8. $f : (G, *) \to (\mathbb{R}, +)$, $f(x) = \operatorname{tg} x$ este izomorfism de grupuri. **9.** Se ține seama de tabla operației. **10.** $f : (G, \circ) \to (\mathbb{R}_+^*, \cdot)$, $f(f_a) = a$ este izomorfism de grupuri. **12.** $\{e\}$; $\mathbb{Z}_2$; $\mathbb{Z}_3$; $\mathbb{Z}_4$; $\mathbb{K}$; $\mathbb{Z}_5$; $\mathbb{Z}_6$; S_3; $\mathbb{Z}_7$. **13.** Din ipoteză rezultă că G conține un cel mai mic număr strict pozitiv x_0. Fie $x \in G$ arbitrar. Luând $k = \left[\frac{x}{x_0}\right] \in \mathbb{Z}$, avem $k \leq \frac{x}{x_0} < k + 1$, de unde $0 \leq x - kx_0 < x_0$. Cum $x, x_0 \in G \Rightarrow x - kx_0 \in G$ și ținând seama de minimalitatea lui x_0, rezultă $x - kx_0 = 0$, deci $x = kx_0 \in <x_0>$. Așadar $G = <x_0>$, adică G este grup ciclic infinit, prin urmare $G \simeq \mathbb{Z}$. **14.** În $(\mathbb{Q}, +)$ avem proprietatea: $\forall$ $a \in \mathbb{Q}$, $\forall\, n \in \mathbb{N}^*$, $\exists\, b \in \mathbb{Q}$ cu $nb = a$, în timp ce în $(\mathbb{Z}, +)$ nu este valabilă această proprietate. **15.** Ecuația $x^2 = 1$ are în $(\mathbb{R}^*, \cdot)$ două soluții, iar în $(\mathbb{R}_+^*, \cdot)$ o singură soluție. **16.** Pentru $n \geq 3$ ecuația $x^n = 1$ are în $(\mathbb{R}^*, \cdot)$ cel mult două soluții, pe când în $(\mathbb{C}^*, \cdot)$ are n soluții. **17.** $x \circ y = yx$. **18.** Se arată că $f(x) = xf(1)$, $\forall\, x \in \mathbb{Q}$. **19.** Notând $f_a : \mathbb{Q} \to \mathbb{Q}$, $f_a(x) = ax$ pentru fiecare $a \in \mathbb{Q}$, rezultă că endomorfismele lui $(\mathbb{Q}, +)$ sunt toate funcțiile f_a, $a \in \mathbb{Q}$, iar automorfismele lui $(\mathbb{Q}, +)$ sunt funcțiile f_a, cu $a \in \mathbb{Q}^*$. **20.** Cu notația din ex. 19, endomorfismele lui $(\mathbb{Z}, +)$ sunt funcțiile f_a, $a \in \mathbb{Z}$, iar automorfismele lui $(\mathbb{Z}, +)$ sunt $f_1 = 1_{\mathbb{Z}}$ și $f_{-1} = -1_{\mathbb{Z}}$. **21.** Morfismul nul. **22.** Dacă prin absurd $\exists\, G$ subgrup propriu al lui $\mathbb{Q}$ și un izomorfism de grupuri $f : \mathbb{Q} \to G$, atunci $f(x) = ax$ cu $a \in G$, $a \neq 0$, deci $\operatorname{Im} f = \mathbb{Q}$, adică $G = \mathbb{Q}$, contradicție. **26.** Fie $x \in H$ arbitrar și $a \in G \setminus H$ fixat. Cum $ax \in G \setminus H \Rightarrow f_1(ax) = f_2(ax) \Rightarrow f_1(a)f_1(x) = f_2(a)f_2(x)$. Dar $f_1(a) = f_2(a)$ și atunci $f_1(x) = f_2(x)$, $\forall\, x \in H$.

Inele și corpuri

3. c) $a + b\zeta \in U(\mathbb{Z}[\zeta]) \Leftrightarrow \exists\, c + d\zeta \in \mathbb{Z}[\zeta]$ cu $(a + b\zeta)(c + d\zeta) = 1$, $(a,b,c,d \in \mathbb{Z})$. Trecem la module și ridicăm la pătrat și avem $|a + b\zeta|^2 |c + d\zeta|^2 = 1$, adică $(a^2 + ab + b^2)(c^2 + cd + d^2) = 1$, de unde $a^2 + ab + b^2 = 1$. Rezolvăm această ecuație în $\mathbb{Z} \times \mathbb{Z}$, gândind-o mai întâi ca o ecuație de gradul doi în a. Obținem $(a, b) \in \{(0, -1), (1, -1), (1, 0), (-1, 0), (-1, 1), (0, 1)\}$ și de aici $U(\mathbb{Z}[\zeta]) = \{-\zeta, 1 - \zeta, 1, -1, -1 + \zeta, \zeta\}$ $= \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\} = U_6$; am ținut seama că $\zeta = \dfrac{1 + i\sqrt{3}}{2} = \cos\dfrac{2\pi}{6} + i\sin\dfrac{2\pi}{6} \in U_6$. **4.** b) $U(\mathbb{Z}[i], +, *) = \{\pm 1 + bi \mid b \in \mathbb{Z}\}$. **6.** b) Dacă A are divizori ai lui zero, există $X_1 = \begin{pmatrix} a_1 & b_1 \\ db_1 & a_1 \end{pmatrix} \neq 0$, $X_2 = \begin{pmatrix} a_2 & b_2 \\ db_2 & a_2 \end{pmatrix} \neq 0$ astfel încât $X_1X_2 = 0_2$. Rezultă ușor $b_1 \neq 0$, $b_2 \neq 0$ și cum $\det(X_1X_2) = 0$, avem $\det(X_1) = 0$ sau $\det(X_2) = 0$. Așadar $d = \left(\dfrac{a_1}{b_1}\right)^2$ sau $d = \left(\dfrac{a_2}{b_2}\right)^2$, adică d este pătratul unui număr rațional. Cum $d \in \mathbb{Z}$, rezultă că d este pătratul unui număr întreg (pătrat perfect). Reciproc, dacă d este pătrat perfect, luând $X_1 = \begin{pmatrix} \sqrt{d} & 1 \\ d & \sqrt{d} \end{pmatrix}$, $X_2 = \begin{pmatrix} -\sqrt{d} & 1 \\ d & -\sqrt{d} \end{pmatrix}$, avem $X_1 \neq 0_2$, $X_2 \neq 0_2$ dar $X_1X_2 = 0_2$, adică inelul A are divizori ai lui zero. c) Cum $A \subseteq \mathcal{M}_2(\mathbb{Z})$ şi $U(\mathcal{M}_2(\mathbb{Z})) = \{X \mid \det X = \pm 1\}$, deducem că $X \in U(A) \Rightarrow \det X = \pm 1$. i) Dacă $d = 0$, avem $A = \left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| a \in \mathbb{Z}\right\}$, deci $X = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \Rightarrow \det X = a^2$. Aşadar $X \in U(A) \Rightarrow a^2 = 1 \Rightarrow a = \pm 1$, deci $U(A) =$ $= \{I_2, -I_2\}$. ii) Dacă $d = -1$, avem $A = \left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{Z}\right\}$, deci $X = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \Rightarrow$ $\det X = a^2 + b^2$. Atunci $X \in U(A) \Rightarrow a^2 + b^2 = 1 \Rightarrow (a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$, deci $U(A) = \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}\right\}$. iii) Dacă $d \leq -2$, $\det X = \pm 1$ $\Rightarrow a^2 + db^2 = 1 \Rightarrow a = \pm 1,\ b = 0 \Rightarrow U(A) = \left\{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right\} = \{I_2, -I_2\}$.

7. b) $XY = 0_3$. c) Ca şi în problema precedentă $X \in U(A) \Rightarrow \det X = \pm 1$. Dacă $X = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \in U(A)$ atunci $\det X = a^3 + b^3 + c^3 - 3abc = \frac{1}{2}(a+b+c)\left[(a-b)^2 + (b-c)^2 + (c-a)^2\right] =$ $= \pm 1$, duce la $(a+b+c)\left[(a-b)^2 + (b-c)^2 + (c-a)^2\right] = \pm 2$. Paranteza mare fiind pozitivă, trebuie să fie egală cu 2 (dacă ar fi egală cu 0, atunci $a = b = c$, deci $\det X =$ 0, iar dacă ar fi egală cu 1, rezultă $(a - b)^2 = 1$, $(b - c)^2 = 0$, $(c - a)^2 = 0$ sau analoagele, de unde iarăşi $a = b = c$, deci $\det X = 0$). Dar $(a-b)^2 + (b-c)^2 + (c-a)^2 = 2$ duce la $(a - b)^2 = 1$, $(b - c)^2 = 1$, $(c - a)^2 = 0$ sau analoagele, de unde $a - b = \pm 1$, $b - c = \pm 1$, $c = a$, deci $a = c = b \pm 1$. Scriind că $a + b + c = 1$ sau $a + b + c = -1$ obţinem $a = c = 0$, $b = \pm 1$ şi analoagele, de unde deducem că $U(A)$ este cel din enunţ. **9.** b) Dacă $f \neq 0$ este divizor al lui zero, $\exists\ g \in A$, $g \neq 0$ cu $fg = 0$. Cum $g \neq 0$, $\exists\ x_0 \in \mathbb{R}$ cu $g(x_0) \neq 0$ şi cum g este funcţie continuă, există un interval I (neredus la un punct) astfel încât $g(x) \neq 0$, $\forall\ x \in I$; rezultă $f(x) = 0$, $\forall\ x \in I$. Reciproc, dacă f se anulează pe un interval $I = (a, b)$, definim funcţia $g : \mathbb{R} \to \mathbb{R}$ prin $g(x) = \begin{cases} 0, & x \notin I \\ (x-a)(x-b), & x \in I \end{cases}$ şi avem $g \in A$, $g \neq 0$ şi $fg = 0$, ceea ce arată că f este divizor al lui zero în inelul A.

Morfisme şi izomorfisme de inele şi corpuri

1. a) Se ţine seama de faptul că numerele $C_p^1, C_p^2, \ldots, C_p^{p-1}$ se divid cu p, dacă p este prim. b) Se ţine seama de faptul că $f \circ f \circ \ldots \circ f$ (de n ori) este tot un endomorfism, **8.** Funcţia $f : (\mathbb{Q}, +, \cdot) \to (K, +, \circ)$, $f(a) = f_a$ este un izomorfism de corpuri.

9. $f : (K, +, \circ) \to (\mathbb{Q}, +, \cdot)$, $f(f_a) = a$ este un izomorfism de corpuri. **11.** Funcţia

$f : K \to \mathbb{H}$, $f(\lambda_0 e_0 + \lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3) = \lambda_0 + \lambda_1 i + \lambda_2 j + \lambda_3 k$ este un izomorfism de corpuri. **17.** $f = 1_{\mathbb{Z}}$ şi $f = 0$ (care este un endomorfism neunitar). **18.** Automorfismul identic şi automorfismul conjugare pătratică. **19.** Dacă f este un endomorfism al lui $\mathbb{R}$, mai întâi e clar că $f(x) = x$, $\forall\ x \in \mathbb{Q}$. Apoi, dacă $x > 0 \Rightarrow f(x) = f\left(\sqrt{x}\cdot\sqrt{x}\right) = f\left(\sqrt{x}\right)\cdot f\left(\sqrt{x}\right) > 0$, iar dacă $x_1 < x_2 \Rightarrow x = x_2 - x_1 > 0 \Rightarrow f(x_2 - x_1) > 0 \Rightarrow f(x_1) < f(x_2)$, deci f este funcţie strict crescătoare. Dacă $x \in \mathbb{R} \setminus \mathbb{Q}$, există şirurile $(x'_n) \subseteq \mathbb{Q}$ şi $(x''_n) \subseteq \mathbb{R} \setminus \mathbb{Q}$, convergente la x, primul strict crescător, al doilea strict descrescător. Deci $x'_n < x < x''_n$, $\forall\ n \in \mathbb{N}^* \Rightarrow f(x'_n) < f(x) < f(x''_n) \Rightarrow x'_n < f(x) < x''_n$, $\forall\ n \in \mathbb{N}^*$ şi trecând la limită când $n \to \infty$, rezultă $x \le f(x) \le x$, adică $f(x) = x$. Aşadar $f(x) = x$, $\forall x \in \mathbb{R}$, adică $f = 1_{\mathbb{R}}$ este singurul endomorfism al corpului $\mathbb{R}$.

Forma algebrică a unui polinom, funcţia polinomială

1. a) 2 dacă $m \in \mathbb{Z}\setminus\{-1; 0\}$; 1 dacă $m = 0$; 0 dacă $m = -1$; b) 4 dacă $m \in \mathbb{Q} \setminus \left\{-\frac{2}{3}, \frac{2}{3}\right\}$; 2 dacă $m = -\frac{2}{3}$; 3 dacă $m = \frac{2}{3}$; c) 3 dacă $m \in \mathbb{R} \setminus \left\{\pm\sqrt{2}, \pm\sqrt{3}\right\}$; 1 dacă $m = \pm\sqrt{2}$; 2 dacă $m = \pm\sqrt{3}$; d) 5 dacă $m \in \mathbb{C} \setminus \{\pm 1, \pm i\}$; 4 dacă $m = \pm 1$; 2 dacă $m = \pm i$.

5. $f = aX$, cu $a \in K$. **7.** a) Fie $n = \text{grad}(f)$, $m = \text{grad}(g)$. Din $f\left(\frac{1}{x}\right) = \frac{1}{x^n} f(x)$ şi $g\left(\frac{1}{x}\right) = \frac{1}{x^m} g(x)$ rezultă prin înmulţire că $(fg)\left(\frac{1}{x}\right) = \frac{1}{x^{n+m}} (fg)(x)$.

Împărţirea cu rest, divizibilitatea polinoamelor, polinoame ireductibile

1. a) $q = 2X^3 + 4X^2 - 11X + 23$; $r = -2X - 45$; d) $q = \frac{1+i}{2} X^2 + \frac{2-i}{2} X - \frac{1+5i}{4}$; $r = \frac{-13+3i}{2} X + \frac{5+5i}{4}$. **2.** c) $q = \pi X^2 + (2-\pi^2)X + \pi^3 - 3\pi - 1$; $r = -\pi^4 + 3\pi^2 + \pi + 1$; d) $q = (2+3i)X^4 + (2-3i)X^3 - (3+2i)X^2 + (-2+3i)X + 4 + 2i$; $r = 1 - 4i$.

3. $m = \pm\frac{1}{2}$. **5.** $m = 15$; $n = -33$. **9.** a) 1; b) $X^2 - 1$; c) $X - i$.

13. $(X-1)^{1500}(X-2)^{500}\left(X^2 + X + 1\right)^{1000}$; b) $(X-1)^{20}(X+1)^{20}\left(X^2+1\right)^{10}$.

15. $f = (X+\hat{3})(X^2 + \hat{2}X + \hat{4})$. **16.** $f = (X+a)^p$. **17.** $f = \prod_{k=0}^{n-1}\left(X - 2\cos\frac{2k\pi}{n} - i\sin\frac{2k\pi}{n}\right)$.

18. a) $f=(X-1)(X+1)\cdot\prod_{k=1}^{n-1}\left(X^2-2\cos\frac{k\pi}{n}X+1\right)$; b) $f=(X-1)\prod_{k=1}^{n}\left(X^2-2\cos\frac{2k\pi}{2n+1}X+1\right)$.

Rădăcini ale polinoamelor, descompunerea în factori liniari, ecuații algebrice

2. Presupunem grad(f) ≥ 1. Dacă $x_0 \in \mathbb{C}$ este rădăcină pentru f, atunci x_0+1, x_0+2, x_0+3, ... sunt rădăcini pentru f, contradicție. **3.** $f=0$. **4.** $f=a(X-1)$, $a\in\mathbb{C}$.

5. $f=\frac{1}{n!}(X+1)(X+2)...(X+n)$ și se obține prin inducție. **6.** $a_1=-1$; $b_1=-2$; $c_1=2$ când rădăcinile lui f sunt $x_1=x_2=1$, $x_3=-1+i$, $x_4=-1-i$ și rădăcinile lui g sunt $x_1'=x_2'=1$, $x_3'=-2$ sau $a_2=-1$, $b_2=2$, $c_2=-2$ când rădăcinile lui f sunt $x_1=$ $=x_2=-1$, $x_3=1+i$, $x_4=1-i$ și rădăcinile lui g sunt $x_1'=x_2'=-1$, $x_3'=2$.

7. Dacă, prin absurd, f ar avea o rădăcină multiplă x_0, atunci $f(x_0)=0$ și $f'(x_0)=0$, de unde prin scădere rezultă $x_0=0$, contradicție. **8.** a) 0; b) $-2i$; c) -3; d) -2.

9. Dacă, prin absurd, f are cel puțin 3 rădăcini reale x_1, x_2, x_3, din $x_1+x_2+x_3+x_4=$ $=-(a+1)$ rezultă $x_4\in\mathbb{R}$, deci constatăm că toate rădăcinile sunt reale; atunci $0\leq x_1^2+x_2^2+x_3^2+x_4^2=(a+1)^2-2\left(a^2+\frac{a}{2}+1\right)=-a^2+a-1<0$, contradicție.

10. $y^3+(b-3)y^2+(a-2b)y-a+b=0$. **11.** $m=-1$, $x_1=3$, $x_2=4$, $x_3=-2$.

12. $m=2$, $n=-1$, $x_1=x_2=x_3=1$, $x_4=\frac{-1+i\sqrt{3}}{2}$, $x_5=\frac{-1-i\sqrt{3}}{2}$.

13. $m=24$, $x_1=3$, $x_2=4$, $x_3=-2$. **14.** $m=124$, $x_1=\frac{5+\sqrt{13}}{2}$, $x_2=\frac{5+\sqrt{13}}{2}$, $x_3=\frac{5-\sqrt{13}}{2}$, $x_4=\frac{5-\sqrt{13}}{2}$. **15.** $m=30$, $x_1=2$, $x_2=-5$, $x_3=-1$, $x_4=3$.

16. Scriem $f=(X-x_1)(X-x_2)(X-x_3)(X-x_4)$ cu $x_1=a-3r$, $x_2=a-r$, $x_3=a+r$, $x_4=a+3r$, calculăm f' etc. **20.** 48 km/h, 60 km/h. **21.** a) $\zeta=\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5}$ verifică $\zeta^4+\zeta^3+\zeta^2+\zeta+1=0$; împărțim prin ζ^2 și notăm $x=\zeta+\frac{1}{\zeta}=2\cos\frac{2\pi}{5}$, obținând ecuația $x^2+x-1=0$. Cum $x>0$, rezultă $\cos\frac{2\pi}{5}=\frac{x}{2}=\frac{-1+\sqrt{5}}{4}$. b) Analog, luând $\zeta=\cos\frac{2\pi}{7}+i\sin\frac{2\pi}{7}$. **22.** Notând cu $2x$, $2y$ bazele trapezului, avem sistemul: $4x+4y=20$, $\frac{(2x+2y)2\sqrt{xy}}{2}=20$ etc. Laturile sunt 8, 2, 5,5. **23.** Se arată prin inducție că $P_n=2^{n-1}X^n+...$, $Q_{n-1}=2^{n-1}X^{n-1}+...$.

Rezolvarea ecuațiilor algebrice cu coeficienți în $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$

1. $x_1 = 1 + i$, $x_2 = 1 - i$, $x_3 = -7$, $x_4 = 1$. **2.** $m = -23$, $n = 10$, $x_1 = 2 +$, $x_2 = 2 - i$, $x_3 = 1$, $x_4 = 2$. **3.** $m = 5$, $n = 2$, $x_1 = x_2 = i$, $x_3 = x_4 = -i$, $x_5 = -\frac{2}{5}$. **4.** $x_1 = 2\sqrt{5}$, $x_2 = -2\sqrt{5}$, $x_3 = \frac{-1+i\sqrt{3}}{2}$, $x_4 = \frac{-1-i\sqrt{3}}{2}$. **5.** $m = 7$, $n = 2$, $x_1 = -2 + \sqrt{6}$, $x_2 = -2 - \sqrt{6}$, $x_3 = -1$, $x_4 = -2$. **6.** $x_1 = \sqrt{3}$, $x_2 = i$, $x_3 = -\sqrt{3}$, $x_4 = -i$, $x_5 = -\frac{1}{3}$.
7. Rădăcinile întregi sunt $x_1 = -1$, $x_2 = 2$, iar celelalte rădăcini sunt $x_3 = \frac{1+i\sqrt{7}}{2}$, $x_4 = \frac{1+i\sqrt{7}}{2}$. **8.** Rădăcinile raționale sunt $x_1 = 1$, $x_2 = -3$, $x_3 = -\frac{1}{2}$, $x_4 = -\frac{1}{3}$, iar celelalte rădăcini sunt $x_5 = i$, $x_6 = -i$. **9.** Numărul rădăcinilor complexe nereale este par, căci fiecare rădăcină se grupează cu conjugata sa (unele asemenea grupări se pot repeta, în funcție de ordinul de multiplicitate al rădăcinilor respective). Cum gradul polinomului este impar, există cel puțin o rădăcină reală. **10.** Dacă prin absurd polinomul $f = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{Z}[X]$, cu n par și a_0, a_1, ..., a_n impare, ar avea o rădăcină rațională $x = \frac{p}{q}$, cu $p,q \in \mathbb{Z}$ și $(p, q) = 1$, atunci $f\left(\frac{p}{q}\right) = 0$, de unde ar rezulta $a_np^n + a_{n-1}p^{n-1}q + \ldots + a_1pq^{n-1} + a_0q^n = 0$ (1). Dar $p \mid a_0$ și $q \mid a_n$, deci p, q ar fi impare și atunci membrul stâng din (1) ar fi impar (fiind o sumă cu un număr impar de termeni impari), contradicție.

Probleme recapitulative

2. a) Din $(k, n) = 1 \Leftrightarrow \exists\, a,b \in \mathbb{Z}$ cu $ak + bn = 1$. Evident, f este endomorfism. Arătăm că f este injectiv, determinând nucleul lui f. Fie $x \in \operatorname{Ker} f$, deci $x^k = e$; deoarece $|G| = n$, avem și $x^n = e$, deci $x = x^{ak+bn} = (x^k)^a \cdot (x^n)^b = e$. Așadar $\operatorname{Ker} f = \{e\} \Rightarrow f$ injectiv și cum G este finit, f este bijectiv, deci f este automorfism. b) Dacă f_{k_1}, $f_{k_2} \in \Gamma$ avem $f_{k_1} \circ f_{k_2} = f_{k_1k_2} \in \Gamma$. Elementul neutru în Γ este $f_1 = 1_G$. Să observăm că pentru $k - k' = \mathcal{M}n$ avem $f_k = f_{k'}$; într-adevăr, $k - k' = qn \Rightarrow f_k(x) = x^k = x^{k'+qn} = x^{k'}(x^n)^q = x^{k'} = f_{k'}(x)$, $\forall\, x \in G$. Să determinăm inversul unui automorfism din Γ. Fie $f_k \in \Gamma$. Cum $(k, n) = 1$, $\exists\, a,b \in \mathbb{Z}$ cu $ak + bn = 1 \Rightarrow ak - 1 = \mathcal{M}n \Rightarrow f_{ak} = f_1 \Rightarrow f_a \circ f_k = f_k \circ f_a = 1_G$, deci $f_k^{-1} = f_a \in \Gamma$. Rezultă că $(\Gamma, \circ)$ este un grup abelian. Pentru $k \in \mathbb{Z}$, $(k, n) = 1$ avem $k - r = \mathcal{M}n$, unde r este restul împărțirii lui k prin n și atunci

$f_k = f_r$. Dacă $r_1 = 1$, r_2, ..., $r_{\varphi(n)}$ sunt toate resturile pe care le dau numerele întregi prime cu n la împărțirea cu n, vom avea egalitatea $\Gamma = \{f_{r_1}, f_{r_2}, \dots, f_{r_{\varphi(n)}}\}$, deci, Γ este un grup finit. Când $G = \mathbb{K}$ avem $\Gamma = \{f_1, f_3\}$; dar $f_1 = f_3$, căci $f_3(x) = x^3 = x = f_1(x)$, $\forall\, x \in \mathbb{K}$, prin urmare $|\Gamma| = 1$. Când $\Gamma = U_n$, rezultă că $f_{r_1}, f_{r_2}, \dots, f_{r_{\varphi(n)}}$ sunt distincte două câte două și prin urmare $|\Gamma| = \varphi(n)$. **3.** Fie $A \in G_n$, $A = (a_{ij})$. Luând un $i \in \{1, 2, \dots, n\}$, există un unic $j \in \{1, 2, \dots, n\}$ astfel încât $a_{ji} = 1$ și definim permutarea $\sigma_A \in S_n$ prin $\sigma(i) = j$. Așadar $\sigma_A(i) = j \Leftrightarrow a_{ji} = 1$. Arătăm că funcția $f : G_n \to S_n$, $f(A) = \sigma_A$ este un izomorfism de grupuri. Fie $A = (a_{ij})$, $B = (b_{ij}) \in G_n$ și $AB = (c_{ij})$, unde $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$. Avem: $\sigma_{AB}(i) = j \Leftrightarrow c_{ji} = 1 \Leftrightarrow \sum_{k=1}^{n} a_{jk}b_{ki} = 1 \Leftrightarrow \exists!\, k \in \{1, 2, \dots, n\}$ cu $a_{jk} = b_{ki} = 1 \Leftrightarrow \sigma_A(k) = j$ și $\sigma_B(i) = k \Leftrightarrow (\sigma_A\sigma_B)(i) = j \Leftrightarrow \sigma_{AB} = \sigma_A\sigma_B \Leftrightarrow f(AB) = f(A)f(B)$, adică f este morfism de grupuri. Fie $A \in \operatorname{Ker} f \Leftrightarrow f(A) = e$ (permutarea identică) $\Leftrightarrow \sigma_A = e \Leftrightarrow e(i) = j$ dacă și numai dacă $a_{ji} = 1 \Leftrightarrow i = j$ dacă și numai dacă $a_{ji} = 1 \Leftrightarrow a_{ii} = 1$, $\forall\, i \in \{1, 2, \dots, n\}$ și $a_{ij} = 0$, $i \neq j \Leftrightarrow A = I_n$ (matricea unitate). Așadar $\operatorname{Ker} f = \{I_n\}$, adică f este un morfism injectiv. Întrucât $|G_n| = |S_n| = n!$, rezultă f este și surjectiv, deci f este izomorfism de grupuri. **5.** b) $I(G)$ este subgrup al lui $\operatorname{Aut}(G)$, deoarece $i_a \circ i_b = i_{ab} \in I(G)$ și $i_a^{-1} = i_{a^{-1}} \in I(G)$, $\forall\, a,b \in G$. c) Dacă G este abelian, $i_a(x) = axa^{-1} = x = i_e(x)$, deci $i_a = i_e$, $\forall\, a \in G$. Reciproc, dacă i_e este singurul automorfism interior, atunci $i_a = i_e$, $\forall\, a \in G$, deci $i_a \circ i_b = i_b \circ i_b = i_e$, $\forall\, a,b \in G$, adică $i_{ab} = i_{ba} \Rightarrow ab = ba$, $\forall\, a,b \in G$, deci G este abelian. **6.** a) $U_n \subseteq U_m \Rightarrow n \mid m$ (teorema lui Lagrange). Reciproc, $n \mid m \Rightarrow U_n \subseteq U_m$, deoarece $\forall\, x \in U_n \Rightarrow x^n = 1 \Rightarrow x^m = 1 \Rightarrow x \in U_m$. b) $U_n \cap U_m$ este subgrup al grupului $(\mathbb{C}^*, \cdot)$, deci $U_n \cap U_m = U_d$, cu $d \in \mathbb{N}^*$ și arătăm că $d = (n, m)$. Din $U_d \subseteq U_n$, $U_d \subseteq U_m$ rezultă $d \mid n$, $d \mid m$; fie acum $d' \in \mathbb{N}^*$ cu $d' \mid n$, $d' \mid m$, deci $U_{d'} \subseteq U_n$, $U_{d'} \subseteq U_m \Rightarrow U_{d'} \subseteq U_n \cap U_m = U_d \Rightarrow d' \mid d$. Rezultă că $d = (n, m)$. c) U_nU_m este subgrup finit al grupului $(\mathbb{C}^*, \cdot)$, deci $U_nU_m = U_k$, cu $k \in \mathbb{N}^*$ și arătăm egalitatea $k = [n, m]$. Din $U_n \subseteq U_k$, $U_m \subseteq U_k$ rezultă $n \mid k$, $m \mid k$; fie acum $k' \in \mathbb{N}^*$ cu $n \mid k'$, $m \mid k'$, deci $U_n \subseteq U_k$, $U_m \subseteq U_{k'} \Rightarrow U_k = U_nU_m \subseteq U_{k'} \Rightarrow k \mid k'$. Rezultă $k = [n, m]$. **8.** Aplicația $f : \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m$, $f(\hat{x}) = (\bar{x}, \dot{x})$ este un morfism injectiv de grupuri; cum $|\mathbb{Z}_{nm}| = |\mathbb{Z}_n \times \mathbb{Z}_m| = nm$, rezultă că f este bijectiv, deci este un izomorfism (am notat cu $\wedge$, $-$, $\cdot$ clasele de resturi din grupurile $\mathbb{Z}_{nm}$, $\mathbb{Z}_n$, $\mathbb{Z}_m$ respectiv). **12.** a) Avem $(1 + 1)^2 = 1 + 1$ adică $1 + 1 + 1 + 1 = 1 + 1$, deci $1 + 1 = 0$. b) Avem $(x + y)^2 = x + y \Leftrightarrow (x + y)(x + y) = x + y \Leftrightarrow x^2 + xy + yx + y^2 = x + y \Leftrightarrow x + xy + yx + y = x + y \Leftrightarrow xy + yx = 0 \Leftrightarrow xy = -yx \Leftrightarrow xy = yx$, $\forall\, x,y \in A$, deci A este inel comutativ. **13.** b) $x \notin U(A) \Rightarrow x^2 = 0 \Rightarrow (1 + x)(1 - x) = 1 - x^2 = 1 \Rightarrow (1 - x)^{-1} = 1 - x$. c) Fie $x,y \in A$; dacă $x,y \in U(A)$, deoarece $U(A)$ este grup abelian (căci $x^2 = 1$, $\forall\, x \in U(A)$) rezultă $xy = yx$; dacă $x \in U(A)$, $y \notin U(A) \Rightarrow x \in U(A)$, $1 + y \in U(A) \Rightarrow$

$x(1 + y) = (1+ y)x \Rightarrow xy = yx$; dacă $x \notin U(A)$, $y \in U(A)$ analog; dacă $x,y \notin U(A) \Rightarrow 1 + x,\ 1 + y \in U(A) \Rightarrow (1 + x)(1 + y) = (1 + y)(1 + x) \Rightarrow xy = yx$. **14.** Fie $|U(A)| = 2n + 1$, $n \in \mathbb{N}$. Cum $-1 \in U(A) \Rightarrow (-1)^{2n+1} = 1 \Rightarrow -1 = 1 \Rightarrow 1 + 1 = 0$. **15.** Din $x^3 = x$ rezultă $x^4 = x^2$. Prin calcul rezultă că $\left(x^2yx^2 - x^2y\right)^2 = \left(x^2yx^2 - yx^2\right)^2 = 0$. Atunci $x^2yx^2 - x^2y = \left(x^2yx^2 - x^2y\right)^3 = \left(x^2yx^2 - x^2y\right)^2\left(x^2yx^2 - x^2y\right) = 0$. Rezultă $x^2yx^2 = x^2y$, $\forall\, x,y \in A$ şi analog $x^2yx^2 = yx^2$, de unde $x^2y = yx^2$, $\forall\, x,y \in A$. Aşadar, pătratele elementelor din A comută cu toate elementele din A. Rezultă: $xy = x^3y^3 = x(x^2y^3) = xy^3x^2 = (xy^2)(yx^2) = (y^2x)(yx^2) = y(yx)(yx)x = y(yx)^2x = (yx)^2yx = (yx)^3 = yx$, $\forall\, x,y \in A$, deci A este inel comutativ. **16.** Presupunem prin absurd că există un izomorfism de grupuri $f : (A, +) \to (U(A), \cdot)$. Cum $-1 \in U(A)$ şi f este surjectiv, există $a \in A$ cu $f(a) = -1$. Atunci $f(a + a) = f(a)f(a) = (-1)\cdot(-1) = 1 = f(0)$ şi cum f este injectiv rezultă $a + a = 0$ sau $a(1 + 1) = 0$. Cum A este integru, rezultă $a = 0$ sau $1 + 1 = 0$. Dacă $a = 0 \Rightarrow f(a) = f(0) = 1$ şi cum $f(a) = -1$ rezultă $1 = -1 \Rightarrow 1 + 1 = 0$. Aşadar în inelul A avem oricum $1 + 1 = 0$ (inelul are caracteristica 2). Atunci, $\forall\, x \in A \Rightarrow x + x = x(1 + 1) = 0 \Rightarrow f(x + x) = f(0) \Rightarrow \left(f(x)\right)^2 = 1 \Rightarrow \left(f(x) - 1\right)\left(f(x) + 1\right) = 0 \Rightarrow f(x) = 1$ sau $f(x) = -1$, $\forall\, x \in A$. Prin urmare $\operatorname{Im} f \subseteq \{-1, 1\}$, adică $U(A) = \{1\}$ şi cum f este bijectivă rezultă $|A| = |U(A)| = 1$, deci A are un singur element, adică $0 = 1$, contradicţie. **17.** $|U(A)| = 2^n - 1 = \text{impar} \Rightarrow 1 + 1 = 0$, conform cu exerciţiul 13. Atunci în grupul $(A, +)$ avem $x + x = 0$, $\forall\, x \in A$ şi de aici $|A| = 2^m$ cu $m \geq n$. Dacă am avea $m > n$, adică $m \geq n + 1$, atunci numărul elementelor neinversabile este $2^m - (2^n - 1) \geq 2^{n+1} - (2^n - 1) = 2^n + 1 > 2^n - 1$, contradicţie. Deci $m = n$, ceea ce înseamnă că A are 2^n elemente, din care $2^n - 1$ sunt inversabile. Înseamnă că unicul element neinversabil este 0, prin urmare A este un corp cu 2^n elemente.
18. c) Arătăm că $x^2 - x \in Z(A)$, $\forall\, x \in A \Rightarrow A$ inel comutativ. Vom arăta că $\forall\, x \in A \Rightarrow x \in Z(A)$. Fie $x \in A$ fixat. Pentru $y \in A$ oarecare avem $(x + y)^2 - (x + y) \in Z(A) \Rightarrow x^2 + y^2 + xy + yx - x - y \in Z(A) \Rightarrow (x^2 - x) + (y^2 - y) + (xy + yx) \in Z(A) \Rightarrow xy + yx \in Z(A) \Rightarrow x(xy + yx) = (xy + yx)x \Rightarrow x^2y + xyx = xyx + yx^2 \Rightarrow x^2y = yx^2$. Aşadar $x^2 \in Z(A)$ şi cum $x^2 - x \in Z(A)$, rezultă $x \in Z(A)$. $\forall\, x \in A$. Aşadar $Z = Z(A)$ şi inelul este comutativ. **19.** I) $1 \leq p \leq n$. Avem egalităţile: $s_{p-1}\sigma_1 = s_p + \sum a_1^{p-1}a_2$; $s_{p-2}\sigma_2 = \sum a_1^{p-1}a_2 + \sum a_1^{p-2}a_2a_3$; $s_{p-3}\sigma_3 = \sum a_1^{p-2}a_2a_3 + \sum a_1^{p-3}a_2a_3a_4$; ...; $s_1\sigma_{p-1} = \sum a_1^2a_2...a_{p-1} + p\sigma_p$. Se adună aceste egalităţi, înmulţite din două în două cu -1. ii) $p \geq n + 1$. Avem egalităţile: $s_{p-1}\sigma_1 = s_p + \sum a_1^{p-1}a_2$; $s_{p-2}\sigma_2 = \sum a_1^{p-1}a_2 + \sum a_1^{p-2}a_2a_3$; ...; $s_{p-n}\sigma_n = \sum a_1^{p-n+1}a_2a_3...a_n$. Se adună aceste egalităţi, înmulţite din două în două cu -1. **20.** Orice $x \in A \setminus \{0\}$ este inversabil, având $x^{-1} = x$, deci A este un corp. Dacă $x \in A \setminus \{0\}$ este oarecare, ipoteza $x^2 = 1$ se scrie $(x - 1)(x + 1) = 0$, de unde $x = \pm 1$.

Rezultă $A \setminus \{0\} \subseteq \{-1, 1\}$ şi $A \subseteq \{-1, 0, 1\}$ şi cum $\{-1, 0, 1\} \subseteq A$, avem $A = \{-1, 0, 1\}$. Dacă $-1 = 1$, egalitatea precedentă devine $A = \{0, 1\}$, deci $A = \mathbb{Z}_2$. Dacă $-1 \neq 1$, avem $1 + 1 + 1 = 0$, căci grupul $(A, +)$ are ordinul 3, prin urmare $-1 = 1 + 1$ şi astfel $A = \{0, 1, 1+1\}$, adică $A = \mathbb{Z}_3$. **22.** În inelul A există 2 elemente neinversabile şi anume 0 şi a, $a \neq 0$. Aşadar $A = \{0, a\} \cup U(A)$. Arătăm că nu putem avea $U(A) = \{1\}$. Presupunem prin absurd că $U(A) = \{1\}$, deci $A = \{0, a, 1\}$ şi considerăm elementul $b = 1 + a \in A$; dacă $b = 0 \Rightarrow a = -1 \in U(A)$, fals; dacă $b = a \Rightarrow 1 = 0$, fals; dacă $b = 1 \Rightarrow a = 0$, fals. Aşadar $|U(A)| \geq 2$, deci $|A| \geq 4$. Vom arăta că $|A| = 4$. Arătăm mai întâi că $a^2 = 0$. Presupunem prin absurd că $a^2 \neq 0$, deci $a^2 = a$ sau $a^2 \in U(A)$; dacă $a^2 \in U(A)$, atunci $a \in U(A)$, fals, iar dacă $a^2 = a \Rightarrow a(a - 1) = 0$ şi cum $a-1 \notin \{0, a\}$ avem $a - 1 \in U(A)$, iar din $a(a - 1) = 0$ rezultă atunci $a = 0$, fals. Mai mult, rezultă că dacă $ay = 0$, cu $y \in A$, atunci $y = 0$ sau $y = a$. Fie acum $x \in U(A) \setminus \{1\}$ arbitrar. Considerăm elementul $ax \in A$. Nu putem avea $ax = 0$, căci ar rezulta $a = 0$; nu putem avea nici $ax \in U(A)$, căci ar rezulta $a \in U(A)$; aşadar, $ax = a \Rightarrow a(x - 1) = 0$ şi cum $x-1 \neq 0$, rezultă $x - 1 = a \Rightarrow x = 1 + a$. Aşadar $U(A) \setminus \{1\} = \{1 + a\} \Rightarrow U(A) = \{1, 1+a\}$ $\Rightarrow A = \{0, a, 1, 1 + a\}$, deci $|A| = 4$. Caracteristica inelului A, adică ordinul lui 1 în grupul $(A, +)$, este un divizor al lui 4, deci este 2 sau 4. Când caracteristica este 4 avem $1 + 1 \neq 0$ şi cum $1 + 1 \notin \{1, 1 + a\}$, rezultă $1 + 1 = a$, deci $A = \{0, 1, 1+1, 1+1+1\} \approx \mathbb{Z}_4$. Când caracteristica este 2, grupul $(A, +)$ este izomorf cu grupul lui Klein şi tabla adunării în A este uşor de întocmit; pentru completarea tablei înmulţirii, observăm că $a(1+a) = a + a^2 = a$, $(1+a)^2 = 1 + a(1+1) + a^2 = 1$, deci această tablă arată astfel:

$\cdot$	0	1	a	$1+a$
0	0	0	0	0
1	0	1	a	$1+a$
a	0	a	0	a
$1+a$	0	$1+a$	a	1

Aşadar inelele care satisfac problema sunt $\mathbb{Z}_4$ şi cel descris mai sus, având o adunare de tip Klein şi o înmulţire dată de tabla anterioară. **23.** Deoarece $|U(A)| = 4$ şi $U(A)$ este subgrup al grupului $(\mathbb{C}^*, \cdot)$, rezultă $U(A) = U_4 = \{1, -1, i, -i\}$. Aşadar $i \in A$, deci $i = u + v\alpha$ cu $u,v \in \mathbb{Z}$, $v \neq 0$. Rezultă $\alpha = \dfrac{i-u}{v}$. Deoarece A este inel avem $\alpha^2 \in A$, adică $\alpha^2 = a + b\alpha$ cu $a,b \in \mathbb{Z}$, deci α este rădăcină a polinomului $f = X^2 - bx - a \in \mathbb{Z}[X]$. Cealaltă rădăcină a polinomului f este $\overline{\alpha} = -\dfrac{i+u}{v}$, iar din formulele lui Viète avem $\alpha + \overline{\alpha} = b \in \mathbb{Z}$, $\alpha\overline{\alpha} = -a \in \mathbb{Z}$. Atunci $(\alpha - \overline{\alpha})^2 = (\alpha + \overline{\alpha})^2 - 4\alpha\overline{\alpha} = b^2 + 4a \in \mathbb{Z}$, adică $\left(\dfrac{2i}{v}\right)^2 \in \mathbb{Z}$, deci $\dfrac{4}{v^2} \in \mathbb{Z}$. Rezultă $v^2 = 1$ sau $v^2 = 4$. Dar $\alpha\overline{\alpha} = \dfrac{u^2+1}{v^2}$ şi cum $u^2 + 1$ nu se divide cu 4, deducem că nu e posibilă varianta $v^2 = 4$. Rezultă $v = \pm 1$, deci $\alpha = \dfrac{i-u}{\pm 1} \in \mathbb{Z}[i]$ şi atunci $A \subseteq \mathbb{Z}[i]$. Cum $i \in A$ avem şi incluziunea $\mathbb{Z}[i] \subseteq A$, deci egalitatea de inele $A = \mathbb{Z}[i]$. **24.** Dacă $A = \mathbb{Z}_4$ polinomul $f = \hat{2}X \in \mathbb{Z}_4[X]$ de gradul 1 are în $\mathbb{Z}_4$ rădăcinile $x_1 = \hat{0}$, $x_2 = \hat{2}$. **25.** Fie $K = \{a_1, a_2, \ldots, a_n\}$. Polinomul $P \in K[X]$, $P(X) = \sum\limits_{i=1}^{n} \dfrac{(X-a_1)\ldots(X-a_{i-1})(X-a_{i+1})\ldots(X-a_n)}{(a_i-a_1)\ldots(a_i-a_{i-1})(a_i-a_{i+1})\ldots(a_i-a_n)} \cdot f(a_i)$ (numit ***polinomul de interpolare*** al lui Lagrange) are proprietatea că $P(a_i) = f(a_i)$, $i = \overline{1,n}$, deci $f = \tilde{P}$.

26. Este suficient să arătăm că f nu se poate scrie ca produs a două polinoame din $\mathbb{Z}[X]$de grad mai mic ca n. Presupunem prin absurd că $f = gh$, cu $g,h \in \mathbb{Z}[X]$, $g = b_0 + b_1X + \ldots + b_rX^r$, $h = c_0 + c_1C + \ldots + c_sX^s$ cu $r < n$, $s < n$. Cum $p \mid a_0 = b_0c_0$, dar $p^2 \nmid a_0$, avem $p \mid b_0$ (de exemplu) şi $p \nmid c_0$. Cum $p \mid a_1 = b_0c_1 + b_1c_0$, rezultă $p \mid b_1c_0$, deci $p \mid b_1$; cum $p \mid a_2 = b_0c_2 + b_1c_1 + b_2c_0$ rezultă $p \mid b_2c_0$, deci $p \mid b_2$; continuând raţionamentul, ajungem la concluzia că $p \mid b_r$, deci $p \mid b_rc_s$, adică $p \mid a_n$, contradicţie.

27. a) Scriind $\Phi_p(X) = \dfrac{X^p - 1}{X-1}$, avem $\Phi_p(X+1) = \dfrac{(X+1)^p - 1}{(X+1)-1} =$

$$= \frac{X^p + C_p^1X^{p-1} + \ldots + C_p^{p-1}X + 1 - 1}{X} = X^{p-1} + C_p^1X^{p-2} + \ldots + C_p^{p-2}X + C_p^{p-1}$$

şi se aplică criteriul lui Eisenstein din exerciţiul 26. b) Dacă $\Phi_p(X)$ ar fi reductibil, ar rezulta că şi $\Phi_p(X+1)$ este reductibil, în contradicţie cu punctul a). **28.** Corpul K are caracteristica $\neq 2$ (căci 1+1 = 0 $\Rightarrow$ 5 · 1 = 1 $\Rightarrow X^2 - 5 = X^2 - 1 = (X-1)(X+1)$, contrar ipotezei că $X^2 - 5$ este ireductibil). Dacă $a = 0$, e clar. Fie aşadar $a \neq 0$. Arătăm că ecuaţia $x^5 = 1$ are în K^* doar soluţia $x = 1$. Într-adevăr $x^5 = 1 \Leftrightarrow$ $(x-1)(x^4+x^3+x^2+x+1) = 0 \Leftrightarrow (x-1)\left(x^2+x+1+\dfrac{1}{x}+\dfrac{1}{x^2}\right) = 0 \Leftrightarrow x = 1$ sau $x^2+x+1+\dfrac{1}{x}+\dfrac{1}{x^2} = 0$. Ultima ecuaţie se scrie $\left(x+\dfrac{1}{x}\right)^2 - 2\cdot 1 + \left(x+\dfrac{1}{x}\right) + 1 = 0$ sau $t^2 + t - 1 = 0$, unde $t = x + \dfrac{1}{x}$ şi nu are soluţii în K, deoarece $\Delta = 1 + 4 \cdot 1 = 5$, care nu este pătrat perfect în K (polinomul $X^2 - 5$ fiind ireductibil). Funcţia $f : K^* \to K^*$, $f(x) = x^5$ este atunci injectivă, deoarece $f(x_1) = f(x_2) \Rightarrow x_1^5 = x_2^5 \Rightarrow \left(\dfrac{x_1}{x_2}\right)^5 = 1 \Rightarrow$ $\dfrac{x_1}{x_2} = 1 \Rightarrow x_1 = x_2$. Cum K^* este mulţime finită, f este surjectivă, deci $\exists\, b \in K^*$ cu $f(b) = a$, adică $a = b^5$. Atunci $X^5 - a = X^5 - b^5$ şi se divide cu $X - b$.

Observaţie. Am ţinut seama că un corp finit este comutativ (teorema lui Wedderburn) şi că într-un corp de caracteristică $\neq 2$ o ecuaţie de gradul 2 are soluţii dacă şi numai dacă discriminantul este pătrat perfect în acel corp, formula de rezolvare rămânând cea cunoscută din cazul corpului $\mathbb{R}$.

29. Caracteristica lui K este un număr prim, divizor al lui $|K| = 2^n$, deci este egală cu 2, adică $1 + 1 = 0$. Arătăm că dacă n este par polinomul $f = X^4 + X + 1$ este reductibil, iar dacă n este impar polinomul f este ireductibil în $K[X]$.

I) $n = 2q$. Deoarece $|K^*| = 2^n - 1 = 2^{2q} - 1 = 4^q - 1 \vdots 3$, există în grupul $(K^*, \cdot)$ un element α de ordin 3 (conform unei teoreme a lui Cauchy: dacă p este un divizor prim al ordinului unui grup finit, există în acel grup un element de ordin p). Aşadar $\alpha^3 = 1$ şi $\alpha \neq 1$, deci $\alpha^2 + \alpha + 1 = 0$. Atunci: $(X^2 + X + \alpha)(X^2 + X + \alpha + 1) =$
$= (X^2 + X)^2 + (2\alpha + 1)(X^2 + X) + (\alpha^2 + \alpha) = X^4 + X^2 + X^2 + X - 1 = X^4 + X + 1 = f$, adică f este reductibil în $K[X]$.

II) $n = 2q + 1$. Mai întâi arătăm că f nu poate avea un factor liniar în $K[X]$, adică altfel spus, f nu are rădăcini în K. Într-adevăr, să admitem prin absurd că f are o rădăcină $x_0 \in K$. Deoarece $2^n - 1 = 2^{2q+1} - 1 = 2 \cdot 4^q - 1 = 2 \cdot (3+1)^q - 1 = M3 + 1$, înseamnă că $(2^n - 1, 3) = 1$, deci există $r, s \in \mathbb{Z}$ astfel încât $3r + (2^n - 1)s = 1$ (1). Din $f(x_0) = 0$ rezultă $(x_0^2 + x_0)^2 + (x_0^2 + x_0) + 1 = 0$ şi de aici $(x_0^2 + x_0)^3 = 1$. Folosind (1) putem scrie (ţinând seama şi de faptul că $x_0^2 + x_0 \in K^*$): $x_0^2 + x_0 = (x_0^2 + x_0)^{3r + (2^n - 1)s} =$
$= \left[(x_0^2 + x_0)^3\right]^r \cdot \left[(x_0^2 + x_0)^{2^n - 1}\right]^s = 1$, adică în definitiv $x_0^2 + x_0 + 1 = 0$. De aici $x_0^3 = 1$ şi urmând acelaşi raţionament făcut pentru $x_0^2 + x_0$, obţinem $x_0 = 1$. Aşadar $f(1) = 0 \Leftrightarrow$ $\Leftrightarrow 1 + 1 + 1 = 0 \Leftrightarrow 1 = 0$, absurd. Arătăm acum că f nu se poate descompune nici în produsul a doi factori de gradul 2. Să presupunem prin absurd că
$f = (X^2 + aX + b)(X^2 + cX + d)$, cu $a, b, c, d \in K$. Rezultă uşor $a + c = 0$, $b + d + ac = 0$, $ad + bc = 1$, $bd = 1$. De aici deducem $a = b$, $b + d = c^2$, $b + d = \frac{1}{c}$, deci $c^3 = 1$. Cu raţionamentul deja evidenţiat deducem $c = 1$ şi atunci $b = 1 + d$, deci $(1 + d)d = 1$ sau $d^2 + d + 1 = 0$. De aici $d^3 = 1$, apoi $d = 1$, deci $1 + 1 + 1 = 0 \Leftrightarrow 1 = 0$, absurd.

30. Descompunerea fracţiei raţionale $\frac{1}{f}$ în fracţii simple este $\frac{1}{f} = \sum_{i=1}^{n} \frac{1}{f'(x_i)(X - x_i)}$, de unde $\frac{1}{f(x)} = \sum_{i=1}^{n} \frac{1}{f'(x_i)(x - x_i)}$, $\forall\, x \in \mathbb{C} \setminus \{x_1, \ldots, x_n\}$. Înmulţim cu x şi avem $\frac{x}{f(x)} = \sum_{i=1}^{n} \frac{1}{f'(x_i)} \cdot \frac{x}{x - x_i}$ şi dacă luăm $x \in \mathbb{R}$ şi trecem la limită când $x \to \infty$, obţinem egalitatea din enunţ.

31. a) $f = \prod_{k=1}^{n} \left(X - \cos\frac{2k\pi}{n} - i \sin\frac{2k\pi}{n}\right)$; b) Se trece la valoarea numerică în punctul $x = 1$ şi se efectuează calculele în membrul drept din egalitatea precedentă. **32.** $1° \Rightarrow 2°$. Dacă $f(x) = f(-x)$, $\forall\, x \in \mathbb{C}$, există $h \in \mathbb{C}[X]$ cu $f(x) = h(x^2)$, $\forall\, x \in \mathbb{C}$. Polinomul h are o descompunere în factori liniari în $\mathbb{C}[X]$ de forma $h = a(X - x_1)(X - x_2)...(X - x_n)$. Fie $x_1 = y_1^2$, $x_2 = y_2^2$, ..., $x_n = y_n^2$ ($x_k, y_k \in \mathbb{C}$). Atunci: $f(x) = h(x^2) = a(x^2 - y_1^2)(x^2 - y_2^2)...(x^2 - y_n^2) = (-1)^n a(x + y_1)\, ...\, (x + y_n)(-x + y_1) \cdot$ $\cdot\, ...\, \cdot (-x + y_n)$. Luând $b \in \mathbb{C}$ cu $b^2 = (-1)^n a$ şi $g \in \mathbb{C}[X]$, $g = b(X + y_1)...(X + y_n)$, am obţinut că $f(x) = g(x)g(-x)$, $\forall\, x \in \mathbb{C}$. $2° \Rightarrow 1°$. Evident.

33. $1° \Rightarrow 2°$. Dacă $P = \lambda Q$, atunci $f(x) = |Q(x)|(|\lambda| - 1)$ şi această funcţie nu îşi schimbă semnul pe $\mathbb{C}$.

$2° \Rightarrow 1°$. Să presupunem că f nu îşi schimbă semnul, de exemplu $f(x) \geq 0$, $\forall\, x \in \mathbb{C}$. Aceasta înseamnă că $|P(x)| \geq |Q(x)|$, $\forall\, x \in \mathbb{C}$ (1).

Dacă $x_0 \in \mathbb{C}$ este o rădăcină a lui P, din (1) rezultă $Q(x_0) = 0$, deci x_0 este rădăcină şi pentru Q. Aşadar rădăcinile (distincte) ale lui P se află printre rădăcinile (distincte) ale lui Q. Fie $x_1, x_2, ..., x_k$ rădăcinile distincte ale lui Q, având ordinele de multiplicitate respectiv $\beta_1, \beta_2, ..., \beta_k$ ($\beta_i \geq 1$). Atunci P are rădăcinile $x_1, x_2, ..., x_k$, având ordinele de multiplicitate respectiv $\alpha_1, \alpha_2, ..., \alpha_k$ ($\alpha_i \geq 0$), luând $\alpha_i = 0$ dacă x_i nu este rădăcină pentru polinomul P. Avem aşadar: $P = a(X - x_1)^{\alpha_1}(X - x_2)^{\alpha_2}...(X - x_k)^{\alpha_k}$, $Q = b(X - x_1)^{\beta_1}(X - x_2)^{\beta_2}...(X - x_k)^{\beta_k}$, unde $a, b \in \mathbb{C}^*$. Inegalitatea (1) se scrie:

$|a||x - x_1|^{\alpha_1}|x - x_2|^{\alpha_2}...|x - x_k|^{\alpha_k} \geq |b||x - x_1|^{\beta_1}|x - x_2|^{\beta_2}...|x - x_k|^{\beta_k}$, $\forall\, x \in \mathbb{C}$ (2).

Arătăm mai întâi că $\alpha_1 \leq \beta_1$, $\alpha_2 \leq \beta_2$, ..., $\alpha_k \leq \beta_k$. Probăm prima inegalitate, celelalte fiind analoage. Presupunem prin absurd $\alpha_1 > \beta_1$. Atunci, pentru $x \in \mathbb{C} \setminus \{x_1, x_2, ..., x_k\}$ împărţind în (2) prin $|x - x_1|^{\beta_1}$ şi apoi trecând la limită când $x \to x_1$, obţinem $0 \geq |b||x_1 - x_2|^{\beta_2}...|x_1 - x_k|^{\beta_k}$, contradicţie. Arătăm acum că niciuna din inegalităţile $\alpha_i \leq \beta_i$ nu este strictă. Probăm tot pentru prima. Să presupunem prin absurd că $\alpha_1 < \beta_1$. Pentru $x \in \mathbb{C} \setminus \{x_1, x_2, ..., x_k\}$ împărţind în (2) prin $|x - x_1|^{\alpha_1}|x - x_2|^{\alpha_2}...|x - x_k|^{\alpha_k}$ şi apoi trecând la limită când $|x - x_1| \to \infty$, obţinem $|a| \geq \infty$, contradicţie. Aşadar $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2$, ..., $\alpha_k = \beta_k$ şi soluţia se încheie. **34.** Să presupunem că rădăcinile polinomului f sunt $x_0 = 1$, $x_1 = -1$ (ca numere reale de modul 1) având ordinele de multiplicitate $\alpha_0, \alpha_1 \in \mathbb{N}$, apoi nişte rădăcini complexe nereale, care apar în perechi de numere conjugate având acelaşi ordin de multiplicitate, fie acestea x_2, $\overline{x_2}$ cu ordinul α_2, apoi x_3, $\overline{x_3}$ cu ordinul α_3, ..., x_k, $\overline{x_k}$ cu ordinul α_k. Descompunerea lui f în factori liniari în inelul $\mathbb{C}[X]$ este: $f = a(X - 1)^{\alpha_1}(X + 1)^{\alpha_1}[(X - x_2)(X - \overline{x_2})]^{\alpha_2}[(X - x_3)(X - \overline{x_3})]^{\alpha_3} \cdot$ $\cdot\, ...\, \cdot [(X - x_k)(X - \overline{x_k})]^{\alpha_k}$. Dar dacă $t \in \mathbb{C} \setminus \mathbb{R}$, $|t| = 1$, avem $(X - t)(X - \overline{t}) =$

$=X^2-(t+\overline{t})X+1$ care este un polinom reciproc de speța I și dat fiind că produsul polinoamelor reciproce de speța I este un polinom reciproc de speța I, deducem că polinomul $a(X+1)^{\alpha_1}\left[(X-x_2)(X-\overline{x}_2)\right]^{\alpha_2}\ldots\left[(X-x_k)(X-\overline{x}_k)\right]^{\alpha_k}$ este reciproc de speța I. Însă $X-1$ este reciproc de speța a II-a și deoarece produsul a două polinoame reciproce de speța a II-a este unul reciproc de speța I, iar produsul dintre un polinom reciproc de speța I și unul de speța a II-a este unul reciproc de speța a II-a, rezultă că $(X-1)^{\alpha_0}$ este reciproc de speța I, respectiv a II-a, după cum α_0 este par, respectiv impar. Atunci și f este reciproc de aceeași speță cu $(X-1)^{\alpha_0}$, ceea ce înseamnă că avem relația între coeficienții săi $a_i=(-1)^{\alpha_0}a_{n-i}$, i = 0, 1, 2, ..., n. **35.** Dacă polinomul $f=a_0+a_1X+\ldots+a_nX^n\in\mathbb{R}[X]$ are rădăcinile $x_1, x_2, \ldots, x_n$, toate de modulul $r>0$, atunci polinomul $g\in\mathbb{R}[X]$, definit prin $g(X)=f(rX)$ are rădăcinile $\frac{x_1}{r}, \frac{x_2}{r}, \ldots, \frac{x_n}{r}$, toate de modul 1. Dar $g(X)=\sum_{i=0}^{n}a_ir^iX^i$ și aplicând problema precedentă pentru polinomul g, obținem $a_ir^i=(-1)^{\alpha_0}a_{n-i}r^{n-i}$, adică $a_i=(-1)^{\alpha_0}r^{n-2i}a_{n-i}$, $i=0, 1, 2, \ldots, n$.

Elemente de analiză matematică

Primitive

I. 7. $\frac{5}{4}\sqrt[5]{x^4}+\mathscr{C}$. **9.** $\frac{x^4}{3}-\frac{x^3}{4}+5x+\mathscr{C}$. **14.** $-\frac{1}{x^3}-\frac{2}{x^4}+\mathscr{C}$. **16.** $-2x^{-\frac{1}{2}}+\frac{3}{2}x^{-\frac{2}{3}}-\frac{4}{3}x^{-\frac{3}{4}}+\mathscr{C}$.

24. $2a\sqrt{ax}-4ax+4x\sqrt{ax}-2x^2+\frac{2x^3}{5\sqrt{ax}}+\mathscr{C}$. **35.** $\ln\left(-\sqrt{x^2-16}-x\right)+\mathscr{C}$.

II. 1. $t=3x+2$. **2.** $t=4x+1$. **3.** $t=2x^2+1$. **4.** $t=x^2+1$. **5.** $t=5x^3+1$. **6.** $t=5x+1$. **7.** $t=3x+1$. **8.** $t=2x-1$. **9.** $t=4-3x$. **10.** $t=3x-1$. **11.** $t=3x-5$. **12.** $t=x^2+3$. **13.** $t=x^4-1$. **14.** $t=1-2x^3$. **15.** $t=5x^4+3$. **16.** $t=4x^3+1$. **17.** $t=x^4-1$. **18.** $t=5x^2$. **19.** $t=-3x^2+1$. **20.** $t=\cos x$. **21.** $t=\sin x$. **22.** $t=e^x+1$. **23.** $t=2\sin x-1$. **24.** $t=3x^4+2$. **25.** $t=1-3x^2$. **26.** $t=x^2+1$. **27.** $t=5x^4+2$. **28.** $t=x^3-1$. **29.** $t=e^x+1$. **30.** $t=1-\sin x$. **31.** $t=1+\ln x$. **32.** $t=\sqrt{x}$. **33.** $t=\sqrt{x}$. **34.** $t=x^3$. **35.** $t=1+x^3$. **36.** $t=-x^2$. **37.** $t=\cos x$. **38.** $t=\sin x$. **39.** $t=\sqrt{x}$. **40.** $t=\frac{1}{x}$. **41.** $t=\ln x$. **42.** $t=e^x$. **43.** $t=\ln x$. **44.** $t=e^x$. **45.** $t=\ln x$. **46.** $t=\frac{1}{x}$. **47.** $t=x^3$. **48.** $t=\operatorname{arctg} x$. **49.** $t=\arcsin x$. **50.** $t=x+\cos x$. **51.** $t=\ln x$.

52. $t=x^2$. **53.** $t=1+\ln x$. **54.** $t=\sin^2 x$. **55.** $\frac{1}{\sin^2 x\cos^2 x}=\frac{4}{\sin^2 2x}$, $t=2x$.

56. $t=\ln\left(x+\sqrt{x^2+1}\right)$.

III. 11. $x\arcsin x+\sqrt{1-x^2}+\mathscr{C}$. **19.** $x\ln\left(x+\sqrt{1+x^2}\right)-\sqrt{1+x^2}+\mathscr{C}$. **26.** Se integrează de două ori prin părţi şi se obţine: $\frac{1+x^2}{2}(\text{arctg } x)^2-x \text{ arctg}x+\frac{1}{2}\ln(1+x^2)+\mathscr{C}$.

Integrala definită

I.1. $\|\Delta_n\|=\frac{1}{n}$, $\lim\limits_{n\to\infty}\|\Delta_n\|=0$. **2. a)** $\sigma(f,\Delta_n,\xi_n)=\sum\limits_{i=1}^{n}\left(\frac{i}{n}\cdot\frac{1}{n}\right)=\frac{1}{n^2}\cdot\sum\limits_{i=1}^{n}i=\frac{n+1}{2n}$,

$\lim\limits_{n\to\infty}\sigma(f,\Delta_n,\xi_n)=\frac{1}{2}$. **b)** $\sigma(f,\Delta_n,\xi_n)=\sum\limits_{i=1}^{n}\left(e^{\frac{i}{n}}\cdot\frac{1}{n}\right)=\frac{1}{n}\cdot\sum\limits_{i=1}^{n}e^{\frac{i}{n}}=\frac{1}{n}\cdot\frac{e^{\frac{1}{n}}(1-e)}{1-e^{\frac{1}{n}}}$,

$\lim\limits_{n\to\infty}\sigma(f,\Delta_n,\xi_n)=e-1$. **II. 1.** $\frac{1}{2}$. **4.** $e-1$. **15.** 0. **20.** $\frac{\pi}{8}$.

Metode de calcul al integralelor

I. 14. 52. **22.** e^2-1. **29.** $\frac{\pi}{4}$. **35.** $\frac{2}{\sqrt{5}}\text{arctg}\frac{1}{\sqrt{5}}$. **36.** $\frac{2\pi}{\sqrt{5}}$.

III. a) Scriem $\left(1-x^2\right)^n=\left(1-x^2\right)^{n-1}(1-x^2)=\left(1-x^2\right)^{n-1}-x\cdot x\left(1-x^2\right)^{n-1}$ şi când integrăm, a doua integrală se calculează prin părţi. **c)** Dezvoltăm $\left(1-x^2\right)^n$ cu formula binomului lui Newton şi calculăm I_n integrând termen cu termen, apoi ţinem seama de punctul b).

Integralele funcţiilor raţionale

I. 17. $\ln(x+1)+\frac{x+2}{3(x^2+x+1)}+\frac{5}{3\sqrt{3}}\text{arctg}\frac{2x+1}{\sqrt{3}}-\frac{1}{2}\ln(x^2+x+1)+\mathscr{C}$. **23.** Scriem $\frac{1}{x(x^7+1)}=\frac{x^6}{x^7(x^7+1)}=x^6\left(\frac{1}{x^7}-\frac{1}{x^7+1}\right)=\frac{1}{x}-\frac{x^6}{x^7+1}$ şi se obţine: $\ln x-\frac{1}{7}\ln(x^7+1)+\mathscr{C}$.

Legătura dintre unele clase remarcabile de funcţii (extindere)

I. 1. Continuă. **2.** Continuă. **3.** Procedăm ca şi în cazul $\alpha=1$. **4.** Analog cu exerciţiul 3. **5, 6, 7.** Folosim formulele de transformare a produselor de funcţii trigonometrice în sume.

II. 1. $f(\mathbb{R})=\mathbb{Z}\Rightarrow f$ nu are proprietatea lui Darboux $\Rightarrow f$ nu are primitive. **2.** $f(x)=x-[x]$ şi în această sumă $f_1(x)=x$ are primitive, iar $f_2(x)=-[x]$ nu are primitive, deci suma $f = f_1 + f_2$ nu are primitive. **3.** Avem $f(x)=\begin{cases}\sin\frac{1}{x}, & x\neq 0\\ 0, & x=0\end{cases}+\begin{cases}0, & x\neq 0\\ \lambda, & x=0\end{cases}$ şi în această sumă prima funcţie are primitive, iar a doua nu are (neavând proprietatea lui Darboux), prin urmare f nu are primitive. **4.** Analog cu exerciţiul 3. **5.** Avem $\sin^2\alpha=\frac{1-\cos 2\alpha}{2}$, deci $f(x)=\begin{cases}\frac{1}{2}, & x\neq 0\\ 0, & x=0\end{cases}-\frac{1}{2}\begin{cases}\cos\frac{2}{x}, & x\neq 0\\ 0, & x=0\end{cases}$ şi în această sumă prima funcţie nu are primitive, iar a doua are primitive, prin urmare f nu are primitive. **6.** Analog cu exerciţiul 5.

Aplicaţii ale integralei definite

I.1. $\frac{64}{3}$. **2.** 8. **3.** $\frac{383}{6}$. **4.** $\frac{1}{6}$. **5.** 4. **6.** $\frac{7}{6}$. **7.** $\frac{8}{3}$. **8.** $48\ln 2-\frac{45}{4}$. **9.** $\frac{1}{\ln 3}$.

II. $a=\pm\sqrt{\frac{2}{3}}$.

Volumul unui corp de rotaţie

2. $\frac{\pi}{4}$. **8.** $\frac{4\pi}{3}$. **10.** $p^3\pi$.

Calculul unor limite de şiruri folosind integrala definită

1. $\frac{1}{p+1}$. **2.** $\frac{\pi}{4}$. **3.** $\ln\left(1+\sqrt{2}\right)$. **4.** $\frac{\pi}{4}+\frac{1}{2}\ln 2$. **5.** 0. **6.** $\frac{2}{\pi}$. **7.** $\frac{2\left(2\sqrt{2}-1\right)}{3}$. **8.** $\frac{2-\sin 2}{4}$.

Probleme recapitulative

I. 1. Scriem $\int_{-a}^{a} f(x)dx=\int_{-a}^{0} f(x)dx+\int_{0}^{a} f(x)dx$ şi în prima integrală din membrul drept facem substituţia $x=-t$. **3.** Facem substituţia $t=a+b-x$. **5.** În integrala a doua facem substituţia $y=f(x)$. **II. 7.** Facem substituţia $t=\frac{\pi}{4}-x$ ca la ex. I.3. **8, 9.** Se aplică identitatea lui Young din ex. I.5. **III. 2. a)** Avem $\left(\lambda f(x)-g(x)\right)^2\geq 0$ şi integrăm pe intervalul $[a, b]$. **b)** Funcţia de gradul doi în λ de la punctul a) este pozitivă pe $\mathbb{R}$, deci are discriminantul negativ şi de aici rezultă inegalitatea cerută. **3. a)** În inegalitatea Jensen $f\left(\sum_{i=1}^{n}\lambda_i a_i\right)\leq\sum_{i=1}^{n}\lambda_i f(a_i)$, cu $\lambda > 0$ şi $\sum_{i=1}^{n}\lambda_i=1$, luăm $\lambda_i=\frac{dx_i}{b-a}=\frac{x_i-x_{i-1}}{b-a}$, iar $a_i=g(\xi)$, $i=\overline{1,n}$ şi se obţine inegalitatea cerută. **b)** Trecem la limită când $n \to \infty$ şi $\| \Delta \| \to 0$ în inegalitatea de la punctul a). **V. 2.** Scriem $f(t)=\int_0^{2t} e^{x^2} dx - \int_0^t e^{x^2} dx$, iar în prima integrală efectuăm schimbarea de variabilă $u = 2t$. **VI. a)** Facem substituţia $t = 1 - x$. **VII. a)** Facem substituţia $t = \sin^2 x$.

VIII. $\dfrac{2^{n+1}-1}{n+1}$. **IX.** Fie $F, G : \mathbb{R} \to \mathbb{R}$ primitive pentru funcţiile $f\cdot\sin$, respectiv $f\cdot\cos$, adică $F'(x) = f(x) \sin x$ şi $G'(x) = f(x) \cos x$. Observăm că $(F(x)\sin x + G(x)\cos x)' =$ $= F'(x)\sin x + G'(x)\cos x + F(x)\cos x - G(x)\sin x$. Funcţia $F(x)\cos x - G(x)\sin x$ are primitive, fiind continuă şi atunci funcţia $F'(x)\sin x + G'(x)\cos x$ are primitive. Dar $F'(x)\sin x + G'(x)\cos x = f(x)\sin^2 x + f(x)\cos^2 x = f(x)$, prin urmare f are primitive.

X. Funcţia continuă f are o primitivă F. Arătăm că $\lim\limits_{x\to 0} xF\left(\dfrac{1}{x}\right)=\dfrac{1}{T}\int_0^T f(t)dt$, (1).

Într-adevăr, notând $n_x = \left[\dfrac{x}{T}\right]$ avem $\lim\limits_{x\to\infty}\dfrac{n_x}{x}=\dfrac{1}{T}$, $n_x T \le x < (n_x+1)T$ şi cum $\int_0^{n_x T} f(t)dt = n_x \cdot \int_0^T f(t)dt$, putem scrie: $\dfrac{1}{T}\int_0^T f(t)dt = \lim\limits_{x\to\infty}\dfrac{n_x}{x}\cdot\int_0^T f(t)dt =$

$$=\lim_{x\to\infty}\frac{1}{x}\int_0^{n_x T} f(t)dt = \lim_{x\to\infty}\frac{1}{x}\left(\int_0^{n_x T} f(t)dt + \int_{n_x T}^{x} f(t)dt\right) = \lim_{x\to\infty}\frac{1}{x}\int_0^{x} f(t)dt =$$

$$=\lim_{x\to\infty}\frac{1}{x}\left(F(x)-F(0)\right) = \lim_{\substack{x\to 0\\ x>0}} xF\left(\frac{1}{x}\right)$$ şi analog $\dfrac{1}{T}\int_0^T f(t)dt = \lim\limits_{\substack{x\to 0\\ x<0}} xF\left(\dfrac{1}{x}\right)$; am ţinut seama şi de faptul că $\lim\limits_{x\to\infty}\dfrac{1}{x}\int_{n_x T}^{x} f(t)dt = 0$, căci f este o funcţie mărginită pe $[0, T]$, deci şi pe $[n_x T, (n_x+1)T]$. Să presupunem mai întâi că $\lambda = \dfrac{1}{T}\int_0^T f(t)dt$ şi să arătăm că funcţia corespunzătoare $f(x)=\begin{cases} f\left(\dfrac{1}{x}\right), & x\neq 0 \\ \dfrac{1}{T}\int_0^T f(t)dt, & x=0 \end{cases}$ are primitive. Considerăm funcţia $H : \mathbb{R} \to \mathbb{R}$, $H(x)=\begin{cases} x^2F\left(\dfrac{1}{x}\right), & x\neq 0 \\ 0, & x=0 \end{cases}$; este clar că H este derivabilă pe $\mathbb{R}$, căci pe $\mathbb{R}^*$ este produsul a două funcţii derivabile, iar în $x = 0$ avem $H'(0)=\lim\limits_{x\to 0}\dfrac{H(x)-H(0)}{x-0}=$

$$=\lim_{x\to 0} xF\left(\frac{1}{x}\right)\overset{(1)}{=}\frac{1}{T}\int_0^T f(t)dt \in \mathbb{R}.$$ Considerăm atunci derivata $h : \mathbb{R} \to \mathbb{R}$ a funcţiei H, adică funcţia $h(x)=\begin{cases} 2xF\left(\dfrac{1}{x}\right)+x^2 f\left(\dfrac{1}{x}\right)\cdot\left(-\dfrac{1}{x}\right), & x\neq 0 \\ H'(0), & x=0 \end{cases}=$

$$=\begin{cases} 2xF\left(\frac{1}{x}\right), & x\neq 0 \\ H'(0), & x=0 \end{cases} - \begin{cases} f\left(\frac{1}{x}\right), & x\neq 0 \\ H'(0), & x=0 \end{cases} = \begin{cases} 2xF\left(\frac{1}{x}\right), & x\neq 0 \\ 2\cdot\int_0^T f(t)dt, & x=0 \end{cases} - \begin{cases} F\left(\frac{1}{x}\right), & x\neq 0 \\ \frac{1}{T}\cdot\int_0^T f(t)dt, & x=0 \end{cases} =$$

$$=u(x)-g(x), \text{ unde } u:\mathbb{R}\to\mathbb{R},\ u(x)=\begin{cases} 2xF\left(\frac{1}{x}\right), & x\neq 0 \\ 2\cdot\frac{1}{T}\cdot\int_0^T f(t)dt, & x=0 \end{cases}$$ este o funcţie continuă.

Rezultă $g=u-h$ şi deoarece u şi h au primitive (u fiind continuă, iar h fiind derivata lui H), deducem că g are primitive. Reciproc, dacă g are primitive, scriind:

$$g(x)=\begin{cases} f\left(\frac{1}{x}\right), & x\neq 0 \\ \frac{1}{T}\cdot\int_0^T f(t)dt, & x=0 \end{cases} + \begin{cases} 0, & x\neq 0 \\ \lambda-\frac{1}{T}\cdot\int_0^T f(t)dt, & x=0 \end{cases}$$ şi ţinând seama de faptul că

prima funcţie din membrul drept are şi ea primitive, deducem că funcţia $f:\mathbb{R}\to\mathbb{R}$,

$$v(x)=\begin{cases} 0, & x\neq 0 \\ \lambda-\frac{1}{T}\int_0^T f(t)dt, & x=0 \end{cases}$$ are primitive, de unde, în mod necesar, $\lambda=\frac{1}{T}\int_0^T f(t)dt$.

XI. Se aplică exerciţiul X. La punctul a) avem: $\lambda_n=\frac{1}{2\pi}\int_0^{2\pi}\sin^n x\,dx=\frac{1}{2\pi}\int_{-\pi}^{\pi}\sin^n x\,dx$ şi cum n este impar, rezultă $\lambda_n=0$. La punctul b), pentru n par, avem:

$$\lambda_n=\frac{1}{2\pi}\int_{-\pi}^{\pi}\sin^n x\,dx=\frac{1}{2\pi}\cdot 2\int_0^{\pi}\sin^n x\,dx=\frac{1}{\pi}\left(\int_0^{\frac{\pi}{2}}\sin^n x\,dx+\int_{\frac{\pi}{2}}^{\pi}\sin^n x\,dx\right)=$$

$$=\frac{1}{\pi}\left(\int_0^{\frac{\pi}{2}}\sin^n x\,dx+\int_0^{\frac{\pi}{2}}\cos^n x\,dx\right)=\frac{2}{\pi}\int_0^{\frac{\pi}{2}}\sin^n x\,dx=\frac{2}{\pi}\cdot\frac{(2n-1)!!}{(2n)!!}\cdot\frac{\pi}{2}=\frac{(2n-1)!!}{(2n)!!};$$

am utilizat şi rezultatul $\int_0^{\frac{\pi}{2}}\sin^n x\,dx=\frac{(2n-1)!!}{(2n)!!}\cdot\frac{\pi}{2}$, pentru n par, stabilit în exerciţiul rezolvat de la pag. 190 punctul c). **XII. a)** Fie $F: I\to\mathbb{R}$ o primitivă pentru f. Cum $F'=f$ nu se anulează, înseamnă că F' are semn constant deci F este strict monotonă, deci injectivă. Atunci funcţia $F: I\to F(I)$ este bijecţie şi cum F este continuă, inversa $F^{-1}: F(I)\to I$ este de asemenea continuă. Funcţia continuă $g\circ F^{-1}$ are o primitivă G şi $(G\circ F)'=(G'\circ F)F'=(g\circ F^{-1}\circ F)f=gf$, deci funcţia fg are primitive.
b) Dacă f este mărginită, există $m\in\mathbb{R}$ astfel încât $f(x)>m$, $\forall\, x\in\mathbb{R}$. Atunci funcţia $f-m$ are primitive şi nu se anulează pe $\mathbb{R}$. Conform cu a) rezultă că funcţia $(f-m)g=$ $=fg-mg$ are primitive şi cum funcţia $-mg$ are primitive (fiind continuă), deducem că funcţia fg are primitive. **XIII.** Se aplică XII. **XIV.** Fie $a,b\in I$, $a<b$ şi λ între

$\frac{f(a)}{g(a)}$ şi $\frac{f(b)}{g(b)}$, de exemplu $\frac{f(a)}{g(a)} < \lambda < \frac{f(b)}{g(b)}$, (1). Arătăm că există $c \in (a, b)$ cu $\lambda = \frac{f(c)}{g(c)}$. Funcţia g are proprietatea lui Darboux (având primitive) şi nu se anulează, deci menţine semn constant pe I, de exemplu $g(x) > 0$, $\forall\, x \in I$. Funcţia $h = f - \lambda g$ are primitive, deci are proprietatea lui Darboux. Însă, din (1) avem $h(a) < 0$, $h(b) > 0$, deci există $c \in (a, b)$ cu $h(c) = 0 \Leftrightarrow \lambda = \frac{f(c)}{g(c)}$. **XVII.** Dacă h este o funcţie integrabilă, se arată, cu ajutorul criteriului de integrabilitate al lui Darboux, că funcţia h^2 este integrabilă. (Este suficient să considerăm cazul când h este pozitivă, deoarece h fiind mărginită, prin adunare cu o constantă convenabilă, devine pozitivă). Atunci, dacă f şi g sunt funcţii integrabile pe un acelaşi interval $[a, b]$, scriind $fg = \frac{1}{4}\left[(f+g)^2 - (f-g)^2\right]$, rezultă că funcţia fg este integrabilă. **XVIII.** Să notăm $S_n = n\left(\int_0^1 f(x)dx - \frac{1}{n}\sum_{i=1}^{n} f\left(\frac{i}{n}\right)\right)$. Notând cu m_i', M_i' marginile inferioară şi superioară ale derivatei f' pe intervalul $\left[\frac{i-1}{n}, \frac{i}{n}\right]$, $i = \overline{1, n}$ şi cu $\xi_i(x)$ punctul care rezultă dacă aplicăm teorema lui Lagrange funcţiei f pe intervalul de extremităţi x şi $\frac{i}{n}$, avem:

$$S_n = n\sum_{i=1}^{n}\left(\int_{\frac{i-1}{n}}^{\frac{i}{n}} f(x)dx - \frac{1}{n} f\left(\frac{i}{n}\right)\right) = n\sum_{i=1}^{n}\int_{\frac{i-1}{n}}^{\frac{i}{n}}\left(f(x) - f\left(\frac{i}{n}\right)\right)dx = n\sum_{i=1}^{n}\int_{\frac{i-1}{n}}^{\frac{i}{n}}\left(x - \frac{i}{n}\right) f'(\xi_i(x))\,dx ,$$

unde $m_i' \le f'(\xi_i(x)) \le M_i'$. Atunci, deoarece $x - \frac{i}{n} \le 0$ pentru $x \in \left[\frac{i-1}{n}, \frac{i}{n}\right]$, putem scrie:

$$S_n \ge n\sum_{i=1}^{n}\int_{\frac{i-1}{n}}^{\frac{i}{n}}\left(x - \frac{i}{n}\right) M_i'\, dx = n\sum_{i=1}^{n} M_i' \int_{\frac{i-1}{n}}^{\frac{i}{n}}\left(x - \frac{i}{n}\right) dx = -\frac{1}{2n}\sum_{i=1}^{n} M_i' \qquad (1)$$

şi analog $S_n \le -\frac{1}{2n}\sum_{i=1}^{n} m_i'$. (2)

Dar $\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n} M_i' = \int_0^1 f'(x)dx = f(x)\Big|_0^1 = f(1) - f(0)$ şi analog $\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n} m_i' = f(1) - f(0)$, deoarece aceste sume sunt nişte sume Darboux pentru funcţia f' şi diviziunea $\left(0, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, 1\right)$ a intervalului [0, 1]. Din (1), (2) şi criteriul cleştelui, rezultă că $\lim_{n\to\infty} S_n = \frac{f(0) - f(1)}{2}$. **XIX.** Notând cu L limita din membrul stâng şi cu M marginea superioară a funcţiei f pe intervalul $[a, b]$, se arată că $L \le M$ şi $L \ge M - \varepsilon$, $\forall$ $\varepsilon > 0$, de unde $L \ge M$ şi de aici $L = M$.

CUPRINS

ELEMENTE DE ALGEBRĂ

ELEMENTE DE ANALIZĂ MATEMATICĂ

SOLUŢII

ART
Grup Editorial

ISBN 978-973-124-549-2
9 789731 245492