Fundamentele algebrice ale informaticii

Adelina-Loredana MANEA

October 4, 2020

Cuprins

Prefaţă

Capitolul 1

Mulţimi. Relaţii. Funcţii

Teoria mulţimilor, aşa cum o utilizăm noi astăzi, a fost iniţiată de matematicianul Georg Cantor în ultimul sfert al secolului al XIX-lea. Conform lui Cantor, prin mulţime înţelegem *orice colecţie de obiecte distincte şi bine definite ale intuiţiei şi ale gândirii noastre, considerată ca un întreg.* Mai exact, prin mulţime înţelegem o colecţie de obiecte conectate între ele într-un fel neprecizat.

Abordarea lui Cantor a condus însă la paradoxuri. Este celebru paradoxul lui Rusell care spune că dacă putem vorbi despre orice fel de mulţimi, atunci putem să considerăm mulţimea tuturor mulţimilor care nu se conţin ca elemente:

$$A = \{X| \quad X \notin X\}.$$

De exemplu, într-o bibliotecă sunt cataloage (indexuri) care conţin evidenţa volumelor din biblioteca respectivă. La rândul lor, aceste cataloage se găsesc în bibliotecă, deci este posibil ca ele să apară în conţinutul unora dintre cataloage. Adică un catalog poate sau nu să apară ca element al său.

Fie A acel catalog care conţine toate cataloagele (şi doar pe acelea) care nu se conţin ca elemente. Existenţa acestei mulţimi conduce la un paradox: dacă $A \in A$, conform condiţiei care defineşte A, $A \notin A$. Dacă $A \notin A$, atunci A nu verifică condiţia de definiţie a sa, deci $A \in A$. Contradicţie!

Astfel de paradoxuri au dus la abordarea axiomatică a acestei teoriei mulţimilor la începutul secolului XX, prin contribuţiile matematicienilor Bertrand Rusell, Ernst Zermelo, Abraham Fraenkel, John von Neumann. Abordarea axiomatică nu face obiectul acestui curs.

Îndreptându-ne spre utilitatea matematicii ca model pentru diferite situaţii practice, în ultimii ani s-a dezvoltat o nouă idee, care schimbă percepţia asupra

noţiunii de apartenenţă a unui element la o mulţime, mai ales in contextul analizării unor situaţii a căror cunoaştere nu ne este accesibilă total. În teoria clasică a mulţimilor, un element aparţine sau nu aparţine unei mulţimi, neexistând o altă alternativă. Prin contribuţia lui Lotfi Zadeh, apare pe la mijlocul secolului XX ideea de *mulţimi nuanţate* sau *fuzzy sets*, în care un element aparţine într-o oarecare măsură (cu o oarecare probabilitate) unei mulţimi. Se introduce o funcţie de apartenenţă, "fuzzy membership function", al cărei codomeniu este intervalul $[0, 1]$ şi care generalizează cumva funcţia caracteristică a unei mulţimi. Astfel, considerând X ca o parte a unei mulţimi A, funcţia membru se defineşte astfel:

$$\mu_X : A \to [0, 1],$$

$\mu_X(x)$ este măsura în care (sau probabilitatea ca) x aparţine mulţimii X. De exemplu, în teoria clasică a mulţimilor, o persoană este fie săracă, fie bogată din punct de vedere al unui anumit criteriu X, cum ar fi deţinerea unei locuinţe. Dacă nu are o locuinţă, $\mu_X(x) = 0$, iar dacă are, $\mu_X(x) = 1$. În realitate, orice persoană este într-o oarecare măsură (posibil 0), bogată, relativ la calitatea locuinţei pe care o deţine. Îaceastă abordare putem nuanţa apartenenţa la una dintre categorii (bogat/sărac), în funcţie de valoare locuinţei pe care o are.

Noua abordare a relaţiei de apartenenţă are la bază noţiunea de vag, imprecis, care se pretează uneori mai bine realităţii şi care a fost formulată în 1893 de către Gottlieb Frege. De exemplu, un număr natural este fie par, fie nu este par, ceea ce este o noţiune clară, pe când dacă un tablou este sau nu frumos, este greu de precizat, nefiind o noţiune exactă în absenţa unor criterii care oricum nu ar face decât să trunchieze realitatea. Această idee permite asocierea la o mulţime a unei zone de graniţă formată din elemente pentru care nu pot preciza dacă aparţin sau nu mulţimii. Apare ideea de "rough set theory", teoria imprecisă a mulţimilor, unde unei mulţimi X, submulţime a unui univers U, i se asociază aproximări ale sale, relativ la o relaţie de echivalenţă R pe U. Relaţia R se numeşte relaţia de nediscernământ şi descrie lipsa noastră de cunoaştere a universului.

Pentru un element a al universului U, notăm $R(a)$ clasa lui de echivalenţă, numită granulă generată de R şi definim:

-cea mai mică aproximare a mulţimii $X \subset U$, o mulţime formată din elementele a ale mulţimii, pentru care orice element echivalent cu a este tot în X, adică

$$R_*X = \cup_{a \in U}\{R(a) | \quad R(a) \subset X\};$$

-cea mai mare aproximare, mulctimea elmentelor universului ale căror clase

de echivalenţă au elemente comune cu X:

$$R^*X = \cup_{a\in U}\{R(a)| \quad R(a)\cap X \neq \Phi\};$$

- regiunea de graniţă, definită matematic ca fiind $R^*X - R_*X$.

De remarcat faptul că aceste noi teorii, care devin foarte interesante pentru informaticieni sub aspectul inteligenţei artificiale, nu reprezintă o alternativă a teoriei clasice a mulţimilor, ci sunt parte a acesteia. Toate noile teorii folosesc ca fundamente noţiunile şi rezultatele din teoria clasică.

1.1 Preliminarii

Pentru buna parcurgere a acestui curs considerăm necesară reactualizarea unei tehnici matematice cunoscute din liceu, care apare în multe demonstraţii, şi anume *Inducţia matematică*.

Inducţia matematică este un procedeu prin care se demonstrează afirmaţii matematice referitoare la orice număr natural $n \geq n_0$.

Există mai multe variante ale inducţiei matematice, dintre care amintim inducţia simplăşi inducţia completă.

Fie $P(n)$ o afirmaţie matematică şi $n_0 \in \mathbb{N}$ un număr natural fixat. Se cere să se arate că $P(n)$ este adevărată pentru orice $n \geq n_0$.

Inducţia matematică constă în doi paşi: *verificarea* şi *etapa de demonstraţie*, numită şi *etapa inductivă*.

Inducţia simplă:

- Verificăm $P(n_0)$ adevărat.
- Presupunem $P(k)$ adevărat şi demonstrăm $P(k+1)$ adevărat.

Exemplul 1.1.1. *Putem folosi inducţia matematică simplă pentru a demonstra următoarea proprietate:*

Pentru orice numere reale $a_1, ..., a_n \geq 0$ are loc inegalitatea

$$\prod_{i=1}^{n}(1+a_i) \geq 1 + \sum_{i=1}^{n} a_i.$$

Vom aplica procedeul inducţiei pentru numărul numerelor pozitive din enunţ. Evident, nu are sens să consideră zero numere, deci $n \geq 1$.

Pasul 1. Verificarea: Dacă $n = 1$, atunci proprietatea se scrie

$$1 + a_1 \geq 1 + a_1,$$

ceea ce este adevărat (avem chiar egalitate).

Pasul 2. Etapa inductivă: Presupunem proprietatea adevărată pentru k numere reale pozitive şi o demonstrăm pentru $k + 1$ numere reale pozitive.

Presupunem deci că oricare ar fi numerele reale $a_1, ..., a_k \geq 0$, are loc inegalitatea

$$\prod_{i=1}^{k}(1 + a_i) \geq 1 + \sum_{i=1}^{k} a_i,$$

şi fie a_{k+1} un număr real pozitiv. Trebuie să verificăm faptul că

$$\prod_{i=1}^{k+1}(1 + a_i) \geq 1 + \sum_{i=1}^{k+1} a_i.$$

Pornim de la ipoteza de inducţie şi înmulţim inegalitatea $\prod_{i=1}^{k}(1 + a_i) \geq 1 + \sum_{i=1}^{k} a_i$ cu numărul pozitiv $1 + a_{k+1}$, ceea ce conduce la

$$\prod_{i=1}^{k+1}(1 + a_i) \geq \left(1 + \sum_{i=1}^{k} a_i\right)(1 + a_{k+1}).$$

Membrul drept al inegalităţii este egal cu

$$1 + \sum_{i=1}^{k+1} a_i + \sum_{i=1}^{k} a_i \cdot a_{k+1},$$

care este mai mare decât $1 + \sum_{i=1}^{k+1} a_i$. Am obţinut deci inegalitatea dorită, proprietatea este valabilă pentru $k + 1$ numere reale pozitive. Conform principiului inducţiei matematice, proprietatea anunţată este adevărată pentru orice numere reale pozitive.

Inducţia completă:

- Verificăm $P(n_0)$ adevărat.
- Presupunem $P(k)$ adevărat pentru orice $n_0 \leq k \leq n$ şi demonstrăm $P(n+1)$ adevărat.

Exemplul 1.1.2. *Să se determine numerele reale strict pozitive $a_1, a_2, ..., a_n$ astfel încât*

$$a_1^2 + a_2^2 + ... + a_n^2 = \frac{2n+1}{3}(a_1 + a_2 + ... + a_n), \quad \forall n \in \mathbb{N}^*.$$

Cheia rezolvării o reprezintă relaţia dată în ipoteză şi care are loc pentru orice n natural nenul. Vom da valori lui n pentru a determina a_n.

Dacă $n = 1$, atunci relaţia devine $a_1^2 = a_1$, care are soluţiile 0 şi 1. Ipoteza ca numerele să fie strict pozitive conduce la $a_1 = 1$.

Pentru $n = 2$, relaţia din ipoteză se scrie $a_1^2 + a_2^2 = \frac{5}{3}(a_1 + a_2)$. Ştim că $a_1 = 1$, deci a_2 este soluţia pozitivă a ecuaţiei $3a_2^2 - 5a_2 - 2 = 0$, de unde rezultă $a_2 = 2$. Aceste două valori obţinute: $a_1 = 1$, $a_2 = 2$, sugerează ca posibilitate $a_n = n$, pentru orice $n \in \mathbb{N}^*$.

Vom demonstra prin inducţie matematică completă propoziţia $a_n = n$, $(\forall)n \in \mathbb{N}^*$.

Pasul 1. Verificare: Pentru $n = 1$, s-a determinat mai sus $a_1 = 1$, deci este adevărat.

Pasul 2. Etapa inductivă. Presupunem $a_i = i$, $(\forall)i \in \{1, 2, ..., k\}$ şi demonstrăm $a_{k+1} = k + 1$. Remarcăm aici necesitatea inducţiei complete, deoarece relaţia din ipoteză, pentru $n = k + 1$, implică toate elementele a_i, cu $i \leq k + 1$.

Obţinem $1^2 + 2^2 + ... + k^2 + a_{k+1}^2 = \frac{2k+3}{3}(1 + 2 + ... + k + a_{k+1}$. Folosind formulele de calcul

$$1 + 2 + ... + k = \frac{k(k+1)}{2},$$

$$1^2 + 2^2 + ... + k^2 = \frac{k(k+1)(2k+1)}{6},$$

şi rezolvând ecuaţia obinută, găsim $a_{k+1} = k + 1$, ceea ce încheie demonstraţia.

Conform principiului inducţiei matematice, $a_n = n$, $(\forall)n \in \mathbb{N}^*$.

1.2 Mulţimi

Deoarece acest curs se adresează studenţilor de anul I şi reprezintă fundamentele albegrice ale informaticii, ne vom referi exclusiv la teoria clasică a mulţimilor în ceea ce urmează.

Prin urmare, noţiunea de mulţime trebuie gândită ca una primitivă, suficient de bine înţeleasă intuitiv, care nu este precis definită, dar care poate fi utilizată

în definirea altor noţiuni. Aşadar vom considera mulţimile ca fiind colecţii de obiecte numite elementele mulţimii.

O mulţime poate fi descrisă prin enumerarea elementelor sale sau prin precizarea unei proprietăţi pe care o au toate elementele sale şi doar ele.

Exemplul 1.2.1. *Mulţimea numerelor naturale pare mai mici decât 10 poate fi dată prin enumerare* $\{0, 2, 4, 6, 8\}$ *sau prin precizarea proprietăţii descrise,*

$$\{x \in \mathbb{N} | x < 10, \quad 2|x\}.$$

Notăm mulţimile cu litere mari ale alfabetului latin $(A, B, C, ..., X, Y, Z)$, iar elementele le notăm cu litere mici ale alfabetului latin $(a, b, c, ..., x, y, z)$. Dacă elementul a este obiect al mulţimii A vom spune că el *aparţine* mulţimii A şi vom nota acest fapt prin $a \in A$. În caz contrar, vom spune că a nu aparţine mulţimii A şi vom scrie $x \notin A$. Dacă toate elementele mulţimii A sunt şi elemente ale mulţimii B, atunci vom spune că mulţimea A este *inclusă* în mulţimea B şi vom nota acest fapt prin $A \subseteq B$. Dacă B are şi alte elemente în afară de cele ale mulţimii A, spunem că A este *inclusă strict* în mulţimea B şi notăm $A \subset B$.

Spunem că două mulţimi sunt egale dacă au aceleaşi elemente. Deci două mulţimi sunt egale dacă fiecare este inclusă în cealaltă.

Numărul de elemente al unei mulţimi A îl numim *cardinalul* mulţimii A şi îl notăm $|A|$. Mulţimile de cardinal finit se numesc mulţimi finite, iar cele de cardinal infinit se numesc mulţimi infinite. Mulţimea cu 0 elemente se numeşte mulţimea vidă şi se notează Φ. De remarcat faptul că două mulţimi de cardinale diferite nu pot fi egale.

Date fiind două elemente a, b, numim *pereche ordonată* notată (a, b) mulţimea $\{\{a\}, \{a, b\}\}$. Evident, egalitatea $(a, b) = (c, d)$ este posibilă dacă şi numai dacă $a = c$ şi $b = d$.

Date fiind două mulţimi A, B, din ele putem obţine noi mulţimi prin următoarele operaţii cu mulţimi:

1. *Intersectia* $(\cap)$: $A \cap B = \{x | x \in A$ şi $x \in B\}$. În cazul în care $A \cap B = \Phi$ spunem că mulţimile A şi B sunt *disjuncte*.
2. *Reuniunea* $(\cup)$: $A \cup B = \{x | x \in A$ sau $x \in B\}$.
3. *Diferenţa* $(-)$: $A - B = \{x | x \in A$ şi $x \notin B\}$.
4. *Diferenţa simetrică* (Δ): $A \Delta B = (A - B) \cup (B - A)$.
5. *Produs cartezian* $(\times)$: $A \times B = \{(a, b) | a \in A$ şi $b \in B\}$.

Operaţiile cu mulţimi au următoarele proprietăţi a căror verificare o lăsăm în

seama cititorului ca exerciţiu. Amintim doar faptul că egalitatea a două mulţimi se demonstrează prin dublă incluziune.

Propoziţia 1.2.1. *Fie A, B, C mulţimi. Atunci:*
(1) $A \cap (B \cap C) = (A \cap B) \cap C$ *(asociativitate);*
(2) $A \cap B = B \cap A$ *(comutativitate);*
(3) $A \cap A = A$ *(idempotenţă);*
(4) $A \cap \Phi = \Phi$;
(5) $A \cup (B \cup C) = (A \cup B) \cup C$ *(asociativitate);*
(6) $A \cup B = B \cup A$ *(comutativitate);*
(7) $A \cup A = A$ *(idempotenţă);*
(8) $A \cup \Phi = A$;
(9) $A - A = \Phi$, $A - \Phi = A$, $\Phi - A = \Phi$;
(10) $A - (B - C) = (A - B) \cup (A \cap C)$;
(11) $(A - B) \cup C = (A \cup C) - (B - C)$;
(12) $(A - B) \cap C = (A \cap C) - B = A \cap (C - B)$;
(13) $A \times (B \cap C) = (A \times B) \cap (A \times C)$; $(B \cap C) \times A = (B \times A) \cap (C \times A)$;
(14) $A \times (B \cup C) = (A \times B) \cup (A \times C)$; $(B \cup C) \times A = (B \times A) \cup (C \times A)$;
(15) $A \times (B - C) = (A \times B) - (A \times C)$;
(16) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.

Pentru o mulţime A notăm cu $P(A)$ mulţimea tuturor submulţimilor sale, numită *mulţimea părţilor lui A*. Au loc egalităţile
$P(A) \cap P(B) = P(A \cap B)$;
$P(A) \cup P(B) \subseteq P(A \cup B)$.

Exemplul 1.2.2. *Pentru $A = \{1, 2, 3\}$, mulţimea $P(A)$ este:*

$$\{\Phi, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}.$$

Propoziţia 1.2.2. *Dacă A este o mulţime finită cu $|A| = m$, atunci $|P(A)| = 2^m$.*

Demonstraţie: Vom demonstra prin inducţie matematică, după m.
Pas 1. $m = 0$, $A = \Phi$, $P(A) = \{\Phi\}$, deci $|P(A)| = 2^0$.
Pas 2. Presupunem că orice mulţime cu $m - 1$ elemente are exact 2^{m-1} submulţimi şi fie A cu m elemente. Fie $x \in A$, fixat arbitrar, iar $A' = A - \{x\}$. Toate submulţimile lui A care nu conţin elementul x sunt submulţimi ale lui A',

în număr de 2^{m-1}, conform ipotezei de inducţie. Submulţimile lui A care conţin x sunt de forma $B \cup \{x\}$, cu $B \subseteq A'$, deci tot 2^{m-1}. Avem deci

$$P(A) = P(A') \cup \{B \cup \{x\} | \quad B \in P(A')\}.$$

Mai mult cele două mulţimi de mai sus sunt disjuncte, deci

$$|P(A)| = 2^{m-1} + 2^{m-1} = 2^m.$$

□

Observaţia 1.2.1. *Afirmaţia din Propoziţia 1.1.2 se poate justifica şi utilizând identitatea*

$$C_m^0 + C_m^1 + ... + C_m^m = 2^m,$$

deoarece în $P(A)$ se află C_m^k submulţimi cu k elemente, $\forall k = \overline{0, m}$.

Propoziţia 1.2.3. *Dacă A,B sunt două mulţimi finite cu $|A| = m$, $|B| = n$, atunci*

$$|A \times B| = m \cdot n.$$

Demonstraţie: Afirmaţia se demonstrază prin inducţie matematică după m (sau n) şi o lăsăm cititorului. Remarcăm faptul că dacă $A = \Phi$ sau $B = \Phi$, atunci $A \times B = \Phi$.

Fie M o mulţime şi A o submulţime a sa. Diferenţa $M - A$ se mai numeşte *complementara* mulţimii A şi se notează $C_M A$ sau simplu $\bar{A}$ dacă mulţimea M se subînţelege din context.

Propoziţia 1.2.4. *Fie M o mulţime nevidă şi A, B două submulţimi ale sale. Au loc următoarele egalităţi:*

a) $C_M(C_M A) = A$; $C_M \Phi = M$; $C_M M = \Phi$;

b) $C_M(A \cap B) = C_M A \cup C_M B$; $C_M(A \cup B) = C_M A \cap C_M B$, *(legile lui De Morgan);*

c) $A \cap C_M A = \Phi$; $A \cup C_M A = M$; $A - B = A \cap C_M B$.

Demonstraţie: Se verifică fiecare egalitate prin dublă incluziune.

De exemplu, pentru prima lege a lui De Morgan, fie $x \in C_M(A \cap B)$, deci $x \in M$, dar $x \notin (A \cap B)$. De aici, $x \in A - B$ sau $x \in B - A$ sau $x \in M - (A \cup B)$, deci x se află în $C_M A$ sau se află în $C_M B$, adică $x \in C_M A \cup C_M B$. Am obţinut $C_M(A \cap B) \subseteq C_M A \cup C_M B$.

Fie acum $x \in C_M A \cup C_M B$, adică $x \in M$, $x \notin A$ sau $x \notin B$. Deci x poate fi în A dar nu în B, sau invers, de unde $x \in C_M(A \cap B)$. □

De multe ori, problemele legate de mulţimi finite implică necesitatea cunoaşterii numărului de cazuri pentru anumite situaţii. Cardinalul reuniunii unui număr finit de mulţimi finite este util de cunoscut. Evident, dacă mulţimile sunt disjuncte, atunci cardinalul reuniunii este suma cardinalelor. În cazul general acest fapt nu mai este valabil şi lăsăm ca exerciţiu stabilirea prin inducţie matematică a următorului rezultat, cunoscut sub numele de *Principiul includerii şi excluderii*:

Propoziţia 1.2.5. *Cardinalul reuniunii a m mulţimi este dat de formula de mai jos*

$$|A_1 \cup A_2 \cup ... \cup A_m| = \sum_{i=1}^{m} |A_i| - \sum_{1 \le i < j \le m} |A_i \cap A_j| + ...+$$

$$+(-1)^k \sum_{1 \le i_1 < i_2 < ... < i_k \le m} |A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_k}| + ... + (-1)^{n+1} | \cap_{i=1}^{m} |A_i||.$$

1.3 Relaţii

Intuitiv, prin relaţie între două mulţimi înţelegem o legătură oarecare între elementele lor. Fie A şi B mulţimi nevide.

Definiţia 1.3.1. *Numim **relaţie** de la A la B un triplet $R = (A, B, G_R)$, unde G_R este o submulţime a produsului cartezian $A \times B$. Dacă $A = B$, relaţia R se numeşte relaţie binară pe A.*

Dacă R este o relaţie de la mulţimea A la mulţimea B şi elementul $a \in A$ se află în relaţia R cu elementul $b \in B$, atunci $(a, b) \in G_R$ sau, mai simplu, putem scrie aRb. Mulţimea A se numeşte domeniul relaţiei, B codomeniul, iar G_R graficul relaţiei R.

Exemplul 1.3.1. *a) $R = (A, B, G_R)$, cu $G_R = \{(a, 1), (a, 2), (b, 1)\}$ este o relaţie de la mulţimea $A = \{a, , b, c, d\}$ la mulţimea $B = \{1, 2, 3, 4, 5\}$.*

b) Relaţia de divizibilitate pe mulctimea numerelor întregi: $R = (\mathbb{Z}, \mathbb{Z}, G_R)$, este definită prin graficul $G_R = \{(a, ka) | a, k \in \mathbb{Z}\}$.

c) Relaţia de asociere în divizibilitate pe $\mathbb{Z}$, are graficul $\{(a,-a)|a\in\mathbb{Z}\}$.

d) Relaţia de incluziune pe $P(A)$: $G_{\subseteq}=\{(B,A)|B\subseteq A\}$.

e) Relaţia de congruenţă modulo n pe $\mathbb{Z}$, are graficul $\{(x,x+nk)\in\mathbb{Z}\times\mathbb{Z}$ $|x,k\in\mathbb{Z}\}$.

f) Relaţia totală pe mulţimea A, are graficul $A\times A$.

g) Relaţia de egalitate pe o mulţime oarecare A, cu graficul $\{(a,a)|a\in A\}$, este numită diagonala mulţimii A.

Date fiind două relaţii $R=(A,B,G_R)$ şi $S=(C,D,G_S)$, dacă B şi C nu sunt disjuncte, atunci putem obţine o nouă relaţie din cele două, numită compusa lor şi notată $S\circ R$. Această nouă relaţie, $S\circ R=(A,D,G_{S\circ R})$, este definită prin graficul

$$G_{S\circ R}=\{(a,d)|(\exists)x\in B\cap C,(a,x)\in R,(x,d)\in S\}.$$

Dată fiind relaţia R de la A la B, relaţia inversă este R^{-1} de la B la A definită prin:

$$G_{R^{-1}}=\{(x,y)\in B\times A|(y,x)\in G_R\}.$$

Exemplul 1.3.2. *Fie mulţimile $A=\{1,2,3\}$, $B=\{1,2,3,4\}$, $C=\{2,3,4,5\}$ şi relaţiile R şi S cu graficele $G_R\subseteq A\times B$, $G_S\subseteq B\times C$:*

$$G_R=\{(1,1),(1,2),(2,3),(2,1),(3,4)\},\quad G_S=\{(1,2),(2,3),(2,4),(3,3),(3,5)\}.$$

Putem calcula

$$G_{S\circ R}=\{(x,y)\in A\times C|(\exists)z\in B,(x,z)\in R,(z,y)\in S\}=$$
$$=\{(1,2),(1,3),(1,4),(2,3),(2,5),(2,2)\},$$
$$G_{R^{-1}}=\{(1,1),(2,1),(3,2),(1,2),(4,3)\}\subseteq B\times A.$$

Fie relaţia $R=(A,B,G_R)$. De multe ori se foloseşte şi următoarea terminologie, restrângâd noţiunile de domeniu şi codomeniu astfel: Mulţimea elementelor x din A cu proprietatea că există $y\in B$ astfel încât $(x,y)\in R$ se numeşte *domeniul* relaţiei R. Mulţimea elementelor y din B cu proprietatea că există $x\in A$ astfel încât $(x,y)\in R$ se numeşte *codomeniul* relaţiei R.

O relaţie $R=(A,B,G_R)$ se numeşte *peste tot definită* dacă domeniul său în accepţiunea de mai sus este A. Relaţia R din exemplul anterior este peste tot definită, dar relaţia S nu este peste tot definită deoarece domeniul relaţiei S este $\{1,2,3\}$ şi nu coincide cu B.

O relaţie peste tot definită $R = (A, B, G_R)$ se numeşte *funcţională* dacă pentru orice $x \in A$ există exact un y în B astfel încât $(x, y) \in R$. Relaţia R din exemplul anterior nu este funcţională deoarece elementului $1 \in A$ îi asociază mai mult de un element din B. Relaţia R^{-1} din al cărei grafic excludem $\{(1, 1)\}$, din acelaşi exemplu, este funcţională.

Fie $x, y \in A$ şi $R = (A, A, G_R)$ o relaţie binară pe A.

Relaţia binară R se numeşte:
a) *reflexivă* dacă xRx, $(\forall)x \in A$;
b) *simetrică* dacă xRy implică yRx;
c) *tranzitivă* dacă xRy şi yRz implică xRz;
d) *antisimetrică* dacă xRy şi yRx implică $x = y$.

O relaţie binară R pe o mulţime A se poate reprezenta sub formă de reţea în care nodurile sunt elementele mulţimii iar între două noduri $a, b \in A$ există un arc orientat de la a la b dacă şi numai dacă $(a, b) \in R$. Relaţia este reflexivă dacă în fiecare nod avem buclă. Este simetrică dacă pentru fiecare arc între două noduri există arc invers şi este tranzitivă dacă oricare două arce în care vârful primului coincide cu originea celuilalt se închid formând un triunghi ca la suma vectorilor (pentru arcele (a, b) şi (b, c) există şi arcul (a, c)).

Definiţia 1.3.2. *O relaţie reflexivă, tranzitivă şi simetrică se numeşte* ***relaţie de echivalenţă****.*

O relaţie reflexivă, tranzitivă şi antisimetrică se numeşte ***relaţie de ordine****.*

Relaţiile de echivalenţă se notează de obicei cu $\approx$, $\equiv$, iar cele de ordine $\leq$.

Exemplul 1.3.3. *a) Relaţia de egalitate pe orice mulţime şi cea de congruenţă modulo n pe $\mathbb{Z}$ sunt relaţii de echivalenţă.*

b) Relaţiile de divizibilitate în $\mathbb{N}$, de incluziune pe $P(A)$ sunt relaţii de ordine.

c) Relaţia de "mai mic sau egal" pe oricare din mulţimile de numere: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, este o relaţie de ordine.

d) Relaţia de divizibilitate pe $\mathbb{Z}$ nu este o relaţie de ordine deoarece nu este antisimetrică ($a|-a$, $-a|a$, dar $a \neq -a$ pentru a nenul), iar relaţia de asociere în divizibilitate este relaţie de echivlenţă pe $\mathbb{Z}$.

Fie $\approx$ o relaţie de echivalenţă pe mulţimea A. Pentru orice $a \in A$, notăm $\widehat{a}$

mulţimea

$$\widehat{a} = \{x \in A / x \approx a\},$$

şi o numim *clasa de echivalenţă a elementului a*. De remarcat faptul că $a \approx x$ este echivalent cu $\widehat{a} = \widehat{x}$. Într-adevăr, dacă $a \approx x$, atunci orice element $y \in \widehat{a}$ va verifica şi $y \approx x$ din tranzitivitatea şi simetria relaţiei $\approx$.

Mulţimea tuturor claselor de echivalenţă se numeşte *mulţimea cât* şi se notează $A/_{\approx}$.

Numim *sistem de reprezentanţi* pentru relaţia de echivalenţă $\approx$ o familie de elemente $(x_i)_{i \in I}$ din A cu proprietatea că pentru orice $x \in A$ există un unic $i \in I$ astfel încât $x \approx x_i$. Intuitiv, obţinem un sistem de reprezentanţi ai claselor de echivalenţă alegând câte un element din fiecare clasă de echivalenţă. Fundamentarea teoretică a posibilităţii acestor alegeri o reprezintă Axioma Alegerii, dar acest fapt depăşeşte cadrul acestui curs.

Notăm $(x_i)_{i \in I}$ sistemul de reprezentanţi ales, iar $|I|$ este numărul clselor de echivalenţă. Atunci

$$A/_{\approx} = \{\widehat{x_i} | i \in I\}.$$

Exemplul 1.3.4. *Fie $n \in \mathbb{N} - \{0, 1\}$. Relaţia de congruenţă modulo n pe $\mathbb{Z}$ se defineşte astfel:*

Fie $x, y \in \mathbb{Z}$. Prin definiţie,

$$x \equiv y(mod n) \Leftrightarrow n \,|(x - y)$$

Din proprietăţile divizibilităţii, rezultă imediat că este o relaţie de echivalenţă. Clasele de echivalenţă se numesc clase de resturi modulo n. Mullţimea cât se notează $\mathbb{Z}_n$. Folosind teorema împărţirii cu rest în $\mathbb{Z}$ se arată că $\mathbb{Z}_n$ are n elemente, $\mathbb{Z}_n = \{\widehat{0}, \widehat{1}, ..., \widehat{n-1}\}$. Într-adevăr, $(\forall)x \in \mathbb{Z}$, $(\exists)c, r \in \mathbb{Z}$, $x = c \cdot n + r$, $0 \leq r < n$, deci $x \equiv r(mod n)$. Prin urmare toate numerele întregi de forma $nk + r$ aparţin clasei cu reprezentantul r. Restul r poate lua valorile $0, 1, ..., n-1$, deci există exact n clase de echivalenţă în raport cu relaţia de congruenţă modulo n.

Exemplul 1.3.5. *Fie $A = \{1, 2, 3, 4\}$ şi*

$$G_R = \{(1,1), (1,2), (2,1), (2,2), (3,3), (3,4), (4,3), (4,4)\} \subseteq A \times A$$

graficul unei relaţii binare pe A. Reprezentând acestă relaţie ca o reţea se verifică faptul că este o relaţie de echivalenţă. Clasele de echivalenţă sunt $\{1, 2\}$ şi $\{3, 4\}$.

Ele pot fi numite prin oricare dintre elementele care le alcătuiesc, adică un sistem de reprezentanţi pentru R este $(1,3)$. Prima clasă este $\widehat{1}=\widehat{2}$, iar a doua $\widehat{3}=\widehat{4}$. Mulţimea cât este $A/_R=\{\widehat{1},\widehat{3}\}$.

Definiţia 1.3.3. *Fie A o mulţime nevidă. Numim **partiţie** a mulţimii A o familie de submulţimi nevide şi disjuncte ale lui A, a căror reunuiune este A, adică o submulţime $\{M_i\}_{i\in I}$ a mulţimii părţilor lui A, astfel încât:*

1. *$M_i\neq\Phi,(\forall)i\in I$,*
2. *$M_i\cap M_j=\Phi,(\forall)i\neq j,i,j\in I$,*
3. *$A=\cup_{i\in I}M_i$.*

Exemplul 1.3.6. *Mulţimea $A/_R$ din ultimul exemplu este o partiţie a mulţimii $\{1,2,3,4\}$.*

Observaţia 1.3.1. *a) Dacă $\{M_i\}_{i\in I}$ este o partiţie a unei mulţimi finite A, atunci I, M_i sunt finite, $(\forall)i\in I$ şi, fiind disjuncte,*

$$|A|=\sum_{i\in I}|M_i|.$$

b) Pe o mulţime de cardinal patru $A=\{1,2,3,4\}$, există 15 partiţii posibile, deoarece cardinalul 4 se poate "acoperi" astfel:

$4=4$ într-un singur mod, corespunzător partiţiei $A=A$,

$4=3+1$ în C_4^1 moduri, corespunzător partiţiilor de tipul $A=\{1\}\cup\{2,3,4\}$,

$4=2+1+1$ în C_4^2 moduri, corespunzător partiţiilor de tipul $A=\{1\}\cup\{2\}\cup\{3,4\}$,

$4=2+2$ în $\frac{C_4^2}{2}$ moduri, corespunzător partiţiilor de tipul $A=\{1,2\}\cup\{3,4\}$. Aici am împărţit la 2 numărul alegerilor de submulţimi de câte două elemente deoarece alegerea mulţimii $\{1,2\}$ care dă partiţia de mai sus, conduce la aceeaşi partiţie cu alegerea submulţimii $\{3,4\}$.

$4=1+1+1+1$ într-un singur mod, $A=\{1\}\cup\{2\}\cup\{3\}\cup\{4\}$.

Teorema 1.3.1. *O relaţie de echivalenţă pe o mulţime determină o partiţie a acesteia şi reciproc.*

Demonstraţie: Fie $\approx$ o relaţie de echivalenţă pe mulţimea A şi

$$A/_\approx=\{\hat{x_i}|i\in I\},$$

mulţimea cât, unde $(x_i)_{i\in I}$ este un sistem de reprezentanţi pentru $\approx$. Următoarele afirmaţii sunt adevărate:

a) $x \in \widehat{x}$, $(\forall)x \in A$, deoarece $\approx$ este reflexivă;

b) $\widehat{x} = \widehat{y} \Leftrightarrow x \approx y$. Într-adevăr, implicaţia directă are loc deoarece $x \in \widehat{x}$, iar cea inversă din definiţia clasei de echivalenţă.

c) $(\forall)x, y \in A$, $\widehat{x} \cap \widehat{y} = \Phi$ sau $\widehat{x} = \widehat{y}$. Presupunând că $\widehat{x} \cap \widehat{y} \neq \Phi$ obţinem $x \approx y$ din tranzitivitatea relaţiei $\approx$, deci conform b) cele două clase sunt egale.

d) $A = \cup_{i \in I} \widehat{x_i}$. Egalitatea aceasta se verifică prin dublă incluziune. Avem incluziunea directă deoarece din definiţia sistemului de reprezentanţi, fiecare element $x \in A$ aparţine unei clase $\hat{x_i}$, cu $i \in I$.

Relaţiile a), b), c) afirmă că $A/_{\approx}$ este o partiţie a mulţimii A.

Reciproc, dacă $\{M_i\}_{i \in I} \subseteq P(A)$ este o partiţie a mulţimii A, atunci relaţia:

$$x \approx y \Leftrightarrow (\exists)i \in I, x, y \in M_i,$$

este o relaţie de echivalenţă pe A (verificarea o lăsăm cititorului). Clasele de echivalenţă ale acestei relaţii sunt exact elementele partiţiei date. □

Fie acum $\leq$ o relaţie de ordine pe A. Mai spunem că $(A, \leq)$ este o mulţime ordonată. Mulţimea A este *total ordonată* prin relaţia $\leq$ dacă $(\forall)x, y \in A$ avem $x \leq y$ sau $y \leq x$.

Exemplul 1.3.7. *Relaţia $\subseteq$ pe $P(A)$ este o relaţie de ordine care nu este totală.*

Relaţia $\leq$ pe mulţimea numerelor reale este o relaţie de ordine totală.

Un element $m \in A$ se numeşte:

- *cel mai mic element* dacă $m \leq x$, $(\forall)x \in A$; -

- *element minimal* dacă $x \leq m$ implică $x = m$ (nu există în A elemente mai mici decât m).

Un element $M \in A$ se numeşte:

- *cel mai mare element* dacă $x \leq M$, $(\forall)x \in A$;

- *element maximal* dacă $M \leq x$ implică $x = M$ (nu există în A elemente mai mari decât M).

Fie x, y două elemente din mulţimea ordonată $(A, \leq)$.

Elementul $a \in A$ se numeşte *infimumul* mulţimii $\{x, y\}$ dacă $a \leq x$, $a \leq y$ şi pentru orice $a' \in A$ cu $a' \leq x$, $a' \leq y$, are loc $a' \leq a$. Notăm $a = inf\{x, y\}$.

Elementul $b \in A$ se numeşte *supremumul* mulţimii $\{x, y\}$ dacă $x \leq b$, $y \leq b$ şi pentru orice $b' \in A$ cu $x \leq b'$, $y \leq b'$, are loc $b \leq b'$. Notăm $b = sup\{x, y\}$.

Fie $(A, \leq)$ o mulţime ordonată şi $B \subseteq A$ o submulţime a sa.

Elementul $a \in A$ se numeşte:
- *minorant* al mulţimii B dacă $a \leq x$, $(\forall)x \in B$;
- infimumul mulţimii B dacă este cel mai mare minorant. Notăm $a = infB$;
- *majorant* al mulţimii B dacă $x \leq a$, $(\forall)x \in B$;
- supremumul mulţimii B dacă este cel mai mic majorant. Notăm $a = supB$.

Exemplul 1.3.8. *a) Mulţimea ordonată $(P(A), \subseteq)$ are cel mai mare element A şi cel mai mic element mulţimea vidă.*

b)Fie $A = \{1, 2, 3, 4, 5, 6\}$, ordonată prin relaţia de divizibilitate. Cel mai mic element este 1, cel mai mare nu există. Elementele maximale sunt $4, 6$; $inf\{4, 6\} = 2$, $sup\{4, 6\}$ nu există. Văzută ca submulţime a mulţimii ordonate $(\mathbb{N}, |)$, $supA = 60$.

O mulţime ordonată se numeşte *bine ordonată* dacă orice submulţime nevidă a sa are un cel mai mic element. Mulţimea numerelor naturale cu relaţia de ordine uzuală este un exemplu de mulţime bine ordonată. Mulţimea de la punctul b) din ultimul exemplu este bine ordonată.

O mulţime ordonată se numeşte *inductiv ordonată* dacă orice submulţime total ordonată a sa admite un majorant. Foarte important este următorul rezultat:

Teorema 1.3.2. ***Lema lui Zorn*** *Orice mulţime ordonată nevidă care este inductiv ordonată are cel puţin un element maximal.*

O mulţime ordonată în care există infimumul şi supremumul pentru orice două elemente se numeşte *latice*. Dacă în plus există şi cel mai mic (notat 0), respectiv cel mai mare (notat 1) element, laticea se numeşte *latice cu 0 şi 1.*

Exemplul 1.3.9. *a) Mulţimea ordonată $(P(A), \subseteq)$ este o latice cu 0 şi 1, deoarece pentru orice $X, Y \in P(A)$, $inf\{X, Y\} = X \cap Y$, $sup\{X, Y\} = X \cup Y$, Φ e cel mai mic element, A este cel mai mare element.*

b) Mulţimea numerelor naturale odonată cu relaţia de ordine obişnită $\leq$ este o latice doar cu 0, deoarece nu există cel mai mare element. Pentru orice două numere naturale x, y, $inf\{x, y\} = min\{x, y\}$, $sup\{x, y\} = max\{x, y\}$.

c) Mulţimea D_n a divizorilor naturali ai numărului natural n este o latice cu 0 şi 1 în raport cu relaţia de divizibilitate, deoarece $(\forall)x, y \in D_n$, $inf\{x, y\} = (x, y)$, $sup\{x, y\} = [x, y]$, unde $(x, y), [x, y]$ sunt notaţiile uzuale pentru cel mai mare divizor comun, respectiv cel mai mic multiplu comun al elementelor x, y. Cel mai mare element al mulţimii ordonate este n, iar cel mai mic este 1.

1.4 Funcţii

Noţiunea de funcţie se introduce în gimnaziu ca fiind o lege f care asociază fiecărui element dintr-o mulţime A numită *domeniu de definiţie*, un element şi numai unul din altă mulţime B, numită *codomeniu*.

Putem defini funcţia ca fiind o relaţie funcţională $f = (A, B, G_f)$.

Scriem $f : A \to B$, unde mulţimile A, B sunt domeniul, respectiv codomeniul funcţiei f. Pentru a defini o funcţie trebuie precizate domeniul, codomeniul şi legea de definiţie.

Două funcţii sunt egale dacă au acelaşi domeniu, codomeniu şi aceeaşi lege de definiţie.

Mulţimea funcţiilor definite pe A cu valori în B se notează B^A.

Exemplul 1.4.1. *Fie* $A = \{1, 2, 3\}$, $B = \mathbb{N}$.

a) $f : A \to B$, $\begin{array}{c|ccc} x & 1 & 2 & 3 \\ \hline f(x) & 1 & 4 & 9 \end{array}$ *şi* $g : A \to B$, $g(x) = x^2$ *sunt egale.*

b) $f : A \to B$, $f(x) = x - 2$ *nu este funcţie deoarece* $f(1) \notin B$.

c) Dată fiind o mulţime nevidă A*, funcţia*

$$\mathbf{1}_A : A \to A, \quad \mathbf{1}_A(x) = x, \quad (\forall)x \in A,$$

se numeşte funcţia identitate a mulţimii A*. Pentru* $a \in A$ *fixat, funcţia*

$$f : A \to A, \quad f(x) = a, \quad (\forall)x \in A,$$

se numeşte funcţia constantă a.

d) Pentru o mulţime nevidă A *se defineşte funcţia :*

$$\chi : P(A) \to \{0, 1\}^A, \quad \chi(A') = \chi_{A'} : A \to \{0, 1\},$$

$$\chi_{A'}(x) = 1, \quad x \in A', \quad \chi_{A'}(x) = 0, \quad x \notin A'.$$

Funcţia $\chi_{A'}$ *se numeşte funcţia caracteristică a submulţimii* $A' \subseteq A$.

Exemplul 1.4.2. *Fie* $A = \{1, 2, 3\}$ *şi* $B = \{a, b\}$. *Atunci*

$$B^A = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\},$$

unde:

x	1	2	3
$f_1(x)$	a	a	a
$f_2(x)$	a	a	b
$f_3(x)$	a	b	a
$f_4(x)$	a	b	b
$f_5(x)$	b	a	a
$f_6(x)$	b	a	b
$f_7(x)$	b	b	a
$f_8(x)$	b	b	b

.

Propoziţia 1.4.1. *Dacă mulţimile A, B sunt finite, de cardinal m, respectiv n, atunci $|B^A| = n^m$.*

Demonstraţie: Demonstraţia se face prin inducţie după m (cardinalul domeniului).

Pentru $m = 1$, $A = \{a_1\}$, $B = \{b_1, b_2, ..., b_n\}$, se pot defini n funcţii de la A la B prin $f_i(a_1) = b_i$, $(\forall)i \in \{1, 2, ..., n\}$.

Presupunem că de la mulţimea A' de cardinal $k-1$ la mulţimea B de mai sus există n^{k-1} funcţii şi fie $x \notin A'$ şi $A = A' \cup \{x\}$. Pentru a defini o funcţie de la A la B trebuie asociat fiecărui element din A unul şi numai unul din B. Elementului x îi putem asocia $f(x) \in B$ în n moduri. Pentru fiecare alegere a lui $f(x)$, mai avem de pus în corespondenţă elementele din A' cu cele din B, ceea se face în exact n^{k-1} moduri, conform ipotezei de inducţie. În final obţinem n^k funcţii de la A la B, deci propoziţia este adevărată pentru $m = k$.

Conform principiului inducţiei matematice, afirmaţia din ipoteză este adevărată pentru orice $m \in \mathbb{N}$. □

Fie funcţia $f : A \to B$. Mulţimea $G_f = \{(x, f(x))|x \in A\}$ se numeşte *graficul funcţiei f* şi tripletul (A, B, G_f) este o relaţie funcţională peste tot definită de la A la B. Remarcăm faptul că noţiunea de funcţie s-ar putea introduce şi pornind de la o relaţie funcţională peste tot definită de la domeniul de definiţie la codomeniu.

Fie funcţia $f : A \to B$, şi submulţimile $A' \subseteq A$, $B' \subseteq B$. Prin *imaginea mulţimii A' prin f* înţelegem

$$f(A') = \{b \in B/(\exists)a \in A', f(a) = b\} \subseteq B,$$

sau, echivalent,

$$f(A') = \{f(a)/a \in A'\} \subseteq B.$$

Submulţimea $Im(f) = f(A)$ a lui B se numeşte *imaginea funcţiei f.*

Prin *imaginea inversă* sau *preimaginea mulţimii B' prin f* înţelegem

$$f^{-1}(B') = \{a \in A / f(a) \in B'\} \subseteq A.$$

Exemplul 1.4.3. *a) Pentru funcţia* $f : \{1,2,3,4\} \to \{a,b,c\}$ *definită prin*

$$\begin{array}{c|cccc} x & 1 & 2 & 3 & 4 \\ \hline f(x) & a & a & b & a \end{array},$$

$Imf = \{a,b\}$, $f(\{1,2\}) = \{a\}$, $f^{-1}(\{c\}) = \Phi$, $f^{-1}(\{a,c\}) = \{1,2,4\}$.

b) Pentru funcţia $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2, (\forall)x \in \mathbb{R}$, *avem:*

$$Imf = [0,\infty), \quad f((-2,4]) = [0,16], \quad f^{-1}([4,9)) = (-3,-2] \cup [2,3),$$

$$f^{-1}(-\infty, 0]) = \{0\}.$$

Propoziţia 1.4.2. *Fie* $f : A \to B$, $A' \subseteq A$ *şi* $B' \subseteq B$. *Au loc incluziunile:*

$$A' \subseteq f^{-1}(f(A')); \quad f(f^{-1}(B')) \subseteq B'.$$

Demonstraţie: Fie $x \in A'$. Deoarece $f(x) \in f(A')$, rezultă că x este un element care prin funcţia f este "dus" în submulţimea $f(A')$ a codomeniului. Din definiţia preimaginii unei submulţimi printr-o funcţie rezultă $x \in f^{-1}(f(A'))$, ceea ce trebuia demonstrat.

Pentru a doua incluziune, fie $y \in f(f^{-1}(B'))$. Deci există $x \in f^{-1}(B')$ astfel încât $y = f(x)$. Dar apartenenţa lui x la $f^{-1}(B')$ revine la $f(x) \in B'$, de unde avem $y \in B'$. □

Definiţia 1.4.1. *Spunem că funcţia* $f : A \to B$ *este:*

a) ***injectivă*** *dacă* $f(x_1) = f(x_2)$ *implică* $x_1 = x_2$, *sau, echivalent, pentru* $x_1 \neq x_2$, $f(x_1) \neq f(x_2)$;

b) ***surjectivă*** *dacă* $Im(f) = B$;

c) ***bijectivă*** *dacă este injectivă şi surjectivă.*

Observaţia 1.4.1. *Din definiţie rezultă că o funcţie* $f : A \to B$ *este bijectivă dacă pentru orice element* $b \in B$ *există in mod unic un element* $a \in A$ *astfel încât* $b = f(a)$.

Exemplul 1.4.4. *a) Funcţia identică* $\mathbf{1}_A : A \to A$, $\mathbf{1}_A(x) = x$, $(\forall)x \in A$, *este bijectivă.*

b) Pentru $A' \subseteq A$, *funcţia incluziune* $i : A' \to A$, $\quad i(x) = x, (\forall)x \in A'$ *este injectivă dar nu mereu surjectivă.*

c) Funcţia caracteristică a submulţimii A', $\chi_{A'} : A \to \{0,1\}$, $\chi_{A'}(x) = 1$, *pentru* $x \in A'$, *respectiv* $\chi_{A'}(x) = 0$, *dacă* $x \notin A'$, *nu este nici injectivă nici surjectivă. Funcţia* $\chi : P(A) \to \{0,1\}^A$, $\chi(A') = \chi_{A'}$ *este bijectivă. (Verificaţi!).*

Două mulţimi între care există o bijecţie se numesc *echipotente*, sau *cardinal echivalente* deoarece au acelaşi număr de elemente.

Exemplul 1.4.5. *a) Mulţimile P(A) şi* $\{0,1\}^A$ *sunt echipotente, deoarece funcţia* χ *din exemplul anterior este bijectivă. În consecinţă,* $|P(A)| = 2^{|A|}$.

b) Funcţia $f : \mathbb{R} \to (0,1)$, *definită prin* $f(x) = \frac{e^x}{1+e^x}$ *este bijectivă, deci mulţimea numerelor reale este echipotentă cu intervalul* $(0,1)$.

Lăsăm ca exerciţiu următoarele afirmaţii:

Propoziţia 1.4.3. *Fie funcţia* $f : A \to B$, $A' \subseteq A$ *şi* $B' \subseteq B$.

a) Dacă f este injectivă, atunci $A' = f^{-1}(f(A'))$.

b) Dacă f este surjectivă, atunci $f(f^{-1}(B')) = B'$.

Fie funcţiile $f : A \to B$, $g : B \to C$. Prin *compunerea funcţiilor f* şi g se obţine funcţia $g \circ f : A \to C$ definită prin $(g \circ f)(x) = g(f(x))$, $(\forall)x \in A$. Se verifică cu uşurinţă faptul că:

Propoziţia 1.4.4. *Compunerea funcţiilor este asociativă.*

Definiţia 1.4.2. *O funcţie* $f : A \to B$ *se numeşte* ***inversabilă*** *dacă există* $g : B \to A$ *astfel încât* $g \circ f = \mathbf{1_A}$ *şi* $f \circ g = \mathbf{1_B}$. *Funcţia g se numeşte inversa funcţiei f şi se notează* f^{-1}.

Observaţia 1.4.2. *Când vorbim despre preimaginea unei mulţimi prin funcţia f folosim aceeaşi notaţie* f^{-1}, *fără nicio legătură însă cu inversa lui f, care există doar dacă f este bijectivă, după cum vom demonstra mai jos.*

Propoziţia 1.4.5. *O funcţie este inversabilă dacă şi numai dacă este bijectivă.*

Demonstraţie: Fie $f : A \to B$ o funcţie inversabilă şi g inversa sa. Pentru a demonstra injectivitatea lui f, fie $x, y \in A$ astfel încât $f(x) = f(y)$. Aplicăm funcţia g egalităţii anterioare şi obţinem $g(f(x)) = g(f(y))$. Din definiţia funcţiei inverse ştim că $g \circ f = \mathbf{1_A}$, deci rezultă $x = y$, adică funcţia f este injectivă. Pentru a arăta că f este surjectivă, fie $y \in B$, abitrar ales. Căutăm un $x \in A$ astfel încât $f(x) = y$. Existenţa funcţiei inverse $g : B \to A$ asigură asocierea fiecărui $y \in B$ cu un element din A şi anume $x = g(y)$. Mai mult, deoarece $f \circ g = \mathbf{1_B}$, rezultă $f(x) = f(g(y)) = y$, ceea ce trebuia demonstrat.

Reciproc, fie acum $f : A \to B$ o funcţie bijectivă. Din surjectivitatea lui f rezultă că putem asocia fiecărui $y \in B$ elementul $x \in A$ pentru care $f(x) = y$. Mai mult, acest element este unic din injectivitatea lui f. Deci această asociere defineşte o funcţie $g : B \to B$, $g(y) = x \Leftrightarrow y = f(x)$, $(\forall)y \in B$.

$$(f \circ g)(y) = y, \quad (g \circ f)(x) = x, \quad (\forall)x \in A, (\forall)y \in B,$$

deci g este inversa funcţiei f, prin urmare f este inversabilă. □

Încheiem acest paragraf cu câteva aspecte privind funcţiile cu domeniul şi codomeniul finit.

Propoziţia 1.4.6. *Fie A, B două mulţimi finite, $|A| = n$, $|B| = m$.*

a) Dacă $n \leq m$ atunci există funcţii injective $f : A \to B$. Numărul acestora este A_m^n. Dacă $n > m$ atunci nu există funcţii injective de la A la B.

b) Dacă $n \geq m$ atunci există funcţii surjective $f : A \to B$. Numărul acestora este

$$m^n - C_m^1(m-1)^n + C_m^2(m-2)^n - C_m^3(m-3)^n + ... + (-1)^{m-2}C_m^{m-2}2^n + (-1)^{m-1}C_m^{m-1}.$$

Dacă $n < m$ atunci nu există funcţii surjective de la A la B.

c) Dacă $m = n$ atunci există funcţii bijective $f : A \to B$. Numărul acestora este $n!$. Dacă $m \neq n$ atunci nu există funcţii bijective de la A la B.

Am notat cu A_m^n aranjamente de m luate câte n şi cu C_m^k combinări de m luate câte k.

Demonstraţie: Fie A, B două mulţimi finite ca în ipoteză şi $f : A \to B$.

a) Dacă f e injectivă, atunci două elemente distincte x, y din A au imagini distincte, deci $|A| \leq |B|$. Prin urmare aceasta este o condiţie necesară pentru existenţa funcţiilor injective de la A la B. Numărul funcţiilor injective este numărul

submulţimilor ordonate de n elemente, elementele mulţimii $f(A)$, submulţime a mulţimii B, cu m elemente, prin urmare A_m^n.

b) Dacă f este surjectivă, atunci fiecare element din B este imaginea cel puţin a unui element din A, deci $|A| \geq |B|$, ceea ce reprezintă o condiţie necesară pentru existenţa funcţiilor surjective de la A la B.

Pentru a stabili numărul funcţiilor surjective de la A la B, fie $B = \{b_1, b_2, ..., b_m\}$ şi pentru fiecare $i \in \{1, 2, .., m\}$ notăm cu $\mathbf{F}_i = \{f : A \to B | b_i \notin Imf\}$ mulţimea funcţiilor din B^A pentru care sigur b_i nu este imaginea unui element din A. Cu alte cuvinte, $\mathbf{F}_i$ conţine funcţiile definite pe A cu valori în $B - \{b_i\}$. Din Propoziţia 1.3.1 rezultă $|\mathbf{F}_i| = (m-1)^n$. Mulţimea funcţiilor de la A la B pentru care b_i şi b_j nu sunt imagini de elemente din A este $\mathbf{F}_i \cap \mathbf{F}_j$. Cardinalul acestei mulţimi este $(m-2)^n$ şi există C_m^2 astfel de mulţimi, numărul de alegeri $\{i, j\} \subset \{1, 2, ..., n\}$, etc. Mulţimea funcţiilor care nu sunt surjective este

$$\mathbf{F}_1 \cup \mathbf{F}_2 \cup ... \cup \mathbf{F}_m.$$

Cardinalul acestei mulţimi este, conform principiului includeriii şi excluderii,

$$|\mathbf{F}_1 \cup \mathbf{F}_2 \cup ... \cup \mathbf{F}_m| = \sum_{i=1}^{m} |\mathbf{F}_i| - \sum_{1 \leq i < j \leq m} |\mathbf{F}_i \cap \mathbf{F}_j| + ...+$$

$$+(-1)^k \sum_{1 \leq i_1 < i_2 < ... < i_k \leq m} |\mathbf{F}_{i_1} \cap \mathbf{F}_{i_2} \cap ... \cap \mathbf{F}_{i_k}| + ... + (-1)^{n+1} | \cap_{i=1}^{m} |\mathbf{F}_i| =$$

$$= m(m-1)^n - C_m^2(m-2)^n + ... + (-1)^k C_m^k (m-k)^n + ... + (-1)^{m-1} C_m^{m-1}(m-m+1)^n + 0.$$

Mulţimea funcţiilor surjective este deci

$$B^A - (\mathbf{F}_1 \cup \mathbf{F}_2 \cup ... \cup \mathbf{F}_m),$$

a cărui cardinal este

$$m^n - C_m^1(m-1)^n + C_m^2(m-2)^n - C_m^3(m-3)^n + ... + (-1)^{m-2} C_m^{m-2} 2^n + (-1)^{m-1} C_m^{m-1}.$$

c) Din a) şi b) rezultă că o condiţie necesară pentru existenţa funcţiilor bijective de la A la B este $m = n$. Numărul funcţiilor bijective este egal cu numărul de moduri în care asociem celor n argumente din A elemente distincte din cele n ale lui B, deci $n!$. □

Observaţia 1.4.3. *Fie mulţimea A finită şi $f : A \to A$. Funcţia f este injectivă dacă şi numai dacă este surjectivă. Într-adevăr, f este injectivă dacă şi numai dacă pentru orice $x \neq y$ din A, $f(x) \neq f(y)$ deci $f(A)$ are $|A|$ elemente. Mai mult, $f(A) \subset A$, deci $f(A) = A$, ceea ce este echivalent cu f este surjectivă.*

1.5 Exerciţii

Sugerăm cititorului rezolvarea următoarelor exerciţii pentru fixarea noţiunilor prezentate în acest capitol:

1. Fie $A = \{1, 2, 3, 4\}$, $B = \{2, 3, 4, 5\}$ şi $R = (A, A, G_R)$, $S = (A, B, G_S)$ relaţiile date prin

$$G_R = \{(1, 2), (1, 1), (2, 4), (3, 2), (3, 3), (4, 1), (4, 2), (4, 4)\},$$

$$G_S = \{(1, 3), (1, 5), (2, 2), (2, 3), (2, 4), (3, 2), (3, 5), (4, 2)\}.$$

Scrieţi relaţiile R^{-1}, S^{-1}, $R \circ R$, $S \circ R$, $(S \circ R)^{-1}$, $(R \circ S)^{-1}$, $R^{-1} \circ S^{-1}$, $S^{-1} \circ R^{-1}$.

2. Scrieţi toate partiţiile mulţimii $A = \{a, b, c, d\}$. Demonstraţi că o mulţime cu 5 elemente admite 52 de partiţii.

3. O relaţie R pe mulţimea A se numeşte circulară dacă $(\forall)x, y, z \in A$ astfel încât xRy şi yRz atunci zRx. Demonstraţi că o relaţie reflexivă şi circulară este o relaţie de echivalenţă.

4. Să se arate că dacă relaţiile binare R, S pe mulctimea A sunt relaţii de echivalenţă, atunci $R \circ S$ şi $S \circ R$ sunt relaţii de echivalenţă dacă şi numai dacă $R \circ S = S \circ R$.

5. Fie A, B două mulţimi nevide şi $f : A \to B$. Demonstraţi că f este injectivă dacă şi numai dacă

$$|f^{-1}(f(x))| = 1, \quad (\forall)x \in A.$$

6. Fie funcţiile $f : A \to B$ şi $g : B \to C$. Demonstraţi că:
a) Dacă $g \circ f$ este injectivă, atunci f este injectivă.
b) Dacă $g \circ f$ este surjectivă, atunci g este surjectivă.
c) Dacă $g \circ f$ este bijectivă, atunci f este injectivă şi g este surjectivă.

7. Fie $f : A \to B$ o funcţie surjectivă şi $\approx$ o relaţie binară pe A definită prin

$$x \approx y \Leftrightarrow f(x) = f(y).$$

Demonstraţi că $\approx$ este o relaţie de echivalenţă ale cărei clase de echivalenţă sunt $\{f^{-1}(b)| \quad b \in B\}$.

8. Demonstraţi că relaţiile R_1, R_2, R_3, R_4 pe mulţimea numerelor complexe $\mathbf{C}$, definite prin

$$zR_1w \Leftrightarrow Re(z) = Re(w),$$

$$zR_2w \Leftrightarrow Im(z) = Im(w),$$

$$zR_3w \Leftrightarrow arg(z) = arg(w) sauz = w = 0,$$

$$zR_4w \Leftrightarrow |z| = |w|,$$

sunt relaţii de echivalenţă pe mulţimea numerelor complexe, unde am notat prin $Re(z)$, $Im(z)$, $arg(z)$, $|z|$ partea reală, coeficientul părţii imaginare, argumentul, respectiv modulul numărului complex z. Reprezentaţi grafic clasa de echivalenţă a elementului $1 + i$ în raport cu fiecare relaţie.

9. Pe mulţimea numerelor reale se definesc relaţiile R_1 şi R_2 date prin

$$xR_1y \Leftrightarrow [x] = [y],$$

$$xR_2y \Leftrightarrow \{x\} = \{y\},$$

unde $[x]$ este partea întreagă, iar $\{x\}$ este partea fracţionară a numărului real x. Demonstraţi că R_1 şi R_2 sunt relaţii de echivalnţă. Arătaţi că mulţimea cât $\mathbb{R}/_{R_1}$ este cardinal echivalentă cu mulţimea numerelor întregi şi mulţimea cât $\mathbb{R}/_{R_2}$ este cardinal echivalentă cu intervalul [0,1).

Capitolul 2

Structuri algebrice. Monoid. Grup

2.1 Legi de compoziţie

Fie A o mulţime nevidă. O funcţie $\cdot : A \times A \to A$ se numeşte *lege de compoziţie* binară pe A.

Fie o lege de compoziţie "$\cdot$" pe mulţimea A. Unei perechi $(x, y) \in A \times A$ îi corespunde un element notat $x \cdot y \in A$.

Definiţia 2.1.1. *O mulţime A dotată cu o lege de compoziţie se numeşte* ***magmă****.*

Definiţia 2.1.2. *Legea de compoziţie $\cdot$ pe mulţimea A se numeşte:*
a) ***asociativă*** *dacă $(\forall)x, y, z \in A$ are loc $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.*
b) ***comutativă*** *dacă $(\forall)x, y \in A$ are loc $x \cdot y = y \cdot x$.*
c) ***cu element neutru*** *dacă*

$$(\exists)e \in A, \quad (\forall)x \in A, \quad x \cdot e = e \cdot x = x.$$

Definiţia 2.1.3. *O mulţime A dotată cu o lege de compoziţie asociativă se numeşte* ***semigrup****.*

O submulţime $A' \subset A$ spunem că este parte stabilă în raport cu "$\cdot$" dacă

$$(\forall)x, y \in A', \quad x \cdot y \in A'.$$

De multe ori legea de compoziţie se notează aditiv, " $+$ ". Vom prefera notaţia multiplicativă, rămânând ca cititorul să transpună toate noţiunile ce vor fi introduse şi în notaţie aditivă.

Propoziţia 2.1.1. *Dacă legea de compoziţie "$\cdot$" pe A admite element neutru, atunci acesta este unic.*

Demonstraţie: Fie e şi e' două elemente din A cu proprietatea că $(\forall)x \in A$ are loc $x \cdot e = e \cdot x = x$ şi $x \cdot e' = e' \cdot x = x$. Pentru $x = e'$ în primul şir de egalităţi şi $x = e$ în al doilea, rezultă $e' = e' \cdot e = e$, deci elementul neutru este unic. □

In cazul notaţiei aditive, elementul neutru (dacă există) îl notăm 0 şi îl mai numim *elementul nul /zero.* În notaţie multiplicativă, elementul neutru se noteză 1 şi se mai numeşte *elementul unu/unitate.* În general, elementul neutru se notează cu e.

2.2 Monoid

Definiţia 2.2.1. *O mulţime A pe care s-a dat o lege de compoziţie asociativă şi cu element neutru se numeşte* ***monoid****.*

Exemplul 2.2.1. *a) Mulţimile de numere: naturale, întregi, raţionale, reale, sunt monoizi în raport cu adunarea, respectiv cu înmulţirea uzuale definite pe acestea.*

b) Dată fiind o mulţime nevidă, mulţimea A^A a tuturor funcţiilor definite pe A cu valori în A este monoid în raport cu compunerea funcţiilor. Elementul neutru este aici funcţia identică $\mathbf{1_A}$.

Fie $(A, \cdot)$ un monoid şi e elementul său neutru.

Definiţia 2.2.2. *Un element $x \in A$ se numeşte* ***simetrizabil*** *dacă există un element $x' \in A$ astfel încât*

$$x \cdot x' = x' \cdot x = e.$$

Elementul x' din definiţia anterioară se numeşte în general *simetricul lui x.* În cazul notaţiei aditive, simetricul lui x (dacă există) se mai numeşte *opusul* lui x şi se notează $-x$. În notaţie multiplicativă, simetricul lui x (dacă există) se mai numeşte *inversul* lui x şi se notează x^{-1}.

Mulţimea elementelor simetrizabile ale monoidului A se notează $U(A)$.

Exemplul 2.2.2. *a) În monoidul $(\mathbb{N}, +)$ singurul element simetrizabil este 0, pe când în monoizii $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, toate elementele sunt simetrizabile, opusul unui element x fiind numărul $-x$.*

b) În monoidul $(\mathbb{N}, \cdot)$ *singurul element simetrizabil este* 1, *în monoidul* $(\mathbb{Z}, \cdot)$ *singurele elemente simetrizabile sunt* $-1, 1$, *pe când în monoizii* $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, *toate elementele diferite de zero sunt simetrizabile, inversul unui element nenul* x *fiind numărul* $\frac{1}{x}$.

c) În monoidul $(A^A, \circ)$ *elementele simetrizabile sunt funcţiile bijective, ştiut fiind faptul că orice funcţie bijectivă este inversabilă şi reciproc. Mulţimea* $U(A^A)$ *se notează* $S(A)$ *şi se numeşte mulţimea permutărilor mulţimii* A.

Propoziţia 2.2.1. *Fie* $(A, \cdot)$ *un monoid. Dacă* $x \in A$ *este simetrizabil, atunci simetricul său este unic.*

Demonstraţie: Fie x' şi $x"$ două elemente din monoidul $(A, \cdot)$ cu proprietatea că

$$x \cdot x' = x' \cdot x = e, \quad x \cdot x" = x" \cdot x = e.$$

Înmulţind primul şir de egalităţi la stânga cu $x"$ şi al doilea la dreapta cu x', obţinem

$$x" = x" \cdot x \cdot x' = x',$$

deci simetricul unui element, dacă există, este unic. □

Fie $(A, \cdot)$ un monoid şi n un întreg pozitiv. Notăm

$$x^n = \underbrace{x \cdot x \cdot ... \cdot x}_{n} \in A.$$

În notaţie aditivă pentru un monoid $(A, +)$, egalitatea de mai sus se scrie

$$nx = \underbrace{x + x + ... + x}_{n}.$$

Au loc următoarele reguli de calcul într-un monoid $(A, \cdot)$ cu elementul neutru e, reguli pe care sugerăm cititorului să le transcrie şi pentru un monoid $(A, +)$:

Propoziţia 2.2.2. *a) Dacă* $x, y \in U(A)$, *atunci* $x \cdot y \in U(A)$ *şi* $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.

b) Dacă $x \in U(A)$, *atunci* $x^{-1} \in U(A)$ *şi* $(x^{-1})^{-1} = x$.

c) Pentru orice întregi pozitivi n, m *şi* $x \in A$, *au loc relaţiile:*

$$e^n = e, \quad x^n \cdot x^m = x^{n+m}, \quad (x^n)^{-1} = (x^{-1})^n, \quad (x^m)^n = x^{nm}.$$

d) Pentru orice $x, y \in A$ *astfel încât* $x \cdot y = y \cdot x$, *are loc egalitatea*

$$(x \cdot y)^n = x^n \cdot y^n.$$

Demonstraţie: a) Deoarece $x, y \in U(A)$, există $x^{-1}, y^{-1} \in U(A)$ astfel încât $x \cdot x^{-1} = x^{-1} \cdot x = e$, $y \cdot y^{-1} = y^{-1} \cdot y = e$. Calculăm

$$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = x \cdot (y \cdot y^{-1}) \cdot x^{-1} = x \cdot x^{-1} = e,$$

$$(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = y^{-1} \cdot (x^{-1} \cdot x) \cdot y = y^{-1} \cdot y = e,$$

deci elementul $x \cdot y$ admite simetricul $y^{-1} \cdot x^{-1}$.

b) Elementul x simetrizabil în monoidul $(A, \cdot)$ implică existenţa lui $x^{-1} \in A$ cu proprietatea

$$x \cdot x^{-1} = x^{-1} \cdot x = e,$$

ceea ce înseamnă că pentru elementul $x^{-1} \in A$ există $x \in A$ cu proprietatea simetricului. Deci $x^{-1} \in U(A)$ şi $(x^{-1})^{-1} = x$.

c) Evident $e^n = e$. Relaţiile $x^n \cdot x^m = x^{n+m}$ şi $(x^n)^m = x^{nm}$ sunt adevărate din definiţia lui x^n. Se arată prin inducţie matematică după n că $(x^n)^{-1} = (x^{-1})^n$, $(\forall) n \in \mathbb{N}$.

d) Din ipoteza $x \cdot y = y \cdot x$ rezultă prin inducţie matematică

$$x \cdot y^n = y^n \cdot x, \quad (\forall) n \in \mathbb{N}^*.$$

Vom demonstra acum prin inducţie matematică

$$(x \cdot y)^n = x^n \cdot y^n, \quad (\forall) n \in \mathbb{N}^*.$$

Pentru $n = 1$ este evident. Presupunem că $(x \cdot y)^k = x^k \cdot y^k$, oricare ar fi $k < n$ şi să demonstrăm $(x \cdot y)^n = x^n \cdot y^n$. Calculăm

$$(x \cdot y)^n = (x \cdot y)^{n-1} \cdot (x \cdot y) = x^{n-1} \cdot (y^{n-1} \cdot x) \cdot y = x^{n-1} \cdot (x \cdot y^{n-1}) \cdot y = x^n \cdot y^n.$$

□

Fie $(A, \cdot)$, $(B, *)$ monoizi, cu elementele neutre e_A, respectiv e_B.

Definiţia 2.2.3. *O funcţie $f : A \to B$ se numeşte **morfism de monoizi** dacă verifică:*

$$f(x \cdot y) = f(x) * f(y), \quad (\forall) x, y \in A.$$

Observaţia 2.2.1. *În multe monografii se consideră morfism de monoizi doar acele morfisme care satisfac şi condiţia $f(e_A) = e_B$, aşa numitele morfisme unitare de monoizi.*

2.3 Monoidul liber generat de o mulţime

Un exemplu remarcabil de monoid este *monoidul liber generat de o mulţime nevidă*:

Fie I o mulţime nevidă, cel mult numărabilă, numită *alfabet*. Elementele ei le numim simboluri. Numim *cuvânt de lungime n în alfabetul I* imaginea ordonată a unei funcţii

$$f : \{1, 2, ..., n\} \to I, \quad \alpha = f(1)f(2)...f(n),$$

sau, altfel spus, o secvenţă finită, ordonată, de n elemente din I:

$$\alpha = a_1a_2...a_n, \quad a_i \in I, \quad i = \overline{1, n},$$

unde $n \in \mathbb{N}^*$. Am notat $a_i = f(i)$ simbolul de pe poziţia i în cuvântul α. Numim lungimea cuvântului α numărul simbolurilor sale. Dacă $\alpha = a_1a_2...a_n$, atunci notăm lungimea sa $l(\alpha) = n$.

Din definiţia cuvintelor ca funcţii, este evident că două cuvinte $\alpha = a_1a_2...a_n$ şi $\beta = b_1b_2...b_m$ sunt egale dacă $n = m$ (au aceeaşi lungime) şi $a_i = b_i$, pentru orice $i = \overline{1, n}$.

Fie $L(I)$ mulţimea tuturor cuvintelor cu simboluri din I. Facem convenţia că în $L(I)$ există şi cuvântul e care nu are niciun simbol, adică $l(e) = 0$.

Pe $L(I)$ definim operaţia de concatenare (juxtapunere / alăturare), care acţionează astfel:

$$(\forall)\alpha = a_1a_2...a_n, \quad \beta = b_1b_2...b_m, \quad \alpha\beta = a_1a_2...a_nb_1b_2...b_m.$$

Concatenarea este o lege de compoziţie pe $L(I)$, asociativă şi care admite elementul neutru e. Prin urmare $(L(I), \cdot)$ este un monoid, numit monoidul liber generat de I.

Funcţia lungime $l : L(I) \to \mathbb{N}$, unde $l(\alpha)$ este lungimea cuvântului α, este morfism unitar surjectiv de monoizi.

Fie $\alpha \in L(I)$. Notăm

$$\alpha^0 = e, \quad \alpha^2 = \alpha\alpha, \quad \alpha^n = \alpha\alpha^{n-1}, \quad (\forall)n \in \mathbb{N}.$$

Dacă $I = \{a\}$, atunci $L(I) = \{e, a, a^2, ..., a^n, ...\}$ este un monoid comutativ. Mai mult, funcţia

$$f : \mathbb{N} \to L(I), \quad f(n) = a^n, \quad (\forall)n \in \mathbb{N}$$

, este bijectivă, fiind inversa funcţiei lungime definită pe acest monoid.

Dacă $|I| \geq 2$, atunci $(L(I), \cdot)$ este monoid necomutativ. Într-adevăr, dacă există două simboluri diferite $a \neq b$ în I, atunci cuvintele ab şi ba sunt diferite.

Deoarece egalitatea a două cuvinte revine la identificarea simbolurilor, putem afirma că monoidul liber generat de o mulţime este un monoid cu simplificare la stânga, adică

$$\alpha\beta = \alpha\gamma \Leftrightarrow \beta = \gamma.$$

Cuvântul α se numeşte *prefix* al cuvântului $\alpha\beta$. Regula de mai sus spune că dacă două cuvinte au acelaşi prefix, atunci sunt egale dacă stergând prefixul de la ambele, cuvintele rămase sunt egale.

Următoarele afirmaţii reprezintă aşa-numitele *Proprietăţi aritmetice ale monoidului liber generat de o mulţime*:

Propoziţia 2.3.1. *Fie I o mulţime nevidă şi $(L(I), \cdot)$ monoidul liber generat de I. Dacă pentru cuvintele $p, q \in L(I)$ există un număr natural nenul n astfel încât $p^n = q^n$, atunci $p = q$.*

Demonstraţie: Pentru $n = 1$ este evident. Pentru $n \geq 2$, din egalitatea $l(p^n) = l(q^n)$ rezultă $l(p) = l(q)$. Fie $p = a_1a_2..a_k$ şi $q = b_1b_2...b_k$. Egalitatea din ipoteză se scrie

$$a_1a_2..a_kp^{n-1} = b_1b_2...b_kq^{n-1}.$$

Identificând simbolurile, rezultă $a_i = b_i$, $(\forall)i = \overline{1,k}$, deci $p = q$. □

Propoziţia 2.3.2. *Fie p şi q două cuvinte peste alfabetul I, cu proprietarea $pq = qp$. Atunci există $r \in L(I)$ şi $n, m \in \mathbb{N}$ astfel încât $p = r^n$, $q = r^m$.*

Demonstraţie: Vom face demonstraţia prin inducţie matematică, după lungimea cuvântului pq.

Dacă $l(pq) = 0$, atunci $p = e$ şi $q = e$, iar concluzia este adevărată.

Presupunem că pentru orice cuvinte p, q cu $l(pq) < n$ şi $pq = qp$, există un cuvânt astfel încât p şi q sunt puteri ale sale.

Fie acum cuvintele p, q cu $l(pq) = n$ şi $pq = qp$. Fără a restrânge generalitatea, putem presupune $l(p) < l(q)$. Egalitatea $pq = qp$ spune că p este prefix al lui q, deci există $p_1 \in L(I)$ astfel încât $q = pp_1$. Simplificând la dreapta cu p relaţia $ppp_1 = pp_1p$, obţinem $pp_1 = p_1p$. Mai mult, are loc şi $l(pp_1) < n$. Aplicând ipoteza de inducţie, rezultă că există $r \in L(I)$ şi numerele naturale m, n astfel încât $p = r^n$, $p_1 = r^m$. Rezultă $q = r^{n+m}$. □

Propoziţia 2.3.3. *Dacă p, q, r sunt cuvinte peste alfabetul I pentru care există un număr natural nenul k astfel încât $pq^k = r^k p$, atunci pentru orice număr natural n are loc egalitatea $pq^n = r^n p$.*

Demonstraţie: Pentru $n = 0$, este adevărat.

Dacă demonstrăm pentru $n = 1$, adică $pq = rp$, atunci prin inducţie matematică se demonstrează pentru orice n. Într-adevăr, presupunând că $pq^i = r^i p$, concatenăm la dreapta cu q, deci $pq^{i+1} = r^i pq$, iar din $pq = rp$ rezultă $pq^{i+1} = r^i rp$, adică $pq^{i+1} = r^{i+1} p$. Conform principiului inducţiei matematice $pq^n = r^n p$ pentru orice număr natural n.

A rămas să demonstrăm $pq = rp$. Din ipoteză, există $k \in \mathbb{N}^*$ astfel încât $pq^k = r^k p$. Dacă $k = 1$, atunci am terminat. Dacă $k \geq 2$, atunci, prin inducţie matematică rezultă $pq^{km} = r^{km} p$, pentru orice $m \in \mathbb{N}^*$.

Egalitatea cuvintelor $pq^k = r^k p$ conduce la faptul că au aceeaşi lungime şi aceleaşi simboluri, în aceeaşi ordine. Primul fapt $l(pq^k) = l(r^k p)$ implică $l(p) + kl(q) = kl(r) + l(p)$, deci cuvintele q şi r au aceeaşi lungime. Pentru a folosi identitatea simbolurilor, vom compara lungimea lui p cu lungimea lui r^k.

Dacă $l(p) \leq l(r^k)$, atunci p este prefix de lungime $l(p)$ al cuvântului r^k.

Dacă $l(p) < l(r^k)$, atunci există un număr natural m pentru care $l(p) < l(r^{mk})$. Îl alegem pe cel mai mic m cu această proprietate. Mai exact, acest număr este $\left[\frac{l(p)}{kl(r)}\right] + 1$. Considerăm egalitatea $pq^{km} = r^{km} p$, de unde rezultă că p este prefix al cuvântului r^{mk}, adică este de forma $p = r^s r_1$, unde am scris $r = r_1 r_2$ pentru a exprima acel prefix al cuvântului r care intră în componenţa lui p, după eventuale s expresii întregi ale lui r. Avem $s = \left[\frac{l(p)}{l(r)}\right]$, iar r_1 este prefixul de lungime $l(p) - sl(r)$ al lui r.

Revenind în egalitatea $pq^{km} = r^{km} p$ cu forma $p = r^s r_1$, obţinem succesiv

$$r^s r_1 q^{km} = r^{mk+s} r_1 \Rightarrow r_1 q^{km} = r^{km} r_1 \Rightarrow r_1 q^{km} = r_1 r_2 r^{km-1} r_1 \Rightarrow$$

$$q^{km} = r_2 (r_1 r_2)^{km-1} r_1 \Rightarrow q^{km} = (r_2 r_1)^{km}.$$

Folosind Propoziţia 2.3.1, rezultă $q = r_2 r_1$.

Calculăm $pq = r^s r_1 r_2 r_1 = r^{s+1} r_1$ şi $rp = r r^s r_1 = r^{s+1} r_1$, de unde obţinem $pq = rp$, ceea ce trebuia demonstrat. □

Exemplul 2.3.1. *Fie I un alfabet şi $p, q, r \in L(I)$ astfel încât $pq^2 = r^2 p$, $l(p) = 8$, $l(r) = 3$. Atunci $pq = rp$.*

Conform ultimei proprietăţi aritmetice demonstrate, are loc $pq^n = r^n p$, pentru orice n natural.

Dorim totuşi să reluăm raţionamentul din demonstraţia anterioară, pentru o mai bună înţelegere a acesteia.

Într-adevăr, din egalitatea de cuvinte de mai sus rezultă mai întâi că $l(pq^2) = l(r^2p)$*, deci* $l(q) = l(r)$*, apoi, prin inducţie matematică,* $pq^{2m} = r^{2m}p$*, pentru orice număr natural* m*.*

Evaluăm apoi egalitatea $pq^2 = r^2p$ *din punct de vedere al lungimilor:* $l(p) = 8$ *este mai mic decât* $l(r^2) = 6$*. Considerăm egalitatea* $pq^4 = r^4p$*, de unde, din* $l(p) < l(r^4)$*, rezultă că* p *este un prefix de lungime* 8 *al cuvântului* r^4*. Adică* p *este format din primele* 8 *simboluri din cele* 12 *ale lui* r^4*. Deoarece* $l(r) = 3$ *putem scrie* $r = a_1a_2a_3$ *şi obţinem* $p = r^2a_1a_2$*.*

Înlocuind expresia obţinută pentru p *în relaţia* $pq^4 = rp$ *putem calcula:*

$$r^2a_1a_2q^4 = r^4r^2a_1a_2 \Rightarrow a_1a_2q^4 = (a_1a_2a_3)^4a_1a_2 \Rightarrow a_1a_2q^4 = a_1a_2a_3(a_1a_2a_3)^3a_1a_2,$$

care implică $q^4 = (a_3a_1a_2)^4$*, deci, conform Propoziţiei 2.3.1,* $q = a_3a_1a_2$*. Am obţinut astfel*

$$pq = r^2a_1a_2a_3a_1a_2 = r^3a_1a_2 = rp.$$

Remarcăm că scrierea $r = r_1r_2$ *din demonstraţia Propoziţiei anterioare corespunde în exemplul acesta cu* $r_1 = a_1a_2$*,* $r_2 = a_3$*.*

2.4 Grupuri. Morfisme de grupuri

Definiţia 2.4.1. *Un monoid* $(G, \cdot)$ *în care orice element este simetrizabil se numeşte* ***grup****. Dacă legea* $\cdot$ *este comutativă, atunci grupul se numeşte* ***comutativ*** *sau* ***abelian****.*

Din definiţie rezultă că pentru un grup $(G, \cdot)$, $U(G) = G$.

Ţinând cont de Propoziţia 2.2.2 a), avem:

Propoziţia 2.4.1. *Dacă* $(A, \cdot)$ *este monoid, atunci* $(U(A), \cdot)$ *este grup.*

Exemplul 2.4.1. *Din Exemplul 2.2.2 c) şi Propoziţia anterioară rezultă că mulţimea permutărilor unei mulţimi* A *nevide este grup în raport cu compunerea funcţiilor.*

Grupul $(S(A), \circ)$ *se numeşte grupul permutărilor mulţimii* A*.*

Exemplul 2.4.2. *a)* $(\mathbb{Z}, +)$*,* $(\mathbb{Q}, +)$*,* $(\mathbb{R}, +)$*,* $(\mathbb{Q}^*, \cdot)$*,* $(\mathbb{R}^*, \cdot)$*, sunt grupuri abeliene.*

b) Fie două grupuri $(G,+)$ *şi* $(G',*)$*. Produsul cartezian* $G\times G'$ *este grup în raport cu operaţia*

$$(x,x')\circ(y,y')=(x+y,x'*y'),$$

numit produsul direct al grupurilor G *şi* G'*.*

c) Pe mulţimea claselor de resturi modulo n*,* $\mathbb{Z}_n$*, introdusă în Exemplul1.3.4, se definesc două legi de compoziţie:*

$$+:\mathbb{Z}_n\times\mathbb{Z}_n\to\mathbb{Z}_n,\quad \hat{k}+\hat{l}=\widehat{k+l},$$

$$\cdot:\mathbb{Z}_n\times\mathbb{Z}_n\to\mathbb{Z}_n,\quad \hat{k}\cdot\hat{l}=\widehat{k\cdot l},$$

$(\forall)\hat{k},\hat{l}\in\mathbb{Z}_n$*, numite adunarea, respectiv înmulţirea claselor de echivalenţă modulo* n*. În raport cu prima operaţie* $\mathbb{Z}_n$ *este grup abelian de ordin* n *cu elementul neutru* $\hat{0}$*, opusul unei clase* $\hat{k}$ *fiind* $\widehat{n-k}$*. În raport cu înmulţirea,* $\mathbb{Z}_n$ *este monoid comutativ cu elementul neutru* $\hat{1}$*. Elementele inversabile în monoidul claselor de resturi modulo* n*,* $(\mathbb{Z}_n,\cdot)$*, sunt* $\hat{x}\in\mathbb{Z}_n$*, cu* $(x,n)=1$*. În situaţia particulară* n *număr prim,* $\mathbb{Z}_n^*=\mathbb{Z}_n-\{\hat{0}\}$ *este grup.*

Într-un grup $(G,\cdot)$ au loc următoarele reguli de calcul, în plus faţă de cele din Propoziţia 2.2.2.

Propoziţia 2.4.2. *Fie* $(G,\cdot)$ *grup şi* $a,b\in G$*. Ecuaţiile*

$$a\cdot x=b,\quad x\cdot a=b, \tag{2.4.1}$$

au soluţie unică, $x_1=a^{-1}\cdot b$*, respectv* $x_2=b\cdot a^{-1}$*. Mai mult, un semigrup în care pentru orice elemente* a,b *ecuaţiile* (2.4.1) *au soluţii unice, este grup.*

Demonstraţie: Într-adevăr, x_1 verifică prima ecuaţie. Orice altă soluţie x a ecuaţiei se poate determina prin compunerea egalităţii $a\cdot x=b$ cu a^{-1}, la stânga. Rezultă $x=x_1$. Analog pentru a doua ecuaţie.

Fie acum semigrupul $(G,\cdot)$ cu proprietatea că $(\forall)a,b\in G$, ecuaţiile $a\cdot x=b$ şi $x\cdot a=b$ au câte o soluţie în G, unică. Fie a un element fixat arbitrar din G şi e_a unica soluţie a ecuaţiei $a\cdot x=a$. Folosind asociativitatea operaţiei '$\cdot$', au loc egalităţile $a\cdot e_a\cdot a=a^2$ şi $a\cdot a=a^2$, iar din unicitatea soluţiei ecuaţiei $a\cdot x=a^2$, rezultă $e_a\cdot a=a$. Apoi, ecuaţia $a\cdot x=a\cdot b$ are soluţiile b şi $e_a\cdot b$, iar ecuaţia $x\cdot a=b\cdot a$ are soluţiile $b\cdot e_a$ ş b. Unicitatea soluţiei conduce la $b\cdot e_a=e_a\cdot b=b$, $(\forall)b\in G$, deci e_a este element neutru în semigrupul $(G,\cdot)$. Vom nota simplu e acest element. Pentru orice element $a\in G$, fie $a'\in G$ unica soluţie a ecuaţiei

$a \cdot x = e$. Cu alte cuvinte, a' este simetricul la dreapta al elementului a. Au loc'şi egaităţile $a \cdot a' \cdot a = a$, $a \cdot e = a$, iar din unicitatea soluţiei ecuaţiei $a \cdot x = a$ obţinem $a' \cdot a = e$, adică elementul a' este şi simetric la stânga pentru a. Rezultă că orice element din G este simetrizabil în monoidul $(G, \cdot)$, deci $(G, \cdot)$ este grup. □

Definiţia 2.4.2. *Fie $(G, \cdot)$, $(G', *)$ grupuri. Funcţia $f : G \to G'$ se numeşte* ***morfism de grupuri*** *dacă verifică*

$$f(x \cdot y) = f(x) * f(y), \quad (\forall)x, , y \in G.$$

Observaţia 2.4.1. *Deoarece orice grup este monoid, putem spune că funcţia f din Definiţia de mai sus este morfism de grupuri dacă este morfism de monoizi. De multe ori, când vorbim despre morfisme de monoizi/grupuri, se foloseşte notaţia*

$$f : (G, \cdot) \to (G', *).$$

Propoziţia 2.4.3. *Dacă $f : (A, \cdot) \to (B, *)$ este un morfism de grupuri, atunci au loc relaţiile:*

a) $f(e_A) = e_B$;

b) $f(x^{-1}) = (f(x))^{-1}$, $(\forall)x \in A$;

c) $f(x^k) = (f(x))^k$, $(\forall)x \in A$, $(\forall)k \in \mathbb{Z}$, unde

$$x^k = \begin{cases} \underbrace{x \cdot x \cdot ... \cdot x}_{k}, & k > 0 \\ e, & k = 0 \\ \underbrace{x^{-1} \cdot x^{-1} \cdot ... \cdot x^{-1}}_{-k}, & k < 0, \end{cases}$$

Demonstraţie: a) Funcţia f fiind morfism de grupuri, are loc

$$f(x \cdot y) = f(x) * f(y), \quad (\forall)x, y \in A.$$

Scriiind relaţia anterioară pentru $x = y = e_A$, obţinem în grupul B ecuaţia $f(e_A) * f(e_A) = f(e_A)$. Din Propoziţia 2.4.2 rezultă că singura soluţie a ecuaţiei $f(e_A) * y = f(e_A)$ este $f(e_A) = e_B$.

b) Fie $x \in A$. Conform punctului anterior, $e_B = f(e_A) = f(x \cdot x^{-1})$, deci $f(x) * f(x^{-1}) = e_B$. În grupul $(B, *)$ ecuaţia $f(x) * y = e_B$ are soluţia unică $f(x^{-1}) = (f(x))^{-1}$.

c) Se arată prin inducţie matematică pentru orice $n \in \mathbb{N}$, apoi se foloseşte punctul b). □

Exemplul 2.4.3. *a) Pentru orice grup, funcţia identică este morfism de grupuri.*

b) Pentru $I = \{a\}$, funcţia $f : \mathbb{N} \to L(I)$, $f(n) = a^n$, $(\forall)n \in \mathbb{N}$, este morfism de monoizi: $(\mathbb{N}, +)$, $(L(I), \cdot)$, unde ultimul este monoidul liber generat de mulţimea I.

c) Oricare ar fi grupul $(G, \cdot)$, funcţia $f : \mathbb{Z} \to G$, definită prin $f(k) = x^k$, $(\forall)k \in \mathbb{Z}$, este morfism între grupurile $(\mathbb{Z}, +)$, $(G, \cdot)$ (verificaţi!).

Propoziţia 2.4.4. *Prin compunerea a două morfisme de grupuri(monoizi) obţinem un morfism de grupuri (monoizi).*

Demonstraţie: Fie $f : (G, \cdot) \to (G', *)$ şi $g : (G', *) \to (G", \bullet)$ morfisme de grupuri. Fie $x, y \in G$, arbitrar alese.

$$(g \circ f)(x \cdot y) = g(f(x \cdot y)) = g(f(x) * f(y)) = g(f(x)) \bullet g(f(y)) =$$

$$= (g \circ f)(x) \bullet (g \circ f)(y).$$

□

Definiţia 2.4.3. *Un morfism $f : (G, \cdot) \to (G, \cdot)$ se numeşte **endomorfism** al grupului $(G, \cdot)$. Mulţimea endomorfismelor grupului G se notează $End(G)$.*

Observaţia 2.4.2. *Propoziţia 2.4.4, asociativitatea compunerii funcţiilor şi existenţa morfismului identitate arată că $(End(G), \circ)$ este monoid.*

Definiţia 2.4.4. *Un morfism de grupuri (monoizi) $f : (G, \cdot) \to (G', *)$ se numeşte **izomorfism** dacă există un morfism de grupuri $g : (G', *) \to (G, \cdot)$ astfel încât $g \circ f = \mathbf{1_G}$ şi $f \circ g = \mathbf{1_{G'}}$. Un izomorfism $f : (G, \cdot) \to (G, \cdot)$ se numeşte **automorfism** al grupului $(G, \cdot)$.*

Propoziţia 2.4.5. *Orice morfism bijectiv de grupuri (monoizi) este izomorfism şi reciproc.*

Demonstraţie: Fie $f : (G, \cdot) \to (G', *)$ un morfism bijectiv de grupuri. Fiind o funcţie bijectivă, rezultă că există inversa funcţiei f, funcţia $f^{-1} : G' \to G$, astfel încât $f \circ f^{-1} = \mathbf{1}_{G'}$, $f^{-1} \circ f = \mathbf{1}_G$. Rămâne să arătăm că f^{-1} este morfism de grupuri.

Fie $y_1, y_2 \in G'$, arbitrar aleşi. Din surjectivitatea lui f, există $x_1, x_2 \in G$ astfel încât $y_1 = f(x_1)$ şi $y_2 = f(x_2)$.

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

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

deci f^{-1} este morfism de grupuri. Rezultă că f este izomorfism de grupuri.

Implicaţia inversă rezultă dintr-un raţionament analog. □

Notăm cu $Aut(G)$ mulţimea automorfismelor grupului G. Din $Aut(G)$=$U(End(G))$, conform Propoziţiei 2.4.1, are loc:

Propoziţia 2.4.6. *Mulţimea automorfismelor unui grup este grup în raport cu compunerea funcţiilor.*

Exemplul 2.4.4. *Unul din cele mai simple exemple de grupuri este grupul aditiv al numerelor întregi, $(\mathbb{Z}, +)$. Vom determina endomorfismele, apoi automorfismele acestui grup. Un endomorfism $f : \mathbb{Z} \to \mathbb{Z}$ este unic determinat de $f(1) = a \in \mathbb{Z}$, deoarece din condiţia de morfism, $f(x + y) = f(x) + f(y)$, $(\forall)x, y \in \mathbb{Z}$, rezultă imediat prin inducţie $f(n) = n \cdot a$, $\forall n \in \mathbb{N}$. Proprietatea b) din Propoziţia 2.4.3, care în cazul grupurior aditive devine $f(-x) = -f(x)$, $(\forall)x \in \mathbb{Z}$, conduce la $f(k) = a \cdot k$, $(\forall)k \in \mathbb{Z}$.*

Deci $End(Z) = \{f_a : \mathbb{Z} \to \mathbb{Z} | \quad a \in \mathbb{Z}\}$. Oricare endomorfism f_a, $a \neq 0$ este injectiv. Condiţia de surjectivitate conduce la $k \cdot a = 1$, deci există doar două automorfisme: f_{-1}, f_1.

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

Definiţia 2.4.5. *Preimaginea elementului neutru $e_{G'}$ prin morfismul f se numeşte **nucleul** morfismului f şi se notează $Ker(f)$.*

Din definiţia anterioară rezultă

$$Ker(f) = \{x \in G | \quad f(x) = e_{G'}\},$$

deci nucleul morfismului f conţine toate elementele domeniului G care prin morfismul f sunt asociate elementului neutru din G'. Mai mult, Propoziţia 2.4.3 ne asigură că $e_G \in Ker(f)$, deci nucleul unui morfism este nevid.

Propoziţia 2.4.7. *Următoarele afirmaţii sunt echivalente:*

a) Morfismul de grupuri $f : (G, \cdot) \to (G', *)$ este injectiv.

b) Nucleul morfismului f conţine doar elementul neutru din G, adică

$$Ker(f) = \{e_G\}.$$

Demonstraţie: "a)⇒ b)": Fie $x \in Ker(f)$, arbitrar ales. Rezultă

$$f(x) = e_{G'} = f(e_G),$$

ultima egalitate fiind conform a) din Propoziţia 2.4.3. Dar f este funcţie injectivă, deci $x = e_G$, de unde $Ker(f) = \{e_G\}$.

"b)⇒ a)": Fie $x, y \in G$ astfel încât $f(x) = f(y)$. Egalitatea aceasta poate fi prelucrată în grupul G' astfel:

$$f(x) * (f(y))^{-1} = e_{G'} \Rightarrow f(x) * f(y^{-1}) = e_{G'} \Rightarrow f(x \cdot y^{-1}) = e_{G'}$$

$$\Rightarrow x \cdot y^{-1} \in Ker(f) = \{e_G\} \Rightarrow x \cdot y^{-1} = e_G \Rightarrow x = y,$$

ţinând cont de proprietăţile morfismelor de grupuri. Rezultă f injectiv. □

Propoziţia 2.4.8. *Fie $f : (G, \cdot) \to (G', *)$ un morfism de grupuri. Pentru un $y \in G'$, mulţimea soluţiilor ecuaţiei $f(x) = y$ este vidă dacă $y \notin Im(f)$ şi este cardinal echivalentă cu $Ker(f)$, dacă $y \in Im(f)$.*

Demonstraţie: Dacă $y \notin Im(f)$, atunci oricare ar fi $x \in G$, $f(x) \neq y$. Mulţimea soluţiilor este vidă.

Dacă $y \in Im(f)$, atunci există $x_0 \in G$, astfel încât $y = f(x_0)$. Pentru orice $x \in Ker(f)$, are loc egalitatea

$$f(x_0 \cdot x) = f(x_0) * f(x) = y * e_{G'} = y,$$

adică $x_o \cdot x$ este de asemenea soluţie. Cum într-un grup $x_0 \cdot x_1 \neq x_0 \cdot x_2$ dacă $x_1 \neq x_2$, obţinem că numărul soluţiilor este mai mare sau egal cu cardinalul nucleului.

Fie acum x o soluţie diferită de x_0 a ecuaţiei date. Din $f(x) = f(x_0)$, rezultă că $f(x_0 \cdot x^{-1}) = e_{G'}$, deci $x_0 \cdot x^{-1} \in Ker(f)$. Prin urmare numărul soluţiilor este mai mic sau egal cu cardinalul nucleului.

Rezultă în final cardinalul mulţimii soluţiilor egal cu $|Ker(f)|$. □

Notăm cu $Hom(G, G')$ mulţimea tuturor morfismelor de la grupul G la grupul G'.

Propoziţia 2.4.9. *Fie $(G_1, \cdot)$, $(G_2, \cdot)$, grupuri, $(G_1 \times G_2, \cdot)$ grupul produs direct al lor şi $(G, \cdot)$ un grup abelian. Are loc egalitatea*

$$Hom(G_1 \times G_2, G) = Hom(G_1, G) \times Hom(G_2, G).$$

Demonstraţie: Fie $f : G_1 \times G_2 \to G$ un morfism de grupuri.

Definim $f_1 : G_1 \to G$ şi $f_2 : G_2 \to G$ prin $f_1(x_1) = f(x_1, e_2)$, $f_2(x_2) = f(e_1, x_2)$ pentru orice $x_1 \in G_1$, respectiv $x_2 \in G_2$ unde am notat cu e_1, e_2, elementele neutre în grupurile G_1, respectiv G_2. Avem:

$$f_1(x_1 \cdot y_1) = f(x_1 \cdot y_1, e_2) = f((x_1, e_2) \cdot (y_1, e_2)) = f((x_1, e_2)) \cdot f((y_1, e_2)) = f_1(x_1) \cdot f_1(y_1),$$

$$f_2(x_2 \cdot y_2) = f(e_1, x_2 \cdot y_2) = f((e_1, x_2) \cdot (e_1, y_2)) = f((e_1, x_2)) \cdot f((e_1, y_2)) = f_2(x_2) \cdot f_2(y_2),$$

pentru orice $x_1, y_1 \in G_1$, $x_2, y_2 \in G_2$, unde am folosit definiţia operaţiei din grupul produs direct (vezi Exemplul 2.4.2 b)) şi faptul că f este morfism de grupuri. Putem spune că fiecărui morfism $f \in Hom(G_1 \times G_2, G)$ îi corespunde o pereche de morfisme $(f_1, f_2) \in Hom(G_1, G) \times Hom(G_2, G)$.

Reciproc, pentru orice două morfisme de grupuri $f_1 : G_1 \to G$ şi $f_2 : G_2 \to G$, putem defini $f : G_1 \times G_2 \to G$ prin

$$f(x_1, x_2) = f_1(x_1) \cdot f_2(x_2) \quad (\forall)(x_1, x_2) \in G_1 \times G_2.$$

Se verifică faptul că f este morfism folosind comutativitatea în G. □

Fie $(G, \cdot)$ un grup.

Definiţia 2.4.6. *Cardinalul mulţimii G se numeşte **ordinul** grupului.*

Dacă grupul este finit, atunci legea de compoziţie se poate prezenta prin tabla operaţiei. Cele mai simple exemple de grupuri finite sunt grupurile aditive ale claselor de resturi modulo n, $(\forall) n \in \mathbb{N}^* - \{1\}$.

Exemplul 2.4.5. *Exemplificăm tabla operaţiei de adunare pentru $(\mathbb{Z}_n, +)$, unde $n = 2$ şi $n = 3$:*

$+$	$\hat{0}$	$\hat{1}$
$\hat{0}$	$\hat{0}$	$\hat{1}$
$\hat{1}$	$\hat{1}$	$\hat{0}$

$+$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{0}$	$\hat{1}$

Se verifică cu uşurinţă faptul că relaţia de "a fi izomorfe" pe mulţimea grupurilor este o relaţie de echivalenţă. Clasa de echivalenţă a unui grup în raport cu această relaţie se numeşte *tipul* grupului respectiv.

Exemplul 2.4.6. *Există un singur tip de grup cu 2 elemente, sau, echivalent, orice grup cu două elemente este izomorf cu* $(\mathbb{Z}_2, +)$.

Într-adevăr, fie $(G, \cdot)$ *un grup cu 2 elemente. Notăm elementele sale* e *şi* a*, unde* e *este elementul neutru şi întocmim tabla operaţiei "*$\cdot$*". Linia şi coloana elementului* e *se completează din proprietatea elemenutului neutru si rămâne de precizat* $a \cdot a$*. Legea "*$\cdot$*" fiind lege de compoziţie internă,* $a \cdot a \in G$*, deci* $a \cdot a = e$ *sau* $a \cdot a = a$*. Dar într-un grup ecuaţia* $x \cdot a = a$ *are soluţie unică, iar din a doua variantă am obţine* $a = e$*, ceea ce contrazice* $|G| = 2$*. Rezultă deci* $a \cdot a = e$*, adică tabla este unică:*

$$\begin{array}{c|cc} \cdot & e & a \\ \hline e & e & a \\ a & a & e \end{array},$$

şi este identică cu tabla grupului $(\mathbb{Z}_2, +)$*, prin corespondenţa*

$$f : \mathbb{Z}_2 \to G, \quad f(\hat{0}) = e, \quad f(\hat{1}) = a.$$

Deci cele două grupuri sunt izomorfe. Dar grupul G *a fost ales arbitrar, de unde rezultă că orice grup de ordin 2 e izomorf cu* $(\mathbb{Z}_2, +)$.

Se va demonstra ca există un singur tip de grup cu număr prim de elemente, două tipuri de grupuri de ordin 4, etc. Dat fiind un grup, determinarea tipului său este una din cele mai importante probleme ale teoriei grupurilor.

Încheiem secţiunea cu o problemă de numărare:

Propoziţia 2.4.10. *Numărul morfismelor de grupuri de la* $(\mathbb{Z}_n, +)$ *la* $(\mathbb{Z}_m, +)$ *este* $d = (n, m)$*, cel mai mare divizor comun al numerelor* m *şi* n.

Demonstraţie: Fie $f : (\mathbb{Z}_n, +) \to (\mathbb{Z}_m, +)$ un morfism de grupuri. Avem $f(\hat{0}) = [0]$, unde am notat $\hat{x}$, $[x]$ clasa de echvalenţă a elementului x în $\mathbb{Z}_n$, respectiv în $\mathbb{Z}_m$. Fie $f(\hat{1}) = [a]$, cu $a \in \{0, 1, ..., m-1\}$. Este clar că alegerea lui a determină toate valorile morfismului f prin

$$f(\hat{k}) = f(\underbrace{\hat{1} + \hat{1} + ... + \hat{1}}_{k}) = \underbrace{[a] + ... + [a]}_{k} = [a \cdot k],$$

pentru orice $k \in \{0, 1, .., n-1\}$. Prin urmare numărul morfismelor este egal cu numărul alegerilor posibile pentru a. Morfismul f trebuie să fie corect definit, adică $f(\hat{n}) = f(\hat{0})$, deci $m|n \cdot a$. Fie $d = (m, n)$ şi $k \in \mathbb{Z}$ astfel încât $m \cdot k = n \cdot a$. Avem

$$m = d \cdot m_1, \quad n = d \cdot n_1, \quad (m_1, n_1) = 1,$$

$$m_1 \cdot k = n_1 \cdot a, \quad (m_1, n_1) = 1 \Rightarrow m_1|a \Rightarrow (\exists) a_1 \in \mathbb{Z}, \quad a = m_1 \cdot a_1.$$

Dar

$$0 \leq a < m \Rightarrow 0 \leq a_1 \cdot m_1 < d \cdot m_1 \Rightarrow 0 \leq a_1 < d,$$

deci există d valori posibile pentru a. Mulţimea morfismelor cerute este $Hom(\mathbb{Z}_n, \mathbb{Z}_m)$, deci am obţinut

$$|Hom(\mathbb{Z}_n, \mathbb{Z}_m)| = (m, n).$$

□

Exerciţiu: Determinaţi pentru ce valori $a \in \{0, 1, 2, 3, ..., 14\}$, funcţia

$$f : \mathbb{Z}_{12} \to \mathbb{Z}_{15},$$

este corect definită prin $f(\hat{x}) = [a \cdot x]$, $\hat{x} \in \mathbb{Z}_{12}$, unde am notat $[x]$ clasa de resturi modulo 15 a numărului întreg x, iar cu $\hat{x}$ clasa de resturi modulo 12 a lui x. Pentru oricare dintre valorile determinate, arătaţ că f este morfism de grupuri, $(\mathbb{Z}_{12}, +)$, $(\mathbb{Z}_{15}, +)$. Determinaţi nucleul şi imaginea morfismului f pentru $a = 5$. Câte soluţii are ecuaţia $f(x) = [10]$?

Rezolvare: Condiţia pentru ca f să fie corect definită este să respecte definiţia funcţiei, adică fiecărui element din domeniu să îi corespundă un element şi numai unul în codomeniu. Ne punem această problemă aici, deoarece elementele domeniului sunt clase de echivalenţă, care pot fi exprimate prin diferiţi reprezentanţi. De exemplu, clasa de echivalenţă $\hat{4} \in \mathbb{Z}_{12}$ poate fi exprimată şi prin numerele întregi 16 sau 28, deoarece diferenţa lor este multiplu de 12. Mai exact, $\hat{x} = \hat{y}$ în $\mathbb{Z}_{12}$ dacă şi numai dacă $x - y$ este multiplu de 12. Pentru ca f să fie funcţie, trebuie ca, pentru orice $\hat{x} = \hat{y}$ în $\mathbb{Z}_{12}$, să aibă loc şi $f(\hat{x}) = f(\hat{y})$, adică $[ax] = [ay]$ în $\mathbb{Z}_{15}$. Condiţia este deci $15|a \cdot (x - y)$, pentru orice $x - y = 12k$, $k \in \mathbb{Z}$. Se impune a divizibil cu 5, deci $a \in \{0, 5, 10\}$.

Pentru oricare $a \in \{0, 5, 10\}$, are loc

$$f(\hat{x} + \hat{y}) = f(x \hat{+} y) = [a \cdot (x + y)] = [a \cdot x + a \cdot y] = [a \cdot x] + [a \cdot y] = f(\hat{x}) + f(\hat{y}),$$

orcare ar fi $\hat{x}, \hat{y} \in \mathbb{Z}_{12}$, deci f este morfism de grupuri. Deci pentru toate cele 3 valori ale lui a, f este morfism de grupuri. Se confirmă rezultatul Propoziţiei 2.4.10, că numărul morfismelor de la grupul $(\mathbb{Z}_{12}, +)$ la $(\mathbb{Z}_{15}, +)$ este $(12, 15) = 3$.

În cazul $a = 5$, legea morfismului f este $f(\hat{x}) = [5x]$, $(\forall)\hat{x} \in \mathbb{Z}_{12}$. Nucleul acestui morfism este

$$\begin{aligned} Ker(f) &= \{\hat{x} \in \mathbb{Z}_{12} | \quad f(\hat{x}) = [0]\} = \\ &= \{\hat{x} \in \mathbb{Z}_{12} | \quad [5 \cdot x] = [0]\} = \\ &= \{\hat{x} \in \mathbb{Z}_{12} | \quad 15 \quad | \quad 5 \cdot x\} = \\ &= \{\hat{0}, \hat{3}, \hat{6}, \hat{9}\}, \end{aligned}$$

iar imaginea sa este

$$Im(f) = \{[y] \in \mathbb{Z}_{15} | \quad (\exists)\hat{x} \in \mathbb{Z}_{12}, [y] = f(\hat{x})\}.$$

Ţinând cont că $f(\hat{x}) = [0]$ pentru orice x multiplu de 3, rezultă $f(\hat{x}) = [5]$ pentru $x = 3k + 1$ şi $f(\hat{x}) = [10]$ pentru $x = 3k + 2$. Obţinem $Im(f) = \{[0], [5], [10]\}$.

Pentru ultima cerinţă, deoarece $[10] \in Im(f)$, putem spune că mulţimea soluţiilor ecuaţiei nu este vidă. Folosind Propoziţia 2.4.8, răspunsul este "ecuaţia are 4 soluţii".

Fără a utiliza rezultatul teoretic folosit anterior, am putea observa, din studiul imaginii morfismului f, că valoarea [10] se obţine pentru argumentele $\hat{x} \in \mathbb{Z}_{12}$ de forma $x = 3k + 2$, adică mulţimea soluţiilor este $\{\hat{2}, \hat{5}, \hat{8}, \hat{11}\}$.

2.5 Exemple remarcabile de grupuri

2.5.1 Grupuri de permutări

Fie M şi N două mulţimi şi $(S(M), \circ)$, $(S(N), \circ)$ grupurile lor de permutări introduse în Exemplul 2.4.1.

Propoziţia 2.5.1. *Dacă M şi N sunt echipotente, atunci grupurile $(S(M), \circ)$ şi $(S(N), \circ)$ sunt izomorfe.*

Demonstraţie: Din definiţia grupului de permutări a unei mulţimi, $S(M) = \{f : M \to M | \quad f$ bijectivă$\}$,

$S(N) = \{h : N \to N | \quad h$ bijectivă$\}$.

Din ipoteza M, N echipotente, există o bijecţie $\varphi : M \to N$. Definim funcţia

$$\gamma : S(M) \to S(N), \quad \gamma(f) = \varphi \circ f \circ \varphi^{-1}, \quad (\forall) f \in S(M),$$

unde φ^{-1} este inversa bijecţiei φ. Deoarece compunerea funcţiilor bijective este tot o funcţie bijectivă, γ este corect definită. Vom demonstra că γ este morfism bijectiv de grupuri:

$$\gamma(f_1 \circ f_2) = \varphi \circ (f_1 \circ f_2) \circ \varphi^{-1} = \varphi \circ f_1 \circ (\varphi^{-1} \circ \varphi) \circ f_2 \circ \varphi^{-1} =$$

$$= (\varphi \circ f_1 \circ \varphi^{-1}) \circ (\varphi \circ f_2 \circ \varphi^{-1}) = \gamma(f_1) \circ \gamma(f_2),$$

$(\forall) f_1, f_2 \in S(M)$, deci γ este morfism de la grupul $(S(M), \circ)$ la grupul $(S(N), \circ)$.

Fie acum $f \in Ker(\gamma)$, deci $f : M \to M$ bijectivă astfel încât $\gamma(f)$ este elementul neutru în $S(N), \circ)$, adică $\gamma(f) = \mathbf{1}_N$. Din definiţia funcţiei γ rezultă $\varphi \circ f \circ \varphi^{-1} = \mathbf{1}_N$, de unde $f = \varphi^{-1} \circ \varphi = \mathbf{1}_M$. Prin urmare nucleul morfismului γ conţine doar elementul neutru din domeniul de definiţie şi, conform Propoziţiei 2.4.7, γ este injectiv.

Pentru $h \in S(N)$ arbitrar ales, există $f = \varphi^{-1} \circ h \circ \varphi \in S(M)$ care are proprietatea că $\gamma(f) = h$. Rezultă că morfismul γ este şi surjectiv, deci este un izomorfism. □

Observaţia 2.5.1. *O consecinţă imediată a Propoziţiei 2.5.1 este faptul că grupurile de permutări ale tuturor mulţimilor cu n elemente sunt izomorfe, fiind izomorfe cu S_n, grupul de permutări al mulţimii $I_n = \{1, 2, ..., n\}$. Grupul $(S_n, \circ)$ se numeşte grupul simetric S_n.*

Fie $(S_n, \circ)$ grupul introdus mai sus. Un element $\sigma \in S_n$ este o funcţie bijectivă, $\sigma : I_n \to I_n$. Această funcţie o numim permutare şi o putem reprezenta printr-un tablou

$$\begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}, \quad \sigma(i) \neq \sigma(j), \quad (\forall) i \neq j.$$

Permutarea identică corespunde funcţiei identice şi o notăm de obicei cu e. De exemplu, S_2 are elementele $e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$.

Deoarece grupul $(S_n, \circ)$ are ca elemente toate bijecţiile de la o mulţime cu n elemente la ea însăşi, rezultă:

Propoziţia 2.5.2. *Ordinul grupului simetric S_n este $n!$, $(\forall) n \geq 2$.*

Fie $\sigma \in S_n$. Numim *ciclu* o permutare $\sigma \in S_n$ cu proprietatea că există o secvenţă $(i_1, i_2, ..., i_m)$ de elemente din I_n, astfel încât $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$,...,

$\sigma(i_m) = i_1$ şi $\sigma(i) = i$, $(\forall)i \notin \{i_1, ..., i_m\}$. Numărul m se numeşte *lungimea ciclului*. Scriem $\sigma = (i_1, i_2, ..., i_m)$.

Exemplul 2.5.1. *Ciclul* $(1, 3, 2) \in S_7$ *este permutarea*

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 4 & 5 & 6 & 7 \end{pmatrix},$$

iar $(4, 5, 7, 6) \in S_7$ *este permutarea* $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 5 & 7 & 4 & 6 \end{pmatrix}$.

O permutare poate conţine mai multe cicluri.

Exemplul 2.5.2. *a) Permutarea identică din* S_n *conţine* n *cicluri de lungime* 1.

b) Permutarea $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 5 & 7 & 4 & 6 \end{pmatrix}$ *conţine două cicluri:* $(1, 3, 2)$ *şi* $(4, 5, 7, 6)$.

Observaţia 2.5.2. *Dacă* $\sigma = (i_1, i_2, ..., i_k)$ *este un ciclu din* S_n*, atunci inversul acestuia în* S_n *este tot un ciclu şi anume*

$$\sigma^{-1} = (i_k, i_{k-1}, ..., i_2, i_1).$$

Într-adevăr, din definiţia permutării, există funcţia inversă, $\sigma^{-1}(j) = i$ *pentru care* $\sigma(i) = j$*. Evident, compunând cele două permutări găsim permutarea identică.*

Fie $\sigma = (i_1, i_2, ..., i_m)$. Mulţimea $\{i_1, i_2, ..., i_m\}$ reprezintă mulţimea de definiţie a ciclului σ. Două cicluri se numesc *disjuncte* dacă mulţimile lor de definiţie sunt disjuncte.

Propoziţia 2.5.3. *Dacă* σ_1, $\sigma_2 \in S_n$ *sunt două cicluri disjuncte , atunci*

$$\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1.$$

Mai spunem că oricare două cicluri disjuncte comută.

Demonstraţie: Fie $\sigma_1 = (i_1, i_2, ..., i_n)$ şi $\sigma_2 = (j_1, j_2, ..., j_m)$ cele două cicluri. Ciclurile fiind disjuncte rezultă că $\sigma_1(i) = i$, $(\forall)i \in \{j_1, ..., j_m\}$ şi $\sigma_2(i) = i$, $(\forall)i \in \{i_1, ..., i_n\}$. Calculăm

$$\sigma_1 \circ \sigma_2(i) = \begin{cases} \sigma_1(i), & (\forall)i \notin \{j_1, ..., j_m\} \\ \sigma_1(j_{k+1}), & i = j_k, (\forall)k \in \{1, ..., m-1\} \\ \sigma_1(j_1), & i = j_m \end{cases}$$

$$= \begin{cases} i, & (\forall) i \notin \{i_1, ..., i_n, j_1, ..., j_m\} \\ i_{l+1}, & i = i_l, (\forall) l \in \{1, ..., n-1\} \\ i_1, & i = i_n, \\ j_{k+1}, & i = j_k, (\forall) k \in \{1, ..., m-1\} \\ j_1, & i = j_m \end{cases}$$

apoi

$$\sigma_2 \circ \sigma_1(i) = \begin{cases} \sigma_2(i), & (\forall) i \notin \{i_1, ..., i_n\} \\ \sigma_2(i_{l+1}), & i = i_l, (\forall) l \in \{1, ..., n-1\} \\ \sigma_2(i_1), & i = i_n \end{cases}$$

$$= \begin{cases} i, & (\forall) i \notin \{i_1, ..., i_n, j_1, ..., j_m\} \\ i_{l+1}, & i = i_l, (\forall) l \in \{1, ..., n-1\} \\ i_1, & i = i_n, \\ j_{k+1}, & i = j_k, (\forall) k \in \{1, ..., m-1\} \\ j_1, & i = j_m \end{cases}$$

Am obţinut aceeaşi lege de definiţie pentru permutările $\sigma_1 \circ \sigma_2$ şi $\sigma_2 \circ \sigma_1$, deci sunt egale. □

Propoziţia 2.5.4. *Pentru orice permutare $\sigma \in S_n$, există un număr natural k şi ciclurile $\sigma_1, \sigma_2, ..., \sigma_k \in S_n$, disjuncte două câte două astfel încât*

$$\sigma = \sigma_1 \circ \sigma_2 \circ ... \circ \sigma_k.$$

În plus, descompunerea este unică, abstracţie făcând de ordinea factorilor.

Demonstraţie: Pornind căutarea de la 1, identificăm primul ciclu din σ şi îl notăm $\sigma_1 = (i_1, ..., i_k)$. Calculăm $\sigma_1^{-1} \circ \sigma$ şi în noua permutare obţinută astfel elementul i_l este dus în el însuşi deoarece prin σ era dus în i_{l+1}, iar prin σ_1^{-1}, i_{l+1} este dus în i_l, $(\forall) l \in \{1, ..., k-1\}$. Analog pentru i_k. Deci în această nouă permutare elementele ciclului σ_1 nu mai sunt implicate în niciun alt ciclu. Identificând aici următorul ciclu σ_2, acesta va fi deci disjunct de σ_1. Cum mulţimea de definiţie a permutării σ este finită, după un număr finit de paşi obţinem descompunerea lui σ în produs de cicluri disjuncte. Datorită Propoziţiei 2.5.3, nu are importanţă ordinea în care se compun ciclurile. □

Exemplul 2.5.3. *Permutarea* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 5 & 7 & 4 & 6 \end{pmatrix}$ *se descompune* $\sigma = (132) \circ (4576)$. *De obicei se omite scrierea operaţiei de compunere, deci* $\sigma =$

$(132)(4576)$. *Permutarea* $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 1 & 5 & 6 & 4 & 8 & 7 \end{pmatrix}$ *se descompune* $\tau = (13)(2)(456)(78)$.

Compunerea permutărilor se poate face mai uşor folosind descompunerea lor în produs de cicluri disjuncte

$$\sigma \circ \tau = (132)(4576) \circ (13)(2)(456)(78),$$

astfel: prin τ *elementul* 1 *este dus în* 3*, iar prin* σ *elementul* 3 *este dus în* 2*. Scriem deci la rezultat începutul unui ciclu* $1, 2$*. Am rămas la* 2*, care prin* τ *este dus în el însuşi fiind element al unui ciclu de lungime 1. De remarcat faptul că ciclurile de lungime 1 reprezintă permutarea identică şi se pot omite la descompunere. Prin urmare absenţa unui element din scrierea unei permutări ca produs de cicluri disjuncte arată că acel element e dus în el însuşi. Continuăm calculul,* 2 *e dus prin* σ *în* 1*, deci închidem ciclul* (12)*. Continuăm cu primul element în ordine crescătoare care nu a apărut la rezultat, în cazul nostru cu* 3*. Prin* τ 3 *e dus în* 1*, care e dus în* 3 *prin* σ *. Permutarea rezultat invariază elementul* 3*, deci scriu* (3) *sau îl omit. Continuăm cu* 4*. Prin* τ *este dus în* 5*, iar acesta e dus în* 7 *prin* σ*. Scriem deci* $4, 7$*. Elementul* 7 *merge prin* τ *în* 8 *care prin* σ *merge în* 8*. Scriem după* 7 *elementul* 8 *la rezultat. Prin* τ*,* 8 *este dus în* 7*, care prin* σ *este dus în* 6*. Scriem* 6 *şi continuăm cu el.* 6 *e dus prin* τ *în* 4*, iar prin* σ 4 *este dus în* 5*. Scriem* 5 *după* 6 *la rezultat. Elementul* 5 *e dus prin* τ *în* 6 *care prin* σ *e dus în* 4*, deci ciclul se încheie. Obţinem*

$$\sigma \circ \tau = (12)(47865).$$

Analog putem calcula

$$\tau \circ \sigma = (13)(2)(456)(78) \circ (132)(4576) = (23)(46587).$$

Definiţia 2.5.1. *Un ciclu de lungime 2 se numeşte* ***transpoziţie****.*

Observaţia 2.5.3. *Orice ciclu* $(i_1 i_2 ... i_m)$ *se poate scrie ca produs (compunere) de transpoziţii:* $(i_1 i_2)(i_2 i_3)...(i_{m-1} i_m)$*, ceea ce se verifică prin calcul direct.*

Ţinând cont de Observaţia anterioară şi de Propoziţia 2.5.4, rezultă că:

Propoziţia 2.5.5. *Orice permutare se descompune în produs de transpoziţii.*

Observaţia 2.5.4. *Descompunerea in produs de transpoziţii nu este unică, iar ordinea transpoziţiilor contează. Pentru orice descompunere a unei permutări în produs de transpoziţii, numărul acestora are aceeaşi paritate.*

Exemplul 2.5.4. *a) Permutarea* $\sigma = (132)(4576)$ *se scrie ca produs de transpoziţii astfel:* $\sigma = (13)(32)(45)(57)(76)$.

b) Orice transpoziţie (ij) *se poate scrie* $(1,i)(i,j)(1,j)$.

Fie $\sigma \in S_n$. O pereche ordonată (i,j), cu $1 \leq i < j \leq n$, se numeşte *inversiune a permutării* σ dacă $\sigma(i) > \sigma(j)$. Numărul inversiunilor permutării σ se notează $inv(\sigma)$.

O permutare se numeşte *pară*, respectiv *impară* dacă are număr par, respectiv impar de inversiuni.

Numărul

$$sgn(\sigma) = (-1)^{inv(\sigma)},$$

notat şi $\epsilon(\sigma)$, se numeşte *semnul* sau *signatura* permutării σ. Evident, $sgn(\sigma) = 1$, dacă σ este permutare pară şi $sgn(\sigma) = -1$, dacă σ este permutare impară.

Propoziţia 2.5.6. *Avem*

$$sgn(\sigma) = \prod_{1 \leq i \leq j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Demonstraţie: Din faptul că orice permutare σ este o bijecţie rezultă că membrul drept al egalităţii din enunţ este raportul dintre produsul diferenţelor de tipul $(k - l)$, cu $k \neq l$, $1 \leq k, l \leq n$ şi acelaşi produs, eventual cu semne schimbate acolo unde σ are o inversiune. Deci

$$\prod_{1 \leq i \leq j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = (-1)^{inv(\sigma)} = sgn(\sigma).$$

□

Propoziţia 2.5.7. *Orice transpoziţie este o permutare impară.*

Demonstraţie: Fie transpoziţia $(ij) \in S_n$, adică permutarea

$$(ij) = \begin{pmatrix} 1 & 2 & ... & i-1 & i & i+1 & ... & j-1 & j & j+1 & ... & n \\ 1 & 2 & ... & i-1 & j & i+1 & ... & j-1 & i & j+1 & ... & n \end{pmatrix}$$

Observăm că are următoarele inversiuni: (i,j), (i,k), (k,j), $(\forall)k \in \{i+1, ..., j-1\}$, adică număr impar de inversiuni. Conform definiţiei semnului unei permutări, rezultă că orice transpoziţie este impară. □

Propoziţia 2.5.8. *Funcţia $sgn : S_n \to \{-1, 1\}$ definită mai sus este un morfism de la grupul $(S_n, \circ)$ la grupul $(\{-1, 1\}, \cdot)$, unde $\cdot$ este înmulţirea uzuală a numerelor întregi.*

Demonstraţie: Pentru orice $\sigma, \tau \in S_n$, avem:

$$sgn(\sigma \circ \tau) = \prod_{1 \le i \le j \le n} \frac{(\sigma \circ \tau)(j) - (\sigma \circ \tau)(i)}{j - i} = \prod_{1 \le i \le j \le n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} =$$

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

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

□

Observaţia 2.5.5. *Din Propoziţiile 2.5.7, 2.5.8 şi Observaţia 2.5.3, rezultă că un ciclu este permtare pară sau impară, după cum lungimea lui este număr impar, respectiv par.*

Exemplul 2.5.5. *Semnul permutării $\sigma = (1354)(267)$ se stabileşte astfel: descompunem σ în produs de transpoziţii $(13)(35)(54)(26)(67)$ şi semnul produsului de transpoziţii este produsul semnelor conform Propoziţiei 2.5.8, adică $(-1)^5 = -1$, de unde rezultă σ impară. O altă metodă este să utilizăm Observaţia 2.5.5, conform căreia $sgn((1354)) = -1$, $sgn((267)) = 1$, deci $sgn(\sigma) = -1$.*

Încheiem secţiunea cu o problemă de numărare: Câte cicluri de lungime k există în S_n?

Fie $(i_1 i_2 ... i_k)$ un ciclu de lungime $k \leq n$ din S_n. Alegerea ordonată a elementelor $i_1, i_2, ..., i_n$ din cele n ale mulţimii I_n se face în $A_n^k = \frac{n!}{(n-k)!}$ moduri. Dar ciclurile $(i_1 i_2 ... i_k)$, $(i_2 i_3 ... i_k i_1)$, ..., $(i_k i_1 ... i_{k-1})$ coincid, deci numărul ciclurilor distincte de lungime k este $\frac{A_n^k}{k} = C_n^k (k-1)!$. În particular, există $\frac{n(n-1)}{2}$ transpoziţii şi $(n-1)!$ cicluri de lungime n în S_n.

2.5.2 Grupuri diedrale

Grupul diedral de grad n este grupul D_n al simetriilor unui poligon regulat cu n laturi. Notăm cu σ rotaţia de unghi $\frac{2\pi}{n}$ în jurul centrului poligonului şi cu τ simetria într-una din axele de simetrie ale poligonului. Rezultă $\sigma^n = e$, $\tau^2 = e$ şi $\tau \circ \sigma = \sigma^{n-1} \circ \tau$.

$$D_n = \{e, \sigma, ..., \sigma^{n-1}, \tau, \sigma \circ \tau, ..., \sigma^{n-1} \circ \tau\}.$$

Grupul diedral D_3 este grupul simetriilor unui triunghi echilateral. Triunghiul echilateral este invariant la rotaţii de unghi multiplu de $2\pi/3$ în jurul centrului de greutate şi la simetriile faţă de înălţimi.

Notând cu $1, 2, 3$ vârfurile triunghiului în sens trigonometric, rotaţia de unghi $2\pi/3$ în sens trigonometric se poate descrie printr-o permutare din S_3: $\sigma = (123)$. Atunci σ^2 va fi rotaţia de unghi $4\pi/3$, iar σ^3 chiar identitatea. Fie $\tau = (23) \in S_3$ simetria faţă de înălţimea din vârful 1. Evident, τ^2 este identitatea, iar simetriile în raport cu celelalte două axe sunt date de $\sigma \circ \tau$, $\sigma^2 \circ \tau$. Obţinem $D_3 = S_3$.

Grupul diedral D_4 este grupul simetriilor unui pătrat. Pătratul este invariat de rotaţii de unghi multiplu de $\pi/2$ şi de simetriile faţă de axele de simetrie: mediatoarele laturilor, diagonalele.

Notând cu $1, 2, 3, 4$ vârfurile pătratului în sens trigonometric, putem descrie izometriile de mai sus prin permutări din S_4:

a) $\sigma = (1234)$ este rotaţia de unghi $\pi/2$;
b) $\sigma^2 = (13)(24)$ este rotaţia de unghi π;
c) $\sigma^3 = (1432)$ este rotaţia de unghi $3\pi/2$;
d) $\sigma^4 = (1)$ este identitatea;
e) $\tau = (12)(34)$ este simetria faţă de mediatoarea laturilor 1-2, 3-4;
f) $\tau \circ \sigma = (24)$ este simetria faţă de diagonala 1-3;
g) $\tau \circ \sigma^2 = (14)(23)$ este simetria mediatoarea laturilor 1-4, 2-3;

h) $\tau \circ \sigma^3 = (13)$ este simetria faţă de diagonala 2-4;

Mulţimea $D_4 = \{e, \sigma, \sigma^2, \sigma^3, \tau, \tau \circ \sigma, \tau \circ \sigma^2, \tau \circ \sigma^3\}$ este grup necomutativ în raport cu compunerea permutărilor (înmulţirea ciclurilor).

2.5.3 Grupul cuaternionilor

Fie următoarele matrice de ordin 2 cu elemente din $\mathbf{C}$:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad j = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad k = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

unde $i^2 = -1$. Prin calcul direct se stabileşte că

$$j^2 = -1, \quad k^2 = -1, \quad jk = -kj,$$

unde 1 este matricea unitate notată mai sus. Mulţimea

$$Q = \{1, -1, j, -j, k, -k, jk, -jk\},$$

este grup necomutativ în raport cu înmulţirea matricelor, numit *grupul cuaternionilor*.

2.6 Exerciţii

Sugerăm cititorului să exerseze cunoştinţele dobândite până acum rezolvând următoarele exerciţii.

1. Fie A o mulţime nevidă. Demonstraţi că:

a) $P(A)$ este monoid în raport cu intersecţia mulţimilor.

b) Mulţimea funcţiilor $\{0,1\}^A$ este monoid în raport cu produsul funcţiilor: $(\forall) f, g : A \to \{0,1\}$, $f \cdot g \in \{0,1\}^A$, definit prin $(f \cdot g)(x) = f(x) \cdot g(x)$, $(\forall) x \in A$.

c) Funcţia $\varphi : P(A) \to \{0,1\}^A$, $\varphi(A') = \chi_{A'}$, $(\forall) A' \subseteq A$, este izomorfism de monoizi.

2. Demonstraţi că orice grup de ordin trei este izomorf cu $(\mathbb{Z}_3, +)$.

3. Se consideră mulţimea de funcţii $K = \{f_0, f_1, f_2, f_3\}$, cu $f_i : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $(\forall) i \in \{0, 1, 2, 3\}$, unde $f_0(x, y) = (x, y)$, $f_1(x, y) = (x, -y)$, $f_2(x, y) = (-x, y)$, $f_3(x, y) = (-x, -y)$, $(\forall)(x, y) \in \mathbb{R} \times \mathbb{R}$. Întocmiţi tabla operaţiei de compunere pe K şi demonstraţi că mulţimea K este grup în raport cu compunerea funcţiilor. Acest grup se numeşte *grupul lui Klein*. Elementele sale reprezintă simetriile în plan faţă de axele de coordonate şi origine, respectiv. Demonstraţi că grupurile $(K, \circ)$ şi $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ sunt izomorfe.

4. Fie $f : \mathbb{Z}_{15} \to \mathbb{Z}_{20}$ definită prin $f(\hat{k}) = [4 \cdot k]$, pentru orice $\hat{k} \in \mathbb{Z}_{15}$, unde am notat cu $[x]$ clasa de resturi modulo 20 a întregului x.

a) Arătaţi că f este corect definită, adică nu depinde de reprezentanţi.

b) Demonstraţi că f este morfism între grupurile $(\mathbb{Z}_{15}, +)$ şi $(\mathbb{Z}_{20}, +)$.

c) Determinaţi $Ker(f)$ şi $Im(f)$.

d) Aceleaşi cerinţe de mai sus pentru funcţia $f : \mathbb{Z}_{20} \to \mathbb{Z}_{15}$ definită prin $f([k]) = 3 \hat{\cdot} k$.

6. Determinaţi toate morfismele de grupuri:

a)$f : (\mathbb{Z}_n, +) \to (\mathbb{Z}, +)$;

b)$f : (\mathbb{Q}, +) \to (\mathbb{Z}, +)$;

c)$f : (\mathbb{Z}, +) \to (\mathbb{Q}, +)$.

Indicaţie: a) Un morfism $f : \mathbb{Z}_n \to \mathbb{Z}$ este unic determinat de $f(\hat{1}) = a \in \mathbb{Z}$. Din condiţia de morfism rezultă $f(\hat{k}) = k \cdot a$. Pentru a fi corect definit, trebuie asigurată condiţia $f(\hat{0}) = f(\hat{n})$, deci $0 = n \cdot a$, de unde $a = 0$. Există deci un singur morfism, cel nul.

b) Un morfism $f : \mathbb{Q} \to \mathbb{Z}$ este unic determinat de $f(1) = a \in \mathbb{Z}$. Din condiţia de morfism rezultă $f(k) = k \cdot a$, $(\forall) k \in \mathbb{Z}$. Pentru orice număr natural n, $a = f(1) = f(n \cdot \frac{1}{n}) = n \cdot f(\frac{1}{n})$, deci $n|a$, de unde $a = 0$. Există deci un singur morfism, cel nul.

c) Pentru fiecare $a \in \mathbb{Z}$, există câte un morfism $f : \mathbb{Z} \to \mathbb{Q}$, dat de $f(k) = k \cdot a$, $(\forall) k \in \mathbb{Z}$.

7. Să se arate că următoarele perechi de grupuri nu pot fi izomorfe:

a)$(\mathbb{Z}, +)$ şi $(\mathbb{Q}, +)$;

b) $(\mathbb{Q}, +)$ şi $(\mathbb{R}, +)$;

c)$(\mathbb{Q}, +)$ şi $(\mathbb{Q}_+^*, \cdot)$;

d)$(\mathbb{R}^*, \cdot)$ şi $(\mathbb{R}, +)$;

Indicaţie: a) Dacă ar exista un izomorfism $f : (\mathbb{Z}, +) \to (\mathbb{Q}, +)$ cu $f(1) = \frac{a}{b}$, atunci $Im(f) = \frac{a}{b} \cdot \mathbb{Z} \neq \mathbb{Q}$, contradicţie cu f surjecţie.

b) Mulţimea $\mathbb{Q}$ este numărabilă, iar $\mathbb{R}$ este de puterea continumuului, deci nu pot fi echipotente.

c) Dacă ar exista un izomorfism $f : (\mathbb{Q}, +) \to (\mathbb{Q}_+^*, \cdot)$, atunci $f(0) = 1$. Fie $f(a) = 2$. Din proprietatea de morfism, $2 = f(\frac{a}{2} + \frac{a}{2}) = \left(f(\frac{a}{2})\right)^2$, contradicţie cu $\sqrt{2} \notin \mathbb{Q}$.

d) Dacă ar fi izomorfe prin $f : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$, atunci există $a \in \mathbb{R}^*$ astfel încât $f(a) = -1$. Avem $f(0) = 1 = (-1) \cdot (-1) = f(2a)$, deci $2a = 0$, de unde $1 = f(0) = -1$, contradicţie.

8. Demonstraţi că funcţia $f : \mathbb{Z} \to \mathbb{Z}_n$ definită prin $f(k) = \hat{k}$, $(\forall)k \in \mathbb{Z}$ este un morfism surjectiv de grupuri de la $(\mathbb{Z}, +)$ la $(\mathbb{Z}_n, +)$. Determinaţi nucleul acestui morfism.

9. Întocmiţi tabla grupului simetric $(S_3, \circ)$ scriind toate elementele sale în funcţie de ciclurile $\sigma = (123)$ şi $\tau = (23)$.

10. Fie permutările

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 1 & 2 & 6 & 3 & 8 & 7 \end{pmatrix}, \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 7 & 1 & 3 & 4 & 8 & 6 \end{pmatrix},$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 8 & 1 & 5 & 6 & 4 & 3 & 2 \end{pmatrix}.$$

Descompuneţi permutările în produs de cicluri disjuncte, apoi în produs de transpoziţii şi precizaţi semnul fiecăreia. Determinaţi permutările σ^2, σ^3, σ^{-1}, $\sigma \circ \pi$, $\pi \circ \sigma$, $\sigma \circ \tau$, $\tau \circ \sigma$, $\tau \circ \pi$, $\pi \circ \tau$, efectuând calcul cu cicluri. Precizaţi elementele $\sigma^{100}(3)$, $\tau^{1000}(7)$.

11. Fie numerele naturale $n \geq l \geq 2$. Demonstraţi că:
a) Numărul transpoziţiilor din S_n este C_n^2.
b) Numărul ciclurilor de lungime n din S_n este $(n-1)!$.
c) Numărul ciclurilor de lungime l din S_n este $C_n^l \cdot (l-1)!$.

Capitolul 3

Subgrupuri. Teorema lui Lagrange. Teoreme de izomorfism

3.1 Subgrup

Fie $(G, \cdot)$ un grup şi H o submulţime nevidă a sa. Fie 1 elementul neutru al grupului dat. Amintim că elementul neutru al unui grup se notează în general e, dar pentru grupuri cu legea de compoziţie în notaţie aditivă se notează 0, iar pentru grupuri multiplicative se mai notează 1. Simetricul unui element x dintr-un grup multiplicativ se notează x^{-1} şi se numeşte inversul elementului x, iar simetricul unui element oarecare x dintr-un grup aditiv se notează $-x$ şi se mai numeşte opusul elementului x.

Amintim că H este parte stabilă în raport cu legea de compoziţie " $\cdot$ " dacă

$$x \cdot y \in H, \quad (\forall) x, y \in H.$$

Definiţia 3.1.1. *Submulţimea H se numeşte **subgrup** al lui G dacă legea $\cdot$ induce pe H o structură de grup, adică H este parte stabilă în raport cu $\cdot$ şi $(H, \cdot)$ este grup.*

*Subgrupul H se numeşte **normal** dacă $x \cdot H = H \cdot x$, pentru orice $x \in G$, unde*

$$x \cdot H = \{x \cdot h | \quad h \in H\}, \quad H \cdot x = \{h \cdot x | \quad h \in H\}.$$

Notăm cu $H \leq G$ faptul că H este subgrup al lui G şi cu $\mathbf{S}(G)$ mulţimea subgrupurilor grupului G. Dacă H este subgrup normal, scriem $H \lhd G$.

Propoziţia 3.1.1. *Fie H o submulţime a grupului $(G, \cdot)$. Următoarele afirmaţii sunt echivalente:*

a) H este subgrup al grupului $(G, \cdot)$.

b) $1 \in H$ şi $(\forall)x, y \in H$, $x \cdot y \in H$ şi $x^{-1} \in H$.

c) $H \neq \Phi$ şi $(\forall)x, y \in H$, $x \cdot y^{-1} \in H$.

Demonstraţie: a)$\Rightarrow$ b): Din definiţia subgrupului, H este parte stabilă în raport cu $\cdot$, adică $(\forall)x, y \in H$, $x \cdot y \in H$.

Mai mult, $(H, \cdot)$ este grup şi fie e elementul neutru în acest grup. Pentru un element $h \in H$, ecuaţiile $x \cdot h = h$, $h \cdot x = h$ au în G două soluţii: e şi 1. Dar într-un grup astfel de ecuaţii au soluţie unică (Propoziţia 2.4.2), deci $e = 1$ este elementul neutru în grupul $(H, \cdot)$.

Analog, dacă vom considera h' simetricul elementului $h \in H$ în grupul $(H, \cdot)$, atunci ecuaţiile $x \cdot h = 1$, $h \cdot x = 1$ au în G câte două soluţii, h^{-1} şi h', deci $h' = h^{-1}$, adică $h^{-1} \in H$, $(\forall)h \in H$.

b) $\Rightarrow$ a): Condiţiile de la b) arată că H este o submulţime nevidă a grupului $(G, \cdot)$, pe care $\cdot$ este lege de compoziţie. Deoarece $\cdot$ este asociativă pe G, la fel este pe H. Elementul neutru al grupului G aparţinând lui H, el este element neutru şi pentru restricţa operaţiei $\cdot$ la H. La fel pentru simetricul oricărui element din H, deci $(H, \cdot)$ este grup.

b) $\Rightarrow$ c): Deoarece $1 \in H$ rezultă că H este submulţime nevidă a grupului G. Fie acum $x, y \in H$, arbitrar alese. Din condiţiile de la punctul b) avem $y^{-1} \in H$ şi $x \cdot y^{-1} \in H$, ceea ce trebuia demonstrat.

c) $\Rightarrow$ b): Condiţia H nevidă conduce la existenţa unui element $h \in H$. Din a doua condiţie de la c) avem $h \cdot h^{-1} \in H$, adică $1 \in H$. Fie acum două elemente oarecare $x, y \in H$. Din $1, y \in H$, rezultă $y^{-1} = 1 \cdot (y^{-1}) \in H$, apoi $x \cdot y = x \cdot (y^{-1})^{-1} \in H$. □

Observaţia 3.1.1. *În cazul unui grup aditiv $(G, +)$, condiţiile b) şi c) din Propoziţia anterioară devin: $0 \in H$, $x + y \in H$, $-x \in H$, respectiv $x - y \in H$, pentru orice $x, y \in H$.*

Exemplul 3.1.1. *a) Dacă $(G, \cdot)$ este grup, atunci $\{1\}$, G sunt subgrupuri, numite improprii, ale lui G. Orice alt subgrup se numeşte propriu. Subgrupurile improprii sunt în mod evident normale.*

b) Pentru un grup oarecare $(G, \cdot)$, mulţimea elementelor sale care comută cu oricare element este subgrup normal al grupului G, numit ***centrul*** *grupului G.*

Se notează $Z(G)$:

$$Z(G) = \{x \in G| \quad x \cdot y = y \cdot x, \quad (\forall)y \in G\}.$$

Mai mult, grupul $(Z(G), \cdot)$ este abelian.

c) Dacă grupul este abelian, atunci orice subgrup al său este normal.

d) În grupul permutărilor $(S_3, \circ)$, submulţimea $H = \{e, (12)\}$ este subgrup care nu este normal.

Într-adevăr, pentru $\sigma = (123) \in S_3$, avem

$$\sigma \circ H = \{(123), (13)\}, \quad H \circ \sigma = \{(123), (23)\},$$

deci sunt diferite. Submulţimea $H' = \{e, (123), (132)\}$ este subgrup normal al grupului $(S_3, \circ)$.

Definiţia 3.1.2. *Un grup ale cărui subgrupuri normale sunt doar cele improprii se numeşte* ***grup simplu****.*

Propoziţia 3.1.2. *Fie $f : (G, +) \to (G', \cdot)$ un morfism de grupuri. Nucleul său este subgrup normal al domeniului de definiţie, iar imaginea sa este subgrup (nu neapărat normal) al codomeniului.*

Demonstraţie: Verificăm condiţiile c) din Propoziţia 3.1.1 pentru $Ker(f) = \{x \in G| \quad f(x) = 1\}$. Notăm cu 0, respectiv 1, elementele neutre din domeniu, respectiv codomeniu. Deoarece printr-un morfism de grupuri elementele neutre corespund unul celuilalt, avem $f(0) = 1$, de unde $0 \in Ker(f)$, deci $Ker(f) \neq \Phi$.

Fie acum $x, y \in Ker(f)$, deci $f(x) = f(y) = 1$, şi calculăm

$$f(x - y) = f(x) \cdot f(-y) = f(x) \cdot (f(y))^{-1} = 1 \cdot 1 = 1,$$

de unde $x - y \in Ker(f)$. Am obţinut $Ker(f) \in \mathbf{S}(G)$.

Mai trebuie demonstrat $y + Ker(f) = Ker(f) + y$, pentru $(\forall)y \in G$. Au loc echivalenţele:

$$z \in y + Ker(f) \Leftrightarrow (\exists)x \in Ker(f), z = y + x \Leftrightarrow$$

$$\Leftrightarrow f(z) = f(y) \Leftrightarrow f(z) \cdot (f(y))^{-1} = 1 \Leftrightarrow$$

$$\Leftrightarrow z - y \in Ker(f) \Leftrightarrow (\exists) h \in Ker(f), z = h + y \in Ker(f) + y,$$

adică $y + Ker(f) = Ker(f) + y$, pentru $(\forall) y \in G$. Rezultă că subgrupul $Ker(f)$ este subgrup normal al grupului $(G, +)$.

Analog pentru $Im(f)$, deoarece $f(0) = 1$ rezultă $Im(f) \neq \Phi$. Fie $y_1, y_2 \in Im(f)$, deci există $x_1, x_2 \in G$, $f(x_1) = y_1$, $f(x_2) = y_2$. Calculăm

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

unde am folosit Propoziţia 2.4.3 şi faptul că $x_1, x_2 \in G \Rightarrow x_1 - x_2 \in G$. Rezultă că $Im(f)$ este subgrup al grupului $(G', \cdot)$. □

În continuare ne ocupăm de obţinerea de noi subgrupuri din subgrupuri date ale unui grup $(G, \cdot)$.

Propoziţia 3.1.3. *Dacă $H_1, H_2 \in \boldsymbol{S}(G)$, atunci $H_1 \cap H_2 \in \boldsymbol{S}(G)$. Mai mult, $H_1 \cap H_2$ este cel mai mare subgrup inclus în cele două subgrupuri, deci $H_1 \cap H_2 = inf\{H_1, H_2\}$ în mulţimea ordonată $(\boldsymbol{S}(G), \subseteq)$.*

Demonstraţie: Deoarece H_1 şi H_2 sunt subgrupuri, ele îndeplinesc condiţiile b) din Propoziţia 3.1.1. Vom demonstra că aceleaşi condiţii le îndeplineşte şi $H_1 \cap H_2$.

Evident $1 \in H_1 \cap H_2$. Fie $x, y \in H_1 \cap H_2$, arbitrar alese, deci se află în fiecare din cele două subgrupuri. Avem prin urmare $x \cdot y$ şi x^{-1} în fiecare din cele două subgrupuri, adică $x \cdot y, x^{-1} \in H_1 \cap H_2$.

Vom arăta că în mulţimea ordonată $(\mathbf{S}(G), \subseteq)$, $H_1 \cap H_2$ este cel mai mare minorant al mulţimii $\{H_1, H_2\}$. Evident $H_1 \cap H_2 \subseteq H_1$ şi $H_1 \cap H_2 \subseteq H_2$, deci este minorant. Fie acum $H \in \mathbf{S}(G)$, un minorant oarecare, adică $H \subseteq H_1$, $H \subseteq H_2$. Obţinem $H \subseteq H_1 \cap H_2$, deci $H_1 \cap H_2 = inf\{H_1, H_2\}$. □

Afirmaţia din Propoziţia 3.1.3 se poate generaliza pentru o familie de subgrupuri ale unui grup şi demonstraţia este analoagă celei de mai sus. Astfel, avem:

Propoziţia 3.1.4. *Dacă $\{H_i\}_{i \in I}$ este o familie de subgrupuri ale grupului $(G, +)$, atunci $\cap_{i \in I} H_i$ este subgrup al lui G şi este infimumul familiei date în mulţimea ordonată $(\boldsymbol{S}(G), \subseteq)$.*

Propoziţia 3.1.5. *Pentru orice subgrup H al grupului $(G, \cdot)$ are loc $H \cdot H = H$ şi $H = H^{-1}$, unde am notat prin H^{-1} mulţimea simetricelor tuturor elementelor din H, iar $H \cdot H = \{h_1 \cdot h_2 \quad | \quad h_1, h_2 \in H\}$.*

Demonstraţie: Prima egalitate este evidentă din faptul că orice subgrup este parte stabilă la legea de compoziţie din grup. Pentru a doua egalitate, avem $(\forall)x \in H$, $x^{-1} \in H$ care implică $(x^{-1})^{-1} \in H^{-1}$, deci $H \subseteq H^{-1}$. Reciproc, pentru $x \in H^{-1}$ rezultă că x este simetricul unui element $h \in H$, deci $x = h^{-1}$. Dar $(\forall)h \in H$, $h^{-1} \in H$ implică $x \in H$, adică $H^{-1} \subseteq H$. □

Fie $(G, \cdot)$ un grup. Pe mulţimea $P(G)$ a părţilor mulţimii G se poate defini o operaţie notată tot multiplicativ, astfel:

$$H_1 \cdot H_2 = \{x_1 \cdot x_2 | \quad x_1 \in H_1, x_2 \in H_2\},$$

pentru orice două submulţimi H_1, H_2 ale lui G. Chiar dacă cele două submulţimi sunt subgrupuri, $H_1 \cdot H_2$ nu este în general subgrup, ci avem:

Propoziţia 3.1.6. *Fie $H_1, H_2 \in \boldsymbol{S}(G)$. Atunci $H_1 \cdot H_2 \in \boldsymbol{S}(G)$ dacă şi numai dacă $H_1 \cdot H_2 = H_2 \cdot H_1$.*

Demonstraţie: Dacă $H_1 \cdot H_2 \in \mathbf{S}(G)$, atunci, conform Propoziţiei 3.1.5, avem

$$H_1 \cdot H_2 = (H_1 \cdot H_2)^{-1} = (H_2)^{-1} \cdot (H_1)^{-1} = H_2 \cdot H_1.$$

Fie acum $H_1, H_2 \in \mathbf{S}(G)$ astfel încât $H_1 \cdot H_2 = H_2 \cdot H_1$.

Avem $1 \in H_1 \cap H_2$, de unde $1 = 1 \cdot 1 \in H_1 \cdot H_2$.

Fie $x, y \in H_1 \cdot H_2$, arbitrar alese. Avem $x = h_1 \cdot h_2$ şi $y = a_1 \cdot a_2$, cu $h_1, a_1 \in H_1$, $h_2, a_2 \in H_2$. Calculăm

$$x \cdot y = (h_1 \cdot h_2) \cdot (a_1 \cdot a_2) = h_1 \cdot (h_2 \cdot a_1) \cdot a_2.$$

Deoarece $h_2 \cdot a_1 \in H_2 \cdot H_1 = H_1 \cdot H_2$, rezultă că există $b_1 \in H_1$ şi $b_2 \in H_2$ astfel încât $h_2 \cdot a_1 = b_1 \cdot b_2$. Găsim $x \cdot y = h_1 \cdot b_1 \cdot b_2 \cdot a_2 \in H_1 \cdot H_2$.

Are loc şi $x^{-1} = (h_2)^{-1} \cdot (h_1)^{-1} \in H_2 \cdot H_1 = H_1 \cdot H_2$, deci $H_1 \cdot H_2$ satsface condiţiile b) din Propoziţia 3.1.1. Rezultă că $H_1 \cdot H_2$ este subgrup. □

O consecinţă a Propoziţiei anterioare este că dacă $(G, \cdot)$ este abelian, atunci $H_1 \cdot H_2 \in \mathbf{S}(G)$ pentru orice $H_1, H_2 \in \mathbf{S}(G)$.

Propoziţia 3.1.7. *Fie $(G, \cdot)$ grup şi $H_1, H_2 \in \boldsymbol{S}(G)$ astfel încât $H_1 \cdot H_2 = H_2 \cdot H_1$. Atunci $H_1 \cdot H_2$ este cel mai mic subgrup care include H_1 şi H_2, deci supremumul mulţimii $\{H_1, H_2\}$ în $(\boldsymbol{S}(G), \subseteq)$.*

Demonstraţie: Din Propoziţia 3.1.6, ştim că $H_1 \cdot H_2$ este subgrup. Evident acest subgrup include mulţimile $H_1 = \{x_1 \cdot 1| \quad x_1 \in H_1\}$ şi $H_2 = \{1 \cdot x_2| \quad x_2 \in H_2\}$.

Mai trebuie să arătăm că $H_1 \cdot H_2$ este $sup\{H_1, H_2\}$ în $(\mathbf{S}(G), \subseteq)$. Fie $H \in \mathbf{S}(G)$ astfel încât $H_1 \subseteq H$ şi $H_2 \subseteq H$ (adică H este un majorant în $(\mathbf{S}(G), \subseteq)$). Pentru orice element $z \in H_1 \cdot H_2$, există $x \in H_1$, $y \in H_2$ cu proprietatea $z = x \cdot y$. Din faptul că H include H_1 şi H_2 rezultă că $x, y \in H$, deci şi $z = x \cdot y \in H$, de unde $H_1 \cdot H_2 \subseteq H$. Am obţinut că $H_1 \cdot H_2$ este cel mai mic majorant al mulţimii $\{H_1, H_2\}$. □

Propoziţia 3.1.8. *Toate subgrupurile grupului* $(\mathbb{Z}, +)$ *sunt de forma* $n\mathbb{Z}$*, cu* $n \in \mathbb{N}$*. Mai mult, pentru orice întregi* $n_1, n_2 \geq 1$ *au loc*

$$n_1\mathbb{Z} + n_2\mathbb{Z} = d\mathbb{Z}, \quad n_1\mathbb{Z} \cap n_2\mathbb{Z} = m\mathbb{Z},$$

unde d *şi* m *sunt cel mai mare divizor comun, respectiv cel mai mic multiplu comun al numerelor* n_1 *şi* n_2*.*

Demonstraţie: Pentru orice întreg $n \geq 1$, se verifică imediat că mulţimea

$$n\mathbb{Z} = \{n \cdot k| \quad k \in \mathbb{Z}\}$$

satisface condiţiile b) din Propoziţia 3.1.1, deci este subgrup în $(\mathbb{Z}, +)$. Vom arăta că orice subgrup al grupului aditiv al numerelor întregi este de această formă.

Fie $H \in \mathbf{S}(\mathbb{Z})$. Dacă $H = \{0\}$, atunci putem scrie $H = 0\mathbb{Z}$. Dacă H are şi elemente nenule, deoarece pentru orice $x \in H$ are loc şi $-x \in H$, rezultă că $H \cap \mathbb{N} \neq \Phi$. Din proprietatea de bună ordonare a mulţimii numerelor naturale obţinem existenţa unui cel mai mic element nenul din $H \cap \mathbb{N}$, fie el n_0. Din proprietatea de parte stabilă a subgrupului H, mulţimea tuturor multiplilor lui n_0 este inclusă în H, deci $n_0\mathbb{Z} \subseteq H$. Fie acum un element oarecare $x \in H$. Din teorema împărţirii cu rest în $\mathbb{Z}$, există $c, r \in \mathbb{Z}$ astfel încât

$$x = n_0 \cdot c + r, \quad 0 \leq r < n_0.$$

Dar $x, n_0 \cdot c \in H$, deci $r \in H$, de unde $r = 0$, altfel ar contrazice alegerea lui n_0 ca fiind cel mai mic element nenul din $H \cap \mathbb{N}$. Rezultă $x \in n_0\mathbb{Z}$, deci $H \subseteq n_0\mathbb{Z}$. Am obţinut mai sus şi incluziunea inversă, aşadar $H = x_0\mathbb{Z}$.

Să calculăm acum suma şi intersecţia a două subgrupuri din $(\mathbb{Z}, +)$.

Este util să observăm că pentru doi întregi $n, m \geq 1$ are loc echivalenţa:

$$n\mathbb{Z} \subseteq m\mathbb{Z} \quad \Leftrightarrow \quad m|n.$$

Într-adevăr, incluziunea conduce la $n \in m\mathbb{Z}$, deci $n = mk$ pentru un întreg k, deci $m|n$. Reciproc, dacă $n = mk_0$, atunci toate elementele din $n\mathbb{Z}$, fiind multipli de n, vor fi şi multipli de m, adică are loc incluziunea.

Fie acum $n_1, n_2 \geq 1$ doi întregi arbitrar aleşi. Deoarece grupul $(\mathbb{Z}, +)$ este abelian, conform Propoziţiei 3.1.7, $n_1\mathbb{Z} + n_2\mathbb{Z}$ este cel mai mic subgrup din $\mathbf{S}(\mathbb{Z})$ care include $n_1\mathbb{Z}$ şi $n_2\mathbb{Z}$. Fiind subgrup al grupului aditiv al numerelor întregi, există un întreg pozitiv d astfel încât

$$n_1\mathbb{Z} + n_2\mathbb{Z} = d\mathbb{Z}.$$

Avem

$$n_1\mathbb{Z} \subseteq d\mathbb{Z} \Rightarrow d|n_1,$$

$$n_2\mathbb{Z} \subseteq d\mathbb{Z} \Rightarrow d|n_2,$$

deci d este un divizor comun pentru n_1 şi n_2. Fie d' un alt divizor comun. Relaţiile $d'|n_1$ şi $d'|n_2$ conduc la $n_1\mathbb{Z} \subseteq d'\mathbb{Z}$, $n_2\mathbb{Z} \subseteq d'\mathbb{Z}$. Dar $n_1\mathbb{Z} + n_2\mathbb{Z}$ este cel mai mic subgrup din $\mathbf{S}(\mathbb{Z})$ care include $n_1\mathbb{Z}$ şi $n_2\mathbb{Z}$, deci $d\mathbb{Z} \subseteq d'\mathbb{Z}$, adică $d'|d$. Am obţinut astfel că d este cel mai mare divizor comun al numerelor întregi n_1 şi n_2, notat de obicei (n_1, n_2).

Analog se demonstrează că $n_1\mathbb{Z} \cap n_2\mathbb{Z} = m\mathbb{Z}$, unde m este cel mai mic multiplu comun al numerelor n_1 şi n_2, folosind Propoziţia 3.1.3. Lăsăm ca exerciţiu această demonstraţie. □

Din Propoziţia 3.1.8 rezultă următoarea consecinţă foarte utilă:

Propoziţia 3.1.9. *Fie $n_1, n_2 \geq 1$ doi întregi arbitrar aleşi şi $d = (n_1, n_2)$. Există $k, l \in \mathbb{Z}$ astfel încât $d = k \cdot n_1 + l \cdot n_2$.*

Demonstraţie: Am obţinut $n_1\mathbb{Z} + n_2\mathbb{Z} = d\mathbb{Z}$, deci $d = d \cdot 1 \in n_1\mathbb{Z} + n_2\mathbb{Z}$. Rezultă că d este suma dintre un multiplu de n_1 şi un multiplu de n_2, adică există $k, l \in \mathbb{Z}$ astfel încât $d = k \cdot n_1 + l \cdot n_2$. □

3.2 Subgrup generat de o mulţime

Fie $(G, \cdot)$ un grup şi $S \subset G$ o submulţime nevidă a sa. Numim *subgrupul generat de* S intersecţia tuturor subgrupurilor lui G, care au proprietatea că includ S:

$$< S >= \underbrace{\cap}_{H \leq G, S \subset H} H.$$

Din modul în care este definit, $< S >$ este cel mai mic subgrup al lui G care include submulţimea S. Elementele mulţimii S se numesc generatorii subgrupului $< S >$. Dacă $S = \{x_1, x_2, ..., x_k\}$, atunci subgrupul generat de S se mai notează $< x_1, x_2, ..., x_k >$.

Definiţia 3.2.1. *Un grup G pentru care există $x \in G$ astfel încât $G =< x >$, se numeşte* ***ciclic****.*

Propoziţia 3.2.1. *Fie $(G, \cdot)$ un grup şi $S \subset G$. Are loc egalitatea*

$$< S >= \{x_1 \cdot x_2 \cdot ... \cdot x_m / \quad m \in \mathbb{N}, x_i \in S \quad sau \quad (x_i)^{-1} \in S\}.$$

Demonstraţie: Trebuie să demonstrăm că intersecţia tuturor subgrupurilor lui G care includ S este egală cu mulţimea tuturor compunerilor de elemente din S şi din S^{-1}. Notăm această mulţime cu A, deci

$$A = \{x_1 \cdot x_2 \cdot ... \cdot x_m / \quad m \in \mathbb{N}, x_i \in S \quad sau \quad (x_i)^{-1} \in S\}.$$

În A avem şi elementul $x \cdot x^{-1}$ pentru un x oarecare din S, deci $1 \in A$.

Pentru orice două elemente din A, rezultatul operaţiei din G dintre ele va avea aceeaşi formă, deci $(A, \cdot)$ e parte stabilă. Mai mult, pentru orice $x_1 \cdot x_2 \cdot ... \cdot x_m \in A$, $(x_1 \cdot x_2 \cdot ... \cdot x_m)^{-1} = (x_m)^{-1} \cdot (x_{m-1})^{-1} \cdot ... \cdot (x_1)^{-1}$ este tot o compunere de elemente din S şi din S^{-1}.

Rezultă că A este subgrup în G. Acest subgrup conţine şi compuneri de câte un element din S, deci include S. Prin urmare A este unul din subgrupurile a căror intersecţie este $< S >$, de unde $< S > \subseteq A$.

Pentru orice subgrup H al lui G, care include S, din proprietatea de parte stabilă, H va conţine şi toate compunerile de elemente din S şi din S^{-1}, adică $A \subseteq H$. Cum H este ales arbitrar, $A \subseteq \underbrace{\cap}_{H \leq G, S \subset H} H$, deci $A \subseteq < S >$. Aveam şi incluziunea inversă, aşadar $< S >= A$. □

Are loc şi:

Propoziţia 3.2.2. *Fie $(G,\cdot)$ un grup şi $H_1, H_2 \in \boldsymbol{S}(G)$. Atunci subgrupul generat de $H_1 \cup H_2$ este $sup\{H_1, H_2\}$ în $(\boldsymbol{S}(G), \subseteq)$. Dacă $H_1 \cdot H_2 = H_2 \cdot H_1$, atunci $H_1 \cdot H_2 =< H_1 \cup H_2 >$.*

Observaţia 3.2.1. *a) Dacă elementele $x_1, x_2, ..., x_k$ din grupul aditiv $(G,+)$ comută două câte două, atunci*

$$< x_1, x_2, ..., x_k >= \{n_1x_1 + n_2x_2 + ... + n_kx_k / \quad n_i \in \mathbb{Z}, i = \overline{1,n}\}.$$

În particular, subgrupul ciclic generat de un element $x \in G$ este

$$< x >= \{nx / n \in \mathbb{Z}\}.$$

b) În notaţie multiplicativă, subgrupul generat de elementele $x_1, x_2, ..., x_k$ din $(G,\cdot)$ care comută două câte două, este

$$< x_1, x_2, ..., x_k >= \{x_1^{n_1} \cdot x_2^{n_2} \cdot ... \cdot x_k^{n_k} / \quad n_i \in \mathbb{Z}, i = \overline{1,n}\}.$$

iar subgrupul ciclic generat de un element x din grupul $(G,\cdot)$ este de forma

$$< x >= \{x^n | \quad n \in \mathbb{Z}\}.$$

În finalul paragrafului anterior am văzut că toate subgrupurile grupului $(\mathbb{Z},+)$ sunt de forma $n\mathbb{Z}$, cu $n \in \mathbb{N}$. Putem spune că:

Propoziţia 3.2.3. *Toate subgrupurile grupului aditiv al numerelor întregi sunt grupuri ciclice.*

Exemplul 3.2.1. *a) Grupul aditiv al numerelor întregi este ciclic,*

$$\mathbb{Z} =< 1 >=< -1 > .$$

b) Grupul aditiv al claselor de resturi modulo n este ciclic, $\mathbb{Z}_n =< \widehat{1} >$.

c) Grupul diedral D_4 introdus mai înainte este subgrupul generat de $\sigma = (1234)$ şi $\tau = (12)(34)$ în $(S_4, \circ)$.

Vom reveni la studiul grupurilor ciclice într-un alt capitol.

3.3 Comportarea subgrupurilor la morfisme

Următoarea afirmaţie este cunoscută sub numele de *Teorema de corespondenţă.*

Propoziţia 3.3.1. *Fie $f : (G, \cdot) \to (G', +)$ un morfism de grupuri.*

a) Dacă $H \leq G$, atunci $f(H) \leq G'$. Dacă $H \lhd G$ şi f surjectivă, atunci $f(H) \lhd G'$.

b) Dacă $K \leq G'$, atunci $f^{-1}(K) \leq G$. Dacă $K \lhd G'$ atunci $f^{-1}(K) \lhd G$.

c) Dacă $f : (G, \cdot) \to (G', +)$ este morfism surjectiv de grupuri, atunci există o corespondenţă bijectivă între subgrupurile (normale) lui G care includ $Kerf$ şi subgrupurile (normale) lui G'.

Demonstraţie: a) Fie H un subgrup al grupului $(G, \cdot)$. Imaginea sa prin morfismul f este mulţimea

$$f(H) = \{y \in G' | \quad (\exists) x \in H, \quad f(x) = y\} = \{f(x) | \quad x \in H\}.$$

Vom nota cu 1 şi 0 elementele neutre în grupurile $(G, \cdot)$, respectiv $(G', +)$. Deoarece $1 \in H$ şi, conform Propoziţiei 2.4.3, $f(1) = 0$, avem $0 \in f(H)$. Fie acum două elemente $y_1, y_2 \in f(H)$. Există $x_1, x_2 \in H$ astfel încât $f(x_1) = y_1$ şi $f(x_2) = y_2$. Calculăm

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

unde am folosit proprietăţile morfismului f şi faptul că H este subgrup. Am obţinut că submulţimea $f(H)$ a lui G' satsiface condiţiile b) din Propoziţia 3.1.1, deci este subgrup.

Să arătăm că dacă H este subgrup normal, în ipoteza de surjectivitate a lui f, subgrupul $f(H)$ este şi el normal. Pentru aceasta, fie $y \in G'$, arbitrar ales. Trebuie demonstrată egalitatea mulţimilor

$$y + f(H) = f(H) + y.$$

Avem în vedere $y = f(x)$ pentru un $x \in G$ din surjectivitate. Fie un element arbitrar din prima mulţime. El este de forma $y + f(h) = f(x) + f(h) = f(x \cdot h)$, cu $h \in H$. Dar H este normal în G, deci $x \cdot h \in x \cdot H = H \cdot x$. Aşadar există un $a \in H$ astfel încât $x \cdot h = a \cdot x$. Obţinem

$$y + f(h) = f(a) + f(x) = f(a) + y \in f(H) + y,$$

deci $y + f(H) \subseteq f(H) + y$. Analog se demonstrează incluziunea inversă, deci $f(H) \lhd G'$.

b) Fie $K \in \mathbf{S}(G')$. Preimaginea sa prin morfismul f este mulţimea

$$f^{-1}(K) = \{x \in G| \quad f(x) \in K\}.$$

Din $f(1) = 0 \in K$ rezultă $1 \in f^{-1}(K)$. Fie $x_1, x_2 \in f^{-1}(K)$, arbitrar alese. Avem $f(x_1), f(x_2) \in K$ şi K subgrup, deci $f(x_1) + f(x_2) \in K$, de unde, folosind faptul că f este morfism, $f(x_1 \cdot x_2) \in K$. Am obţinut $x_1 \cdot x_2 \in f^{-1}(K)$. Analog, $f(x_1^{-1}) = -f(x_1) \in K$, deci $x_1^{-1} \in f^{-1}(K)$. Rezultă că $f^{-1}(K) \leq G$.

Presupunem acum $K \lhd G'$. Vom demonstra egalitatea de mulţimi

$$x \cdot f^{-1}(K) = f^{-1}(K) \cdot x,$$

pentru un $x \in G$, arbitrar ales. Fie $x \cdot a \in x \cdot f^{-1}(K)$, deci $f(x \cdot a) = f(x) + f(a) \in f(x) + K$. Subgrupul K fiind normal, $f(x) + K = K + f(x)$, deci există $y \in K$ astfel încât $f(x \cdot a) = y + f(x)$. Obţinem $f(x \cdot a \cdot x^{-1}) = y \in K$, deci $x \cdot a \cdot x^{-1} \in f^{-1}(K)$, adică $x \cdot a \in f^{-1}(K) \cdot x$. Rezultă incluziunea

$$x \cdot f^{-1}(K) \subseteq f^{-1}(K) \cdot x.$$

Analog se arată incluziunea inversă, deci preimaginea unui subgrup normal printr-un morfism de grupuri este subgrup normal.

c) Vom demonstra că dacă f este morfism surjectiv, atunci următoarele aplicaţii sunt inverse una celeilalte şi deci bijective:

$$\varphi : [Ker(f), G] \to \mathbf{S}(G'), \quad \varphi(H) = f(H), \quad (\forall) H \in [Ker(f), G],$$

$$\eta : \mathbf{S}(G') \to [Ker(f), G], \quad \eta(K) = f^{-1}(K), \quad (\forall) K \in \mathbf{S}(G'),$$

unde $[Ker(f), G] = \{H \in \mathbf{S}(G)| \quad Ker(f) \subseteq H\}$.

Remarcăm faptul că η e corect definită. Într-adevăr, pentru orice subgrup K din G', $f^{-1}(K)$ include $Ker(f)$ deoarece $0 \in K$ implică $f^{-1}(0) \subseteq f^{-1}(K)$.

Din surjectivitatea morfismului f şi Propoziţia 1.4.3, rezultă $f(f^{-1}(K)) = K$ pentru orice $K \in \mathbf{S}(G')$, deci $\varphi \circ \eta = \mathbf{1}_{\mathbf{S}(G')}$.

Avem şi $H \subseteq f^{-1}(f(H))$, $(\forall) H \in \mathbf{S}(G)$. Pentru un subgrup H care include nucleul morfismului f, fie $x \in f^{-1}(f(H))$. Obţinem $f(x) \in f(H)$, deci $(\exists) h \in H$ astfel încât $f(x) = f(h)$.

$$f(x) - f(h) = 0 \Rightarrow f(x \cdot h^{-1}) = 0 \Rightarrow x \cdot h^{-1} \in Ker(f) \subseteq H \Rightarrow x \in H.$$

Din cele de mai sus rezultă $\eta \circ \varphi = \mathbf{1}_{[Ker(f),G]}$. □

Observaţia 3.3.1. *Ştim că* $\{0\} \triangleleft G'$. *Conform Propoziţiei 3.3.1,* $f^{-1}(\{0\}) \triangleleft G$ *şi regăsim astfel unul dintre rezultatele din Propoziţia 3.1.2:*

$$Kerf = f^{-1}(\{0\}) = \{x \in G/ \quad f(x) = 0\} \triangleleft G.$$

Ştim de asemenea că $G \leq G$, *atunci imaginea morfismului* f, $Imf = f(G)$, *este subgrup în* G'. *Dacă* f *este injectivă, atunci* $f : G \to Imf$ *este izomorfism de grupuri, deci putem spune că* G *este izomorf cu un subgrup al lui* G'.

În contiunare vom folosi Teorema de corespondenţă (Propoziţia 3.3.1) pentru a stabili forma subgrupurilor grupului aditiv al claselor de resturi modulo n, pentru un întreg $n \geq 2$, fixat.

Propoziţia 3.3.2. *Toate subgrupurile grupului* $(\mathbb{Z}_n, +)$ *sunt ciclice, generate de câte un divizor natural al lui* n.

Demonstraţie: Fie mulţimea claselor de resturi modulo n, $\mathbb{Z}_n = \{\hat{0}, \hat{1}, ..., \widehat{n-1}\}$. În Exemplul 2.4.5 s-a dotat această mulţime cu o structură de grup în raport cu adunarea claselor. Aplicaţia

$$s : \mathbb{Z} \to \mathbb{Z}_n, \quad s(k) = \hat{k},$$

este morfism surjectiv de grupuri, de la $(\mathbb{Z}, +)$ la $(\mathbb{Z}_n, +)$, numit surjecţia canonică. Vom aplica Teorema de corespondenţă acestui morfism de grupuri pentru a determina subgrupurile codomeniului.

Fie $K \in \mathbf{S}(\mathbb{Z}_n)$, arbitrar ales. Dacă $K = \{\hat{0}\}$, atunci acesta poate fi văzut ca subgrupul generat de elementul $\hat{0} \in \mathbb{Z}_n$. Fie $K \neq \{\hat{0}\}$. Deoarece s este morfism surjectiv, conform Propoziţiei 3.3.1c), există în mod unic un subgrup $H \in [Ker(s), \mathbb{Z}]$ astfel încât $K = s(H)$. Evident, $H \neq \{0\}$. Din Propoziţia 3.1.8 rezultă că $H = m\mathbb{Z}$, unde m este cel mai mic întreg pozitiv din H. Mai mult,

$$Ker(s) = \{k \in \mathbb{Z}| \quad \hat{k} = \hat{0}\} = \{k \in \mathbb{Z}| \quad n|k\} = n\mathbb{Z},$$

şi $Ker(s) \subseteq H$ revine la $n\mathbb{Z} \subseteq m\mathbb{Z}$, ceea ce se caracterizează prin $m|n$. Obţinem

$$K = s(H) = s(m\mathbb{Z}) = \{\hat{k}| \quad k \in m\mathbb{Z}\} =$$

$$= \{\widehat{m \cdot a}| \quad a \in \mathbb{Z}\} = m \cdot \mathbb{Z}_n,$$

deci orice subgrup al grupului $(\mathbb{Z}_n, +)$ este ciclic, generat de un divizor al lui n. □

Încheiem acest paragraf cu un rezultat remarcabil:

Teorema 3.3.1. *[Cayley] Orice grup este izomorf cu un grup de permutări al său. Mai exact, dacă $(G, \cdot)$ este un grup şi $(S(G), \circ)$ grupul său de permutări, atunci G este izomorf cu un subgrup al lui $S(G)$.*

Demonstraţie: Fie funcţia

$$\Psi : G \to S(G), \quad \Psi(x) = \psi_x,$$

unde

$$\psi_x : G \to G, \quad \psi_x(g) = x \cdot g.$$

Se arată că Ψ este corect definită, adică pentru orice $x \in G$, ψ_x este bijecţie (verificaţi!). Funcţia Ψ este morfism injectiv de grupuri:

$$\Psi(x \cdot y)(g) = \psi_{x \cdot y}(g) = (x \cdot y) \cdot g = x \cdot (y \cdot g) = \psi_x(y \cdot g) = \psi_x(\psi_y(g)) =$$

$$= (\psi_x \circ \psi_y)(g), \quad (\forall) g \in G, (\forall) x, y \in G.$$

$$Ker(\Psi) = \{x \in G | \quad \Psi(x) = \mathbf{1}_G\} = \{x \in G | \quad \psi_x(g) = g, (\forall) g \in G\} =$$

$$= \{x \in G | \quad x \cdot g = g, (\forall) g \in G\} = \{1\}.$$

Conform Observaţiei 3.3.1, grupul $(G, \cdot)$ este izomorf cu un subgrup al grupului său de permutări. □

3.4 Grupul factor

În acest paragraf preferăm notaţia aditivă pentru legea de compoziţie a grupurilor considerate, deoarece ideile se reiau în studiul inelelor, relativ la grupul aditiv al unui inel.

Fie $(G, +)$ un grup şi H un subgrup al său. Definim relaţiile de congruenţă modulo H la stânga, $\equiv_s$, respectiv la dreapta $\equiv_d$, prin:

$$x, y \in G, \quad x \equiv_s y (mod H) \Leftrightarrow -x + y \in H,$$

$$x, y \in G, \quad x \equiv_d y (mod H) \Leftrightarrow x - y \in H.$$

Propoziţia 3.4.1. *Cele două relaţii definite mai sus sunt relaţii de echivalenţă.*

Demonstraţie: Vom arăta că relaţia de congruenţă modulo H la stânga este o relaţie de echivalenţă, demonstraţia fiind analoagă şi pentru relaţia de congruenţă modulo H la dreapta.

1. reflexivitatea:

$$-x + x = 0 \in H, (\forall)x \in G \Rightarrow x \equiv_s x(modH), (\forall)x \in G.$$

2. simetria:

$$x \equiv_s y(modH) \Leftrightarrow -x + y \in H \Rightarrow -(-x + y) \in H \Rightarrow$$

$$\Rightarrow -y + x \in H \Rightarrow y \equiv_s x(modH).$$

3. tranzitivitatea:

$$x \equiv_s y(modH), y \equiv_s z(modH) \Rightarrow -x + y, -y + z \in H \Rightarrow$$

$$\Rightarrow (-x + y) + (-y + z) = -x + z \in H \Rightarrow x \equiv_s z(modH).$$

Am folosit în raţionamentul de mai sus faptul că H este subgrup, deci parte stabilă în raport cu legea de compoziţie din G. □

Clasa de echivalenţă a elementului $x \in G$ în raport cu $\equiv_s$, numită şi clasa laterală a elementului x, este mulţimea

$$\hat{x} = \{y \in G | x \equiv_s y(modH)\} = \{y \in G | -x+y \in H\} = \{y \in G | y \in x+H\} = x+H,$$

iar în raport cu $\equiv_d$ este mulţimea $H + x$. Mulţimile cât (mulţimile claselor de echivalenţă) relativ la cele două relaţii de echivalenţă sunt:

$$(G/H)_s = \{x + H| \quad x \in G\}, \quad (G/H)_d = \{H + x| \quad x \in G\}.$$

Observaţia 3.4.1. *Dacă H este subgrup normal al grupului G, atunci cele două mulţimi cât coincid, ca o consecinţă directă a definiţiei subgrupului normal.*

În general, pentru orice subgrup H avem:

Propoziţia 3.4.2. *Mulţimile cât (numite şi factor) $(G/H)_s$ şi $(G/H)_d$ sunt echipotente.*

Demonstraţie: Fie funcţia $f : (G/H)_s \to (G/H)_d$ definită prin

$$f(x+H) = H + (-x), \quad (\forall) x + H \in (G/H)_s.$$

Fiind o funcţie ale cărei argumente sunt clase de echivalenţă trebuie să ne asigurăm că este corect definită, adică legea ei nu depinde de reprezentanţi. Fie $x' \in x + H$, deci există $h \in H$, $x' = x + h$ şi $x + H = x' + H$. Avem

$$f(x'+H) = H + (-x') = H - h - x = H + (-x) = f(x+H),$$

de unde rezultă că f este corect definită.

Fie două clase la stânga $x + H, y + H$ cu $f(x+H) = f(y+H)$.

$$f(x+H) = f(y+H) \Rightarrow H + (-x) = H + (-y) \Rightarrow -x \equiv_d -y(modH) \Rightarrow$$

$$\Rightarrow -y + x \in H \Rightarrow y \equiv_s x(modH) \Rightarrow x + H = y + H,$$

deci f este injectivă.

Pentru orice clasă de echivalenţă la dreapta modulo H, $H + x$, există clasa $(-x) + H \in (G/H)_s$ care are proprietatea $f((-x) + H) = H + x$, deci f este surjectivă. Am obţinut prin urmare o bijecţie între cele două mulţimi cât, deci ele au acelaşi cardinal,

$$|(G/H)_s| = |(G/H)_d|.$$

□

Definiţia 3.4.1. *Cardinalul mulţimii cât $(G/H)_s$ se numeşte **indicele subgrupului** H **în** G şi se notează $|G : H|$.*

Exemplul 3.4.1. *Indicele subgrupului $H = \{\hat{0}, \hat{3}, \hat{6}, \hat{9}\} \subseteq \mathbb{Z}_{12}$ este 3 deoarece mulţimea cât $(\mathbb{Z}_{12}/H)_s$ are trei elemente:*

$$\hat{0} + H = H = \hat{3} + H = \hat{6} + H = \hat{9} + H,$$

$$\hat{1} + H = \{\hat{1}, \hat{4}, \hat{7}, \hat{10}\} = \hat{4} + H = \hat{7} + H = \hat{10} + H,$$
$$\hat{2} + H = \{\hat{2}, \hat{5}, \hat{8}, \hat{11}\} = \hat{5} + H = \hat{8} + H = \hat{11} + H.$$

Teorema 3.4.1. *[Lagrange] Dacă H este un subgrup al grupului G, atunci*

$$|G| = |H| \cdot |G : H|.$$

Demonstraţie: Fie $H \in \mathbf{S}(G)$. Folosim faptul că o relaţie de echivalenţă determină o partiţie a mulţimii pe care este definită. Aici, $\equiv_s$ determină partiţie a lui G în clasele din $(G/H)_s$, mai exact G este reunuiunea disjunctă a elementelor mulţimii factor $(G/H)_s$. Cum această mulţime are $|G : H|$ elemente, iar fiecare element este o mulţime de forma $x+H$, deci echipotentă cu H, obţinem rezultatul dorit. □

O consecinţă imediată a teoremei lui Lagrange este:

Propoziţia 3.4.3. *Dacă G este un grup finit, atunci ordinul oricărui subgrup al său este divizor al ordinului grupului.*

Această consecinţă permite exemplificarea noţiunii de grup simplu introdus în Definiţia 3.1.2:

Propoziţia 3.4.4. *Pentru orice număr prim p grupul aditiv al claselor de resturi modulo p este grup simplu.*

Demonstraţie: Amintim că un grup este simplu dacă singurele sale subgrupuri normale sunt cele improprii. Grupul $(\mathbb{Z}_p, +)$ fiind abelian, orice subgrup al său este normal. De fapt vom demonstra că acest grup are doar două subgrupuri. Fie $H \leq \mathbb{Z}_p$. Conform Propoziţiei 3.4.3, ordinul lui H este un divizor al ordinului grupului $\mathbb{Z}_p$, deci al numărului prim p. Cum singurii săi divizori naturali sunt 1 şi p rezultă că $H = \{\hat{0}\}$ sau $H = \mathbb{Z}_p$. □

Un alt rezultat important este

Propoziţia 3.4.5. *Orice subgrup de indice 2 este normal.*

Demonstraţie: Fie $(G, +)$ un grup şi H un subgrup al său, cu $|G : H| = 2$, adică mulţimile cât $(G/H)_s$, $(G/H)_d$) au câte două elemente. Fiecare din acestea conţine H ca fiind clasa de echivalentă a elementului neutru din G şi încă un element, care va fi $G - H$ deoarece $(G/H)_s$, $(G/H)_d$ reprezintă partiţii ale lui G. Deci $(G/H)_s = (G/H)_d$). Fie $x \in G$, arbitrar ales. Clasa la stânga $x + H$ este sau H sau $G - H$. La fel clasa la dreapta, $H + x$. Presupunem prin absurd că ar fi diferite. Rezultă că $x \in H$ şi $x \notin H$, contradicţie. Am obţinut că $H \lhd G$. □

Fie $(G, +)$ grup şi $H \lhd G$. Conform Observaţiei 3.4.1, mulţimile $(G/H)_s$ şi $(G/H)_d$ coincid şi le vom nota (G/H). Considerăm elementele acestei mulţimi de forma $x + H$ (care coincide de fapt cu $H + x$).

Definim pe (G/H) o operaţie notată tot aditiv:

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

Se verifică faptul că operaţia este corect definită, adică nu depinde de reprezentanţi şi că:

Propoziţia 3.4.6. *Perechea $(G/H,+)$ este grup, şi aplicaţia*

$$s:(G,+)\to(G/H,+),\quad s(x)=x+H,(\forall)x\in G,$$

este morfism surjectiv de grupuri.

Grupul $(G/H,+)$ este numit *grupul factor al grupului G prin subgrupul H*, Elementul neutru al acestui grup este mulţimea H, clasa de echivalenţă a elemenului neutru al grupului G. Morfismul s din Propoziţia 3.4.6 se numeşte *surjecţia canonică.*

Exemplul 3.4.2. *a) Grupul factor $G/\{0\}=\{\{x\}/x\in G\}$ este izomorf cu G.*

b) Grupul factor $G/G=\{G\}$ este izomorf cu $\{0\}$.

c) Fie H un subgrup de indice 2 al lui G. Conform Propoziţiei 3.4.5, H este subgrup normal, deci are sens grupul factor G/H. Deoarece indicele lui H este 2, rezultă că acest grup factor are doar 2 elemente, H şi $G-H$, deci este izomorf cu $(\mathbb{Z}_2,+)$, conform afirmaţiei din Exemplul 2.4.6.

Încheiem acest paragraf cu o aplicaţie referitoare la caracterizarea grupurilor factor simple.

Definiţia 3.4.2. *Un subgrup normal H al grupului G se numeşte **maximal** dacă $H\neq G$ şi pentru orice subgrup normal $K\in[H,G]$ $(H\leq K\leq G)$, avem $H=K$ sau $K=G$.*

Propoziţia 3.4.7. *Fie H un subgrup normal al grupului $(G,+)$. Subgrupul H este maximal dacă şi numai dacă grupul factor G/H este simplu.*

Demonstraţie: Fie H un subgrup maximal al grupului $(G,+)$. Trebuie să arătăm că G/H are doar două subgrupuri normale, cele improprii.

Fie A un subgrup normal al grupului factor. Aplicând Teorema de corespondenţă morfismului surjectiv

$$\pi:G\to G/H,\quad \pi(x)=x+H,\quad (\forall)x\in G,$$

subgrupul A este preimaginea prin π a unui subgrup normal K din G, care include $Ker(\pi)$. Obţinem şirul de subgrupuri normale $H \leq K \leq G$. Dar H este maximal, deci $H = K$ sau $K = G$, deci $A = \pi(K)$ este G/H sau G/G, respectiv. Prin urmare singurele subgrupuri normale sunt cele improprii.

Lăsăm ca exerciţiu demonstrarea implicaţiei inverse. □

3.5 Teoreme de izomorfism pentru grupuri

Teorema 3.5.1. *[Teorema fundamentală de izomorfism] Fie $f : (G, +) \to (G', +)$ un morfism de grupuri. Atunci grupul factor $G/Ker(f)$ este izomorf cu subgrupul $Im(f)$ al lui G'.*

Demonstraţie: Conform Propoziţiei 3.1.2, nucleul unui morfism este subgrup normal al domeniului de definiţie, deci are sens grupul factor $G/Ker(f)$. Considerăm funcţia

$$\varphi : G/Ker(f) \to G', \quad \varphi(x + Ker(f)) = f(x), (\forall)x + Ker(f) \in G/Ker(f).$$

Aceasta este corect definită deoarece pentru orice $x' + Ker(f) = x + Ker(f)$, deci $x - x' \in Ker(f)$, avem $f(x - x') = 0$, adică $f(x) = f(x')$.

Funcţia φ este morfism de grupuri:

$$\varphi((x+Ker(f))+(y+Ker(f))) = \varphi((x+y)+Ker(f)) = f(x+y) = f(x)+f(y) =$$

$$= \varphi(x + Ker(f)) + \varphi(y + Ker(f)).$$

Nucleul acestui morfism este

$$Ker(\varphi) = \{x+Ker(f)| \quad f(x) = 0\} = \{x+Ker(f)| \quad x \in Ker(f)\} = \{Ker(f)\},$$

care este elementul neutru în grupul factor $G/Ker(f)$, deci φ este morfism injectiv. Imaginea morfismului φ este

$$Im(\varphi) = \{f(x)| \quad x + Ker(f) \in G/Ker(f)\} = Im(f).$$

Restrângând codomeniul morfismului injectiv φ la imaginea sa, obţinem φ izomorfism de grupuri. □

Exemplul 3.5.1. *Grupurile factor ale lui* $(\mathbb{Z}, +)$
Avem morfismul surjectiv

$$f : \mathbb{Z} \to \mathbb{Z}_n, \quad f(k) = \widehat{k}, \quad (\forall)k \in \mathbb{Z}.$$

Nucleul său este $n\mathbb{Z}$*, deci* $\mathbb{Z}_n$ *este izomorf cu grupul factor* $\mathbb{Z}/(n\mathbb{Z})$*. Mai mult, acestea sunt toate grupurile factor ale grupului* $(\mathbb{Z}, +)$*.*

Exemplul 3.5.2. *a) Am văzut în Propoziţia 2.5.8 că funcţia*

$$sgn : (S_n, \circ) \to (\{-1, 1\}, \cdot),$$

este morfism surjectiv de grupuri. Nucleul acestui morfism se notează cu A_n *şi se numeşte grupul altern de grad* n*. Fiind nucleul unui morfism, este subgrup normal, conform Propoziţiei 3.1.2. Imaginea morfismului sgn este un grup cu 2 elemente, izomorf deci cu* $(\mathbb{Z}_2, +)$*. Conform Teoremei fundamentale de izomorfism (T.F.I.), avem*

$$(S_n/A_n, \circ) \approx (\mathbb{Z}_2, +).$$

De aici putem observa că $|S_n : A_n| = 2$*, iar din teorema lui Lagrange şi Propoziţia 2.5.2, rezultă* $|A_n| = \frac{n!}{2}$*.*

b) Funcţia $f : (\mathbb{R}, +) \to (\boldsymbol{C}, \cdot)$*, definită prin* $f(t) = \cos 2t\pi + i \cdot \sin 2t\pi$ *este morfism de grupuri. Avem* $Kerf = \mathbb{Z}$*,* $Imf = \{z \in \boldsymbol{C} / \, |z| = 1\}$*. Din Teorema fundamentală de izomorfism rezultă izomorfismul dintre grupul factor* $(\mathbb{R}/\mathbb{Z}, +)$ *şi* $(Imf, \cdot)$*.*

c) Un alt exemplu în care putem aplica Teorema 3.5.1 este legat de grupul automorfismelor unui grup. Se ştie că dacă $(G, +)$ *este grup, atunci mulţimea endomorfismelor* $End(G)$ *sale formează monoid necomutativ în raport cu compunerea funcţiilor. Mulţimea elementelor inversabile din acest grup,* $U(End(G))$ *s-a notat cu* $Aut(G)$ *şi este grup în rapor cu compunerea. Elementele sale sunt automorfismele grupului* G *(izomorfismele* $: G \to G$*).*

Pentru orice $g \in G$*, definim* $\tau_g : G \to G$*,* $\tau_g(x) = g + x - g$*. Dacă legea de compoziţie în grupul* G *era notată multiplicativ, definiţia anterioară ar fi fost:* $\tau_g(x) = gxg^{-1}$*.*

Se arată că τ_g *este automorfism al lui* G *şi îl numim automorfism interior; notăm mulţimea automorfismelor interioare cu*

$$Inn(G) = \{\tau_g / g \in G\}.$$

Mulţimea $Inn(G)$ este subgrup normal al lui $Aut(G)$ (lăsăm verificarea acestui fapt ca exerciţiu!).

Fie aplicaţia

$$\phi : G \to Aut(G), \quad \phi(g) = \tau_g, \quad (\forall)g \in G.$$

Evident $Im(\phi) = Inn(G)$ şi obţinem

$$Ker(\phi) = \{g \in G/ \quad g + x = x + g, \quad (\forall)x \in G\} = Z(G).$$

Conform Teoremei fundamentale de izomorfism,

$$(Inn(G), \circ) \approx (G/Z(G), +).$$

Teorema 3.5.2. *[Prima teoremă de izomorfism pentru grupuri]*

Fie morfismul surjectiv de grupuri $f : (G, +) \to (G', \cdot)$ şi $H \triangleleft G$ astfel încât $Ker(f) \subseteq H$. Atunci grupurile factor $(G/H, +)$ şi $(G'/f(H), \cdot)$ sunt izomorfe.

Demonstraţie: Din Propoziţia 3.3.1 rezultă că $f(H) \triangleleft G'$, deci există grupul factor $G'/f(H)$. Elementele sale sunt clasele de echivalenţă modulo $f(H)$, deci $y \cdot f(H)$, cu $y \in G'$.

Fie funcţia $\varphi : G \to G'/f(H)$ definită prin

$$\varphi(x) = f(x) \cdot f(H), \quad (\forall)x \in G.$$

Avem

$$\varphi(x + y) = f(x + y) \cdot f(H) = (f(x) \cdot f(y)) \cdot f(H) =$$
$$= (f(x) \cdot f(H)) \cdot (f(y) \cdot f(H)) = \varphi(x) \cdot \varphi(y),$$

pentru orice $x, y \in G$. Mai mult, din surjectivitatea lui f, rezultă $(\forall)y \cdot f(H) \in G'/f(H)$, există $x \in G$, $y = f(x)$. Obţinem

$$y \cdot f(H) = f(x) \cdot f(H) = \varphi(x),$$

deci φ este morfism surjectiv de grupuri.

Avem şi

$$Ker(\varphi) = \{x \in G| \quad f(x) \cdot f(H) = f(H)\} = \{x \in G| \quad f(x) \in f(H)\},$$

deci un element x din nucleu va verifica $f(x) = f(h)$ pentru $h \in H$. Obţinem $x - h \in Ker(f) \subseteq H$, deci $x \in H$. Rezultă $Ker(\varphi) = H$ şi rezultatul se obţine aplicând Teorema fundamentală de izomorfism morfismului φ. □

O consecinţă a Teoremei 3.5.2 este:

Propoziţia 3.5.1. *Dacă $(G, +)$ este grup şi $K \triangleleft G$, $H \triangleleft K$, atunci grupurile factor G/K şi $\frac{G/H}{K/H}$ sunt izomorfe.*

Demonstraţie: Fie surjecţia canonică $\pi : G \to G/H$. Pentru morfismul π şi subgrupul normal K al lui G putem aplica Teorema 3.5.2 şi rezultă că grupurile factor G/K şi $\frac{G/H}{\pi(K)}$ sunt izomorfe. Dar

$$\pi(K) = \{\pi(x) | \quad x \in K\} = \{x + H | \quad x \in K\} = K/H,$$

de unde se obţine rezultatul anunţat. □

Aplicaţie: *Grupurile factor ale lui $(\mathbb{Z}_n, +)$*:

Am văzut în Propoziţia 3.3.2 că toate subgrupurile lui $(\mathbb{Z}_n, +)$ sunt ciclice, generate de câte un divizor natural al lui n. Ne propunem să determinăm $\frac{\mathbb{Z}_n}{d\mathbb{Z}_n}$, pentru $d|n$ fixat arbitrar. Din Exemplul 3.5.1, $\mathbb{Z}_n \approx \mathbb{Z}/n\mathbb{Z}$. Relaţia $d|n$ conduce la $n\mathbb{Z} \subseteq d\mathbb{Z}$ şi se verifică uşor că $n\mathbb{Z} \triangleleft d\mathbb{Z}$. Mai mult, grupul factor $d\mathbb{Z}/n\mathbb{Z}$ este izomorf cu $d\mathbb{Z}_n$. Obţinem următorul şir de izomorfisme, folosind Propoziţia 3.5.1 şi Exemplul 3.5.1:

$$\frac{\mathbb{Z}_n}{d\mathbb{Z}_n} \approx \frac{\mathbb{Z}/n\mathbb{Z}}{d\mathbb{Z}/n\mathbb{Z}} \approx \frac{\mathbb{Z}}{d\mathbb{Z}} \approx \mathbb{Z}_d.$$

3.6 Exerciţii

În finalul acestui capitol propunem cititorului rezolvarea câtorva exerciţii.

1. Scrieţi toate subgrupurile grupului $(\mathbb{Z}_{12}, +)$, determinaţi indicele şi verificaţi Teorema lui Lagrange pentru fiecare.

2. Scrieţi toate subgrupurile grupului simetric $(S_3, \circ)$, determinaţi indicele şi verificaţi Teorema lui Lagrange pentru fiecare. Precizaţi care dintre subgrupuri este normal şi pentru acestea scrieţi grupurile factor.

Indicaţie: Consideraţi grupul simetric S_3 scris astfel: $S_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$, unde $\sigma = (123)$, $\tau = (23)$.

3. Fie $(G, \cdot)$ un grup şi $H, K \in \mathbf{S}(G)$ astfel încât $H \cup K \leq G$. Demonstraţi că $H \subseteq K$ sau $K \subseteq H$.

4. Fie $(G, \cdot)$ un grup finit de ordin par. Demonstraţi că ecuaţia $x^2 = 1$ are cel puţin două soluţii distincte în G.

Indicaţie: Presupunem prin absurd că singura soluţie este elementul neutru 1. Deci $(\forall)x \in G - \{1\}$, $x^{-1} \neq x$. Putem partiţiona mulţimea $G - \{1\}$ în $\{(x, x^{-1})\}$. Contradicţie cu $|G|$ par.

5. Determinaţi toate grupurile factor ale grupului $(\mathbb{Z}_{12}, +)$.

6. Fie M o mulţime nevidă şi $(S(M), \circ)$ grupul ei de permutări. Demonstraţi că dacă $|M| \geq 3$, atunci centrul grupului $S(M)$ conţine doar funcţia identitate.

Indicaţie: Pentru $|M| = 2$, $Z(S_2) = S_2$. Fie $|M| \geq 3$. Presupunem prin absurd că există $f \in Z(S(M)) - \{\mathbf{1}_M\}$. Există $a, b \in M$, distincte, cu $f(a) = b$. Cum $|M| \geq 3$, $(\exists)c \in M - \{a, b\}$ şi f comută cu orice permutare din $S(M)$, deci şi cu transpoziţia (bc). Obţinem

$$((bc) \circ f)(a) = (f \circ (bc))(a) \Leftrightarrow (bc)(b) = f(a) \Leftrightarrow c = b.$$

8. Fie $(G, \cdot)$ un grup de ordin 6. Demonstraţi că oricum am alege trei subgrupuri proprii ale sale, cel puţin două sunt izomorfe.

Indicaţie: Ordinul unui subgrup propriu al unui grup de ordin 6 poate fi 2 sau 3, conform Teoremei lui Lagrange. Oricum am alege subgrupuri proprii, cel puţin două au acelaşi ordin, 2 sau 3. Stim că orice grup de ordin 2 e izomorf cu $(\mathbb{Z}_2, +)$ şi orice grup de ordin 3 e izomorf cu $(\mathbb{Z}_3, +)$.

9. Fie $(G, +)$ un grup de ordin 2017. Demonstraţi că toate subgrupurile sale sunt normale.

10. Fie $(G, +)$ un grup de ordin 2018. Poate să aibă un subgrup de ordin 70? Justificaţi!

Capitolul 4

Grupuri ciclice. Ordinul unui element

4.1 Ordinul unui element

Fie $(G, \cdot)$ un grup cu elementul neutru e şi $x \in G$. În Observaţia 3.2.1 am precizat că subgrupul ciclic generat de elementul x în G este

$$< x >= \{x^k | \quad k \in \mathbb{Z}\}.$$

Definiţia 4.1.1. *Ordinul subgrupului generat de elementul $x \in G$ în grupul $(G, \cdot)$ se numeşte **ordinul elementului** x şi se notează $o(x)$.*

Amintim că ordinul unui grup este cardinalul său, notat $|G|$ sau $o(G)$. Din Definiţia 4.1.1 şi Propoziţia 3.4.3 rezultă:

Propoziţia 4.1.1. *Într-un grup finit ordinul fiecărui element este divizor al ordinului grupului.*

Observaţia 4.1.1. *a) Afirmaţia anterioară spune, de exemplu, că un grup de ordin 10 nu poate avea elemente de ordin 3.*

b) Într-un grup oarecare $(G, \cdot)$, singurul element de ordin 1 este elementul neutru e, deoarece subgrupul generat de el este $\{e\}$.

Exemplul 4.1.1. *a) În $(\mathbb{Z}_6, +)$, $o(\widehat{2}) = 3$ deoarece subgrupul generat de $\hat{2}$ este $\{\hat{0}, \hat{2}, \hat{4}\}$. Analog aflăm că $o(\widehat{3}) = 2$, $o(\widehat{4}) = 3$, $o(\widehat{1} = o(\widehat{5}) = 6$.*

b) În grupul simetric $(S_3, \circ)$ *elementul* $\sigma = (123)$ *este de ordin 3, subgrupul generat de* σ *fiind* $\{e, \sigma, \sigma^2\}$*, iar* $\tau = (23)$ *este de ordin 2 deoarece generează subgrupul* $\{e, \tau\}$*.*

c) În grupul lui Klein toate elementele cu exceptia celui neutru sunt de ordin 2.

d) Ordinul oricărui element nenul n *din grupul* $(\mathbb{Z}, +)$ *este infinit, subgrupul generat de acesta fiind* $n\mathbb{Z}$*.*

Propoziţia 4.1.2. *Fie* $(G, \cdot)$ *un grup şi* $x \in G$ *un element de ordin finit. Sunt adevărate următoarele afirmaţii:*

a) Ordinul elementului x *este cel mai mic întreg pozitiv* n_0 *cu proprietatea* $x^{n_0} = e$*, adică:*

$$o(x) = min\{n \in \mathbb{Z}_+^* | \quad x^n = e\}.$$

b) Pentru orice $m \in \mathbb{Z}$*,* $x^m = e \Leftrightarrow o(x)$ *divide* m*.*

c) $(\forall) p, q \in \mathbb{Z}$*,*

$$x^p = x^q \Leftrightarrow p \equiv q(mod \quad o(x)).$$

d) Dacă $o(x) = n$*, atunci pentru orice întreg* m*,*

$$o(x^m) = \frac{n}{(m, n)},$$

unde am notat cu (a, b) *cel mai mare divizor comun al întregilor* a *şi* b*.*

Demonstraţie: a) Dacă $< x >= \{e\}$, ceea ce este echivalent cu $x = e$, atunci $o(x) = 1$ şi afirmaţia este adevărată.

Dacă $x \neq e$, deoarece din în ipoteză avem

$$o(x) = |\{x^k | \quad k \in \mathbb{Z}\}| < \infty,$$

rezultă că nu toate elementele din $< x >$ sunt distincte. Există întregii $k > l$ astfel încât $x^k = x^l$. Compunând la dreapta cu $(x^l)^{-1}$ rezultă că există întregul pozitiv $n = k - l$ cu proprietatea $x^n = e$. Aşadar submulţimea numerelor naturale $\{n \in \mathbb{Z}_+^* | \quad x^n = e\}$ este nevidă. Din proprietatea de bună ordonare a mulţimii $\mathbb{N}$, există un cel mai mic element n_0 al acestei submulţimi.

Vom demonstra că

$$< x >= \{e, x, x^2, ..., x^{n_0 - 1}\}.$$

Notăm cu A mulţimea din membrul drept al egalităţii de mai sus. Incluziunea '$\supseteq$'este evidentă din forma elementelor din $< x >$.

Pentru a demonstra incluziunea inversă, fie $y \in < x >$ arbitrar ales. Există $m \in \mathbb{Z}$ astfel încât $y = x^m$. Aplicăm Teorema împărţirii cu rest numerelor întregi m şi n_0, deci există $c, r \in \mathbb{Z}$ cu proprietatea $m = c \cdot n_0 + r$, $0 \leq r < n_0$. Ţinând cont că $x^{n_0} = e$, obţinem

$$x^m = x^{c \cdot n_0 + r} = (x_0^n)^c \cdot x^r = x^r, \quad 0 \leq r < n_0 \Rightarrow x^m \in A,$$

deci avem şi incluziunea inversă. Rezultă cardinalul mulţimii $< x >$ egal cu n_0, de unde $o(x) = n_0$.

b) Fie $m \in \mathbb{Z}$ pentru care $x^m = e$. Rezultă că m este un element al mulţimii $M = \{n \in \mathbb{Z}_+^* | \quad x^n = e\}$ al cărei minim este $n_0 = o(x)$. Aplicăm din nou Teorema împărţirii cu rest numerelor întregi m şi n_0, deci există $c, r \in \mathbb{Z}$ cu proprietatea $m = c \cdot n_0 + r$, $0 \leq r < n_0$. Calculând x^m obţinem $x^r = e$, cu r nul sau mai mic strict decât n_0. Dacă presupunem $r \neq 0$, contrazicem faptul că n_0 este minimul mulţimii M. Deci $r = 0$, aşadar $o(x)|m$.

Implicaţia inversă este evidentă.

c) Fie $p, q \in \mathbb{Z}$, cu proprietatea că $x^p = x^q$. Compunând la dreapta cu $(x^q)^{-1}$, egalitatea este echivalentă cu $x^{p-q} = e$, ceea ce este echivalent cu $o(x)|(p-q)$, conform b).

d) Fie $o(x) = n$, şi un întreg arbitrar m. Considerăm cel mai mare divizor comun al lor $d = (m, n)$. Există numerele întregi m_1, n_1, prime între ele, cu $m = m_1 \cdot d$ şi $n = n_1 \cdot d$.

Numărul $a = o(x^m)$ este, conform a), cel mai mic întreg pozitiv cu proprietatea $(x^m)^a = e$. Deoarece avem $x^{n_1 \cdot d} = e$, avem şi $(x^m)^{n_1} = e$, deci $o(x^m)$ divide n_1, din b).

Avem $(x^m)^a = e$ şi $o(x) = n$, deci $n|m \cdot a$. Există $k \in \mathbb{Z}$ astfel încât

$$m \cdot a = n \cdot k \Leftrightarrow m_1 \cdot d \cdot a = n_1 \cdot d \cdot k \Leftrightarrow m_1 \cdot a = n_1 \cdot k \Rightarrow n_1 | m_1 \cdot a.$$

Aveam şi $(m_1, n_1) = 1$, deci $n_1|a$. Numerele întregi pozitive a şi n_1 se divid unul pe celălalt, prin urmare am obţinut egalitatea dorită, $o(x^m) = a = n_1 = \frac{n}{d}$. □

Observaţia 4.1.2. *Afirmaţia a) din Propoziţia 4.1.2 este adesea considerată definiţia ordinului unui element pentru elementele de ordin finit. Ea oferă o metodă mai simplă de a determina ordinul unui element, decât determinarea subgrupului generat de acel element şi a ordinului acestuia.*

Observaţia 4.1.3. *În grupul simetric $(S_n, \circ)$ orice transpoziţie este element de ordin 2, iar un ciclu de lungime k este element de ordin k. Într-adevăr, pentru $\sigma = (i_1, i_2, ..., i_k)$ putem calcula:*

$$\sigma^2 = (i_1 i_3 .... i_{k-1})(i_2 i_4 ... i_k), \quad (\forall) k = par,$$

$$\sigma^2 = (i_1 i_3 ... i_k i_2 i_4 ... i_{k-1}), \quad (\forall) k = impar.$$

Observăm că regula este "salt peste 2". Pentru σ^l, regula va fi "salt peste l", deci $\sigma^k = e$.

O consecinţă este următorul mod de a determina ordinul unei permutări. Se descompune permutarea în produs de cicluri. Ordinul permutării este cel mai mic multiplu comun al lungimilor ciclurilor din care e alcătuită.

De exemplu, $o((32)(56)(7891)) = 2$, $o((123)(4789)(56)) = 12$.

Exemplul 4.1.2. *Pentru a determina ordinul elementului $\hat{3}$ în grupul $(\mathbb{Z}_{15}, +)$, observăm*

$$2 \cdot \hat{3} \neq \hat{0}, \quad 3 \cdot \hat{3} \neq \hat{0}, \quad 4 \cdot \hat{3} \neq \hat{0}, \quad 5 \cdot \hat{3} = \hat{0} \rightarrow o(\hat{3}) = 5.$$

Faptul că ordinul unui element este divizor al ordinului grupului uşurează calculul. Ordinul lui $\hat{3}$ ar putea fi doar 1, 3, 5 sau 15. Dar singurul element de ordin 1 este cel neutru, deci îl compunem pe $\hat{3}$ cu el însuşi de 3, apoi de 5 ori şi observăm că $o(\hat{3}) = 5$.

Ştiind ordinul elementului $\hat{3}$, ordinul elementului $\hat{12} = 4 \cdot \hat{3}$ se determină folosind punctul d) al Propoziţiei 4.1.2:

$$o(4 \cdot \hat{3}) = \frac{o(\hat{3})}{(o(\hat{3}), 4)} = \frac{5}{(5, 4)} = 5.$$

Propoziţia 4.1.3. *Fie $(G, \cdot)$ un grup finit. Pentru orice element $x \in G$ are loc $x^{o(G)} = e$.*

Demnostraţie: Conform Propoziţiei 4.1.1, $o(x)|o(G)$. Există deci $k \in \mathbb{Z}$ astfel încât $o(G) = k \cdot o(x)$. Din Propoziţia 4.1.2 a) se ştie că $x^{o(x)} = e$, deci putem calcula

$$x^{o(G)} = x^{k \cdot o(x)} = (x^{o(x)})^k = e^k = e.$$

□

Propoziţia 4.1.4. *Fie $(G,\cdot)$ un grup şi $x,y\in G$ două elemente de ordin finit care comută. Dacă $o(x)$ şi $o(y)$ sunt prime între ele, atunci $o(x\cdot y)=o(x)o(y)$.*

Demonstraţie: Fie $m=o(x)$, $n=o(y)$ şi $s=o(x\cdot y)$. Dacă $x=e$ sau $y=e$, atunci rezultatul este evident. Putem presupune deci $m,n>1$. Avem $x^m=e$, $y^n=e$, de unde $(xy)^{mn}=e$. Conform Propoziţiei 4.1.2 b), $o(xy)=s$ implică $s|mn$. Din ipoteza $(m,n)=1$, această relaţie se realizează în trei situaţii: fie $s|m$, fie $s|n$, fie $s=s_1\cdot s_2$, cu $s_1|m$ şi $s_2|n$.

Cazul $s|m$. Deoarece $(m,n)=1$, rezultă $(s,n)=1$. Există $a\in\mathbb{Z}$ astfel încât $m=s\cdot a$. De aici şi din $x\cdot y=y\cdot x$, are loc

$$e=(xy)^s\Rightarrow e=(xy)^{s\cdot a}=(xy)^m=x^m\cdot y^m=y^m,$$

ceea ce implică $n|m$, contradicţie cu $(m,n)=1$. analog se elimină cazul $s|n$.

Cazul $s=s_1\cdot s_2$, cu $s_1|m$, $s_2|n$. Avem $m=s_1\cdot a$, $n=s_2\cdot b$, cu $a,b\in\mathbb{Z}_+^*$. Calculăm

$$e=(xy)^{s\cdot a}=(xy)^{m\cdot s_2}=(x^m)^{s_2}y^{m\cdot s_2}=y^{m\cdot s_2},$$

de unde $n|m\cdot s_2$. Dar $(m,n)=1$ implică $n|s_2$. Aveam şi $s_2|n$, deci $n=s_2$. Analog se arată $m=s_1$, deci $s=m\cdot n$. □

4.2 Grupuri ciclice

Fie $(G,\cdot)$ un grup cu elementul neutru e şi grupul aditiv al numerelor întregi, $(\mathbb{Z},+)$. Fie $x\in G$, arbitrar fixat. Funcţia

$$f_x:\mathbb{Z}\to G,\quad f_x(k)=x^k,\quad (\forall)k\in\mathbb{Z},$$

este un morfism de grupuri. Imaginea morfismului f_x este subgrupul generat de x în G. Nucleul său este un subgrup în $\mathbb{Z}$, deci, conform Propoziţiei 3.1.8, este ciclic şi este fie $\{0\}$, fie generat de cel mai mic întreg pozitiv n_0 pe care îl conţine, $Ker(f_x)=n_0\mathbb{Z}$.

Pentru morfismul f_x avem două situaţii:

(I) $Ker(f_x)=\{0\}$, ceea ce este echivalent cu f_x injectivă. În acest caz funcţia $f_x:\mathbb{Z}\to<x>$ este bijecţie, deci subgrupul generat de x este izomorf cu $(\mathbb{Z},+)$. O consecinţă imediată de aici este că G este grup infinit, din moment ce conţine un subgrup infinit.

(II) $Ker(f_x) \neq \{0\}$, deci $Ker(f_x) = n_0\mathbb{Z}$, $n_0 > 0$, adică n_0 este cel mai mic element al mulţimii $\{k \in \mathbb{Z} | x^k = e\}$. Conform Propoziţiei 4.1.2 a), generatorul nucleului este chiar ordinul elementului x. Aceasta conduce la $(< x >, \cdot)$ izomorf cu $(\mathbb{Z}_{n_0}, +)$ prin $\varphi : \mathbb{Z}_{n_0} \to < x >$, $\varphi(\widehat{k}) = x^k$, conform Teoremei fundamentale de izomorfism.

Din cele discutate mai sus reiese că:

Teorema 4.2.1. *Într-un grup $(G, \cdot)$, subgrupul ciclic $(< x >, \cdot)$ generat de $x \in G$ este izomorf cu $(\mathbb{Z}, +)$ dacă $o(x)$ este infinit, respectiv cu $(\mathbb{Z}_{o(x)}, +)$, pentru $o(x)$ finit.*

Fie $(G, \cdot)$ un grup ciclic (a se revedea Definiţia 3.2.1), deci există $x \in G$ astfel încât $G =< x >$. Un astfel de element x se numeşte *generator* al grupului.

Exemplul 4.2.1. *a) Elementele $1, -1$ sunt generatori ai grupului ciclic $(\mathbb{Z}, +)$.*
b) În grupul $(\mathbb{Z}_n, +)$ elementul $\hat{1}$ este generator.

Observaţia 4.2.1. *Un grup finit este ciclic dacă şi numai dacă conţine un element de ordin egal cu ordinul grupului.*

O consecinţă a Teoremei 4.2.1 este:

Teorema 4.2.2. *Orice grup ciclic infinit este izomorf cu grupul aditiv al numerelor întregi. Orice grup ciclic finit de ordin n este izomorf cu grupul aditiv al claselor de resturi modulo n.*

O consecinţă imediată a Teoremei 4.2.2 este:

Propoziţia 4.2.1. *Oricare două grupuri ciclice de acelaşi ordin sunt izomorfe.*

Propoziţia 4.2.2. *Orice grup de ordin p prim este ciclic, deci izomorf cu $(\mathbb{Z}_p, +)$.*

Demonstraţie: Fie $(G, \cdot)$ grup, $|G| = p$, cu p număr prim, şi x un element din G, diferit de elementul neutru. Fie n ordinul subgrupului $< x >$ generat de x în G. Conform Propoziţiei 4.1.1, n divide p, deci $n \in \{1, p\}$. Dar singurul element de ordin 1 este cel neutru şi $x \neq e$, de unde rezultă $o(x) = p$, deci G este ciclic. A doua afirmaţie rezultă aplicând Teorema 4.2.2. □

Încheiem paragraful cu câteva caracterizări ale generatorilor unui grup ciclic. Pentru aceasta avem nevoie de următoarea funcţie, numită *Indicatorul lui Euler*:

$$\varphi : \mathbb{N}^* \to \mathbb{N}, \quad \varphi(n) = |\{k \in \mathbb{N} | \quad k < n, \quad (k, n) = 1\}|,$$

definită prin: $\varphi(1) = 1$ şi pentru orice număr natural $n \geq 1$, $\varphi(n)$ este egal cu numărul numerelor mai mici decât n, prime cu n.

Exemplul 4.2.2. $\varphi(6) = 2$ *pentru că singurele numere prime cu* 6, *mai mci decât el, sunt* 1 *şi* 5.

Următoarea Propoziţie oferă o metodă de determinare a valorilor indicatorului lui Euler:

Propoziţia 4.2.3. *a) Dacă p este prim, atunci $\varphi(p) = p - 1$.*

b) Dacă p este prim, atunci $\varphi(p^l) = p^l - p^{l-1}$.

c) Dacă $(m, n) = 1$, atunci $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

d) Pentru $n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$ este descompunerea în factori primi a numărului natural n, atiunci

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_k}).$$

Demonstraţie: a) Pentru p prim, toate numerele nenule mai mici decât p: 1,2,..,$p - 1$, sunt prime cu el.

b) Fie p număr prim. Există p^l numere naturale mai mici decât p^l. Dintre acestea nu sunt prime cu p^l următoarele:

$$0, p, 2p, 3p, ..., p^2, p(p + 1), ..., p(p^{l-1} - 1),$$

adică p^{l-1} numere. Deci rămân $p^l - p^{l-1}$ numere prime cu p.

c) În primul rând remarcăm faptul că definiţia indicatorului lui Euler conduce la

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

Fie numerele naturale nenule m, n, prime între ele şi funcţia

$$f : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_{mn}, \quad f(\hat{x}, \breve{y}) = [nx + my],$$

unde am notat cu $\hat{k}$, $\breve{k}$, $[k]$, clasele de resturi modulo m, n, respectiv mn, ale numărului k.

Funcţia f este corect definită deoarece $\hat{x} = \hat{x'}$, $\breve{y} = \breve{y'}$ implică $m|(x - x')$ şi $n|(y - y')$, de unde $nx + my - nx' - my'$ este divizibil prin mn, deci $[nx + my] = [nx' + my']$.

Funcţia f este injectivă deoarece $[nx + my] = [nx' + my']$ duce la

$$mn|(nx + my - nx' - my') \Rightarrow m|n(x - x'), \quad n|m(y - y').$$

Dar m şi n sunt prime între ele, deci $\hat{x} = \hat{x'}$ şi $\breve{y} = \breve{y'}$. Domeniul şi codomeniul acestei funcţii sunt de acelaşi cardinal finit ($=mn$). Deoarece f este injectivă rezultă că şi este surjectivă.

Fie acum $(x, m) = 1, (y, n) = 1$. Fie $d = (nx + my, mn)$, de unde $d|mn$. Dar $(m, n) = 1$ implică d divide exact unul din ele şi este prim cu celălalt. Fie $d|m$,$(d, n) = 1$. Aplicând proprietăţile cunoscute ale relaţiei de divizibilitate obţinem $d|(x, m)$, deci $d = 1$. Reciproc, pentru întregii x, y, m, n, cu $(nx + my, mn) = 1$, fie $d = (x, m)$ Rezultă $d|1$, deci $(x, m) = 1$. Analog $(y, n) = 1$. Am obţinut

$$(x, m) = 1, (y, n) = 1 \Leftrightarrow (nx + my, mn) = 1,$$

deci restricţia funcţiei f la $\{\hat{x} \in \mathbb{Z}_m| \quad (x, m) = 1\} \times \{\breve{y} \in \mathbb{Z}_n| \quad (y, n) = 1\}$ are codomeniul $\{[z] \in \mathbb{Z}_{mn}| \quad (z, mn) = 1\}$. Prin urmare cele două mulţimi de mai sus sunt cardinal echivalente, aşadar $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

d) Rezultatul se obţine aplicând formulele de la b) şi c) descompunerii în factori primi a lui n. □

Exemplul 4.2.3. $\varphi(125) = \varphi(5^3) = 5^3 - 5^2 = 120$, $\varphi(36) = \varphi(2^2 \cdot 3^2) = 36(1 - \frac{1}{2})(1 - \frac{1}{3}) = 12$.

Revenim la studiul grupurilor ciclice cu următorul rezultat:

Propoziţia 4.2.4. *Fie $(G, \cdot)$ un grup finit şi $x \in G$.*

a) x este generator pentru G dacă şi numai dacă

$$x^{\frac{|G|}{q}} \neq e,$$

pentru orice factor prim q al ordinului grupului G.

b) Dacă x este generator al grupului G, atunci, pentru orice $m \in \mathbb{Z}$, x^m este generator al grupului G dacă şi numai dacă $(m, |G|) = 1$.

c) Dacă G este ciclic, atunci el are $\varphi(|G|)$ generatori.

Demonstraţie: a) Fie x un generator al lui G, deci $o(x) = |G|$, şi fie q un divizor prim al lui $|G|$. Avem $|G| = q \cdot n$, cu $q \geq 2$, deci $n < |G|$. Presupunem prin absurd că $x^n = x^{\frac{|G|}{q}} = e$. Conform Propoziţiei 4.1.2 b), $o(x)|n$, contradicţie cu $n < |G|$.

Reciproc, dacă $x^{\frac{|G|}{q}} \neq e$, pentru orice factor prim q al lui ordinului grupului G, atunci ordinul elementului x, fiind divizor al lui $|G|$, nu poate fi decât $|G|$, deci $G =< x >$.

b) Fie x un generator al grupului G. Fie m un întreg cu proprietatea că x^m este de asemenea generator al lui G. Avem deci $o(x) = o(x^m) = |G|$. Din Propoziţia 4.1.2 d) avem $o(x^m) = \frac{|G|}{(m,|G|)}$, de unde rezultă $(m, |G|) = 1$. Analog se arată implicaţia inversă.

c) Fie G un grup ciclic finit generat de un element x. Grupul G este

$$G = \{e, x, x^2, ..., x^{|G|-1}\}.$$

Deci orice element al lui G este de forma x^m, cu $0 \leq m \leq |G|-1$. Rezultatul de la punctul b) spune că un generator de această formă trebuie să satisfacă $(|G|, m) = 1$. Există $\varphi(|G|)$ astfel de numere, deci G are exact $\varphi(|G|)$ generatori. □

Suntem acum în măsură să dă o clasificare a grupurilor de ordin 4, respeciv 6:

Aplicaţie: *Grupuri de ordin 4*

Fie $(G, \cdot)$ un grup de ordin 4, arbitrar ales. Exemple de astfel de grupuri sunt: $(\mathbb{Z}_4, +)$, $(U(\mathbb{Z}_8), \cdot)$, $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ (vezi Exemplul 2.4.2 pentru produs direct de grupuri), grupul lui Klein $(K, \circ)$.

Dacă grupul G ales este ciclic, atunci, conform Teoremei 4.2.2, este izomorf cu $(\mathbb{Z}_4, +)$.

Dacă G nu este ciclic, atunci, conform Observaţiei 4.2.1, nu conţine niciun element de ordin 4. Rezultă că toate elementele diferite de cel neutru sunt de ordin 2, acesta fiind singurul divizor propriu al numărului 4. Fie $a \in G - \{e\}$, unde am notat cu e elementul neutru din G. Subgrupul generat de a realizează o partiţie a lui G în $< a > \cup < a > \cdot b$, pentru un $b \in G - < a >$ fixat arbitrar. Avem deci $G = \{e, a, b, a \cdot b\}$. Din faptul că toate elementele diferite de e sunt de ordin 2 rezultă $(ab)^2 = e = a^2b^2$, care compusă la stânga cu a şi la dreapta cu b conduce la $ba = ab$. Ţinând cont de egalitatea anterioară şi de $a^2 = e$, $b^2 = e$, tabla operaţiei $\cdot$ este:

$\cdot$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

.

Tabla operaţiei de adunare în grupul produs direct $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ este:

$+$	$(\hat{0},\hat{0})$	$(\hat{0},\hat{1})$	$(\hat{1},\hat{0})$	$(\hat{1},\hat{1})$
$(\hat{0},\hat{0})$	$(\hat{0},\hat{0})$	$(\hat{0},\hat{1})$	$(\hat{1},\hat{0})$	$(\hat{1},\hat{1})$
$(\hat{0},\hat{1})$	$(\hat{0},\hat{1})$	$(\hat{0},\hat{0})$	$(\hat{1},\hat{1})$	$(\hat{1},\hat{0})$
$(\hat{1},\hat{0})$	$(\hat{1},\hat{0})$	$(\hat{1},\hat{1})$	$(\hat{0},\hat{0})$	$(\hat{0},\hat{1})$
$(\hat{1},\hat{1})$	$(\hat{1},\hat{1})$	$(\hat{1},\hat{0})$	$(\hat{0},\hat{1})$	$(\hat{0},\hat{0})$

.

Observăm că cele două table sunt identice, deci grupurile sunt izomorfe prin morfismul $f : (G, \cdot) \to (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, $f(e) = (\hat{0},\hat{0})$, $f(a) = (\hat{0},\hat{1})$, $f(b) = (\hat{1},\hat{0})$, $f(ab) = (\hat{1},\hat{1})$.

Am obţinut astfel că există doar două tipuri de grupuri de ordin 4:

Propoziţia 4.2.5. *Orice grup de ordin* 4 *este izomorf sau cu* $(\mathbb{Z}_4, +)$ *(dacă e ciclic) sau cu* $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$*, (dacă toate elementele diferite de cel neutru au ordinul* 2*).*

Precizaţi de ce tip sunt grupurile: $(U(\mathbb{Z}_8), \cdot)$, grupul lui Klein.

Aplicaţie: *Grupuri de ordin 6*

Fie $(G, \cdot)$ un grup de ordin 6, arbitrar ales. Exemple de astfel de grupuri sunt: $(\mathbb{Z}_6, +)$, $(U(\mathbb{Z}_9), \cdot)$, $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$, $(S_3, \circ)$

Dacă grupul G ales este ciclic, atunci, conform Teoremei 4.2.2, este izomorf cu $(\mathbb{Z}_6, +)$.

Dacă G nu este ciclic, atunci, conform Observaţiei 4.2.1, nu conţine niciun element de ordin 6. Rezultă că toate elementele diferite de cel neutru sunt de ordin 2 sau 3, aceştia fiind singurii divizori proprii ai numărului 6.

Presupunând că toate elementele diferite de e ar fi de ordin 2, obţinem că G admite un subgrup de forma $\{e, a, b, ab\}$, cu $a \neq b$ arbitrare din $G - \{e\}$. Contradicţie cu Propoziţia 3.4.3, deoarece 4 nu divide 6. Prin urmare există cel puţin un element de ordin 3 în G, fie acesta x.

Subgrupul generat de x, fiind de ordin 3, are indicele 2 şi este deci subgrup normal în G (vezi Propoziţia 3.4.5). El realizează o partiţie a lui G în $< x > \cup < x > \cdot y$, pentru un

$$y \in G - < x >,$$

fixat arbitrar.

Ordinul elementului y poate fi 2 sau 3. Dacă ar fi de ordin 3, atunci y^2 ar fi unul dintre elementele x sau x^2 (nu poate fi y, xy sau x^2y deoarece ar rezulta

$y = e$ sau $x = y$ sau$x^2 = y$, ceea ce ar contrazice alegerea lui y). Dacă $y^2 = x$, atunci $e = y^3 = xy$, care compusă la stânga cu x^2 duce la $x^2 = y$. Dacă $y^2 = x^2$, analog găsim $y = x$. În ambele situaţii am ajuns la contradicţie, deci $o(y) = 2$.

Avem prin urmare $G = \{e, x, x^2, y, x \cdot y, x^2 \cdot y\}$.

Un raţionament analog celui de mai sus ne conduce la următoarele egalităţi: $yx = x^2y$, $x^2 = xy$. Ţinând cont de egalităţile anterioare şi de $x^3 = e$, $y^2 = e$, tabla operaţiei $\cdot$ este:

$\cdot$	e	x	x^2	y	xy	x^2y
e	e	x	x^2	y	xy	x^2y
x	x	x^2	e	xy	x^2y	y
x^2	x^2	e	x	x^2y	y	xy
y	y	x^2y	xy	e	x^2	x
xy	xy	y	x^2y	x	e	x^2
x^2y	x^2y	xy	y	x^2	x	e

.

În grupul $(S_3, \circ)$ există elemente de ordin 3, de exemplu $\sigma = (123)$ şi de ordin 2, $\tau = (23)$. Putem scrie $S_3 = \{e, \sigma, \sigma^2, \tau, \sigma \circ \tau, \sigma^2 \circ \tau\}$. Tabla operaţiei de compunere a permutărilor în grupul $(S_3, \circ)$ este

$\circ$	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
e	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	e	$\sigma\tau$	$\sigma^2\tau$	τ
σ^2	σ^2	e	σ	σ^2y	y	σy
τ	τ	$\sigma^2\tau$	$\sigma\tau$	e	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^2\tau$	σ	e	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	e

.

Observăm că cele două table sunt identice, deci grupurile sunt izomorfe.

Remarcăm şi faptul că grupul ciclic este comutativ, iar $(S_3, \circ)$ este necomutativ.

Am obţinut astfel că există doar două tipuri de grupuri de ordin 6:

Propoziţia 4.2.6. *Orice grup de ordin* 6 *este izomorf sau cu* $(\mathbb{Z}_6, +)$ *(dacă e ciclic) sau cu* $(S_3, \circ)$*, (dacă nu e ciclic).*

Precizaţi de ce tip sunt grupurile: $(U(\mathbb{Z}_9), \cdot)$, $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$.

4.3 Subgrupurile unui grup ciclic

Fie $(G, \cdot)$ un grup ciclic şi x_0 un generator al său.

Vom studia separat cazurile $|G|$ infinit, respectiv finit. Caracterizarea grupurilor ciclice este dată de Teorema 4.2.2.

(I) $|G| = \infty$. În acest caz, grupul $(G, \cdot)$ este izomorf cu $(\mathbb{Z}, +)$ prin

$$f_{x_0} : \mathbb{Z} \to G, \quad f_{x_0}(k) = x_0^k, \quad (\forall)k \in \mathbb{Z}.$$

Putem aplica Teorema de corespondenţă(Propoziţia 3.3.1) morfismului surjectiv f_{x_0}. Obţinem că orice subgrup K al grupului G este imaginea prin f_{x_0} a unui subgrup H al domeniului $\mathbb{Z}$, deci, conform Propoziţiei 3.1.8, a unui subgrup ciclic de forma $n\mathbb{Z}$.

$$K = f_{x_0}(n\mathbb{Z}) = \{x_0^{nk} | \quad k \in \mathbb{Z}\} = \{(x_0^n)^k | \quad k \in \mathbb{Z}\} =< x_0^n >,$$

adică este subgrupul lui G generat de elementul x_0^n. Am demonstrat că:

Propoziţia 4.3.1. *Subgrupurile unui grup ciclic $(G, \cdot)$ infinit generat de un element $x_0 \in G$ sunt grupuri ciclice, generate de x_0^n, pentru orice $n \in \mathbb{N}$.*

(II) Dacă $|G| = n < \infty$, atunci $o(x_0) = n$ şi $(G, \cdot)$ este izomorf cu $(\mathbb{Z}_n, +)$ prin

$$f_{x_0} : \mathbb{Z}_n \to G, \quad f_{x_0}(\hat{k}) = x_0^k, \quad (\forall)k \in \mathbb{Z}_n.$$

Orice subgrup K al grupului G este imaginea prin f_{x_0} a unui subgrup H al grupului $\mathbb{Z}_n$, deci, conform Propoziţiei 3.3.2, a unui subgrup ciclic de forma $\hat{d}\mathbb{Z}_n$, cu $d|n$.

$$K = f_{x_0}(\hat{d}\mathbb{Z}_n) = \{x_0^{dk} | \quad \hat{k} \in \mathbb{Z}_n\} = \{(x_0^d)^k | \quad k \in \mathbb{Z}\} =< x_0^d >,$$

deci este subgrupul lui G generat de elementul x_0^d, cu $d|n$. Fie $n = d \cdot d'$. Ordinul subgrupului K este egal cu ordinul elementului x_0^d, pe care îl calculăm folosind Propoziţia 4.1.2 d):

$$o(x_0^d) = \frac{o(x_0)}{(o(x_0), d)} = \frac{n}{d} = d'.$$

Vom demonstra că are loc egalitatea $K = M_{d'}$, unde

$$M_{d'} = \{x \in G | \quad x^{d'} = e\}.$$

Incluziunea directă este adevărată deoarece

$$(x_0^{dk})^{d'} = (x_0^n)^k = e^k = e.$$

Fie $x \in G$ astfel încât $x^{d'} = e$. Din $x \in G$ şi $G =< x_0 >$ rezultă că există $0 \leq a \leq n-1$ cu $x = x_o^a$. Avem

$$e = x^{d'} = (x_0^a)^{d'} = x_0^{a \cdot d'} \Rightarrow n | a \cdot d' \Rightarrow (\exists) b \in \mathbb{Z}, a \cdot d' = n \cdot b = d \cdot d' \cdot b \Rightarrow$$

$$\Rightarrow a = d \cdot b \Rightarrow x = (x_0^d)^b \in K,$$

deci are loc şi inversiunea inversă. Am demonstrat că:

Propoziţia 4.3.2. *Fie $(G, \cdot)$ un grup ciclic de ordin finit n şi K un subgrup al său. Următoarele afirmaţii sunt adevărate:*

a) Dacă x_0 este un generator al grupului G, atunci K este generat de x_0^d, unde $d|n$.

b) Fie $d \cdot d' = n$ unde d este divizorul lui n de la punctul a). Atunci $K = \{x \in G | \quad x^{d'} = e\}$.

c) Ordinul subgrupului K este d'.

Putem acum demonstra că:

Propoziţia 4.3.3. *Orice grup abelian simplu este ciclic, finit şi de ordin număr prim.*

Demonstraţie: Fie $(G, \cdot)$ un grup ca în ipoteză şi x un element al său, diferit de elementul neutru. Grupul fiind abelian, subgrupul $< x >$ generat de x în G este normal, diferit de $\{e\}$. Din ipoteză G este simplu, deci singurele sale subgrupuri normale sunt G şi $\{e\}$. Rezultă că $< x >= G$, adică G este ciclic.

Presupunem prin absurd că G este infinit. Fiind ciclic infinit, $(G, \cdot)$ are şi alte subgrupuri normale, proprii, generate de x^n, cu $n \neq 0$, conform Propoziţiei 4.3.1. Contradicţie cu G simplu.

Deci G este finit, de ordin n. Fiind şi ciclic, conform Propoziţiei 4.3.2, are subgrupuri normale generate de x^d, cu $d|n$. Dacă n nu este prim, atunci G nu este simplu, contradicţie. □

Folosind caracterizarea din Propoziţia 4.3.2 a subgrupurilor unui grup ciclic, putem demonstra:

Propoziţia 4.3.4. *Are loc următoarea egalitate pentru indicatorul lui Euler al oricărui număr natural nenul, n:*

$$\sum_{d|n} \varphi(d) = n.$$

Demonstraţie: Fie grupul ciclic $(\mathbb{Z}_n, +)$ şi d un divizor al lui n. Fie mulţimea $A_d = \{x \in \mathbb{Z}_n | \quad o(x) = d\}$, a tuturor elementelor de ordin d din $\mathbb{Z}_n$. Mulţimea acestor submulţimi realizează o partiţie a mulţimii $\mathbb{Z}_n$. Într-adevăr, orice element din $\mathbb{Z}_n$ are ordinul unul din divizorii lui n, deci aparţine unui A_d. Mulţimile $\{A_d\}_{d|n}$ sunt disjuncte deoarece ordinul unui element este unic, şi sunt nevide deoarece pentru orice d divizor al lui n, elementul cu reprezentantul $d' = \frac{n}{d}$ este de ordin d.

Orice element $\hat{k}$ din $\mathbb{Z}_n$ se scrie $\hat{k} = k\hat{1}$ şi ordinul său este

$$o(\hat{k}) = \frac{o(\hat{1})}{(o(\hat{1}), k)} = \frac{n}{(n, k)}.$$

Acest element e de ordin d dacă şi numai dacă $(n, k) = d'$, adică $\hat{k} = d' \hat{\cdot} k_1$, cu $(d, k_1) = 1$. Din $k < n$ avem şi $k_1 < d$, deci cardinalul mulţimii A_d este numărul numerelor mai mici decât d, prime cu d, adică $\varphi(d)$.

Mulţimea $\{A_d\}_{d|n}$ fiind o partţie, avem egalitatea

$$|\mathbb{Z}_n| = \sum_{d|n} |M_d| = \sum_{d|n} \varphi(d).$$

□

Observaţia 4.3.1. *Egalitatea din Propoziţia 4.3.4 se poate justifica direct astfel: din următoarele n numere raţionale*

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, ..., \frac{n-1}{n}, \frac{n}{n},$$

scrindu-le ca fracţii ireductibile, după ce simplificăm printr-un divizor d al lui $n = d \cdot d'$ sunt exact $\varphi(d')$ fracţii ireductibile cu numitorul d'.

O consecinţă a Propoziţiei anterioare este:

Propoziţia 4.3.5. *Fie $(G, \cdot)$ un grup de ordin finit n cu proprietatea că pentru orice divizor d al lui n există cel mult un subgrup de ordin d. Atunci G este ciclic.*

Demonstraţie: Să remarcăm mai întâi că grupul $(\mathbb{Z}_n, +)$ are exact un subgrup de ordin d, pentru fiecare $d|n$. Într-adevăr, avem ca mai sus $n = d \cdot d'$ şi subgrupul $\hat{d'}\mathbb{Z}_n$ are exact d elemente. Cum d' este unic determinat de d, subgrupul este unic.

Fie G un grup ca în ipoteză. Fie $A_d = \{x \in G| \quad o(x) = d\}$. Dacă A_d este nevidă, atunci există $x_0 \in G$ cu $o(x_0) = d$ şi unicul subgrup de ordin d este generat de x_0. Mai mult, pentru orice alt y din A_d, subgrupul generat de acesta coincide cu $< x_0 >$ din ipoteză. Aşadar A_d conţine toţi generatorii grupului $< x_0 >$. Grupul ciclic $< x >$ de ordin d este izomorf cu $\mathbb{Z}_d$ şi are exact $\varphi(d)$ generatori, conform Propoziţiei 4.2.4 c). Prin urmare cardinalul mulţimii A_d este 0 dacă nu există elemente de ordin d sau $\varphi(d)$. Deci avem $|A_d| \leq \varphi(d)$.

Se arată ca în demonstraţia Propoziţiei 4.3.4 că $\{A_d\}_{d|n}$ este o partiţie a mulţimii G, deci

$$n = |G| = \sum_{d|n} |A_d| \leq \sum_{d|n} \varphi(d) = n.$$

Rezultă că avem peste tot egaliatate, deci $|A_d| = \varphi(d)$ pentru orice divizor al lui n, inclusiv n. Aşadar A_n este nevidă, aşadar există elemente de ordin n, adică G este ciclic. □

4.4 Grupul $(U(\mathbb{Z}_n), \cdot)$

Ştim că grupul $(\mathbb{Z}_n, +)$ este ciclic (un generator este $\widehat{1}$), $((\forall))n \geq 2$. Care ar fi alţi generatori?

Propoziţia 4.4.1. *Fie $x \in \mathbb{Z}_n$. Următoarele afirmaţii sunt echivalente:*

a) $\widehat{x}$ generator în grupul $(\mathbb{Z}_n, +)$;

b) $\widehat{x}$ inversabil în monoidul $(\mathbb{Z}_n, \cdot)$;

c) Numerele x şi n sunt prime între ele: $(x, n) = 1$.

Demonstraţie: "a)⇒ b)" Avem $\mathbb{Z}_n =< \hat{x} >$, deci orice element din $\mathbb{Z}_n$ se scrie ca un multiplu de $\hat{x}$. Prin urmare există $k \in \mathbb{Z}$, $k\hat{x} = \hat{1}$. Egalitatea anterioară conduce la $k \hat{\cdot} x = \hat{1}$, deci $\hat{x} \in U(\mathbb{Z}_n)$, cu $\hat{x}^{-1} = \hat{k}$.

"b)⇒ a)" Fie $\hat{x} \in U(\mathbb{Z}_n)$, deci există $\hat{k} \in \mathbb{Z}_n$, $\hat{k} \cdot \hat{x} = \hat{1}$. Egalitatea anterioară se mai poate scrie $k\hat{x} = \hat{1}$. Orice element din $\mathbb{Z}_n$ este de forma $\hat{a} = a\hat{1} = a \cdot k\hat{x}$, deci $\hat{x}$ este generator al grupului ciclic $(\mathbb{Z}_n, +)$.

"b)⇒ c)" Fie $\hat{x} \in U(\mathbb{Z}_n)$, deci există $\hat{k} \in \mathbb{Z}_n$,

$$\hat{k} \cdot \hat{x} = \hat{1} \Rightarrow (\exists) m \in \mathbb{Z}, \quad k \cdot x + n \cdot m = 1.$$

Fie $d = (x, n)$. Din $d|n$, $d|x$ şi egalitatea $k \cdot x + n \cdot m = 1$ rezultă $d|1$, deci $d = 1$.

"c)⇒ a)" Ştim că $(x, n) = 1$. Din Propoziţia 3.1.9 rezultă existenţa a doi întregi $k, l \in \mathbb{Z}$ cu proprietatea $k \cdot x + l \cdot n = 1$. Trecând egalitatea anterioară în $\mathbb{Z}_n$ avem $\hat{x} \cdot \hat{k} = \hat{1}$, adică $\hat{x} \in U(\mathbb{Z}_n)$. □

Observaţia 4.4.1. *a) O consecinţă a Propoziţiei anterioare este că în monoidul* $(\mathbb{Z}_n, \cdot)$ *avem*

$$U(\mathbb{Z}_n) = \{\hat{x} \in \mathbb{Z}_n | \quad (x, n) = 1\},$$

deci indicatorul lui Euler, $\varphi(n)$*, este ordinul grupului* $(U(\mathbb{Z}_n), \cdot)$*, fiind egal cu numărul numerelor prime cu* n*, mai mici decât* n*. b) Pentru* p *prim, în monoidul* $(\mathbb{Z}_p, \cdot)$*, oricare* $x \in \mathbb{Z}_p^*$ *este inversabil, deci* $(\mathbb{Z}_p^*, \cdot)$ *este grup.*

Aplicând Propoziţia 4.1.3 grupului $(U(\mathbb{Z}_n), \cdot)$, obţinem un rezultat foarte important:

Teorema 4.4.1. *[Teorema lui Euler] Pentru orice întreg* x *prim cu* n *are loc relaţia*

$$x^{\varphi(n)} \equiv 1 (mod \quad n).$$

Cazul $n = p$ prim conduce la :

Teorema 4.4.2. *[Mica teoremă a lui Fermat] Pentru orice întreg* x*, prim cu numărul prim* p*, are loc*

$$x^{p-1} \equiv 1 (mod \quad p).$$

Observaţia 4.4.2. *Cele două teoreme celebre: Teorema lui Euler şi Mica teoremă a lui Fermat prezintă rezultate din teoria numerelor, care în ultimele decenii şi-au găsit aplicabilitate în informatică, mai exact în criptografie.*

Exemplul 4.4.1. *Teoremele 4.4.1, 4.4.2 permit calculul restului care se obţine la împărţirea unei puteri mari printr-un număr:*

Dacă dorim determinarea restului modulo 24 a lui 7^{2012}*, calculăm* $\varphi(24) = 24(1-\frac{1}{2})(1-\frac{1}{3}) = 8$ *folosind Propoziţia 4.2.3 şi aplicăm Teorema lui Euler deoarece* $(7,24) = 1$*,*

$$7^8 \equiv 1(mod 24) \Rightarrow 7^{2012} = (7^8)^{251} \cdot 7^4 \equiv 7^4(mod 24).$$

Prin calcul direct stabilim $7^2 = 49 \equiv 1(mod 24)$*, deci restul cerut este 1.*

Un alt rezultat util tot din teoria numerelor este:

Propoziţia 4.4.2 (Teorema lui Wilson)**.** *Fie întregul* $p \geq 2$*. Următoarele afirmaţii sunt echivalente:*

a)Numărul p este prim;

b) Are loc relaţia

$$(p-1)! + 1 \equiv 0(mod \quad p).$$

Demonstraţie: "a)⇒b)" Dacă p prim, atunci oricare $x \in \mathbb{Z}_p^*$ este inversabil. Fie $x \in \mathbb{Z}_p$ nenul şi $\widehat{x}'$ inversul lui $\widehat{x}$. Presupunem că $\widehat{x} = \widehat{x}'$. Rezultă $\widehat{x}^2 = \widehat{1}$, de unde p divide $(x-1)(x+1)$. Cum p este prim, p divide $x-1$ sau p divide $x+1$. Deci $\widehat{x} = \widehat{1}$ sau $\widehat{x} = \widehat{p-1}$. În rest, fiecare element $\widehat{2}, ..., \widehat{p-2}$ este diferit de inversul său. Atunci produsul lor este $\widehat{1}$, de unde obţinem

$$(p-1)! + 1 \equiv 0(mod p).$$

"a)⇒ b)" Presupunem prin absurd că p nu este prim, deci există $a, b \in \mathbb{Z}$, $1 < a, b < p$, $p = a \cdot b$. Ţinând cont de ipoteza $p|(p-1)! + 1$ şi că $a < p$ revine la faptul că a este factor în $(p-1)!$, avem următorul şir de implicaţii:

$$a|p \Rightarrow a|(p-1)! + 1, \quad a|(p-1)! \Rightarrow a|1 \Rightarrow a = 1,$$

ceea ce contrazice alegerea elementului a ca divizor propriu al lui p. Rezultă că presupunerea făcută este falsă, deci p este număr prim. □

Revenind acum la grupul $U(\mathbb{Z}_n), \cdot)$, remarcăm faptul că acesta nu este întotdeauna ciclic.

Exemplul 4.4.2. *a)* $U(\mathbb{Z}_7) = \{\hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}, \hat{6}\}$ *este grup de ordin* 6 *în raport cu* $\cdot$ *în care elementul* $\hat{1}$ *este de ordin* 1*, elementele* $\hat{2}, \hat{4}$ *sunt de ordin* 3*, iar elementele* $\hat{3}, \hat{5}, \hat{6}$ *sunt de ordin* 6*, deci generatori pentru* $U(\mathbb{Z}_7)$*. Remarcăm că numărul generatorilor este* $\varphi(6)$ *, după cum ştiam din Propoziţia 4.2.4.*

b) $U(\mathbb{Z}_8) = \{\hat{1}, \hat{3}, \hat{5}, \hat{7}\}$ *este grup de ordin* 4 *în raport cu* $\cdot$ *în care elementul* $\hat{1}$ *este de ordin* 1*, iar celelalte elemente sunt de ordin* 2*. Prin urmare niciun element nu are ordinul egal cu al grupului, deci nu este grup ciclic.*

Definiţia 4.4.1. *Dacă* $(U(\mathbb{Z}_n), \cdot)$ *este grup ciclic, atunci un generator al său se numeşte* ***rădăcină primitivă modulo*** n*.*

Observaţia 4.4.3. *Este clar că un element* $\hat{a} \in U(\mathbb{Z}_n)$ *este rădăcină primitivă modulo* n *dacă şi numai dacă* $o(\hat{a}) = \varphi(n)$ *în* $(U(\mathbb{Z}_n), \cdot)$*.*

Exemplul 4.4.3. *Elementele* $\hat{3}, \hat{5}, \hat{6}$ *sunt rădăcini primitive modulo* 6*.*

Aplicând Propoziţia 4.2.4, putem spune că:

Propoziţia 4.4.3. *Fie* $n \geq 2$ *şi* $x \in U(\mathbb{Z}_n)$*. Au loc următoarele proprietăţi:*

a) x *este rădăcină primitivă modulo* n *dacă şi numai dacă pentru orice factor prim al lui* $\varphi(n)$*,* $x^{\frac{\varphi(n)}{q}}$ *nu este echivalent modulo* n *cu* 1*.*

b) Dacă x *este rădăcină primitivă modulo* n*, atunci pentru orice* $k \geq 1$*,* x^k *este rădăcină primitivă modulo* n *dacă şi numai dacă* $(k, \varphi(n)) = 1$*.*

c) Dacă există rădăcini primitive modulo n*, atunci numărul lor este* $\varphi(\varphi(n))$*.*

4.5 Logaritmul discret (extindere)

Teorema lui Euler şi Mica teoremă a lui Fermat prezentate în paragraful anterior permit calcularea resturilor modulo n pentru puteri mari ale unui număr, ceea ce îşi găseşte aplicaţii în criptografie. Criptografia este o ştiinţă matematică care se ocupă cu transformarea datelor în forme neinteligibile pentru prevenirea accesului neautorizat. Un element algebric important în criptografie este logaritmul discret.

Fie $(G, \cdot)$ un grup finit ciclic, de ordin n, şi $a \in G$ un generator al său.

Definiţia 4.5.1. ***Logaritmul discret*** *al unui element* $x \in G$ *este un întreg* $k \in \{0, 1, ..., n-1\}$*, notat* $log_a x$*, cu proprietatea că*

$$x = a^k.$$

Trebuie remarcat faptul că logaritmul discret $log_a x$ există pentru orice $x \in G$ doar dacă a este generator al grupului G.

Exemplul 4.5.1. *Grupul* $(\mathbb{Z}_{11}^*, \cdot)$ *este ciclic, generat de exemplu de* $\hat{6}$*, deoarece* $\hat{6}^{10} = \hat{1}$*, conform Micii Teoreme a lui Fermat şi* $\hat{6}^2 = \hat{3}$*,* $\hat{6}^5 = \hat{10}$*, deci nicun divizor al ordinului grupului (10) nu e ordinul elementului* $\hat{6}$*. Rămâne* $o(\hat{6}) = 10$*, adică este generator. Prin calcul direct determinăm*

x	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{6}$	$\hat{7}$	$\hat{8}$	$\hat{9}$	$\hat{10}$
$log_{\hat{6}} x$	0	9	2	8	6	1	3	7	4	5

pe când $log_{\hat{3}} x$ *nu există pentru orice element din* $\mathbb{Z}_{11}^*$*:*

x	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{6}$	$\hat{7}$	$\hat{8}$	$\hat{9}$	$\hat{10}$
$log_3 x$	0	$-$	1	4	3	$-$	$-$	$-$	3	$-$

deoarece $o(\hat{3}) = 5$*, deci* $\hat{3}$ *nu este generator al grupului.*

Problema logaritmului discret constă în determinarea întregului $k = log_a x$ când se dau grupul ciclic G, generatorul a şi elementul $x \in G$.

Un algoritm de criptare bazat pe dificultatea calculării logaritmului discret este algoritmul **El Gamal cu cheie privată**:

1. **Codificarea**:

-Alegem un număr prim p mare şi g un generator al lui $\mathbb{Z}_p^*$, adică o rădăcină primitivă modulo p.

-Alegem un exponent privat $x \in \{0, 1, ..., p-2\}$ şi calculăm un exponent public $y = g^x$. Remarcăm faptul că x poate fi ales orice întreg, dar, datorită Micii Teoreme a lui Fermat, $g^{p-1} = 1 = g^0$, deci are sens alegerea lui x din mulţimea menţionată. Cheia publică este (p, g, y). Securitatea criptării este asigurată de dificultatea calculării lui $x = log_g y$.

-Alegem un element arbitrar $k \in \{0, 1, ..., p-2\}$ şi calculăm $K = y^k$.

-Pentru a transmite mesajul $m \in \mathbb{Z}_p$, calculez $c_1 = g^k$, $c_2 = K \cdot m$. Mesajul cifrat este $c_1 c_2$.

2. **Decodificarea**:

-Recepţionăm $c_1 c_2$. Folosim cheia privată x şi calculăm $K = c_1^k$, $m = c_2 K^{-1}$.

Justificarea calculului pentru K din decodificare constă în următorul şir de egalităţi evidente:

$$c_1^x = (g^k)^x = (g^x)^k = y^k.$$

Exemplul 4.5.2. *Pentru* $p = 11$*, fie generatorul* $g = 6$*, în* $(\mathbb{Z}_{11}^*, \cdot)$*. Pentru simplificarea scrierii omitem simbolul de clasa modulo 11, înţelegând prin* 6 *de fapt* $\hat{6} \in \mathbb{Z}_{11}$*.*

Alegem cheia privată $x = 4$ *şi elementul arbitrar* $k = 3$*. Calculăm în* $\mathbb{Z}_{11}$*:*

$$y = g^x = 6^4 = 9, \quad K = y^k = 9^3 = 3.$$

Anunţăm cheia publică $(11, 6, 9)$*.*

Codificarea*: În vederea transmiterii de mesaje, calculăm*

$$c_1 = g^k = 6^3 = 7.$$

Dacă dorim transmiterea mesajului $m = 10$*, calculăm:*

$$c_2 = K \cdot m = 3 \cdot 10 = 8.$$

Transmit succesiunea de elemente din $\mathbb{Z}_{11}$*:* 78*.*

Decodificarea*: Se recepţionează* 78*. Şiind cheia privată* $x = 4$ *(ea se furnizează celor cărora li s-a autorizat accesul), calculăm:*

$$K = c_1^x = 7^4 = 3, \quad m = c_2 \cdot K^{-1} = 8 \cdot 4 = 10,$$

deci citesc mesajul 10*.*

Dacă dorim transmiterea unei secvenţe de elemente din $\mathbb{Z}_{11}$*, de exemplu* 7925*, vom codifica fiecare simbol în parte:*

$$m = 7 \Rightarrow c_2 = K \cdot m = 3 \cdot 7 = 10,$$
$$m = 9 \Rightarrow c_2 = 3 \cdot 9 = 5,$$
$$m = 2 \Rightarrow c_2 = 3 \cdot 2 = 6,$$
$$m = 5 \Rightarrow c_2 = 3 \cdot 5 = 4.$$

Calculez şi $c_1 = 7$*, ca mai înainte. Transmitem* 710564*.*

Cel care recepţionează ştie că primul simbol este $c_1 = 7$*, apoi restul semnifică simboluri codificate. Calculăm* $K = 3$ *şi* $K^{-1} = 4$ *ca mai înainte şi decodific. Din păcate pot să apară erori detectabile doar dacă mesajul decriptat va fi incoerent, după cum consider simbolurile primite ca elemente din* $\mathbb{Z}_{11}$*:*

$$10, 5, 6, 4 \Rightarrow 7, 9, 2, 5,$$

caz în care am decriptat corect, fie

$$1, 0, 5, 6, 4 \Rightarrow 4, 0, 9, 2, 5,$$

deci citesc un alt mesaj decât cel transmis.

4.6 Exerciţii

La finalul acetui capitol propunem cititorului câteva exerciţii pentru aprofundarea noţiunilor acumulate.

1. Fie $(G, \cdot)$ un grup cu elementul neutru e şi $o(x) = 2$, $(\forall)x \in G - \{e\}$. Demonstraţi că G este abelian.

2. Aplicând Teorema lui Euler şi Mica Teoremă a lui Fermat, arătaţi că:
a) $880|(3^{40} - 1)$;
b) $19|5^{403} + 2^{203} \cdot 3^{202} + 2^{202} \cdot 3^{201}$.
c) $7|(5^{2018} + 3)$;
d) Restul la împărţirea lui $7^{200} + 3^{200}$ prin 13 este 12.
e) Restul la împărţirea lui 7^{290} prin 360 este 49.
f) Pentru orice întreg n care nu e multiplu nici de 3, nici de 7,

$$63|(n^6 - 1).$$

4. Găsiţi ordinul fiecărui element din următoarele grupuri şi precizaţi care dintre ele este grup ciclic:
a) $(U(\mathbb{Z}_9), \cdot)$;
b) $(U(\mathbb{Z}_{15}), \cdot)$;
c) $(U(\mathbb{Z}_{13}), \cdot)$.

5. Determinaţi toate rădăcinile primitive modulo 12.

6. Demonstraţi că oricum am alege două grupuri de ordin 2011 ele sunt izomorfe.

7. Demonstraţi că oricum am alege trei grupuri de ordin 6, cel puţin două dintre ele sunt izomorfe.

8. Fie $(G, \cdot)$ un grup şi x, y două elemente distincte ale sale. Determinaţi subgrupul generat de $\{x, y\}$ în următoarele condiţii:
a) $o(x) = 2$, $o(y) = 2$ şi $x \cdot y = y \cdot x$;
b) $o(x) = 2$, $o(y) = 3$ şi $x \cdot y = y \cdot x$;

c) $o(x) = 3$, $o(y) = 2$ şi $x \cdot y = y \cdot x^2$.

Indicaţie: a) Prin definiţie $< x, y >$ este intersecţia tuturor subgrupurilor lui G care conţin x şi y. Notăm $H_0 = \{e, x, y, x \cdot y\}$ şi demonstrăm că este subgrup în G. Fiind unul din subgrupurile a căror intersecţie este $< x, y >$, avem $< x, y > \subseteq H_0$. Avem şi $H_0 \subseteq H$, pentru orice $H \in S(G)$, cu $x, y \in H$, deci $H_0 =< x, y >$. Observăm $(H_0, \cdot)$ izomorf cu grupul lui Klein.

Analog se arată că subgrupul cerut la b) este izomorf cu $(\mathbb{Z}_6, +)$ şi că subgrupul de la c) este izomorf cu $(S_3, \circ)$.

9. Determinaţi $\sigma^{2012}(5)$ pentru:

a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 7 & 1 & 2 & 5 & 9 & 3 & 8 \end{pmatrix}$;

b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 9 & 5 & 8 & 7 & 2 & 1 & 6 & 4 \end{pmatrix}$,

calculând ordinul permutării σ.

10. Aplicaţi algoritmul de criptare El Gamal pentru a codifica $MESAJ$ considerând asociat fiecărei litere din alfabetul latin un număr, astfel:

litera	A	B	C	D	E	F	G	H	I	J	K	L	M	N
$\mathbb{Z}_{23}$	1	2	3	4	5	6	7	8	9	10	11	12	13	14

,

O	P	R	S	T	U	V	Z
15	16	17	18	19	20	21	22

.

Indicaţie: Grupul $(\mathbb{Z}_{23}^*, \cdot)$ este ciclic, un generator al său fiind $g = 3$. Trebuie criptată secvenţa $13, 5, 18, 1, 10$. Alegând $x = 7$, $k = 2$, obţinem $K = 4$, $c_1 = 9$ şi mesajul codificat 96203417. Decodificaţi!

Capitolul 5

Inele şi corpuri

5.1 Inel. Corp

Fie A o mulţime nevidă pe care s-au definit două legi de compoziţie interne binare, notate "$\oplus$", respectiv "$\otimes$", numite adunare, respectiv înmulţire.

Definiţia 5.1.1. *Tripletul* $(A, \oplus, \otimes)$ *se numeşte* ***semiinel*** *dacă sunt verificate condiţiile:*

a) $(A, \oplus)$ *este monoid comutativ, fie* ϵ *elementul neutru;*

b) $(A, \otimes)$ *este monoid comutativ, fie* e *elementul neutru;*

c) înmulţirea este distributivă faţă de adunare:

$$x \otimes (y \oplus z) = x \otimes y \oplus x \otimes z, \quad (y \oplus z) \otimes x = y \otimes x \oplus z \otimes x, \quad (\forall) x, y, z \in A;$$

d) $\epsilon \otimes e = e \otimes \epsilon = \epsilon$.

Exemplul 5.1.1. *a) Cel mai simplu exemplu de semiinel este mulţimea numerelor naturale, în raport cu adunarea şi înmulţirea uzuale.*

b) Considerăm mulţimea $\mathbb{R}_{min} = \mathbb{R} \cup \{\infty\}$*, cu legile de compoziţie*

$$x \oplus y = \min\{x, y\}, \quad x \otimes y = x + y, \quad (\forall) x, y \in \mathbb{R}_{min}$$

unde $\min\{x, y\}$ *reprezintă minimul dintre elementele* x, y*, iar* $+$ *este adunarea uzuală, cu regulile binecunoscute*

$$x + \infty = \infty + x = \infty, \quad \infty + \infty = \infty, \quad (\forall) x \in \mathbb{R}.$$

Tripletul $(\mathbb{R}_{min}, \oplus, \otimes)$ *este un semiinel, cu* $\epsilon = \infty$*,* $e = 0$.

c) Considerăm mulţimea $\mathbb{R}_{max} = \mathbb{R} \cup \{-\infty\}$*, cu legile de compoziţie*

$$x \oplus y = \max\{x, y\}, \quad x \otimes y = x + y, \quad (\forall) x, y \in \mathbb{R}_{max}$$

unde $\max\{x, y\}$ *reprezintă maximul dintre elementele* x, y*, iar* $+$ *este adunarea uzuală, cu regulile binecunoscute*

$$x + (-\infty) = -\infty + x = -\infty, \quad -\infty + (-\infty) = \infty, \quad (\forall) x \in \mathbb{R}$$

Tripletul $(\mathbb{R}_{max}, \oplus, \otimes)$ *este un semiinel, cu* $\epsilon = -\infty$*,* $e = 0$*.*

Definiţia 5.1.2. *Tripletul* $(A, \oplus, \otimes)$ *se numeşte* ***inel*** *dacă sunt verificate condiţiile:*

a) $(A, \oplus)$ *este grup abelian;*

b) înmulţirea este asociativă;

c) înmulţirea este distributivă faţă de adunare.

Fie $(A, \oplus, \otimes)$ un inel. În acest caz, în mod uzual, operaţiile de adunare şi înmulţire se notează simplu prin $+$, respectiv $\cdot$. Dacă mai mult, $(A, \cdot)$ este monoid, atunci inelul se numeşte *unitar* sau cu unitate, iar elementul neutru din monoidul $(A, \cdot)$ se notează cu 1 şi îl numim *elementul unu* al inelului. Dacă operaţia $\cdot$ este comutativă, atunci inelul se numeşte *inel comutativ*. Elementul neutru în grupul $(A, +)$ se notează cu 0 şi se numeşte *elementul zero* al inelului, iar simetricul unui element x în grupul $(A, +)$ se notează $-x$ şi se numneşte *opusul* lui x.

Exemplul 5.1.2. *a)* $(\mathbb{Z}, +, \cdot)$*,* $(\mathbb{Q}, +, \cdot)$*,* $(\mathbb{R}, +, \cdot)$ *sunt inele unitare comutative, unde* $+$*,* $\cdot$ *sunt operaţiile uzuale de adunare şi înmulţire a numerelor.*

b) $(\mathbb{Z}_n, +, \cdot)$ *inelul claselor de resturi modulo* n*, pentru orice întreg* $n \geq 1$ *este unitar şi comutativ;*

c) Mulţimea numerelor întregi pare, în raport cu operaţiile de adunare şi înmulţire uzuale, este un inel comutativ fără unitate.

d) Dacă $(G, +)$ *este grup abelian, atunci mulţimea endomorfismelor sale,* $(End(G), +, \circ)$*, este inel unitar necomutativ.*

e) Mulţimea matricelor pătratice $M_n(\mathbb{C})$ *este inel unitar necomutativ în raport cu adunarea şi înmulţirea de matrice, uzuale. Acest inel va fi prezentat în detaliu într-un paragraf următor.*

f) Submulţimea $\mathbb{Z}[i] = \{a + i \cdot b, \quad a, b \in \mathbb{Z}\}$ *a mulţimii numerelor complexe este inel comutativ în raport cu adunarea şi înmulţirea uzuale din* $\mathbb{C}$*, numit inelul lui Gauss.*

e) Fie $\theta \notin \mathbb{Q}$ o rădăcină a ecuaţiei $x^2+mx+n=0$, cu m,n numere întregi. Submulţimea numerelor complexe de forma $a+\theta b$, cu $a,b \in \mathbb{Z}$ este inel în raport cu operaţiile uzuale de adunare şi înmulţire din $\mathbb{C}$. Acest inel se notează $\mathbb{Z}[\theta]$ şi se numeşte inel de întregi pătratici. Pentru $m=0, n=1$ regăsim inelul lui Gauss.

Fie $(A,+,\cdot)$ un inel unitar şi $m,n \in \mathbb{Z}$. Sunt valabile regulile de calcul din grupul $(A,+)$, prezentate anterior, la studiul grupurilor. În plus avem şi:

Propoziţia 5.1.1. *În inelul unitar $(A,+,\cdot)$ au loc:*
a) $0 \cdot x = x \cdot 0 = 0$, pentru orice $x \in A$;
b) $x \cdot (-y) = (-x) \cdot y = -(x \cdot y)$, şi $(-x) \cdot (-y) = x \cdot y$;
c) $x \cdot (y-z) = x \cdot y - x \cdot z$, $(\forall) x,y,z \in A$;
d) $(-x)^n = x^n$ dacă n par, $(-x)^n = -x^n$ dacă n impar,
e) $x \cdot (y_1+y_2+...+y_n) = x \cdot y_1 + x \cdot y_2 + ... + x \cdot y_n$, $(\forall) n \in \mathbb{N}^*$, $(\forall) x, y_i \in A$, $i = \overline{1,n}$;
f) Dacă elementele $x,y \in A$ comută, deci $x \cdot y = y \cdot x$, atunci au loc:

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + ... + xy^{n-2} + y^{n-1}),$$

$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^{n-k} y^k, \quad C_n^k = \frac{n!}{(n-k)!k!},$$

unde ultima egalitate este cunoscută sub numele de Binomul lui Newton.

Demonstraţie: a) Facem următorul calcul, ţinând cont că 0 este element neutru la adunare şi că înmulţirea este distributivă faţă de adunare:

$$0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x \Rightarrow 0 \cdot x = 0.$$

Analog, $x \cdot 0 = 0$.

b) Folosim rezultatul de la punctul anterior după cum urmează:

$$0 = x \cdot 0 = x \cdot (y + (-y)) = x \cdot y + x \cdot (-y) \Rightarrow x \cdot (-y) = -(x \cdot y).$$

Analog se arată $(-x) \cdot y = -(x \cdot y)$. Avem şi

$$(-x) \cdot (-y) = -(x \cdot (-y)) = -(-(x \cdot y)) = x \cdot y.$$

Punctul c) este o consecinţă a distributivităţii înmulţirii faţă de adunare şi a rezultatului de la punctul b).

Punctele d) şi e) se demonstrează prin inducţie. De exemplu, la punctul d), pentru $n = 2k$, facem inducţie după numărul k. Pentru $k = 1$, atunci conform punctului b),

$$(-x)^2 = (-x) \cdot (-x) = x \cdot x = x^2.$$

Presupunem adevărat că $(-x)^{2k} = x^{2k}$ şi vom arăta că $(-x)^{2(k+1)} = x^{2(k+1)}$. Într-adevăr,

$$(-x)^{2(k+1)} = (-x)^{2k} \cdot (-x)^2 = x^{2k} \cdot x^2 = x^{2k+2}.$$

Rezultatele de la punctul f) se demonstrează de asemenea prin inducţie după n. □

În cele ce urmează inelele le vom considera unitare, dacă nu se precizează altfel. Într-un inel unitar $(A, +, \cdot)$, perechea $(A, \cdot)$ este moniod. Mulţimea elementelor inversabile în acest monoid se numeşte mulţimea elementelor inversabile în inelul A şi se notează $U(A)$. Propoziţia 2.4.1 ne asigură că $(U(A), \cdot)$ este grup.

Exemplul 5.1.3. *a) În inelul numerelor întregi* $(\mathbb{Z}, +, \cdot)$, $U(\mathbb{Z}) = \{-1, 1\}$.

b) În inelul claselor de resturi modulo n, $(\mathbb{Z}_n, +, \cdot)$, *conform Propoziţiei 4.4.1, avem*

$$U(\mathbb{Z}_n) = \{\hat{a} | \quad (a, n) = 1\}.$$

c) În cazul inelelor de întregi pătratici, determinarea elementelor inversabile se face prin intermediul următoarei funcţii, numită funcţia normă:

$$N : \mathbb{Z}[\theta] \to \mathbb{N}, \quad N(a + \theta b) = |(a + \theta b)(a + \theta' b)|,$$

unde θ' *este a doua rădăcină a ecuaţiei* $x^2 + mx + n = 0$. *Funcţia normă are forma echivalentă*

$$N(a + \theta b) = |a^2 - mab + nb^2|,$$

şi următoarele proprietăţi:

1. $N(a + \theta b) = 0 \Leftrightarrow a = b = 0$;

Într-adevăr, $N(a + \theta b) = 0$ *este echivalent cu* $a + \theta b = 0$ *sau* $a + \theta' b = 0$. *Din faptul că* $\theta, \theta' \notin \mathbb{Q}$ *rezultă* $a = b = 0$.

2. $N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2)$, $(\forall) z_1, z_2 \in \mathbb{Z}[\theta]$, *adică* N *este funcţie multiplicativă.*

Calculând fiecare din cei doi membri, avem:

$$z_1 \cdot z_2 = (a_1 + \theta b_1)(a_2 + \theta b_2) = a_1 a_2 - n b_1 b_2 + \theta(a_1 b_2 + a_2 b_1 - m b_1 b_2),$$

$$N(z_1 \cdot z_2) = |a_1^2 a_2^2 + n^2 b_1^2 b_2^2 - m a_1 a_2^2 b_1 - m a_1^2 a_2 b_1 + n a_2^2 b_1^2 + n a_1^2 b_2^2 -$$
$$- mn a_2 b_1^2 b_2 - mn a_2 b_1 b_2^2 + m^2 a_1 a_2 b_1 b_2 == N(z_1) \cdot N(z_2).$$

3. $U(\mathbb{Z}[\theta]) = \{z \in \mathbb{Z}[\theta] | \quad N(z) = 1\}$.
Într-adevăr, dacă $(\exists) z' \in \mathbb{Z}[\theta]$, *cu* $z \cdot z' = 1$, *proprietatea 2 conduce la*

$$N(z) \cdot N(z') = N(1) = 1,$$

care este echivalent cu $N(z) = N(z') = 1$.

Reciproc, $N(z) = 1$ *implică* $(a + \theta b)(a + \theta' b) = \pm 1$, *pentru* $z = a + \theta b$. *Dar* $a + \theta' b = a + (-m - \theta)b = a - mb - \theta b$, *deci* z *admite invers în* $\mathbb{Z}[\theta]$, *inversul fiind unul dintre* $\pm(a - mb - \theta b)$.

d) Să determinăm elementele inversabile în inelul lui Gauss $\mathbb{Z}[i]$. *Fie un element inversabil* $a + i \cdot b \in \mathbb{Z}[i]$. *Deci există* $x + i \cdot y \in \mathbb{Z}[i]$ *cu* $(a + i \cdot b)(x + i \cdot y) = 1$, *egalitate care conduce la* $1 = (a^2 + b^2)(x^2 + y^2)$ *prin trecerea la modulul numerelor complexe. Prin urmare elementul inversabil* $a + i \cdot b$ *verifică* $a^2 + b^2 = 1$. *Obţinem*

$$U(\mathbb{Z}[i]) = \{1, -1, i, -i\}.$$

Definiţia 5.1.3. *Un element nenul* a *al inelului* $(A, +, \cdot)$ *se numeşte* ***divizor al lui zero*** *la sânga (dreapta) dacă există* $b \in A^* = A - \{0\}$ *astfel încât* $a \cdot b = 0$, *(respectiv* $(b \cdot a = 0)$.

Dacă inelul este comutativ, atunci cele două noţiuni coincid.

Definiţia 5.1.4. *Un inel fără divizori ai lui zero se numeşte* ***inel integru***. *Un inel integru comutativ se numeşte* ***domeniu de integritate***.

Exemplul 5.1.4. *a)* $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ *sunt domenii de integritate.*

b) $(\mathbb{Z}_6, +, \cdot)$ *nu este inel integru,* $\widehat{2} \cdot \widehat{3} = \widehat{0}$; *mai general, dacă* n *nu este prim, atunci* $(\mathbb{Z}_n, +, \cdot)$ *nu este integru, clasa de echivalentă modulo* n *a oricărui divizor propriu al lui* n *fiind divizor al lui zero în* $\mathbb{Z}_n$;

c) În inelele de clase de resturi orice element nenul şi neinversabil este divizor al lui zero. Într-adevăr, $\hat{x} \in \mathbb{Z}_n$ *nenul şi neinversabil verifică* $(x, n) = d$, $d \neq 1$, $d \neq n$. *Deci* $x = d \cdot y$, $n = d \cdot m$, *cu* $(y, m) = 1$. *Deoarece* $\hat{x} \cdot \hat{m} = \widehat{d \cdot y \cdot m} = \hat{0}$, *rezultă că* $\hat{x}$ *este divizor al lui zero.*

d) Dacă p *este prim, atunci* $(\mathbb{Z}_p, +, \cdot)$ *este domeniu de integritate.*

e) Toate inelele de întregi pătratici sunt domenii de integritate.

Observaţia 5.1.1. *Niciun element din* $U(A)$ *nu poate fi divizor al lui zero. Într-adevăr, dacă* $x \in U(A)$, *atunci există* $x^{-1} \in A$, *cu*

$$x \cdot x^{-1} = x^{-1} \cdot x = 1.$$

Dacă am presupune că $x \cdot z = 0$, *pentru un nenul* $z \in A$, *atunci înmulţind ultima egalitate la stânga cu* x^{-1} *obţinem* $z = 0$, *contradicţie cu definiţia divizorilor lui zero.*

Propoziţia 5.1.2. *În inelul integru* $(A, +, \cdot)$ *au loc:*

a) $x \cdot y = 0$ *dacă şi numai dacă* $x = 0$ *sau* $y = 0$.

b) $a \cdot x = a \cdot y$ *sau* $x \cdot a = y \cdot a$, *cu* $a \neq 0$ *implică* $x = y$.

Demonstraţie: a) Dacă x şi y ar fi nenuli, ei ar fi divizori ai lui zero în inelul A, ceea ce contrazice ipoteza A inel integru. Implicaţia inversă este evidentă, din Propoziţia 5.1.1.

b) Egalităţile din ipoteză sunt echivalente cu $a \cdot (x - y) = 0$, respectiv $(x - y) \cdot a = 0$. Din A integru, conform punctului a), rezultă $a = 0$ sau $x - y = 0$ şi, deoarece a este nenul, avem $x = y$. □

Definiţia 5.1.5. *Un inel* $(A, +, \cdot)$ *cu cel puţin două elemente (*$1 \neq 0$*) este* ***corp*** *dacă* $U(A) = A^*$, *adică orice element nenul este inversabil.*

Conform Observaţiei 5.1.1, un corp nu are divizori ai lui zero, deci:

Propoziţia 5.1.3. *Orice corp este un inel integru.*

Exemplul 5.1.5. *a)* $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ *sunt corpuri comutative.*

b) Dacă p *este prim, atunci* $(\mathbb{Z}_p, +, \cdot)$ *este corp comutativ.*

c) Fie $d \in \mathbb{Z} - \{1\}$ *un întreg liber de pătrate (*d *nu se divide cu pătratul niciunui număr întreg* $\neq 1$*). Mulţimea*

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} / \quad a, b \in \mathbb{Q}\},$$

este corp comutativ, numit corp pătratic. Elementele acestui corp se numesc numere pătratice.

Propoziţia 5.1.4. *Orice domeniu de integritate finit este corp.*

Demonstraţie: Fie $(A,+,\cdot)$, $A=\{a_1,...a_n\}$ un domeniu de integritate finit. Pentru orice $a\in A^*$, mulţimile $a\cdot A$ şi A coincid. Dar A este inel unitar, deci $1\in a\cdot A$, de unde rezultă că există $a_i\in A$ astfel încât $a\cdot a_i=1$. Am obţinut a inversabil. □

5.2 Subinel, subcorp, ideal

În această secţiune prezentăm submulţimi remarcabile ale unui inel sau corp.

Fie $(A,+,\cdot)$ un inel şi B o submulţime nevidă a sa.

Definiţia 5.2.1. *B se numeşte **subinel** al lui A dacă este inel în raport cu operaţiile induse de cele două operaţii din A. Dacă A este corp şi B are proprietatea anterioară, atunci el se numeşte subinel al corpului A. Dacă A este corp şi B este tot corp în raport cu operaţiile induse, atunci B se numeşte **subcorp** al lui A, iar A **extindere** a corpului B.*

Exemplul 5.2.1. *a) Pentru un inel oarecare $(A,+,\cdot)$, $\{0\}$, A sunt subinele.*

Dacă A este corp, atunci submulţimea $\{0\}$ este subinel, iar A este subcorp.

b) $(\mathbb{Z},+,\cdot)$ este subinel al corpului $(\mathbb{Q},+,\cdot)$, care este subcorp în $(\mathbb{R},+,\cdot)$.

c) Oricare ar fi $n\in\mathbb{Z}$, $(n\mathbb{Z},+,\cdot)$ este subinel în $(\mathbb{Z},+,\cdot)$. Mai mult, deoarece orice subinel este subgrup al grupului aditiv al inelului şi orice subgrup al grupului $(\mathbb{Z},+)$ este de forma $n\mathbb{Z}$ (vezi Propoziţia 3.1.8), acestea sunt toate subinelele lui $\mathbb{Z}$.

Propoziţia 5.2.1. *a) Submulţimea nevidă B a inelului $(A,+,\cdot)$ este subinel dacă şi numai dacă pentru orice $x,y\in B$, au loc $x-y\in B$ şi $x\cdot y\in B$.*

b) Submulţimea nevidă B a corpului A este subcorp dacă şi numai dacă pentru orice $x,y\in B$, $y\neq 0$ au loc $x-y\in B$ şi $x\cdot y^{-1}\in B$.

Demonstraţie: a) Implicaţia directă este evidentă din proprietatea de parte stabilă a inelului B în raport cu operaţiile din A. Reciproc, dacă pentru orice $x,y\in B$ are loc $x-y\in B$, atunci $(B,+)$ este subgrup în $(A,+)$. Condiţia

$x \cdot y \in B$ pentru orice $x, y \in B$, asigură $(B, \cdot)$ parte stabilă, de unde rezultă că axiomele specifice structurii de inel, valabile în A, se menţin şi în B.

b) Analog cu raţionamentul anterior. □

Se verifică imediat că:

Propoziţia 5.2.2. *Intersecţia unei familii de subinele (subcorpuri) este subinel (subcorp).*

Fie $(A, +, \cdot)$ un inel şi I o submulţime nevidă a sa.

Definiţia 5.2.2. *I se numeşte **ideal la stânga (la dreapta)** al lui A dacă $0 \in I$, $x + y \in I$ şi $a \cdot x \in I$ (respectiv $x \cdot a \in I$), pentru orice $x, y \in I$ şi $a \in A$. O submulţime care este ideal la stânga şi la dreapta se numeşte ideal **bilateral**, sau, mai simplu, ideal.*

Observaţia 5.2.1. *Orice ideal la stânga (dreapta) al unui inel comutativ este ideal bilateral.*

Observaţia 5.2.2. *Din definiţie rezultă imediat că orice ideal este subinel. Reciproc nu este adevărat, nu orice subinel este şi ideal: subinelul $\mathbb{Z}$ al lui $\mathbb{Q}$ nu este ideal, deoarece, de exemplu $\frac{2}{3} \cdot 5 \notin \mathbb{Z}$.*

Exemplul 5.2.2. *a) În orice inel $(A, +, \cdot)$, $\{0\}$, A sunt ideale, numite idealul nul, respectiv idealul total. Acestea sunt idealele improprii ale inelului; celelalte ideale se numesc ideale proprii.*

b) Fie $x \in A$, arbitrar ales. Mulţimile

$$x \cdot A = \{x \cdot a, \quad a \in A\}, \quad A \cdot x = \{a \cdot x, \quad a \in A\},$$

sunt ideale la dreapta, respectiv la stânga, ale inelului A.

*Aceste ideale sunt generate de elementul x. Astfel de ideale (generate de un element) se numesc **ideale principale**.*

c) Singurele ideale ale lui $(\mathbb{Q}, +, \cdot)$ sunt $\{0\}$ şi $\mathbb{Q}$. Într-adevăr, considerând un ideal I diferit de cel nul, acesta conţine cel puţin un element nenul, fie acesta x. $\mathbb{Q}$ este corp, deci $x^{-1} \in \mathbb{Q}$. Din definiţia idealului obţinem succesiv $x \cdot x^{-1} = 1 \in I$, apoi $\mathbb{Q} \subseteq I$, deci $I = \mathbb{Q}$. Rezultatul este valabil pentru orice corp, după cum urmează.

Propoziţia 5.2.3. *Inelul $(A, +, \cdot)$ este corp, dacă şi numai dacă singurele sale ideale sunt cel nul şi cel total, sau, altfel spus, cele trei mulţimi de ideale ale sale coincid cu $\{\{0\}, A\}$.*

Demonstraţie: Analog cu justificarea de la exemplul anterior, lăsăm stabilirea implicaţiei directe cititorului. Reciproc, fie A un inel cu $Id_s(A) = Id_d(A) = Id(A) = \{\{0\}, A\}$ şi $x \in A^*$. Idealul generat de x, notat xA, este prin urmare $\{0\}$ sau A. Cum x este nenul şi se află în xA, rezultă $xA = A$, deci $1 \in xA$, de unde avem x inversabil. Deoarece x a fost ales arbitrar, am obţinut A corp. □

Definiţia 5.2.3. *Un domeniu de integritate în care toate idealele sunt principale se numeşte* ***inel principal****.*

Propoziţia 5.2.4. *Inelul numerelor întregi este principal. Un ideal al său este fie idealul nul (generat deci de* 0*), fie este generat de cel mai mic număr pozitiv pe care îl conţine.*

Demonstraţie: Deoarece orice ideal este în particular subgrup al grupului aditiv, rezultă conform Propoziţiei 3.1.8, că orice ideal al inelului numerelor întregi este de forma $n\mathbb{Z}$, pentru un $n \in \mathbb{N}$. Orice astfel de submulţime a lui $\mathbb{Z}$ este ideal în $\mathbb{Z}$, deci toate idealele inelului numerelor întregi sunt principale. Mai mult, ele coincid cu subinelele sale şi cu subgrupurile grupului aditiv al numerelor întregi, deci au forma precizată în enunţ. □

Proprietăţile următoare, afirmate pentru ideale la sânga, se menţin adevărate şi în cazul idealelor la dreapta sau al celor bilaterale.

Propoziţia 5.2.5. *Fie A un inel unitar şi I un ideal la stânga. Următoarele afirmaţii sunt adevărate:*

a) $I = A$ *dacă şi numai dacă* $1 \in I$.

b) $I = A$ *dacă şi numai dacă* $U(A) \cap I \neq \Phi$.

Demonstraţie: Implicaţia directă este evidentă la ambele afirmaţii.

a) Pentru reciprocă, fie $a \in A$, arbitrar ales. Din definiţia idealului, ipoteza $1 \in I$ conduce la $a \cdot 1 \in I$, deci $A \subset I$. Rezultă $A = I$.

b) Dacă I conţine un inversabil a, inversul său este un element $a^{-1} \in A$, iar rezultatul $a^{-1} \cdot a$ este în I. Obţinem $1 \in I$ şi, conform a), $I = A$. □

5.3 Operaţii cu ideale

Fie $(A, +, \cdot)$ un inel unitar şi $Id_s(A)$, $Id_d(A)$, $Id(A)$ mulţimea idealelor sale la stânga, la dreapta, respectiv bilaterale.

Rezultatele care urmează vor fi formulate pentru ideale la stânga ale inelului A, dar sunt valabile şi pentru idealele sale la dreapta, respectiv cele bilaterale.

Propoziţia 5.3.1. *Intersecţia unei familii de ideale la sânga este ideal la stânga. Mai mult, este cel mai mare (în sensul incluziunii) ideal la stânga inclus în fiecare ideal din familia dată.*

Demonstraţie: Fie $\{I_i\}_{i\in K}$ o familie de ideale la stânga ale inelului A, unde K este o mulţime de indici. Notăm $I = \underbrace{\cap}_{i\in K} I_i$. Deoarece fiecare I_i este ideal, avem $0 \in I_i$, deci $0 \in I$.

Fie $a \in A$ şi $x, y \in I$, deci $x, y \in I_i$, $(\forall) i \in K$. Pentru fiecare $i \in K$, rezultă $x+y \in I_i$ şi $a\cdot x \in I_i$ din definiţia idealului (I_i ideal), de unde avem $x+y, a\cdot x \in I$.

Evident I este inclus in fiecare I_i. Fie acum J un alt ideal la stânga al inelului A astfel încât $J \subseteq I_i$, $(\forall) i \in K$. Rezultă $J \subseteq I$, deci I este infimumul familiei de ideale $\{I_i\}_{i\in K}$ în mulţimea parţial ordonată $(Id_s(A), \subseteq)$. □

Fie S o submulţime a inelului unitar A. Conform Propoziţiei anterioare, mulţimea

$$< S >_s = \underbrace{\cap}_{I\subseteq Id_s(A), S\subset I} I.$$

este un ideal la stânga al inelului A. Mai mult, $< S >_s$ este cel mai mic ideal la stânga al lui A care include submulţimea S. Elementele mulţimii S se numesc generatorii idealuluii $< S >_s$. Dacă S este finită, atunci idealul $< S >_s$ se numeşte *finit generat*; în caz contrar, *infinit generat*. Dacă $S = \{x_1, x_2, ..., x_k\}$, atunci idealul la stânga generat de S se mai scrie $< x_1, x_2, ..., x_k >_s$.

Idealul generat de mulţimea vidă este idealul $\{0\}$. Se demonstrează că:

Propoziţia 5.3.2.

$$< S >_s = \{\sum_{i=1}^{m} a_i \cdot x_i / \quad m \in \mathbb{N}, \quad a_i \in A, x_i \in S\},$$

$$< S >_d = \{\sum_{i=1}^{m} x_i \cdot a_i / \quad m \in \mathbb{N}, \quad a_i \in A, x_i \in S\},$$

$$< S >_b = \{\sum_{i=1}^{m} a_i \cdot x_i \cdot b_i / \quad m \in \mathbb{N}, \quad a_i, b_i \in A, x_i \in S\},$$

unde definiţiile idealelor $< S >_d$, $< S >_b$ *sunt analoage celei pentru* $< S >_s$, *considerând însă idealele la dreapta, respectiv cele bilaterale care includ* S.

Alte operaţii cu ideale sunt suma, produsul, radicalul:

Propoziţia 5.3.3. *Dacă* $I, J \in Id_s(A)$, *atunci*

$$I + J = \{x + y/ \quad x \in I, y \in J\},$$

este ideal la stânga al lui A, *numit* ***suma idealelor*** I *şi* J. *Mai mult, este cel mai mic (în sensul incluziunii) ideal din* $Id_s(A)$ *care include* I *şi* J.

Demonstraţie: Deoarece I şi J sunt ideale, ele conţin elementul zero al inelului, iar din $0 = 0 + 0$, avem $0 \in I + J$. Fie $z_1, z_2 \in I + J$, arbitrar alese. Există $x_1, x_2 \in I$ şi $y_1, y_2 \in J$ astfel încât $z_1 = x_1 + y_1$, $z_2 = x_2 + y_2$. Obţinem

$$z_1 + z_2 = (x_1 + y_1) + (x_2 + y_2) = (x_1 + x_2) + (y_1 + y_2) \in I + J,$$

$$a \cdot z_1 = a \cdot (x_1 + y_1) = a \cdot x_1 + a \cdot y_1 \in I + J,$$

din faptul că I, J sunt ideale la stânga. Am obţinut că şi $I + J$ satisface axiomele idealului la stânga.

Evident, $I = \{x + 0| \quad x \in I\} \subset I + J$, $J = \{0 + y| \quad y \in J\} \subset I + J$. A rămas să arătăm că $I + J$ este cel mai mic ideal la stânga care include I şi J.

Fie $K \in Id_s(A)$, $I \subset K$, $J \subset K$. Pentru orice $z \in I + J$, există $x \in I$, $y \in J$ astfel încât $z = x + y$. Dar $x \in I$, $y \in J$ implică $x, y \in K$ şi, deoarece K este ideal, avem $x + y \in K$, de unde $z \in K$, deci $I + J \subset K$. Am obţinut că $I + J$ este supremumul mulţimii $\{I, J\}$ în mulţimea parţial ordonată $(Id_s(A), \subseteq)$. $\square$

Propoziţia 5.3.4. *Dacă* $I, J \in Id_s(A)$, *atunci*

$$I \cdot J = \{\sum_{i=1}^{m} x_i \cdot y_i/ \quad m \in \mathbb{N}, \quad x_i \in I, y_i \in J\},$$

este ideal la stânga al lui A, *numit* ***produsul idealelor*** I *şi* J.

Demonstraţie: Mulţimea $I \cdot J$ definită mai sus conţine toate sumele posibile de produse de câte două elemente din A, primul fiind din I şi al doilea din J. În particular, conţine şi elementul $0 \cdot 0 = 0$. Orice două elemente am alege din $I \cdot J$,

fiecare dintre acestea este o sumă descrisă mai sus. Evident şi suma lor va fi tot o sumă de produse de câte două elemente din A, primul fiind din I şi al doilea din J, deci aparţine lui $I \cdot J$. Pentru orice $a \in A$ şi $z = \sum_{i=1}^{m} x_i \cdot y_i \in I \cdot J$,

$$a \cdot z = a \cdot \sum_{i=1}^{m} x_i \cdot y_i = \sum_{i=1}^{m} a \cdot x_i \cdot y_i \in I \cdot J,$$

deoarece $a \cdot x_i \in I$, $(\forall) i = \overline{1, m}$. □

Exemplul 5.3.1. *În inelul numerelor întregi, fie idealele $a\mathbb{Z}$, $b\mathbb{Z}$, generate de numerele a şi b. Idealele intersecţie, respectiv sumă sunt generate de cel mai mic multiplu comun $[a, b]$, respectiv de cel mai mare divizor comun (a, b) al celor două numere, (vezi şi Propoziţia 3.1.8). Idealul produs $a\mathbb{Z} \cdot b\mathbb{Z}$ este generat de produsul numerelor a şi b (verificaţi!).*

Propoziţia 5.3.5. *Dacă A este un inel comutativ şi I un ideal al său, atunci mulţimea*

$$\sqrt{I} = \{x \in A / \quad (\exists) n \in \mathbb{N}, \quad x^n \in I\},$$

*este ideal al lui A, numit **radicalul idealului** I. Idealul $\sqrt{0}$ este mulţimea elementelor **nilpotente** ale inelului A.*

Demonstraţie:: Trebuie verificate condiţiile din definiţia idealului. Avem $0^1 \in I$ deoarece I este ideal, deci $0 \in \sqrt{I}$.

Fie $x, y \in \sqrt{I}$, deci există m, n naturale astfel încât $x^n, y^m \in I$. Inelul A fiind comutativ, calculăm cu binomul lui Newton:

$$(x+y)^{m+n} = \sum_{i=0}^{n+m} C_{n+m}^{i} x^{n+m-i} y^i = \sum_{i=0}^{m} C_{n+m}^{i} x^{n+m-i} y^i + \sum_{j=m+1}^{n+m} C_{n+m}^{j} x^{n+m-j} y^j.$$

Pentru orice $i \leq m$, $x^{n+m-i} = x^n \cdot x^{m-i}$ este un produs în A, dintre un element din I (x^n) şi un element din A, deci este un element din idealul I. De asemenea suma $\sum_{i=0}^{m} C_{n+m}^{i} x^{n+m-i} y^i$ este în I. Analog suma $\sum_{j=m+1}^{n+m} C_{n+m}^{j} x^{n+m-j} y^j$ este în I, fiecare termen al său conţinând factorul y^m. Rezultă aşadar $x + y \in \sqrt{I}$.

În final, fie $a \in A$ şi $x \in I$, arbitrar alese. Există n natural cu $x^n \in I$, care din comutativitatea lui A conduce la

$$(a \cdot x)^n = a^n \cdot x^n \in I.$$

□

Observaţia 5.3.1. *1. Elementele nilpotente ale unui inel sunt importante mai ales în studiul inelelor de polinoame cu coeficienţi în acel inel.*

2. Deoarece un element nilpotent nenul este şi divizor al lui 0*, într-un inel integru* $\sqrt{0} = \{0\}$*. Dacă inelul nu e integru, atunci există şi alte elemente nilpotente. De exemplu, în inelul* $(\mathbb{Z}_8, +, \cdot)$*,* $\sqrt{0} = \{\hat{0}, \hat{2}, \hat{4}, \hat{6}\}$*.*

3. Este evident că $I \subseteq \sqrt{I}$*.*

4. În inelul numerelor întregi, avem $\sqrt{p\mathbb{Z}} = p\mathbb{Z}$ *şi* $\sqrt{p^n\mathbb{Z}} = p\mathbb{Z}$*, pentru orice număr prim* p*.*

5. Dacă $n = p_1^{a_1}p_2^{a_2}...p_k^{a_k}$*, atunci elementele nilpotente din inelul* $\mathbb{Z}_n$ *sunt multiplii lui* $\hat{a} = \widehat{p_1p_2...p_k}$*, deoarece orice element de forma* $\widehat{ma}$ *ridicat la puterea* $\max\{a_1, a_2, ..., a_k\}$ *este* $\hat{0}$*.*

Propoziţia 5.3.6. *Fie* A *un inel comutativ şi* I*,* J *două ideale ale sale. Mulţimea*

$$I : J = \{x \in A| \quad a \cdot x \in I, (\forall)a \in J\},$$

este ideal în A*, numit* ***câtul*** *idealului* I *prin* J*.*

Demonstraţie: Deoarece I este ideal, el conţine elementul zero. Dar $0 = a \cdot 0$, pentru orice $a \in J$, deci $0 \in I : J$.

Fie $x, y \in I : J$. Pentru orice $a \in J$, avem $a \cdot x, a \cdot y \in I$ şi

$$a \cdot (x + y) = a \cdot x + a \cdot y \in I,$$

adică $x + y \in I : J$.

Fie $x \in I : J$ şi $b \in A$, arbitrar alese. Pentru orice $a \in J$ are loc relaţia $a \cdot b \in J$, de unde avem şi

$$a \cdot (b \cdot x) = (a \cdot b) \cdot x \in I,$$

aşadar $b \cdot x \in I : J$. □

5.4 Morfisme de inele şi corpuri

Fie $(A, +, \cdot)$, $(B, +, \cdot)$ două inele oarecare, nu neapărat unitare.

Definiţia 5.4.1. *O aplicaţie $f : A \to B$ care verifică*

$$f(x+y) = f(x) + f(y), \quad f(x \cdot y) = f(x) \cdot f(y), \quad (\forall)x, y \in A,$$

se numeşte ***morfism de inele****. Dacă în plus inelele sunt unitare şi $f(1) = 1$, atunci f se numeşte* ***morfism unitar de inele****.*

Dacă A şi B sunt corpuri, atunci un morfism unitar de inele $f : A \to B$ se numeşte ***morfism de corpuri****.*

Ca şi în cazul grupurilor, morfismele $f : A \to A$ se numesc endomorfismele inelului A.

Exemplul 5.4.1. *a) $f : \mathbb{Z} \to \mathbb{Q}$, $f(k) = k$, $(\forall)k \in \mathbb{Z}$, este morfism unitar injectiv de inele.*

b) Pentru orice inel unitar $(A, +, \cdot)$, şi k un număr întreg, notăm $k1 = \underbrace{1 + 1 + ... + 1}_{k}$, pentru $k > 0$, $k1 = 0$ pentru $k = 0$ şi $k1 = \underbrace{-1 - 1 - ... - 1}_{-k}$, pentru $k < 0$. Funcţia

$$f : \mathbb{Z} \to A, \quad f(k) = k1, \quad (\forall)k \in \mathbb{Z},$$

este morfism unitar de inele. Mai mult, acest morfism este unic determinat de $f(1) = 1$.

c) Fie $(A, +, \cdot)$, $(B, +, \cdot)$ două inele oarecare. Funcţia

$$f : A \to B, \quad f(x) = 0, \quad (\forall)x \in A,$$

este morfism (neunitar) de inele, numit ***morfismul nul****, iar funcţia identică, $\mathbf{1}_A : A \to A$, este morfism (unitar, dacă inelul A este unitar), de inele, numit* ***morfismul identic****.*

Propoziţia 5.4.1. *Dacă $f : A \to B$ este morfism de inele, atunci au loc următoarele egalităţi:*

$$f(0) = 0, \quad f(-x) = -f(x), \quad f(x-y) = f(x) - f(y),$$

pentru orice $x, y \in A$.

Dacă $f : A \to B$ este morfism de unitar de inele, atunci, pe lângă cele de mai sus avem şi

$$f(x^{-1}) = (f(x))^{-1}, \quad (\forall)x \in U(A).$$

Demonstraţie Deoarece f este morfism de inele, au loc următoarele şiruri de egalităţi:

$$f(0) = f(0+0) = f(0) + f(0) \Rightarrow f(0) = 0,$$

$$0 = f(0) = f(x + (-x)) = f(x) + f(-x) \Rightarrow f(-x) = -f(x),$$

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

În cazul morfismului unitar pentru orice element inversabil x din domeniul de definiţie, avem:

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

deci $f(x) \in U(B)$. □

Un morfism de inele $f : A \to B$ se numeşte *izomorfism* dacă există un morfism de inele $g : B \to A$ astfel încât $g \circ f = \mathbf{1}_A$ şi $f \circ g = \mathbf{1}_B$. Ca şi în teoria grupurilor, un endomorfism bijectiv se numeşte *automorfism*. Se verifică imediat, analog cu demonstraţiile Propoziţiilor 2.4.4 şi 2.4.5 următoarele afirmaţii:

Propoziţia 5.4.2. *Compunerea a două morfisme de inele este morfism de inele.*

Propoziţia 5.4.3. *Un morfism unitar de inele este izomorfism dacă şi numai dacă este funcţie bijectivă.*

Următorul rezultat stabileşte modul de comportare a subinelelor şi idealelor la morfisme de inele:

Teorema 5.4.1. *Fie $f : A \to B$ un morfism de inele şi $A' \subseteq A$, $B' \subseteq B$, subinele, $I \in Id_s(A)$ ($Id_d(A)$, $Id_b(A)$), $J \in Id_s(B)$ (respectiv $Id_d(B)$, $Id_b(B)$). Sunt adevărate următoarele afirmaţii:*

a) $f(A')$ este subinel al inelului B şi $f^{-1}(B')$ este subinel al inelului A.

b) $f^{-1}(J)$ este ideal la stânga al lui A (respectiv la dreapta sau bilateral, după cum este şi J), şi $Ker(f) \subseteq f^{-1}(J)$.

c) Dacă f este surjectiv, atunci $f(I)$ este ideal al inelului B, de acelaşi tip cu idealul I.

Demonstraţie: a) Pentru a demonstra că submulţimile date sunt subinele, folosim caracterizarea din Propoziţia 5.2.1.

Pentru orice $y_1, y_2 \in f(A')$, există $x_1, x_2 \in A'$ astfel încât $y_1 = f(x_1)$, $y_2 = f(x_2)$. Din proprietatea de morfism a lui f şi deoarece A' este subinel (prin urmare $x_1 - x_2 \in A'$ şi $x_1 \cdot x_2 \in A'$), avem:

$$y_1 - y_2 = f(x_1 - x_2) \in f(A'),$$

$$y_1 \cdot y_2 = f(x_1 \cdot x_2) \in f(A').$$

Rezultă $f(A')$ subinel în B.

Fie $x_1, x_2 \in f^{-1}(B')$, arbitrar alese. Avem $f(x_1), f(x_2) \in B'$, f e morfism de inele şi B' este subinel, aşadar

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

$$f(x_1 \cdot x_2) = f(x_1) \cdot f(x_2) \in B' \Rightarrow x_1 \cdot x_2 \in f^{-1}(B').$$

Am obţinut $f^{-1}(B')$ subinel în A.

b) Ştim că $0 = f(0)$ se află în idealul J, deci $0 \in f^{-1}(J)$. Fie $x_1, x_2 \in f^{-1}(J)$ şi $a \in A$, arbitrar alese. Din f morfism şi J ideal în B, avem

$$f(x_1 + x_2) = f(x_1) + f(x_2) \in J \Rightarrow x_1 + x_2 \in f^{-1}(J),$$

$$f(a \cdot x_1) = f(a) \cdot f(x_1) \in J \Rightarrow a \cdot x_1 \in f^{-1}(J),$$

deci $f^{-1}(J)$ ideal în A.

Pentru orice element $x \in Ker(f)$, $f(x) = 0 \in J$, de unde rezultă $x \in f^{-1}(J)$.

c) Ştim că elementul zero al inelului A se află în idealul I, deci $0 = f(0) \in f(I)$.

Fie $y_1, y_2 \in f(I)$ şi $b \in B$, arbitrar alese. Există $x_1, x_2 \in I$ astfel încât $y_1 = f(x_1)$, $y_2 = f(x_2)$ şi, din ipoteza de surjectivitate a lui f, există $a \in A$ cu $f(a) = b$. Din propietatea de morfism a lui f şi din faptul că I este ideal, rezultă

$$y_1 + y_2 = f(x_1 + x_2) \in f(I),$$

$$b \cdot y_1 = f(a \cdot x_1) \in f(I),$$

adică $f(I)$ este ideal. □

Observaţia 5.4.1. *Din Teorema 5.4.1 rezultă următoarele consecinţe:*
a) Nucleul morfismului f

$$Kerf = f^{-1}(\{0\}) = \{x \in A/ \quad f(x) = 0\},$$

este subinel, dar şi ideal bilateral în A, deoarece mulţimea $\{0\}$ este subinel şi ideal bilateral în B.

b) Imaginea morfismului f, $Imf = f(A)$ este subinel în B, iar dacă f este surjectivă este ideal, fiind chiar idealul total B.

Tot o consecinţă a Teoremei 5.4.1 este şi:

Propoziţia 5.4.4. *Dacă morfismul f este surjectiv, atunci următoarele corespondenţe sunt inverse una celeilate, deci bijective:*

$$\Phi : [Ker(f), A]_s \to Id_s(B), \quad \Phi(I) = f(I), \quad (\forall)I \in [Ker(f), A]_s,$$

$$\Psi : Id_s(B) \to [Ker(f), A]_s, \quad \Psi(J) = f^{-1}(J), \quad (\forall)J \in Id_s(B),$$

unde prin $[I, A]_s$ înţelegem toate idealele la stânga ale lui A, care conţin idealul I.

Ca şi la grupuri, se poate demonstra că morfismul f de inele este injectiv dacă şi numai dacă $Kerf = \{0\}$. Are loc şi:

Propoziţia 5.4.5. *Orice morfism de corpuri este injectiv.*

Demonstraţie: Fie $f : A \to B$ un morfism de corpuri, deci de inele unitare. Nucleul său este ideal al domeniului de definiţie. Dar un corp are doar idealele improprii (vezi Propoziţia 5.2.3), iar morfismul nul nu este morfism de corpuri (este necesar $f(1) = 1$). Rezultă $Kerf$ este idealul nul, deci f injectiv. □

5.5 Inelul factor

Fie $(A, +, \cdot)$ un inel şi I un ideal bilateral al său. Un astfel de ideal există întotdeauna: $\{0\}$, sau A, sau nucleul unui morfism cu domeniul de definiţie A.

Din definiţia idealului, grupul $(I, +)$ este subgrup normal în grupul abelian $(A, +)$, deci există grupul factor $(A/I, +)$, unde

$$A/I = \{x + I/ \quad x \in A\}, \quad x + I = \{y \in A/ \quad y - x \in I\} = \{x + a/ \quad a \in I\}.$$

Adunarea elementelor din mulţimea cât A/I este definită prin $(x+I)+(y+I) = (x+y)+I$ şi dă acestei mulţimi structură de grup, cu elementul neutru I, (vezi secţiunea *Grupul factor*).

Vom defini pe această mulţime încă o operaţie, notată multiplicativ:

$$(x+I)\cdot(y+I) = (x\cdot y)+I,$$

folosind înmulţirea din inelul A.

Propoziţia 5.5.1. *Operaţia multiplicativă definită mai sus nu depinde de reprezentanţi şi* $(A/I, +, \cdot)$ *este inel, numit* ***inelul factor*** *al inelului* A *prin idealul* I*.*

Demonstraţie: Fie $x' \in x+I$ şi $y' \in y+I$, deci $x'-x, y'-y \in I$. Calculăm

$$x'\cdot y' - x\cdot y = x'\cdot y' - x'\cdot y + x'\cdot y - x\cdot y = x'\cdot(y'-y) + (x'-x)\cdot y,$$

care este un element din I, deoarece I este ideal, deci produsul unui element al său cu orice element din A este în I.

Vom demonstra că operaţia "$\cdot$" pe A/I dă grupului $(A/I, +)$ structură de inel. Pentru orice elemente $x+I, y+I, z+I$ din A/I, au loc:

$$[(x+I)\cdot(y+I)]\cdot(z+I) = [(x\cdot y)+I]\cdot(z+I) = [(x\cdot y)\cdot z]+I = [x\cdot(y\cdot z)]+I =$$

$$= (x+I)\cdot[(y+I)\cdot(z+I)],$$

din asociativitatea înmulţirii în A, deci "$\cdot$" asociativă în A/I.

Dacă A este inel unitar, atunci

$$(1+I)\cdot(x+I) = x+I = (x+I)\cdot(1+I),$$

unde 1 este elementul unitate în A, deci $1+I$ este element neutru la înmulţirea din A/I.

$$[(x+I)+(y+I)]\cdot(z+I) = [(x+y)+I]\cdot(z+I) = [(x+y)\cdot z]+I = (x\cdot z+y\cdot z)+I =$$

$$= [(x\cdot z)+I]+[(y\cdot z)+I] = (x+I)\cdot(z+I)+(y+I)\cdot(z+I),$$

din distributivitatea operaţiei "$\cdot$" faţă de "$+$" în inelul A şi din definiţiile operaţiilor în A/I. Analog se verifică distributivitatea la stânga. □

Observaţia 5.5.1. *a) Dacă inelul A este comutativ, atunci şi inelul factor este comutativ.*

b) Aplicaţia $\pi : A \to A/I$ definită prin $\pi(x) = x + I$, $(\forall)x + I \in A/I$, este morfism surjectiv de inele, numit ***surjecţia canonică****.*

c) O întrebare firească ar fi de ce nu construim inelul factor printr-un subinel al lui A, un subinel fiind de asemenea subgrup normal. Răspunsul este: operaţia de înmulţire definită mai sus nu ar mai fi independentă de alegerea reprezentanţilor.

Exemplul 5.5.1. *a) Inelul factor $A/\{0\}$, este izomorf cu A, iar inelul factor A/A este izomorf cu $\{0\}$.*

b) Fie I un ideal al inelului numerelor întregi $\mathbb{Z}$. Se ştie (Propoziţia 5.2.4) că I este ideal principal, deci există $n \in \mathbb{N}$ astfel încât $I = n\mathbb{Z}$. Inelul factor $\mathbb{Z}/I$ este chiar inelul claselor de resturi modulo n, deoarece relaţia de echivalenţă $\equiv (modI)$ coincide cu relaţia de congruenţă modulo n, (vezi şi Exemplul 3.5.1).

O noţiune necesară mai ales în studiul corpurilor este cea definită mai jos:

Definiţia 5.5.1. *Un ideal I al inelului comutativ A se numeşte* ***ideal maximal*** *dacă este diferit de A şi $[I, A] = \{I, A\}$.*

Propoziţia 5.5.2. *Fie A un inel comutativ şi I un ideal propriu al său. Inelul factor A/I este corp dacă şi numai dacă idealul I este maximal.*

Demonstraţie: Ştim din Propoziţia 5.2.3 că un inel este corp dacă şi numai dacă are doar două ideale.

Aplicând Propoziţia 5.4.4 surjecţiei canonice $\pi : A \to A/I$, între mulţimile $Id(A/I)$ şi $[Ker\pi, A]$ există o bijecţie, deci sunt cardinal echivalente. Avem şi $Ker\pi = I$, deci are loc şirul de echivalenţe:

$$A/Icorp \Leftrightarrow |Id(A/I)| = 2 \Leftrightarrow |[I, A]| = 2 \Leftrightarrow Imaximal.$$

□

Observaţia 5.5.2. *Orice ideal maximal al inelului $(A, +, \cdot)$ este subgrup maximal al grupului $(A, +)$ (vezi Definiţia 3.4.2).*

5.6 Teoreme de izomorfism pentru inele

În acest paragraf vom prezenta teorema fundamentală de izomorfism pentru inele folosind rezultatele din teoria grupurilor. De aceea sugerăm revederea noţiunilor şi rezultatelor din paragraful *Teoreme de izomorfism pentru grupuri*.

Teorema 5.6.1. *[Teorema fundamentaă de izomorfism pentru inele]*
Fie $f : A \to B$ un morfism de inele. Inelul factor $A/Kerf$ este izomorf cu subinelul Imf al lui B.

Demonstraţie: Considerând grupurile $(A, +)$, $(B, +)$, din teorema de izomorfism pentru grupuri (Teorema 3.5.1) aplicată morfismului de grupuri $f : A \to B$, rezultă că funcţia

$$\varphi : A/Kerf \to Imf, \quad \varphi(x + Kerf) = f(x), \quad (\forall)x \in A,$$

este izomorfism de grupuri. Aceasta verifică şi

$$\varphi((x + Kerf) \cdot (y + Kerf)) = \varphi((x \cdot y) + Kerf) = f(x \cdot y) = f(x) \cdot f(y) =$$

$$= \varphi(x + Kerf) \cdot \varphi(y + Kerf), \quad (\forall)x, y \in A,$$

deci φ este izomorfism de inele. □

Observaţia 5.6.1. *Surjecţia canonică $\pi : A \to A/Kerf$ satisface egalitatea*

$$\varphi \circ \pi = f.$$

Teorema 5.6.2. *[Prima teoremă de izomorfism pentru inele]*
Fie morfismul surjectiv de inele $f : A \to B$ şi I un ideal bilateral al lui A care include $Kerf$. Inelele factor A/I şi $B/f(I)$ sunt izomorfe.

Demonstraţie: Definim funcţia $\zeta : A \to B/f(I)$, prin

$$\zeta(x) = (\pi \circ f)(x) = f(x) + f(I),$$

unde π este surjecţia canonică a inelului factor $B/f(I)$, adică ζ asociază fiecărui element din A clasa de echivalentă din $B/f(I)$ a imaginii sale prin f. Deoarece f şi π sunt ambele morfisme surjective, la fel este şi ζ. Deoarece $Kerf \subseteq I$, determinăm

$$Ker\zeta = \{x \in A| \quad f(x) \in f(I)\} = \{x \in A| \quad (\exists)y \in I, \quad f(x) = f(y)\} =$$

$$\{x \in A| \quad (\exists) y \in I, \quad x - y \in Kerf\} = \{x \in A| \quad x \in I\} = I.$$

Aplcând acum teorema fumdamentală de izomorfism morfismului de inele ζ, obţinem izomorfismul dintre inelele factor A/I şi $B/f(I)$. □

Exemplul 5.6.1. *În inelul $(\mathbb{Z}, +, \cdot)$, idealul $n\mathbb{Z}$ este bilateral şi $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, iar $p : \mathbb{Z} \to \mathbb{Z}_n$ este surjecţia canonică. Conform Propoziţiei 5.4.4, există o bijecţie între $Id(\mathbb{Z}_n)$ şi mulţimea idealelor lui $\mathbb{Z}$ care conţin $Kerp = n\mathbb{Z}$. Un astfel de ideal este de forma $m\mathbb{Z}$, deoarece inelul numerelor întregi este principal şi incluziunea $n\mathbb{Z} \subseteq m\mathbb{Z}$ implică $m|n$.*

Rezultă că toate idealele lui $\mathbb{Z}_n$ sunt de forma $(m\mathbb{Z})/(n\mathbb{Z})$, cu m divizor al lui n. Aplicând prima teoremă de izomorfism morfismului surjectiv p şi idealului $m\mathbb{Z}$, rezultă

$$\mathbb{Z}/(m\mathbb{Z}) \approx \mathbb{Z}_n/(\widehat{m}\mathbb{Z}_n),$$

adică inelul factor al inelului $\mathbb{Z}_n$ prin idealul generat de $\widehat{m}$ în $\mathbb{Z}_n$ este izomorf cu $\mathbb{Z}_m$.

Teorema 5.6.3. *[A doua teoremă de izomorfism]*

Fie A un inel, A' un subinel şi I un ideal bilateral al său. Atunci mulţimea $A' + I = \{a' + x/ \quad a' \in A', x \in A\}$ este un subinel al lui A, care conţine I, iar $A' \cap I$ este un ideal bilateral al lui A' şi are loc izomorfismul de inele

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

Demonstraţie: Deoarece A' este subinel şi I este ideal în inelul A, ambele conţin elementul 0 şi sunt parte stabilă la adunare. Rezultă că $A' + I$ conţine 0 şi este parte stabilă la adunare. Mai trebuie probat faptul că este parte stabilă şi la înmulţire. Fie $a + x, b + y \in A' + I$, cu $a, b \in A'$ şi $x, y \in I$. Calculăm prin distributivitate

$$(a + x) \cdot (b + y) = a \cdot b + a \cdot y + x \cdot b + x \cdot y.$$

Subinelul A' este parte stabilă la înmulţire, deci $a \cdot b \in A'$. Idealul I conţine elementele x, y, deci şi produsele acestora cu orice elemente din A, de unde $a \cdot y + x \cdot b + x \cdot y \in I$. Am obţinut $(a + x) \cdot (b + y) \in A' + I$, deci $A' + I$ este subinel în inelul A. Evident, $I \subseteq A' + I$.

Analog se verifică faptul că $A' \cap I$ este ideal bilateral în A'.

Fie funcţia $f : A' \to A/I$ restricţia surjecţiei canonice $\pi : A \to A/I$ la A'. Evident este morfism de inele.

$$Imf = \pi(A') = \{a' + I| \quad a' \in A'\} = (A' + I)/I,$$

deoarece I este ideal în $A' + I$, nu în A' (în general I nu este submulţime a lui A').

$$Kerf = \{a' \in A'| \quad \pi(a') = I\} = \{a' \in A'| \quad a' \in I\} = A' \cap I.$$

Aplicând Teorema fundamentală de izomorfism morfismului f obţinem izomorfismul cerut. □

Exemplul 5.6.2. *Fie n_1, n_2 două numere întregi, d cel mai mare divizor comun şi m cel mai mic multiplu comun al lor. Ştim că $n_1\mathbb{Z}$ şi $n_2\mathbb{Z}$ sunt atât subinele, cât şi ideale ale lui $\mathbb{Z}$, conform Exemplului 5.2.1 c) şi Propoziţiei 5.2.4. Mai mult, din Propoziţia 3.1.8, avem $n_1\mathbb{Z} + n_2\mathbb{Z} = d\mathbb{Z}$ şi $n_1\mathbb{Z} \cap n_2\mathbb{Z} = m\mathbb{Z}$. Conform celei de-a doua teoreme de izomorfism pentru inele, inelele factor $d\mathbb{Z}/n_2\mathbb{Z}$ şi $n_1\mathbb{Z}/m\mathbb{Z}$ sunt izomorfe. În particular, aceasta înseamnă că sunt echipotente, de unde avem binecunoscuta relaţie aritmetică*

$$n_1 \cdot n_2 = d \cdot m.$$

5.7 Caracteristica unui inel

Fie $(A, +, \cdot)$ un inel unitar şi 0, 1 elementele neutre la adunarea, respectiv înmulţirea în A.

Definiţia 5.7.1. *Inelul A se numeşte de caracteristică pozitivă dacă există $n \in \mathbb{N}^*$ astfel încât*

$$n1 = \underbrace{1 + 1 + ...1}_{n} = 0.$$

Cel mai mic număr n cu proprietatea de mai sus se numeşte ***caracteristica inelului*** *A şi se notează $car(A)$.*

În caz contrar, numim inelul A de caracteristică nulă şi scriem $car(A) = 0$.

Exemplul 5.7.1. *$car(\mathbb{Z}) = 0$, $car(\mathbb{R}) = 0$, $car(\mathbb{Z}_n) = n$.*

Propoziţia 5.7.1. *Caracteristica unui inel integru de caracteristică pozitivă este un număr prim.*

Demonstraţie: Fie $car(A) = n > 0$, unde A este un inel integru. Presupunem prin absurd că n nu este prim, deci se poate scrie $n = m \cdot r$, cu m, r divizori proprii ai lui n. Din definiţia caracteristicii unui inel, avem

$$0 = n1 = \underbrace{1 + 1 + ...1}_{n} = \underbrace{\underbrace{1 + 1 + ... + 1}_{m} + \underbrace{1 + 1 + ...1}_{m} + ... + \underbrace{1 + 1 + ... + 1}_{m}}_{r},$$

în care, dacă dăm factor comun $\underbrace{1 + 1 + ... + 1}_{m}$, obţinem

$$0 = (\underbrace{1 + 1 + ... + 1}_{m}) \cdot (\underbrace{1 + 1 + ... + 1}_{n}) = m1 \cdot r1.$$

Dar inelul este integru, deci $m1 = 0$ sau $r1 = 0$, ceea ce contrazice minimalitatea lui $n = car(K)$ (evident orice divizor propriu al unui număr este mai mic strict decât acesta). Rezultă că presupunerea făcută este falsă, deci $car(K) > 0$ este număr prim. □

Observaţia 5.7.1. *Conform Propoziţiei 5.1.3, orice corp este inel integru, deci caracteristica unui corp de caracteristică pozitivă este număr prim.*

Fie f unicul morfism de inele din Exemplul 5.4.1 b)

$$f : \mathbb{Z} \to A, \quad f(k) = k1, \quad (\forall)k \in \mathbb{Z}.$$

Deoarece nucleul acestui morfism,

$$Kerf = \{n \in \mathbb{Z} | \quad n1 = 0\},$$

este ideal în inelul numerelor întregi, rezultă conform Propoziţiei 5.2.4 că este fie idealul nul, fie generat de cel mai mic element pozitiv din $Kerf$. Putem spune că f este injectiv dacă şi numai dacă $car(A) = 0$, respectiv f nu este injectiv dacă şi numai dacă inelul A este de caracteristică pozitivă. În acest ultim caz, $Kerf$ este generat de $car(K)$.

În cazul corpurilor, caracteristica corpului permite identificarea celui mai mic subcorp al său.

Fie $(K, +, \cdot)$ un corp. Amintim că $Id(K) = \{\{0\}, K\}$ şi că o submulţime $L \subseteq K$, nevidă este subcorp al lui K dacă conţine elementele zero şi 1 ale corpului K şi $(\forall)x, y \in L$, $x - y \in L$ şi $x \cdot y^{-1} \in L$. Intersecţia unei familii de subcorpuri este subcorp.

Definiţia 5.7.2. *Un corp care nu are alte subcorpuri în afară de el însuşi se numeşte* ***corp prim****.*

Exemplul 5.7.2. *a) Corpul numerelor raţionale $(\mathbb{Q}, +, \cdot)$ este corp prim. Într-adevăr, fie L un subcorp al corpului numerelor raţionale $\mathbb{Q}$. Din $0, 1 \in L$ rezultă că $\mathbb{Z} \subset L$. Pentru orice $m, n \in \mathbb{Z}$, $m \neq 0$, din L subcorp rezultă $n \cdot m^{-1} \in L$, deci $\mathbb{Q} \subset L$, de unde $\mathbb{Q} = L$.*

b) Corpul claselor de resturi $(\mathbb{Z}_p, +, \cdot)$, cu p număr prim este corp prim, deoarece orice subcorp al său este în particular subgrup al său şi, conform Propoziţiei 3.4.4, $(\mathbb{Z}_p, +)$ este grup simplu.

Fie $(K, +, \cdot)$ un corp arbitrar şi K_0 subcorpul obţinut prin intersecţia tuturor subcorpurilor lui K. Corpul K_0 este corp prim deoarece un subcorp al său, L, ar fi subcorp şi al lui K, deci termen al intersecţiei K_0, adică $K_0 \subseteq L$. Dar aveam şi $L \subseteq K_0$, deci K_0 admite un singur subcorp, el însuşi. Corpul prim obţinut mai sus se numeşte **subcorpul prim** al lui K. De aici rezultă că orice corp conţine ca subcorp un corp prim.

Propoziţia 5.7.2. *Fie K_0 un corp prim. Dacă $car(K_0) = 0$, atunci K_0 este izomorf cu corpul numerelor raţionale $\mathbb{Q}$, iar dacă K_0 este de caracteristică pozitivă p, atunci este izomorf cu $(\mathbb{Z}_p, +, \cdot)$.*

Demonstraţie: Considerăm $f : \mathbb{Z} \to K_0$, unicul morfism de inele de la $\mathbb{Z}$ la K_0, descris mai sus. Am văzut că nucleul său este determinat de caracteristica corpului.

Dacă $car(K_0) = 0$, atunci $Kerf = \{0\}$ şi f este injectiv, deci $\mathbb{Z}$ este izomorf cu un subinel $A_0 = f(\mathbb{Z})$ al lui K_0. Cum K_0 este corp, rezultă că mulţimea

$$\bar{A_0} = \{x \cdot y^{-1} | \quad x \in A_0, y \in A_0^*\},$$

este un subcorp al lui K_0, izomorf cu $\mathbb{Q}$. Dar K_0 este corp prim, deci $K_0 = \bar{A_0}$.

Dacă $car(K_0) = p > 0$, atunci Teorema fundamentală de izomorfism aplicată morfismului f conduce la $Imf \approx \mathbb{Z}_p$. Deoarece p este prim, rezultă $\mathbb{Z}_p$ corp, deci Imf este subcorp al corpului prim K_0. Obţinem $K_0 = Imf$. □

Observaţia 5.7.2. *O consecinţă a Propoziţiei 5.7.2 este că orice corp prim este comutativ.*

Din Propoziţia 5.7.2 rezultă:

Teorema 5.7.1. *Orice corp de caracteristică* 0 *conţine un subcorp prim izomorf cu* $(\mathbb{Q}, +, \cdot)$.

Orice corp de caracteristică pozitivă p *conţine un subcorp prim izomorf cu* $(\mathbb{Z}_p, +, \cdot)$.

Observaţia 5.7.3. *O altă exprimare a enunţului din Teorema 5.7.1, des utilizată, este:*

Orice corp de caracteristică zero este o extindere a corpului numerelor raţionale.

Orice corp de caracteristică pozitivă p *este o extindere a corpului claselor de resturi modulo* p.

Propoziţia 5.7.3. *Orice corp finit este de caracteristică pozitivă.*

Demonstraţie: Fie K un corp finit. Presupunem prin absurd că este de caracteristică 0. Din Teorema 5.7.1, rezultă că este o extindere a corpului numerelor, raţionale, contradicţie cu faptul că este finit. □

Propoziţia 5.7.4. *Caracteristica unui subcorp este aceeaşi cu caracteristica corpului.*

Demonstraţie: Fie L un subcorp al corpului K, de caracteristică p. Evident, elementele 0 şi 1 ale subcorpului coincid cu cele ale corpului.

Dacă $p = 0$, atunci nu există niciun număr natural nenul n astfel încât $n1 = 0$. Acest fapt e valabil şi în L, deci nu se poate ca L să fie de caracteristică pozitivă, de unde avem $car(L) = 0$.

Dacă $p > 0$, atunci 1 adunat cu el însuşi de p ori este 0 atât în K, cât şi în L, deci şi L este de caracteristică pozitivă. Fie $car(L) = q > 0$. Avem $\underbrace{1 + 1 + ... + 1}_{q} = 0$ şi $\underbrace{1 + 1 + .. + 1}_{p} = 0$. Dacă presupun $p > q$, atunci există $0 < r < q$, natural, restul împărţirii lui p prin q şi din cele două egalităţi de mai sus rezultă $r1 = 0$, ceea ce contrazice minimalitatea lui $q = car(L)$. Analog se exclude cazul $q > p$, deci obţinem $car(L) = car(K)$. □

Observaţia 5.7.4. *Se poate demonstra, folosind teoria spaţiilor vectoriale, că orice corp finit are cardinalul o putere a caracteristicii sale. Mai mult, dacă corpul K de caracteristică pozitivă p are p^n elemente, atunci un subcorp al său are p^m elemente, cu m un divizor al lui n.*

Deoarece probarea următorului rezultat necesită cunoştinţe despre polinoame ciclotomice, anunţăm fără demonstraţie un rezultat celebru referitor la corpurile finite.

Teorema 5.7.2 (Wedderburn)**.** *Orice corp finit este comutativ.*

Propoziţia 5.7.5. *Fie $(K, +, \cdot)$ un corp cu p^n elemente, p număr prim. Atunci $car(K) = p$ şi*

$$(x + y)^p = x^p + y^p, \quad , (\forall)x, y \in K.$$

Demonstraţie: Corpul K fiind finit, este comutativ şi de caracteristică pozitivă, fie $car(K) = q$. Conform Observaţiei anterioare, $|K| = q^m$, de unde rezultă $q^m = p^n$. Dar p şi q sunt numere prime, deci $p = q$.

Calculăm cu binomul lui Newton

$$(x + y)^p = \sum_{k=0}^{p} C_p^k x^{p-k} y^k.$$

Numărul p este prim şi pentru orice $k = \overline{1, p-1}$, avem

$$C_p^k = \frac{(p-k+1)(p-k+2)....p}{k!} \in \mathbb{N},$$

iar factorii din $k!$ sunt numere naturale nenule mai mici decât p, deci prime cu p. Prin urmare factorul p de la numărătorul fracţiei C_p^k nu se simplifică, adică p divide C_p^k, $(\forall)k = \overline{1, p-1}$.

Numărul natural p fiind caracteristica lui K, orice $z \in K$ verifică $\underbrace{z + z + .. + z}_{p} =$ 0, aşadar termenii $C_p^k x^{p-k} y^k$ sunt nuli, $(\forall)k = \overline{1, p-1}$. Am obţinut rezultatul cerut. Mai mult, aplicaţia

$$f : K \to K, \quad f(x) = x^p, \quad (\forall)x \in K,$$

este endomorfism al corpului K. □

5.8 Exemple remarcabile de inele şi corpuri

5.8.1 Inel booleean

Definiţia 5.8.1. *Inelul* $(A, +, \cdot)$ *se numeşte* ***booleean*** *dacă* $x^2 = x$, $(\forall)x \in A$.

Exemplul 5.8.1. *a) Inelul* $(\mathbb{Z}_2, +, \cdot)$ *este booleean.*

b) Pentru orice mulţime A*, tripletul* $(\boldsymbol{P}(A), \Delta, \cap)$ *este un inel booleean, unde* $\boldsymbol{P}(A)$ *este mulţimea părţilor mulţimii* A *şi* Δ *este diferenţa simetrică a mulţimilor.*

Propoziţia 5.8.1. *Dacă* $(A, +, \cdot)$ *este un inel booleean, atunci:*

a) $x + x = 0$, $(\forall)x \in A$ *şi este comutativ.*

b) Nu există inele booleene cu număr impar de elemente.

c) Dacă inelul A *este unitar, atunci* $U(A) = \{1\}$.

d) Relaţia $x \leq y$ *dacă şi numai dacă* $x = x \cdot y$ *este o relaţie de ordine pe* A *în care* 0 *este cel mai mic element. Dacă* A *este unitar, atunci* 1 *este cel mai mare element.*

e) Pentru orice $x, y \in A$, $inf\{x, y\} = x \cdot y$, $sup\{x, y\} = x + y + x \cdot y$, *în raport cu relaţia de ordine definită la punctul d).*

f) Pentru orice $x \in A$ *elementul* $x' = 1 + x$ *satisface relaţiile;* $inf\{x, x'\} = 0$, $sup\{x, x'\} = 1$. x' *se numeşte complementul lui* x *în mulţimea ordonată* $(A, \leq)$.

Demonstraţie: a) Inelul fiind booleean, pentru orice element x al său au loc relaţiile $x^2 = x$, $(x+x)^2 = x+x$. Din distributivitatea înmulţirii faţă de adunare, a doua egalitate conduce la $x^2 + x^2 + x^2 + x^2 + x^2 = x + x$, care este echivalentă cu $x + x + x + x = x + x$. Deoarece $(A, +)$ este grup, există opusul elementului x, deci obţinem $x + x = 0$.

Fie $x, y \in A$, arbitrar aleşi. Au loc relaţiile $x^2 = x$, $y^2 = y$, $(x + y)^2 = x + y$. Din nou calculăm produsul $(x + y)(x + y)$ folosind distributivitatea şi cele trei relaţii de mai sus conduc la $x \cdot y + y \cdot x = 0$. Conform punctului a) are loc şi relaţia $x \cdot y + x \cdot y = 0$, iar unicitatea simetricului într-un grup (concret, unicitatea opusului elementului $x \cdot y$ în grupul $(A, +)$), implică $x \cdot y = y \cdot x$. Deci inelul booleean este comutativ.

b) O consecinţă imediată a relaţiei $x + x = 0$, este că x este element de ordin doi în grupul $(A, +)$. Conform Propoziţiei 4.1.1, ordinul grupului este număr par. Deci inelul booleean are număr par de elemente.

c) Fie x un element inversabil în inelul A. Evident, x este nenul şi fie x^{-1} inversul său. Calculăm $x \cdot (x+1) = x^2 + x = x + x = 0$. Înmulţind cu x^{-1}, rezultă $x + 1 = 0$, de unde $x = 1$.

d) Se verifică proprietăţile relaţiei de ordine (reflexivă, antisimetrică, tranzitivă).

Proprietăţile e) şi f) se verifică direct. □

Observaţia 5.8.1. *O mulţime ordonată în care există cel mai mic şi cel mai mare element, infimumul şi supremumul pentru orice două elemente şi un complement pentru fiecare element, se numeşte algebră Boole.*

Propoziţia anterioară afirmă că orice inel booleean este o algebră Boole. Se poate arăta şi reciproc, că orice algebră Boole are structură de inel booleean.

5.8.2 Corpul numerelor complexe

Fie $(\mathbb{R}, +, \cdot)$ corpul numerelor reale. Considerăm grupul produs direct $(\mathbb{R}\times\mathbb{R}, +)$, pe care definim o operaţie de înmulţire:

$$(a,b)\cdot(a',b') = (aa' - bb', ab' + a'b), \quad (\forall)(a,b),(a',b') \in \mathbb{R}\times\mathbb{R}.$$

Se demonstrează (verificaţi!) că $(\mathbb{R}\times\mathbb{R}, +, \cdot)$ este corp comutativ. Aplicaţia

$$j : \mathbb{R} \to \mathbb{R}\times\mathbb{R}, \quad j(a) = (a,0), \quad (\forall)a \in \mathbb{R},$$

este morfism de corpuri, deci, conform Propoziţiei 5.4.5, injectiv. De aici rezultă că $(\mathbb{R}, +\cdot)$ este izomorf cu subcorpul $Imj = \{(a,0)/a \in \mathbb{R}\}$ al corpului $\mathbb{R}\times\mathbb{R}$. Identificând elementul $(a,0)$ cu a şi notând $i = (0,1)$, din regula de înmulţire definită mai sus avem:

$$i^2 = (0,1)\cdot(0,1) = (-1,0) = -1,$$

$$i\cdot b = (0,1)\cdot(b,0) = (0,b),$$

$$(a,b) = (a,0) + (0,1)\cdot(b,0) = a + i\cdot b.$$

Mulţimea $\{a + i\cdot b/a, b \in \mathbb{R}\}$ se notează $\mathbb{C}$ şi prin notaţia de mai sus se identifică cu $\mathbb{R}\times\mathbb{R}$, dotat cu cele două operaţii. Am obţinut *corpul numerelor complexe*. Elementul $z = a + ib$ se numeşte *număr complex*, iar $a - ib$ se notează $\overline{z}$ şi se numeşte *conjugatul* numărului complex z.

5.8.3 Corpul cuaternionilor

În mulţimea matricelor $M_2(\mathbb{C})$, considerăm următoarele matrice:

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

Prin calcul direct se stabilesc egalităţile matriceale:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \quad \mathbf{ij} = -\mathbf{ji}, \quad \mathbf{jk} = -\mathbf{kj}, \quad \mathbf{ki} = -\mathbf{ik}.$$

Submulţimea inelului $(M_2(\mathbb{C}), +, \cdot)$

$$\mathbb{H} = \{a \cdot \mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} / \quad a, b, c, d \in \mathbb{R}\} = \{\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} / z, w \in \mathbb{C}\},$$

cu $z = a + id$, $w = b + ic$, $\overline{z}$ conjugatul lui z, este corp (verificaţi!). Acest corp se numeşte *corpul cuaternionilor*. Aplicaţia

$$\xi : \mathbb{C} \to \mathbb{H}, \quad \xi(z) = \begin{pmatrix} z & 0 \\ 0 & \overline{z} \end{pmatrix}, \quad (\forall) z \in \mathbb{C},$$

este morfism de corpuri, deci corpul numerelor complexe poate fi identificat cu un subcorp al lui $\mathbb{H}$.

Avem astfel şirul de extinderi de corpuri $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$.

Observaţia 5.8.2. *Corpul cuaternionilor este corp necomutativ.*

5.8.4 Corpul de fracţii al unui inel integru

Fie A un inel comutativ unitar şi S o submulţime nevidă a sa, cu proprietatea că

$$0 \notin S, \quad 1 \in S, \quad x \cdot y \in S, \quad (\forall) x, y \in S.$$

O astfel de submulţime se numeşte *sistem multiplicativ închis al lui A.*

Exemplul 5.8.2. *În inelul unitar şi comutativ A, următoarele submulţimi sunt sisteme multiplicativ închise:*

a) $\{1\}$*;* $U(A)$*;* S *mulţimea non-divizorilor lui zero din* A*.*

b) Dacă $a \in A^*$*,* $S = \{a^n / \quad n \in \mathbb{N}\}$*.*

Pe mulţimea $A \times S = \{(x, s)/ \quad x \in A, s \in S\}$ definim relaţia

$$(x, s) \approx (y, t) \Leftrightarrow (\exists) \quad r \in A^*, \quad r \cdot (xt - ys) = 0,$$

adică perechile (x, s) şi (y, t) sunt în relaţia $\approx$ dacă şi numai dacă elementul $xt - ys$ este un divizor al lui zero. Dacă A este inel integru, atunci cele două perechi sunt echivalente când $xt = ys$.

Exemplul 5.8.3. *În inelul $\mathbb{Z}_{12}$, fie $S = \mathbb{Z}_{12}^*$ sistem multiplicativ închis. Avem $(\widehat{5}, \widehat{7}) \approx (\widehat{1}, \widehat{2})$, deoarece $\widehat{4} \cdot (\widehat{5} \cdot \widehat{2} - \widehat{7} \cdot \widehat{1}) = \widehat{0}$.*

Se verifică imediat că relaţia definită mai sus este una de echivalenţă (reflexivă, tranzitivă, simetrică).

Mulţimea cât $A \times S/_{\approx}$ se notează cu $S^{-1}A$, iar clasa de echivalenţă a elementului (a, s) se notează $\frac{a}{s}$.

Pe mulţimea $S^{-1}A$ definim operaţiile:

$$\frac{x}{s} + \frac{y}{t} = \frac{x \cdot t + y \cdot s}{s \cdot t}, \quad \frac{x}{s} \cdot \frac{y}{t} = \frac{x \cdot y}{s \cdot t}.$$

Cele două operaţii sunt corect definite, adică nu depind de reprezentanţi (verificaţi!). Mai mult, are loc:

Propoziţia 5.8.2. *$(S^{-1}A, +, \cdot)$ este un inel comutativ şi unitar. Aplicaţia*

$$i^S : A \to S^{-1}A, \quad i^S(a) = \frac{a}{1}, \quad (\forall) a \in A,$$

este morfism unitar de inele.

Inelul $S^{-1}A$ se numeşte *inelul de fracţii* al lui A cu numitori în S.

Propoziţia 5.8.3. *Dacă A este domeniu de integritate şi $S = A^*$, atunci $S^{-1}A$ este corp, numit* ***corpul de fracţii al lui*** *A.*

De exemplu, corpul de fracţii al inelului integru $\mathbb{Z}$ este corpul numerelor raţionale.

5.8.5 Inele de matrice

Un exemplu remarcabil de inele se referă la inelele de matrice. Considerăm cunoscută noţiunea de matrice, din liceu. Amintim totuşi cîteva noţiuni.

Fie $(R, +, \cdot)$ un inel unitar comutativ. Numim matrice de dimensiune (m, n) cu elemente din R o funcţie

$$A : \{1, 2, ..., m\} \times \{1, 2, ..., n\} \to R,$$

pe care de obicei o reprezentăm printr-un tablou

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

unde am notat $A(i, j) = a_{ij}$.

Precizând matricea A, o vom considera $A = (a_{ij})_{i=\overline{1,m}, j=\overline{1,n}}$.

Definiţia 5.8.2. *Dacă $A_{ij} \in M_{m(i),n(i)}(R)$, $i = \overline{1,k}$, $j = \overline{1,p}$ sunt matrice, şi $m = m(1) + m(2) + ... + m(k)$, $n = n(1) + n(2) + ... + n(p)$, atunci matricea*

$$A = \begin{pmatrix} A_{11} & A_{12} & ... & A_{1p} \\ A_{21} & A_{22} & ... & A_{2p} \\ ... & ... & ... & ... \\ A_{k1} & A_{k2} & ... & A_{kp} \end{pmatrix} \in M_{mn}(R),$$

*se numeşte **matrice cu blocuri**, iar matricele A_{ij} sunt blocurile matricei A.*

Observaţia 5.8.3. *Orice matrice $A \in M_{mn}(R)$, cu $m, n \geq 2$, poate fi partiţionată în mai multe moduri în blocuri. De exemplu matricea*

$$A = \begin{pmatrix} 2 & 1 & 4 & -1 \\ 0 & 1 & -3 & 5 \\ 0 & -1 & 1 & 1 \\ 1 & 2 & 0 & 0 \end{pmatrix} = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} = \begin{pmatrix} B_{11} \\ B_{21} \end{pmatrix},$$

unde $A_{11} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$, $A_{12} = \begin{pmatrix} 4 & -1 \\ -3 & 5 \end{pmatrix}$, $A_{21} = \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}$, $A_{22} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$,
$B_{11} = \begin{pmatrix} 2 & 1 & 4 & -1 \\ 0 & 1 & -3 & 5 \end{pmatrix}$, $B_{21} = \begin{pmatrix} 0 & -1 & 1 & 1 \\ 1 & 2 & 0 & 0 \end{pmatrix}$.

Notăm $M_{m,n}(R)$ mulţimea matricelor de tip (m,n) cu elemente din inelul $(R,+,\cdot)$. În raport cu adunarea matricelor, definită pentru două matrice $A = (a_{ij})_{i=\overline{1,m},j=\overline{1,n}}, B = (b_{ij})_{i=\overline{1,m},j=\overline{1,n}} \in M_{m,n}(R)$ prin

$$A + B = (a_{ij} + b_{ij})_{i=\overline{1,m},j=\overline{1,n}},$$

mulţimea $M_{m,n}(R)$ este grup abelian. Elementul neutru este matricea cu toate elementele egale cu elementul 0 al inelului R, iar elementul simetric al matricei $A = (a_{ij})_{i=\overline{1,m},j=\overline{1,n}}$ în raport cu adunarea este $-A = (-a_{ij})_{i=\overline{1,m},j=\overline{1,n}}$.

Fie $A = (a_{ij})_{i=\overline{1,m},j=\overline{1,n}} \in M_{m,n}(R)$, $B = (b_{ij})_{i=\overline{1,m},j=\overline{1,n}} \in M_{p,q}(R)$ două matrice de dimensiune (m,n), respectiv (p,q). Dacă $n = p$, atunci se defineşte produsul matricelor A şi B ca fiind matricea $C = A \cdot B$ cu elementele $(c_{ij})_{i=\overline{1,m},j=\overline{1,q}}$,

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

Fie $A = (a_{ij})_{i=\overline{1,m},j=\overline{1,n}} \in M_{m,n}(R)$. Transpusa ei este o matrice A^t de tip (n,m) cu elementele $(a'_{ji})_{j=\overline{1,n},i=\overline{1,m}}$ cu proprietatea că $a'_{ji} = a_{ij}$. Se verifică următoarele relaţii

$$(A+B)^t = A^t + B^t, \quad (A^t)^t = A, \quad (AB)^t = B^t A^t, \quad (\alpha A)^t = \alpha A^t.$$

Pentru $m = n$, mulţimea $M_n(R)$ a matricelor pătratice, este monoid necomutativ în raport cu înmulţirea matricelor. Elementul neutru este matricea unitate $I_n = (\delta_{ij})_{i,j=\overline{1,n}}$, unde δ_{ij} este simbolul lui Kronecker, definit prin $\delta_{ii} = 1$, $\delta_{ij} = 0$, pentru $i \neq j$. Se verifică prin calcul direct că înmulţirea în $M_n(R)$ este distributivă faţă de adunare. Are loc deci:

Propoziţia 5.8.4. *Tripletul $(M_n(R),+,\cdot)$ este un inel necomutativ.*

Observaţia 5.8.4. *Inelele de matrice nu sunt inele integre. De exemplu, în inelul matricelor pătratice $M_2(R)$ avem:*

$A \cdot B = O_2$, unde

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Fie $A = (a_{ij})_{i,j=\overline{1,n}} \in M_n(R)$ o matrice pătratică (numărul de linii este egal cu numărul de coloane).

Definiţia 5.8.3. *Elementul*

$$detA = \sum_{\sigma_n \in S_n} sgn(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} ... a_{n\sigma(n) \in R}$$

se numeşte determinantul matricei A.

Observăm că $detA$ este o sumă de $n!$ termeni. În fiecare dintre aceştia apare ca factor câte un singur element de pe fiecare linie şi coloană, iar pentru $n \geq 2$ numărul semnelor de plus este egal cu numărul semnelor de minus, corespunzător signaturii permutării $\sigma \in S_n$.

Exemplul 5.8.4. *Pentru* $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, *avem*

$$detA = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}$$

$$-a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}.$$

Definiţia 5.8.4. *Numim minor de ordin p al unei matrice* $A = (a_{ij})_{i=\overline{1,m}, j=\overline{1,n}} \in M_{m,n}(R)$, $p \leq \min\{m, n\}$ *un determinant*

$$\Delta^{i_1 i_2 ... i_p}_{j_1 j_2 ... j_p} = \begin{vmatrix} a_{i_1 j_1} & a_{i_1 j_2} & ... & a_{i_1 j_p} \\ a_{i_2 j_1} & a_{i_2 j_2} & ... & a_{i_2 j_p} \\ ... & ... & ... & ... \\ a_{i_p j_1} & a_{i_p j_2} & ... & a_{i_p j_p} \end{vmatrix},$$

unde $1 \leq i_1 \leq i_2 \leq ... \leq i_p \leq m$, $1 \leq j_1 \leq j_2 \leq ... \leq j_p \leq n$.

Dacă $A \in M_n(R)$ este o matrice pătratică şi $\Delta^{i_1 i_2 ... i_p}_{j_1 j_2 ... j_p}$ este un minor de ordin p al matricei A, atunci minorul $\Delta^{i_{p+1} i_{p+2} ... i_n}_{j_{p+1} j_{p+2} ... j_n}$ de ordin $n - p$, cu

$$\{i_1, i_2, ..., i_p, i_{p+1}, ..., i_n\} = \{j_1, j_2, ..., j_p, j_{p+1}, ..., i_n\} = \{1, 2, .., n\},$$

se numeşte *minor complementar.* Numărul

$$A_{i_1 i_2 ... i_p j_1 j_2 ... j_p} = (-1)^{i_1 + i_2 + ... + i_p + j_1 + ... + j_p} \cdot \Delta^{i_1 i_2 ... i_p}_{j_1 j_2 ... j_p},$$

se numeşte *complementul algebric* al minorului $\Delta_{j_1 j_2 \ldots j_p}^{i_1 i_2 \ldots i_p}$.

Minorii de ordin unu sunt elementele matricei. Pentru matricele pătratice, complementul algebric al elementului a_{ij} este $A_{ij} = (-1)^{i+j} \cdot \Delta_{ij}$, unde Δ_{ij} este determinantul de ordin $n-1$ obţinut din A prin eliminarea liniei i şi a coloanei j.

Amintim câteva din proprietăţile determinanţilor, uşor deductibile din definiţie.

Propoziţia 5.8.5. *Fie $A = (a_{ij})_{i,j=\overline{1,n}} \in M_n(R)$ o matrice pătratică.*

a) Determinantul matricei este egal cu suma produselor dintre elementele liniei fixate i (sau ale unei coloane fixate) şi complementii algebrici ai acestora:

$$det(A) = a_{i1} \cdot A_{i1} + a_{i2} \cdot A_{i2} + ... + a_{in} \cdot A_{in}.$$

b) Determinantul unei matrice este egal cu determinantul matricei transpuse.

c) Dacă toate elementele unei linii/coloane ale unei matrice sunt nule, atunci determinantul matricei este nul.

d) Dacă permutăm liniile unei matrice din $M_n(R)$ astfel încât linia k devine linia $\tau(k)$, cu $\tau \in S_n$, atunci obţinem o matrice A' pentru care $detA' = sgn(\tau)detA$. În particular, dacă schimbăm între ele două linii ale determinantului, semnul său se schimbă.

e) Dacă elementele liniei i sunt sume de forma

$$a_{ij} = a'_{ij} + a"_{ij}, \quad (\forall) j = \overline{1, n},$$

atunci $detA = detA' + detA"$ unde $A', A"$ sunt matricele obţinute din A înlocuind linia i cu $(a'_{ij})_{j=\overline{1,n}}$, respectiv cu $(a"_{ij})_{j=\overline{1,n}}$.

f) Dacă într-un determinant două linii(coloane) sunt proporţionale, atunci valoarea determinantului este zero.

g) Valoarea unui determinant nu se schimbă dacă la elementele unei linii adăugăm combinaţii liniare formate cu elementele altor linii.

h) Dacă înmulţim toate elementele unei linii (coloane) a unui determinant cu $\alpha \in R$, atunci valoarea determinantului se înmulţeşte cu α.

Demonstraţie: a) În formula care defineşte $det(A)$ elementul a_{i1} apare în exact $(n-1)!$ termeni, în fiecare dintre aceştia fiind înmmulţit cu un produs de forma $sgn(\sigma)a_{i_2 2}a_{i_3 3}...a_{i_n n}$, unde $\sigma = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ i & i_2 & i_3 & ... & i_n \end{pmatrix}$. Dând factor comun a_{i1} din aceşti termeni, suma care se înmulţeşte cu el este exact complementul

său algebric, A_{i1}. Am folosit faptul că $sgn(\sigma) = (-1)^{i+1} \cdot sgn(\tau)$, unde $\tau = \begin{pmatrix} 1 & 2 & ... & n-1 \\ i_2 & i_3 & ... & i_n \end{pmatrix}$. Analog pentru celelalte elemente ale liniei i.

Celelalte proprietăţi rezultă imediat aplicând proprietatea a). □

Dăm fără demonstraţie următoarea teoremă, care reprezintă generalizarea proprietăţii a) din Propoziţia anterioară (dezvoltarea determinantului după o linie/coloană):

Teorema 5.8.1. *[Laplace]*
Determinantul matricei A este egal cu suma produselor dintre minorii de ordin p care se pot construi cu p linii fixate din A cu complementii lor algebrici.

O consecinţă a teoremei lui Laplace este

Propoziţia 5.8.6. *Fie $A, B \in M_n(R)$. Are loc egalitatea*

$$det(AB) = detA \cdot detB.$$

Demonstraţie: Se calculează în două moduri determinantul matricei cu blocuri de ordinul $2n$

$$M = \begin{pmatrix} A & O_n \\ -I_n & B \end{pmatrix}.$$

Aplicând regula lui Laplace pentru minorii de ordin n formaţi cu primele n linii ale matricei M avem $detM = detA \cdot detB$. Pe de altă parte putem face zerouri pe poziţiile (i, j), $i, j = \overline{1, n}$ din $detM$ înmulţind ultimele n linii cu $a_{i1}, a_{i2}, ..., a_{in}$ şi adunând la linia i. Aplicând din nou regula lui Laplace pentru aceiaşi minori, avem $detM = det(AB)$. □

Revenind la structura algebrică de inel a mulţimii maticelor $M_n(R)$, este firesc să studiem mulţimea elementelor inversabile. O matrice $A \in M_n(R)$ este inversabilă dacă există $A' \in M_n(R)$ astfel încât $AA' = A'A = I_n$.

Propoziţia 5.8.7. *Matricea $A \in M_n(R)$ este inversabilă ($A \in U(M_n(R))$ dacă şi numai dacă $detA$ este inversabil în monoidul $(R, \cdot)$.*

Demonstraţie: Implicaţia directă este imediată, pentru o matrice inversabilă avem, conform Propoziţiei 5.8.6, $detA \cdot detA' = 1$. Reciproc, pentru o matrice cu determinantul nenul se construieşte matricea adjunctă A^* ale cărei elemente sunt

complementţii algebrici ai elementelor transpusei lui A. Prin calcul direct obţinem, ţinând cont de proprietatea a) din Propoziţia 5.8.5, $AA^* = A^*A = (detA)I_n$. Deci A este inversabilă, cu inversa egală cu $A^{-1} = (det(A))^{-1} \cdot A^*$. □

Exemplul 5.8.5. *Fie* $A = \begin{pmatrix} \widehat{1} & \widehat{0} & \widehat{2} \\ \widehat{0} & \widehat{1} & \widehat{1} \\ \widehat{3} & \widehat{2} & \widehat{3} \end{pmatrix} \in M_3(\mathbb{Z}_6)$. *Se cere inversa matricei, dacă există.*

Calculăm $detA = \widehat{1} \in U(\mathbb{Z}_6)$, *deci există* A^{-1}. *Transpusa matricei* A *este* $A^t = \begin{pmatrix} \widehat{1} & \widehat{0} & \widehat{3} \\ \widehat{0} & \widehat{1} & \widehat{2} \\ \widehat{2} & \widehat{1} & \widehat{3} \end{pmatrix}$. *Matricea adjunctă se obţine din* A^t *înlocuind fiecare element cu complementul său algebric, deci are elementele:*

$$A_{11} = (-1)^{1+1} \begin{vmatrix} \widehat{1} & \widehat{2} \\ \widehat{1} & \widehat{3} \end{vmatrix} = \widehat{1}, \quad A_{12} = (-1)^{1+2} \begin{vmatrix} \widehat{0} & \widehat{2} \\ \widehat{2} & \widehat{3} \end{vmatrix} = \widehat{4},$$

$$A_{13} = (-1)^{1+3} \begin{vmatrix} \widehat{0} & \widehat{1} \\ \widehat{2} & \widehat{1} \end{vmatrix} = \widehat{4}, \quad A_{21} = (-1)^{1+2} \begin{vmatrix} \widehat{0} & \widehat{3} \\ \widehat{1} & \widehat{3} \end{vmatrix} = \widehat{3},$$

$$A_{22} = (-1)^{2+2} \begin{vmatrix} \widehat{1} & \widehat{3} \\ \widehat{2} & \widehat{3} \end{vmatrix} = \widehat{3}, \quad A_{23} = (-1)^{2+3} \begin{vmatrix} \widehat{1} & \widehat{0} \\ \widehat{2} & \widehat{1} \end{vmatrix} = \widehat{5},$$

$$A_{31} = (-1)^{3+1} \begin{vmatrix} \widehat{0} & \widehat{3} \\ \widehat{1} & \widehat{2} \end{vmatrix} = \widehat{3}, \quad A_{32} = (-1)^{3+2} \begin{vmatrix} \widehat{1} & \widehat{3} \\ \widehat{0} & \widehat{2} \end{vmatrix} = \widehat{4},$$

$$A_{33} = (-1)^{2+3} \begin{vmatrix} \widehat{1} & \widehat{0} \\ \widehat{0} & \widehat{1} \end{vmatrix} = \widehat{1},$$

Am găsit $A^{-1} = \begin{pmatrix} \widehat{1} & \widehat{4} & \widehat{4} \\ \widehat{3} & \widehat{3} & \widehat{5} \\ \widehat{3} & \widehat{4} & \widehat{1} \end{pmatrix}$.

Propoziţiile 2.4.1 şi 5.8.7 conduc la faptul că mulţimea

$$U(M_n(R)) = \{A \in M_n(R) / detA \in U(R)\},$$

este grup în raport cu înmulţirea matricelor. Acest grup se numeşte *grupul liniar general* $GL_n(R)$.

Propoziţia 5.8.6 asigură faptul că funcţia

$$\xi : GL_n(R) \to U(R), \quad \xi(A) = detA,$$

este morfism de grupuri de la $(GL_n(R), \cdot)$ la $(U(R), \cdot)$.

Acest morfism este surjectiv, deoarece pentru orice element nenul $r \in R$, există o matrice pătratică de ordin n, de exemplu matricea care are pe diagonala principală un r şi $n-1$ de 1, iar în rest elementele nule, al cărei determinant este egal cu r. Nucleul morfismului ξ este

$$SL_n(R) = \{A \in GL_n(R) | \quad detA = 1\},$$

şi se numeşte grupul liniar special. Fiind nucleul unui morfism, este subgrup normal. Aplicând Teorema fundamentala de izomorfism morfismului de grupuri ξ, avem

$$GL_n(R)/SL_n(R) \approx U(R).$$

În continuare prezentăm alte metode de calcul a inversei unei matrice.

Metoda partiţionării pentru calculul inversei unei matrice

Această metodă constă în descompunerea matricei în blocuri (matrice) de ordin mai mic. Metoda este utilă în cazul matricelor de ordin foarte mare.

Fie matricea $S = \left(\begin{array}{c|c} A & B \\ -- & -- \\ C & D \end{array}\right)$ o matrice partiţionată în patru blocuri, unde A, D matrice sunt pătratice, fie $A \in M_p(R)$, $D \in M_q(R)$, $B \in M_{p,q}(R)$, $C \in M_{q,p}(R)$, cu $p + q = n$. Căutăm S^{-1} de forma $\left(\begin{array}{c|c} X & Y \\ -- & -- \\ Z & T \end{array}\right)$, unde matricele bloc sunt de dimensiuni similare celor din S. Obţinem următorul sistem matriceal:

$$\left\{\begin{array}{c} AX + BZ = I_p \\ CX + DZ = O_{q,p} \\ AY + BT = O_{p,q} \\ CY + DT = I_q \end{array}\right.$$

Dacă A este inversabilă, atunci prima ecuaţie devine $X = A^{-1} - A^{-1}BZ$, iar a treia dacă o amplificăm cu CA^{-1} şi eliminăm CY între ecuaţia obţinută şi a

patra, obţinem $T = (D - CA^{-1}B)^{-1}$. Înlocuind X în a doua ecuaţie din sistem, avem $Z = -TCA^{-1}$, apoi $Y = -A^{-1}BT$. Soluţia sistemului este

$$\begin{cases} T = (D - CA^{-1}B)^{-1} \\ Y = -A^{-1}BT \\ Z = -TCA^{-1} \\ X = A^{-1} - A^{-1}BZ \end{cases}$$

Este preferabilă deci descompunerea în blocuri astfel încât A să fie inversabilă. De asemenea este convenabil sa aleg $p = 2$, deoarece inversa unei matrice de ordinul 2 se scrie imediat:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow \quad A^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Dacă nu este posibilă descompunerea cu A inversabil, dar există o descompunere în blocuri cu D inversabil, atunci sistemul anterior se rezolvă astfel:

$$\begin{cases} X = (A - BD^{-1}C)^{-1} \\ Z = -D^{-1}CX \\ Y = -XBD^{-1} \\ T = D^{-1} - D^{-1}CY \end{cases}$$

Prin această metodă inversarea unei matrice de ordin n revine la inversarea a două matrice de ordin mai mic, p şi q, şi la calcul matriceal simplu.

Exemplul 5.8.6. *Se cere inversa matricei* $S = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 1 & 1 & 1 & 2 \\ 2 & 3 & 3 & 1 \\ 1 & 2 & 2 & 1 \end{pmatrix} \in M_4(\mathbb{R})$. *Aplicăm metoda partiţionării pentru*

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \quad C = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}, \quad D = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix},$$

unde $detA = 1$. *Calculăm*

$$A^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \quad D - CA^{-1}B = \begin{pmatrix} 2 & -4 \\ 2 & -2 \end{pmatrix},$$

$$T = (D - CA^{-1}B)^{-1} = \frac{1}{2} \begin{pmatrix} -1 & 2 \\ -1 & 1 \end{pmatrix},$$

$$Y = -A^{-1}BT = \frac{1}{2}\begin{pmatrix} 3 & -5 \\ 0 & 1 \end{pmatrix}, \quad Z = -TCA^{-1} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix},$$

$$X = A^{-1} - A^{-1}BZ = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Am obţinut matricea $S^{-1} = \frac{1}{2}\begin{pmatrix} 0 & 1 & 3 & -5 \\ -1 & 0 & 0 & 1 \\ 1 & -1 & -1 & 2 \\ 0 & 1 & -1 & 1 \end{pmatrix}$.

Metoda eliminării (Gauss) pentru inversarea unei matrice

O altă modalitate de inversare a unei matrice pleacă de la rezolvarea sistemelor liniare prin metoda eliminării (metoda Gauss). Legătura cu inversarea matricei este aceea că matricea inversă a unei matrice $A \in M_n(K)$, unde K este un corp comutativ, este soluţia ecuaţiei $A \cdot X = I_n$. Mai exact, coloana i a matricei inverse este soluţia ecuaţiei $A \cdot X = B_i$, unde B_i este o matrice coloană care are 1 pe poziţia i şi 0 în rest, adică este coloana i din matricea unitate.

Fie A o matrice pătratică de ordin n şi B o matrice coloană cu n linii. A rezolva un sistem de ecuaţii liniare înseamnă a prelucra informaţiile oferite de legătura $A \cdot X = B$ între necunoscutele $x_1, x_2, ..., x_n$, elementele coloanei X, prin transformări echivalente, adică transformări care lasă neschimbată informaţia, până la aducerea sistemului în forma $I_n \cdot X = S$. Deci matricea sistemului echivalent este I_n, ceea ce reprezintă găsirea soluţiei.

Metoda eliminării constă în prelucrarea ecuaţiilor sistemului prin amplificarea lor cu o constantă şi adunarea la altă ecuaţie, pentru a rămâne prima necunoscută doar in prima ecuaţie, a doua necunoscută doar în a doua ecuaţie, etc.

Mai clar, dacă în prima ecuaţie a sistemului coeficientul necunoscutei x_1 este nenul, atunci cu acestă ecuaţie elimin x_1 din toate celelalte ecuaţii ale sistemului. Dacă nu, fac o schimbare a ecuaţiilor sistemului (ordinea ecuaţiilor unui sistem nu are importanţă din punct de vedere al informaţiei) aducând ca primă ecuaţie pe prima în care x_1 are coeficient nenul. Apoi aplificăm această primă ecuaţie cu inversul coeficientului, pentru a avea x_1 coeficient 1. Lucrăm cu prima ecuaţie pentru a elimina necunoscuta x_1 din toate celelalte, astfel> amplific ecuaţia 1 cu opusul coeficientului lui x_1 din ecuaţia i şi o adun la ecuaţia i. Evident, ceea ce obţinem este un sistem echivalent cu cel iniţial, dar în care x_1 este în

ecuaţia 1 cu coeficient 1, iar în ecuaţia i cu coeficient 0. Aplicând tehnica pentru $i = \{2, 3, .., n\}$, eliminăm necunoscuta x_1 din ecuaţiile $2, 3, ..., n$. Reluăm algoritul cu ecuaţia a doua, eliminâd necunoscuta x_2 din ecuaţiile $1, 3, .., n$, ş.a.m.d. În final obţinem soluţia sistemului.

Exemplul 5.8.7. *Fie sistemul*

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

Prima ecuaţie are necunoscuta x_1 cu coeficient 1. Elimină necunoscuta x_1 din ecuaţia a doua prin amplificarea primei ecuaţii cu (-2) şi adunarea la a doua ecuaţie. Obţinem sistemul echivalent

$$\begin{cases} x_1 + 2x_2 - x_3 &= -2 \\ -x_2 + 5x_3 &= 6 \\ -x_1 + 3x_2 + 2x_3 &= -2 \end{cases}$$

Elimină x_1 din a treia ecuaţie adunând la aceasta ecuaţia 1. Obţinem un sistem în care necunoscuta ax_1 are coeficient nenul doar în prima ecuaţie:

$$\begin{cases} x_1 + 2x_2 - x_3 &= -2 \\ -x_2 + 5x_3 &= 6 \\ 5x_2 + x_3 &= -4 \end{cases}$$

Reluăm algoritmul cu necunoscuta x_2 pe care o elimină din ecuaţiile 1 şi 3, iar în ecuaţia 2 va avea coeficient 1. Amplificăm ecuaţia 2 cu -1, inversul coeficientului lui x_2:

$$\begin{cases} x_1 + 2x_2 - x_3 &= -2 \\ x_2 - 5x_3 &= -6 \\ 5x_2 + x_3 &= -4 \end{cases}$$

Amplificăm ecuaţia 2 cu -2 şi o adunăm la prima ecuaţie, apoi amplificăm ecuaţia 2 cu -5 şi o adunăm la a treia, obţinând succesiv sistemele echivalente

$$\begin{cases} x_1 + 9x_3 &= 10 \\ x_2 - 5x_3 &= -6 \\ 5x_2 + x_3 &= -4 \end{cases} \Leftrightarrow \begin{cases} x_1 + 9x_3 &= 10 \\ x_2 - 5x_3 &= -6 \\ 26x_3 &= 26 \end{cases}$$

Continuăm amplificând ecuaţia 3 cu inversul coeficientului lui x_3, apoi cu ecuaţia a treia obţinută, prin amplificare cu -9, urmată de adunare la prima ecuaţie, apoi amplificare cu 5 şi adunare la a doua ecuaţie, obţinem sistemele echivalente

$$\left\{\begin{array}{rcr} x_1+9x_3 & = & 10 \\ x_2-5x_3 & = & -6 \\ x_3 & = & 1 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcr} x_1+9x_3 & = & 10 \\ x_2 & = & -1 \\ x_3 & = & 1 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcr} x_1 & = & 1 \\ x_2 & = & -1 \\ x_3 & = & 1 \end{array}\right.$$

Ultimul sistem are matricea sistemului I_3 şi reprezintă soluţia. Am adus sistemul la forma echivalentă $I_3 \cdot X = S$, prin transformări elementare asupra ecuaţiilor sistemului.

Să remarcăm că toate prelucrările anterioare s-au făcut de fapt asupra elementelor matricei extinse a sistemului (matricea sistemului completata cu coloana termenilor liberi). Metoda eliminării constă deci în prelucrarea matricei extinse a unui sistem liniar de ecuaţii, prin transformări care schimbă sistemul într-unul echivalent, pentru a duce matricea sistemului la matricea unitate, adică pentru a găsi soluţia. Exemplul anterior se poate prezenta mult mai simplu, lucrând cu liniile matricei extinse. Menţionăm la fiecare pas transformarea aplicată liniilor matricei extinse, deci sistemului:

Exemplul 5.8.8.

$$\begin{pmatrix} 1 & 2 & -1 & -2 \\ 2 & 3 & 3 & 2 \\ -1 & 3 & 2 & -2 \end{pmatrix} \overset{(-2)L_1+L_2}{\Leftrightarrow} \begin{pmatrix} 1 & 2 & -1 & -2 \\ 0 & -1 & 5 & 6 \\ -1 & 3 & 2 & -2 \end{pmatrix} \overset{(-1)L_2}{\Leftrightarrow}$$

$$\begin{pmatrix} 1 & 2 & -1 & -2 \\ 0 & 1 & -5 & -6 \\ -1 & 3 & 2 & -2 \end{pmatrix} \overset{L_1+L_3}{\Leftrightarrow} \begin{pmatrix} 1 & 2 & -1 & -2 \\ 0 & 1 & -5 & -6 \\ 0 & 5 & 1 & -4 \end{pmatrix} \overset{(-2)L_2+L_1}{\Leftrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 9 & 10 \\ 0 & 1 & -5 & -6 \\ 0 & 5 & 1 & -4 \end{pmatrix} \overset{(-5)L_2+L_3}{\Leftrightarrow} \begin{pmatrix} 1 & 0 & 9 & 10 \\ 0 & 1 & -5 & -6 \\ 0 & 0 & 26 & 26 \end{pmatrix} \overset{\frac{1}{26}L_3}{\Leftrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 9 & 10 \\ 0 & 1 & -5 & -6 \\ 0 & 0 & 1 & 1 \end{pmatrix} \overset{5L_3+L_2}{\Leftrightarrow} \begin{pmatrix} 1 & 0 & 9 & 10 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \overset{(-9)L_3+L_1}{\Leftrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

care dă soluţia $x_1 = 1$, $x_2 = -1$, $x_3 = 1$.

Revenind la inversarea unei matrice de ordin n, aceasta constă în reolvarea a n sisteme de ecuaţii liniare, în care coloanele termenilor liberi sunt exact coloanele matricei unitate. Metoda eliminării aplicată matricei extinse permite reolvarea simultană a celor n sisteme.

Exemplul 5.8.9. *Se cere inversa matricei* $S = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 1 & 1 & 1 & 2 \\ 2 & 3 & 3 & 1 \\ 1 & 2 & 2 & 1 \end{pmatrix} \in M_4(\mathbb{R})$. *Formăm matricea extinsă a celor patru sisteme de ecuaţii liniare care ar trebui rezolvate pentru a găsi inversa:*

$$\begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 2 & 0 & 1 & 0 & 0 \\ 2 & 3 & 3 & 1 & 0 & 0 & 1 & 0 \\ 1 & 2 & 2 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

şi aplicăm metoda eliminării

$$\begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 2 & 0 & 1 & 0 & 0 \\ 2 & 3 & 3 & 1 & 0 & 0 & 1 & 0 \\ 1 & 2 & 2 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \overset{(-1)L_1+L_2}{\Leftrightarrow} \begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 1 & -1 & 1 & 0 & 0 \\ 2 & 3 & 3 & 1 & 0 & 0 & 1 & 0 \\ 1 & 2 & 2 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \overset{(-2)L_1+L_3}{\Leftrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 1 & -1 & 1 & 0 & 0 \\ 0 & 3 & -1 & -1 & -2 & 0 & 1 & 0 \\ 1 & 2 & 2 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \overset{(-1)L_1+L_4}{\Leftrightarrow} \begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 1 & -1 & 1 & 0 & 0 \\ 0 & 3 & -1 & -1 & -2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 & -1 & 0 & 0 & 1 \end{pmatrix} \overset{(-3)L_2+L_3}{\Leftrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 1 & -1 & 1 & 0 & 0 \\ 0 & 0 & 2 & -4 & 1 & -3 & 1 & 0 \\ 0 & 2 & 0 & 0 & -1 & 0 & 0 & 1 \end{pmatrix} \overset{(-2)L_2+L_4}{\Leftrightarrow} \begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 1 & -1 & 1 & 0 & 0 \\ 0 & 0 & 2 & -4 & 1 & -3 & 1 & 0 \\ 0 & 0 & 2 & -2 & 1 & -2 & 0 & 1 \end{pmatrix} \overset{\frac{1}{2}L_3}{\Leftrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 1 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -2 & \frac{1}{2} & -\frac{3}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 2 & -2 & 1 & -2 & 0 & 1 \end{pmatrix} \overset{(-2)L_3+L_1}{\Leftrightarrow} \begin{pmatrix} 1 & 0 & 0 & 5 & 0 & 3 & -1 & 0 \\ 0 & 1 & -1 & 1 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -2 & \frac{1}{2} & -\frac{3}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 2 & -2 & 1 & -2 & 0 & 1 \end{pmatrix} \overset{L_3+L_2}{\Leftrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 0 & 5 & 0 & 3 & -1 & 0 \\ 0 & 1 & 0 & -1 & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 & -2 & \frac{1}{2} & -\frac{3}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 2 & -2 & 1 & -2 & 0 & 1 \end{pmatrix} \overset{(-2)L_3+L_4}{\Leftrightarrow} \begin{pmatrix} 1 & 0 & 0 & 5 & 0 & 3 & -1 & 0 \\ 0 & 1 & 0 & -1 & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 & -2 & \frac{1}{2} & -\frac{3}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 2 & 0 & 1 & -1 & 1 \end{pmatrix} \overset{\frac{1}{2}L_4}{\Leftrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 0 & 5 & 0 & 3 & -1 & 0 \\ 0 & 1 & 0 & -1 & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 & -2 & \frac{1}{2} & -\frac{3}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 & 0 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \overset{(-5)L_4+L_1}{\Leftrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{3}{2} & \frac{-5}{2} \\ 0 & 1 & 0 & -1 & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 & -2 & \frac{1}{2} & -\frac{3}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 & 0 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \overset{L_4+L_2}{\Leftrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{3}{2} & \frac{-5}{2} \\ 0 & 1 & 0 & 0 & -\frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 1 & -2 & \frac{1}{2} & -\frac{3}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 & 0 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \overset{2L_4+L_3}{\Leftrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{3}{2} & \frac{-5}{2} \\ 0 & 1 & 0 & 0 & -\frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 1 & 0 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 2 \\ 0 & 0 & 0 & 1 & 0 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

Când matricea A s-a transformat în I_4, avem pe ultimele 4 coloane găsim soluţia, adică inversa matricei S:

$$S^{-1} = \begin{pmatrix} 0 & \frac{1}{2} & \frac{3}{2} & \frac{-5}{2} \\ -\frac{1}{2} & 0 & 0 & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 2 \\ 0 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

5.9 Exerciţii

1. Pe mulţimea numerelor întregi se dau operaţiile

$$x \oplus y = x + y + 3, \quad x \odot y = xy + 3x + 3y + 6.$$

Demonstraţi că tripletul $(\mathbb{Z}, \oplus, \odot)$ este un domeniu de integritate şi determinaţi elementele sale inversabile.

2. Să se arate că inelul de întregi pătratici $\mathbb{Z}[\sqrt{2}]$ are o infinitate de elemente inversabile, iar inelul de întregi pătratici $\mathbb{Z}[i\sqrt{2}]$ are doar două elemente inversabile. Analog pentru $\mathbb{Z}[\sqrt{5}]$, respectiv $\mathbb{Z}[i\sqrt{5}]$.

Indicaţie: Elementele inversabile din inelele de întregi pătratici se caracterizează prin condiţia 3 din Exemplul 6.1.2. Funcţia normă pe $\mathbb{Z}[\sqrt{2}]$ este $N(a + b\sqrt{2}) = |a^2 - 2b^2|$, iar

$z = a + \sqrt{2}b \in U(\mathbb{Z}[\sqrt{2}]$ dacă şi numai dacă $N(z) = 1$. Observăm $3 + 2\sqrt{2} \in U(\mathbb{Z}[\sqrt{2}]$, deci şi $(3 + 2\sqrt{2})^k \in U(\mathbb{Z}[\sqrt{2}]$, pentru orice k natural.

4. Fie $(A, +, \cdot)$ inel unitar, $1 \neq 0$, cu $x^2 = 1$, $(\forall)x \in A^*$. Să se arate că A este un corp izomorf cu $(\mathbb{Z}_2, +, \cdot)$ sau cu $(\mathbb{Z}_3, +, \cdot)$.

Indicaţie: Condiţia $x^2 = 1$ asigură existenţa inversului pentru orice x nenul, deci A este corp. Avem şi $(x - 1)(x + 1) = 0$, care în inel integru duce la $x = 1$ sau $x = -1$. Deci A are 2 elemente, dacă $1 = -1$, sau 3, dacă $1 \neq -1$.

5. Fie $(A, +, \cdot)$ şi $(B, +, \cdot)$ două inele unitare. Pe grupul produs direct $(A \times B, +)$ definit în Exemplul 2.3.2, definim operaţia $\cdot$ prin

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2), \quad (\forall)(a_1, b_1), (a_2, b_2) \in A \times B.$$

Să se arate că $(A \times B, +, \cdot)$ este inel unitar şi $U(A \times B) = U(A) \times U(B)$.

7. Fie numerele naturale $m > 1$, $n > 1$, prime între ele. Să se arate că inelul $\mathbb{Z}_n \times \mathbb{Z}_m$ este izomorf cu $\mathbb{Z}_{mn}$ şi să se deducă de aici că $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$, unde φ este indicatorul lui Euler.

8. Fie $(A, +, \cdot)$ un inel unitar. Să se arate că orice element idempotent diferit de 0 şi 1 este divizor al lui zero.

9. Fie $(A, +, \cdot)$ un inel unitar comutativ. Să se arate că produsul elementelor idempotente nenule din A este 1 dacă 1 este singurul element idempotent nenul şi este 0 dacă există elemente idempotente diferite de 0 şi 1.

Indicaţie: Dacă 1 este singurul element idempotent, evident că produsul cerut este egal cu 1. Dacă există şi elemente idempotente nenule, fie $a \in A$ unul dintre ele. El verifică $a(1 - a) = 0$. $(1 - a)^2 = a^2 - a - a + 1 = 1 - a$, deci şi $1 - a$ este idempotent. Aşadar toate elementele idempotente diferite de 0 şi 1 pot fi grupate câte două, $\{a, 1 - a\}$, evident distincte. Produsul lor va fi nul.

10. Să se determine endomorfismele, apoi automorfismele inelului numerelor întregi.

Indicaţie: Deoarece orice endomorfism al inelului $(\mathbb{Z}, +, \cdot)$ este un endomorfism al grupului $(\mathbb{Z}, +)$, folosim exerciţiul 5 din paragraful 2.5. Un endomorfism al grupului aditiv $\mathbb{Z}$ este de forma $f_a(k) = a \cdot k$, $(\forall)k \in \mathbb{Z}$. Sunt endomorfisme de inele cele care verifică $f_a(k_1 \cdot k_2) =$

$f_a(k_1) \cdot f_a(k_2)$, deci $a^2 = 1$. Există două endomorfisme ale inelului $\mathbb{Z}$, f_0, f_1, iar f_1 este singurul automorfism.

11. Să se determine toate morfismele de inele de la inelul numerelor întregi la inelul claselor de resturi modulo n.

Indicaţie: Ca la exerciţiul anterior, avem morfismele $f_a(k) = k \hat{\cdot} a$, $a \in \mathbb{Z}_n$, care trebuie să verifice $a^2 = a$.

12. Să se arate că există un singur morfism de inele $f : \mathbb{Z}_n \to \mathbb{Z}$, morfismul nul.

Indicaţie: Din $f(\hat{1}) = k_0$ şi proprietatea de morfism rezultă $f(n \cdot \hat{1}) = f(\hat{0}) = 0$, deci $n \cdot k_0 = 0$.

13. Să se determine morfismele de inele $f : \mathbb{Z}_n \to \mathbb{Z}_m$.

Indicaţie: Găsim $f_a(\hat{1}) = a$, $a \in \mathbb{Z}_m$, cu $m | n \cdot a$ şi $a^2 = a$.

14. Să se determine endomorfismele corpului numerelor reale.

Indicaţie: Fie $f : \mathbb{R} \to \mathbb{R}$ un endomorfism. Din $f(1) = 1$ şi din definiţia şi proprietăţile morfismelor de inele rezultă $f(x) = x$, $(\forall) x \in \mathbb{Q}$. Se arată că f etse strict crescătoare. Pentru aceasta, observăm că pentru orice $x > 0$, $f(x) = f(\sqrt{x} \cdot \sqrt{x}) = (f(\sqrt{x})^2 > 0$. Atunci, pentru $x > y$, $f(x - y) > 0$, deci $f(x) > f(y)$. Folosind f crescătoare, arătăm $f(x) = x$, $(\forall) x \in \mathbb{R}$. Presupunem prin absurd că există $x_0 \in \mathbb{R}$, cu $f(x_0) > x_0$. Există un număr raţional a, cu $x_0 < a < f(x_0)$ (de exemplu media artimetică a două aproximări raţionale convenabile ale numerelor reale x_0 şi $f(x_0)$). Rezultă $f(x_0) < f(a) = a$, contradicţie. Analog se exclude cazul $x_0 > f(x_0)$.

15. Fie $(A, +, \cdot)$ un inel unitar comutativ şi I, J,K ideale ale sale. Să se arate că:

a) $I : I = A$, $I : A = A$, $(I \cap J) : K = (I : K) \cap (J : K)$, $I : (J + K) = (I : J) \cap (I : K)$;

b) $J \cdot (I : J) \subseteq I \subseteq I : J \subseteq A$;

c) $(I : J) : K = I : (I \cdot K)$;

c) $\sqrt{\sqrt{I}} = \sqrt{I}$, $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$, $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$;

d) $\sqrt{I \cdot J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

16. Fie $(K, +, \cdot)$ un corp cu 81 de elemente. Să se arate că:

a) $x + x + x = 0$, $(\forall)x \in K$;
b) $(x + y)^3 = x^3 + y^3$, $(\forall)x, y \in K$.
c) $f : K \to K$, $f(x) = x^3$, $(\forall)x \in K$, este un endomorfism de corpuri.

17. În inelul $(\mathbb{Z}_8, +, \cdot)$, să se determine elementele inversabile, nilpotetnte şi idempotente.

18. Fie A un inel unitar comutativ, $a \in U(A)$ şi x un element nilpotent al său. Să se arate că elementele $a - x$ şi $a + x$ sunt inversabile.

Indicaţie: Deoarece x este un element nilpotent, există n natural cu $x^n = 0$. şi avem

$$a^n = a^n - x^n = (a - x)(a^{n-1} + a^{n-2} \cdot x + ... + a \cdot x^{n-2} + x^{n-1}).$$

Elementul a fiind inversabil, a^n este tot inversabil, cu inversul $(a^{-1})^n$, iar egalitatea de mai sus duce la

$$1 = (a - x)(a^{n-1} + a^{n-2} \cdot x + ... + a \cdot x^{n-2} + x^{n-1})(a^{-1})^n,$$

adică $a - x$ este inversabil.

Din x nilpotent avem şi $-x$ nilpotent, deci $a - (-x)$ inversabil.

19. Să se determine inversa matricei

$$S = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 1 & 1 & 1 & 2 \\ 2 & 3 & 3 & 1 \\ 1 & 2 & 2 & 1 \end{pmatrix} \in M_4(\mathbb{R}),$$

în două moduri.

Capitolul 6

Inele de polinoame

6.1 Construcţia inelelor de polinoame

Unele dintre cele mai importante inele, cu aplicaţii multiple, sunt inelele de polinoame, a căror construcţie o prezentăm în cele ce urmează.

Fie $(A, +, \cdot)$ un inel unitar comutativ. Vom construi mai întâi inelul seriilor formale peste A.

Fie $A^{\mathbb{N}}$ mulţimea tuturor funcţiilor de la $\mathbb{N}$ la A. O astfel de funcţie o scriem prin mulţimea ordonată a valorilor sale, deci $A^{\mathbb{N}}$ este mulţimea şirurilor infinite

$$f = (a_0, a_1, ..., a_n, ...), \quad a_i \in A, (\forall) i \in \mathbb{N},$$

numite serii formale peste A.

Două astfel de şiruri $f = (a_0, a_1, ..., a_n, ...)$, $g = (b_0, b_1, ..., b_n, ...)$ sunt egale dacă $a_i = b_i$, $(\forall) i \in \mathbb{N}$.

Definim operaţiile de adunare

$$f + g = (a_0 + b_0, a_1 + b_1, ..., a_n + b_n, ...),$$

şi de înmulţire

$$f \cdot g = (c_0, c_1, ..., c_n, ...), \quad c_k = \sum_{i=0}^{k} a_i b_{k-i}, \quad (\forall) k \in \mathbb{N}.$$

Propoziţia 6.1.1. *Tripletul $(A^{\mathbb{N}}, +, \cdot)$ este un inel comutativ unitar. Aplicaţia*

$$i : A \to A^{\mathbb{N}}, \quad i(a) = (a, 0, ..., 0, ...), \quad (\forall) a \in A,$$

este morfism unitar injectiv de inele.

Demonstraţie: Se verifică cu uşurinţă că $(A^{\mathbb{N}}, +)$ este un grup comutativ, cu elementul neutru funcţia nulă, $0 = (0, 0, ...)$, care pune pe fiecare pozţie elementul zero al inelului A. Opusul elementului $f = (a_0, a_1, ..., a_n, ...)$ este $-f = (-a_0, -a_1, ..., -a_n, ...)$.

Să probăm asociativitatea înmulţirii în $A^{\mathbb{N}}$. Fie $f = (a_0, a_1, ..., a_n, ...)$, $g = (b_0, b_1, ..., b_n, ...)$, $h = (c_0, c_1, ..., c_n, ...)$ arbitrar alese. Din regula de înmulţire a seriilor formale, avem

$$f \cdot g = (d_0, d_1, ..., d_n, ..), \quad d_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_j, \quad (\forall) k \geq 0,$$

$$(f \cdot g) \cdot h = (e_o, e_1, ..., e_n, ...), \quad e_n = \sum_{k+l=n} d_k c_l, \quad (\forall) n \geq 0,$$

$$g \cdot h = (x_0, x_1, ..., x_n, ...), \quad x_k = \sum_{j+l=k} b_j c_l, \quad (\forall) k \geq 0,$$

$$f \cdot (g \cdot h) = (y_0, y_1, ..., y_n, ..), \quad y_n = \sum_{i+k=n} a_i x_l, \quad (\forall) j \geq 0,$$

Avem

$$e_j = \sum_{k+l=n} d_k c_l = \sum_{k+l=n} \sum_{i+j=k} a_i b_j c_l = \sum_{i+j+l=n} a_i b_j c_l,$$

$$y_n = \sum_{i+k=n} a_i x_l = \sum_{i+k=n} a_i \sum_{j+l=k} b_j c_l = \sum_{i+j+l=n} a_i b_j c_l = e_n, \quad (\forall) n \geq 0,$$

deci $(f \cdot g) \cdot h = f \cdot (g \cdot h)$.

Elementul $1 = (1, 0, 0, ..., 0, ..)$ corespunde funcţiei $1(n) = \delta_0^n$, unde δ_i^j este simbolul lui Kronecker, adică este 1 dacă $i = j$ şi este zero în rest. Acest element are proprietatea că

$$1 \cdot f = (c_0, c_1, ..., c_n, ...), \quad c_k = \sum_{i=0}^{k} \delta_0^i a_{k-i} = a_k, \quad (\forall) k \in \mathbb{N},$$

deci $1 \cdot f = f$. Analog $f \cdot 1 = f$, pentru orice $f = f = (a_0, a_1, ..., a_n, ...) \in A^{\mathbb{N}}$, deci 1 este element neutru la înmulţirea din $A^{\mathbb{N}}$.

Înmulţirea seriilor formale este distributivă faţă de adunare, deoarece pentru seriile formale f, g, h considerate mai sus avem

$$f \cdot (g + h) = (d_0, d_1, ..., d_n, ..), \quad d_n = \sum_{i+j=n} a_i (b_j + c_j), \quad (\forall) n \geq 0,$$

$$f \cdot g + f \cdot h = (e_0, e_1, ..., e_n, ...), \quad e_n = \sum_{i+j=n} a_i b_j + \sum_{i+j=n} a_i c_j = d_n, \quad (\forall) n \geq 0,$$

din distributivitatea înmulţirii faţă de adunare în A. Rezultă aşadar

$$f \cdot (g + h) = f \cdot g + f \cdot h.$$

Analog se verifică şi

$$(g + h) \cdot f = g \cdot f + h \cdot f,$$

apoi că operaţia $\cdot$ este comutativă, deci $(A^{\mathbb{N}}, +, \cdot)$ este inel comutativ.

Din definiţiile operaţiilor în $A^{\mathbb{N}}$ rezultă că

$$i(a + b) = (a + b, 0, 0, ..., 0, ...) = (a, 0, 0, ..., 0, ...) + (b, 0, 0, ..., 0, ...) = i(a) + i(b),$$

$$i(a \cdot b) = (a \cdot b, 0, 0, ..., 0, ...) = (a, 0, 0, ..., 0, ...) \cdot (b, 0, 0, ..., 0, ...) = i(a) \cdot i(b), \quad (\forall) a, b \in A.$$

Aşadar i este morfism de inele. Rezultă imediat şi că este morfism unitar şi injectiv de inele. □

Din ultima afirmaţie a Propoziţiei 6.1.1 rezultă că A poate fi considerat un subinel (este de fapt izomorf cu subinelul $i(A)$) al inelului $A^{\mathbb{N}}$, identificând elementul a din A cu seria $(a, 0, ..., 0, ..)$.

Seria $(0, 1, 0, ..., 0, ...)$ o notăm cu X şi o numim *nedeterminată*. Din regula de înmulţire a seriilor formale avem

$$X^2 = (0, 0, 1, 0, ..., 0, ...); \quad X^n = (\underbrace{0, 0, ..., 0}_{n}, 1, 0, ...), \quad (\forall) k \in \mathbb{N},$$

$$aX^n = (a, 0, 0, ..., 0, ...) \cdot (\underbrace{0, 0, ..., 0}_{n}, 1, 0, ...) = (\underbrace{0, 0, ..., 0}_{n}, a, 0, ...).$$

Ţinând cont de cele de mai sus, seria formală $f = (a_0, ..., a_n, ..)$ se scrie

$$f = a_0 + a_1 X + a_2 X^2 + ... + a_n X^n + ... = \sum_{i \geq 0} a_i X^i.$$

Elementele $a_i \in A$ se numesc coeficienţii seriei f.

Definiţia 6.1.1. *O serie formală din $A^{\mathbb{N}}$ care are un număr finit de coeficienţi nenuli se numeşte* ***polinom în nedeterminata X cu coeficienţi în A.***

Notăm cu $A[X]$ mulţimea polinoamelor în nedeterminata X cu coeficienţi în A.

Propoziţia 6.1.2. *Mulţimea $A[X]$ a polinoamelor în nedeterminata X cu coeficienţi în A este subinel al inelului $A^{\mathbb{N}}$, deci este un inel unitar comutativ.*

Demonstraţie: Evident $0 = (0, 0, .., 0, ..)$ şi $1 = (1, 0, ..., 0, ...)$ au număr finit de elemente nenule (0, respectiv 1), deci $A[X]$ conţine elementele neutre din $A^{\mathbb{N}}$. Fie $f, g \in A[X]$, deci ambii au număr finit de elemente nenule. Suma şi produsul lor, ca şi $-f$ au aceeaşi proprietate. □

Din definiţie, pentru $f = \sum_{i\geq 0} a_i X^i \in A[X]$, există $m \in \mathbb{N}$ astfel încât $a_i = 0$, $(\forall) i > m$, adică

$$f = a_0 + a_1 X + ... + a_m X^m.$$

Numărul $m = max\{i/a_i \neq 0\}$ se numeşte *gradul polinomului* f şi se notează $grad(f) = m$. Coeficientul a_m se numeşte *coeficientul dominant* al polinomului f, iar coeficientul a_0 se numeşte *termenul liber*.

Prin convenţie, gradul polinomului nul este $-\infty$ şi amintim următoarele reguli de calcul:

$$-\infty + n = -\infty, \quad (-\infty) \cdot n = -\infty, \quad -\infty - \infty = -\infty,$$

pentru orice $n \in \mathbb{N}$.

Propoziţia 6.1.3. *Dacă $f, g \in A[X]$, atunci au loc relaţiile următoare:*

a) $grad(f + g) \leq max(grad(f), grad(g))$;

b) $grad(f \cdot g) \leq grad(f) + grad(g)$. Dacă în plus $f, g \neq 0$ şi coeficienţii dominanţi ai celor două polinoame nu sunt divizori ai lui zero, atunci în relaţia anterioară avem egalitate.

Demonstraţie: a) Fie $f = \sum_{i=0}^{m} a_i X^i$ şi $g = \sum_{i=0}^{n} b_i X^i$, deci $grad(f) = m$, $grad(g) = n$.

$$f + g = \begin{cases} \sum_{i=0}^{m}(a_i + b_i)X^i + \sum_{i=m+1}^{n} b_i X^i, & m < n, \\ \sum_{i=0}^{m}(a_i + b_i)X^i, & m = n, \\ \sum_{i=0}^{n}(a_i + b_i)X^i + \sum_{i=n+1}^{m} a_i X^i, & m > n \end{cases}$$

În cazul $m = n$, dacă $a_n = -b_n$, atunci gradul polinomului $f + g$ este $n - 1$. În celelalte cazuri, $grad(f+g)$ este cel mai mare dintre gradele celor două polinoame.

b) Produsul celor două polinoame este

$$f \cdot g = (c_0, c_1, ..., c_i, ...), \quad c_i = \sum_{j+k=i} a_j b_k.$$

Cel mai mare indice cu $c_i \neq 0$ este $m+n$, dacă a_n şi b_m nu sunt divizori ai lui zero. □

Exemplul 6.1.1. *În inelul* $\mathbb{Z}_6[X]$, *fie* $f = \hat{2}X^2 + X + \hat{1}$, $g = \hat{3}X + \hat{2}$. *Produsul lor este*

$$f \cdot g = X^2 + \hat{5}X + \hat{1},$$

deoarece $\hat{2} \cdot \hat{3} = \hat{0}$.

O consecinţă directă a Propoziţiei 6.1.3 este:

Propoziţia 6.1.4. *Dacă A este un domeniu de integritate, atunci pentru orice $f, g \in A[X]$, $grad(f \cdot g) = grad(f) + grad(g)$.*

Avem şi următorul rezultat important de reţinut.

Propoziţia 6.1.5. *Dacă A este un domeniu de integritate, atunci şi inelul $A[X]$ este domeniu de integritate.*

Demonstraţie: Trebuie să demonstrăm că $A[X]$ nu are divizori ai lui 0, deci un produs $f \cdot g$ este polinomul nul doar dacă unul dintre factori este 0.

Fie $f, g \in A[X]$, $f \cdot g = 0$. Deoarece A este integru, conform Propoziţiei 6.1.4, $grad(f) + grad(g) = -\infty$, ceea ce nu este posibil dacă $f \neq 0$ şi $g \neq 0$. □

Încheiem acest paragraf cu modul în care un morfism între două inele unitare comutative induce un morfism între inelele de polinoame într-o nedeterminată, cu coeficienţi în cele două inele, respectiv.

Propoziţia 6.1.6. *Fie $(A, +, \cdot)$, $(B, +, \cdot)$ două inele unitare comutative şi morfismul unitar de inele $\varphi : A \to B$. Aplicaţia*

$$\varphi^* : A[X] \to B[X], \quad \varphi^*(a_0 + a_1X + ... + a_nX^n) = \varphi(a_0) + \varphi(a_1)X + ... + \varphi(a_n)X^n,$$

$(\forall) f = a_0 + a_1 X + ... + a_n X^n \in A[X]$, *este un morfism unitar de inele. Mai mult, are loc egalitatea* $\varphi^*(X) = X$ *şi morfismul* φ^* *face următoarea diagramă comutativă:*

$$\begin{array}{ccc} A & \stackrel{\varphi}{\to} & B \\ i_A \downarrow & & \downarrow i_B \\ A[X] & \stackrel{\varphi^*}{\to} & B[X] \end{array},$$

adică $\varphi^* \circ i_A = i_B \circ \varphi$.

Demonstraţie: Modul de definire a funcţiei φ^* şi faptul că φ este morfism de inele asigură

$$\varphi^*(f+g) = \varphi^*(f) + \varphi^*(g), \quad \varphi^*(f \cdot g) = \varphi^*(f) \cdot \varphi^*(g),$$

iar $\varphi^*(X) = X$ este evident.

Pentru orice $a \in A$, avem

$$\varphi^* \circ i_A(a) = \varphi^*(a) = \varphi(a) \in B,$$

şi $i_B \circ \varphi(a) = \varphi(a)$, deci diagrama este comutativă. □

6.2 Elemente inversabile în inele de polinoame

Fie $(A, +, \cdot)$ un inel unitar comutativ şi $A[X]$ inelul polinoamelor în nedeterminata X, cu coeficienţi în A. Amintim că $U(A)$ reprezintă mulţimea elementelor inversabile ale inelului A.

Propoziţia 6.2.1. *a) Fie* $a \in A$. *Avem* $a \in U(A) \Leftrightarrow a \in U(A[X])$, *unde identificăm polinomul constant* $a \in A[X]$ *cu elementul* a *din* A.

b) Dacă A *este inel inegru, atunci* $A[X]$ *este inel integru şi* $U(A) = U(A[X])$.

Demonstraţie: a) Implicaţia directă este evidentă: din moment ce a are un invers a' în A, polinomul constant a are ca invers polinomul constant a', în $A[X]$.

Reciproc, considerăm un polinom constant inversabil $a \in A[X]$ şi fie $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ inversul său. Din egalitatea $a \cdot f = 1$, rezultă sistemul

$$\left\{ \begin{array}{rcll} a \cdot a_0 & = & 1 & \\ a \cdot a_i & = & 0, & (\forall) i = \overline{1,n} \end{array} \right.$$

Din prima ecuaţie obţinem a inversabil în A, cu inversul a_0 şi din celelalte, deoarece a este inversabil, avem $a_i = 0$, $(\forall) i = \overline{1,n}$.

b) În cazul inelului integru A, am văzut în Propoziţia 6.1.5 că $A[X]$ este de asemenea integru.

Punctul a) asigură incluziunea $U(A) \subseteq U(A[X])$.

Pentru incluziunea inversă, fie $f = \sum_{i=0}^{n} a_i X^i \in U(A[X])$ şi $g = \sum_{i=0}^{m} b_i X^i \in U(A[X])$ inversul său. Deoarece $f \cdot g = 1$ şi A integru, Propoziţia 6.1.4 asigură

$$grad(f) + grad(g) = 0,$$

ceea ce se poate doar dacă ambele polinoame sunt constante. □

Observaţia 6.2.1. *Propoziţia 6.2.1 afirmă că dacă A este integru atunci singurele polinoame inversabile în $A[X]$ sunt polinoamele constante egale cu elemente inversabile în A.*

Exemplul 6.2.1. *a) $U(\mathbb{Z}[X]) = \{-1, 1\}$;*

b) Pentru K un corp comutativ, $U(K[X]) = K^*$.

c) Dacă A nu este integru, atunci există polinoame neconstante inversabile. De exemplu, $f = \widehat{2}X + \widehat{1} \in \mathbb{Z}_4[X]$ este inversabil, inversul său fiind el însuşi.

Ultimul exemplu de mai sus duce la întrebarea firească: care sunt polinoamele inversabile în $A[X]$, cu A inel cu divizori ai lui zero? Răspunsul este dat de:

Propoziţia 6.2.2. *Fie A un inel unitar comutativ şi $A[X]$ inelul polinoamelor cu coeficienţi în A. Au loc următoarele:*

a) $f \in A[X]$ este nilpotent dacă şi numai dacă toţi coeficienţii săi sunt elemente nilpotente din A.

b) $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ este inversabil dacă şi numai dacă $a_0 \in U(A)$ şi $a_1, ..., a_n$ sunt elemente nilpotente din A.

Demonstraţie: Amintim că un element x din inelul A este nilpotent dacă există $n \in \mathbb{N}$ astfel încât $x^n = 0$ (x aparţine idealului $\sqrt{0}$, vezi Propoziţia 5.3.5).

a) Fie f un polinom nilpotent din $A[X]$, deci există $n \in \mathbb{N}$, cu $f^n = 0$. Dacă f este polinomul nul, atunci rezultatul este evident.

Pentru $f \neq 0$, fie $m = gradf$. Demonstrăm prin inducţie după m că toţi coeficienţii lui f sunt nilpotenţi.

Pas 1. Verificare: $m = 0$, deci $f = a$, $a \in A$. Din $f^n = 0$ avem $a^n = 0$, deci a nilpotent în A.

Pas 2. Presupunem că orice polinom nilpotent de grad cel mult $m-1$ are toţi coeficienţii nilpotenţi şi arătăm că rezultatul e valabil şi pentru polinoamele de grad m. Fie

$$f = a_0 + a_1X + a_2X^2 + ... + a_mX^m,$$

un polinom nilpotent din $A[X]$.

Coeficientul dominant al polinomului f^n este a_m^n şi din $f^n = 0$ rezultă a_m nilpotent în A. De aici avem şi $(a_mX^m)^n = 0$, deci polinomul a_mX^m este de asemenea nilpotent în $A[X]$. Dar mulţimea elementelor nilpotente formează un ideal conform Propoziţiei 5.3.5, de unde obţinem că şi $f - a_mX^m$ este nilpotent. Din ipoteza de inducţie, polinomul

$$f - a_mX^m = a_0 + a_1X + ... + a_{m-1}X^{m-1},$$

are toţi coeficienţii nilpotenţi, deci toţi coeficienţii polinomului f sunt nilpotenţi.

Reciproc, fie elementele a_0, a_1,...,a_m nilpotente în A şi polinomul

$$f = a_0 + a_1X + a_2X^2 + ... + a_mX^m.$$

Din faptul că elementele $a_0, a_1, ..., a_m$ sunt nilpotente rezultă că şi polinoamele a_0, a_1X, a_2X^2,...,a_mX^m sunt nilpotente. Mulţimea elementelor nilpotente în $A[X]$ fiind ideal, este parte stabilă la adunare, deci f este nilpotent.

b) Fie polinomul $f = \sum_{i=0}^{m} a_iX^i \in A[X]$, unde termenul liber a_0 este inversabil şi restul coeficienţilor sunt nilpotenţi. Conform punctului anterior, polinomul $g = a_1X + a_2X^2 + ... + a_mX^m$ este nilpotent în $A[X]$, iar din Propoziţia 6.2.1, polinomul constant a_0 este inversabil. Aplicăm rezultatul din exerciţiul 18 propus la finalul capitolului anterior şi obţinem a_0+g inversabil, deci f inversabil.

Reciproc, fie $f = \sum_{i=0}^{m} a_iX^i \in U(A[X])$. Evident, $f \neq 0$. Vom demonstra prin inducţie după $m = grad(f)$ că $a_0 \in U(A)$ şi a_1,....,a_m nilpotente.

Pas 1. Verificare: Pentru polinoamele constante rezultatul este valabil conform Propoziţiei 6.2.1.

Pas 2. Presupunem că toate polinoamele inversabile de grad cel mult $m-1$ din $A[X]$ au termenul liber inversabil şi restul coeficienţilor nilpotenţi şi arătăm că polinoamele inversabile de grad m au aceeaşi proprietate.

Fie $f = \sum_{i=0}^{m} a_iX^i \in U(A[X])$. Există

$$g = b_0 + b_1X + ... + b_nX^n \in A[X], \quad f \cdot g = 1.$$

Obţinem sistemul

$$\begin{cases} a_0 \cdot b_0 & = & 1 \\ a_1 \cdot b_0 + a_0 \cdot b_1 & = & 0 \\ a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2 & = & 0 \\ ..... & .. & ... \\ a_m \cdot b_{n-1} + a_{m-1} \cdot b_n & = & 0 \\ a_m \cdot b_n & = & 0, \end{cases}$$

Înmulţind penultima ecuaţie din sistem cu a_m şi ţinând cont de ultima ecuaţie, rezultă $a_m^2 \cdot b_{n-1} = 0$. Repetând procedeul cu celelalte ecuaţii, obţinem, din aproape în aproape, $a_m^k \cdot b_{n-k+1} = 0$, care pentru $k = n+1$ duce la

$$a_m^{n+1} \cdot b_0 = 0.$$

Dar b_0 este inversabil conform primei ecuaţii din sistem. Am obţinut a_m nilpotent, deci şi polinomul $a_m X^m$ este nilpotent. Polinomul f este inversabil din ipoteză şi aplicăm din nou exerciţiul 18 propus la finalul caiptolului anterior, de unde rezultă

$$f - a_m X^m = a_0 + a_1 X + ...a_{m-1} X^{m-1} \in U(A[X]).$$

Din ipoteza de inducţie rezultă $a_0 \in U(A)$ şi $a_1, ..., a_{m-1}$ nilpotenţi. □

Exemplul 6.2.2. *Pentru a găsi ce polinoame de grad 1 din $\mathbb{Z}_4[X]$ sunt inversabile, stabilim mai întâi $U(\mathbb{Z}_4) = \{\hat{1}, \hat{3}\}$, (vezi Propoziţia 4.4.1)şi $\sqrt{0} = \{\hat{0}, \hat{2}\}$. Din Propoziţia 6.2.2 rezultă că $f = a + bX \in U(\mathbb{Z}_4)$ dacă şi numai dacă $a \in U(\mathbb{Z}_4)$ şi $b \in \sqrt{0}$. Avem şi $b \neq 0$, deci obţinem polinoamele $\hat{1} + \hat{2}X$, $\hat{3} + \hat{2}X$.*

Observaţia 6.2.2. *În inelele de polinoame există elemente nenule şi neinversabile care nu sunt divizori ai lui zero. Polinomul $\hat{2} + X$ nu este inversabil, şi nu există niciun polinom nenul $g \in \mathbb{Z}_4[X]$ astfel încât $(\hat{2} + X) \cdot g = 0$.*

6.3 Rădăcini ale polinoamelor

Fie $(A, +, \cdot)$ un inel unitar comutativ şi $A[X]$ inelul polinoamelor cu coeficienţi în A, iar i morfismul incluziune

$$i : A \to A[X], \quad i(a) = a, \quad (\forall) a \in A.$$

Următorul rezultat se numeşte **Proprietatea de universalitate a inelului de polinoame**:

Propoziţia 6.3.1. *Oricare ar fi inelul unitar comutativ* $(B, +, \cdot)$ *şi morfismul unitar de inele* $v : A \to B$*, pentru un element fixat arbitrar* $x \in B$*, există un unic morfism de inele*

$$\varphi : A[X] \to B,$$

care satisface condiţiile: $\varphi(X) = x$*,* $\varphi \circ i = v$*.*

Demonstraţie: Definim $\varphi : A[X] \to B$ prin

$$\varphi(a_0+a_1X+...+a_nX^n) = v(a_0)+v(a_1)x+...+v(a_n)x^n, \quad (\forall) f = \sum_{i=0}^{n} a_iX^i \in A[X].$$

Din faptul că v este morfism de inele şi din proprietăţile de asociativitate, distributivitate, ale operaţiilor din inelele $A[X]$, A, B, obţinem prin calcul direct că φ este morfism unitar de inele.

Pentru $f = X$, din definiţia funcţiei φ avem $\varphi(X) = x$.

Pentru orice $a \in A$, are loc

$$(\varphi \circ i)(a) = \varphi(a) = v(a),$$

deci $\varphi \circ i = v$.

Fie $\xi : A[X] \to B$ un morfism unitar de inele astfel încât $\xi(X) = x$ şi $\xi \circ i = v$. Atunci au loc relaţiile:

$$\xi(a) = \xi(i(a)) = (\xi \circ i)(a) = v(a), \quad (\forall) a \in A,$$

$$\xi(X^k) = \xi(X \cdot X^{k-1}) = \xi(X)\xi(X^{k-1}) = x^k, \quad (\forall) k \in \mathbb{N}^*.$$

Din cele de mai sus şi din faptul că funcţia ξ este morfism de inele, rezultă

$$\xi(a_0 + a_1X + ... + a_nX^n) = \xi(a_0) + \xi(a_1)\xi(X) + ... + \xi(a_n)\xi(X^n) =$$

$$= v(a_0) + v(a_1)x + ... + v(a_n)x^n = \varphi(a_0 + a_1X + ... + a_nX^n),$$

pentru orice $f = \sum_{i=0}^{n} a_iX^i \in A[X]$, deci $\xi = \varphi$, adică morfismul este unic. □

Fie A un inel unitar comutativ şi B un subinel al său. Atunci incluziunea

$$u : B \to A, \quad u(b) = b, \quad (\forall) b \in B,$$

este morfism unitar de inele. Aplicând Propoiziţia 6.3.1 inelului B, morfismului u, şi elementului fixat arbitrar $x \in B$, rezultă că există în mod unic un morfism unitar de inele

$$\varphi_x : A[X] \to A,$$

care asociază fiecărui polinom $f = \sum_{i=0}^{n} a_i X^i$ elementul $\varphi_x(f)$, pe care îl notăm $f(x)$ şi îl numim *valoarea polinomului* f în x. Obţinem

$$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n,$$

din definiţia morfismului φ dată în demonstraţia Propoziţiei 6.3.1.

Definiţia 6.3.1. *Un element $x \in B$ se numeşte **rădăcină** a polinomului f dacă $f(x) = 0$.*

Exemplul 6.3.1. *Elementul $x = 2 \in \mathbb{Z}$ este rădăcină a polinomului $f = X^2 - 4 \in \mathbb{Z}[X]$.*

Polinomul $f = 2X + 1 \in \mathbb{Q}[X]$ nu are rădăcini în subinelul $\mathbb{Z} \subset \mathbb{Q}$, dar are rădăcina $x = -\frac{1}{2} \in \mathbb{Q}$.

Polinomul $f = \widehat{3} + \widehat{3}X \in \mathbb{Z}_6[X]$ are trei rădăcini în $\mathbb{Z}_6[X]$: $\widehat{1}$, $\widehat{3}$, $\widehat{5}$.

De multe ori polinoame cu coeficienţi într-un corp nu au toate rădăcinile în corpul respectiv, ci într-o extindere a acestuia.

Exemplul 6.3.2. *a) Polinomul $X^2 + 1$ din $\mathbb{R}[X]$ nu are nicio rădăcină în $\mathbb{R}$, dar are toate rădăcinile în $\boldsymbol{C}$.*

b) Polinomul $(X - 1)(X^2 - 2) \in \mathbb{Q}[X]$ are o rădăcină în $\mathbb{Q}$ şi două în $\mathbb{R} - \mathbb{Q}$.

Fie $f \in A[X]$ arbitrar ales. Putem asocia polinomului f o funcţie

$$\widetilde{f} : A \to A, \quad \widetilde{f}(x) = f(x), \quad (\forall) x \in A,$$

care asociază fiecărui element $x \in A$ valoarea polinomului f în x. Această funcţie se numeşte *funcţia polinomială asociată lui f.*

Exemplul 6.3.3. *Fie polinoamele $f = \widehat{1} + X$, $g = \widehat{1} + X^2 \in \mathbb{Z}_2[X]$. Funcţiile polinomiale asociate sunt:*

$$\widetilde{f} : \mathbb{Z}_2 \to \mathbb{Z}_2, \quad \widetilde{f}(\widehat{0}) = \widehat{1}, \quad \widetilde{f}(\widehat{1}) = \widehat{0},$$

,

$$\widetilde{g} : \mathbb{Z}_2 \to \mathbb{Z}_2, \quad \widetilde{g}(\widehat{0}) = \widehat{1}, \quad \widetilde{g}(\widehat{1}) = \widehat{0},$$

. Observăm că funcţiile polinomiale sunt egale, deşi polinoamele sunt diferite.

În continuare vom considera A un domeniu de integritate. Conform Propoziţiei 6.1.5, $A[X]$ este de asemenea un domeniu de integritate. Fie $f, g \in A[X]$.

Definiţia 6.3.2. *Spunem că polinomul g **divide** polinomul f şi scriem $g|f$ dacă există $h \in A[X]$ astfel încât $f = g \cdot h$.*

Este evident că $f|f$, $1|f$, $f|0$, pentru orice $f \in A[X]$.

Propoziţia 6.3.2. *Fie A inel integru comutativ, $f \in A[X]$ şi $x \in A$. Următoarele afirmaţii sunt echivalente:*
a) x_0 este rădăcină a lui f;
b) $(X - x_0)$ divide f.

Demonstraţie: A doua afirmaţie o implică pe prima în mod evident: dacă $f = (X - x_0) \cdot h$ în $A[X]$, atunci

$$f(x_0) = 0 \cdot h(x_0) = 0.$$

Reciproc, dacă $f(x_0) = 0$, atunci putem calcula

$$f = f - f(x_0) = a_1(X - x_0) + a_2(X^2 - x_0^2) + ... + a_n(X^n - x_0^n),$$

de unde, ţinând cont că în inelul comutativ $A[X]$ avem descompunerea

$$X^k - x_0^k = (X - x_0)(X^{k-1} + X^{k-2}x_0 + ... + x_0^{k-1}),$$

rezultă

$$f = (X-x_0)[a_nX^{n-1}+(a_nx_0+a_{n-1})X^{n-2}+...+(a_nx_0^{n-1}+a_{n-1}x_0^{n-2}+...+a_2x_0+a_1)],$$

deci $(X - x_0)$ divide f. □

Observaţia 6.3.1. *Pentru $x_0 \in A$ un element oarecare şi $f \in A[X]$, un calcul asemănător celui din demonstraţia Propoziţiei anterioare duce la*

$$f = (X - x_0)[a_nX^{n-1} + (a_nx_0 + a_{n-1})X^{n-2} + ...+$$
$$+(a_nx_0^{n-1} + a_{n-1}x_0^{n-2} + ... + a_2x_0 + a_1)] + f(x_0),$$

unde polinomul

$$a_nX^{n-1} + (a_nx_0 + a_{n-1})X^{n-2} + ... + (a_nx_0^{n-1} + a_{n-1}x_0^{n-2} + ... + a_2x_0 + a_1),$$

şi elementul $f(x_0)$ se numesc câtul, respectiv restul împărţirii lui f prin $X - x_0$.

Observaţia 6.3.2. *Relaţia de mai sus se poate descrie într-o schemă, numită* ***Schema lui Horner****.*

$$\begin{array}{c|cccccc} & a_n & a_{n-1} & \dots & a_1 & a_0 \\ \hline x_0 & a_n & x_0 \cdot a_n + a_{n-1} & \dots & a_n x_0^{n-1} + a_{n-1} x_0^{n-2} + \dots + a_2 x_0 + a_1 & f(x_0) \end{array},$$

care furnizează câtul şi restul împărţirii unui polinom printr-un polinom de forma $X - x_0$*.*

Dacă $a \in U(A)$, atunci schema lui Horner poate determina câtul şi restul şi la împărţirea printr-un polinom de grad I, $aX + b$, după cum urmează:

Fie $g \in A[X]$, $r \in A$, cu $f = (aX + b)g + r$. Avem, echivalent,

$$f = a(X + a^{-1}b)g + r,$$

deci efectuând schema lui Horner pentru $X - (-a^{-1}b)$ găsim câtul la împărţirea prin $X - (-a^{-1}b)$, deci $a \cdot g$ şi restul r.

Exemplul 6.3.4. *Să se determine câtul şi restul împărţirii polinomului*

$$f = X^5 + 3X^4 - X^2 + 2X + 1 \in \mathbb{R}[X]$$

prin $g = 2X - 1$*.*

$$\begin{array}{c|cccccc} & 1 & 3 & 0 & -1 & 2 & 1 \\ \hline \frac{1}{2} & 1 & \frac{5}{2} & \frac{5}{4} & -\frac{3}{8} & \frac{29}{16} & \frac{61}{32} \end{array},$$

deci câtul este $\frac{1}{2}(X^4 + \frac{5}{2}X^3 + \frac{5}{4}X^2 - \frac{3}{8}X + \frac{29}{16})$*, iar restul este* $\frac{61}{32}$*.*

6.3.1 Rădăcini multiple

Propoziţia 6.3.2 din paragraful anterior sugerează utilizarea divizibilităţii în inelul $A[X]$ pentru a caracteriza rădăcinile unui polinom. O generalizare imediată este:

Definiţia 6.3.3. *Spunem că* $x \in A$ *este* ***rădăcină de ordin*** k *a lui* $f \in A[X]$ *dacă* $(X - x)^k | f$ *şi* $(X - x)^{k+1}$ *nu divide polinomul* f*.*

Propoziţia 6.3.3. *Dacă* A *este domeniu de integriate şi* $x \in A$ *este rădăcină multiplă de ordin* i *a lui* $f \in A[X]$*, respectiv este rădăcină multiplă de ordin* j *a lui* $g \in A[X]$*, atunci* x *este rădăcină multiplă de ordin* $i + j$ *a lui* $f \cdot g$*.*

Demonstraţie: Din definiţia rădăcinii multiple avem:

$$(X-x)^i | f \Rightarrow (\exists) h_1 \in A[X], \quad f = (X-x)^i h_1,$$

$$(X-x)^j | g \Rightarrow (\exists) h_2 \in A[X], \quad g = (X-x)^j h_2,$$

şi h_1, h_2 nu se divid prin $(X-x)$. Atunci

$$f \cdot g = (X-x)^{i+j} h_1 h_2,$$

iar $(X-x)^{i+j+1}$ nu divide $f \cdot g$, deci x este rădăcină multiplă de ordin $i+j$ pentru $f \cdot g$. □

Propoziţia 6.3.4. *Fie A un domeniu de integritate şi $f \in A[X]$, nenul. Dacă $x_1, x_2, ..., x_r \in A$ sunt rădăcini multiple distincte cu ordinele de multiplicitate $i_1, i_2, ..., i_r$, atunci există $g \in A[X]$, nenul, astfel încât*

$$f = (X-x_1)^{i_1}(X-x_2)^{i_2}...(X-x_r)^{i_r} \cdot g.$$

Demonstraţie: Din ipoteză x_1 e rădăcină de ordin i_1 a lui f, deci $(\exists) h_1 \in A[X]$ astfel încât $f = (X-x_1)^{i_1} h_1$, $h(x_1) \neq 0$, adică h_1 nu se divide prin $X - x_1$. Deoarece x_2 este rădăcină de ordin i_2, avem

$$(X-x_2)^{i_2} | (X-x_1)^{i_1} h_1.$$

Cum $(X-x_2)^{i_2}$ şi $(X-x_1)^{i_1}$ nu au factori comuni, rezultă $(X-x_2)^{i_2} | h_1$. Reluăm raţinamentul şi se obţine, din aproape în aproape, rezultatul dorit. □

O consecinţă importantă a Propoziţiei 6.3.4 este:

Propoziţia 6.3.5. *Dacă A este un domeniu de integritate şi $f \in A[X]$ este un polinom de grad n, atunci f are cel mult n rădăcini în A.*

Demonstraţie: Fie $x_1, x_2, ..., x_r \in A$ toate rădăcinile distincte ale lui f din A, cu ordinele de multiplicitate $i_1, i_2, ..., i_r$. Polinomul f are deci $m = i_1 + i_2 + ... + i_r$ rădăcini în A. Conform Propoziţiei anterioare, există $g \in A[X]$, nenul, astfel încât $f = (X-x_1)^{1_1}(X-x_2)^{i_2}...(X-x_r)^{i_r} g$. A fiind inel integru, $n = grad(f) = m + grad(g)$, iar g nenul implică $grad(g) \geq 0$. Rezultă $n \geq m$. □

Observaţia 6.3.3. *O consecinţă imediată este aceea că dacă $f \in A[X]$ de grad n are rădăcinile $x_1, ..x_n \in A$, atunci*

$$f = a(X - x_1)(X - x_2)...(X - x_n),$$

unde a este coeficientul dominant al polinomului f.

Observaţia 6.3.4. *Propoziţia 6.3.5 este valabilă doar pentru polinoame cu coeficienţi în domenii de integritate. Dacă A nu este inel integru, sau nu este comutativ, atunci se poate ca un polinom din $A[X]$ să aibă mai multe rădăcini decât gradul său.*

Exemplul 6.3.5. *a) Orice polinom de grad n cu coeficienţi reali are cel mult n rădăcini reale.*

b) $\mathbb{Z}_6$ nu este inel integru. De aceea Propoziţia 6.3.5 nu este valabilă în $\mathbb{Z}_6[X]$, unde polinomul de grad 1 $f = \widehat{3} + \widehat{3}X \in \mathbb{Z}_6[X]$ are trei rădăcini în $\mathbb{Z}_6[X]$: $\widehat{1}$, $\widehat{3}$, $\widehat{5}$.

c) Propoziţia 6.3.5 este valabilă pentru polinoamele cu coeficienţi în orice corp comutativ.

d) Corpul cuaternionilor este necomutativ. În acest corp, polinomul de grad 2 $f = 1+X^2$ are o infinitate de rădăcini. Într-adevăr, un element $b\cdot i+c\cdot j+d\cdot k \in \mathbb{H}$ cu $b^2 + c^2 + d^2 = 1$ este rădăcină a polinomului $X^2 + 1$. Există o infinitate de triplete (b, c, d) de numere reale cu această proprietate, de exemplu

$$(\frac{\sqrt{m}}{\sqrt{m+n+p}}, \frac{\sqrt{n}}{\sqrt{m+n+p}}, \frac{\sqrt{p}}{\sqrt{m+n+p}}), \quad (\forall)m, n, p \in \mathbb{N}^*.$$

Propoziţia 6.3.6. *Pentru un domeniu de integritate A şi $f = a_0 + a_1X + ... + a_nX^n \in A[X]$ cu $x_1, x_2, ..., x_n \in A$ toate rădăcinile sale, nu neapărat distincte, au loc egalităţile:*

$$-a_{n-1} = a_n(x_1 + x_2 + ... + x_n),$$

$$.....$$

$$(-1)^k a_{n-k} = a_n \sum_{1 \le i_1 \le ... \le i_k \le n} x_{i_1}x_{i_2}...x_{i_k},$$

$$.....$$

$$(-1)^n a_0 = a_n x_1 x_2 ... x_n.$$

Demonstraţie: Conform Propoziţiei 6.3.4, există $g \in A[X]$, nenul, astfel încât

$$f = (X - x_1)....(X - x_n)g.$$

Obţinem $grad(g) = 0$, apoi, desfăcând parantezele prin distributivitate, rezultă $g = a_n$. Egalând coeficienţii, obţinem relaţiile de mai sus între rădăcinile şi coeficienţii polinomului f, numite **Relaţiile lui** *Viète*. □

Exemplul 6.3.6. *Fie polinomul* $f = 2X^4 + 3X^3 - 4X^2 - X - 5 \in \mathbb{R}[X]$, *cu rădăcinile* x_1, x_2, x_3, x_4. *Relaţiile lui Viète se scriu astfel:*

$$\begin{cases} 2(x_1 + x_2 + x_3 + x_4) &= -3 \\ 2(x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4) &= -4 \\ 2(x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4) &= 1 \\ 2x_1x_2x_3x_4 &= -5 \end{cases}$$

Ca aplicaţie la relaţiile lui *Viète*, dăm o nouă demonstraţie Teoremei 4.4.2, numită Teorema lui Wilson, al cărei enunţ este:

Numărul natural $p \geq 2$ *este număr prim dacă şi numai dacă*

$$(p-1)! + 1 \equiv 0(mod \quad p).$$

Demonstraţie: Dacă p este prim, atunci $(\mathbb{Z}_p^*, \cdot)$ este grup abelian de ordin $p-1$, deci orice element al său este rădăcină a polinomului $X^{p-1} - \widehat{1} = \widehat{0}$. Aşadar rădăcinile acestui polinom sunt $\widehat{1}, \widehat{2}, ..., \widehat{p-1}$. Scriind ultima relaţie a lui *Viète*, găsim rezultatul dorit. □

6.4 Polinoame cu coeficienţi într-un corp comutativ

6.4.1 Derivata formală a unui polinom.

În acest paragraf dăm o caracterizare a rădăcinilor multiple ale polinoamelor cu coeficienţi într-un corp comutativ.

Fie K un corp comutativ şi $K[X]$ inelul polinoamelor în nedeterminata X cu coeficienţi în K. Principalul avantaj pe care îl oferă studiul polinoamelor cu

coeficienţi într-un corp este: toţi coeficienţii nenuli (deci şi coeficientul dominant) sunt inversabili.

Definim funcţia

$$d : K[X] \to K[X], \quad d(a) = 0, \quad d(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n-1} i a_i X^{i-1},$$

pentru orice $a, a_i \in K$, $i = \overline{1, n}$, $n \in \mathbb{N}^*$. Din definiţie, avem relaţiile

$$d(X^i) = iX^{i-1}, \quad d(X^{i+j}) = (i+j)X^{i+j-1} = iX^{i-1}X^j + jX^iX^{j-1}, \quad (\forall) i, j \geq 1.$$

Această funcţie se numeşte *derivarea polinoamelor*. Pentru un polinom f, polinomul $d(f)$ se numeşte *derivata polinomului* f.

Notăm

$$f^{(0)} = f, \quad f' = d(f),$$

şi $f^{(n)} = d(f^{(n-1)})$, numită *derivata de ordin* n a polinomului f.

Propoziţia 6.4.1. *Pentru orice* $f, g \in K[X]$, *avem:*

a) $d(f+g) = d(f) + d(g)$,

b) $d(af) = ad(f)$, $(\forall) a \in K$

c) $d(f \cdot g) = d(f) \cdot g + f \cdot d(g)$.

Demonstraţie: a) Fie $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{j=0}^{m} b_j X^j$, şi presupunem $n < m$.

$$d(f+g) = d(\sum_{i=0}^{m} (a_i + b_i) X^i) = \sum_{i=0}^{m-1} i(a_i + b_i) X^{i-1},$$

unde am notat $a_i = 0$, $(\forall) i > n$.

$$d(f) + d(g) = \sum_{i=0}^{n-1} i a_i X^{i-1} + \sum_{i=0}^{m-1} i b_i X^{i-1} = \sum_{i=0}^{m-1} i(a_i + b_i) X^{i-1},$$

cu aceeaşi convenţie pentru $a_i = 0$, $i > n$.

b) Prin calcul direct, după definiţie.

c) $f \cdot g = \sum_{k=0}^{m+n} c_k X^k$, cu $c_k = \sum_{i+j=k} a_i b_j$. Folosind aditivitatea derivatei formale, avem

$$d(f \cdot g) = \sum_{k=0}^{m+n} d(c_k X^k) = \sum_{k=0}^{m+n} d(\sum_{i+j=k} a_i b_j X^{i+j}) =$$

$$= \sum_{k=0}^{m+n} \sum_{i+j=k} a_i b_j (iX^{i-1}X^j + jX^i X^{j-1}) =$$

$$= \sum_{k=0}^{m+n} \sum_{i+j=k} ia_i b_j X^{i-1}X^j + \sum_{k=0}^{m+n} \sum_{i+j=k} a_i b_j j X^i X^{j-1} = d(f) \cdot g + f \cdot d(g).$$

□

Propoziţia 6.4.2. *Fie $f \in K[X]$ un polinom nenul de grad n şi $x_0 \in K$, arbitrar ales. Există elementele $b_i \in K$, $i = \overline{1,n}$, astfel încât polinomul f se poate scrie*

$$f = \sum_{i=0}^{n} b_i (X - x_0)^i.$$

Dacă, în plus, $car(K) = 0$, atunci scrierea este unică.

Demonstraţie: Pentru $n = 0$, $f = a_0$, $b_0 = a_0$. Vom demonstra prin inducţie după $n \geq 1$.

Pas 1. Verificare: $n = 1$, $f = a_0 + a_1 X$ putem să îl scriem

$$f = a_0 + x_0 \cdot a_1 + a_1(X - x_0), \quad b_0 = a_0 + x_0 \cdot a_1, \quad b_1 = a_1.$$

Pas 2. Presupunem că orice polinom de grad cel puţin $n-1$ admite o scriere ca în enunţ şi demonstrăm că $f = a_0 + a_1 X + ... + a_n X^n$ are aceeaşi proprietate.

Considerăm polinomul $h = f - f(x_0)$, care verifică $h(x_0) = 0$, deci admite rădăcina x_0. Conform Propoziţiei 6.3.2, $X - x_0$ divide h, deci există $g \in K[X]$ astfel încât $h = (X - x_0) \cdot g$, deci

$$f = (X - x_0) \cdot g + f(x_0).$$

Deoarece g este un polinom de grad $n - 1$, din ipoteza de inducţie rezultă că se poate scrie de forma

$$g = \sum_{i=0}^{n-1} c_i (X - x_0)^i, \quad c_i \in K, \quad i = \overline{1, n-1}.$$

Obţinem

$$f = \sum_{i=0}^{n-1} c_i (X - x_0)^{i+1} + f(x_0),$$

deci f admite scrierea dorită, cu $b_i = c_{i-1}$, $(\forall) i = \overline{1,n}$ şi $b_0 = f(x_0)$.

Fie $f = \sum_{i=0}^{n} b_i (X - x_0)^i$. Calculând derivatele lui f în x_0 şi ţinând cont de $b_0 = f(x_0)$, obţinem

$$k! b_k = f^{(k)}(x_0), \quad (\forall) k = \overline{0,n}.$$

În ipoteza $car(K) = 0$, elementul $k!1 \in K$ este nenul, deci inversabil şi din relaţiile de mai sus putem exprima în mod unic coeficienţii b_i prin valorile derivatelor polinomului f în x_0:

$$b_k = f^{(k)}(x_0) \cdot (k!1)^{-1}, \quad (\forall) k = \overline{0,n}.$$

□

Observaţia 6.4.1. *Într-un corp de caracteristică pozitivă p, avem $k!1 = 0$ pentru orice $k \geq p$ şi coeficienţii b_k nu pot fi determinaţi din relaţiile $k! b_k = f^{(k)}(x_0)$.*

Teorema 6.4.1. *Fie K un corp comutativ, $f \in K[X]$ polinom nenul, $r \geq 1$ un număr natural şi $x_0 \in K$.*

a) Dacă x_0 este rădăcină multiplă de ordinul r a lui f, atunci

$$f^{(i)}(x_0) = 0, \quad i = \overline{1, r-1}. \quad (*)$$

Dacă, în plus, $car(K) = 0$, atunci are loc şi $f^{(r)}(x_0) \neq 0$.

b) Pentru $car(K) = 0$, dacă $x_0 \in K$ verifică relaţia (*) de mai sus, atunci x_0 este rădăcină multiplă de ordinul r a lui f.

Demonstraţie: Aplicând Propoziţia 6.4.2 polinomului f şi elementului x_0, există $b_i \in K$ astfel încât $f = \sum_{i=0}^{n} b_i (X - x_0)^i$, cu $k! b_k = f^{(k)}(x_0)$, $(\forall) k = \overline{0,n}$.

a) Dacă x_0 este rădăcină multiplă de ordinul r a lui f, atunci $(X - x_0)^r | f$, deci toţi coeficienţii b_i, cu $i = \overline{0, r-1}$ sunt nuli, iar $b_r \neq 0$. Rezultă $f^{(i)}(x_0) = 0$, $(\forall) i = \overline{0, r-1}$. Pentru $car(K) = 0$, $r!1 \neq 0$ şi obţinem acelaşi rezultat.

b) Fie $car(K) = 0$ şi

$$f^{(i)}(x_0) = 0, \quad i = \overline{1, r-1}, \quad f^{(r)}(x_0) \neq 0.$$

Deoarece în corpurile de caracteristică nulă coeficienţii b_k sunt unic determinaţi de valorile $f^{(k)}(x_0)$, rezultă

$$b_i = 0, \quad i = \overline{1, r-1}, \quad b_r \neq 0 \Rightarrow f = b_r (X - x_0)^r + ... + b_n (X - x_0)^n,$$

deci x_0 este rădăcină multiplă de ordin r. □

Exemplul 6.4.1. *Polinomul*

$$f = 1 + X + \frac{1}{2!}X^2 + ... + \frac{1}{n!}X^n \in \mathbb{R}[X],$$

nu are rădăcini multiple.

Într-adevăr, dacă presupunem prin absurd că α este o radăcină multiplă, atunci $f(\alpha) = 0$, $f'(\alpha) = 0$, adică

$$1 + \alpha + \frac{1}{2!}\alpha^2 + ... + \frac{1}{n!}\alpha^n = 0,$$

$$1 + \alpha + \frac{1}{2!}\alpha^2 + ... + \frac{1}{(n-1)!}\alpha^{n-1} = 0,$$

de unde obţinem

$$\frac{1}{n!}\alpha^n = 0 \Rightarrow \alpha = 0.$$

Dar $f(0) \neq 0$.

Folosind derivata formală a unui polinom, se stabileşte următoarea legătură între un polinom $f \in K[X]$ şi derivata sa:

Propoziţia 6.4.3. *Fie K un corp comutativ şi $f \in K[X]$ un polinom de grad n, cu rădăcinile $x_1, ..., x_n \in K$, iar f' derivata sa. Atunci putem scrie, în corpul de fracţii al inelului $K[X]$, egalitatea*

$$f' = f \cdot \left(\frac{1}{X - x_1} + \frac{1}{X - x_2} + ... + \frac{1}{X - x_n} \right).$$

Demonstraţie: Conform Observaţiei 6.3.3,

$$f = a(X - x_1)(X - x_2)...(X - x_n), \quad a \in K.$$

Aplicând regulile din Propoziţia 6.4.1, calculăm

$$f' = a(X - x_2)...(X - x_n) + a(X - x_1)(X - x_3)...(X - x_n) + ...+$$
$$+a(X - x_1)(X - x_2)...(X - x_{n-1}).$$

În corpul de fracţii al inelului $K[X]$ putem continua calculul lui f' dând factor comun forţat $f = a(X - x_1)(X - x_2)...(X - x_n)$ şi obţinem rezultatul dorit. □

Exemplul 6.4.2. *Se dă polinomul* $f = X^n + X + 5 \in \boldsymbol{C}[X]$, *cu rădăcinile* $x_1, x_2, ..., x_n \in \boldsymbol{C}$. *Conform Propoziţiei 6.4.3, avem egalitatea*

$$S = \sum_{i=1}^{n} \frac{1}{1 - x_i} = \frac{f'(1)}{f(1)} = \frac{n+1}{7}.$$

6.4.2 Teorema împărţirii cu rest în $K[X]$

Noţiunile de cât şi rest la împărţirea unui polinom f cu coeficienţi într-un inel comutativ A printr-un polinom $X - a$, introduse în Observaţia 6.3.1, sunt generalizate în acest paragraf pentru polinoame cu coeficienţi în corpuri comutative.

Teorema 6.4.2. *Fie* K *un corp comutativ şi* $f, g \in K[X]$, $g \neq 0$. *Atunci există* $q, r \in K[X]$ *astfel încât*

$$f = q \cdot g + r, \quad grad(r) < grad(g).$$

În plus, q *şi* r *sunt unic determinaţi şi se numesc* ***câtul****, respectiv* ***restul*** *împărţirii polinomului* f *prin polinomul* g.

Demonstraţie: Fie

$$f = a_0 + a_1X + a_2X^2 + ... + a_nX^n, \quad g = b_0 + b_1X + b_2X^2 + ... + b_mX^m.$$

Dacă $m > n$, atunci putem scrie

$$f = 0 \cdot g + f \Rightarrow c = 0, \quad r = f,$$

deci $grad(r) = n < grad(g)$.

Dacă $n \geq m$, facem demonstraţia prin inducţie după n.
Pas 1. Verificare $n = m$. Are loc

$$f = a_nb_n^{-1} \cdot g + (a_{n-1} - a_nb_n^{-1}b_{n-1})X^{n-1} + ... + a_0 - a_nb_n^{-1}b_0,$$

deci $q = a_nb_n^{-1}$, $r = (a_{n-1} - a_nb_n^{-1}b_{n-1})X^{n-1} + ... + (a_0 - a_nb_n^{-1}b_0)$, cu $grad(r) = n - 1 < grad(g)$.

Pas 2. Presupunem că pentru toate polinoamele de grad s, cu $n-1 \geq s \geq m$ există câtul şi restul la împărţirea prin g ca în enunţ şi demonstrăm că polinomul $f = a_0 + a_1X + a_2X^2 + ... + a_nX^n$ are aceeaşi proprietate. Putem scrie

$$f = a_n b_m^{-1} X^{n-m} \cdot g + h,$$

iar polinomului

$$h = (a_{n-1} - a_n b_m^{-1} b_{m-1})X^{n-1} + ... + (a_{n-m} - a_n b_m^{-1} b_0)X^{n-m} + a_{n-m-1}X^{n-m-1} + ... + a_0,$$

să-i aplicăm ipoteza de inducţie.

Există deci $c_1, r_1 \in K[X]$ astfel încât

$$h = g \cdot c_1 + r_1, \quad grad(r_1) < grad(g).$$

Obţinem

$$f = (a_n b_m^{-1} X^{n-m} + c_1) \cdot g + r_1, \quad grad(r_1) < grad(g),$$

deci există polinoamele $q = a_n b_m^{-1} X^{n-m} + c_1$, $r = r_1$ din $K[X]$ cu proprietăţile cerute.

În continuare demonstrăm unicitatea câtului şi restului. Fie $f = q \cdot g + r$,cu $q, r \in K[X]$ şi $grad(r) < grad(g)$. Presupunem că există şi $q'r'nK[X]$, cu aceleaşi proprietăţi. Are loc

$$f = q \cdot g + r = q' \cdot g + r' \Rightarrow (q - q') \cdot g = r' - r.$$

Dacă presupunem prin absurd că $q - q' \neq 0$, atunci

$$grad(r' - r) = grad((q - q') \cdot g = grad(q - q') + grad(g) > grad(g),$$

ceea ce contrazice faptul că polinoamele r şi r' sunt de grad mai mic strict decât $grad(g)$. Rezultă că presupunerea făcută este falsă, deci $q = q'$, ceea ce implică şi $r = r'$. □

Observaţia 6.4.2. *Câtul şi restul oferite de schema lui Horner pentru f şi $X - a$ sunt evident aceleaşi cu cele obţinute prin împărţire directă.*

O consecinţă importantă a Teoremei 6.4.2 este:

Propoziţia 6.4.4. *Inelul polinoamelor într-o nedeterminată cu coeficienţi într-un corp comutativ este inel principal.*

Demonstraţie: Trebuie să demonstrăm că orice ideal $I \in Id(K[X])$ este principal, deci generat de un singur element.

Evident, idealul $\{0\}$ este generat de polinomul nul.

Fie I un ideal diferit de idealul nul. El conţine deci şi polinoame de grad ≥ 0. Din proprietatea de bună ordonare a numerelor naturale, mulţimea

$$M = \{grad(f) | \quad f \in I, \quad f \neq 0\},$$

are un cel mai mic element.

Fie f_0 polinomul nenul de grad minim din I, cu coeficientul dominant 1. Un astfel de polinom există deoarece pentru orice polinom de grad minim n_0 din I, cu coeficientul dominant a, amplificatul acestuia cu polinomul constant a^{-1} este un polinom de tipul cerut. Vom arăta că I este generat de f_0.

Evident idealul generat de f_0, $(f_0) = \{f_0 \cdot g | \quad g \in K[X]\}$ este inclus în I.

Fie acum un element arbitrar $f \in I$. Din Teorema împărţirii cu rest în $K[X]$ există în mod unic $c, r \in K[X]$,

$$f = f_0 \cdot c + r, \quad grad(r) < grad(f_0).$$

Dar r trebuie să fie polinomul nul, altfel $r = f - f_0 \cdot c \in I$ ar fi un polinom nenul de grad mai mic decât $grad(f_0)$, ceeea ce ar contrazice alegerea lui f_0. Rezultă $f = f_0 \cdot g$, deci $I = (f_0)$. □

6.4.3 Polinoame ireductibile

Fie K un corp comutativ şi $f \in K[X]$ un polinom de grad ≥ 1.

Definiţia 6.4.1. *Polinomul f se numeşte **ireductibil în** $K[X]$ dacă nu poate fi scris ca produsul a două polinoame din $K[X]$, ambele cu gradul strict mai mic decât gradul lui f.*

Din definiţie rezultă că orice polinom de gradul 1 din $K[X]$ este ireductibil.

Din Propoziţia 6.3.2 avem:

Propoziţia 6.4.5. *Dacă polinomul $f \in K[X]$ are o rădăcină $x_0 \in K$, atunci f nu este ireductibil (spunem că este reductibil).*

Exemplul 6.4.3. *a)* $f = X^2 - 3X + 2 \in \mathbb{R}[X]$ *este reductibil,* 1 *fiind rădăcină a sa. Avem* $f = (X-1)(X-2)$.

b)$f = X^3 + \widehat{2}X^2 + \widehat{4}X + \widehat{3} \in \mathbb{Z}_5[X]$ *este reductibil,* $\widehat{1}$ *fiind rădăcină a sa. Avem* $f = (X + \widehat{4})(X^2 + \widehat{3}X + \widehat{2})$.

c) $f = X^2 + X + 1 \in \mathbb{R}[X]$ *este ireductibil.*

Un polinom din $K[X]$ poate fi reductibil şi dacă nu are rădăcini în K.

Exemplul 6.4.4. *a)* $f = X^4 + \widehat{1} \in \mathbb{Z}_2[X]$ *nu are rădăcini în* $\mathbb{Z}_2$*, dar*

$$f = (X^2 + \widehat{1})(X^2 + \widehat{1}).$$

b) $f = X^4 + X^2 + 1 \in \mathbb{R}[X]$ *nu are rădăcini reale, dar*

$$f = (X^2 + X + 1)(X^2 - X + 1).$$

Un polinom ireductibil în $K[X]$ poate fi reductibil în $E[X]$, unde E este o extindere comutativă a corpului K.

Exemplul 6.4.5. *Polinomul* $f = X^2 + X + 1$ *este ireductibil în* $\mathbb{R}[X]$*, dar reductibil (deoarece are rădăcini) în* $\boldsymbol{C}[X]$.

O consecinţă imediată a Propoziţiei 6.4.5 este:

Propoziţia 6.4.6. *Dacă polinomul* $f \in K[X]$ *de grad* ≥ 2 *este ireductibil, atunci nu are rădăcini în* K*. Mai mult, un polinom de grad* 2 *sau* 3 *este ireductibil în* $K[X]$ *dacă şi numai dacă nu are rădăcini în* K.

Afirmaţia nu este adevărată pentru polinoamele cu coeficienţi în inele care nu sunt corpuri.

Exemplul 6.4.6. *Polinomul* $f = \widehat{2}X^3 + X^2 + X + \widehat{3} \in \mathbb{Z}_4[X]$ *este reductibil,* $f = (\widehat{2}X + \widehat{1})(\widehat{3}X^2 + \widehat{3}X + \widehat{3})$*, dar nu are nicio rădăcină în* $\mathbb{Z}_4$.

Teorema 6.4.3. *[Teorema de descompunere în factori ireductibili]*

Orice polinom din $K[X]$ *se poate scrie ca un produs finit de polinoame ireductibile în* $K[X]$.

Demonstraţie: Vom demonstra prin inducţie după gradul polinomului. Fie $f \in K[X]$, $grad(f) = n$.

Pas 1. $n = 1$, $f = f$ este descompunerea cerută deoarece orice polinom de grad I este ireductibil.

Pas 2. Presupunem că orice polinom de grad cel mult $n-1$ din $K[X]$ se scrie ca produs finit de polinoame ireductibile şi fie $f \in K[X]$ de grad n. Dacă f este ireductibil, atunci descompunerea este $f = f$. Dacă f este reductibil, rezultă că există $g, h \in K[X]$ de grade strict mai mici decât n astfel încât $f = g \cdot h$.

Aplicând ipoteza de inducţie polinoamelor g şi h, obţinem descompunerea lui f în factori ireductibili. □

Propoziţia 6.4.7. *Dacă polinomul $f \in K[X]$ este ireductibil, atunci idealul generat de el în $K[X]$ este ideal maximal (vezi Definiţia 5.5.1).*

Demonstraţie: Fie $f \in K[X]$ ireductibil. Idealul generat de f este

$$(f) = \{g \cdot f | \quad g \in K[X]\},$$

şi în mod evident nu coincide cu $K[X]$, deci este ideal propriu. Vom arăta că singurul ideal propriu din $[(f), K[X]]$ este (f).

Fie $I \in Id(K[X])$, $(f) \subseteq I$. Conform Propoziţiei 6.4.4, inelul $K[X]$ este principal, deci $I = (h)$, $h \in K[X]$. Incluziunea $(f) \subseteq (h)$ duce la $f \in (h)$, deci f este un multiplu în $K[X]$ al lui h. Rezultă h divizor al lui f, care este polinom ireductibil. Obţinem $h = f$ sau h inversabil. În primul caz $I = (f)$, iar în al doliea $I = K[X]$. □

O consecinţă imediată a Propoziţiei 6.4.7, folosind Propoziţia 5.5.2, este:

Propoziţia 6.4.8. *Dacă polinomul $f \in K[X]$ este ireductibil, atunci inelul factor $K[X]/(f)$ este corp.*

Exemplul 6.4.7. *a) Să determinăm forma elementelor din inelul factor $\mathbb{Z}_2[X]/_{(X^2+X+1)}$. Prin $(X^2 + X + 1)$ înţelegem idealul generat de polinomul $f = X^2 + X + 1$ în inelul $\mathbb{Z}_2[X]$.*

Din definiţia inelului factor avem

$$\mathbb{Z}_2[X]/_{(X^2+X+1)} = \{\hat{g} | g \in \mathbb{Z}_2[X]\},$$

$$\hat{g} = \{h \in \mathbb{Z}_2[X] | \quad (X^2 + X + 1) | (g - h)\},$$

deci $\hat{g}$ conţine toate elementele din $\mathbb{Z}_2[X]$ care dau acelaşi rest cu g la împărţirea prin X^2+X+1. Dar restul respectiv poate fi doar un polinom de grad maxim 1 şi găsim

$$\mathbb{Z}_2[X]/_{(X^2+X+1)} = \{\hat{0}, \hat{1}, \widehat{X}, \widehat{X+1}\}.$$

Întocmind tablele operaţiilor de adunare şi înmulţire în inelul factor, se constată că este corp.

b) Inelul factor $\boldsymbol{C}[X]/(X^2+1)$ nu este integru. Într-adevăr, elementele inelului factor sunt clase de echivalentă ale polinoamelor de grad 1. Dar $\widehat{X-i} \cdot \widehat{X+i} = \hat{0}$, deci acest inel are divizori ai lui zero.

6.4.4 Corpul de descompunere a unui polinom

Propoziţia 6.4.9. *Fie K un corp comutativ şi $f \in K[X]$, cu $grad(f) \geq 1$. Există o extindere L a corpului K, care conţine cel puţin o rădăcină a polinomului f.*

Demonstraţie: Deoarece $grad(f) \geq 1$, conform Propoziţiei 6.2.1, f nu este inversabil.

Dacă f are rădăcini în K, acesta este corpul căutat (K).

Dacă f nu are nicio rădăcină în K, considerăm descompunerea sa în polinoame ireductibile în $K[X]$. Fie f_1 unul din aceşti factori. Fiind polinom ireductibil, conform Propoziţiei 6.4.8, inelul factor

$$K_1 = \frac{K[X]}{(f_1)},$$

este corp. Elementele acestui corp sunt clase de echivalenţă ale polinoamelor din $K[X]$ în raport cu relaţia de congruenţă modulo idealul (f_1).

Pentru un $g \in K[X]$ oarecare, din teorema împărţirii cu rest în $K[X]$, există $c, r \in K[X]$ astfel încât

$$g = f_1 \cdot c + r, \quad grad(r) < grad(f_1),$$

de unde rezultă că g şi restul său r la împărţirea prin f_1 determină aceeaşi clasă de echivalenţă.

Dacă $n_1 = grad(f_1)$, avem din cele de mai sus:

$$K_1 = \{[a_{n_1-1}X^{n_1-1} + ... + a_1X + a_0] | \quad [f_1] = 0\},$$

unde am notat $[g]$ clasa de echivalenţă a polinomului g, modulo idealul generat de polinomul f_1.

Din modul de definire a operaţiilor cu clase de echivalenţă obţinem

$$K_1 = \{a_{n_1-1}\epsilon^{n_1-1} + ... + a_1\epsilon + a_0| \quad f_1(\epsilon) = 0\},$$

unde am notat $\epsilon = [X]$, clasa de echivalenţă a polinomului X.

Rezultă că am obţinut o extindere K_1 a corpului K, în care f_1 are rădăcina ϵ.

Dar f_1 era factor al lui f, deci am găsit o extindere a lui K în care se află cel puţin o rădăcină a lui f. □

Din Propoziţia 6.4.9, reluând procedeul pentru descompunerea polinomului f în factori ireductibili în $K_1[X]$, obţinem:

Propoziţia 6.4.10. *Există o extindere a lui K în care se află toate rădăcinile polinomului $f \in K[X]$.*

Definiţia 6.4.2. *Fie K un corp comutativ şi $f \in K[X]$. Cea mai mică extindere a lui K în care se află toate rădăcinile lui f se numeşte* ***corpul de descompunere*** *a polinomului f.*

Exemplul 6.4.8. *Corpul numerelor complexe este corpul de descompunere a polinomului $X^2 + 1$, deoarece este cel mai mic corp care conţine $\pm i$.*

Corpul $\mathbb{R}$ nu este corpul de descompunere a polinomului

$$(X - 1)(X^2 - 2) \in \mathbb{Q}[X],$$

deşi conţine toate rădăcinile acestui polinom, ci $\mathbb{Q}(\sqrt{2})$, deoarece acesta este cel mai mic subcorp al lui $\mathbb{R}$, care conţine $-\sqrt{2}, \sqrt{2}$.

6.5 Criterii de ireductibilitate pentru polinoame

În acest paragraf particularizăm studiul la polinoamele ireductibile din $\mathbf{C}[X]$ şi $\mathbb{R}[X]$.

Ţinând cont de faptul că orice polinom din $\mathbf{C}[X]$ are toate rădăcinile complexe (Teorema fundamentală a algebrei) şi de Propoziţia 6.4.6, următorul enunţ precizează care sunt toate polinoamele ireductibile din $\mathbf{C}[X]$ şi $\mathbb{R}[X]$:

Propoziţia 6.5.1. *a) Polinomul $f \in \boldsymbol{C}[X]$ este ireductibil dacă şi numai dacă este de gradul I.*

b) Polinomul $f \in \mathbb{R}[X]$ este ireductibil dacă şi numai dacă este de gradul I sau de gradul II fără rădăcini reale.

Din Teorema de descompunere în factori ireductibili 6.4.3 şi din Propoziţia anterioară, avem:

Propoziţia 6.5.2. *a) Orice polinom $f \in \boldsymbol{C}[X]$, nenul şi neinversabil, se descompune în mod unic în produs de factori liniari (de gardul I) în $\boldsymbol{C}[X]$.*

b) Orice polinom $f \in \mathbb{R}[X]$, nenul şi neinversabil, se descompune în mod unic în produs de factori liniari (de gradul I) sau de gradul II fără rădăcini reale în $\mathbb{R}[X]$:

$$f = c(X-\alpha_1)^{k_1}...(X-\alpha_l)^{k_l}(X^2+p_1X+q_1)^{s_1}...(X^2+p_rX+q_r)^{s_r},$$

unde c este o constantă reală nenulă.

Dăm în continuare câteva criterii de ireductibilitate pentru polinoamele cu coeficienţi numerici.

Definiţia 6.5.1. *Un polinom $f \in \mathbb{Z}[X]$ se numeşte **primitiv** dacă nu admite ca factor un polinom constant.*

Din definiţia de mai sus rezultă că f este primitiv dacă cel mai mare divizor comun al coeficienţilor săi este 1.

Propoziţia 6.5.3. *[Criteriul lui Eisenstein] Fie $f = a_0 + a_1X + a_2X^2 + ... + a_nX^n \in \mathbb{Z}[X]$ un polinom primitiv. Dacă există un element prim $p \in \mathbb{Z}$ astfel încât p divide a_i, $(\forall)i = \overline{0, n-1}$, p nu divide a_n şi p^2 nu divide a_0, atunci f este ireductibil în $\mathbb{Z}[X]$.*

Demonstraţie: Presupunem prin absurd că f este reductibil în $\mathbb{Z}[X]$, deci există $g, h \in \mathbb{Z}[X]$, de grad cel puţin 1 fiecare, astfel încât $f = g \cdot h$. Fie

$$g = b_0 + b_1X + ... + b_mX^m, \quad h = c_0 + c_1X + ... + c_rX^r, \quad m + r = n.$$

Din egalitatea $f = g \cdot h$ obţinem sistemul

$$\begin{array}{c} a_0 = b_0c_0 \\ a_i = \sum_{k+l=i} b_kc_l \\ a_n = b_mc_r \end{array} .$$

Din ipoteza p duvide a_0, cu p prim, rezultă $p|b_0c_0$, deci $p|b_0$ sau $p|c_0$ şi deoarece p^2 nu divide a_0, rezultă că p divide exact unul dintre b_0 , c_0. Presupunem p divide b_0 şi p nu îl divide pe c_0.

Din ipoteza p nu divide a_n rezultă că p nu divide f (un polinom e divizibil printr-un număr dacă fiecare coeficient al său este un multiplu al acelui număr). Prin urmare p nu divide nici g. Există deci un coeficient b_i al polinomului g, nedivizibil prin p. Fie i_0 cel mai mic indice pentru care p nu divide b_{i_0}. Evident, $i_0 < n$. Avem

$$p|a_{i_0} \to p|\sum_{k+l=i_0} b_k c_l = b_{i_0}c_0 + \sum_{k+l=i_0, k<i_0} b_k c_l,$$

unde $p|b_k$, $(\forall)k < i_0$, deci $p|b_{i_0}c_0$. Dar aceasta contrazice faptul că p nu divide nici b_{i_0}, nici c_0. Deci presupunerea facută este falsă, aşadar f este ireductibil. □

Exemplul 6.5.1. *a) Pentru polinomul $f = 7 + 14X + 21X^3 + 3X^4 \in \mathbb{Z}[X]$, observăm că $7, 14, 21$ sunt multipli de 7, şi 7 nu divide 3 (coeficientul dominant) şi 7^2 nu divide termenul liber. Conform Criteriului lui Eisenstein pentru $p = 7$, f este ireductibil.*

b) $f = X^n + 2 \in \mathbb{Z}[X]$ este ireductibil, conform Criteriului Eisenstein pentru $p = 2$.

Să remarcăm faptul că un polinom ireductibil în $\mathbb{Z}[X]$ şi primitiv este ireductibil şi în $\mathbb{Q}[X]$.

Într-adevăr, dacă polinomul primitiv $f \in \mathbb{Z}[X]$ ar fi reductibil în $\mathbb{Q}[X]$, atunci s-ar scrie $f = g \cdot h$, cu $g, h \in \mathbb{Q}[X]$, şi $grad(g), grad(h) > 1$. Aducând la acelaşi numitor toţi coeficienţii din g, respectiv h şi notând a produsul numitorilor, am avea $af = g' \cdot h'$, cu $g', h' \in \mathbb{Z}[X]$. Dar f este primitiv, deci numărul a de fapt se simplifică cu divizori ai polinoamelor g', h', de unde rezultă f reductibil în $\mathbb{Z}[X]$, contradicţie.

Propoziţia 6.5.4. *Fie polinomul $f = a_0 + a_1X + ... + a_nX^n \in A[X]$, cu A inel integru. Polinomul f este ireductibil dacă şi numai dacă:*

a) $f(X + 1)$ este ireductibil în $A[X]$.

b) Termenul liber din f este nenul şi $r(f) = a_n + a_{n-1}X + ... + a_0$ este ireductibil în $A[X]$. Polinomul $r(f)$ se numeşte reciprocul polinomului f.

Demonstraţie: a) Demonstraţia se face prin reducere la absurd, remarcând că o descompunere $f = g \cdot h$ pentru f în nedeterminata X este echivalentă cu

$f(X+1) = g(X+1) \cdot h(X+1)$, deci cu o descompunere a lui f în nedeterminata $X+1$.

b) În corpul de facţii al inelului $A[X]$, avem $r(f) = X^n f(\frac{1}{X})$. Pentru polinoamele g, h de grade m, respectiv q, avem

$$r(g \cdot h) = X^{m+q}(g \cdot h)(\frac{1}{X}) = X^m g(\frac{1}{X}) X^q h(\frac{1}{X}) = r(g) \cdot r(h).$$

Mai mult, trecerea la polinomul reciproc păstrează gradul şi $f = r(r(f))$.

Fie f ireductibil şi presupunem $r(f)$ reductibil, deci $r(f) = g \cdot h$, atunci

$$f = r(r(f)) = r(g) \cdot r(h),$$

deci f reductibil, contradicţie. Analog implicaţia inversă. □

Exemplul 6.5.2. *a) Polinomul $f = X^{p-1} + X^{p-2} + ... + X + 1$, cu p număr întreg prim, este ireductibil în $\mathbb{Q}[X]$.*

Într-adevăr, observăm că $f(X) \cdot (X-1) = X^p - 1$, de unde $f(X+1) \cdot X = (X+1)^p - 1$, deci

$$f(X+1) \cdot X = X^p + C_p^1 X^{p-1} + C_p^2 X^{p-2} + ... + C_p^{p-1} X.$$

Obţinem $f(X+1) = X^{p-1} + pX^{p-2} + C_p^2 X^{p-3} + ... + C_p^{p-2} + p$. Conform criteriului lui Eisenstein, $f(X+1)$ este ireductibil în $\mathbb{Q}[X]$, deci la fel este şi f.

b) Polinomul $f = 3X^7 - 15X^3 + 6X^2 + 24X + 5 \in \mathbb{Z}[X]$ este ireductibil deoarece reciprocul său, $r(f) = 5X^7 + 24X^6 + 6X^5 - 15X^4 + 3$ este ireductibil conform Criteriului lui Eisenstein pentru $p = 3$.

Fie $f = a_0 + a_1 X + a_2 X^2 + ... + a_n X^n \in A[X]$ un polinom primitiv şi B un inel comutativ pentru care există $u : A \to B$ morfism de inele astfel încât $u(a_n) \neq 0$. Conform Propoziţiei **??**, acest morfism se extinde la morfismul de inele $u^* : A[X] \to B[X]$.

Propoziţia 6.5.5. *Dacă $u^*(f) = u(a_0) + u(a_1)X + u(a_2)X^2 + ... + u(a_n)X^n$ este ireductibil în $B[X]$, atunci f este ireductibil în $A[X]$.*

Exemplul 6.5.3. *Polinomul $f = 3X^3 + 8X^2 + 17X + 7 \in \mathbb{Z}[X]$ este ireductibil deoarece pentru morfismul $s : \mathbb{Z} \to \mathbb{Z}_2$, $s^*(f) = X^3 + X + 1 \in \mathbb{Z}_2[X]$ este ireductibil, neavând nicio rădăcină în $\mathbb{Z}_2$ (vezi Propoziţia 6.4.6).*

6.6 Exerciţii

1. Să se determine elementele inversabile în fiecare dintre următoarele inele de polinoame:
$(\mathbb{Z}[X],+,\cdot)$, $(\mathbb{Q}[X],+,\cdot)$, $\mathbb{R}[X],+,\cdot)$, $(\mathbf{C}[X],+,\cdot)$, $(\mathbb{Z}_p[X],+,\cdot)$, pentru p prim.

2. Scrieţi toate polinoamele inversabile de grad 2 din $(\mathbb{Z}_4[X],+,\cdot)$ şi determinaţi inversul elementului $f=2X^2+2X+1\in\mathbb{Z}_4[X]$.

Indicaţie: Folosim Propoziţia 6.2.2.

3. a) Fie $(A,+,\cdot)$ un domeniu de integritate infinit şi $f,g\in A[X]$. Să se arate că $f=g$ dacă şi numai dacă funcţiile polinomiale $\tilde{f}$, $\tilde{g}$ sunt egale.
b) Fie $(A,+,\cdot)$ un domeniu de integritate finit cu n elemente, $A=\{a_1,a_2,...,a_n\}$ şi $f,g\in A[X]$. Să se arate că $\tilde{f}=\tilde{g}$ dacă şi numai dacă

$$(X-a_1)(X-a_2)...(X-a_n)|(f-g).$$

Indicaţie: a) Implicaţia directă este evidentă. Dacă $\tilde{f}=\tilde{g}$, atunci $(\forall)a\in A$ este rădăcină a polinomului $f-g\in A[X]$. Presupunem prin absurd $f\neq g$, deci polinomul de grad finit $f-g$ are o infinitate de rădăcini. Contradicţie cu Propoziţia 7.3.4.
b) Ca mai sus, a_i este rădăcină a polinomului $f-g$, $(\forall)i=\overline{1,n}$, iar Propoziţia 6.3.2 asigură $(X-a_1)(X-a_2)...(X-a_n)|(f-g)$.

Observaţia 6.6.1. *Rezultatul de la punctul a) permite aplicarea metodei coeficienţilor nedeterminaţi pentru polinoame cu coeficienţi în domenii de integritate infinite.*

4. Determinaţi forma elementelor din inelul factor $\mathbb{Z}_2[X]/_{(X^3+X+1)}$. Calculaţi $\widehat{X^2+1}\cdot\widehat{X^2+X}+1$. Este acest inel corp? Justificaţi!

Indicaţie: Din definiţia inelului factor avem

$$\mathbb{Z}_2[X]/_{(X^3+X+1)}=\{\hat{g}|\quad g\in\mathbb{Z}_2[X]\}\quad \hat{g}=\{h\in\mathbb{Z}_3[X]|\quad (X^3+X+1)|(g-h)\},$$

deci $\hat{g}$ conţine toate elementele din $\mathbb{Z}_2[X]$care dau acelaşi rest cu g la împărţirea prin X^3+X+1. Dar restul respectiv poate fi doar un polinom de grad maxim 2 şi obţinem

$$\mathbb{Z}_2[X]/_{(X^3+X+1)}=\{\hat{0},\hat{1},\hat{X},\widehat{X+1},\widehat{X^2},\widehat{X^2+1},\widehat{X^2+X},\widehat{X^2+X+1}\}.$$

Întocmind tablele operaţiilor de adunare şi înmulţire în inelul factor, se constată că este corp, sau , folosind Propoziţia 6.4.8, este suficient să stabilim dacă polinomul $X^3 + X + 1$ este ireductibil. Deoarece este un polinom de grad 3, este suficient să verificăm dacă are rădăcini în $\mathbb{Z}_2$.

Calculul cerut se face calculând restul împărţirii polinomului $(X^2 + 1) \cdot (X^2 + X + 1)$ prin $X^3 + X + 1$. Rezultatul este clasa de echivalenţă modulo $X^3 + X + 1$ a restului găsit.

5. Determinaţi forma elementelor din inelul factor $\mathbb{Z}_3[X]/_{(X^2+X+2)}$. Calculaţi $\widehat{X+2} \cdot \widehat{X+1}$. Este acest inel corp? Justificaţi!

6. Să se arate că inelul factor $\mathbb{R}[X]/(X^2 + 1)$ este izomorf cu $(\mathbf{C}, +, \cdot)$.

Indicaţie: Aplicăm teorema fundamentală de izomorfism pentru inele morfismului

$$\gamma : \mathbb{R}[X] \to \mathbf{C}, \quad \gamma(a) = a, \quad (\forall)a \in \mathbb{R}, \quad \gamma(X) = i.$$

7. Se dă polinomul $f = X^7 + 2X^6 - X^5 + X^3 + 5 \in \mathbf{C}[X]$, cu rădăcinile $x_1, x_2, ..., x_7 \in \mathbf{C}$. Să se calculeze

$$\frac{1}{1 - x_1} + \frac{1}{1 - x_2} + ... + \frac{1}{1 - x_7}.$$

Indicaţie: Se foloseşte Propoziţia 6.4.3.

8. Să se arate că dacă polinomul $f \in \mathbb{Z}[X]$ are trei rădăcini întregi care dau resturi diferite la împărţirea prin 3, atunci pentru orice $n \in \mathbb{Z}$, 3 divide $f(n)$.

Indicaţie: Fie $3a$, $3b + 1$, $3c + 2$ rădăcinile din enunţ. Avem $f = (X - 3a)(X - 3b - 1)(X - 3c - 2) \cdot g$, $g \in \mathbb{Z}[X]$. Pentru un întreg arbitrar n, $f(n)$ este multiplu de 3, orice formă ar avea n: $3k$, $3k + 1$ sau $3k + 2$.

9. Să se determine rădăcinile polinomului $f = aX^3 + bX^2 + cX + d \in \mathbb{R}$, $a \neq 0$.

Indicaţie: Deoarece $a \neq 0$, consideră ecuaţia echivalentă

$$x^3 + px^2 + qx + r = 0, \quad p = b \cdot a^{-1}, \quad q = c \cdot a^{-1}, \quad r = d \cdot a^{-1}.$$

Fie schimbarea de necunoscută $x = y - \frac{p}{3}$. Ecuaţia devine

$$y^3 + \alpha y + \beta = 0, \quad \alpha = -\frac{p^2}{3} + q, \quad \beta = \frac{2p^3 - 9pq}{27} + r.$$

Pentru această ecuaţie căutăm soluţie de forma $y = u+v$, astfel încât $u^3+v^3 = -\beta$, $3uv = -\alpha$. Avem şi $u^3 - v^3 = \pm\sqrt{\beta^2 + 4\frac{\alpha^3}{27}}$, deci

$$u^3 = -\frac{\beta}{2} \pm \sqrt{\left(\frac{\beta}{2}\right)^2 + \left(\frac{\alpha}{3}\right)^3}, \quad v^3 = -\frac{\beta}{2} \mp \sqrt{\left(\frac{\beta}{2}\right)^2 + \left(\frac{\alpha}{3}\right)^3}.$$

$y = u_i+v_j$, unde u_i, v_j, $i, j = 1, 2, 3$ sunt rădăcinile ecuaţiilor binome de mai sus, cu proprietatea că $u_iv_j = -\frac{\alpha}{3}$.

10. Să se rezolve în $\mathbf{C}$ ecuaţiile:
a) $x^3 - 15x - 126 = 0$.
b) $x^3 + 6x^2 + 9x + 5 = 0$.

Indicaţie: Se aplică algoritmul de la exerciţiul anterior.

a) Ecuaţia este în forma redusă, deci căutăm $x = u + v$, $u^3 + v^3 = 126$, $uv = 5$. Obţinem $u^3 = 125$, $v^3 = 1$, deci $x = 5\epsilon_i + \epsilon_j$, unde ϵ_i sunt rădăcinile de ordin 3 ale unităţii, iar perechea (i, j) e aleasă astfel încât $\epsilon_i\epsilon_j = 1$. Găsim

$$x_1 = 6, \quad x_2 = -3 + 2\sqrt{3}i, \quad x_3 = -3 - 2\sqrt{3}i.$$

b) Cu transformarea $x = y - 2$ ecuaţia devine $y^3 - 3y + 3 = 0$, etc.

Capitolul 7

Polinoame în mai multe nedeterminate

7.1 Polinoame în mai multe nedeterminate

În capitolul anterior, pentru inelul unitar comutativ A, s-a dat construcţia inelului de polinoame $A[X]$ într-o nedeterminată, cu coeficienţi în A.

Deoarece $A[X]$ este tot un inel unitar comutativ, are sens inelul de polinoame cu coeficienţi în $A[X]$, $A[X][Y]$. Acest inel îl vom nota $A[X,Y]$ şi îl numim *inelul polinoamelor în nedeterminatele X, Y, cu coeficienţi în A*. Un element $f \in A[X,Y]$ este de forma

$$f = f_0 + f_1 Y + f_2 Y^2 + ... + f_n Y^n, \quad f_i \in A[X], \quad i = \overline{0,n}, \quad n \in \mathbb{N}.$$

Fiecare coeficient este un polinom de forma

$$f_i = a_{0i} + a_{1i}X + a_{2i}X^2 + ... + a_{n_i i}X^{n_i} = \sum_{k=0}^{n_i} a_{ki}X^k.$$

Obţinem forma elementelor din $A[X,Y]$:

$$f = \sum_{i,k} a_{ki}X^k Y^i.$$

Elementele $a_{ki} \in A$ se numesc *coeficienţii* polinomului f.

Inductiv, definim polinoame într-un număr finit de nederminate $X_1, ..., X_n$, astfel:

$$A[X_1, X_2, ..., X_n] = A[X_1, ..., X_{n-1}][X_n].$$

Se arată că forma elementelor inelului $A[X_1, X_2, ..., X_n]$ este

$$f = \sum a_{i_1 i_2 ... i_n} X_1^{i_1} X_2^{i_2} ... X_n^{i_n}.$$

Elementele $a_{i_1 ... i_n} \in A$ se numesc coeficienţii polinomului f.

Un polinom $a_{i_1 i_2 ... i_n} X_1^{i_1} X_2^{i_2} ... X_n^{i_n}$ se numeşte *monom*. Numărul natural

$$i_1 + i_2 + ... + i_n,$$

se numeşte *gradul monomului*. Orice polinom se scrie ca o sumă de monoame, numite termenii polinomului.

Fie $f \in A[X_1, X_2, ..., X_n]$. Gradul polinomului f este $-\infty$ dacă $f = 0$ sau maximul gradelor monoamelor care îl formează, dacă $f \neq 0$.

Observaţia 7.1.1. *Spre deosebire de cazul polinoamelor într-o nedeterminată, unde era un singur monom de grad maxim, iar coeficientul acestuia era numit coeficient dominant, un polinom în mai multe nedeterminate poate să aibă mai multe monoame de grad maxim.*

Exemplul 7.1.1. *a)* $f = 2 + X + 6Y - XY + 4X^2 - 7XY^3 \in \mathbb{Z}[X, Y]$, $grad(f) = 4$.

b) $f = \widehat{2} + X + \widehat{3}Y + \widehat{4}X^3Y + \widehat{2}XY^3 \in \mathbb{Z}_5[X, Y]$, $grad(f) = 4$, *două monoame având acest grad.*

c)$f = X + 6Y - 3Z - XY + 2XZ + 4X^2Z - 7XY^3Z^2 \in \mathbb{Z}[X, Y, Z]$, $grad(f) = 6$.

Toate proprietăţile referitoare la inele de polinoame prezentate în capitolul anterior rămân valabile pentru inelul $A[X_1, X_2, ..., X_n]$, privit ca $A[X_1, X_2, ..., X_{n-1}][X_n]$.

Observaţia 7.1.2. *Inelul* $A[X_1, X_2, ..., X_n]$ *poate fi considerat, în funcţie de necesităţi, ca* $A[X_1, X_2, ..., X_{i-1}, X_{i+1}, ..., X_n][X_i]$.

Exemplul 7.1.2. *Fie polinomul*

$$f = 2X^4 + 5X^3Y + 2X^2Y^2 - 10X^2Y - 4X^3 - 4XY^2 + 2X^2 + 2Y^2 + 5XY \in \mathbb{Z}[X, Y].$$

Dacă îl scriem

$$f = 2X^4 + (5Y-4)X^3 + 2(Y^2-5Y+1)X^2 + (-4Y^2+5Y)X + 2Y^2 \in \mathbb{Z}[Y][X],$$

putem aplica schema lui Horner pentru a găsi o descompunere a lui f. Căutăm un divizor de forma $X-g$, unde $g \in \mathbb{Z}[Y]$ e un divizor al termenului liber, $2Y^2$. Polinomul g poate fi ± 1, $\pm Y$, ± 2, $\pm 2Y$, $\pm Y^2$, $\pm 2Y^2$.

	2	$5Y-4$	$2Y^2-10Y+2$	$-4Y^2+5Y$	$2Y$
1	2	$5Y-2$	$2Y^2-5Y$	$-2Y^2$	0

Restul fiind nul, avem $f = (X-1)[2X^3 + (5Y-2)X^2 + (2Y^2-5Y)X - 2Y^2]$, iar pentru câtul obţinut mai sus facem din nou schema lui Horner:

	2	$5Y-2$	$2Y^2-5Y$	$-2Y^2$
$-2Y$	2	$Y-2$	$-Y$	0

deci $f = (X-1)(X+2Y)(2X^2 + (Y-2)X - Y)$, care se mai poate descompune în $f = (X-1)^2(X+2Y)(2X+Y)$.

Desigur, polinomul poate fi văzut şi

$$f = 2(X^2-2X+1)Y^2 + 5X(X^2-2X+1)Y + 2X^4 - 4X^3 + 2X^2 \in \mathbb{Z}[X][Y],$$

de unde descompunerea se vede imediat.

Definiţia 7.1.1. *Un polinom în care toate monoamele au acelaşi grad se numeşte polinom* ***omogen****.*

Exemplul 7.1.3. *În $\mathbb{Z}[X,Y]$, $f = XY + 3X^2$, $g = -X^3 + 2X^2Y + XY^2$ sunt polinoame omogene, iar $h = X + Y - XY$ este polinom neomogen.*

Propoziţia 7.1.1. *Orice polinom $f \in A[X_1, X_2, ..., X_n]$ se scrie ca sumă de polinoame omogene.*

Demonstraţie: Fie n gradul polinomului f. Fie f_i suma tuturor monoamelor de grad i din f, $i = \overline{0,n}$. Polinomul f_i este omogen şi

$$f = f_n + f_{n-1} + ... + f_1 + f_0.$$

□

Exemplul 7.1.4. *Polinomul*

$$f = 2X^4+5X^3Y+2X^2Y^2-10X^2Y-4X^3-4XY^2+2X^2+2Y^2+5XY \in \mathbb{Z}[X,Y]$$

se scrie

$$f = f_4 + f_3 + f_2,$$

unde

$$f_4 = 2X^4 + 5X^3Y + 2X^2Y^2,$$

$$f_3 = -10X^2Y - 4X^3 - 4XY^2, \quad f_2 = 2X^2 + 2Y^2 + 5XY.$$

7.2 Polinoame simetrice

Fie $n \in \mathbb{N}^*$, $(S_n, \circ)$ grupul permutărilor de n obiecte şi $\sigma \in S_n$. Se verifică imediat că funcţia

$$\varphi_\sigma : A[X_1, X_2, ...X_n] \to A[X_1, X_2, ..., X_n],$$

$$\varphi_\sigma(f)(X_1, X_2, ..., X_n) = f(X_{\sigma(1)}, X_{\sigma(2)}, ..., X_{\sigma(n)}),$$

este morfism unitar de inele.

Observaţia 7.2.1. *φ_σ permută nedeterminatele polinomului f.*

De exemplu, pentru $f = 3X_1X_2 + 2X_3$ şi $\sigma = (3,1,2) \in S_3$,

$$\varphi_\sigma(f) = 3X_2X_3 + 2X_1.$$

Pentru $\tau = (23) \in S_3$, $\varphi_\tau(f) = 3X_1X_3 + 2X_2$.

Definiţia 7.2.1. *Un polinom $f \in A[X_1, ..., X_n]$ se numeşte* ***simetric*** *dacă*

$$\varphi_\sigma(f) = f, \quad (\forall)\sigma \in S_n.$$

Exemplul 7.2.1. *În $\mathbb{Z}[X_1, X_2, X_3]$,*

$$f = X_1X_2X_3, \quad g = X_1 + X_2 + X_3 + X_1X_2 + X_1X_3 + X_2X_3,$$

sunt polinoame simetrice, dar $h = X_1X_2$ nu este simetric.

Să observăm că dacă $f \in A[X_1, ..., X_n]$ este polinom simetric şi $aX_1^{i_1}...X_n^{i_n}$ este un monom al său, atunci şi $aX_{\sigma(1)}^{i_1}...X_{\sigma(n)}^{i_n}$ este monom al lui f, pentru orice permutare $\sigma \in S_n$.

Propoziţia 7.2.1. *Mulţimea S a polinoamelor simetrice în n nedeterminate cu coeficienţi în inelul unitar comutativ A este inel, subinel al inelului $A[X_1, ..., X_n]$.*

Demonstraţie: Verificăm condiţiile din Propoziţia 5.2.1 a), care caracterizează noţiunea de subinel.

Fie $f, g \in S$, deci $\varphi_\sigma(f) = f$, $\varphi_\sigma(g) = g$, $(\forall)\sigma \in S_n$. Din proprietatea de morfism a lui φ_σ, avem

$$\varphi_\sigma(f - g) = \varphi_\sigma(f) - \varphi_\sigma(g) = f + g,$$

$$\varphi_\sigma(f \cdot g) = \varphi_\sigma(f) \cdot \varphi_\sigma(g) = f \cdot g,$$

deci $f - g \in S$, $f \cdot g \in S$. □

Propoziţia 7.2.2. *Polinoamele $s_1, s_2, ..., s_n \in A[X_1, ..., X_n]$, definite prin*

$$s_1 = X_1 + X_2 + ... + X_n = \sum_{i=1}^{n} X_i,$$

$$s_2 = X_1X_2 + ... + X_1X_n + X_2X_3 + ... + X_{n-1}X_n = \sum_{0 \le i < j \le n} X_iX_j,$$

.....

$$s_n = X_1X_2...X_n,$$

sunt polinoame simetrice omogene, numite ***polinoamele simetrice fundamentale*** *în nedeterminatele $X_1, ..., X_n$. Prin convenţie notăm $s_0 = 1$, $s_m = 0$, $(\forall)m > n$.*

Demonstraţie: Evident fiecare s_k este omogen de grad k. Pentru a demonstra că sunt simetrice, arătăm mai întâi că în inelul $A[X_1, ...X_n][X]$ are loc relaţia

$$(X - X_1)(X - X_2)...(X - X_n) = X^n - s_1X^{n-1} + s_2X^{n-2} - ... + (-1)^n s_n.$$

Demonstrăm prin inducţie după n.

Pas 1. Pentru $n = 1$, $s_1(X_1) = X_1$ şi $X - X_1 = X - s_1$, e de forma din enunţ.

Pas 2. Presupunem că pentru s'_k, $k = \overline{1, n-1}$, polinoamele simetrice fundamentale în $n-1$ nedeterminate $\{X_1, ..., X_{n-1}\}$, avem

$$(X - X_1)(X - X_2)...(X - X_{n-1}) = X^{n-1} - s'_1 X^{n-2} + s'_2 X^{n-3} - ... + (-1)^{n-1} s'_{n-1}.$$

Calculăm în $A[X_1, ...X_n][X]$

$$(X - X_1)(X - X_2)...(X - X_n) =$$

$$= (X^{n-1} - s'_1 X^{n-2} + s'_2 X^{n-3} - ... + (-1)^k s'_k X^{n-k-1} + ... + (-1)^{n-1} s'_{n-1})(X - X_n) =$$

$$= X^n - (s'_1 + X_n)X^{n-1} + ... + (-1)^k (s'_k + s'_{k-1} X_n) X^{n-k} + ... + (-1)^n s'_{n-1} X_n =$$

$$= X^n - s_1 X^{n-1} + s_2 X^{n-2} - ... + (-1)^n s_n,$$

deoarece $s_k = s'_k + X_n s'_{k-1}$.

Pentru orice permutare $\sigma \in S_n$, morfismul φ_σ induce, conform Propoziţiei 6.1.6, un morfism

$$\varphi^*_\sigma : A[X_1, ..., X_n][X] \to A[X_1, ..., X_n][X],$$

la care polinomul g este invariant, deoarece oricum am permuta nedeterminatele, rămâne tot g. Avem deci

$$g = \varphi^*_\sigma(g) = X^n - \varphi_\sigma(s_1)X^{n-1} + \varphi_\sigma(s_2)X^{n-2} - ... + (-1)^n \varphi_\sigma(s_n),$$

de unde $\varphi_\sigma(s_k) = s_k$, $(\forall)k = \overline{1, n}$. □

Exemplul 7.2.2. *Polinoamele simetrice fundamentale în trei nedeterminate sunt:*

$$\begin{array}{c} s_0 = 1, \\ s_1 = X_1 + X_2 + X_3, \\ s_2 = X_1X_2 + X_1X_3 + X_2X_3, \\ s_3 = X_1X_2X_3. \end{array}.$$

Observaţia 7.2.2. *a) Polinomul fundamental s_k în n nedeterminate este suma tuturor produselor de k nedeterminate distincte alese din $\{X_1, ..., X_n\}$. Deci s_k este o sumă de C_n^k termeni.*

b) Atunci când se pot creea confuzii, polinomul fundamental s_k în n nedeterminate se notează $s_k(X_1, ..., X_n)$.

Propoziţia 7.2.3. *Orice polinom simetric se scrie în mod unic ca sumă de polinoame simetrice şi omogene.*

Demonstraţie: Fie $f \in A[X_1, X_2, ..., X_n]$ un polinom simetric de grad m. Atunci, conform Propoziţiei 7.1.1,

$$f = f_0 + f_1 + ... + f_m,$$

unde f_k este suma tuturor monoamelor de grad k din f. Evident, f_k este polinom omogen. Mai mult, scrierea lui f ca sumă de aceste polinoame omogene este unică. Din faptul că f este simetric, rezultă că $\varphi_\sigma(f) = f$, pentru orice $\sigma \in S_n$. Avem deci

$$f = \varphi_\sigma(f_0) + \varphi_\sigma(f_1) + ... + \varphi_\sigma(f_m),$$

iar morfismul φ_σ invariază gradele polinoameleor. Rezultă că avem mai sus f scris din nou ca sumă de polinoame omogene. Scrierea fiind unică, rezultă $\varphi_\sigma(f_k) = f_k$, adică f_k simetric, $(\forall)k = \overline{0, m}$. □

7.3 Teorema fundamentală a polinoamelor simetrice

În această secţiune introducem pe mulţimea polinoamelor de mai multe nedeterminate un mod de ordonare a termenilor unui polinom care, in particular, în cazul polinoamelor de o nedeterminată, revine la ordonarea după puterile nedeterminatei. Această ordonare se numeşte *lexicografică* şi este sugerată de ordonarea cuvintelor într-un dicţionar.

Considerăm nedeterminatele ordonate astfel:

$$X_1 > X_2 > ... > X_n.$$

Două monoame $\lambda = X_1^{i_1} X_2^{i_2} ... X_n^{i_n}$, $\mu = X_1^{j_1} X_2^{j_2} ... X_n^{j_n}$ sunt în relaţia

$$\lambda \leq \mu \Rightarrow (\exists) 1 \leq r \leq n, \quad i_1 = j_1, ..., i_r = j_r, i_{r+1} < j_{r+1}.$$

Exemplul 7.3.1. *În $A[X_1, X_2, X_3, X_4]$, au loc relaţiile:*

$$X_1^2 X_3 < X_1^2 X_2, \quad X_3^6 X_4^7 < X_2 X_3^4 X_4^3, \quad X_2 X_3 X_4 < X_1 X_4.$$

Relaţia de ordine introdusă mai sus pe mulţimea monoamelor simple (fără coeficienţi) este totală şi compatibilă cu înmulţirea, adică pentru orice trei monoame λ, μ, ν, din $\lambda \leq \mu$ rezultă $\nu \cdot \lambda \leq \nu \cdot \mu$.

Ordinea lexicografiă induce pe mulţimea tuturor monoamelor o relaţie de preordine (reflexivă şi tranzitivă) prin

$$a\lambda \leq b\mu \Leftrightarrow \lambda \leq \mu, \quad (\forall)a, b \in A.$$

Relaţia nu e simetrică deoarece $a\lambda \leq b\lambda$ şi $b\lambda \leq a\lambda$ pentru $a \neq b$.

Orice polinom nenul din $A[X_1, ...X_n]$ se scrie în mod unic ca sumă de monoame distincte, termenii polinomului. Cel mai mare termen în raport cu ordinea lexicografică se numeşte *termenul principal* sau *monomul dominant* al polinomului.

Exemplul 7.3.2. *Termenul principal al polinomului*

$$f = 2X^4+5X^3Y+2X^2Y^2-10X^2Y-4X^3-4XY^2+2X^2+2Y^2+5XY \in \mathbb{Z}[X, Y],$$

este $2X^4$*, iar termenul principal al polinomului*

$$g = X^3Y - 3X^2Y^2 + X^2Y - 4X^3 + 6XY^2 + X^2 + 5Y^2 + 2XY \in \mathbb{Z}[X, Y],$$

este X^3Y*.*

Propoziţia 7.3.1. *Dacă* $f, g \in A[X_1, .., X_n]$ *au termenii principali* $a\lambda$*, respectiv* $b\mu$ *şi* $ab \neq 0$*, atunci termenul principal al polinomului* $f \cdot g$ *este* $ab\lambda\mu$*.*

Demonstraţie: Termenii polinomului $f \cdot g$ sunt produse de termeni $c\nu$, $d\varsigma$, $c, d \in A$, $\nu \leq \lambda$, $\varsigma \leq \mu$. Avem

$$\nu\varsigma \leq \lambda\varsigma \leq \lambda\mu \Rightarrow cd\nu\varsigma \leq ab\lambda\mu,$$

deci $ab\lambda\mu$ este cel mai mare termen în raport cu ordinea lexicografică. □

Propoziţia 7.3.2. *Dacă* f *este un polinom simetric din* $A[X_1, ..., Xn]$ *şi* $aX_1^{i_1}X_2^{i_2}...X_n^{i_n}$ *este termenul său principal, atunci*

$$i_1 \geq i_2 \geq ... \geq i_n.$$

Demonstraţie: Polinomul fiind simetric, are ca termeni toate monoamele obţinute din cel dominant prin permutarea nedeterminatelor. Dacă presupunem $i_k < i_{k+1}$, atunci termenul $aX_1^{i_1}X_2^{i_2}...X_k^{i_{k+1}}X_{k+1}^{i_k}...X_n^{i_n}$ este mai mare decât termenul principal, contradicţie. □

Teorema 7.3.1. *[Teorema fundamentală a polinoamelor simetrice] Fie A un inel unitar comutativ. Orice polinom simetric $f \in A[X_1, X_2, ..., X_n]$ se poate exprima în mod unic ca un polinom de polinoame simetrice fundamentale, adică există $g \in A[X_1, X_2, ..., X_n]$ astfel încât*

$$f = g(s_1, s_2, ..., s_n).$$

Demonstraţie: Fie $f \in A[X_1, ..., X_n]$ un polinom simetric. Conform Propoziţiei 7.2.3, f se scrie ca sumă de polinoame simetrice omogene. Putem presupune, fără a restrânge generalitatea, că f este polinom omogen.

Fie $aX_1^{i_1}X_2^{i_2}...X_n^{i_n}$ termenul său principal. Căutăm un polinom h în n nedeterminate a cărui expresie $h(s_1, ..., s_n)$ să aibă acelaşi termen principal cu f.

Deoarece termenul principal al polinomului simetric s_k este $X_1X_2...X_k$, termenul principal al polinomului $s_1^{i_1-i_2}s_2^{i_2-i_3}...s_n^{i_{n-1}-i_n}$ este $X_1^{i_1}X_2^{i_2}...X_n^{i_n}$. Polinomul

$$f_1 = f - as_1^{i_1-i_2}s_2^{i_2-i_3}...s_n^{i_{n-1}-i_n},$$

are termenul principal mai mic decât al lui f. Continuând procedeul, după un număr finit de paşi se găseşte expresia lui f în funcţie de polinoamele fundamentale.

Finitudinea algoritmului se datorează faptului că pentru un monom $X_1^{i_1}X_2^{i_2}...X_n^{i_n}$ cu $i_1 \geq i_2 \geq ... \geq i_n$, există un număr finit de monoame

$$X_1^{j_1}X_2^{j_2}...X_n^{j_n} \leq X_1^{i_1}X_2^{i_2}...X_n^{i_n},$$

cu $j_1 \geq j_2 \geq ... \geq j_n$. Într-adevăr, $i_1 \geq j_1$, deci există un număr finit de variante pentru j_1, iar pentru fiecare j_1 ales, $(j_2, ..., j_n)$ poate fi ales în j_1^{n-1} moduri.

Demonstrăm în continuare unicitatea scrierii.

Vom arăta că dacă $h \in A[X_1, X_2, ..., X_n]$ astfel încât $h(s_1, ..., s_n) = 0$, atunci $h = 0$.

Fie h un polinom cu $h(s_1, ..., s_n) = 0$ şi presupunem prin absurd că este nenul, deci există un coeficient nenul, fie acesta al monomului $aX_1^{i_1}X_2^{i_2}...X_n^{i_n}$.

Corespunzător acestui monom, $as_1^{i_1}s_2^{i_2}...s_n^{i_n}$ este termen nenul în $h(s_1,...,s_n)=0$. Rezultă că acest termen se reduce cu un alt termen. Termenul principal din $as_1^{i_1}s_2^{i_2}...s_n^{i_n}$ este $aX_1^{k_1}X_2^{k_2}...X_n^{k_n}$, unde

$$\begin{gathered} k_1 = i_1 + i_2 + ... + i_n, \\ k_2 = i_2 + ... + i_n, \\ ..... \\ k_n = i_n. \end{gathered}$$

Un termen din $h(s_1,...,s_n)=0$ care să reducă $as_1^{i_1}s_2^{i_2}...s_n^{i_n}$ trebuie să aibă acelaşi termen principal. Dar un $s_1^{j_1}s_2^{j_2}...s_n^{j_n}$ cu cel puţin un i_l diferit de j_l are un alt termen principal, deci nu se pot reduce. Rezultă $h=0$. Prin urmare, pentru $h_1, h_2 \in A[X_1,...,X_n]$, cu $f = h_1(s_1,..,s_n) = h_2(s_1,...,s_n)$ avem $h_1 = h_2$. □

Exemplul 7.3.3. *Polinomul simetric*

$$f = X_1^2X_2 + X_1^2X_3 + X_2^2X_1 + X_2^2X_3 + X_3^2X_1 + X_3^2X_2,$$

din $\mathbb{Z}[X_1,X_2,X_3]$ *are termenul principal* $X_1^2X_2$. *Acesta este termenul principal şi al polinomului* s_1s_2.

Calculăm $f - s_1s_2 = 3s_3$, *de unde obţinem* $f = s_1s_2 + 3s_3$. *Există deci polinomul* $g = X_1X_2 + 3X_3 \in \mathbb{Z}[X_1,X_2,X_3]$ *şi* $f = g(s_1,s_2,s_3)$.

Ca aplicaţie a Teoremei fundamentale a polinoamelor simetrice prezentăm *Sumele lui Newton*.

Fie polinomul simetric

$$t_m = X_1^m + X_2^m + ... + X_n^m \in A[X_1,X_2,...,X_n],$$

pentru orice $m \geq 1$. Conform Teoremei 7.3.1, există un polinom

$$h_m \in A[X_1,X_2,...,X_n],$$

astfel încât $t_m = h_m(s_1,...,s_n)$.

Propoziţia 7.3.3. *Are loc următoarea relaţie de recurenţă:*

$$t_m = s_1t_{m-1} - s_2t_{m-2} + ... + (-1)^{m-2}s_{m-1}t_1 + (-1)^{m-1}s_m \cdot m,$$

unde $s_0, s_1, ..., s_m$ *sunt polinoamele simetrice fundamentale din* $A[X_1,X_2,...,X_n]$, *cu* $s_m = 0$, $(\forall)m > n$.

Demonstraţie: Fie $g = (X - X_1)(X - X_2)...(X - X_n) \in A[X_1, ..., X_n][X]$ polinomul considerat şi în demonstraţia Propoziţiei 7.2.2. După cum s-a justificat deja, avem

$$g = X^n - s_1X^{n-1} + s_2X^{n-2} - ... + (-1)^n s_n.$$

Din faptul că $X_1, ..., X_n$ sunt rădăcini ale polinomului g, putem scrie:

$$\begin{gathered} X_1^n - s_1X_1^{n-1} + s_2X_1^{n-2} - ... + (-1)^n s_n = 0 \\ X_2^n - s_1X_2^{n-1} + s_2X_2^{n-2} - ... + (-1)^n s_n = 0 \\ ..... \\ X_n^n - s_1X_n^{n-1} + s_2X_n^{n-2} - ... + (-1)^n s_n = 0. \end{gathered}$$

Pentru orice $m \geq n$, prin înmulţirea fiecărei identităţi de mai sus cu X_1^{m-n}, X_2^{m-n}, respectiv X_n^{m-n} şi prin însumarea relaţiilor obţinute, rezultă

$$t_m - s_1t_{m-1} + s_2t_{m-2} - ... + (-1)^n s_nt_{m-n} = 0,$$

care se poate completa la formula din enunţ folosind $s_k = 0$, $(\forall)k > n$.

A rămas să demonstrăm formula pentru $m < n$.

Avem $t_1 = s_1$,

$$t_2 = X_1^2 + ... + X_n^2 = (X_1 + ... + X_n)^2 - 2\sum_{1 \leq i < j \leq n} X_iX_j = s_1t_1 - 2s_2.$$

Pentru un $r < n$ şi $a_1 \geq ... \geq a_r$ un r-uplet ordonat de numere naturale, notăm cu $s(a_1, ..., a_r)$ unicul polinom simetric din $A[X_1, ..., X_n]$ cu termenul principal $X_1^{a_1}X_2^{a_2}...X_r^{a_r}$.

$$\begin{gathered} s(m) = X_1^m + ... + X_n^m = t_m \\ s(1) = X_1 + ... + X_n = s_1 \\ s(1,1) = X_1X_2 + X_1X_3 + ... + X_{n-1}X_n = s_2 \\ s(1,1,1) = X_1X_2X_3 + X_1X_2X_4 + ... + X_{n-2}X_{n-1}X_n = s_3 \\ ..... \\ s(\underbrace{1,1,1,...,1}_{k}) = X_1X_2...X_k + ... = s_k \\ ..... \\ s(a,1) = X_1^aX_2 + X_1^aX_3 + ... + X_{n-1}^aX_n = \textstyle\sum_{i \neq j} X_i^aX_j \\ s(a,\underbrace{1,1,...,1}_{k}) = \textstyle\sum_{i_1,i_2,...,i_k} X_{i_1}^aX_{i_2}...X_{i_k}, \end{gathered}$$

unde în ultima sumă $i_1, ..., i_k$ sunt distincte două câte două.

Calculăm

$$\begin{gathered} s_1 t_{m-1} = t_m + s(m-1,1) \\ s_2 t_{m-2} = s(m-1,1) + s(m-2,1,1) \\ s_3 t_{m-3} = s(m-2,1,1) + s(m-3,1,1,1) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_{m-1} t_1 = s(2, \underbrace{1,1,...,1}_{m-1}) + m s_m, \end{gathered}$$

care prin amplificare cu $(-1)^k$ corespunzător şi apoi însumare, conduc la formula din enunţ. □

Exemplul 7.3.4. *Pentru $x_1, ..., x_5$ rădăcinile polinomului*

$$f = X^5 - X^4 + 2X^3 - 2X^2 + X - 6,$$

putem folosi sumele lui Newton pentru calculul expresiilor $t_m = x_1^m + ... + x_5^m$, deoarece polinoamele simetrice fundamentale sunt exact expresiile care intervin în relaţiile lui Viete. Avem $s_1 = 1$, $s_2 = 2$, $s_3 = 2$, $s_4 = 1$, $s_5 = 6$, $t_1 = s_1 = 1$, $t_2 = s_1 t_1 - 2s_2 = -3$, $t_3 = s_1 t_2 - s_2 t_1 + 3s_3 = -2$, etc.

7.4 Exerciţii

1. Găsiţi descompuneri pentru următoarele polinoame:
   a) $X^4Y + 8XY^4 + X + 2Y \in \mathbb{Q}[X, Y]$;
   b) $X^3 + Y^3 + Z^3 - 3XYZ \in \mathbb{Q}[X, Y, Z]$;
   c) $X^4 + Y^4 \in \mathbb{Z}_2[X, Y]$.

   Indicaţie: a), b) Folosim schema lui Horner, ca în Exemplul 7.1.2.
   c) În $\mathbb{Z}_2[X, Y]$, $2X^2Y^2 = 0$, deci $X^4 + Y^4 = (X^2 + Y^2)^2$, etc.

2. Să se determine forma elementelor din inelul factor $\mathbb{Q}[X, Y]/(X, Y)$, unde (X, Y) este idealul generat de polinoamele X şi Y.

   Demonstraţi că inelul $\mathbb{Q}[X, Y]/(X, Y)$ este un corp izomorf cu corpul numerelor raţionale.

   Indicaţie: Idealul (X, Y) conţine toate polinoamele din $\mathbb{Q}[X, Y]$ care se scriu de forma $gX + hY$, cu $g, h \in \mathbb{Q}[X, Y]$. Cu alte cuvinte, conţine toate polinoamele $f \in \mathbb{Q}[X, Y]$ cu

$f(0,0)=0$, deci cu termen liber nul. Inelul factor este format din clasele de echivalentă modulo idealul (X,Y), ale polinoamelor din $\mathbb{Q}[X,Y]$. Pentru f oarecare $f-f(0,0)\in(X,Y)$, deci

$$\mathbb{Q}[X,Y]/(X,Y)=\{\hat{a}|\quad a\in\mathbb{Q}\},$$

adică clasele de echivalenţă cu reprezentanţi polinoame constante din $\mathbb{Q}[X,Y]$.

Aplicând teorema fundamentală de izomorfism pentru inele morfismului surjectiv $\varphi:\mathbb{Q}[X,Y]\to\mathbb{Q}$, $\varphi(\hat{a})=a$, obţinem izomorfismul cerut, deci inelul factor este corp.

3. Să se aplice Teorema fundamentală a polinoamelor simetrice pentru următoarele polinoame din $\mathbb{R}[X_1,X_2,X_3]$:

a) $f=(X_1-X_2)^2(X_1-X_3)^2(X_2-X_3)^2$;

b) $f=(X_1+X_2)(X_1+X_3)(X_2+X_3)$;

c) $f=(X_1^2+X_2^2)(X_1^2+X_3^2)(X_2^2+X_3^2)$.

Indicaţie: Se obţin expresiile: a) $f=s_1^2s_2^2-4s_1^3s_3-4s_2^3+18s_1s_2s_3-27s_3^2$, b) $f=s_1s_2-s_3$, c) $f=s_1^2s_2^2-2s_1^3s_3-2s_2^3+4s_1s_2s_3-s_3^2$.

4. Fie $p>2$ un număr prim şi $f\in\mathbb{Z}[X]$ un polinom de grad $p-1$ cu proprietatea că pentru orice $a,b\in\mathbb{Z}$, dacă $p|(f(a)-f(b))$, atunci $p|(a-b)$. Să se arate că p divide coeficientul dominant al lui f.

Indicaţie: Fie $f=a_{p-1}X^{p-1}+a_{p-2}X^{p-2}+...+a_1X+a_0$ şi $\varphi:\mathbb{Z}\to\mathbb{Z}_p$ surjecţia canonică, $f_*\varphi^*(f)\in\mathbb{Z}_p[X]$ imaginea polinomului f prin morfismul corespunzător (vezi Propoziţia 7.1.6). Funcţia polinomială $\tilde{f}_*:\mathbb{Z}_p\to\mathbb{Z}_p$ este injectivă deoarece $\tilde{f}_*(\hat{a})=\tilde{f}_*(\hat{b})$ este echivalent cu $p|(f(a)-f(b))$, deci $p|(a-b)$ din ipoteză. Dar $\mathbb{Z}_p$ finită, deci $\tilde{f}_*$ este o funcţie bijectivă. Rezultă că $\{\tilde{f}_*(\hat{0}),...,\tilde{f}_*(p\hat{-}1)\}=\mathbb{Z}_p$, deci $\tilde{f}_*(\hat{0})+...+\tilde{f}_*(p\hat{-}1)=\hat{0}$. Dar

$$\tilde{f}_*(\hat{0})+...+\tilde{f}_*(p\hat{-}1)=\hat{a}_{p-1}\sum_{k=1}^{p-1}\hat{k}^{p-1}+\hat{a}_{p-2}\sum_{k=1}^{p-1}\hat{k}^{p-2}+...+\hat{a}_1\sum_{k=1}^{p-1}\hat{k}+p\hat{a}_0,$$

care duce la $\hat{a}_{p-1}(p-1)=\hat{0}$, deci $p|a_{p-1}$. Am folosit faptul că elementele lui $\mathbb{Z}_p^*$ sunt rădăcinile polinomului $X^{p-1}-1$, iar din relaţiile lui Viete şi formula de recurenţă pentru sumele lui Newton $t_m=\sum_{k=1}^{p-1}\hat{k}^m$ rezultă $t_m=\hat{0}$.

5. Fie polinomul $f=X^n+2X^{n-1}+3X^{n-2}+...+(n-1)X^2+nX+(n+1)$, cu rădăcinile $x_1,...,x_n$. Să se arate că

$$x_1^k+x_2^k+...+x_n^k=-2,\quad(\forall)k=\overline{1,n}.$$

Indicaţie: Se folosesc sumele lui Newton.

Capitolul 8

Spaţii vectoriale. Subspaţii. Bază şi dimensiune.

8.1 Spaţii vectoriale

Fie $(K, +, \cdot)$ un corp comutativ (de exemplu $\mathbb{Z}_p$, $\mathbb{R}$) şi $(V, +)$ un grup abelian. Fie legea de compoziţie externă

$$\cdot_K : K \times V \to V,$$

numită *amplificare cu scalari.*

Definiţia 8.1.1. *Tripletul $(V, +, \cdot_K)$ se numeşte **spaţiu vectorial peste** K, sau K-spaţiu vectorial (K-s.v.), dacă sunt satisfăcute axiomele:*

a) $\alpha \cdot_K (\beta \cdot_K x) = (\alpha \cdot \beta) \cdot_K x$, $(\forall)\alpha, \beta \in K$ *şi* $x \in V$.

b) $(\alpha + \beta) \cdot_K x = \alpha \cdot_K x + \beta \cdot_K x$, *pentru orice scalari* $\alpha, \beta \in K$ *şi* $x \in V$.

c) $\alpha \cdot_K (x + y) = \alpha \cdot_K x + \alpha \cdot_K y$, $(\forall)\alpha, \beta \in K$, $(\forall)\ x, y \in V$.

d) $1 \cdot_K x = x$, *pentru orice* $x \in V$, *unde* 1 *este elementul unu al corpului* K.

*Elementele lui V se numesc **vectori**, iar K este numit **corpul scalarilor**.*

Observaţia 8.1.1. *De multe ori operaţia de amplificare cu scalari '$\cdot_K$' se notează tot '$\cdot$' sau chiar se omite, cititorul înţelegând despre care operaţie este vorba în funcţie de operanzi.*

Exemplul 8.1.1. *a) Pentru orice corp comutativ K, mulţimea* $K^n = \underbrace{K \times K \times ... \times K}_{n}$

este K-s.v. în raport cu operaţiile

$$+ : K^n \times K^n \to K^n, \quad \cdot : K \times K^n \to K^n,$$

definite în mod natural:

$$(x_1, x_2, ..., x_n) + (y_1, y_2, ..., y_n) = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n),$$

$$\alpha(x_1, x_2, ..., x_n) = (\alpha x_1, \alpha x_2, ..., \alpha x_n),$$

adică adunarea se face pe componente, iar amplificarea se face înmulţinând fiecare componentă cu scalarul.

b) Mulţimea $M_{m,n}(K)$ a matricelor de tip (m, n) este un K-s.v. în raport cu adunarea matricelor şi cu amplificarea unei matrice cu un element din corpul K:

$$\cdot : K \times M_{m,n}(K) \to M_{m,n}(K), \quad \alpha \cdot A = (\alpha \cdot a_{ij})_{i=\overline{1,m}, j=\overline{1,n}},$$

pentru orice $\alpha \in K$, $A = (a_{ij})_{i=\overline{1,m}, j=\overline{1,n}} \in M_{m,n}(K)$.

c) Mulţimea polinoamelor $K[X]$ cu coeficienţi în corpul K este spaţiu vectorial în raport cu adunarea polinoamelor şi cu amplificarea unui polinom cu un element din corpul K, adică produsul unui polinom cu un polinom de grad 0 sau cu polinomul nul.

d) Fie $(K, +, \cdot)$ un corp comutativ şi L un subcorp al său. Restrângem operaţia de înmulţire din K la $\cdot_L : L \times K \to K$Se verifică imediat că tripletul $(K, +, \cdot_L)$ este spaţiu vectorial peste corpul L.

e) Notăm V mulţimea numerelor reale strict pozitive şi definim operaţia $\oplus$ pe V, ca fiind restricţia înmmulţii numerelor reale la $V \times V$. Fie

$$\otimes : \mathbb{R} \times V \to V, \quad \alpha \otimes x = x^\alpha, \quad (\forall)\alpha \in \mathbb{R}, (\forall)x \in V.$$

Evident, $(V, \oplus)$ este grup abelian. Să verificăm axiomele din Definiţia 8.1.1. Fie elementele arbitrare $x, y \in V$, $\alpha, \beta \in \mathbb{R}$.

$$\alpha \otimes (\beta \otimes x) = \alpha \otimes x^\beta = (x^\beta)^\alpha = x^{\alpha\beta} = (\alpha \cdot \beta) \otimes x,$$

deci prima axiomă este adevărată.

$$(\alpha + \beta) \otimes x = x^{\alpha+\beta} = x^\alpha \cdot x^\beta = (\alpha \otimes x) \oplus (\beta \otimes x),$$

ceea ce arată că a doua axiomă este verificată. Tot prin calcul direct se verifică şi ultimele două axiome:

$$\alpha \otimes (x \oplus y) = \alpha \otimes (xy) = (xy)^\alpha = x^\alpha y^\alpha = (\alpha \times x) \oplus (\alpha \otimes y),$$

$$1 \otimes x = x^1 = x.$$

Am demonstrat astfel că tripletul $(V, \oplus, \otimes)$ este un $\mathbb{R} - s.v.$.

Fie $(V, +, \cdot)$ un spaţiu vectorial peste corpul comutativ K şi fie 0_V vectorul nul, adică elementul neutru în grupul $(V, +)$, iar $-x$ opusul vectorului x în acelaşi grup. Notăm cu 0, 1, elementele zero, respectiv unu din corpul K.

Propoziţia 8.1.1. *Au loc următoarele relaţii:*
a) $0 \cdot x = 0_V$*, pentru orice* $x \in V$*;*
b) $\alpha \cdot 0_V = 0_V$*, pentru orice* $\alpha \in K$*;*
c) $1 \cdot (-x) = (-1) \cdot x = -x$*,* $(\forall) x \in V$*;*
d) $\alpha \cdot x = 0_V$ *dacă şi numai dacă* $\alpha = 0$ *sau* $x = 0_V$*;*

Demonstraţie: a) Scriem $0 = 0 + 0$ şi folosim axioma b) din Definiţia 8.1.1 în următorul calcul:

$$0 \cdot x = (0 + 0) \cdot x \Leftrightarrow 0 \cdot x = 0 \cdot x + 0 \cdot x.$$

Din ultima relaţie considerată în grupul $(V, +)$, rezultă $0 \cdot x = 0_V$.

b) Rezultatul vine dintr-un calcul analog, scriind $0_V = 0_V + 0_V$ şi folosind axioma c) din definiţia spaţiului vectorial.

c) Opusul elementului $x \in V$ este definit de $x + (-x) = 0_V$. Conform punctului b), are loc $1 \cdot (x + (-x)) = 0_V$. Aplicăm axiomele c) şi d) din definiţia spaţiului vectorial şi obţinem egalitatea $x + 1 \cdot (-x) = 0_V$ în grupul $(V, +)$. Rezultă $1 \cdot (-x) = -x$.

Elementul $-1 \in K$ are proprietatea $1 + (-1) = 0$. Folosim rezultatul demonstrat la punctul a) şi axiomele b) şi d) şi obţinem:

$$(1 + (-1)) \cdot x = 1 \cdot x + (-1) \cdot x \Rightarrow 0_V = x + (-1) \cdot x \Rightarrow (-1) \cdot x = -x.$$

d) Fie $\alpha \in K$ şi $x \in V$ astfel încât $\alpha \cdot x = 0_V$. Dacă $\alpha \neq 0$, atunci este inversabil, deci există $\alpha^{-1} \in K$, $\alpha^{-1}\alpha = 1$. Amplificăm relaţia $\alpha \cdot x = 0_V$ cu α^{-1} şi aplicăm axiomele a) şi d), şi rezultatul de la punctul b):

$$\alpha^{-1} \cdot (\alpha \cdot x) = 0_V \Rightarrow 1 \cdot x = 0_V \Rightarrow x = 0_V.$$

Am obţinut că $\alpha = 0$ sau, dacă nu, $x = 0_V$. □

8.2 Subspaţii vectoriale

Fie $(V, +, \cdot)$ un K-spaţiu vectorial şi o submulţime nevidă V' a sa.

Definiţia 8.2.1. *Dacă restricţiile operaţiilor din V la $V' \times V'$, respectiv $K \times V'$ dau mulţimii V' structură de K-spaţiu vectorial, atunci V' este subspaţiu vectorial al lui V. Notăm în acest caz $V' \leq V$.*

Propoziţia 8.2.1. *$V' \subset V$ este subspaţiu vectorial dacă şi numai dacă*

$$\alpha x + \beta y \in V', \quad (\forall) x, y \in V', \quad \alpha, \beta in K.$$

Demonstraţie: Dacă $V' \leq V$, atunci $(V', +|_{V' \times V'}, \cdot|_{K \times V'})$ este spaţiu vectorial peste K, deci V' este parte stabilă la cele două legi de compoziţie. Atunci, pentru orice scalari α, β şi orice elemente $x, y \in V'$, $\alpha \cdot x + \beta \cdot y \in V'$.

Reciproc, dacă submulţimea V' satisface condiţia din ipoteză, atunci, pentru $\alpha = \beta = 1$ obţinem $x + y \in V'$, iar pentru $\alpha = 1$, $\beta = 0$ obţinem $\alpha \cdot x \in V'$, $(\forall) x, y \in V'$. Deci restricţiile $+|_{V' \times V'}, \cdot|_{K \times V'}$ sunt legi de compoziţie internă, respectiv externă, pe V'. Axiomele referitoare la amplificarea cu scalari din definiţia spaţiului vectorial V rămân valabile în V'.

Pentru $\alpha = \beta = 0$, condiţia din ipoteză conduce la $0_V \in V'$, iar scalarii $\alpha = -1$, $\beta = 0$ conduc la $-x \in V'$, pentru orice $x \in V'$. Am obţinut astfel că V' este subgrup al grupului $(V, +)$. Prin urmare $(V', +)$ este grup abelian. Rezultă că $(V', +, \cdot)$ este un K-spaţiu vectorial. □

Observaţia 8.2.1. *Condiţia din Propoziţia anterioară este echivalentă cu*

$$x + y \in V', \quad \alpha \cdot x \in V', \quad (\forall) x, y \in V', (\forall) \alpha \in K.$$

Dacă $V' \subset V$ este subspaţiu vectorial, atunci în particular este subgrup în $(V, +)$, deci conţine vectorul nul. Prin urmare o submulţime a unui spaţiu vectorial, care nu conţine vectorul nul, nu poate fi subspaţiu vectorial.

Exemplul 8.2.1. *a) $\{0_V\}$, V sunt subspaţii vectoriale ale spaţiului vectorial V.*

b) $\mathbb{Z}_p \times \{0\}$ este subspaţiu vectorial în $\mathbb{Z}_p$-s.v. $\mathbb{Z}_p \times \mathbb{Z}_p$.

c) $V' = \{(x_1, x_2, x_3) \in \mathbb{Z}_2^3, \quad x_1 + x_2 + x_3 = \widehat{0}\}$ este subspaţiu vectorial al $\mathbb{Z}_2$-s.v. $\mathbb{Z}_2^3$. Mai exact, $V' = \{(\widehat{0}, \widehat{0}, \widehat{0}), (\widehat{0}, \widehat{1}, \widehat{1}), (\widehat{1}, \widehat{0}, \widehat{1}), (\widehat{1}, \widehat{1}, \widehat{0})\}$.

d) Mulţimea matricelor simetrice $\{A \in M_n(K) | \cdot A^t = A\}$ este subspaţiu vectorial în K-spaţiul vectorial al matricelor pătratice de ordin n cu elemente în corpul comutativ K.

Definiţia 8.2.2. *Dacă S este o submulţime nevidă a K-spaţiului vectorial $(V, +, \cdot)$, atunci numim **combinaţie liniară finită** de elemente din S un element de forma $\alpha_1 v_1 + \alpha_2 x_2 + ... + \alpha_p v_p \in V$, pentru $\alpha_1, ..., \alpha_p \in K$ şi $v_1, v_2, ..., v_p \in S$.*

Folosind caracterizarea din Propoziţia 8.2.1, rezultă prin verificare directă că:

Propoziţia 8.2.2. *Mulţimea tuturor combinaţiilor liniare finite de elementele din S formează un subspaţiu vectorial al lui V,*

Definiţia 8.2.3. *Subspaţiul vectorial obţinut în Propoziţia anterioară se numeşte* ***subspaţiul generat de*** *S şi se notează $[S]$. Elementele lui S se numesc* ***generatorii*** *subspaţiului $[S]$.*

Observaţia 8.2.2. *Dacă $S \subset V$ este un sistem de vectori astfel încât $V = [S]$, atunci spunem că V este generat de V şi S este sistem de generatori pentru V. Dacă S este mulţime finită, atunci spunem că V este finit generat.*

Exemplul 8.2.2. *În $\mathbb{Z}_2^3$, subspaţiul generat de vectorii $(\widehat{0},\widehat{1},\widehat{1}), (\widehat{1},\widehat{0},\widehat{1})$ este*

$$[(\widehat{0},\widehat{1},\widehat{1}), (\widehat{1},\widehat{0},\widehat{1})] = \{\alpha(\widehat{0},\widehat{1},\widehat{1}) + \beta(\widehat{1},\widehat{0},\widehat{1}), \quad \alpha,\beta \in \mathbb{Z}_2\} = V',$$

de la Exemplul 8.2.1 b). În $\mathbb{Z}_3^3$,

$$[(\widehat{1},\widehat{1},\widehat{2})] = \{\alpha(\widehat{1},\widehat{1},\widehat{2}), \quad \alpha \in \mathbb{Z}_3\} = \{(\widehat{0},\widehat{0},\widehat{0}), (\widehat{1},\widehat{1},\widehat{2}), (\widehat{2},\widehat{2},\widehat{1})\}$$

Propoziţia 8.2.3. *Fie $(V,+,\cdot)$ un K-spaţiu vectorial şi V_1, V_2 două subspaţii vectoriale ale sale. Mulţimile $V1 \cap V_2$ şi*

$$V_1 + V_2 = \{x_1 + x_2 | \quad x_1 \in V_1, x_2 \in V_2\}$$

sunt subspaţii vectoriale în V, numite ***intersecţia****, respectiv* ***suma*** *subspaţiilor V_1 şi V_2.*

Demonstraţie: Verificăm condiţia din Propoziţia 8.2.1 pentru fiecare din cele două submulţimi.

Fie $\alpha,\beta \in K$ şi $x,y \in V_1 \cap V_2$, arbitrar alese. Deoarece V_1 şi V_2 sunt subspaţii vectoriale, $\alpha \cdot x + \beta \cdot y \in V_1$, $\alpha \cdot x + \beta \cdot y \in V_2$, deci $\alpha \cdot x + \beta \cdot y \in V_1 \cap V_2$.

Fie $\alpha,\beta \in K$ şi $x,y \in V_1 + V_2$, arbitrar alese. Din definiţia sumei $V_1 + V_2$, există $x_1,y_1 \in V_1$, $x_2,y_2 \in V_2$ astfel încât $x = x_1 + x_2$, $y = y_1 + y_2$. Calculăm folosind regulile date de axiomele spaţiului vectorial:

$$\alpha \cdot x + \beta \cdot y = \alpha \cdot x_1 + \alpha \cdot x_2 + \beta \cdot y_1 + \beta \cdot y_2 = (\alpha \cdot x_1 + \beta \cdot y_1) + (\alpha \cdot x_2 + \beta \cdot y_2),$$

care este element din $V_1 + V_2$ deoarece $\alpha \cdot x_1 + \beta \cdot y_1 \in V_1$, $\alpha \cdot x_2 + \beta \cdot y_2 \in V_2$. $\square$

Observaţia 8.2.3. *Mulţimile $V_1 - V_2$, $V_2 - V_1$ nu sunt subspaţii vectoriale în V deoarece nu conţin vectorul nul.*

Reunuiunea a două subspaţii vectoriale nu este in general subspaţiu vectorial. De exemplu, fie următoarele subspaţii vectoriale în $\mathbb{R}$-spaţiul vectorial $\mathbb{R}^2$:

$$V_1 = \{(x, y) \in \mathbb{R}^2 | \quad 2|x\}, \quad V_2 = \{(x, y) \in \mathbb{R}^2 | \quad 2|y\},$$

Elementele $(2, 1) \in V_1$ şi $(1, 2) \in V_2$ sunt în $V_1 \cup V_2$. Dacă $V_1 \cup V_2$ ar fi subspaţiu vectorial, atunci suma $(2, 1) + (1, 2) = (3, 3)$ ar trebui să aparţină reuniunii, deci să fie element în V_1 sau V_2, adică să aibă fie prima componentă, fie a doua, pară, ceea ce nu este adevărat. Deci $V_1 \cup V_2$ nu este subspaţiu vectorial.

Propoziţia 8.2.4. *Fie V_1, V_2 două subspaţii vectoriale ale K-spaţiului vectorial V şi $x \in V_1 + V_2$. Descompunerea $x = x_1 + x_2$, $x_1 \in V_1$, $x_2 \in V_2$ este unică dacă şi numai dacă $V_1 \cap V_2 = \{0_V\}$.*

Demonstraţie: Dacă descompunerea este unică, fie $a \in V_1 \cap V_2$. Un vector $x = x_1 + x_2 \in V_1 + V_2$, cu $x_1 \in V_1$, $x_2 \in V_2$ se mai poate scrie $x = x_1 + a + x_2 - a$, şi $x_1 + a \in V_1$, $x_2 - a \in V_2$. Din ipoteză rezultă $x_1 = x_1 + a$ şi $x_2 = x_2 - a$, deci $a = 0_V$.

Reciproc, fie $V_1 \cap V_2 = \{0_V\}$ şi două descompuneri ale vectorului $x \in V_1 + V_2$: $x + x_1 + x_2$, $x = x_1' + x_2'$, cu $x_1, x_1' \in V_1$, $x_2, x_2' \in V_2$. Din $x_1 + x_2 = x_1' + x_2'$ rezultă că elementul $x_1 - x_1' = x_2' - x_2$ este în ambele subspaţii vectoriale, deci este vectorul nul. Am obţinut unicitatea descompunerii. □

Observaţia 8.2.4. *Suma a două subspaţii vectoriale V_1, V_2 se numeşte **sumă directă** dacă orice element din sumă admite descompunere unică, cum s-a precizat mai sus, or, echivalent, dacă cele două subspaţii au în comun doar vectorul nul. Suma subspaţiilor se notează în acest caz $V_1 \oplus V_2$.*

Propoziţia 8.2.5. *Fie V_1, V_2 subspaţii vectoriale în spaţiul vectorial V. Atunci $V_1 + V_2$ coincide cu subspaţiul generat de $V_1 \cup V_2$.*

Demonstraţie: Orice element din suma $V_1 + V_2$ este o combinaţie liniară de elemente din $V_1 \cup V_2$, fiind suma dintre un element din V_1 şi un element din V_2. Deci incluziunea $V_1 + V_2 \subset [V_1 \cup V_2]$ este evidentă.

Fie acum un element x din subspaţiul generat de reuniune. Acest element este o combinaţie liniară de elemente din V_1 şi V_2. Adunarea vectorilor fiind comutativă, putem grupa termenii combinaţiei formaţi cu vectori din V_1 şi să

notăm suma lor cu x_1, iar suma termenilor formaţi cu elemente din V_2 o notăm x_2. Elementul x se scrie $x = x_1 + x_2$, unde $x_1 \in V_1$, $x_2 \in V_2$. am demonstrat astfel incluziunea inversă, $[V_1 \cup V_2] \subset V_1 + V_2$. □

Exemplul 8.2.3. *Fie submulţimile* $V_1 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 | \quad x_1 + x_2 - 3x_3 = 0\}$, $V_2 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 | \quad x_1 = 2x_2 = -x_3\}$. *Să se arate că sunt subspaţii vectoriale ale* $\mathbb{R}$*-spaţiului vectorial* $\mathbb{R}^3$ *şi să se determine intersecţia şi suma lor.*

Putem verifica faptul că sunt subspaţii vectoriale folosind Propoziţia 8.2.1. Fie $\alpha, \beta \in \mathbb{R}$ *şi* $x, y \in V_1$. *Deci* $x = (x_1, x_2, x_3)$, $y = (y_1, y_2, y_3)$ *cu proprietatea* $x_1 + x_2 - 3x_3 = 0$, $y_1 + y_2 - 3y_3 = 0$. *Vectorul*

$$\alpha \cdot x + \beta \cdot y = \alpha(x_1, x_2, x_3) + \beta(y_1, y_2, y_3) = (\alpha x_1 + \beta y_1, \alpha x_2 + \beta y_2, \alpha x_3 + \beta y_3)$$

este în V_1 *dacă şi numai dacă verifică regula din definiţia lui* V_1, *adică dacă*

$$(\alpha x_1 + \beta y_1) + (\alpha x_2 + \beta y_2) - 3(\alpha x_3 + \beta y_3) = 0.$$

Ceea ce este adevărat din proprietatea similară a componentelor vectorilor x *şi* y.

O altă modalitate de a verifica că V_1, V_2 *sunt subspaţii vectoriale, este să studiem forma elementelor din aceste submulţimi. Mai exact, fiecare dintre ele reprezintă mulţimea soluţiilor unui sistem liniar de ecuaţii.* V_1 *conţine soluţiile sistemului liniar şi omogen cu o ecuaţie şi trei necunoscute*

$$x_1 + x_2 - 3x_3 = 0,$$

a cărui matrice este $A = \begin{pmatrix} 1 & 1 & -3 \end{pmatrix}$. *Rangul matricei fiind egal cu 1, sistemul are o singură necunoscută principală, fie aceasta* x_1, *corespunzător minorului principal ales, elementul de pe poziţia* $(1,1)$ *din* A. *Restul necunoscutelor fiind secundare, notăm* $x_2 = \alpha$, $x_3 = \beta$. *Rezultă* $x_1 = -\alpha + 3\beta$, *deci*

$$V_1 = \{(-\alpha + 3\beta, \alpha, \beta) | \quad \alpha, \beta \in \mathbb{R}\},$$

care se mai poate scrie folosind operaţiile de adunare şi amplificare cu scalari din spaţiul vectorial $\mathbb{R}^3$,

$$V_1 = \{(-\alpha, \alpha, 0) + (3\beta, 0, \beta) | \alpha, \beta \in \mathbb{R}\} = \{\alpha(-1, 1, 0) + \beta(3, 0, 1) | \quad \alpha, \beta \in \mathbb{R}\}.$$

Ultima exprimare a mulţimii V_1 *arată că este formată din toate combinaţiile liniare ale vectorilor* $u = (-1, 1, 0)$ *şi* $v = (3, 0, 1)$, *adică* $V1$ *este subspaţiul generat de vectorii* $\{u, v\}$, *deci, conform Propoziţiei 8.2.2,* $V_1 \leq \mathbb{R}^3$.

Analog se verifică faptul că V_2 este subspaţiu vectorial folosind caracterizarea din Propoziţia 8.2.1, sau putem vedea V_2 ca fiind mulţimea soluţiilor sistemului liniar şi omogen cu două ecuaţii şi trei necunoscute

$$x_1 - 2x_2 = 0, \quad x_1 + x_3 = 0.$$

Matricea sistemului este $A = \begin{pmatrix} 1 & -2 & 0 \\ 1 & 0 & 1 \end{pmatrix}$, *are rangul egal cu 2, un minor principal fiind* $\begin{vmatrix} 1 & -2 \\ 1 & 0 \end{vmatrix}$. *Necunoscutele principale corespunzătoare minorului principal ales sunt x_1, x_2, iar x_3, necunoscuta secundară, se notează α. Rezultă $x_1 = -\alpha$, $x_2 = \frac{1}{2}\alpha$,*

$$V_2 = \{(-\alpha, \frac{1}{2}\alpha, \alpha) | \quad \alpha \in \mathbb{R}\} = \{\alpha(-1, \frac{1}{2}, 1) | \quad \alpha \in \mathbb{R}\},$$

deci $\{w = (-1, \frac{1}{2}, 1)\}$ este sistem de generatori pentru V_2, iar V_2 este subspaţiul vectorial generat de w.

Intersecţia celor două subspaţii vectoriale este mulţimea elementelor comune, adică soluţiile sistemului liniar omogen

$$\begin{cases} x_1 + x_2 - 3x_3 &= 0 \\ x_1 - 2x_2 &= \\ x_1 + x_3 &= 0 \end{cases}$$

Obţinem $V_1 \cap V_2 = \{(0, 0, 0)\}$.

Suma celor două subspaţii este mulţimea vectorilor de forma

$$V_1 + V_2 = \{x + y | x \in V_1, y \in V_2\} = \{\alpha(-1, 1, 0) + \beta(3, 0, 1) + \gamma(-1, \frac{1}{2}, 1) | \alpha, \beta, \gamma \in \mathbb{R}\},$$

deci este subspaţiul generat de vectorii $\{u, v, w\}$, adică generat de reuniunea mulţimilor de generatori ale celor două subspaţii.

Dacă dorim să prezentă subspaţiul $V_1 + V_2$ în forma în care s-au data subspaţiile în ipoteză, putem scrie

$$V_1 + V_2 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 | x_1 = -\alpha + 3\beta - \gamma, x_2 = \alpha + \frac{\gamma}{2}, x_3 = \beta + \gamma, \quad \alpha, \beta, \gamma \in \mathbb{R}\},$$

iar studiul sistemului

$$\begin{cases} -\alpha + 3\beta - \gamma &= x_1 \\ \alpha + \frac{\gamma}{2} &= x_2 \\ \beta + \gamma &= x_3 \end{cases}$$

arată că este un sistem Cramer, deci are soluţie unică pentru orice $(x_1, x_2, x_3) \in \mathbb{R}^3$. *Rezultă că orice element din* $\mathbb{R}^3$ *este În* $V_1 + V_2$, *deci* $V_1 + V_2 = \mathbb{R}^3$. *Mai mult, deoarece* $V_1 \cap V_2$ *conţine doar vectorul nul, putem spune că* $\mathbb{R}^3$ *este suma directă a subspaţiilor* V_1 *şi* V_2 *şi notăm* $V1 \oplus V_2 = \mathbb{R}^3$.

Exemplul 8.2.4. *Considerând subspaţiile* V_1 *şi* V_2 *ale spaţiului vectorial* $\mathbb{R}^4$, *generate de vectorii* $(1, 2, -1)$, *respectiv* $(1, -1, 0)$, *subspaţiul sumă este generat de* $\{(1, 2, -1), (1, -1, 0)\}$ *deci conţine vectori de forma*

$$V_1 + V_2 = \{\alpha(1, 2, -1) + \beta(1, -1, 0) | \alpha, \beta \in \mathbb{R}^3\} =$$

$$= \{(x_1, x_2, x_3) \in \mathbb{R}^3 | x_1 = \alpha + \beta, x_2 = 2\alpha - \beta, x_3 = -\alpha, \quad \alpha, \beta \in \mathbb{R}\}.$$

Din sistemul

$$\begin{cases} \alpha + \beta &= x_1 \\ 2\alpha - \beta &= x_2 \\ -\alpha &= x_3 \end{cases}$$

rezultă, eliminând parametrii α, β, *că* $-3x_3 = x_1 + x_2$, *deci putem scrie*

$$V_1 + V_2 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 | x_1 + x_2 + 3x_3 = 0\}.$$

8.3 Bază şi dimensiune

Fie V un K-spaţiu vectorial.

Definiţia 8.3.1. *Un sistem de vectori* $S = \{v_1, v_2, ..., v_p\}$ *din* K*-spaţiul vectorial* V *se numeşte* ***liniar independent*** *dacă o combinaţie liniară a lor este nulă doar dacă scalarii din combinaţia respectvă sunt nuli, adică:*

$$\alpha_1 v_1 + \alpha_2 x_2 + ... + \alpha_p v_p = 0 \Leftrightarrow \alpha_1 = \alpha_2 = ... = \alpha_p = 0.$$

În caz contrar, vectorii se numesc liniar dependenţi deoarece prezenţa unui $\alpha_k \neq 0$ *în ecuaţia de mai sus permite ca* v_k *să se exprime ca o combinaţie liniară de ceilalţi vectori din sistem, deci depinde liniar de aceştia.*

Exemplul 8.3.1. *a) Studiaţi liniar independenţa vectorilor* $(\widehat{1}, \widehat{3}, \widehat{2}), (\widehat{2}, \widehat{1}, \widehat{1}), (\widehat{1}, \widehat{4}, \widehat{1})$ *din* $\mathbb{Z}_5$*-spaţiul vectorial* $\mathbb{Z}_5^3$. *O combinaţie liniară cu scalarii* $\alpha, \beta, \gamma \in \mathbb{Z}_5$ *a vectorilor daţi este nulă dacă şi numai dacă verifică sistemul*

$$\begin{cases} \alpha + \widehat{2}\beta + \gamma = \widehat{0} \\ \widehat{3}\alpha + \beta + \widehat{4}\gamma = \widehat{0} \\ \widehat{2}\alpha + \beta + \gamma = \widehat{0} \end{cases}$$

Soluţia este unică, $(0,0,0) \in \mathbb{Z}_5$*, deoarece determinantul matricei este* $\widehat{3}$*, deci inversabil. Rezultă că vectorii sunt liniar independenţi.*

b) În acelaşi spaţiu vectorial, vectorii $(\widehat{1},\widehat{3},\widehat{2}), (\widehat{2},\widehat{1},\widehat{1}), (\widehat{4},\widehat{2},\widehat{0})$ *sunt liniar dependenţi, ultimul se poate scrie* $\widehat{2}(\widehat{1},\widehat{3},\widehat{2}) + (\widehat{2},\widehat{1},\widehat{1})$.

Observaţia 8.3.1. *a) Mulţimea* $\{0_V\}$ *este liniar dependentă. Vectorul nul nu face parte din niciun sistem de vectori liniar independent. Mai exact, orice sistem de vectori care conţine* 0_V *este liniar dependent.*

b) Dacă $v \in V\ \{0_V\}$*, atunci* $\{v\}$ *este liniar independent, conform regulii c) din Propoziţia 8.1.1.*

b) Orice submulţime a unui sistem liniar independent de vectori (numită şi subsistem de vectori) este sistem liniar independent.

c) Orice mulţime de vectori care conţine o submulţime liniar dependentă este liniar dependentă.

În continuare ne vom referi doar la spaţii vectoriale finit generate (a se vedea Definiţia 8.2.3 şi Observaţia 8.2.2), deci care admit un sistem finit de generatori.

Definiţia 8.3.2. *Fie* V *un spaţiu vectorial finit generat. Un sistem de generatori al său se numeşte* ***bază*** *dacă este liniar independent.*

Observaţia 8.3.2. *a) Un sistem* B *de vectori din spaţiul vectorial* V *este bază dacă este liniar independenţ şi subspaţiul generat de* B *este* V*.*

b) Noţiunea de 'bază a unui spaţiu vectorial' se poate defini şi pentru spaţii infinit generat, dar nu face obiectul cursului pentru informaticieni.

Fie $B = \{v_1, v_2, ..., v_n\}$ o bază în V. Deoarece $[B] = V$, rezultă că oricare ar fi $x \in V$, există scalarii $x_1, x_2, ..., x_n \in K$ astfel încât

$$x = x_1 \cdot v_1 + x_2 \cdot v_2 + ... + x_n \cdot v_n.$$

Scalarii $(x_i)_{i=\overline{1,n}}$ se numesc *componentele vectorului* x *în baza* B.

Propoziţia 8.3.1. *Componentele unui vector într-o bază sunt unice.*

Demonstraţie: Avem ca mai sus, $x = \sum_{i=1}^{n} x_i \cdot v_i$ scrierea vectorului x în baza B. Într-adevăr, dacă elementul x ar admite şi scrierea

$$x = y_1 \cdot v_1 + y_2 \cdot v_2 + ... + y_n \cdot v_n,$$

din egalarea celor două expresii şi prin calcul simplu rezultă

$$(x_1 - y_1) \cdot v_1 + (x_2 - y_2) \cdot v_2 + ... + (x_n - y_n) \cdot v_n = 0.$$

Dar sistemul de vectori B este liniar independent, deci scalarii $x_i - y_i$ sunt nuli, $(\forall) i = \overline{1, n}$. Rezultă unicitatea componentelor unui vector într-o bază. □

Exemplul 8.3.2. *a) În K-s.v. K^n, sistemul de vectori*

$$B_c = \{e_1 = (1, 0, 0, ..., 0, 0), e_2 = (0, 1, 0, .., 0, 0), ..., e_{n-1} = (0, 0, 0, ..., 1, 0), e_n = (0, 0, 0, ..., 0, 1)\},$$

este o bază, numită ***baza canonică*** *a spaţiului.*

Într-adevăr, vectorii din B_c sunt liniar independenţi, ecuaţia $\alpha_1 \cdot e_1 + \alpha_2 \cdot e_2 + ... + \alpha_n \cdot e_n = 0$ fiind echivalentă cu $(\alpha_1, \alpha_2, ..., \alpha_n) = 0 \in K^n$, deci toţi scalarii sunt nuli.

Mai mult, orice element din K^n este de forma $x = (x_1, x_2, ..., x_n)$, cu $x_i \in K$, $(\forall) i = \overline{1, n}$, deci $x = \sum_{i=1}^{n} x_i e_i$. Elementele x_i se numesc componentele vectorului x în baza canonică. Acesta este unul din avantajele bazei canonice, componentele unui vector în această bază se citesc direct din expresia vectorului.

b) În acelaşi spaţiu vectorial, sistemul

$$B' = \{e'_1 = (1, 0, 0, ..., 0, 0), e'_2 = (1, 1, 0, .., 0, 0), ..., e'_{n-1} = (1, 1, 1, ..., 1, 0), e_n = (1, 1, 1, ..., 1, 1)\},$$

este de asemenea o bază, ecuaţia $\alpha_1 e'_1 + \alpha_2 e'_2 + ... + \alpha_n e'_n = 0$ fiind echivalentă cu următorul sistem în K

$$\begin{cases} \alpha_1 + \alpha_2 + ... + \alpha_n = 0 \\ \quad \alpha_2 + ...\alpha_n = 0 \\ \quad ..... \\ \quad \alpha_n = 0 \end{cases}$$

care are soluţia nulă unică, deci este liniar independent. Se arată uşor şi că $[B'] = K^n$, deci este bază.

Din cele două exemple de mai sus rezultă că baza unui spaţiu vectorial nu este unică.

Propoziţia 8.3.2. *Dacă $B = \{v_1, v_2, ...v_n\}$ este un sistem de vectori liniar independent, atunci orice $n + 1$ vectori din subspaţiul generat de B, sunt liniar dependenţi.*

Demonstraţie: Fie $\{w_1, w_2, ..., w_{n+1}\} \subset [B]$. Mulţimea B fiind liniar independentă, ea este bază în subsptaţiul $[B]$ generat de B. Rezultă că există în mod unic scalarii α_{ij}, $i = \overline{1, n+1}$, $j = \overline{1, n}$ astfel încât $w_i = \sum_{j=1}^{n} \alpha_{ij} v_j$.

Fie acum o combinaţie liniară nulă a vectorilor $w_1, w_2, ..., w_{n+1}$:

$$a_1 w_1 + a_2 w_2 + ...a_{n+1} w_{n+1} = 0.$$

Înlocuind w_i şi ţinând cont de liniar independenţa vectorilor $v_1, v_2, ..., v_n$, rezultă sistemul liniar de n ecuaţii cu $n+1$ necunoscute $a_1, a_2, ..a_{n+1}$:

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} + ... + a_{n+1}\alpha_{n+1,1} &= 0 \\ a_1\alpha_{12} + a_2\alpha_{22} + ... + a_{n+1}\alpha_{n+1,2} &= 0 \\ \quad ..... & .. \quad ... \\ a_1\alpha_{1n} + a_2\alpha_{2n} + ... + a_{n+1}\alpha_{n+1,n} &= 0 \end{cases}$$

Sistemul este omogen şi numărul de ecuaţii este mai mic decât numărul de necunoscute, deci este compatibil nedeterminat. Există aşadar scalari nenuli $a_1, ...a_{n+1}$, adică vectorii $w_1, w_2, ..., w_{n+1}$ sunt liniar dependenţi. □

O consecinţă imediată a Propoziţiei anterioare este aceea că într-un spaţiu vectorial generat de n vectori liniar independenţi nu există sisteme de vectori liniar independente de dimensiune mai mare decât n. De aici rezultă imediat că:

Propoziţia 8.3.3. *Orice două baze ale unui spaţiu vectorial finit generat au acelaşi număr de elemente.*

Definiţia 8.3.3. *Numărul de elemente al unei baze într-un spaţiu vectorial se numeşte dimensiunea spaţiului. Dimensiunea spaţiului vectorial care conţine doar vectorul nul este 0 (în acest spaţiu vectorial nu există bază).*

Exemplul 8.3.3. *a) Din Exemplul 8.3.2 rezultă* $dim(K^n) = n$, *pentru orice corp comutativ* K. *În particular,* $dim\mathbb{R}^n = n$ *şi* $dim\mathbb{Z}_p^n = n$, *pentru orice număr prim* p.

b) În Exemplul 8.2.3, $dimV_1 = 2$, *deoarece mulţimea* $\{u, v\}$ *a generatorilor este liniar independentă. Ţinând cont de Observaţia 8.3.1 b),* $dimV_2 = 1$, *iar din definiţia dimensiunii,* $dim(V_1 \cap V_2) = 0$. *Rezultatul* $V_1 + V_2 = \mathbb{R}^3$ *conduce la* $dim(V_1 + V_2) = 3$.

Propoziţia 8.3.4. *Din orice sistem de generatori al unui spaţiu vectorial finit generat se poate extrage o bază. Orice sistem de vectori liniar independent se poate prelungi la o bază.*

Demonstraţie: Evident, enunţul se referă la spaţii vectoriale diferite de $\{O\}$. Fie V un spaţiu vectorial finit generat şi S un sistem de generatori al său. Alegem un vector nenul din S, fie el v_1. DEvident un astfel de vector există, deoarece $V \neq \{0_V\}$. Dacă subspaţiul generat de el este V, adică dacă $V = [v_1]$, atunci $\{v_1\}$ este bază în V. Dacă nu, atunci există $v_2 \in S - [v_1]$. Acest lucru este justificat de faptul că dacă $S \subseteq [v_1]$, atunci toţi vectorii din S ar fi de forma $v_i = \lambda_i v_1$, şi am obţine $V = [S] = [v_1]$.

Considerăm sistemul $\{v_1, v_2\}$, care, din modul de alegere a lui v_2, este liniar independent. Dacă $V = [\{v_1, v_2\}]$, atunci acest sistem de vectori este bază în V. Dacă nu, atunci există $v_3 \in S - [v_1, v_2]$, care nu depinde liniar de v_1, v_2. Continuăm algoritmul cu $\{v_1, v_2, v_3\}$.

Deoarece S este finită, după un număr finit de paşi găsim o bază formată din elementele lui S.

Fie acum $L \subset V$ un sistem de vectori liniar independent. Dacă subspaţiul generat de L este V, atunci L este bază în V. dacă nu, atunci există $u_1 \in V - [L]$, iar sistemul de vectori $L_1 = L \cup \{u_1\}$ este liniar independent. Într-adevăr, elementele din L erau liniar independente, iar u_1 nu este o combinaţie liniară a lor, fiind ales $u_1 \notin [L]$, deci nu depinde liniar de elementele din L.

Reluăm discuţia pentru noul sistem liniar independent L_1 şi, deoarece V este finit generat, după un număr finit de paşi L va fi completat la un sistem liniar independent care este şi sistemn de generatori, adică la o bază. □

Fie V un K-s.v, $dim(V) = n$ şi $B = \{e_1, .., e_n\}$, $B' = \{e'_1, ..., e'_n\}$ două baze în V.

Un vector arbitrar din V se scrie în mod unic în raport cu cele baze $x = \sum_{i=1}^{n} x_i e_i$, respectiv $x = \sum_{i=1}^{n} x'_i e'_i$. În particular, $e'_j = \sum_{k=1}^{n} s_j^k e_k$, pentru orice $j = \overline{1,n}$ Matricea $S = (s_j^i)_{i,j=\overline{1,n}}$ ale cărei coloane sunt componentele vectorilor din B' în raport cu B se numeşte *matricea schimbării de bază* în V.

Revenim la exprimarea vectorului x în bazele B, B'. Avem

$$\sum_{i=1}^{n} x_i e_i = x = \sum_{j=1}^{n} x'_j e'_j = \sum_{j=1}^{n} x'_j \sum_{k=1}^{n} s_j^k e_k = \sum_{j,k=1}^{n} x'_j s_j^k e_k,$$

iar din liniar independenţa sistemuli de vectori B rezultă $x_k = \sum_{j=1}^{n} x'_j s_j^k$, pentru orice $k = \overline{1,n}$. Dacă notăm cu $X, X' \in M_{n,1}(K)$ coloanele componentelor

vectorului x în B, respectiv B', atunci ultima relaţie se scrie matriceal

$$X = SX',$$

şi dă legătura între vechile şi noile componente ale unui vector la schimbarea bazei.

Exemplul 8.3.4. *Dacă dorim să determinăm componentele vectorului* $v = (1, 2, 3)$ *în baza* $B' = \{e'_1 = (1, 1, 0), e'_2 = (1, 0, 1), e'_3 = (0, 1, 1)\}$ *din* $\mathbb{R}$*-spaţiul vectorial* $\mathbb{R}^3$*, atunci trebuie să determinăm constantele* α*,* β*,* γ *cu care verifică*

$$\alpha \cdot e'_1 + \beta \cdot e'_2 + \gamma \cdot e'_3 = v,$$

ceea ce revine la a rezolva sistemul

$$\begin{cases} \alpha + \beta &= 1 \\ \alpha + \gamma &= 2 \\ \beta + \gamma &= 3 \end{cases}$$

Obţinem componentele vectorului v *în baza* B'*:* $(0, 1, 2)$*.*

O altă metodă este să folosim matricea schimbării de bază, de trecere de la baza canonică la baza B'*. Amintim că în raport cu baza canonică, componentele unui vector* $x = (x_1, x_2, x_3)$ *sunt exact numerele* x_1, x_2, x_3*. Deci matricea de trecere de la baza canonică la baza* B' *are pe coloane vectorii bazei* B'*:*

$$S = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

. Componentele vectorului $v = (1, 2, 3)$ *în baza canonică, scise matriceal, sunt* $X = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$*, iar matricea componentelor lui* v *în noua bază o notăm* X'*. După cum am văzut mai sus, legătura dintre ele este* $X' = S \cdot X$*, care nu reprezintă altceva decât scrierea matriceală a sistemului anterior. Rezolvarea matriceală revine la* $X = S^{-1}X'$*, iar prin calcul direct găsim* $X' = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$*.*

Observaţia 8.3.3. *Dacă un spaţiu vectorial* V *are baza* $B = \{v_1, v_2, ..., v_n\}$*, atunci orice vector* $x \in V$ *se scrie unic*

$$x = x_1v_1 + x_2v_2 + .. + x_nv_n,$$

ceea ce putem scrie matriceal $x = G^t \cdot X$, *unde* X *este matricea componentelor lui* x *în baza* B, *iar* $G = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$, *este matricea ale cărei linii sunt componentele vectorilor din bază, şi care se numeşte* ***matricea generatoare*** *a spaţiului* V.

Exemplul 8.3.5. *Fie*

$$S = \{(x_1, x_2, x_3, x_4, x_5) \in \mathbb{Z}_3^5 | x_1 + \hat{2}x_2 + x_3 = \hat{0}, \quad x_4 + \hat{2}x_5 = \hat{0}\},$$

submulţime a $\mathbb{Z}_3$*-spaţiului vectorial* $\mathbb{Z}_3^5$. *Această submulţime este subspaţiu vectorial, deoarece elementele sale, fiind soluţiile sistemului din definiţia lui* S, *sunt de forma* $(\alpha, \beta, \alpha+\beta, \gamma, \gamma)$ *(am ales* $x_1 = \alpha$, $x_2 = \beta$, $x_4 = \gamma$ *necunoscute secundare). Deci*

$$S = \{(\alpha, \hat{0}, \alpha, \hat{0}, \hat{0}) + (\hat{0}, \beta, \beta, \hat{0}, \hat{0}) + (\hat{0}, \hat{0}, \hat{0}, \gamma, \gamma) | \alpha, \beta, \gamma \in \mathbb{Z}_3\},$$

adică S *este subspaţiul generat de* $\{(\hat{1}, \hat{0}, \hat{1}, \hat{0}, \hat{0}), (\hat{0}, \hat{1}, \hat{1}, \hat{0}, \hat{0}), (\hat{0}, \hat{0}, \hat{0}, \hat{1}, \hat{1})\}$. *Matricea generatoare a acestui subspaţiu este*

$$G = \begin{pmatrix} \hat{1} & \hat{0} & \hat{1} & \hat{0} & \hat{0} \\ \hat{0} & \hat{1} & \hat{1} & \hat{0} & \hat{0} \\ \hat{0} & \hat{0} & \hat{0} & \hat{1} & \hat{1} \end{pmatrix},$$

iar un element oarecare se obţine din calculul

$$\begin{pmatrix} \alpha & \beta & \gamma \end{pmatrix} \cdot G$$

.

Încheiem paragraful cu un comentariu referitor la corpuri finite. Fie K un corp finit, deci şi comutativ. Atunci caracteristica sa este un număr prim p şi K este o extindere a lui $\mathbb{Z}_p$. Să observăm că restricţionând înmulţirea din K la $\mathbb{Z}_p \times K$, corpul K are structură de spaţiu vectorial peste $\mathbb{Z}_p$. Fie n dimensiunea acestui spaţiu vectorial. Se demonstrează că mulţimile K şi $\mathbb{Z}_p^n$ sunt cardinal echivalente, deci numărul de elemente din K este o putere a caracteristicii sale, $|K| = p^n$. O consecinţă de aici este că nu există corpuri cu 6 sau cu 10 elemente, de exemplu.

8.4 Produs scalar, ortogonalitate, normă, metrică.

Definiţia 8.4.1. *Fie K un corp comutativ şi V un K-spaţiu vectorial. O aplicaţie $<,>: V \times V \to K$ biliniară şi simetrică se numeşte* ***pseudoprodus scalar*** *pe V.*

Condiţiile din definiţie sunt:

a) $< \alpha x + \beta y, z >= \alpha < x, z > +\beta < y, z >$, $(\forall) x, y, z \in V$, $\alpha\beta \in K$ (liniaritatea în prima componentă);

b) $< x, \alpha y + \beta z >= \alpha < x, y > +\beta < x, z >$, $(\forall) x, y, z \in V$, $\alpha\beta \in K$ (liniaritatea în a doua componentă);

c) $< x, y >=< y, x >$, $(\forall) x, y, z \in V$ (simetria).

Dacă în plus aplicaţia $<,>$ verifică şi

d) $< x, x >\geq 0$, $(\forall) x \in V$ şi $< x, x >= 0 \Leftrightarrow x = 0$, atunci se numeşte **produs scalar**.

Un spaţiu vectorial real (peste corpul numerelor reale) dotat cu un produs scalar se numeşte spaţiu *euclidian.*

Exemplul 8.4.1. *Pentru orice corp comutativ K, aplicaţia $<,>: K^n \times K^n \to K$,*

$$< x, y >= x_1y_1 + x_2y_2 + ... + x_ny_n, (\forall) x = (x_1, ..., x_n), y = (y_1, ..., y_n) \in K^n,$$

este un pseudoprodus scalar, numit ***pseudoprodusul scalar canonic****. Verificarea este imediată, ţinând cont de distributivitatea înmulţirii din K.*

În cazul $K = \mathbb{R}$, $<,>$ este chiar produs scalar.

În spactiul euclidian $(V, <, >)$ se pot defini lungimea (norma) unui vector şi unghiul dintre doi vectori, astfel:

$$\|x\| = \sqrt{< x, x >}, \quad cos(\widehat{x, y}) = \frac{|< x, y >|}{\|x\| \, \|y\|}.$$

Definiţiile de mai sus au sens deoarece $< x, x >\geq 0$ pentru orice $x \in V$, iar produsul scalar verifică *inegalitatea lui Cauchy*:

$$|< x, y >| \leq \|x\| \, \|y\|$$

Într-adevăr, pentru orice $\lambda \in \mathbb{R}$, şi orice $x, y \in V$,

$$< x - \lambda y, x - \lambda y >\geq 0,$$

din definiţia produsului scalar. Din biliniaritatea produsului scalar, relaţia anterioară devine

$$\lambda^2 \|y\|^2 - 2\lambda < x, y > + \|x\|^2 \geq 0, \quad (\forall)\lambda \in \mathbb{R},$$

condiţie echivalentă cu

$$\Delta = 4 < x, y >^2 - 4 \|y\|^2 \|x\|^2 \leq 0.$$

Exemplul 8.4.2. *În spaţiul vectorial real $\mathbb{R}^4$, dotat cu produsul scalar canonic, vom calcula normele următorilor vectori şi unghiul dintre ei: $x = (1, -1, 4, 2)$, $y = (2, 1, -1, 3)$.*

Calculăm:

$$\|x\| = \sqrt{1^2 + (-1)^2 + 4^2 + 2^2} = \sqrt{22}, \quad \|y\| = \sqrt{2^2 + 1^2 + (-1)^2 + 3^2} = \sqrt{15},$$

$$cos(\widehat{x, y}) = \frac{|1 \cdot 2 + (-1) \cdot 1 + 4 \cdot (-1) + 2 \cdot 3|}{\sqrt{22} \cdot \sqrt{15}} = \frac{1}{\sqrt{15 \cdot 22}}.$$

Din definiţia produsului scalar rezultă că

Propoziţia 8.4.1. *Într-un spaţiu euclidian V funcţia $\|\cdot\| : V \to \mathbb{R}_+$ verifică relaţiile:*

a) $\|x\| = 0$ dacă şi numai dacă $x = 0$.

b) $\|\alpha x\| = |\alpha| \|x\|$.

c) $\|x + y\| \leq \|x\| + \|y\|$,

pentru orice vectori $x, y \in V$ şi orice scalar real α.

Un spaţiu vectorial în care s-a definit o aplicaţie cu proprietăţile din Propoziţia 8.4.1 se numeşte *spaţiu normat*. Orice spaţiu euclidian este spaţiu normat.

Numim *distanţa* dintre vectorii x, y din spaţiul euclidian $(V, <, >)$ numărul

$$d(x, y) = \|x - y\|.$$

Se verifică imediat că:

Propoziţia 8.4.2. *a)$d(x, y) \geq 0$ şi $d(x, y) = 0$ dacă şi numai dacă $x = 0$;*

b) $d(x, y) = d(y, x)$;

c)$d(x, y) \leq d(x, z) + d(z, y)$,

pentru orice vectori $x, y, z \in V$.

Un spaţiu vectorial în care s-a definit o aplicaţie cu proprietăţile din Propoziţia 8.4.2 se numeşte *spaţiu metric*. Orice spaţiu euclidian este spaţiu metric.

8.4.1 Ortogonalitate

Fie V un K-spaţiu vectorial dotat cu un pseudoprodus scalar $<,>$.

Definiţia 8.4.2. *Doi vectori $x, y \in V$ spunem că sunt **ortogonali** şi scriem $x \perp y$, dacă $< x, y >= 0$.*

Dacă spaţiul este euclidian, semnificaţia ortogonalităţii a doi vectori se apropie de cel intuitiv, unghiul dintre cei doi vectori fiind drept (cosinusul său este zero).

Definiţia 8.4.3. *Două subspaţii vectoriale ale spaţiului V sunt **ortogonale** dacă fiecare vector din primul subspaţiu este ortogonal pe orice vector din al doilea.*

Mai mult, pentru orice subspaţiu S din V considerăm mulţimea

$$S^{\perp} = \{y \in V, \quad < y, x >= 0, (\forall)x \in S\}.$$

Se verifică imediat că $S^{\perp}$ este subspaţiu vectorial în V, numit *subspaţiul ortogonal* lui S.

Fie $dimV = n$ şi S un subspaţiu p-dimensional al său, cu baza $\{v_1, ..v_p\}$. Atunci orice vector din S se scrie unic $x = \sum_{i=1}^{p} x_i v_i$. Subspaţiul său ortogonal conţine vectorii ortogonali pe orice vector din S, deci conţine toţi vectorii $y \in V$ care verifică $< y, v_i >= 0, (\forall)i = \overline{1, p}$.

Reciproc, orice vector y din V ortogonal pe baza din S este ortogonal pe S deoarece din proprietăţile care definesc produsul scalar,

$$< y, x >= \sum_{I=1}^{p} x_i < y, v_i >= 0.$$

Deci $S^{\perp}$ conţine toţi vectorii din V ortogonali pe baza din S, şi doar pe aceştia.

Fie $\{u_1, u_2, ..., u_q\}$ baza în $S^{\perp}$ şi scalarii $\alpha_1, ..., \alpha_p, \beta_1, ..., \beta_q \in K$ astfel încât

$$\alpha_1 v_1 + ... + \alpha_p v_p + \beta_1 u_1 + ... + \beta_q u_q = 0.$$

Calculând $< v_i, \alpha_1 v_1 + ... + \alpha_p v_p + \beta_1 u_1 + ... + \beta_q u_q >= 0$, obţinem $\alpha_i = 0$, $(\forall)i = \overline{1, p}$, iar din $< u_j, \alpha_1 v_1 + ... + \alpha_p v_p + \beta_1 u_1 + ... + \beta_q u_q >= 0$ rezultă $\beta_j = 0$, $(\forall)j = \overline{1, q}$, deci reuniunea bazelor din S şi $S^{\perp}$ este un sistem de vectori liniar independenţi.

Pe de altă parte, fie $x \in V$ arbitrar ales şi vectorul

$$y = x - \sum_{i=1}^{p} < x, v_i > v_i,$$

evident tot un vector din V. Pentru orice $i = \overline{1,p}$, calculăm $< y, v_i >= 0$, deci $y \in S^{\perp}$, deci există scalarii $y_1, ..., y_q$ astfel încât $y = \sum_{j=1}^{q} y_j u_j$. Avem deci pentru orice $x \in V$ scrierea

$$x = \sum_{i=1}^{p} < x, v_i > v_i + \sum_{j=1}^{q} y_j u_j,$$

deci reuniunea bazelor din cele două subspaţii este bază în V. Rezultă $dim S^{\perp} = n - p$. Obţinem de aici şi $V = S + S^{\perp}$.

Dacă spaţiul $(V, <, >)$ este euclidian, atunci pentru $x \in S \cap S^{\perp}$, x verifică condiţia $< x, x >= 0$. Deci suma $S + S^{\perp}$ este directă, adică $V = S \oplus S^{\perp}$.

Exemplul 8.4.3. *a) În spaţiul vectorial $\mathbb{Z}_3^4$ dotat cu pseudoprodusul scalar canonic, se cere subspaţiul ortogonal subspaţiului S generat de vectorii $(\widehat{1}, \widehat{2}, \widehat{1}, \widehat{0})$, $(\widehat{1}, \widehat{0}, \widehat{1}, \widehat{0})$, $(\widehat{0}, \widehat{1}, \widehat{2}, \widehat{1})$.*

Se verifică liniar independenţa vectorilor generatori, deci ei reprezintă o bază în subspaţiul S al cărui sistem de generatori este mulţimea lor. Subspaţiul ortogonal lui S este format din vectorii $(x_1, x_2, x_3, x_4) \in \mathbb{Z}_3^4$ care sunt soluţii ale sistemului

$$\begin{cases} x_1 + \widehat{2}x_2 + x_3 = \widehat{0} \\ x_1 + x_3 = \widehat{0} \\ x_2 + \widehat{2}x_3 + x_4 = 0 \end{cases}$$

adică $S^{\perp} = \{(2z, 0, z, z,), \quad z \in \mathbb{Z}_3\} = [(\widehat{2}, \widehat{0}, \widehat{1}, \widehat{1})]$. Dimensiunea spaţiului $S^{\perp}$ este unu şi are 3 elemente. Matricele generatoare ale celor două subspaţii sunt

$$G_S = \begin{pmatrix} \hat{1} & \hat{2} & \hat{1} & \hat{0} \\ \hat{1} & \hat{0} & \hat{1} & \hat{0} \\ \hat{0} & \hat{1} & \hat{2} & \hat{1} \end{pmatrix}, \quad G_{S^{\perp}} = \begin{pmatrix} \widehat{2} & \widehat{0} & \widehat{1} & \widehat{1} \end{pmatrix}.$$

b)În spaţiul euclidian standard ($\mathbb{R}^3$,$<, >$) se consideră subspaţiul $S = \{(x_1.x_2, x_3) \in \mathbb{R}^3 \mid x_1 - 2x_2 + x_3 = 0\}$. Să se determine subspaţiul ortogonal lui S.

Subspaţiul S conţine soluţiile ecuaţiei $x_1 - 2x_2 + x_3 = 0$, adică $S = \{(\alpha, \beta, 2\beta - \alpha) \mid \alpha, \beta \in \mathbb{R}\}$. Aşadar, baza în S este $\{v_1 = (1, 0, -1), v_2 = (0, 1, 2)\}$.

Subspaţiul $S^\perp$ ortogonal lui S este format din vectorii (y_1, y_2, y_3) ortogonali pe baza lui S, deci care verifică sistemul

$$\begin{cases} y_1 - y_3 = 0 \\ y_2 + 2y_3 = 0, \end{cases}$$

Am găsit $S^\perp = \{(\alpha, -2\alpha, \alpha) \mid \alpha \in \mathbb{R}\} = [(1, -2, 1)]$

Deoarece matricea generatoare G a unui subspaţiu vectorial şi matricea generatoare H a subspaţiului său ortogonal verifică $G \cdot H^t = 0$, dacă G este de forma $(I \quad A)$, atunci $H = (-A^t \quad I)$, unde I este matricea unitate corespunzătoare dimensiunilor din cele 2 matrice G şi H.

O altă metodă pentru a găsi matricea generatoare a subspaţiului ortogonal pe subspaţiul S cu matricea generatoare G este să o prelucrăm prin transformări elementare, până devine de forma de mai sus. Remarcăm că transformările elementare, constând în adunare de linii eventual amplificare cu scalari, modifică baza din S tot într-o bază, deci într-o altă matrice generatoare a lui S.

Exemplul 8.4.4. *Pentru subspaţiile din exemplul precedent, avem:*

a)

$$G_S = \begin{pmatrix} \hat{1} & \hat{2} & \hat{1} & \hat{0} \\ \hat{1} & \hat{0} & \hat{1} & \hat{0} \\ \hat{0} & \hat{1} & \hat{2} & \hat{1} \end{pmatrix} \overset{\hat{2}L_1 + L_2}{\Leftrightarrow} \begin{pmatrix} \hat{1} & \hat{2} & \hat{1} & \hat{0} \\ \hat{0} & \hat{1} & \hat{0} & \hat{0} \\ \hat{0} & \hat{1} & \hat{2} & \hat{1} \end{pmatrix} \overset{L_2 + L_1}{\Leftrightarrow}$$

$$\begin{pmatrix} \hat{1} & \hat{0} & \hat{1} & \hat{0} \\ \hat{0} & \hat{1} & \hat{0} & \hat{0} \\ \hat{0} & \hat{1} & \hat{2} & \hat{1} \end{pmatrix} \overset{\hat{2}L_2 + L_3}{\Leftrightarrow} \begin{pmatrix} \hat{1} & \hat{0} & \hat{1} & \hat{0} \\ \hat{0} & \hat{1} & \hat{0} & \hat{0} \\ \hat{0} & \hat{0} & \hat{2} & \hat{1} \end{pmatrix} \overset{\hat{2}L_3}{\Leftrightarrow}$$

$$\begin{pmatrix} \hat{1} & \hat{0} & \hat{1} & \hat{0} \\ \hat{0} & \hat{1} & \hat{0} & \hat{0} \\ \hat{0} & \hat{0} & \hat{1} & \hat{2} \end{pmatrix} \overset{\hat{2}L_3 + L_1}{\Leftrightarrow} \begin{pmatrix} \hat{1} & \hat{0} & \hat{0} & \hat{1} \\ \hat{0} & \hat{1} & \hat{0} & \hat{0} \\ \hat{0} & \hat{0} & \hat{1} & \hat{2} \end{pmatrix}$$

Avem G echivalent cu $(I \quad A)$, cu $A^t = \begin{pmatrix} \hat{1} & \hat{0} & \hat{2} \end{pmatrix}$, deci

$$H = \begin{pmatrix} \hat{2} & \hat{0} & \hat{1} & \hat{1} \end{pmatrix},$$

unde am completat $-A^t$, adică $\hat{2}A^t$ cu matricea unitate de ordin 1, adică $\hat{1}$.

Remarcăm că am obţinut o altă matrice decât în exemplul anterior, adică o altă bază, legătura dintre ele fiind

$$(\widehat{2}, \widehat{0}, \widehat{1}, \widehat{1}) = \hat{2} \cdot (\widehat{1}, \widehat{0}, \widehat{2}, \widehat{2}).$$

b) Matricea generatoare este deja în forma dorită, $(I \quad A)$, $G_S = \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}$, *unde* $A = \begin{pmatrix} -1 & 0 \\ 2 & 1 \end{pmatrix}$, *deci matricea generatoare a subspaţiului ortogonal este*

$$H = \begin{pmatrix} 1 & -2 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix},$$

Încheiem paragraful referitor la ortogonalitate cu *Procedeul de ortonormare Gramm-Schmidt*, o metodă de obţinere a unei baze ortonormate într-un spaţiu euclidian.

Într-un spaţiu euclidian, un sistem de vectori se numeşte *ortonormat* dacă orice doi vectori din sistem sunt ortogonali şi toţi vectorii sunt de normă unu.

Pornind de la un sistem de vectori $S = \{v_1, v_2, ..., v_p\}$, se poate găsi un sistem de vectori ortonormat care generează acelaşi spactiu ca şi S. Dacă vectorii sunt liniar independenţi, atunci sistemul ortonormat are tot atâţia vectori cât cel iniţial.

Procedeul prin care se obţine sistemul ortonormat se numeşte *Procedeul de ortonormare Gramm-Schmidt*:

Se determină primul vector din sistemul ortonormat $e_1 = \frac{1}{\|v_1\|} v_1$.

Se calculează $f_k = v_k - \sum_{i=1}^{k-1} < v_k, e_i > e_i$, pentru $k = \overline{2, n-1}$, care este un vector ortogonal pe toţi e_i determinaţi anterior, după cum vom justifica mai jos.

Se normează f_k, determinând următorul vector, e_k, din sistemul ortonormat.

Vectorii obţinuţi astfel sunt în mod evident normaţi, iar fiecare f_k, deci si fiecare e_k, este ortogonal pe e_j, $j = \overline{1, k-1}$. Într-adevăr,

$$< f_2, e_1 >=< v_2 - < v_2, e_1 > e_1, e_1 >=< v_2, e_1 > - < v_2, e_1 >< e_1, e_1 >= 0,$$

din proprietăţile produsului scalar şi din faptul că vectorul e_1 este normat.

Presupunem acum că $< e_i, e_j >= \delta_{ij}$, pentru orice $i, j \in \{1, 2, ..., k-1\}$ şi arătăm că f_k este ortogonal pe e_j, unde δ_{ij} este simbolul lui Kronecker, definit prin $\delta ij = 0$ dacă $i \neq j$ şi $\delta_i i = 1$. Pentru orice $j < k$, fixat, are loc

$$< f_k, e_j >=< v_k, e_j > - \sum_{i=1}^{k-1} < v_k, e_i >< e_i, e_j >=< v_k, e_j > - < v_k, e_j >= 0.$$

Exemplul 8.4.5. *Să se ortonormeze folosind procedeul de ortonormare Gramm-Schmidt următoarele sisteme de vectori din spaţiul euclidian cu produsul scalar canonic* $(\mathbb{R}^3, <, >)$*:*

$\{v_1 = (1,1,0), v_2 = (1,0,1), v_3 = (1,2,-2)\}$

Urmăm algoritmul de ortonormare şi avem primul vector din sistemul ortonormat

$$e_1 = \frac{1}{\| v_1 \|} v_1 = \frac{1}{\sqrt{2}}(1,1,0).$$

Pornind de la vectorul v_2 *găsim un vector* f_2 *ortogonal pe* e_1 *astfel:*

$$f_2 = v_2 - < v_2, e_1 > e_1 = (1,0,1) - \frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0) = (\frac{1}{2}, -\frac{1}{2}, 1).$$

Vectorul f_2 *îl normăm şi obţinem al doilea vector din sistemul ortonormat:*

$$e_2 = \frac{1}{\| f_2 \|} f_2 = \frac{2}{\sqrt{6}}(\frac{1}{2}, -\frac{1}{2}, 1) = (\frac{1}{\sqrt{6}}, -\frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}).$$

Din vectorul v_3 *găsim un vector* f_3 *ortogonal pe vectorii* e_1, e_2 *găsiţi anterior:*

$$f_3 = v_3 - < v_3, e_1 > e_1 - < v_3, e_2 > e_2 =$$

$$= (1,2,-2) - \frac{3}{\sqrt{2}}(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0) - (-\frac{5}{\sqrt{6}}(\frac{1}{\sqrt{6}}, -\frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}) = (\frac{1}{3}, -\frac{1}{3}, -\frac{1}{3}).$$

Ultimul vector din sistemul ortonormat este

$$e_3 = \frac{1}{\| f_3 \|} f_3 = \frac{1}{\sqrt{3}}(\frac{1}{3}, -\frac{1}{3}, -\frac{1}{3}) = (\frac{1}{3\sqrt{3}}, -\frac{1}{3\sqrt{3}}, -\frac{1}{3\sqrt{3}}).$$

8.5 Transformări liniare. Matricea unei transformări liniare

8.5.1 Morfisme liniare

Fie V, W două spaţii vectoriale peste acelaş corp comutativ K.

Definiţia 8.5.1. *O funcţie* $T : V \to W$ *cu proprietatea că*

$$T(x+y) = T(x) + T(y), \quad T(\alpha x) = \alpha T(x), \quad (\forall) x, y \in V, \alpha \in K,$$

se numeşte ***morfism liniar*** *sau transformare liniară.*

Condiţia din definiţia de mai sus se mai poate scrie

$$T(\alpha x + \beta y) = \alpha T(x) + \beta T(y), \quad (\forall) x, y \in V, \alpha, \beta \in K.$$

Remarcăm faptul că pentru orice morfism liniar au loc relaţiile

$$T(0) = 0, \quad T(-x) = -T(x), \quad (\forall) x \in V.$$

Exemplul 8.5.1. *Aplicaţia* $T : \mathbb{R}^2 \to \mathbb{R}^3$*,*

$$T(x) = (x_1 + x_2, 2x_1 - x_2, x_1), \quad (\forall) x = (x_1, x_2) \in \mathbb{R}^2,$$

este un morfism liniar deoarece pentru orice $x = (x_1, x_2), y = (y_1, y_2) \in \mathbb{R}^2$ *şi orice* $\alpha, \beta \in K$ *avem:*

$$T(\alpha x+\beta y) = (\alpha x_1+\beta y_1+\alpha x_2+\beta y_2, 2(\alpha x_1+\beta y_1)-(\alpha x_2+\beta y_2), \alpha x_1+\beta y_1) = \alpha T(x)+\beta T(y).$$

Fie V, W spaţii finit dimensionale, $B_V = \{e_1, ..., e_n\}$, $B_W = \{f_1, ..., f_m\}$, baze în aceste spaţii. Fie $T : V \to W$ un morfism liniar. Orice $x \in V$ se descompune unic $x = \sum_{i=1}^n x_i e_i$. Din liniaritatea morfismului T rezultă $T(x) = \sum_{i=1}^n x_i T(e_i)$, ceea ce înseamnă că aplicaţia T este bine definită dacă cunoaştem valorile ei pe baza din domeniul de definiţie. Pentru orice $i = \overline{1,n}$, $T(e_i)$ este un elemnet din W, deci se descompune unic după baza din codomeniu:

$$T(e_i) = a_i^1 f_1 + a_i^2 f_2 + ... + a_i^m f_m, \quad i = \overline{1,n}.$$

Matricea în care pe coloana i avem componentele vectorului $T(e_i)$, $A = (a_i^j)_{i=\overline{1,n}, j=\overline{1,m}}$ $\in M_{m,n}(K)$ se numeşte *matricea transformării* T în raport cu bazele date. Revenind la un x arbitrar din V, componentele vectorului $T(x)$ în raport cu baza B_W sunt date prin intermediul matricei A:

$$T(x) = \sum_{i=1}^n x_i T(e_i) = \sum_{i=1}^n \sum_{j=1}^m x_i a_i^j f_j,$$

relaţie care se scrie matriceal $Y = AX$, unde $Y \in M_{m,1}(K)$ reprezintă coloana componentelor vectorului $T(x)$ în raport cu B_W, iar $X \in M_{n,1}$ reprezintă coloana componentelor vectorului x în raport cu B_V.

Exemplul 8.5.2. *Scrieţi matricea transformării liniare* $T : \mathbb{Z}_5^3 \to \mathbb{Z}_5^4$,

$$T(x) = (\widehat{2}x_1 + x_3, \widehat{3}x_2 + \widehat{4}x_3, x_1 + x_3, x_1 + x_2 + \widehat{2}x_3), \quad (\forall)x = (x_1, x_2, x_3) \in \mathbb{Z}_5^3,$$

în raport cu bazele canonice din domeniu şi codomeniu.

Bazele canonice sunt $B_1 = \{e_1 = (\widehat{1}, \widehat{0}, \widehat{0}), e_2 = (\widehat{0}, \widehat{1}, \widehat{0}), e_3 = (\widehat{0}, \widehat{0}, \widehat{1})\}$, *respectiv* $B_1 = \{f_1 = (\widehat{1}, \widehat{0}, \widehat{0}, \widehat{0}), f_2 = (\widehat{0}, \widehat{1}, \widehat{0}, \widehat{0}), f_3 = (\widehat{0}, \widehat{0}, \widehat{1}, \widehat{0}), f_4 = (\widehat{0}, \widehat{0}, \widehat{0}, \widehat{1})\}$. *Calculăm*

$$\begin{cases} T(e_1) = (\widehat{2}, \widehat{0}, \widehat{1}, \widehat{1}) = \widehat{2}f_1 + f_3 + f_4 \\ T(e_2) = (\widehat{0}, \widehat{3}, \widehat{0}, \widehat{1}) = \widehat{3}f_2 + f_4 \\ T(e_3) = (\widehat{1}, \widehat{4}, \widehat{1}, \widehat{2}) = f_1 + \widehat{4}f_2 + f_3 + \widehat{2}f_4 \end{cases}$$

de unde matricea transformării este $A = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 3 & 4 \\ 1 & 0 & 4 \\ 1 & 1 & 2 \end{pmatrix}$.

Remarcăm faptul că dacă $W = V$, atunci vorbim despre matricea transformării T în raport cu o singură bază, aceeaşi şi în domeniu şi în codomeniu. Dacă B şi B' sunt douĂ baze în V, cu S matricea schimbării de bază, iar X, X' sunt coloanele componentelor unui vector x şi Y, Y' coloanele componentelor vectorului $T(x)$ în raport cu cele două baze, atunci avem următoarele relaţii:

$$Y = AX, \quad Y' = A'X', \quad X = SX', \quad Y = SY',$$

unde A, A' sunt matricele transformării T în raport cu B, respectiv B'. Din relaţiile de mai sus rezultă legătura între matricele unei transformări la schimbarea bazei:

$$A' = S^{-1}AS.$$

Exemplul 8.5.3. *Scrieţi matricea transformării* $T : \mathbb{R}^3 \to \mathbb{R}^3$, $T_1(x) = (x^1 + 2x^2, -x^3, x^1 + x^3)$, $x = (x^1, x^2, x^3)$; *în raport cu baza* $B' = \{e_1', e_2', e_3'\}$, *unde* $e_1' = (1, -1, 1)$, $e_2' = (0, 1, 1)$, $e_3' = (1, 2, 3)$.

Folosim definiţia matricei unei transformări liniare. Calculăm

$$\begin{gathered} T(e_1') = (-1, -1, 2) \\ T(e_2') = (2, -1, 1) \\ T(e_3') = (5, -2, 4) \end{gathered}$$

Pentru a găsi componentele vectorilor de mai sus în raport cu baza B', trebuie să rezolvăm sistemele de ecuaţii liniare

$$x \cdot e'_1 + y \cdot e'_2 + z \cdot e'_3 = T(e'_i), \quad i = \overline{1,3}.$$

După cum am văzut în paragraful 5.8, putem rezolva simultan aceste trei sisteme de ecuaţii folosind metoda eliminării, astfel:

$$\begin{pmatrix} 1 & 0 & 1 & -1 & 2 & 5 \\ -1 & 1 & 2 & -1 & -1 & -2 \\ 1 & 1 & 3 & 2 & 1 & 4 \end{pmatrix} \overset{L_1+L_2}{\Leftrightarrow} \begin{pmatrix} 1 & 0 & 1 & -1 & 2 & 5 \\ 0 & 1 & 3 & -2 & 1 & 3 \\ 1 & 1 & 3 & 2 & 1 & 4 \end{pmatrix} \overset{-L_1+L_3}{\Leftrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 1 & -1 & 2 & 5 \\ 0 & 1 & 3 & -2 & 1 & 3 \\ 0 & 1 & 2 & 3 & -1 & -1 \end{pmatrix} \overset{-L_2+L_3}{\Leftrightarrow} \begin{pmatrix} 1 & 0 & 1 & -1 & 2 & 5 \\ 0 & 1 & 3 & -2 & 1 & 3 \\ 0 & 0 & -1 & 5 & -2 & -4 \end{pmatrix} \overset{(-1)\cdot L_3}{\Leftrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 1 & -1 & 2 & 5 \\ 0 & 1 & 3 & -2 & 1 & 3 \\ 0 & 0 & 1 & -5 & 2 & 4 \end{pmatrix} \overset{(-1)\cdot L_3+L_1}{\Leftrightarrow} \begin{pmatrix} 1 & 0 & 0 & 4 & 0 & 1 \\ 0 & 1 & 3 & -2 & 1 & 3 \\ 0 & 0 & 1 & -5 & 2 & 4 \end{pmatrix} \overset{(-3)\cdot L_3+L_2}{\Leftrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 0 & 4 & 0 & 1 \\ 0 & 1 & 0 & 13 & -5 & -9 \\ 0 & 0 & 1 & -5 & 2 & 4 \end{pmatrix},$$

deci matricea este

$$A'_{T_1} = \begin{pmatrix} 4 & 0 & 1 \\ 13 & -5 & -9 \\ -5 & 2 & 4 \end{pmatrix}$$

O altă metodă constă în aplicarea formulei care dă matricea unei transformări liniare la schimbarea bazei:

$$A' = S^{-1}.A.S,$$

unde S este matricea schimbării de bază de la B la B', A este matricea transformării în raport cu B iar A' matricea transformării în raport cu B'. Matricea transformării T în raport cu baza canonică este $A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 1 \end{pmatrix}$. Matricea schimbării de la baza canonică la B' din enunţ este

$$S = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 2 \\ 1 & 1 & 3 \end{pmatrix}$$

Inversa sa este

$$S^{-1} = \begin{pmatrix} -1 & -1 & 1 \\ -5 & -2 & 3 \\ 2 & 1 & -1 \end{pmatrix}$$

Obţinem

$$A' = \begin{pmatrix} -1 & -1 & 1 \\ -5 & -2 & 3 \\ 2 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 2 \\ 1 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 0 & 2 \\ 13 & -5 & -7 \\ -5 & 2 & 3 \end{pmatrix}$$

Fie $T : V \to W$ un morfism liniar între K-spactiile vectoriale V, W. Se verifică uşor că nucleul transformării,

$$KerT = T^{-1}\{0\} = \{x \in V, \quad T(x) = 0\},$$

este subspaţiu vectorial în V, iar imaginea sa

$$ImT = T(V) = \{y \in W, \quad (\exists)x \in V, T(x) = y\}$$

este subspaţiu vectorial în W. Într-adevăr, fie doi vectori $y_1, y_2 \in ImT$ arbitrar aleşi şi $\alpha, \beta \in K$, oarecare. Există $x_1, x_2 \in V$ astfel încât

$$\alpha y_1 + \beta y_2 = \alpha T(x_1) + \beta T(x_2) = T(\alpha x_1 + \beta x_2) \in ImT.$$

Dacă A este matricea transformării T în raport cu baze date în cele două spaţii, atunci orice vector din ImT are coloana componentelor AX, cu X coloana componentelor unui vector din V. Se mai scrie că ImT este dat de $A \cdot V$.

Exemplul 8.5.4. *Determinaţi nucleul şi imaginea pentru* $T : \mathbb{R}^3 \to \mathbb{R}^4, \quad T(x) = (x^1 + x^2 - x^3, x^2 - x^3, -x^1 - x^2 + x^3, x^2 - x^3), \ \ x = (x^1, x^2, x^3)$;

Lăsăm cititorului verificarea faptului că T *este transformare liniară. Fie* $x = (x^1, x^2, x^3) \in KerT$. *Ecuaţia* $T(x) = 0$ *conduce la sistemul*

$$\begin{cases} x^1 + x^2 - x^3 = 0 \\ x^2 - x^3 = 0 \\ -x^1 - x^2 + x^3 = 0 \\ x^2 - x^3 = 0 \end{cases}$$

Sistemul este compatibil simplu nedeterminat, soluţia generală fiind $KerT = \{(0, \alpha, \alpha) \mid \ \alpha \in \mathbb{R}\}$, *deci nucleul transformării* T *este un subspaţiu de dimensiune 1 al spaţiului* $\mathbb{R}^3$, *generat de vectorul* $(0, 1, 1)$. *Imaginea aplicaţiei* T *este*

$$ImT = \{T(x) \mid \ x \in \mathbb{R}^3\} = \{(x^1+x^2-x^3, x^2-x^3, -x^1-x^2+x^3, x^2-x^3) \mid \ x^1, x^2, x^3 \in \mathbb{R}\}.$$

Generatorii acestui subspaţiu al lui $\mathbb{R}^4$ *sunt vectorii* $(1,0,-1,0),(1,1,-1,1),(-1,-1,1,-1)$, *vectori liniar dependenţi (rangul matricei care are pe coloane cei trei vectori este 2), de unde rezultă că* ImT *este subspaţiu de dimensiune 2 al codomeniului.*

8.6 Vectori şi valori proprii. Algoritm de diagonalizare a unei matrice. Forme pătratice.

8.6.1 Vectori şi valori proprii

Fie V un K-s.v. şi $T : V \to V$ o transformare liniară.

Definiţia 8.6.1. *Un vector* $x \in V - \{0\}$ *se numeşte* ***vector propriu*** *pentru* T *dacă există un scalar* $\lambda \in K$ *astfel încât* $T(x) = \lambda \cdot x$. *Scalarul* λ *de mai sus se numeşte* ***valoare proprie*** *a lui* T *corespunzătoare vectorului* x.

Remarcăm că vectorul nul satisface egalitatea din definiţia de mai sus pentru orice scalar λ. Dacă A este matricea transformării T în raport cu o bază dată, atunci egalitatea $T(x) = \lambda x$ se scrie matriceal $AX = \lambda X$.

Dacă x este un vector propriu corespunzător unei valori proprii λ, atunci pentru orice scalar $\alpha \in K$, vectorul αx este de asemenea vector propriu pentru aceeaşi valoare proprie:

$$T(\alpha x) = \alpha T(x) = \alpha(\lambda x) = \lambda(\alpha x), \quad (\forall)\alpha \in K.$$

Prin urmare, dacă λ este valoare proprie a lui T, atunci sistemul $(A - \lambda I)X = 0$ are o infinitate de soluţii. Fiind un sistem liniar şi omogen, rezultă că determinantul acestui sistem este nul, deci valorile proprii ale transformării T sunt soluţiile ecuaţiei *caracteristice*

$$det(A - \lambda I) = 0.$$

Propoziţia 8.6.1. *Fie* λ *o valoare proprie a transformării* $T : V \to V$. *Mulţimea* $V_\lambda = \{x \in V | \quad T(x) = \lambda x\}$, *este un subspaţiu vectorial în* V, *invariant la* T, *adică pentru orice* $x \in V_\lambda$, $T(x) \in V_\lambda$.

Demonstraţie: Fie $\alpha, \beta \in K$ şi $x, y \in V_\lambda$, arbitrar alese. Avem $T(x) = \lambda x$, $T(y) = \lambda y$. Din definiţia transformării liniare, putem calcula

$$T(\alpha x + \beta y) = \alpha T(x) + \beta T(y) = \alpha\lambda x + \beta\lambda y = \lambda(\alpha x + \beta y),$$

de unde rezultă $\alpha x + \beta y \in V_\lambda$. Deci V_λ este subspaţiu vectorial în V.

Pentru orice $x \in V_\lambda$, $T(T(x)) = T(\lambda x) = \lambda T(x)$, deci $T(x) \in V_\lambda$. □

Subspaţiul V_λ din Propoziţia anterioară se numeşte **subspaţiul propriu corespunzător valorii proprii** λ.

Are loc următoarea

Propoziţia 8.6.2. *a) Fie λ şi ξ două valori proprii distincte ale transformării liniare $T : V \to V$. Atunci $V_\lambda \cap V_\xi = \{0_V\}$.*

b) Vectori proprii nenuli corespunzători la valori proprii distincte sunt liniar independenţi.

Demonstraţie: a) Presupunem prin absurd că $x \in V - \{0_V\}$ este un element din $V_\lambda \cap V_\xi$. Obţinem $T(x) = \lambda x = \xi x$, care poate fi prelucrat astfel $(\lambda - \xi) \cdot x = 0$. Conform Propoziţiei 8.1.1, rezultă $x = o_v$ sau $\lambda = \xi$, contradicţie. Deci vectorul nul este singurul element din intersecţia spaţiilor de vectori proprii corespunzători la valori proprii distincte.

b) Fie λ şi ξ două valori proprii distincte ale transformării liniare $T : V \to V$ şi vectorii proprii nenuli $x \in V_\lambda$ şi $y \in V_\xi$. Studiem liniar independenţa celor doi vectori, deci fie $\alpha, \beta \in K$ astfel încât $\alpha x + \beta y = 0_V$. Aplică egalităţii anterioare transformarea T şi obţinem $\alpha T(x) + \beta T(y) = 0_V$, care implică $\alpha\lambda x + \beta\xi y = 0_V$. Rezolvăm sistemul

$$\begin{cases} \alpha x + \beta y &= 0_V \\ \alpha\lambda x + \beta\xi y &= 0_V \end{cases}$$

Amplificăm prima ecuaţie cu λ, scădem ecuaţia obţinută din cea de a două ecuaţie a sistemului şi rezultă $\beta(\xi - \lambda)y = 0_V$ Din regulile de calcul în spaţii vectoriale şi $\lambda \neq \xi$, $y \neq 0_V$, rezultă $\beta = 0$, apoi $\alpha = 0$. Vectorii x, y sunt deci liniar independenţi. □

Definiţia 8.6.2. *O transformare liniară $T : V \to V$ se numeşte **diagonalizabilă** dacă există o bază în V astfel încât matricea lui T în această bază să aibă forma diagonală, adică singurele elemente nenule să se afle pe diagonala principală.*

Se poate demonstra că

Teorema 8.6.1. *Transformarea liniară $T : V \to V$ este diagonalizabilă dacă şi numai dacă toate valorile proprii ale lui T sunt din K şi dacă ordinulul de multiplicitate al fiecărei valori proprii λ ca rădăcină a ecuaţiei caracteristice coincide cu dimensiunea spaţiului V_λ.*

Baza în care T admite această formă este reuniunea bazelor din subspaţiile proprii.

Faptul că transformarea liniară T estediagonalizabilă se mai exprimă spunând că matricea A a lui T în raport cu baza canonică din V este diagonalizabilă.

Dăm în continuare un algoritm de diagonalizare a unei transformări liniare/ matrice.

P1) Se fixează o bază (de preferinţă baza canonică) în K-spaţiul vectorial V şi se calculează matricea A a transformării $T : V \to V$ în raport cu această bază.

P2) Se determină valorile proprii λ_j, $j = \overline{1,p}$, rădăcinile ecuaţiei caracteristice $det(A - \lambda I) = 0$.

P3) Se verifică dacă $\lambda_j \in K$, $(\forall) j = \overline{1,p}$. Dacă da, atunci se trece la pasul următor. Dacă nu, atunci T nu este diagonalizabil.

P4) Se stabileşte ordinul de multiplicitate m_j pentru fiecare valoare proprie λ_j, $j = \overline{1,p}$.

P5)Se determină subspaţiile proprii V_{λ_j} şi câte o bază în fiecare din acestea. Se stabileşte dimensiunea $dim(V_{\lambda_j})$, numită multiplicitatea geometrică a valorii proprii λ_j, $j = \overline{1,p}$.

P6) Dacă $m_j = dim(V_{\lambda_j})$, pentru orice $j = \overline{1,p}$, trecem la pasul următor. Dacă nu, atunci T nu este diagonalizabil.

P7) Scriem matricea A' care are pe diagonala principală valorile proprii, fiecare fiind scrisă de m_j ori, iar în rest are zerouri. Această matrice se obţine şi scriind matricea transformării T în raport cu baza obţinută din reuniunea bazelor subspaţiilor proprii.

Exemplul 8.6.1. *Să se determine valorile proprii şi vectorii proprii corespunzători acestora pentru următoarea matrice. Precizaţi dacă admite formă diagonală şi dacă da, în raport cu ce bază se obţine aceasta.*

$$A = \begin{pmatrix} -1 & -1 & 1 \\ -4 & -1 & 2 \\ -6 & -3 & 4 \end{pmatrix}$$

Valorile proprii ale unei matrice sunt rădăcinile ecuaţiei caracteristice:

$$\begin{vmatrix} -1-\lambda & -1 & 1 \\ -4 & -1-\lambda & 2 \\ -6 & -3 & 4-\lambda \end{vmatrix} = 0,$$

sau, echivalent, $\lambda^3 - 2\lambda^2 + \lambda = 0$. *Obţinem valorile proprii* $\lambda_1 = \lambda_2 = 1$, $\lambda_3 = 0$, *toate sunt numere reale, deci trecem la pasul următor.*

Determinăm subspaţiile proprii corespunzătoare valorilor proprii găsite:

Subspaţiul $V_{(1)}$ *corespunzător valorii proprii* $\lambda = 1$ *conţine vectorii pentru care coloana componentelor verifică ecuaţia* $A \cdot X = \lambda X$, *deci soluţiile sistemului:*

$$\begin{cases} -2x_1 - x_2 + x_3 = 0 \\ -4x_1 - 2x_2 + 2x_3 = 0 \\ -6x_1 - 3x_2 + 3x_3 = 0 \end{cases}$$

Avem

$$V_{(1)} = \{(\alpha, \beta, 2\alpha + \beta) \mid \ \alpha, \beta \in \mathbb{R}\} =< (1, 0, 2), (0, 1, 1) > .$$

Analog determinăm subspaţiul propriu corespunzător valorii proprii $\lambda = 0$, *ca fiind mulţimea soluţiilor sistemului*

$$\begin{cases} -x_1 - x_2 + x_3 = 0 \\ -4x_1 - x_2 + 2x_3 = 0 \\ -6x_1 - 3x_2 + 4x_3 = 0 \end{cases}$$

Avem

$$V_{(0)} = \{(\alpha, 2\alpha, 3\alpha) \mid \ \alpha \in \mathbb{R}\} =< (1, 2, 3) > .$$

Valorile proprii sunt reale, deci din câmpul scalarilor spaţiului vectorial $\mathbb{R}^3$.

Multiplicitatea algebrică a valorii proprii 1 *este egală cu* 2, *(este rădăcină dublă a polinomului caracteristic) şi egală cu* $dim V_{(1)}$, *numită multiplicitatea geometrică a valorii proprii date. Analog, multiplicitatea algebrică şi cea geometrică a valorii proprii* 0 *coincid, fiind ambele egale cu* 1. *Toate condiţiile pentru existenţa formei diagonale sunt astfel îndeplinite, deci există forma*

$$A' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

a matricei A. *Dacă* T *este transformarea liniară care are matricea* A *în raport cu baza canonică, atunci* A' *este matricea aceleiaşi transformări în raport cu baza formată din reuniunea bazelor subspaţiilor proprii, în ordinea în care apar valorile proprii pe diagonala lui* A', *deci în baza* $B' = \{(1, 0, 2), (0, 1, 1), (1, 2, 3)\}$. *Notând cu* S *matricea de trecere de la baza canonică la* B', *verificaţi relaţia* $A' = S^{-1}AS$.

8.7 Exerciţii

1) Care dintre următoarele submulţimi din spaţiul vectorial real $\mathbb{R}^4$ sunt subspaţii vectoriale?

1. $S_1 = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 | \quad x_1 + 2x_2 + x_3 - 2x_4 = 0\}$
2. $S_2 = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 | \quad x_1 - x_2 + x_3 = 0\}$
3. $S_3 = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 | \quad x_1 + x_2 + 3x_3 - 2x_4 = 0, \quad x_1 + 3x_4 = 0\}$
4. $S_4 = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 | \quad x_1 + 2x_2 + x_3 - 2x_4 = 7\}$
5. $S_5 = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 | \quad x_1^2 - x_2 + x_3 + x_4 = 0\}$

2) Scrieţi subspaţiile vectoriale generate de următoarele sisteme de vectori din $\mathbb{R}^3$:

a) $\{(1, -1, 1)\}$
b) $\{(-2, 1, 0), (1, -1, 1), (-1, 0, 1)\}$
c) $\{(2, 1, -1), (1, 1, 1), (-1, 4, 2), (1, -1, 3)\}$

3) În spaţiul vectorial real $\mathbb{R}^3$ se dau subspaţiile vectoriale

1. $S_1 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 | \quad x_1 - x_2 + 2x_3 = 0\}$
2. $S_2 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 | \quad x_1 - x_2 + x_3 = 0\}$
3. $S_3 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 | \quad x_1 + x_2 = 0\}$
4. $S_4 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 | \quad x_1 = 2x_2 = x_3 = 0\}$
5. $S_5 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 | \quad x_1 + x_2 = 0, 2x_2 + x_3 = 0\}$

Determinaţi câte o bază şi dimensiunea în fiecare dintre aceste spaţii, apoi în subpaţiile vectoriale $S_1 \cap S_2$, $S_1 + S_2$, $S_1 \cap S_3$, $S_1 + S_3$, $S_1 \cap S_4$, $S_1 + S_4$, $S_1 \cap S_5$, $S_1 + S_5$, $S_3 \cap S_2$, $S_3 + S_2$. Verificaţi de fiecare dată Teorema lui Grassmann.

4) In spaţiul vectorial real $\mathbb{R}^3$ se dă submulţimea

$$S = \{(x_1, x_2, x_3) \in \mathbb{R}^3 | \quad x_1 - 2x_2 + x_3 = 0\}.$$

Demonstraţi că S este subspaţiu vectorial, determinaţi o bază în S şi găsiţi componentele vectorului $(4, 1, -2) \in S$ în raport cu această bază.

5) Studiaţi care dintre următoarele sisteme de vectori sunt liniar independente.

1. $\mathcal{S}_1 = \{(3,1,-1),(2,2,1),(1,0,1),(1,-1,1)\}$ în $\mathbb{R}^3$.
2. $\mathcal{S}_2 = \{(-1,0,1),(1,2,1),(1,4,3)\}$ în $\mathbb{R}^3$.
3. $\mathcal{S}_3 = \{(0,-1,3,1),(1,2,-2,0),(1,1,-1,1)\}$ în $\mathbb{R}^3$.
4. $\mathcal{S}_4 = \{(-1,2),(4,2),(3,4)\}$

6) Demonstraţi că următoarele sisteme de vectori sunt baze în spaţiul vectorial real $\mathbb{R}^3$.

1. $\mathcal{B}_1 = \{v_1 = (1,1,-1), v_2 = (2,-1,1), v_3 = (1,0,1)\}$.
2. $\mathcal{B}_2 = \{u_1 = (2,1,1), u_2 = (1,2,1), u_3 = (1,1,2)\}$
3. $\mathcal{B}_3 = \{w_1 = (0,-1,3), w_2 = (1,2,-2), w_3 = (1,1,-1)\}$

Se cer:

- Găsiţi componentele vectorului $v = (1,2,3)$ în fiecare dintre aceste baze.
- Scrieţi matricea schimbării de bază de la baza $\mathcal{B}_1$ la $\mathcal{B}_2$, folosind baza canonică.
- Scrieţi matricea schimbării de bază de la baza $\mathcal{B}_2$ la $\mathcal{B}_3$, folosind baza canonică şi găsiţi componentele vectorului $w = 2u_1 + u_3$ în baza $\mathcal{B}_3$.

7) Să se ortonormeze următoarele sisteme de vectori din spaţiul vectorial real $\mathbb{R}^3$, folosind procedeul de ortonormare Gramm-Schmidt:

1. $\{v_1 = (1,1,-1), v_2 = (2,-1,1), v_3 = (1,0,1)\}$
2. $\{u_1 = (1,-2,2), u_2 = (-1,0,-1), u_3 = (5,3,-7)\}$
3. $\{w_1 = (2,1,2), w_2 = (1,2,-2), w_3 = (2,-2,1)\}$
4. $\{z_1 = (1,-1,2), z_2 = (1,2,-1), z_3 = (2,1,1)\}$.

8) In spaţiul vectorial real $\mathbb{R}^3$ se dă subspaţiul

$$S = \{(x_1, x_2, x_3) \in \mathbb{R}^3 | \quad 2x_1 + x_2 - x_3 = 0\}.$$

Determinaţi subspaţiul ortogonal $S^\perp$ şi găsiţi proiecţiile vectorului $v = (3, -1, 2)$ pe fiecare din subspaţiile S şi $S^\perp$.

9) Determinaţi subspaţiul ortogonal subspaţiilor S_1, S_2, S_3, S_4, S_5 de la exerciţuil 3, şi câte o bază ortonormată în fiecare S_i, $S_i^\perp$, $i = \overline{1,5}$. Găsiţi proiecţia vectorului $v = (1, 2, 3)$ pe fiecare din subspaţiile S_i, $i = \overline{1,5}$.

10) In spaţiul vectorial real $\mathbb{R}^3$ se dă $g : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$,

$$g(x, y) = \frac{3}{4}(x_1y_1 + x_2y_2 + x_3y_3) - \frac{1}{4}(x_1y_2 + x_1y_3 + x_2y_1 + x_2y_3 + x_3y_1 + x_3y_2).$$

Să se arate că $(\mathbb{R}^3, g)$ este un spaţiu euclidian. Să se arate că $S = \{v = (0.1.1), u = (1, 0, 1)\}$ este un sistem de vectori ortonormat în $(\mathbb{R}^3, g)$ şi să se completeze la o bază ortonotmată în raport cu g.

11) Să se arate că următoarele funcţii $T : \mathbb{R}^3 \to \mathbb{R}^3$ sunt morfisme liniare, să se determine pentru fiecare $Ker(T)$, $Im(T)$ şi matricea în raport cu baza $\mathcal{B}' = \{e_1' = (0, 1, 1), e_2' = (1, 0, 1), e_3' = (1, 1, 0)\}$

a) $T(x) = (x_1 + x_2, x_1 + x_2 + 2x_3, -x_1 - x_2)$;
b) $T(x) = (x_2 - x_3, x_1 + 2x_2 - 2x_3, 3x_1)$;
c) $T(x) = (x_1 + x_2 - x_3, x_1 - x_3, x_1 + x_3)$.

12) Pentru următoarele transformări liniare să se scrie matricea în baza canonică. Studiaţi dacă există forma diagonală pentru fiecare dintre aceste transformări. Determinaţi forma diagonală şi baza în raport cu care au această formă:

a) $T(x) = (-x_1 - 3x_3, 3x_1 + 2x_2 + 3x_3, -3x_1 - x_3)$;
b) $T(x) = (5x_1 + 2x_2 + 3x_3, 2x_1 - x_2, 3x_1 + x_3)$;
c) $T(x) = (x_2, x_1 + x_2 + x_3, x_2)$;
d) $T(x) = (x_1 + 3x_3, 2x_1 + x_2 + 2x_3, 3x_1 + x_3)$;
e) $T(x) = (x_1, x_3, x_2)$;
f) $T(x) = (2x_1 + x_2 - 3x_3, 3x_1 - 2x_2 - 3x_3, x_1 + x_2 - 2x_3)$;
g) $T(x) = (-x_1 + 3x_2 - x_3, -3x_1 + 5x_2 - x_3, -3x_1 + 3x_2 + x_3)$;
h) $T(x) = (2x_1 - x_2 + 2x_3, 5x_1 - 3x_2 + 3x_3, -x_1 - 2x_3)$;

Capitolul 9

Introducere în teoria codurilor

9.1 Codificare şi decodificare

Fie mulţimile nevide A şi B, numite *alfabet sursă*, respectiv *alfabet cod*.

Definiţia 9.1.1. *Numim* ***codificare*** *o aplicaţie injectivă* $k : A \to B^*$, *unde* $(B^*, \cdot)$ *este monoidul liber generat de* B.

Mulţimea $Imk = k(A) \subset B^*$ se numeşte *cod*, iar elementele sale se numesc *cuvinte cod*.

Dacă B are doar două elemente, de obicei $0, 1$, atunci codul se numeşte *binar*.

Fie codificarea $k : A \to B^*$. Numim codificare a mesajelor sursă aplicaţia $k^* : A^* \to B^*$ care este morfism între grupurile libere generate de cele două alfabete. Acest lucru revine la

$$k^*(\lambda) = \lambda, \quad k^*(\alpha\beta) = k^*(\alpha)k^*(\beta),$$

oricare ar fi cuvintele sursă $\alpha, \beta \in A^*$, λ fiind cuvântul vid. Din definiţia de mai sus rezultă că un cuvânt sursă se codifică codificând fiecare simbol al său.

Exemplul 9.1.1. *a) Aplicaţia* $k : \{a, b, c\} \to \{0, 1\}^*$, *definită prin* $k(a) = 01$, $k(b) = 111$, $k(c) = 10$ *este o codificare a alfabetului sursă* $\{a, b, c\}$. *Mesajul-sursă aab se codifică prin* 0101111. *Recepţionând mesajul* 10111010110111 *decodificăm cbaacb*.

b) Codul 2 din 5: Printre secvenţele binare de lungime 5, sunt 10 secvenţe (combinări de 5 luate câte 2) ce conţin câte 2 de 1. Ele pot fi folosite pentru a codifica cifrele din scrierea zecimală:

$$k(1) = 11000, \quad k(2) = 10100, \quad k(3) = 10010, \quad k(4) = 10001, \quad k(5) = 01100,$$

$$k(6) = 01010, \quad k(7) = 01001, \quad k(8) = 00110, \quad k(9) = 00101, \quad k(0) = 00011.$$

Mesajul sursă 173 *are codul* 110000100110010 *Pentru decodificare împărţim mesajul recepţionat în grupe de câte 5 şi decodificarea este unică.*

c) Aplicaţia $k : \{0,1,2,3,4,5,6,7,8,9\} \to \{0,1\}^*$ *cu legea* $k(x)$ *este expresia numărului* x *în baza 2 nu permite decodificarea unică. Într-adevăr, avem codul*

$$k(0) = 0, \quad k(1) = 1, \quad k(2) = 10, \quad , k(3) = 11, \quad k(4) = 100,$$

$$k(5) = 101, \quad k(6) = 110, \quad , k(7) = 111, \quad k(8) = 1000, \quad k(9) = 1001.$$

Mesajul sursă 765 *are codificarea* 111110101. *La recepţionarea acestui mesaj putem decodifica* 765, *dar şi* 3325, *deci pot să apară erori nedetectabile, ambele cuvinte decodate fiind posibile ca mesaj sursă.*

c) Codul Morse este o codificare a alfabetului latin prin trei simbolui, alfabetul cod fiind $\{\cdot, -, spaiu\}$.

Definiţia 9.1.2. *a) Codificarea* k *este cu* ***decodificare unică*** *dacă* k^* *este injectivă, adică oferă o singură soluţie la decodificarea unui mesaj recepţonat.*

b)O codificare în care toate cuvintele au aceeaşi lungime n *se numeşte* ***cod-bloc de lungime*** n.

c) O codificare se numeşte ***instantanee*** *dacă niciun cuvânt cod nu este prefixul altui cuvânt cod.*

Exemplul 9.1.2. *Codul 2 din 5 este o codificare bloc de lungime 5, cu decodificare unică şi instantaneu. Codificarea din exemplul c) de mai sus nu este nici instantanee, deoarece* $k(2)$ *este prefixul lui* $k(5)$, *nici cu decodificare unică.*

Observăm că într-o codificare instantanee decodificarea se face când se identifică un cuvânt cod, indiferent de simbolurile care urmează.

Orice codificare bloc este instantanee deoarece cuvintele cod având aceeaşi lungime, nu se poate ca unul să fie prefixul altuia.

Exemplul 9.1.3. *Următoarele coduri sunt coduri-bloc des întâlnite:*

Codul octal: codifică ciferle de la 0 *la* 7 *prin scrierea lor în baza* 2.

Codul ASCII: codifică 128 de simboluri în secvenţe binare de lungime 8, *în care primele 7 poziţii conţin informaţia, iar ultimul, numit bit de paritate, este suma modulo 2 a primelor 7 cifre.*

Codul ISBN (International Standard Book number) este un cod bloc de lungime 10, cu alfabetul cod $\{0,1,2,...,9,X\}$, X *fiind corespunzător numărului* 10. *Mai*

apare şi simbolul "-", care are rolul de a delimita numerele care reprezintă ţara (România are codul 973), editura, numărul de identificarea cărţii, dat de editură, iar în final un simbol de control, dat de formula $\sum_{i=1}^{10} ia_{11-i} \equiv 0(mod 11)$*, pentru codul ISBN* $a_1a_2...a_{10}$*. De exemplu, pentru codul ISBN* $973-598-141-\alpha$*, ultima cifră trebuie să fie* 7*.*

9.1.1 Construcţia codurilor instantanee

Vrem să construim un cod binar instantaneu peste alfabetul sursă $A = \{a_1, a_2, ..., a_n\}$. Iniţial se specifică lungimile cuvintelor cod: $d_1, d_2, ..., d_n$. Fără a restrânge generalitatea, putem presupune $d_1 \leq d_2 \leq ... \leq d_n$.

-Se alege un cuvânt-cod binar $k(a_1)$ de lungime d_1,arbitrar.

-Se alege un cuvânt -cod binar $k(a_2)$, de lungime d_2, care nu are pe $k(a_1)$. Există 2^{d_2} cuvinte binare de lungime 2 (practic, ele reprezintă numărul de funcţii definite de la o mulţime cu d_2 la o mulţime cu 2 elemente). Există $2^{d_2-d_1}$ cuvinte de lungime d_2 care au pe $k(a_1)$ ca prefix. Prin urmare avem de ales pentru $k(a_2)$ un cuvânt din cele $2^{d_2} - 2^{d_2-d_1} \geq 1$ disponibile. Inegalitatea anteriară se datorează inegalităţii $1 \leq d_1 \leq d_2$.

- Pentru $k(a_3)$ avem de ales dintre cele $2^{d_3} - (2^{d_3-d_2} + 2^{d_3-d_1})$ cuvinte de lungime d_3 care nu ca prefix niciunul din cuvintele cod alese anterior. Acest lucru este posibil dacă şi numai dacă $2^{d_3} - (2^{d_3-d_2} + 2^{d_3-d_1}) \geq 1$, ceea ce este echivalent cu $2^{-d_3} + 2^{-d_2} + 2^{-d_1} \leq 1$, etc.

De fapt, are loc

Teorema 9.1.1. *Fiind dat un alfabet sursă cu n simboluri şi un alfabet cod cu m simboluri, se poate construi un cod instantaneu cu lungimile cuvintelor* $d_1, d_2, ..., d_n$ *dacă şi numai dacă are loc* ***inegalitatea lui Kraft****:*

$$m^{-d_1} + m^{-d_2} + ... + m^{-d_n} \leq 1.$$

Demonstraţia este similară raţionamentului anterior, pentru $m = 2$. Se poate demonstra că

Teorema 9.1.2 (Mc Millan)**.** *Orice codificare cu decodificare unică satisface inegalitatea lui Kraft.*

Propoziţia 9.1.1. *Pentru orice cod cu decodificare unică există un cod instantaneu care are toate cuvintele-cod de aceeaşi lungime.*

Într-adevăr, fie $k : A \to B^*$ un cod cu decodificare unică, unde $|A| = n$, $|B| = m$. Codul este cu decodificare unică cu toate cuvintele de lungime d dacă este verificată inegalitatea lui Kraft, care aici este $nm^{-d} \leq 1$. Pentru orice numere naturale m, n, există d care să verifice inegalitatea.

Exemplul 9.1.4. *Fie $A = \{a, b, c\}$, $B = \{0, 1\}$. Caut un cod cu cuvintele de aceeaşi lungime, fie ea d. Acest număr trebuie să verifice inegalitatea $3 \cdot 2^{-d} \leq 1$, de unde $d \geq 2$. Deci orice mulţime de 3 cuvinte-cod de lungime 2 poate fi folosită drept cod: $\{00, 01, 10\}$, $\{00, 01, 11\}$, $\{00, 10, 11\}$, sau $\{01, 10, 11\}$.*

Există şi alte tipuir de coduri cu decodificare unică, de exemplu *codurile cu virgulă*, coduri în care există un simbol care delimitează cuvintele-cod, cum ar fi codul Morse.

9.2 Coduri liniare

Mesajele urmează calea: sursă—codificator—-decodificator—-receptor. Un mesaj $x_1x_2...x_k$ se codifică în $y_1y_2...y_n$. Datorită paraziţilor de pe canalul de transmitere de la codificator la decodificator, la decodificator ajunge un mesaj $\widetilde{y}_1, \widetilde{y}_2...\widetilde{y}_n$.

Dacă $\widetilde{y}_i = y_i$, $(\forall)i = \overline{1, n}$, atunci transmisia s-a făcut corect.

Dacă însă $\widetilde{y}_i \neq y_i$ pentru un I, atunci există o eroare de transmisie. Dacă $\widetilde{y}_i$ este cuvânt cod, eroarea nu este detectabilă. Eventual se semnalează o incoerenţă în mesaj şi se solicită retransmiterea mesajului. Dacă $\widetilde{y}_i$ nu este cuvânt cod, eroarea este detectabilă.

Codurile liniare fac codificarea astfel încât erorile detectabile sunt semnalate fără a face căutări în mulţimea cuvintelor-cod.

Fie p un număr prim, n, k numere naturale nenule, $k < n$. Se ştie că $(\mathbf{Z}_p, +, \cdot)$ este corp comutativ şi $(\mathbf{Z}_p^k, +, \cdot)$ este un $\mathbf{Z}_p$ -spacţiu vectorial.

Definiţia 9.2.1. *Numim **codificare liniară** un morfism liniar şi injectiv*

$$\varphi : \boldsymbol{Z}_p^k \to \boldsymbol{Z}_p^n.$$

*Imaginea acestui morfism se notează $A_{n,k}$ şi se numeşte **(n,k)-cod liniar**.*

Din Modulul II, din Unitatea de învățare *Spaţii vectoriale* se ştie că imaginea unui morfism liniar este subspaţiu vectorial al codomeniului său. Mai mult, injectivitatea lui φ face ca $A_{n,k}$ să fie izomorf cu domeniul $\mathbf{Z}_p^k$ prin φ. Avem deci

Propoziţia 9.2.1. *Un (n,k)-cod liniar este subspaţiu vectorial de dimensiune k în $\boldsymbol{Z}_p^n$.*

Pentru orice morfism liniar se poate construi matricea sa în raport cu baze din domeniu, respectiv codomeniu. Fie $A_{n,k} = \varphi(\mathbb{Z}_p^k)$ un (n,k) cod linar şi $G^t \in M_{n,k}(\mathbb{Z}_p)$ matricea morfismului liniar φ în raport cu bazele canonice din $\mathbf{Z}_p^k$, respectiv $\mathbb{Z}_p^n$. Matricea G, adică transpusa matricei este exact *matricea generatoare a codului liniar*. A se revedea Observaţia 3.3.3 şi Exemplul 3.3.5 din Unitatea de învăţare 3 Modulul II.

Exemplul 9.2.1. *a) Fie morfismul liniar $\varphi : \boldsymbol{Z}_2^2 \to \boldsymbol{Z}_2^5$ definit prin*

$$\varphi(x_1,x_2) = (x_1,x_2,0,x_1,x_1+x_2), \quad (\forall)(x_1,x_2) \in \boldsymbol{Z}_2^2.$$

Scrieţi matricea generatoare şi codul definit de φ.

Matricea morfismului liniar φ în raport cu bazele canonice este $G^t = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Avem $\boldsymbol{Z}_2^2 = \{00,01,10,11\}$, $A_{5,2} = \varphi(\boldsymbol{Z}_2^2) = \{GX, \quad x \in \boldsymbol{Z}_2^2\}$, unde X este coloana componentelor lui x. Matricea generatoare a codului este

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Rezultă codul $A_{5,2} = \{00000, 01001, 10011, 11010\}$, dat de codificarea

$$\varphi(00) = 00000, \quad \varphi(01) = 01001, \quad \varphi(10) = 10011, \quad \varphi(11) = 11010.$$

b)Fie $\varphi : \boldsymbol{Z}_3^3 \to \boldsymbol{Z}_3^6$ un $(6,3)$-cod liniar cu matricea generatoare

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Această matrice este matricea lui φ în raport cu bazele canonice din domeniul de definiţie şi din codomeniu. Matricea codificării în raport cu baza $\{100, 020, 211\}$ din domeniul de definiţie şi baza canonică din codomeniu este

$$G' = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Codul generat de cele două matrice este acelaşi (evident), dar codificarea diferă. De exemplu cu matricea G mesajul 010 *se codifică în* 002200*, pe când pin a doua matrice se codifică în* 001100*. Această a doua codificare este mai convenabilă, permite o decodificare mai facilă, deoarece fiecare simbol se repetă. Un astfel de cod se numeşte cod cu repetiţie.*

Codurile liniare au la bază ideea de a "lungi" mesajul de la k simboluri la n, astfel încât cele $n-k$ simboluri de pe noile poziţii, numite chiar poziţii de control, să asigure redundanţa necesară refacerii mesajului de informaţie iniţial, dacă apar eventuale perturbaţii pe canalul de transmitere.

Cea mai convenabilă codificare constă în scrierea mesajului de informaţie şi suplimentarea lui cu $n-k$ simboluri de control, adică matricea generatoare a codului să fie de forma $G = \begin{pmatrix} I_k & A \end{pmatrix}$, cu A o matrice de tip $(k, n-k)$.

Definiţia 9.2.2. *Un cod $\varphi(\boldsymbol{Z}_p^k) \subset \boldsymbol{Z}_p^n$ se numeşte* ***sistematic*** *dacă lasă neschimbate în codificarea unui semnal poziţiile de informaţie ale semnalului, adică*

$$\varphi(x) = (x, a(x)), \quad (\forall)x \in \boldsymbol{Z}_p^k, \quad a : \boldsymbol{Z}_p^k \to \boldsymbol{Z}_p^{n-k}.$$

Din liniaritatea aplicaţiei φ rezultă

Propoziţia 9.2.2. *Dacă codul $\varphi(\boldsymbol{Z}_p^k) \subset \boldsymbol{Z}_p^n$ este sistematic, atunci aplicaţia a din definiţia de mai sus este morfism liniar.*

Un cod sistematic realizează acea codificare convenabilă, matricea unui astfel de cod în raport cu bazele canonice având pe coloane $\varphi(e_i) = (e_i, a(e_i))$, $(\forall)i = \overline{1,k}$. Obţinem matricea generatoare a codului $G = \begin{pmatrix} I_k & A \end{pmatrix}$, cu $A \in M_{k,n-k}(\mathbf{Z}_p)$ transpusa matricei morfismului liniar a.

Revenind la coduri liniare oarecare, spunem că două (n,k)-coduri liniare A, A' sunt echivalente dacă există o permutare $\sigma \in S_n$ astfel încât

$$a_1 a_2 ... a_n \in A \Leftrightarrow a_{\sigma(1)} a_{\sigma(2)} ... a_{\sigma(n)} \in A'.$$

Exemplul 9.2.2. *În exemplul anterior, la punctul b), matricea G' generează un cod A' echivalent cu codul A" generat de matricea G" $= \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$, obţinută din G' prin inversarea liniilor 2,4, respectiv 3,6 între ele. Rezultă că există permutarea $\sigma = (24)(36) \in S_6$ astfel încât $(\forall)a_1 a_2 ... a_6 \in A'$, $a_{\sigma(1)} ... a_{\sigma(6)} \in A$". În plus, G"$'$ generează un cod sistematic.*

Se poate demonstra că

Propoziţia 9.2.3. *Orice cod liniar este echivalent cu un cod liniar sistematic.*

9.3 Matrice de control. Sindromul unui vector.

Fie $A_{n,k}$ un cod liniar generat de matricea $G \in M_{k,n}(\mathbf{Z}_p)$. Cuvintele cod sunt elementele mulţimii cod $G^t\mathbf{Z}_p^k$, adică un cuvânt cod $y \in A_{n,k}$ corespunde prin φ unui vector $x \in \mathbf{Z}_p^k$ şi $Y = G^tX$, unde X, Y sunt coloanele componentelor vectorilor x, y. Dacă $\{e_1, ..., e_k\}$ este baza din $\mathbf{Z}_p^k$, atunci $\varphi(e_1), ...\varphi(e_n)$ este bază în $A_{n,k}$. Din definiţia matricei G rezultă că vectorii bazei din $A_{n,k}$ sunt chiar liniile matricei G.

În spaţiul vectorial $\mathbf{Z}_p^n$ dotat cu pseudoprodusul scalar canonic, fie $A^\perp$ subspaţiul ortogonal subspaţiului $A_{n,k}$. Acest subspaţiu este de dimensiune $n-k$ (vezi Unitatea de învăţare 3, Modulul II, ortogonalitate) şi conţine toţi vectorii ortogonali pe $A_{n,k}$, deci pentru care produsul scalar cu elementele bazei este zero. Cum vectorii care formează baza în $A_{n,k}$ sunt liniile matricei generatoare, rezultă că A' este spaţiul soluţiilor sistemului $G \cdot U = 0$, unde U este coloana componentelor unui vector $u \in \mathbf{Z}_p^n$, arbitrar. Fie $\{f_1, f_2, ..., f_{n-k}\} \subset \mathbf{Z}_p^n$ baza în A'. Matricea $H \in M_{n-k,n}(\mathbf{Z}_p$ care are pe coloane componentele vectorilor $f_1, ..., f_{n-k}$ verifică $G \cdot H^t = 0$. Evident, această matrice generează A', avem $A' = H^t \cdot \mathbf{Z}_p^{n-k}$.

Definiţia 9.3.1. *Se numeşte* ***matrice de control*** *a unui cod liniar matricea H cu proprietatea că generează subspaţiul ortogonal codului dat.*

În cazul codurilor liniare sistematice matricea de control se determină foarte uşor:

Propoziţia 9.3.1. *Dacă $A_{n,k}$ este un cod liniar sistematic cu matricea generatoare $G = \begin{pmatrix} I_k & A \end{pmatrix}$, cu $A \in M_{k,n-k}(\boldsymbol{Z}_p$, atunci matricea de control este $H = \begin{pmatrix} -A^t & I_{n-k} \end{pmatrix}$.*

Din definiţia matricei de control rezultă că pentru orice cuvânt cod $y \in A_{n,k}$ avem $H \cdot Y = 0_{k,1}$.

Mai mult, sistemul $H \cdot Y = 0$ arată regula pe care o verifică componentele unui cuvânt cod şi permite astfel decodificarea. Acest sistem se numeşte *sistemul de verificare a parităţii.*

Definiţia 9.3.2. *Fie $y \in \boldsymbol{Z}_p^n$, arbitrar. Vectorul $z \in \boldsymbol{Z}_p^{n-k}$ cu coloana componentelor $Z = H \cdot Y$ se numeşte* ***sindromul*** *vectorului y.*

Din cele de mai sus, avem că dacă $z = 0$, atunci y este cuvânt cod, deci transmisia este corectă sau eroarea, dacă există, este nedetectabilă.

Dacă însă $z \neq 0$, atunci y nu este cuvânt cod, deci avem o eroare detectabilă.

Exemplul 9.3.1. *Fie* $(5,3)$*-codul binar liniar sistematic dat prin matricea* $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$*. Verificaţi dacă* 11101 *este cuvânt cod.*

Codul este sistematic, matricea generatoate fiind de forma $G = \begin{pmatrix} I_3 & A \end{pmatrix}$*, cu* $A \in M_{3,2}(\boldsymbol{Z}_2,\ A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$*. Matricea de control este* $H = \begin{pmatrix} -A^t & I_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$*. Calculăm sindromul vectorului dat şi obţinem* 00*, deci este cuvânt cod. Sistemul de verificare a parităţii este*

$$\begin{cases} y_1 + y_2 + y_4 = 0 \\ y_3 + y_5 = 0 \end{cases}$$

Exprimând din acest sistem $y_4 = y_1 + y_2$*, respectiv* $y_5 = y_3$*, (calculul s-a făcut în* $\mathbb{Z}_2$*, deci* $-1 = 1$*), putem considera că mesajul se află pe poziţiile* $y_1y_1y_3$ *şi a fost prelungit cu două simboluri de control*$y_4 = y_1 + y_2$*,* $y_5 = y_3$*. Prin urmare orice cuvânt cod, cu această regulă de codificare, are pe primele trei poziţii informaţia, adică mesajul sursă. Cuvântul cod* 11101 *se decodifică deci în* 111*.*

O altă opţiune de alegere a necunoscutelor principale din sistemul de verificare a parităţii duce la o altă regulă de codificare/decodificare, regulă care este cunoscută celor doi interlocutori. Astfel, dacă alegem necunoscutele principale y_1*,* y_5*, din sistemul de verificare a parităţii avem* $y_1 = y_2 + y_4$*,* $y_5 = y_3$*, deci mesajul iniţial se aflua pe poziţiile 2,3,4 ş* y_1*,* y_5 *sunt simbolurile de control. În acest caz, mesajul* 11101 *se decodifică* 110*.*

9.4 Tabela standard. Tabela de sindroame. Corectarea erorilor.

Fie $x \in \mathbf{Z}_p^n$. Numărul $w(x)$ de componente nenule din x se numeşte *ponderea* lui x. Evident, $0 \leq w(x) \leq n$.

Pentru $x, y \in \mathbf{Z}_p^n$, numim *distanţa Hamming* dintre x şi y ponderea vectorului $x - y$:

$$d(x, y) = w(x - y).$$

Definiţia 9.4.1. *Se numeşte* ***distanţă Hamming*** *a codului liniar* $A_{n,k} \subset \boldsymbol{Z}_p^n$ *cea mai mică distanţă dintre elementele codului, adică*

$$d = min_{x,y \in A_{n,k}, x \neq y} d(x, y).$$

Cum $d(x, y)$ este ponderea unui vector din $A_{n,k}$, avem de fapt distanţa Hamming a codului $d = min_{x \in A_{n,k}} w(x)$.

Presupunem că la transmiterea unui cuvânt cod x s-a recepţionat un mesaj y care este sau nu este cuvânt cod, după cum sindromul său $H^t y$ este sau nu vectorul nul. Dacă y nu este cuvântul cod transmis, înseamnă că există o eroare $e \in \mathbf{Z}_p^n$ care a perturbat transmisia.

Pentru fiecare vector $e \in \mathbf{Z}_p^n$, mulţimea

$$V_e = \{e + v, \quad v \in A_{n,k}\}$$

conţine toate mesajele care se pot recepţiona dacă a acţionat eroarea e. Remarcăm faptul că $A_{n,k} = V_0$. Pentru orice vector $x \in V_e$, mulţimea V_x conţine vectorii de forma $v + x$, cu $v \in A_{n,k}$. Dar x este de forma $e + u$, cu $u \in A_{n,k}$, iar codul $A_{n,k}$ fiind un subspaţiu vectorial, $u + v \in A_{n,k}$, deci vectorii din V_x sunt aceeaşi din V_e, adică

Propoziţia 9.4.1. *Pentru orice* $x \in V_e$, $V_x = V_e$.

Dacă vrem să depistăm o anumită eroare care modifică cuvintele din $A_{n,k}$ în cuvintele mulţimii V_e, atunci sunt mai uşor de depistat cuvintele de pondere minimă din V_e. Alegem din fiecare V_e un reprezentant, cuvânt cu pondere minimă, fie el x. Avem de mai sus $V_e = V_x$.

Se întocmeşte apoi tabela standard astfel:

-pe prima linie scriem cuvintele cod, începând cu 0;

-pe prima coloană scriem reprezentanţii aleşi, cuvintele de pondere minimă din $\mathbf{Z}_p^n$;

-pe linia i, corespunzătoare erorii e_i, pe coloana cuvântului cod x_j scriem $x_j + e_i$.

Obţinem o tablă cu p^n elemente, care reprezintă un dicţionar de decodare. Orice cuvânt din $\mathbf{Z}_p^n$ recepţionat se corectează prin cuvântul-cod situat în capul coloanei în care se află.

Exemplul 9.4.1. *Fie codul liniar* $\varphi : \boldsymbol{Z}_2^2 \to \boldsymbol{Z}_2^4$ *cu matricea generatoare* $G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$. *Codul este* $A_{4,2} = \{0000, 0111, 1001, 1110\}$. *Se aleg reprezen-*

tanţii cuvintele de pondere minimă, deci

$$0000, 0001, 0010, 0100, 1000.$$

Scriem mulţimile V_e pentru fiecare reprezentant e şi găsim $1000 \in V_{0001}$*, deci elimin acest reprezentant. Tabela standard este*

0000	0111	1001	1110
0001	0110	1000	1111
0010	0101	1011	1100
0100	0011	1101	1010

Dacă recepţionez 1101*, îl corectăm prin* 1001*.*

Problema apare când într-un V_e există mai multe cuvinte de pondere minimă. Corectarea depinde de alegerea reprezentantului. De exemplu, în tabela anterioară am ales reprezentantul 0001, dar puteam alege reprezentantul 1000. Pentru alegerea făcută, 1111 se corectează prin 1110. Dacă însă alegeam pentru mulţimea V_{0001} reprezentantul 1000, cuvântul 1111 recepţionat s-ar fi corectat prin 0111.

Nu putem şti care era mesajul corect. Tot ce se poate face este să alegem erorile cele mai probabile ca reprezentanţi.

Pentru numere p, n mari, tabela standard este greu de întocmit fiind foarte mare (are p^n elemente). Are loc

Propoziţia 9.4.2. *Oricare ar fi $x \in V_e$, x şi e au acelaşi sindrom, adică $H \cdot x = H \cdot e$.*

De aceea vom folosi sindromul unui vector recepţionat, după cum urmează. În loc de tabela standard întocmim un tabel cu sindromul fiecărui reprezentant al erorilor alese ca reprezentanţi. Pentru un mesaj y recepţionat calculez sindromul şi din tabela cu sindromurile reprezentanţilor identificăm eroarea e care a perturbat mesajul, apoi corectăm, obţinând mesajul corect $y - e$.

Exemplul 9.4.2. *Pentru exemplul anterior, avem tabloul cu sindromul fiecărui reprezentant:*

0000	00
0001	01
0010	10
0100	11

Faţă de tabela standard, datele stocate s-au redus la jumătate. Pentru mesajul recepţionat 1101*, calculez sindromul* 11*, deci mesajul a fost perturbat de eroarea* 0100*. Mesajul corect era* $1101 - 0100 = 1001$*.*

Încheiem paragraful cu un exerciţiu rezolvat, care să cuprindă toate aspectele discutate:

Exemplul 9.4.3. *Fie codul liniar binar* $C(5,3)$ *dat prin matricea generatoare*

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Determinaţi matricea de control şi sistemul de verificare a parităţii. Scrieţi codul. Întocmiţi tabela standard şi tabela de sindroame. Corectaţi şi decodificaţi cuvântul recepţionat $y = 11111$*.*

Matricea de control este matricea generatoare a codului ortogonal pe codul dat, fiind soluţie a sistemului $G \cdot Y = 0$*:*

$$\begin{cases} y_1 + y_3 + y_4 + y_5 = 0 \\ y_2 + y_3 + y_5 = 0 \\ y_3 + y_4 = 0 \end{cases}$$

Alegem necunoscutele secundare $y_4 = \alpha$ *şi* $y_5 = \beta$*. Mulţimea soluţiilor este*

$$\{(\beta, \alpha + \beta, \alpha, \alpha, \beta) | \alpha, \beta \in \mathbb{Z}_2\},$$

de unde matricea de control este

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

O altă metodă de a găsi matricea de control constă în rezolvarea sistemului $G \cdot Y = 0$ *prin metoda eliminării, cu obţinerea formei echivalente* $G' = \begin{pmatrix} I_3 & A \end{pmatrix}$*:*

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \overset{L_3 + L_1}{\Leftrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \overset{L_3 + L_2}{\Leftrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \Rightarrow H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Cuvântul recepţionat $y = 11111$ *are sindromul* 11*, deci nu e cuvât cod, el trebuie corectat.*

Sistemul de verificare a parităţii este $H \cdot X = 0$*, deci*

$$\begin{cases} x_2 + x_3 + x_4 = 0 \\ x_1 + x_2 + x_5 = 0 \end{cases}$$

Alegând necunoscutele secundare $x_1 = \alpha$*,* $x_2 = \beta$*,* $x_3 = \gamma$*, cuvintele cod sunt de forma* $(\alpha, \beta, \gamma, \beta+\gamma, \alpha+\beta)$*. Deci mesajul sursă este pe primele trei poziţii, iar* x_4 *şi* x_5 *sunt poziţii de control. Aceasta o considerăm regula de codificare/decodificare.*

Pentru a întocmi tabela standard avem nevoie de elementele codului. Acesta este subspaţiul vectorial generat de vectorii $a = 10111$*,* $b = 01101$*,* $c = 00110$*, liniile matricei generatoare* G*. Deci codul este*

$$C_{(5,3)} = \{\alpha \cdot a + \beta \cdot b + \gamma \cdot c | \alpha, \beta, \gamma \in \mathbb{Z}2\}$$

$$C_{(5,3)} = \{0, a, b, c, a+b, a+c, b+c, a+b+c\}$$

$$C_{(5,3)} = \{00000, 10111, 01101, 00110, 11010, 10001, 01011, 11100\}.$$

Tabela standard este

00000	00000	10111	01101	00110	11010	10001	01011	11100
00001	00001	10110	01100	00111	11011	10000	01010	11101
00010	00010	10101	01111	00100	11000	10011	01001	11110
01000	01000	11111	00101	01110	10010	11001	00011	10100

În sânga liniei verticale avem erorile probabile, iar în dreapta verticalei avem tabela standard, adică toate elementele din $\mathbb{Z}_2^5$*, organizate pe coloane al căror cap de coloană sunt elementele codului.*

Recepţionăm cuvântul $y = 11111$*, pe care îl găsim în tabela standard pe coloana cuvântului-cod* 10111*, ultima linie. Deci* 11111 *se corectează în* 10111 *şi regula de codificare dată de sistemul de verificare a parităţii spune că mesajul sursă este* 101*.*

Tabela de sindroame conţine erorile probabile, de pondere minimă, care dau toate sindroamele posibile: 00*,* 01*,* 10*,* 11*. Ştiind că sindromul unui vector este* $H \cdot y$ *şi că erorile simple au doar un element nenul, rezultatul* $H \cdot e$*, cu* e *eroare simplă este o coloană a lui* H*. Privim deci coloanele lui* H *şi alegem erorile probabile astfel încât să obţinem sindroamele dorite. Ultima coloană a lui* H *este* 01*, deci sindromul acesta corespunde erorii* 00001*. Acelaşi sindrom l-am obţine*

şi considerând eroarea 10000*, fiind şi prima coloană a lui* H*. Se alege cea mai probabilă eroare dintre cele două şi absolut necesar, aceeaşi eroare să fie aleasă şi în tabela standard. Aici, alegem* 00001*. Sindromul* 10 *se găseşte pe coloanele 3 şi 4. Alegem eroarea care e şi în tabela standard,* 00010*. Sindromul* 11 *este pe coloana 2, deci el corespunde erorii* 01000*.*

Tabela de sindroame este:

00000	00
00001	01
00010	10
01000	11

Sindromul cuvântului recepţionat $y = 11111$ *este* 11*, deci asupra lui a acţionat eroarea cu acelaşi sindrom, pe care o citim din tabela de sindroame, apo corectăm:* $y_{corect} = 11111 + 01000 = 10111$*. Decodificăm folosind regula de la sistemul de verificare a parităţii şi găsim mesajul sursă* 101*.*

9.5 Coduri Hamming

Un cod *Hamming* de ordin n este un cod liniar binar

$$\varphi : \mathbf{Z}_2^{2^n-n-1} \to \mathbf{Z}_2^{2^n-1},$$

în care cerem ca matricea de control să ofere informaţii despre eroarea semnalată. Acest lucru revine la a cere ca linia i din H să fie scrierea în baza 2 a numărului i.

Exemplul 9.5.1. *Codul Hamming de ordinul* $n = 3$ *este* $\varphi : \boldsymbol{Z}_2^4 \to \boldsymbol{Z}_2^7$*, cu matricea de control*

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Pentru a găsi matricea generatoare putem rezolva sistemulde verificare a parităţii $HX = 0$ *sau putem aduce matricea* H *de forma* $H = \begin{pmatrix} -A^t & I_k \end{pmatrix}$*, ceea ce revine la aranjarea liniilor lui* H *în ordinea* $3, 5, 6, 7, 4, 2, 1$*. Găsim* $A^t = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$

şi $G' = \begin{pmatrix} I_4 & A \end{pmatrix}$. *Reaşezând acum liniile în ordinea iniţială obţinem* $G^t = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$. *Codificarea mesajului sursă* 1101 *este cuvântul-cod* 1010101.

Avantajul acestui cod este că:

Propoziţia 9.5.1. *Dacă folosim codul Hamming, un cuvânt recepţionat în care o singură poziţie este eronată (mai spunem că avem eroare simplă), atunci eroarea este detectată, sindromul mesajului fiind scrierea în baza 2 a poziţiei eronate.*

Într-adevăr, fie $x \in \mathbf{Z}_2^{2^n-n-1}$ un cuvânt sursă şi $y = \varphi(x) \in \mathbf{Z}_2^{2^n-1}$ codificarea lui. Presupunem că s-a recepţionat $\widetilde{y}$, care diferă de y doar pe poziţia i, adică avem eroare simplă. Atunci $\widetilde{y} = y + e_i$, e_i vectorul care are singura poziţie nenulă (deci=1) i. Sindromul vectorului recepţionat este $H^t\widetilde{y} = H^(y + e_i) = H_i^e$, care este exact linia i din matricea H, adică scierea în baza 2 a lui i.

În exemplul anterior, dacă recepţionăm mesajul 1110101, calculăm sindromul său, 010. Nefiind vectorul nul, rezultă că nu este un cuvânt cod, deci a detectat o eroare. Sindromul arată că poziţia eronată este a doua. Corectăm eroarea şi obţinem 1010101.

Aşadar, codurile liniare binare sunt subspaţii vectoriale în $\mathbb{Z}_2^n$. Instrumente utile în studiul acestor coduri sunt date de baza codului şi matricea generatoare a sa, dar şi de matricea generatoare a codului ortogonal, matricea de control a codului. Marele avantaj al codurilor liniare este acela că sunt coduri detectoare şi corectoare de erori. Decodificarea se realizează stabilind o regulă din sistemul de verificare a parităţii, regulă cunoscută de cel care codifică şi trimite mesajul, dar şi de către cel care îl recepţionează.

9.6 Exerciţii propuse

1. Fie codul liniar binar $C(5, 3)$ dat prin matricea generatoare

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Determinaţi matricea de control şi sistemul de verificare a parităţii. Scrieţi codul. Întocmiţi tabela standard şi tabela de sindroame. Corectaţi şi decodificaţi cuvântul recepţionat $y = 11101$.

2. Se dă matricea
$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix},$$
matricea de control a unui cod liniar binar $(5, 3)$. Determinaţi elementele codului, matricea generatoare, codificaţi 111, apoi corectaţi cu tabela de sindroame cuvân tul recepţionat $y = 10111$ şi decodificaţi.

3. Fie codul liniar binar $C(6, 3)$ dat prin matricea generatoare
$$G = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$
Determinaţi matricea de control şi sistemul de verificare a parităţii. Scrieţi codul. Calculaţi sindromul vectorului $y = 111001$.

Indicaţii de rezolvare a temei de control:
1) Se studiază Exemplul 1.4.3.
2) Folosim Exemplul 1.4.3. A se vedea şi Exemplul 1.5.1 pentru modul de determinare a matricei generatoare când se cunoaşte matricea de control.
3) Similar cu Exemplul 1.3.1. Matricea de control se determină din condiţia $G \cdot Y = 0$.

Bibliografie

[1] I. D. Ion, N. Radu, *Algebra*, Ed. Didactică şi Pedagogică, Bucureşti, 1975.

[2] I. D. Ion, N. Radu, C. Niţă, D. Popescu *Probleme de Algebră*, Ed. Didactică şi Pedagogică, Bucureşti, 1981.

[3] A. Horváth, *Introducere în algebra computaţională-aplicaţii în geometrie, sisteme de ecuaţii, coduri*, Ed. Didactică şi Pedagogică, 2010.

[4] A. Horváth, *Introducere în algebra computaţională-aplicaţii în grupur, ecuaţii algebrice, topologie*, Ed. Didactică şi Pedagogică, 2011.

[5] A. Horváth, *Introducere în algebra computaţională-aplicaţii în teoria numerelor, criptografie, singularităţi*, Ed. Didactică şi Pedagogică, 2012.

[6] C. Năstăsescu, C. Niţă, C. Vraciu, *Bazele algebrei*, vol.1, Ed. Academiei RSR, 1986.

[7] L. Panaitopol, I.C. Drăghicescu, *Polinoame şi ecuaţii algebrice*, Ed. Albatros, Bucureşti, 1980.

[8] I. Purdea, C. Pelea, *Probleme de Algebră*, Ed. Eikon, Cluj-Napoca, 2008.

[9] I.Tofan, A.C.Volf, *Algebră: Inele. Module. Teorie Galois*, Ed. MatrixRom, Bucureşti, 2001.

[10] F. L. Ţiplea, *Fundamentele algebrice ale informaticii*, Ed. Polirom, 2006.

[11] Z.Pawlak,*Rough Sets*, International Journal of Computer and Information Sciences, 11 (1982), 341 356.