TIBERIU DUMITRESCU

ALGEBRA 1

București, 2006

PREFAŢĂ

Lucrarea se adresează studenţilor din anul I de la facultăţile de matematică şi informatică din universităţi. În cuprinsul ei sunt prezentate rezultate de bază referitoare la mulţimi, funcţii, relaţii de echivalenţă, operaţii algebrice, monoizi, grupuri, inele, corpuri, inele de polinoame în una sau mai multe nedeterminate, rădăcini ale polinoamelor, aritmetica lui $\mathbf{Z}$ *şi* $K[X]$*, polinoame simetrice, determinanţi, spaţii vectoriale, sisteme de ecuaţii liniare, şi teoria formei canonice Jordan. Urmând exemplul cărţii [6] a lui Irving Kaplansky, materialul este prezentat ca un şir aproape neîntrerupt de teoreme. Numerotarea teoremelor e făcută în continuare fără a ţine seama de trecerea dintr-un capitol în următorul. Definiţiile şi rezultatele sunt frecvent însoţite de exemple, aplicaţii sau comentarii. Fiecare capitol se termină cu o listă de exerciţii de dificultate variabilă. Soluţiile complete ale acestor exerciţii se găsesc la sfârşitul lucrării. Tot la sfârşit se află un index care facilitează găsirea în text a noţiunilor sau teoremelor importante.*

Autorul

Cuprins

Capitolul 1

Mulţimi şi funcţii

Acest capitol are caracter introductiv. Se trec în revistă conceptele de mulţime, apartenenţă, incluziune, operaţii cu mulţimi, mulţimea părţilor, produs cartezian, funcţie, compunere, injectivitate, surjectivitate, echipotenţă, numărabilitate, familie de mulţimi, relaţie de echivalenţă, mulţime factor.

1.1 Mulţimi

Prin *mulţime* înţelegem o colecţie de obiecte numite *elementele mulţimii*. Dacă x este un element al mulţimii A, atunci spunem că x *aparţine* lui A şi scriem $x \in A$; în caz contrar, spunem că x *nu aparţine* lui A şi scriem $x \notin A$. De exemplu, $1 \in \{1, 2, 3\}$ şi $4 \notin \{1, 2, 3\}$, unde $\{1, 2, 3\}$ este mulţimea având elementele 1, 2 şi 3.

Spunem că două mulţimi A, B sunt *egale* dacă au aceleaşi elemente, adică $A = B \Leftrightarrow (x \in A \Leftrightarrow x \in B)$. Cel mai simplu mod de a descrie o mulţime este specificând elementele sale. De exemplu, $\{1, 2\}$ este mulţimea cu elementele 1 şi 2. Ordinea elementelor şi repetiţiile sunt irelevante. De exemplu, $\{1, 2\} = \{2, 1\} = \{1, 1, 1, 2\}$. O mulţime se poate descrie şi prin precizarea unei proprietăţi caracteristice a elementelor sale. De exemplu, $\{1, 2\} = \{x \in \mathbf{R} |\ x^2 - 3x + 2 = 0\}$.

Fie A, B două mulţimi. Spunem că A este o *submulţime* a lui B sau că A este *inclusă* în B, dacă orice element al lui A este şi element al lui B. Notăm aceasta prin $A \subseteq B$ sau $B \supseteq A$. Dacă, în plus, $A \neq B$, spunem că A este o *submulţime proprie* a lui B sau că A este *strict inclusă* în B şi notăm $A \subset B$ sau $B \supset A$. Rezultă că $A = B \ \Leftrightarrow\ A \subseteq B$ şi $B \subseteq A$.

Se vede imediat că egalitatea şi incluziunea de mulţimi sunt tranzitive, adică, dacă A, B, C sunt mulţimi, atunci
(a) $A \subseteq B$ şi $B \subseteq C$ implică $A \subseteq C$,
(b) $A = B$ şi $B = C$ implică $A = C$.

Avem următoarele exemple importante de mulţimi. Mulţimea numerelor naturale $\mathbf{N} = \{0, 1, 2, ...\}$, mulţimea numerelor întregi $\mathbf{Z} = \{..., -2, -1, 0, 1, 2, ...\}$, mulţimea numerelor raţionale $\mathbf{Q}$, mulţimea numerelor reale $\mathbf{R}$ şi mulţimea numerelor complexe $\mathbf{C}$. Au loc incluziunile

$$\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}.$$

$\mathbf{N}$ se poate introduce prin axiomele lui Peano, iar $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ şi $\mathbf{C}$ se pot obţine prin anumite construcţii pornind de la $\mathbf{N}$ (vezi exerciţiile 24, 25 şi 26). *Mulţimea vidă*, $\emptyset$, este mulţimea care nu are nici un element. Putem scrie

$$\emptyset = \{x|\ x \neq x\}.$$

Mulţimea vidă este submulţime a oricărei mulţimi. Fie A o mulţime. Notăm cu $\mathcal{P}(A)$ şi numim *mulţimea părţilor* lui A mulţimea ale cărei elemente sunt submulţimile lui A, adică

$$\mathcal{P}(A) = \{B|\ B \subseteq A\}.$$

De exemplu, $\mathcal{P}(\emptyset) = \{\emptyset\}$ şi $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$. Fie A, B două mulţimi. Se definesc următoarele operaţii:

$$A \cup B = \{x|\ x \in A \text{ sau } x \in B\} \text{ (reuniunea lui } A \text{ cu } B)$$

$$A \cap B = \{x|\ x \in A \text{ şi } x \in B\} \text{ (intersecţia lui } A \text{ cu } B)$$

$$A \setminus B = \{x \in A|\ x \notin B\} \text{ (diferenţa dintre } A \text{ şi } B).$$

De exemplu, $\{1, 2\} \cup \{1, 3\} = \{1, 2, 3\}$, $\{1, 2\} \cap \{1, 3\} = \{1\}$ şi $\{1, 2\} \setminus \{1, 3\} = \{2\}$. Două mulţimi cu intersecţia vidă se zic *disjuncte*. De exemplu, $\{1, 2\}$ şi $\{3, 4\}$ sunt disjuncte. Cum se arată în teorema următoare, operaţiile de reuniune şi intersecţie sunt comutative, asociative şi fiecare dintre ele este distributivă faţă de cealaltă.

Teorema 1 *Fie A, B, C trei mulţimi. Atunci*
(a) $A \cap B \subseteq A \subseteq A \cup B$,
(b) $A \cup B = B \cup A$ *şi* $A \cap B = B \cap A$,
(c) $(A \cup B) \cup C = A \cup (B \cup C)$ *şi* $(A \cap B) \cap C = A \cap (B \cap C)$,
(d) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, *şi*
(e) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Demonstraţie. Lăsăm demonstraţia cititorului. Pentru exemplificare, probăm (e). Avem şirul de echivalenţe: $x \in A \cup (B \cap C) \Leftrightarrow x \in A$ sau $x \in B \cap C \Leftrightarrow x \in A$ sau ($x \in B$ şi $x \in C$) $\Leftrightarrow$ ($x \in A$ sau $x \in B$) şi ($x \in A$ sau $x \in C$) $\Leftrightarrow x \in (A \cup B) \cap (A \cup C)$. •

Dacă A este o submulţime a mulţimii X, atunci *complementara* lui A în X este $\mathcal{C}_X(A) = X \setminus A$. De exemplu, $\mathcal{C}_X(X) = \emptyset$ şi $\mathcal{C}_X(\emptyset) = X$. Cele două egalităţi următoare poartă numele de *formulele lui De Morgan.*

Teorema 2 *Fie X o mulţime şi $A, B \subseteq X$. Atunci*

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \text{ şi } \overline{A \cap B} = \overline{A} \cup \overline{B}$$

unde $\overline{Y} = \mathcal{C}_X(Y)$.

Demonstraţie. Avem: $x \in \overline{A \cup B} \Leftrightarrow x \in X$ şi $x \notin A \cup B \Leftrightarrow x \in X$ şi $x \notin A$ şi $x \notin B \Leftrightarrow x \in \overline{A}$ şi $x \in \overline{B} \Leftrightarrow x \in \overline{A} \cap \overline{B}$. Cea de-a doua egalitate se probează analog. •

Fie A, B două mulţimi şi $a \in A$, $b \in B$. *Perechea ordonată* (a, b) se defineşte prin

$$(a, b) := \{\{a\}, \{a, b\}\}.$$

Se vede uşor că două perechi (a, b) şi (a', b') sunt egale dacă şi numai dacă $a = a'$ şi $b = b'$. *Produsul cartezian* $A \times B$ al mulţimilor A şi B este mulţimea acestor perechi ordonate, adică

$$A \times B = \{(a, b) |\ a \in A, b \in B\}.$$

De exemplu, $\{1, 2\} \times \{3, 4\} = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$. Rezultă că

$$A \times B = \emptyset \Leftrightarrow A = \emptyset \text{ sau } B = \emptyset.$$

1.2 Funcţii

Fie A şi B două mulţimi. O *funcţie* (sau *aplicaţie*) f de la A la B (notaţie $f : A \to B$) este o submulţime a produsului cartezian $A \times B$ cu proprietatea

$$\text{pentru orice } x \in A \text{ există şi este unic } b_x \in B \text{ cu } (x, b_x) \in f.$$

Deci f asociază fiecărui element $x \in A$ un unic element $b_x \in B$ pe care-l vom nota cu $f(x)$. Aşadar, pentru a defini o funcţie $f : A \to B$ trebuie să precizăm mulţimea A numită *domeniul de definiţie* al lui f, mulţimea B numită *codomeniul* sau *domeniul valorilor* lui f şi asocierea $a \mapsto f(a)$. Mulţimea $\{(a, f(a)) |\ a \in A\} = f$ se mai numeşte şi *graficul lui* f. Mulţimea tuturor funcţiilor $g : A \to B$ se notează cu B^A.

De exemplu, $f : \{1, 2\} \to \{1, 2, 3\}$, $f(n) = n + 1$ este o funcţie cu graficul $\{(1, 2), (2, 3)\}$. Pe de altă parte, $g : \{0, 1, 2\} \to \mathbf{R}$, $g(x) = y$ unde $y \in \mathbf{R}$ şi $x^2 + y^2 = 1$, nu este funcţie, deoarece $g(0) = \pm 1$, deci $g(0)$ nu este unic determinat, iar $g(2)$ nu există. Cu alte cuvinte, submulţimea $\{(0, 1), (0, -1), (1, 0)\}$ a lui $\{0, 1, 2\} \times \mathbf{R}$ nu satisface condiţia din definiţia funcţiei.

Prin definiţie, două funcţii $f : A \to B$ şi $g : C \to D$ sunt *egale* dacă $A = C$, $B = D$ şi $f(x) = g(x)$ pentru orice $x \in A$. Fie două funcţii $f : A \to B$ şi $g : B \to C$. *Compunerea* gf dintre g şi f este funcţia $gf : A \to C$ definită prin

$$(gf)(x) = g(f(x)) \text{ pentru } x \in A.$$

De exemplu, dacă $f, g : \mathbf{R} \to \mathbf{R}$, $f(x) = \sin(x)$, $g(x) = x^2$, atunci $(gf)(x) = \sin^2(x)$ iar $(fg)(x) = \sin(x^2)$, deci $fg \neq gf$. În cazul în care o funcţie σ este definită pe o mulţime finită $A = \{a_1, ..., a_n\}$, σ se poate reprezenta sub forma $\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_n) \end{pmatrix}$. De exemplu, funcţia $f : \{1, 2\} \to \{1, 2, 3\}$, $f(n) = n + 1$ se poate reprezenta $\begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$.

Teorema 3 *Fie funcţiile* $f : A \to B$, $g : B \to C$ *şi* $h : C \to D$. *Atunci* $h(gf) = (hg)f$ (i.e., compunerea funcţiilor este asociativă).

Demonstraţie. Dacă $x \in A$, atunci $(h(gf))(x) = h((gf)(x)) = h(g(f(x)))$ $= (hg)(f(x)) = ((hg)f)(x)$. $\bullet$

O funcţie $f : A \to B$ se numeşte *funcţie injectivă* sau mai simplu *injecţie*, dacă pentru orice $x, y \in A$ cu $x \neq y$ rezultă $f(x) \neq f(y)$ (echivalent dacă pentru orice $x, y \in A$ cu $f(x) = f(y)$ rezultă $x = y$). O funcţie $f : A \to B$ se numeşte *funcţie surjectivă* sau mai simplu *surjecţie*, dacă pentru orice $y \in B$ există $x \in A$ astfel încât $f(x) = y$. O funcţie se numeşte *funcţie bijectivă* sau mai simplu *bijecţie*, dacă este simultan injectivă şi surjectivă.

De exemplu, fie funcţiile $f, g, h, k : \mathbf{Z} \to \mathbf{Z}$ date prin: $f(m) = 2m$, $g(m) = [m/2]$, $h(m) = m + 1$ şi $k(m) = m^2$. Atunci f este injectivă şi nesurjectivă, g este surjectivă şi neinjectivă, h este bijectivă, iar k este neinjectivă şi nesurjectivă.

Dacă A este o submulţime a lui B, atunci injecţia $i : A \to B$, dată prin $i(x) = x$, se numeşte *funcţia (aplicaţia) de incluziune a lui* A *în* B. Bijecţia $\mathrm{I}_A : A \to A$, dată prin $I_A(x) = x$, se numeşte *funcţia (aplicaţia) identică* a mulţimii A. Se verifică imediat că pentru orice funcţie $f : A \to B$ avem $I_B f = f$ şi $f I_A = f$.

Dacă A, B sunt două mulţimi, atunci surjecţiile $p_A : A \times B \to A$ şi $p_B : A \times B \to B$, date prin $p_A(x, y) = x$ şi $p_B(x, y) = y$, se numesc *proiecţiile canonice* ale produsului cartezian $A \times B$ pe prima respectiv a doua componentă. O bijecţie $s : A \to A$ se mai numeşte *permutare* a mulţimii A. De exemplu, $\sigma = \begin{pmatrix} a & b & c & d \\ b & c & a & d \end{pmatrix}$ este o permutare a mulţimii $\{a, b, c, d\}$

Teorema 4 *Fie funcţiile* $f, f' : A \to B$ *şi* $g, g' : B \to C$. *Atunci au loc următoarele implicaţii*

(a) f, g *injecţii* $\Rightarrow gf$ *injecţie,*
(b) f, g *surjecţii* $\Rightarrow gf$ *surjecţie,*
(c) f, g *bijecţii* $\Rightarrow gf$ *bijecţie,*
(d) gf *injecţie* $\Rightarrow f$ *injecţie,*
(e) gf *surjecţie* $\Rightarrow g$ *surjecţie,*
(f) gf *bijecţie* $\Rightarrow f$ *injecţie şi* g *surjecţie,*
(g) $gf = gf'$ *şi* g *injecţie* $\Rightarrow f = f'$,
(h) $gf = g'f$ *şi* f *surjecţie* $\Rightarrow g = g'$.

Demonstraţie. (a). Fie $x, y \in A$ astfel încât $(gf)(x) = (gf)(y)$, adică $g(f(x)) = g(f(y))$. Cum g, f sunt injecţii, obţinem $f(x) = f(y)$ şi apoi $x = y$. (b). Fie $z \in C$. Cum g, f sunt surjecţii, există $y \in B$ cu $g(y) = z$ şi apoi există $x \in A$ cu $f(x) = y$. Obţinem $(gf)(x) = g(y) = z$.

(c) rezultă din (a) şi (b).

(d). Fie $x, y \in A$ cu $f(x) = f(y)$. Aplicând pe g obţinem $(gf)(x) = (gf)(y)$ şi cum gf este injecţie, rezultă $x = y$.

(e). Fie $z \in C$. Cum gf este surjecţie, există $x \in A$ cu $(gf)(x) = z$. Deci $y = f(x) \in B$ şi $g(y) = z$. (f) rezultă din (d) şi (e).

(g). Fie $x \in A$. Cum $gf = gf'$, rezultă $g(f(x)) = g(f'(x))$, deci $f(x) = f'(x)$ deoarece g este injectivă.

(h) Fie $y \in B$. Cum f este surjecţie, există $x \in A$ cu $f(x) = y$. Deoarece $gf = g'f$, rezultă $g(y) = (gf)(x) = (g'f)(x) = g'(y)$. •

Fie funcţiile $f, g : \mathbf{N} \to \mathbf{N}$ date prin $f(n) = n+1$ şi $g(n) = \max(n-1, 0)$. Atunci $gf = I_{\mathbf{N}}$ dar f nu este surjectivă iar g nu este injectivă.

Teorema 5 *Fie $f : A \to B$ o funcţie. Atunci f este bijectivă dacă şi numai dacă există o funcţie $g : B \to A$ astfel încât $gf = I_A$ şi $fg = I_B$. Dacă există, funcţia g este unică; g se numeşte* inversa lui f *şi se notează cu f^{-1}.*

Demonstraţie. Implicaţia $\Leftarrow$ rezultă din punctul (f) al Teoremei 4. $\Rightarrow$. Fie $y \in B$. Cum f este surjectivă, există $y' \in A$ astfel încât $f(y') = y$. Deoarece f este injectivă, y' este unic determinat de y (deoarece $f(y') = y = f(y'')$ implică $y' = y''$). Definim funcţia $g : B \to A$ prin $g(y) = y'$. Pentru orice $y \in B$, rezultă $(fg)(y) = f(y') = y$; deci $fg = I_B$. De asemenea, dacă $x \in A$, atunci $g(f(x)) = f(x)' = x$; deci $gf = I_A$. Unicitatea lui g rezultă din punctele (g) şi (h) ale teoremei 4. •

De exemplu, inversa funcţiei $f : \mathbf{N} \to \mathbf{N}^*$ dată prin $f(m) = m + 1$ este $f^{-1} : \mathbf{N}^* \to \mathbf{N}$ dată prin $f^{-1}(m) = m - 1$. De asemenea, inversa funcţiei $h : \mathbf{R} \to \mathbf{R}$, $h(x) = x^3 + 5x$, $x \in \mathbf{R}$, este funcţia $h^{-1}(y) = \sqrt[3]{y/2 + \sqrt{y^2/4 + 125/27}} + \sqrt[3]{y/2 - \sqrt{y^2/4 + 125/27}}$, $y \in \mathbf{R}$.

Fie $f : A \to B$ o funcţie. Dacă $X \subseteq A$, atunci submulţimea lui B, $f(X) = \{f(x) | \; x \in X\}$ se numeşte *imaginea (directă)* a lui X prin f. $f(A)$ se notează cu $\mathrm{Im}(f)$ şi se numeşte *imaginea* lui f. E clar că f este surjectivă dacă şi numai dacă $\mathrm{Im}(f) = B$. De asemenea, dacă $Y \subseteq B$, atunci submulţimea lui A, $f^{-1}(Y) = \{x \in A | \; f(x) \in Y\}$ se numeşte *pre-imaginea* sau *imaginea inversă* a lui Y prin f.

De exemplu, pentru funcţia $h : \mathbf{N} \to \mathbf{Z}$, dată prin $h(n) = (-1)^n$, avem $\mathrm{Im}(h) = \{1, -1\}$, $h(\{1, 3\}) = \{-1\}$, $h^{-1}(\{2\}) = \emptyset$ şi $h^{-1}(\{1\}) =$ mulţimea numerelor naturale pare.

Teorema 6 *Fie $f : A \to B$ o funcţie, $X, W \subseteq A$ şi $Y, Z \subseteq B$. Atunci*
(a) $X \subseteq W \Rightarrow f(X) \subseteq f(W)$,
(b) $Y \subseteq Z \Rightarrow f^{-1}(Y) \subseteq f^{-1}(Z)$,
(c) $f(X \cup W) = f(X) \cup f(W)$,
(d) $f(X \cap W) \subseteq f(X) \cap f(W)$ (cu egalitate dacă f este injectivă),
(e) $f^{-1}(Y \cup Z) = f^{-1}(Y) \cup f^{-1}(Z)$,
(f) $f^{-1}(Y \cap Z) = f^{-1}(Y) \cap f^{-1}(Z)$,
(g) $f^{-1}(f(X)) \supseteq X$ (cu egalitate dacă f este injectivă),
(h) $f(f^{-1}(Y)) \subseteq Y$ (cu egalitate dacă f este surjectivă).

Demonstraţie. (a) şi (b) sunt clare. (c). Incluziunea $\supseteq$ rezultă din (a). Fie $y \in f(X \cup W)$. Atunci există $x \in X \cup W$ astfel încât $f(x) = y$. Rezultă $x \in X$ sau $x \in W$, deci $y \in f(X)$ sau $y \in f(W)$.

(d). Prima parte e clară. Presupunem f injectivă şi fie $y \in f(X) \cap f(W)$. Există $x \in X$ şi $w \in W$ astfel încât $f(x) = f(w) = y$. Din injectivitatea lui f rezultă $x = w$, deci $y \in f(X \cap W)$.

(e). Avem şirul de echivalenţe: $x \in f^{-1}(Y \cup Z) \Leftrightarrow f(x) \in Y \cup Z \Leftrightarrow f(x) \in Y$ sau $f(x) \in Z \Leftrightarrow x \in f^{-1}(Y) \cup f^{-1}(Z)$.

(f). se probează asemănător cu (e).

(g). Dacă $x \in X$, atunci $f(x) \in f(X)$, deci $x \in f^{-1}(f(X))$. Reciproc, fie $w \in f^{-1}(f(X))$. Atunci $f(w) \in f(X)$, adică există $x \in X$ cu $f(x) = f(w)$, deci $w = x \in X$ dacă f este injectivă.

(h). Relaţia $f(f^{-1}(Y)) \subseteq Y$ este evidentă. Presupunem că f este surjectivă şi fie $y \in Y$. Atunci există $x \in A$ cu $f(x) = y$. Rezultă că $x \in f^{-1}(Y)$, deci $y \in f(f^{-1}(Y))$. •

Teorema 7 *Fie A o mulţime. Afirmaţiile următoare sunt echivalente:*
(a) *A este finită,*
(b) *orice injecţie $f : A \to A$ este bijecţie,*
(c) *orice surjecţie $f : A \to A$ este bijecţie.*

Demonstraţie. $(a) \Rightarrow (b)$ şi $(a) \Rightarrow (c)$. Fie $A = \{a_1, ..., a_n\}$. Dacă f este injectivă, atunci $f(a_1), ..., f(a_n)$ sunt elemente distincte din A, deci $\{f(a_1), ..., f(a_n)\} = A$, adică f este surjectivă.

Dacă f este surjectivă, atunci $\{f(a_1), ..., f(a_n)\} = A$ deci $f(a_1), ..., f(a_n)$ sunt distincte, adică f este injectivă.

$(b) \Rightarrow (a)$ şi $(c) \Rightarrow (a)$. Presupunem că A este infinită. Vom construi funcţiile $f, g : A \to A$, f injectivă nesurjectivă, g surjectivă neinjectivă. Fiind infinită, A posedă o submulţime infinită $B = \{a_1, a_2, ..., a_n, ...\}$. Definim funcţiile $f, g : A \to A$ prin

$$f(x) = \begin{cases} x & \text{dacă } \; x \in A \setminus B \\ a_{n+1} & \text{dacă } \; x = a_n \end{cases} \quad g(x) = \begin{cases} x & \text{dacă } \; x \in A \setminus B \cup \{a_1\} \\ a_{n-1} & \text{dacă } \; x = a_n, n \geq 2. \end{cases}$$

Deoarece $a_1 \notin \mathrm{Im}(f)$, $g(a_1) = g(a_2)$ şi $gf = I_A$, rezultă că f este injectivă dar nesurjectivă iar g este surjectivă dar neinjectivă. •

Proprietatea anterioară ne permite să definim mulţimile finite ca fiind mulţimile A cu proprietatea că orice injecţie (surjecţie) $f : A \to A$ este bijecţie.

Teorema 8 *Fie A, B mulţimi finite cu m respectiv n elemente. Atunci*
(a) *numărul submulţimilor lui B este 2^n*
(b) *numărul funcţiilor de la A la B este n^m*
(c) *numărul permutărilor lui B este $n!$*
(d) *dacă $m \leq n$, numărul injecţiilor de la A la B este $n!/(n-m)!$*
(e) *dacă $m \geq n$, numărul surjecţiilor de la A la B este*

$$n^m - C_n^1(n-1)^m + C_n^2(n-2)^m + \cdots + (-1)^{n-1}C_n^{n-1}.$$

Demonstraţie. (a). Fie $0 \leq k \leq n$. Submulţimile lui B având k elemente sunt în număr de C_n^k. Deci B are $C_n^0 + C_n^1 + \cdots + C_n^n = (1+1)^n = 2^n$ submulţimi. Pentru celelate afirmaţii, vezi exerciţiul 12. •

Spunem că două mulţimi A, B sunt *echipotente* sau că *au acelaşi cardinal* şi notăm $A \simeq B$ sau $|A| = |B|$, dacă există o bijecţie $f : A \to B$. E clar că două mulţimi finite sunt echipotente dacă şi numai dacă au acelaşi număr de elemente. Din acest motiv, pentru o mulţime finită cu n elemente vom scrie $|A| = n$.

Pentru cazul mulţimilor arbitrare, se poate proba uşor că relaţia de echipotenţă posedă proprietăţile reflexivitate($A \simeq A$), simetrie ($A \simeq B \Rightarrow B \simeq A$) şi tranzitivitate ($A \simeq B$ şi $B \simeq C \Rightarrow A \simeq C$). O mulţime echipotentă cu $\mathbf{N}$ se numeşte *mulţime numărabilă.* E clar că A este mulţime numărabilă dacă şi numai dacă elementele lui A se pot aşeza într-un şir infinit. Cum $\mathbf{Z} = \{0, \pm 1, \pm 2, ...\}$, $\mathbf{Z}$ este numărabilă. $\mathbf{N} \times \mathbf{N}$ este de asemeanea numărabilă, deoarece avem bijecţia

$$f : \mathbf{N} \times \mathbf{N} \to \mathbf{N}, \quad f(a,b) = 2^a(2b+1) - 1.$$

Într-adevăr, orice număr natural nenul se scrie în mod unic ca produsul dintre o putere a lui 2 şi un număr impar.

Teorema 9 (Cantor). *Mulţimea numerelor reale este nenumărabilă.*

Demonstraţie. Presupunem că $\mathbf{R}$ este numărabilă. Atunci intervalul $(0,1)$ este numărabil. Fie $\{a_1, ..., a_n, ...\}$ o înşiruire a numerelor din $(0,1)$ şi fie

$$a_n = \overline{0, a_{n1} a_{n2} \cdots a_{nk} \cdots}$$

reprezentarea zecimală a lui a_n. Pentru fiecare n, fie b_{nn} o cifră zecimală diferită de 0, 9 şi a_{nn}. Atunci numărul cu reprezentarea zecimală

$$\overline{0, b_{n1} b_{n2} \cdots b_{nn} \cdots}$$

aparţine lui $(0,1)$ dar nu se găseşte în şirul $\{a_1, ..., a_n, ...\}$, contradicţie. •

Fie A, B două mulţimi. Spunem că A *are cardinal mai mic decât* B şi notăm $|A| \leq |B|$, dacă există o injecţie $f : A \to B$. Dacă în plus, A, B nu sunt echipotente, notăm $|A| < |B|$. Au loc următoarele două rezultate remarcabile.

Teorema 10 (Cantor). *Pentru orice mulţime A, $|A| < |\mathcal{P}(A)|$.*

Demonstraţie. Injecţia $i : A \to \mathcal{P}(A)$, $i(x) = \{x\}$, ne arată că $|A| \leq |\mathcal{P}(A)|$. Presupunem că avem o bijecţie $f : A \to \mathcal{P}(A)$. Se consideră mulţimea $B = \{a \in A | \ a \notin f(a)\}$. Cum f este surjectivă, există $b \in A$ cu $f(b) = B$. Dacă $b \in B$, atunci $b \notin f(b) = B$, contradicţie; iar dacă $b \notin B$, atunci $b \in f(b) = B$, din nou contradicţie. •

Teorema 11 (Cantor-Schröder-Bernstein). *Fie A, B două mulţimi. Dacă $|A| \leq |B|$ şi $|B| \leq |A|$, atunci $|A| = |B|$.*

Demonstraţie. Vezi exerciţiul 9. •

1.3 Familii de mulţimi.

Fie M o mulţime nevidă. Un şir $(x_n)_{n \geq 1}$ de elemente ale lui M înseamnă, de fapt, o funcţie $f : \mathbf{N}^* \to M$, $f(n) = x_n$. Mai general, dacă I este o mulţime, *o* *familie de elemente* $(x_i)_{i\in I}$ *din* M *indexată după mulţimea* I înseamnă funcţia $f : I \to M$, $f(i) = x_i$. I se numeşte *mulţimea indicilor* iar x_i *elementul de indice* i al familiei. Familia se zice *nevidă* dacă I este nevidă. De exemplu, o matrice de tip $m \times n$ de numere reale este o familie indexată după mulţimea $\{1, ..., m\} \times \{1, ..., n\}$.

Fie $(A_i)_{i\in I}$ o familie nevidă de mulţimi (adică, fiecare A_i este mulţime). Operaţiile de reuniune/intersecţie se pot defini pentru familii astfel

$$\bigcup_{i\in I} A_i = \{x | \text{ există } i_x \in I \text{ cu } x \in A_{i_x}\}$$

$$\bigcap_{i\in I} A_i = \{x | \ x \in A_i \text{ pentru orice } i \in I\}.$$

De exemplu, $\cup_{i=1}^{n} A_i = A_1 \cup \cdots \cup A_n$, $\cup_{0<x<1}(0, x] = (0, 1)$ şi $\cap_{i=1}^{\infty}(0, 1/n) = \emptyset$. Proprietăţile reuniunii/intersecţiei din cazul a două mulţimi se extind uşor la cazul familiilor. De exemplu, o versiune generalizată a asociativităţii reuniunii este următoarea. Fie $((A_{i_k})_{i_k\in I_k})_{k\in K}$ o familie de familii mulţimi. Atunci

$$\bigcup_{k\in K} (\bigcup_{i_k\in I_k} A_{i_k}) = \bigcup_{j\in I} A_j \text{ unde } I = \bigcup_{k\in K} I_k.$$

O versiune generalizată a distributivităţii intersecţiei faţă de reuniune este următoarea. Fie $(A_i)_{i\in I}$ şi $(B_j)_{j\in J}$ familii de mulţimi. Atunci

$$(\bigcup_{i\in I} A_i) \cap (\bigcup_{j\in J} B_j) = \bigcup_{(i,j)\in I\times J} (A_i \cap B_j).$$

Într-adevăr, $x \in (\bigcup_{i\in I} A_i) \cap (\bigcup_{j\in J} B_j) \Leftrightarrow$ există $\alpha \in I$ şi $\beta \in J$ cu $x \in A_\alpha \cap B_\beta$ $\Leftrightarrow x \in \bigcup_{(i,j)\in I\times J}(A_i \cap B_j)$.

Formulele lui De Morgan se exprimă astfel. Fie X o mulţime şi fie $(A_i)_{i\in I}$ o familiei de submulţimi ale lui X. Atunci

$$\overline{\bigcup_{i\in I} A_i} = \bigcap_{i\in I} \overline{A_i}$$

$$\overline{\bigcap_{i\in I} A_i} = \bigcup_{i\in I} \overline{A_i}$$

unde $\overline{Y} = \mathcal{C}_X(Y)$. Într-adevăr, $x \in \overline{\bigcup_{i\in I} A_i} \Leftrightarrow x \in X$ şi $x \notin \bigcup_{i\in I} A_i \Leftrightarrow x \in X$ şi $x \notin A_i$ pentru orice $i \in I \Leftrightarrow x \in \bigcap_{i\in I} \overline{A_i}$.

Prin definiţie, *produsul cartezian* $\prod_{i\in I} A_i$ *al unei familii nevide de mulţimi* $(A_i)_{i\in I}$ este

$$\prod_{i\in I} A_i := \{(x_i)_{i\in I} |\ x_i \in A_i \text{ pentru orice } i \in I\}.$$

Dacă A, I sunt mulţimi nevide, atunci A^I este produsul cartezian al familiei $(A_i)_{i\in I}$ cu $A_i = A$ pentru orice $i \in I$. Deci A^I este mulţimea familiilor de elemente din A indexate după I, altfel spus, mulţimea funcţiilor $f : I \to A$. Dacă $I = \{1, ..., n\}$, A^I se notează simplu cu A^n. În teoria axiomatică a mulţimilor, se admite următoarea axiomă:

(Axioma alegerii.) *Produsul cartezian al unei familii nevide de mulţimi nevide* $(A_i)_{i\in I}$ *este nevid, adică există o funcţie*

$$f : I \to \bigcup_{i\in I} A_i \ \textit{cu}\ f(i) \in A_i \ \textit{pentru orice}\ i \in I.$$

1.4 Relaţii de echivalenţă

Fie A o mulţime nevidă. O *relaţie* " $\sim$ " pe mulţimea A este o submulţime a produsului cartezian $A \times A$. Dacă $(a, b) \in\sim$, vom spune că *a este în relaţia $\sim$ cu b* şi vom folosi notaţia (mai comodă) $a \sim b$. De exemplu, $\rho = \{(1, 2)\}$ este o relaţie pe mulţimea $\{1, 2\}$ şi $1\rho 2$. E clar că pe o mulţime cu n elemente sunt 2^{n^2} relaţii.

O relaţie $\sim$ pe mulţimea A se numeşte *relaţie de echivalenţă* dacă $\sim$ este simultan:

reflexivă: $a \sim a$ pentru orice $a \in A$,

simetrică: $a \sim b$ implică $b \sim a$, şi

tranzitivă: $a \sim b$ şi $b \sim c$ implică $a \sim c$.

Exemple de relaţii de echivalenţă: relaţia de egalitate pe o mulţime nevidă, relaţia de paralelism pe mulţimea dreptelor din plan, relaţiile de asemănare/congruenţă pe mulţimea triunghiurilor din plan. Relaţia de inegalitate $\leq$ pe $\mathbf{N}$ nu este relaţie de echivalenţă, nefiind simetrică. Dacă $f : A \to B$ este o funcţie, atunci relaţia $\sim_f$ pe A definită prin

$$x \sim_f y \ :\Leftrightarrow\ f(x) = f(y)$$

este o relaţie de echivalenţă fiind reflexivă: $f(a) = f(a)$ pentru orice $a \in A$, simetrică: $f(a) = f(b)$ implică $f(b) = f(a)$, şi tranzitivă: $f(a) = f(b)$ şi $f(b) = f(c)$ implică $f(a) = f(c)$.

Numim $\sim_f$ *relaţia de echivalenţă asociată lui* f. De exemplu, pentru funcţia $\alpha : \mathbf{R} \to \mathbf{C}$, $\alpha(x) = \cos(2\pi x) + i\,\sin(2\pi x)$, relaţia $x \sim_\alpha y$ înseamnă $x - y \in \mathbf{Z}$. Fie $\sim$ o relaţie de echivalenţă pe mulţimea A. Dacă $a \in A$, mulţimea

$$[a] := \{b \in A|\ b \sim a\}$$

se numeşte *clasa de echivalenţă* a elementului a. Mulţimea claselor de echivalenţă se numeşte *mulţimea factor a lui A modulo* $\sim$ şi se notează cu $A/\sim$. Deci $A/\sim = \{[a]|\ a \in A\}$. Surjecţia

$$p : A \to A/\sim, \quad p(a) = [a]$$

se numeşte *surjecţia canonică*. Se vede că $\sim_p = \sim$. Pentru relaţia de egalitate pe o mulţime nevidă B, clasele de echivalenţă sunt submulţimile lui B cu câte un singur element. O *partiţie* a unei mulţimi nevide A este o familie de submulţimi nevide disjuncte două câte două ale lui A a cărei reuniune este A. De exemplu, $(\{2n, 2n+1\})_{n\in\mathbf{Z}}$ este o partiţie a lui $\mathbf{Z}$ în timp ce $(\{n, n+1\})_{n\in\mathbf{Z}}$ şi $(\{3n, 3n+1\})_{n\in\mathbf{Z}}$ nu sunt partiţii.

Teorema 12 *Fie $\sim$ o relaţie de echivalenţă pe mulţimea A. Atunci*

(a) *$a \in [a]$ pentru orice $a \in A$.*

(b) *Două clase de echivalenţă $[a]$ şi $[b]$ sunt* $\begin{cases} \textit{egale} & \textit{dacă} \quad a \sim b \\ \textit{disjuncte} & \textit{dacă} \quad a \not\sim b. \end{cases}$

În particular, $[a] = [b]$ dacă şi numai dacă $a \sim b$.

(c) *Mulţimea claselor de echivalenţă este o partiţie a lui A.*

Demonstraţie. (a) rezultă din reflexivitate lui $\sim$. (b). Presupunem că există $x \in [a] \cap [b]$ şi fie $y \in [a]$. Cum $\sim$ este simetrică, rezultă că $y \sim a$, $a \sim x$ şi $x \sim b$. Din tranzitivitatea obţinem $y \sim b$, deci $y \in [b]$. Deci $[a] \subseteq [b]$ şi din simetrie obţinem $[a] = [b]$. Am demonstrat astfel şi pe (c). •

Fie A o mulţime nevidă. Unei partiţii $\mathcal{A} = (A_i)_{i\in I}$ a lui A, îi putem asocia relaţia pe A definită prin $x \sim_{\mathcal{A}} y \Leftrightarrow x, y$ se găsesc în acelaşi A_i. Se arată uşor că $\sim_{\mathcal{A}}$ este o relaţie de echivalenţă ale cărei clase de echivalenţă sunt chiar submulţimile A_i. Reciproc, dacă ρ este o relaţie de echivalenţă pe mulţimea A, atunci din teorema precedentă rezultă că A/ρ este o partiţie a lui A şi $\sim_{A/\rho} = \rho$. Am stabilit astfel următorul rezultat.

Teorema 13 *Fie A o mulţime nevidă. Aplicaţiile $\rho \mapsto A/\rho$ şi $\mathcal{A} \mapsto \sim_{\mathcal{A}}$ sunt bijecţii inverse una celeilalte între relaţiile de echivalenţă pe A şi partiţiile lui A.*

De exemplu, pe o mulţimea $\{1, 2, 3\}$ sunt cinci relaţii de echivalenţă deoarece $\{1, 2, 3\}$ are cinci partiţii (vezi şi exerciţiul 16). Fie funcţia $\alpha : \mathbf{R} \to \mathbf{C}$, $\alpha(x) = \cos(2\pi x) + i\ \sin(2\pi x)$. Clasele de echivalenţă ale relaţiei $\sim_\alpha$ sunt submulţimile lui $\mathbf{R}$ de forma $\{x + k|\ k \in \mathbf{Z}\}$ cu $0 \leq x < 1$. În fond, se vede uşor că pentru o funcţie $f : A \to B$, clasele de echivalenţă ale relaţiei $\sim_f$ sunt submulţimile $f^{-1}(b)$ cu $b \in \mathrm{Im}(f)$.

Fie $\sim$ o relaţie de echivalenţă pe mulţimea A. O submulţime S a lui A se numeşte *sistem de reprezentanţi* pentru $\sim$ dacă S conţine exact câte un element din fiecare clasă de echivalenţă. Deci, S este sistem de reprezentanţi pentru $\sim$ dacă şi numai dacă S verifică condiţiile

(1) pentru orice $a \in A$ există $s_a \in S$ cu $a \sim s_a$, şi

(2) orice două elemente distincte ale lui S nu sunt în relaţia $\sim$.

$[0, 1)$ este un sistem de reprezentanţi pentru relaţia $\sim_\alpha$ definită anterior. Pe mulţimea numerelor complexe (identificată cu planul complex), relaţia $z \sim w \Leftrightarrow |z| = |w|$ este o relaţie de echivalenţă (este chiar relaţia asociată funcţiei $d : \mathbf{C} \to \mathbf{R}$, $d(z) = |z|$). Clasele de echivalenţă sunt cercurile de cetru 0, iar $[0, \infty)$ este un sistem de reprezentanţi.

Fie n un număr natural fixat. Spunem că două numere întregi a, b sunt *congruente modulo n* şi scriem $a \equiv b\ (n)$ dacă n divide $a - b$. Relaţia $\equiv (n)$ se numeţe relaţia de *congruenţă modulo n* pe $\mathbf{Z}$. De exemplu, $7 \equiv -5\ (4)$ şi $11 \not\equiv 4\ (6)$. De asemenea, $a \equiv b\ (2) \Leftrightarrow a$ şi b au aceeaşi paritate. Se vede imediat că relaţia de congruenţă modulo 0 este chiar egalitatea şi că orice două numere sunt congruente modulo 1. Aşadar, ne putem restrânge in cele ce urmează la cazul $n \geq 2$.

Teorema 14 *Relaţia de congruenţă modulo n pe $\mathbf{Z}$ este o relaţie de echivalenţă cu clasele de echivalenţă $\widehat{0}$, $\widehat{1}$,...,$\widehat{n-1}$, unde*

$$\widehat{r} = \{nq + r|\ q \in \mathbf{Z}\}.$$

Demonstraţie. Fie $a, b \in \mathbf{Z}$. Împărţind pe fiecare cu rest la n, obţinem $a = nq + r$, $b = ns + t$ cu $q, s \in \mathbf{Z}$ şi $r, t \in \{0, 1, ..., n - 1\}$. Atunci $a \equiv b\ (n)$ $\Leftrightarrow n|a - b \Leftrightarrow n|r - t \Leftrightarrow r = t$, deoarece $|r - t| \leq n - 1$. Aşadar

$$a \equiv b\ (n) \Leftrightarrow a \text{ şi } b \text{ dau acelaşi rest la împărţirea cu } n.$$

Cu această caracterizare se arată uşor că relaţia de congruenţă modulo n este o relaţie de echivalenţă şi că are clasele de echivalenţă $\widehat{0}$, $\widehat{1}$,...,$\widehat{n-1}$. Într-adevăr, pentru $0 \leq r \leq n-1$, $\widehat{r} = \{nq+r |\ q \in \mathbf{Z}\}$ sunt exact numerele ce dau restul r la împărţirea cu n. Altfel spus, mulţimea resturilor $\{0, 1, ..., n-1\}$ este un sistem de reprezentanţi. •

Numim clasele de echivalenţă ale relaţiei de congruenţă modulo n *clasele de resturi modulo* n, iar mulţimea lor o notăm cu $\mathbf{Z}_n$. Deci

$$\mathbf{Z}_n = \{\widehat{0}, \widehat{1}, ..., \widehat{n-1}\}.$$

$\widehat{r}$ se mai scrie $n\mathbf{Z} + r$, unde $n\mathbf{Z}$ este mulţimea multiplilor lui n.

De exemplu, $\mathbf{Z}_2 = \{\widehat{0}, \widehat{1}\}$ unde $\widehat{0}$ (resp. $\widehat{1}$) este mulţimea numerelor întregi pare (resp. impare).

Cu ajutorul relaţilor de echivalenţă se pot defini noi obiecte matematice. De exemple, mulţimea numerelor întregi $\mathbf{Z}$ se poate construi plecând de la $\mathbf{N}$ astfel. Pe $\mathbf{N} \times \mathbf{N}$ considerăm relaţia de echivalenţă $(a, b) \sim (c, d)$ dacă $a + d = b + c$. Dacă notăm clasa de echivalenţă a lui (a, b) cu $a - b$, atunci putem defini pe $\mathbf{Z}$ ca $\mathbf{N} \times \mathbf{N}/\sim = \{a - b |\ a, b \in \mathbf{N}\}$ (vezi exerciţiul 24).

Dăm şi un exemplu geometric. Fie dreptunghiul $D = [0, 9] \times [0, 1]$. Pe D considerăm relaţiile de echivalenţă $\sim$, $\perp$ şi $\approx$ definite prin

$(0, y) \sim (9, y)$ pentru orice $y \in [0, 1]$,

$(0, y) \approx (9, y)$ şi $(x, 0) \approx (x, 1)$ pentru orice $(x, y) \in [0, 9] \times [0, 1]$,

$(0, y) \perp (9, 1 - y)$ pentru orice $y \in [0, 1]$.

Atunci mulţimea factor $D/\sim$ poate fi gândită ca un cilindru, deoarece am "lipit" laturile verticale ale lui D, $D/\approx$ poate fi gândită ca un tor, deoarece am "lipit" şi laturile orizontale ale lui D, iar $D/\perp$ poate fi gândită ca o bandă Möbius, deoarece am "lipit" laturile verticale ale lui D după o răsucire.

1.5 Exerciţii.

1. Fie M o mulţime, $A, B \subseteq M$ şi fie funcţia

$$f : \mathcal{P}(M) \to \mathcal{P}(A) \times \mathcal{P}(B) \text{ definită prin } f(X) = (X \cap A, X \cap B).$$

Arătaţi că f este injectivă $\Leftrightarrow A \cup B = M$ şi că f este surjectivă $\Leftrightarrow A \cap B = \emptyset$.

2. Fie $f : A \to B$ o funcţie. Considerăm funcţiile $f_* : \mathcal{P}(A) \to \mathcal{P}(B)$, $f^* : \mathcal{P}(B) \to \mathcal{P}(A)$, definite prin $f_*(X) = f(X)$ şi $f^*(Y) = f^{-1}(Y)$. Arătaţi că f este injectivă (resp. surjectivă) $\Leftrightarrow$ f_* este surjectivă (resp. f^* injectivă).

3. Arătaţi că funcţia $f : \mathbf{Z}^2 \to \mathbf{R}$, $f(x,y) = (x-\sqrt{2})^2 + (y-1/3)^2$, este injectivă. Ca aplicaţie, arătaţi că pentru orice număr natural n, există un cerc cu centrul în punctul $C = (\sqrt{2}, 1/3)$ care conţine în interior exact n puncte cu coordonatele numere întregi.

4. Găsiţi imaginea funcţiei $f : \mathbf{Z}^2 \to \mathbf{Z}$, $f(x,y) = x^2 - y^2$.

5. Scrieţi elementele mulţimii $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$.

6. Fie $(A_n)_{n\geq 1}$ un şir mulţimi nevide finite şi fie $f_n : A_{n+1} \to A_n$, $n \geq 1$, aplicaţii. Arătaţi că există un şir $(a_n)_{n\geq 1}$, $a_n \in A_n$, astfel încât $f_n(a_{n+1}) = a_n$ pentru $n \geq 1$.

7. Fie A o mulţime. Arătaţi că nu există o injecţie $f : \mathcal{P}(A) \to A$. (Indicaţie: folosiţi mulţimea $B = A \setminus \{f(C) |\ f(C) \in C\}$ şi elementul $b = f(B)$.)

8. Fie $f : B \to A$ o funcţie injectivă, unde A este o submulţime a lui B. Considerăm mulţimea $C = \{f^n(x) |\ x \in B \setminus A,\ n \geq 0\}$, unde $f^0(x) := x$ şi $f^n = ff^{n-1}$ pentru $n \geq 1$. Arătaţi că funcţia $g : B \to A$ definită prin $g(x) = \begin{cases} f(x) & \text{dacă} \quad x \in C \\ x & \text{dacă} \quad x \notin C \end{cases}$ este bijectivă. Aplicaţie: calculaţi g pentru $f : [0,1] \to [0,1)$, $f(x) = x/2$.

9 Folosiţi exerciţiul precedent pentru a arăta că două mulţimi D, E sunt echipotente dacă între ele există injecţii $u : D \to E$ şi $v : E \to D$ (teorema Cantor-Schröder-Bernstein).

10. Fie A, B, C trei mulţimi nevide. Arătaţi că $(B \times C)^A \simeq B^A \times C^A$ şi $(C^B)^A \simeq C^{A\times B}$.

11. (Principiul includerii şi excluderii.) Fie X o mulţime finită nevidă şi $A_1, ..., A_n$ submulţimi ale lui X. Arătaţi că:

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{i<j} |A_i \cap A_j| + \cdots + (-1)^{n+1} |A_1 \cap \cdots \cap A_n|.$$

12. Fie a, b două numere naturale, $A = \{1, 2, ..., a\}$ şi $B = \{1, 2, ..., b\}$. Probaţi afirmaţiile următoare.

(a) Numărul N al funcţiilor de la A la B este b^a.

(b) Dacă $a \leq b$, numărul N_i al injecţiilor de la A la B este $b!/(b-a)!$. În particular, numărul permutărilor unei mulţimi cu n elemente este $n!$.

(c) Dacă $a \geq b$, numărul N_s al surjecţiilor de la A la B este

$$b^a - C_b^1(b-1)^a + C_b^2(b-2)^a + \cdots (-1)^{b-1}C_b^{b-1}.$$

(d) Dacă $a \leq b$, numărul N_r al funcţiilor strict crescătoare de la A la B este C_b^a.

(e) Numărul N_c al funcţiilor crescătoare de la A la B este C_{a+b-1}^a. (Indicaţie. La (c), se numără non-surjecţiile folosind ex. 11, iar (e) se poate reduce la (d).)

13. Fie $k, n \geq 1$. Arătaţi că numărul monoamelor $X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ de grad k este C_{n+k-1}^{n-1}.

14. Arătaţi că numărul permutărilor de grad n fără puncte fixe este $n!(1 - 1/1! + 1/2! - 1/3! + \cdots + (-1)^n/n!)$. (Indicaţie. Folosiţi ex. 11).

15. Pentru $n \geq 1$, fie $\varphi(n)$ numărul întregilor pozitivi $\leq n$ şi primi cu n (funcţia φ se numeşte *indicatorul lui Euler*). Arătaţi că

$$\varphi(n) = n(1 - 1/p_1)(1 - 1/p_2)\cdots(1 - 1/p_s)$$

unde $p_1, p_2, ..., p_s$ sunt factorii primi ai lui n.

16. Număraţi relaţiile de echivalenţă pe o mulţime cu n elemente.

17. Arătaţi că relaţia de congruenţă modulo n este relaţie de echivalenţă folosind definiţia.

18. Care dintre următoarele relaţii pe $\mathbf{R}$ este relaţie de echivalenţă: (a) $x\alpha y$ dacă $x - y \in \mathbf{Z}$, (b) $x\beta y$ dacă $|x-y| < 2$, (c) $x\gamma y$ dacă $x + y \in \mathbf{Z}$?

19. Fie $\mathcal{R}$ mulţimea relaţiilor pe $\{1, 2, 3\}$. Considerăm axiomele de: (1) reflexivitate, (2) simetrie, (3) tranzitivitate, (4) antisimetrie. Calculaţi imaginea funcţiei următoare: $g : \mathcal{R} \to \{0, ..., 15\}$, $g(\rho) = a_1 + 2a_2 + 4a_3 + 8a_4$ unde $a_i = 1$ (resp. $a_i = 0$) dacă ρ satisface (resp. nu satisface) axioma (i).

20. Fie A o mulţime infinită şi F mulţimea funcţiilor $g : A \to A$. Pe F definim relaţia $f \sim g \Leftrightarrow$ mulţimea $D_{fg} = \{a \in A | \; f(a) \neq g(a)\}$ este finită. Arătaţi că $\sim$ este o relaţie de echivalenţă.

21. Pe mulţimea $\mathbf{C}^*$ (=planul complex fără 0) definim relaţia $z \sim w \Leftrightarrow z$, w şi 0 sunt coliniare. Arătaţi că $\sim$ este relaţie de echivalenţă, determinaţi clasele de echivalenţă şi un un sistem de reprezentanţi.

22. Pe mulţimea $\mathbf{C}$ (=planul complex) definim relaţia $z \sim w \Leftrightarrow z - w \in \mathbf{R}$. Arătaţi că $\sim$ este relaţie de echivalenţă, determinaţi clasele de echivalenţă şi un un sistem de reprezentanţi.

23. Fie A o mulţime nevidă. Pe mulţimea H a funcţiilor de la A în A definim relaţia $f \sim g \Leftrightarrow$ există o bijecţie $u \in H$ astfel încât $fu = ug$. Arătaţi că $\sim$ este relaţie de echivalenţă.

24. (Construcţia lui $\mathbf{Z}$.) Fie $\sim$ relaţia pe $\mathbf{N} \times \mathbf{N}$ definită prin $(a, b) \sim (c, d)$ dacă $a + d = b + c$. Arătaţi că $\sim$ este o relaţie de echivalenţă şi că $\mathbf{N} \times \mathbf{N}/\sim$ se identifică în mod natural cu $\mathbf{Z}$.

25. (Construcţia lui $\mathbf{Q}$.) Fie $\sim$ relaţia pe $\mathbf{Z} \times \mathbf{N}^*$ definită prin $(a, b) \sim (c, d)$ dacă $ad = bc$. Arătaţi că $\sim$ este o relaţie de echivalenţă şi că $\mathbf{Z} \times \mathbf{N}^*/\sim$ se identifică în mod natural cu $\mathbf{Q}$.

26. (Construcţia lui $\mathbf{R}$.) Fie $\mathcal{C}$ mulţimea şirurilor Cauchy de numere raţionale (un şir $(a_n)_{n\geq 1}$ se numeşte *şir Cauchy* dacă pentru orice număr natural $k \geq 1$, există un număr natural $N = N(k) \geq 1$ astfel încât $|a_n - a_m| < 1/k$ pentru orice $n, m \geq N$). Pe $\mathcal{C}$ considerăm relaţia $\sim$ definită prin $(a_n)_{n\geq 1} \sim (b_n)_{n\geq 1}$ $\Leftrightarrow \lim\limits_{n\to\infty}(a_n - b_n) = 0$. Arătaţi că $\sim$ este o relaţie de echivalenţă şi că $\mathcal{C}/\sim$ se identifică în mod natural cu $\mathbf{R}$.

27. Pentru ce numere naturale $n \geq 2$ este funcţia $f : \mathbf{Z}_n \to \mathbf{C}$, $f(\hat{k}) = i^k$ bine-definită ?

Capitolul 2

Operaţii algebrice, monoizi.

În acest capitol se introduce noţiunea de operaţie algebrică, noţiune fundamentală pentru înţelegerea tuturor capitolelor următoare. Sunt date apoi câteva proprietăţi ale monoizilor.

2.1 Operaţii algebrice

Fie A o mulţimea nevidă. O *operaţie algebrică binară* $*$ pe mulţimea A (prescurtat, operaţie pe A) este o funcţie $* : A \times A \to A$. Pentru comoditate, vom scrie $a * b$ în loc de $*(a, b)$. Deci, operaţia $*$ asociază fiecărei perechi $(a, b) \in A \times A$ elementul $a * b \in A$. De exemplu, $x * y = x$, $x \perp y = x^2 + y^2$ sunt operaţii pe $\mathbf{R}$.

Fie $*$ o operaţie pe mulţimea A. Operaţia $*$ se zice *asociativă* dacă

$$a * (b * c) = (a * b) * c \quad \text{pentru orice} \quad a, b, c \in A.$$

Operaţia $*$ se zice *comutativă* dacă

$$a * b = b * a \quad \text{pentru orice} \quad a, b \in A.$$

Un element $e \in A$ se numeşte *element neutru* pentru operaţia $*$ dacă

$$a * e = e * a = a \quad \text{pentru orice} \quad a \in A.$$

Dacă există, elementul neutru este unic. Într-adevăr, dacă e, f sunt elemente neutre, atunci $e = e * f = f$.

O submulţime nevidă H a lui A se numeşte *parte stabilă (în raport cu $*$)* dacă

$$x * y \in H \text{ pentru orice } x, y \in H.$$

În acest caz, $*$ se restrânge la o operaţie pe H numită *operaţia indusă.* De exemplu, pe mulţimea $\mathbf{N}$, operaţia de adunare este asociativă, comutativă şi are elementul neutru 0; în plus, $\mathbf{N} \setminus \{0, 1, 2, 4\}$ este parte stabilă. Operaţia de scădere pe $\mathbf{Z}$ nu este nici asociativă nici comutativă şi nu are element neutru, e.g. $1 - (1 - 1) = 1 \neq -1 = (1 - 1) - 1$, $2 - 1 = 1 \neq -1 = 1 - 2$; în plus, $3\mathbf{Z}$ este parte stabilă.

Perechea $M = (A, *)$ se numeşte *semigrup* dacă A este o mulţime nevidă şi $*$ este operaţie asociativă pe A. Un *monoid* este un semigrup cu element neutru. A se numeşte *mulţimea subiacentă* a semigrupului/monoidului M. Semigrupul (monoidul) M se zice *comutativ* dacă $*$ este operaţie comutativă.

De exemplu, $(\mathbf{N} \setminus \{1\}, +)$ este un semigrup comutativ. Pe o mulţime C cu cel puţin două elemente, operaţia $a * b = a$, $a, b \in C$, defineşte o structură de semigrup necomutativ care nu este monoid. Avem exemplele de monoizi comutativi: $(\mathbf{N}, +)$, $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$, $(\mathbf{N}, \cdot)$, $(\mathbf{Z}, \cdot)$, $(\mathbf{Q}, \cdot)$, $(\mathbf{R}, \cdot)$, $(\mathcal{P}(B), \cup)$ şi $(\mathcal{P}(B), \cap)$, unde B este o mulţime arbitrară.

Fie B o mulţime nevidă. Pe mulţimea B^B a tuturor funcţiilor $f : B \to B$, operaţia de compunere determină o structură de monoid. Într-adevăr, compunerea funcţiilor este asociativă (cf. teoremei 3) şi funcţia identică I_B joacă rol de element neutru. Dacă B are cel puţin două elemente, monoidul B^B este necomutativ, după cum putem vedea compunând două aplicaţii constante diferite.

Fie $M = (A, *)$ un monoid cu elementul neutru e. Un element $a \in M$ se numeşte *element inversabil sau simetrizabil* dacă există $a' \in M$ cu

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

Dacă există, elementul a' este unic. Într-adevăr, dacă în plus $b \in A$ şi $a * b = b * a = e$, atunci

$$a' = a' * e = a' * (a * b) = (a' * a) * b = e * b = b.$$

Elementul a' se numeşte *inversul sau simetricul* lui a. Notăm cu $U(M)$ mulţimea elementelor inversabile ale monoidului M numită şi *mulţimea unităţilor* lui M. Cum $e * e = e$, $e \in U(M)$.

Un monoid se numeşte *grup* dacă $U(M) = M$, adică orice element al său este inversabil. De exemplu, monoizii $(\mathbf{N}, +)$ şi $(\mathbf{Z}, \cdot)$ nu sunt grupuri, deoarece $U(\mathbf{N},+)=\{0\}$ şi $U(\mathbf{Z},\cdot)=\{1,-1\}$. Pe de altă parte, $(\mathbf{Z},+)$ este grup; îl vom numi *grupul* $\mathbf{Z}$ subînţelegând că operaţia grupală este adunarea.

Deosebim următoarele tipuri de notaţii. *Notaţie generală*, caz în care operaţia este notată cu un semn de tipul $*$, $\circ$, $\perp$, etc., elementul neutru este notat cu e, I, etc., iar simetricul unui element a este notat de exemplu cu a' sau $\bar{a}$.

Notaţie aditivă, caz în care operaţia este notată cu semnul $+$ şi este numită *adunare*, elementul neutru este notat cu 0 şi este numit *elementul nul*, iar simetricul unui element a este notat cu $-a$ şi este numit *opusul* lui a.

Notaţie multiplicativă, caz în care operaţia este notată cu semnul $\cdot$ şi este numită *înmulţire*, elementul neutru este notat cu 1 şi este numit *elementul unitate*, iar simetricul unui element a este notat cu a^{-1} şi este numit *inversul* lui a. În cazul notaţiei multiplicative, $x\cdot y$ se notează mai simplu cu xy.

Pentru simplificarea scrierii, vom expune rezultatele teoretice referitoare la semigrupuri, monoizi şi grupuri în notaţie multiplicativă. Concret, prin expresia "fie monoidul M" vom înţelege că pe mulţimea nevidă M se consideră operaţia asociativă $(a,b)\mapsto ab$ cu elementul neutru 1 (sau 1_M), iar dacă $a\in U(M)$, atunci inversul său este a^{-1}. Pentru o mai bună întelegere, cititorul e sfătuit să transcrie rezultatele în notaţie aditivă sau generală.

Fie M o mulţime împreună cu o operaţie neasociativă notată multiplicativ şi fie $a,b,c,d\in M$. Pentru a preciza produsul abc putem pune parantezele în două moduri $(ab)c$ sau $a(bc)$. De asemenea, în produsul $abcd$ putem pune parantezele în cinci moduri: $(ab)(cd)$, $a(b(cd))$, $a((bc)d)$, $((ab)c)d$, $(a(bc))d$ (vezi şi ex. 30). Dacă operaţia este asociativă, toate cele cinci produse anterioare dau acelaşi rezultat. De exemplu, $((ab)c)d=(ab)(cd)=a(b(cd))$. Are loc următorul rezultat numit *teorema de asociativitate generalizată.*

Teorema 15 *Dacă M este un semigrup şi $a_1,...,a_n\in M$, atunci valoarea produsului $a_1\cdots a_n$ nu depinde de modul în care s-au pus parantezele.*

Demonstraţie. Probăm afirmaţia prin inducţie după n. Cazurile $n=1$ şi $n=2$ sunt evidente, iar cazul $n=3$ rezultă din asociativitate. Fie $n\geq 4$ şi presupunem că afirmaţia a fost probată pentru produsele de lungime $<n$; deci pentru $b_1,...,b_k\in M$ şi $k<n$, scrierea $b_1\cdots b_k$ este neambiguă. Fie b valoarea produsului $a_1\cdots a_n$ calculat într-un mod oarecare. Rezultă că există i, $1\leq i<n$, cu $b=(a_1\cdots a_i)(a_{i+1}\cdots a_n)$. Dacă $i<n-1$, din ipoteza de inducţie rezultă

$$b=(a_1\cdots a_i)((a_{i+1}\cdots a_{n-1})a_n)=$$

$$= ((a_1 \cdots a_i)(a_{i+1} \cdots a_{n-1}))a_n = (a_1 \cdots a_{n-1})a_n.$$

Deci b nu depinde de modul de calcul ales. Acelaşi rezultat se obţine şi dacă $i = n - 1$. •

Teorema precedentă ne permite să folosim într-un semigrup (monoid) scrierea $a_1 a_2 \cdots a_n$.

Spunem că două elemente a, b ale unui semigrup sunt *permutabile* dacă $ab = ba$.

Teorema 16 *Fie M un semigrup şi $a_1, a_2, ..., a_n \in M$ elemente permutabile două câte două. Atunci produsul $a_1 a_2 \cdots a_n$ nu depinde de ordinea factorilor.*

Demonstraţie. Fie b un produs al elementelor $a_1, a_2, ..., a_n$ într-o ordine oarecare. Prin permutări de elemente vecine, aducem a_1 pe primul loc, apoi a_2 pe locul doi, ş.a.m.d. •

2.2 Monoizi

Teorema 17 *Dacă M este un monoid şi $a_1, a_2, ..., a_n$ sunt elemente inversabile ale lui M, atunci produsul lor $a_1 a_2 \cdots a_n$ este element inversabil şi*

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}.$$

În particular, $U(M)$ este grup faţă de operaţia indusă.

Demonstraţie. Avem

$$(a_1 a_2 \cdots a_n)(a_n^{-1} \cdots a_2^{-1} a_1^{-1}) = (a_1 a_2 \cdots a_{n-1})(a_n a_n^{-1})(a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}) =$$

$$= (a_1 a_2 \cdots a_{n-1})(a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}) = ... = a_1 a_1^{-1} = 1.$$

Analog se arată că $(a_n^{-1} \cdots a_2^{-1} a_1^{-1})(a_1 a_2 \cdots a_n) = 1$. Rezultă că $U(M)$ este un monoid cu toate elementele inversabile, deci $U(M)$ este grup. •

Fie $n \geq 1$. Pe mulţimea $\mathbf{Z}_n = \{\widehat{0}, \widehat{1}, ..., \widehat{n-1}\}$ a claselor de resturi modulo n definim o operaţie de adunare şi una de înmulţire. Fie $\widehat{x}, \widehat{y} \in \mathbf{Z}_n$ cu $x, y \in \mathbf{Z}$. Definim $\widehat{x} + \widehat{y} = \widehat{x+y}$ şi $\widehat{x}\widehat{y} = \widehat{xy}$.

Cele două operaţii sunt bine-definite, adică nu depind de reprezentanţii claselor. Într-adevăr, fie $x', y' \in \mathbf{Z}$ cu $\widehat{x} = \widehat{x'}$ şi $\widehat{y} = \widehat{y'}$. Atunci n divide $x' - x$ şi $y' - y$. Deci n divide $x' + y' - x - y$ şi $x'y' - xy = (x' - x)y' + x(y' - y)$. Rezultă că $\widehat{x+y} = \widehat{x'+y'}$ şi $\widehat{xy} = \widehat{x'y'}$.

Se verifică uşor că $(\mathbf{Z}_n, +)$ şi $(\mathbf{Z}_n, \cdot)$ sunt monoizi comutativi cu elementele neutre $\widehat{0}$ respectiv $\widehat{1}$. Primul este chiar grup deoarece $\widehat{x} + \widehat{(-x)} = \widehat{0}$ pentru orice $\widehat{x} \in \mathbf{Z}_n$. Il vom numi *grupul* $\mathbf{Z}_n$ subînţelegând că operaţia grupală este adunarea.

Considerăm acum monoidul $(\mathbf{Z}_n, \cdot)$. Atunci $U(\mathbf{Z}_n)$ este $\{\widehat{x} | \ x \in \mathbf{Z},\ (x, n) = 1\}$. Într-adevăr, fie $x \in \mathbf{Z}$. Atunci $\widehat{x} \in U(\mathbf{Z}_n) \Leftrightarrow \exists\ y \in \mathbf{Z}$ cu $\widehat{x}\widehat{y} = \widehat{1} \Leftrightarrow \exists\ y, a \in \mathbf{Z}$ cu $xy + an = 1 \Leftrightarrow (x, n) = 1$.

Reamintim (vezi ex. 15) că indicatorul lui Euler $\varphi(n)$ al lui n este numărul întregilor pozitivi $\leq n$ şi primi cu n. Din teorema 17 obţinem

Teorema 18 *$U(\mathbf{Z}_n, \cdot) = \{\widehat{x} | \ x \in \mathbf{Z},\ (x, n) = 1\}$ este un grup abelian cu $\varphi(n)$ elemente.*

De exemplu, $U(\mathbf{Z}_{12}) = \{\widehat{1}, \widehat{5}, \widehat{7}, \widehat{11}\}$.

Fie M un monoid, $a \in M$ şi $n \geq 1$. Definim *puterile lui* a prin: $a^0 = 1_M$, $a^n = aa \cdots a$ (n factori). Dacă a este inversabil, putem extinde definiţia precedentă punând $a^{-n} = (a^{-1})^n$, $n \geq 1$. În cazul notaţiei aditive egalităţile precedente se scriu $0a = 0_M$, $na = a + a + \cdots + a$ (n termeni), $0a = 0_M$ şi $(-n)a = n(-a)$.

Teorema 19 (Reguli de calcul într-un monoid). *Fie M un monoid şi $a, b \in M$. (a) $a^m a^n = a^{m+n}$ pentru orice $m, n \geq 0$ (resp. m, n întregi, dacă a este inversabil).*

(b) $(a^m)^n = a^{mn}$ pentru orice $m, n \geq 0$ (resp. m, n întregi, dacă a este inversabil).

(c) Dacă $ab = ba$, atunci $(ab)^n = a^n b^n$ pentru orice $m, n \geq 0$ (resp. m, n întregi, dacă a, b sunt inversabile).

Demonstraţie. Pentru $m, n \geq 0$, afirmaţiile sunt consecinţe imediate ale definiţiei. Presupunem că a, b sunt inversabile.

(a). Pentru k întreg avem $a^k = a^{k+1}a^{-1} = a^{k+2}a^{-2} = \cdots = a^{k+p}a^{-p}$.

(b). Fie $m \geq 0$ şi $n \leq 0$. Atunci $(a^m)^n = ((a^m)^{-1})^{-n} = ((a^{-1})^m)^{-n} = (a^{-1})^{-mn} = a^{mn}$. Celelalte cazuri rezultă analog.

(c). Fie $n \leq 0$. Atunci $(ab)^n = ((ab)^{-1})^{-n} = (a^{-1}b^{-1})^{-n} = (a^{-1})^{-n}(b^{-1})^{-n}$ $= a^n b^n$. •

Fie A şi B doi monoizi. O funcţie $f : A \to B$ se numeşte *morfism de monoizi* dacă

$$\begin{cases} f(xy) = f(x)f(y) \text{ pentru orice } x, y \in A, \\ f(1_A) = 1_B. \end{cases}$$

Dacă A şi B sunt monoizi, avem morfismele $x \mapsto 1_B : A \to B$ numit *morfismul trivial* şi $I_A : A \to A$, $I_A(x) = x$, numit *morfismul identic.* $n \mapsto 2^n : (\mathbf{N}, +) \to (\mathbf{N}, \cdot)$, $x \mapsto |x| : (\mathbf{Z}, \cdot) \to (\mathbf{N}, \cdot)$ şi $n \mapsto 2n : (\mathbf{N}, +) \to (\mathbf{N}, +)$ sunt exemple concrete de morfisme de monoizi.

Un morfism de monoizi bijectiv se numeşte *izomorfism de monoizi.* Morfismul identic este izomorfism. $X \mapsto B \setminus X : (\mathcal{P}(B), \cup) \to (\mathcal{P}(B), \cap)$, $x \mapsto -x : (\mathbf{Z} \cup \{-\infty\}, max) \to (\mathbf{Z} \cup \{\infty\}, min)$ şi $x \mapsto 2^x : (\mathbf{R}, +) \to ((0, \infty), \cdot)$ sunt exemple concrete de izomorfisme de monoizi.

Teorema 20 (a) *Compunerea a două morfisme de monoizi este un morfism de monoizi.* (b) *Inversul unui izomorfism de monoizi este tot un izomorfism.*

Demonstraţie. (a). Fie $f : A \to B$ şi $g : B \to C$ morfisme de monoizi. Pentru orice $x, y \in A$ avem

$$(gf)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (gf)(x)(gf)(y).$$

De asemenea, $(gf)(1_A) = g(f(1_A)) = g(1_B) = 1_C$.

(b). Presupunem că $f : A \to B$ este un izomorfism de monoizi. Fie $x, y \in B$ şi $x' = f^{-1}(x)$, $y' = f^{-1}(y)$. Atunci

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

De asemenea, din egalitatea $f(1_A) = 1_B$ rezultă $f^{-1}(1_B) = 1_A$. •

Teorema 21 *Fie $f : A \to B$ un morfism de monoizi şi $a \in A$. Atunci*

(a) *$f(a^n) = f(a)^n$ pentru orice $n \geq 1$,*

(b) *dacă $a \in U(A)$, atunci $f(a) \in U(B)$, $f(a)^{-1} = f(a^{-1})$ şi $f(a^n) = f(a)^n$ pentru orice întreg n.*

Demonstraţie. Afirmaţia (a) rezultă din definiţia morfismului. (b). Presupunem că $a \in U(A)$. Aplicând f şirului de egalităţi $aa^{-1} = a^{-1}a = 1_A$ se obţine $f(a)f(a^{-1}) = f(a^{-1})f(a) = f(1_A) = 1_B$, deci $f(a) \in U(B)$ şi $f(a)^{-1} = f(a^{-1})$. Fie $n \leq 0$. Atunci $f(a^n) = f((a^{-1})^{-n}) = f(a^{-1})^{-n} = (f(a)^{-1})^{-n} = f(a)^n$. •

Spunem că monoizii A şi B sunt *izomorfi*, şi scriem $A \simeq B$, dacă între ei există un izomorfism. Doi monoizi izomorfi au aceleaşi proprietăţi monoidale, de aceea nu vom face distinţie între ei. Din teorema 20, rezultă că relaţia de izomorfism între monoizi este reflexivă, simetrică şi tranzitivă.

De exemplu, $(\{1, 0\}, \cdot) \simeq (\{0, \infty\}, +) \simeq (\{1, 2\}, max)$. Pe de altă parte, $(\mathbf{N}, +) \not\simeq (\mathbf{N}^*, \cdot)$, deoarece dacă $f : (\mathbf{N}, +) \to (\mathbf{N}, \cdot)$ este un izomorfism, ar rezulta că toate numerele naturale nenule sunt puteri ale lui $f(1)$.

Fie A o mulţime pe care o vom numi *alfabet* iar elementele sale *litere*. Vom numi *cuvânt* un şir finit $a_1a_2 \cdots a_n$ de litere, incluzând aici şi *cuvântul vid* (cuvântul cu zero litere) notat cu $\sqcup$. Prin definiţie, două cuvinte $a_1a_2 \cdots a_n$ şi $b_1b_2 \cdots b_m$ sunt egale dacă $m = n$ şi $a_1 = b_1$,...,$a_n = b_n$, adică dacă au acelaşi număr de litere şi literele corespunzătoare sunt egale. Fie $W(A)$ mulţimea cuvintelor cu litere din A. Atunci $W(A)$ este monoid în raport cu operaţia de concatenare

$$(a_1a_2 \cdots a_n)(b_1b_2 \cdots b_m) = a_1a_2 \cdots a_nb_1b_2 \cdots b_m.$$

numit *monoidul liber generat de mulţimea A*. Elementul său neutru este cuvântul vid. De exemplu, dacă $B = \{b\}$, atunci $W(B) = \{\sqcup, b, bb, ..., b^n, ...\}$. Este clar că $W(B)$ este izomorf cu $(\mathbf{N}, +)$ prin izomorfismul $n \mapsto b^n : \mathbf{N} \to W(B)$. Dacă $D = \{a, b\}$, atunci monoidul $W(D) = \{\sqcup, a, b, ab, ba, abb, bab, aab, ...\}$ este necomutativ, deoarece $ab \neq ba$.

Mesajul teoremei următoare este că morfismele de monoizi $W(A) \to M$ se pot defini "pe litere". Demonstraţia se face prin calcul.

Teorema 22 *Fie A o mulţime, M un monoid şi $f : A \to M$ o funcţie. Atunci funcţia*

$$F : W(A) \to M, \ F(a_1a_2 \cdots a_n) = f(a_1)f(a_2) \cdots f(a_n), \ a_1, ..., a_n \in A$$

este un morfism de monoizi. În particular, există un morfism surjectiv de monoizi $W(M) \to M$.

2.3 Exerciţii

28. Câte operaţii se pot defini pe o mulţime cu n elemente şi câte dintre acestea sunt comutative, respectiv cu element neutru ?

29. Fie S un semigrup finit. Arătaţi că există $n > m \geq 1$ astfel încât $x^n = x^m$ pentru orice $x \in S$.

30. Arătaţi că numărul de moduri T_n în care se pot pune parantezele într-un produs neasociativ $a_1 a_2 \cdots a_n$ este $T_n = C_{2n-2}^{n-1}/n$ (numărul lui Catalan).

31. Considerăm următoarele operaţii algebrice pe $\mathbf{N}$: (a) $x * y = x + 1$, (b) $x * y = x$, (c) $x * y = xy + 1$, (d) $x * y = 0$, (e) $x * y = max(x, y)$. Precizaţi dacă ele sunt asociative, comutative, sau posedă element neutru.

32. Fie $\mathcal{A}$ mulţimea operaţiilor algebrice pe $\mathbf{N}$. Considerăm axiomele de: (1) asociativitate, (2) comutativitate, (3) existenţa elementului neutru. Calculaţi imaginea funcţiei următoare: $f : \mathcal{A} \to \{0, ..., 7\}$, $f(\rho) = a_1 + 2a_2 + 4a_3$ unde $a_i = 1$ (resp. $a_i = 0$) dacă ρ satisface (resp. nu satisface) axioma (i). (Indicaţie: folosiţi ex. precedent).

33. Daţi exemple de operaţii algebrice care să arate că axiomele de asociativitate, comutativitate şi de existenţă a elementului neutru sunt independente.

34. Ce proprietăţi are operaţia $x * y = x + [y]$ pe $\mathbf{R}$?

35. Fie $a, b, c \in \mathbf{Z}$, $b \neq 0$. Pe $\mathbf{Z}$ definim operaţia $x * y = axy + b(x + y) + c$. Arătaţi că $M_{a,b,c} = (\mathbf{Z}, *)$ este monoid $\Leftrightarrow$ $b = b^2 - ac$ şi $b \mid c$. Mai mult, pentu $a \neq 0$, avem izomorfismele de monoizi $M_{a,b,c} \simeq M_{a,1,0} \simeq K_a$ unde K_a este monoidul multiplicativ $\{am + 1 | \ m \in \mathbf{Z}\}$.

36. Arătaţi că oricare doi dintre monoizii comutativi $(\mathbf{N}, +)$, $(\mathbf{N}, cmmmc)$, $(\mathbf{N}, max)$ şi $(\mathbf{N} \cup \{\infty\}, min)$ sunt neizomorfi.

37. Descrieţi endomorfismele monoiziilor $(\mathbf{N}, +)$, $(\mathbf{N}, max)$ şi morfismele dintre ei.

38. Găsiţi un morfism injectiv de monoizi $f : (\mathbf{N}, max) \to (\mathcal{P}(\mathbf{N}), \cup)$.

39. Arătaţi că monoizii multiplicativi $M_2(\mathbf{Z})$ şi $M_3(\mathbf{Z})$ nu sunt izomorfi.

40. Fie M un monoid şi $\theta \notin M$. Extindem operaţia din M pe $M' = M \cup \{\theta\}$ prin $x\theta = \theta x = \theta$ pentru orice $x \in M'$. Arătaţi că M' este monoid cu $U(M) = U(M')$. Dacă $1 \leq a \leq b$, arătaţi că există un monoid cu b elemente dintre care a sunt inversabile.

41. Numim *atom* al unui monoid M un element neinversabil a care nu se poate scrie ca produsul a două elemente neinversabile. Găsiţi atomii monoidului $(\mathbf{N}^n, +)$ şi arătaţi că $(\mathbf{N}^m, +) \simeq (\mathbf{N}^n, +) \Leftrightarrow m = n$.

42. Daţi exemplu de doi monoizi neizomorfi care au câte doi atomi.

43. Fie S, T mulţimi finite cu s respectiv t elemente. Arătaţi că monoizii liberi $W(S)$, $W(T)$ sunt izomorfi dacă şi numai dacă $s = t$.

44. Arătaţi că în monoidul multiplicativ $M_n = \{nk + 1 |\ k \in \mathbf{N}\}$, $n \in \mathbf{N}$, $n \geq 3$, există trei atomi distincţi p, q, r cu $pq = r^2$. (Indicaţie: pentru $n \neq 5, 8$, $(2n-1)^2$ şi $(n-1)(2n-1)$ sunt atomi).

45. Descrieţi atomii monoizilor multiplicativi $M_n = \{nk+1 |\ k \in \mathbf{N}\}$ pentru $n = 2, 3$ şi arătaţi că monoizii nu sunt izomorfi.

Capitolul 3

Grupuri

În acest capitol se introduc noţiunile de bază ale teoriei grupurilor: grup, morfism de grupuri, subgrup, sistem de generatori, congruenţe modulo un subgrup, grup factor, ordinul unui element într-un grup, grup ciclic, grup de permutări. Se demonstrează teoreme importante precum teorema lui Lagrange, teorema fundamentală de izomorfism, teorema de structură a grupurilor ciclice, teorema de descompunere a unei permutări în produs de cicluri disjuncte, ecuaţia claselor de elemente conjugate şi teorema lui Cauchy.

3.1 Exemple de grupuri

Reamintim că un grup este un monoid cu toate elementele inversabile. Aşadar, un grup este o mulţime inzestrată cu o operaţie asociativă care are element neutru şi astfel încât orice element este inversabil. Un grup se zice *grup abelian* sau *comutativ* dacă operaţia grupală este comutativă şi se zice *finit* dacă mulţimea subiacentă este finită (numărul de elemente se numeşte *ordinul grupului*).

Mulţimile numerice $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ şi $\mathbf{C}$ sunt grupuri abeliene în raport cu adunarea. De asemenea, $\mathbf{Q}^*$, $\mathbf{R}^*$ şi $\mathbf{C}^*$ sunt grupuri abeliene în raport cu înmulţirea.

Pentru $n \geq 2$, mulţimea $\mathbf{Z}_n = \{\widehat{0}, \widehat{1}, ..., \widehat{n-1}\}$ a claselor de resturi modulo n este grup faţă de adunare iar $U(\mathbf{Z}_n, \cdot) = \{\widehat{x} |\ x \in \mathbf{Z},\ (x, n) = 1\}$ este grup faţă de înmulţire (vezi teorema 18).

Conform teoremei 17, unităţile unui monoid formează grup în raport cu operaţia indusă. De exemplu, dacă A este o mulţime, mulţimea A^A a funcţiilor de la A la A este monoid faţă de compunerea funcţiilor. $U(A^A)$ este grupul bijecţiilor $A \to A$, numit *grupul permutărilor mulţimii* A, grup notat cu S_A. Dacă $A = \{1, ..., n\}$, S_A se notează mai simplu S_n şi se numeşte *grupul permutărilor de grad* n.

Fie $n \geq 1$ şi $a_1, ..., a_k$ numere distincte între 1 şi n. Prin *permutarea ciclică (ciclul)* $(a_1, ..., a_k)$ se înţelege permutarea din S_n definită prin $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_n \mapsto a_1$ şi $x \mapsto x$ pentru $x \neq a_i$. Un ciclu de forma (ij) se numeşte *transpoziţie*. De exemplu, S_3 constă din permutarea identică I, transpoziţiile (12), (13), (23) şi ciclurile (123), (132).

Dacă G, H sunt grupuri, produsul cartezian $G \times H$ devine grup faţă de operaţia de "înmulţire pe componente" $(a, b)(a', b') := (aa', bb')$ pentru $a, a' \in G$ şi $b, b' \in H$. Acest grup se numeşte *produsul direct al grupurilor* G *şi* H. Asociativitatea se verifică imediat, unitatea lui $G \times H$ este $(1_G, 1_H)$ iar $(a, b)^{-1} = (a^{-1}, b^{-1})$. Produsul direct $G \times G$ se notează mai simplu cu G^2. De exemplu, grupul multiplicativ $\{\pm 1\}^2$ se numeşte *grupul lui Klein*.

Construcţia produsului direct de grupuri se poate generaliza uşor pentru familii arbitrare de grupuri. De exemplu, $\mathbf{Z}^\mathbf{N}$ este grupul aditiv al şirurilor de numere întregi.

Se numeşte *izometrie* a planului euclidian $\mathbf{R}^2$ o funcţie $f : \mathbf{R}^2 \to \mathbf{R}^2$ care păstrează distanţele, adică satisface egalitatea $d(f(P), f(Q)) = d(P, Q)$ pentru orice $P, Q \in \mathbf{R}^2$, unde

$$d((x_1, x_2), (y_1, y_2)) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2}.$$

Se poate arăta că orice izometrie este bijectivă şi că mulţimea izometriilor $Izo(\mathbf{R}^2)$ este un grup faţă de compunere (vezi [3, pag. 213]). Orice izometrie este o translaţie, rotaţie, simetrie (faţă de o dreaptă) sau compunerea dintre o translaţie şi o simetrie; în plus, orice izometrie se poate obţine compunând cel mult trei simetrii (vezi [3, pag. 216]).

Fie acum o submulţime Y a lui $\mathbf{R}^2$. Izometriile f care invariază pe Y în ansamblu, adică $f(Y) = Y$, formează un subgrup al lui $Izo(\mathbf{R}^2)$ notat cu $Sim(Y)$ şi numit *grupul de simetrie al lui* Y. Într-adevăr, fie $f, g \in Sim(Y)$. Atunci $f(Y) = Y$ şi $g(Y) = Y$, deci $g^{-1}(Y) = Y$ şi rezultă că $(fg^{-1})(Y) = Y$.

Fie R un dreptunghi care nu este pătrat. Atunci $Sim(R)$ constă din transformarea identică, cele două simetrii faţă de mediatoarele laturilor şi rotaţia de π radiani în jurul punctului de intersecţia al diagonalelor.

Fie P un pătrat. $Sim(P)$ constă din transformarea identică, rotaţiile de $\pi/2$, π, $3\pi/2$ radiani în jurul centrului pătratului şi cele patru simetrii faţă de mediatoarele laturilor şi diagonale. Grupul este neabelian deoarece, de exemplu, simetriile faţă de diagonale nu comută. El este numit *grupul diedral al pătratului* şi este notat cu D_4 (vezi şi ex. 56).

Mai general, *grupul diedral* D_n se defineşte ca grupul de simetrie al unui poligon regulat cu n laturi. D_n constă din rotaţiile de $2k\pi/n$ radiani, $k = 0, 1, ..., n-1$, în jurul centrului poligonului şi cele n simetrii faţă de axele de simetrie ale poligonului.

3.2 Morfisme de grupuri

Fie G şi H două grupuri. O funcţie $f : G \to H$ se numeşte *morfism de grupuri* dacă

$$f(xy) = f(x)f(y) \text{ pentru orice } x, y \in G.$$

Fie $e = f(1_G)$. Din $1_G^2 = 1_G$ rezultă $e^2 = e = e1_H$ şi, prin amplificare la stânga cu e^{-1}, rezultă $e = 1_H$. Rezultă că $f(1_G) = 1_H$, deci f este şi morfism de monoizi. Un morfism de grupuri bijectiv se numeşte *izomorfism de grupuri*. Un *automorfism* este un izomorfism de la un grup în el însuşi.

Fie G, H grupuri şi $a \in G$. Atunci aplicaţia $x \mapsto 1_H : G \to H$ este un morfim numit *morfismul trivial* iar aplicaţia identică $I_A : A \to A$ este un automorfism numit *(auto)morfismul identic*. Mai general, aplicaţia $x \mapsto axa^{-1} : G \to G$, este un automorfism numit *automorfismul interior definit de a*.

Ca exemple concrete, $f : (\mathbf{Z}, +) \to (\mathbf{Z}, +)$, $f(n) = 2n$ este morfism de grupuri, iar $g : (\mathbf{R}, +) \to ((0, \infty), \cdot)$, $g(x) = 2^x$ este izomorfism.

Teorema 23 (*a*) *Compunerea a două morfisme de grupuri este un morfism de grupuri.* (*b*) *Inversul unui izomorfism de grupuri este tot un izomorfism.*

Demonstraţie. Rezultă din afirmaţiile corespunzătoare pentru morfismele de monoizi (teorema 20). •

Spunem că grupurile G şi H sunt *izomorfe* sau că *au acelaşi tip*, şi scriem $G \simeq H$, dacă există un izomorfism de grupuri $f : G \to H$. De exemplu, $(\mathbf{R}, +) \simeq ((0, \infty), \cdot)$. Dimpotrivă, $(\mathbf{R}, +) \not\simeq (\mathbf{R}^*, \cdot)$, deoarece dacă $f : (\mathbf{R}^*, \cdot) \to (\mathbf{R}, +)$ este un morfism, atunci $0 = f((-1)^2) = 2f(-1)$, deci $f(-1) = f(1) = 0$.

Se vede că dacă $f : G \to H$ este un izomorfism de grupuri, atunci orice proprietate a grupală a lui G se poate transporta prin f în H. De aceea, nu vom face distincţie între două grupuri izomorfe. De exemplu, fiecare dintre grupurile izomorfe $(\{\pm 1\} \times \{\pm 1\}, \cdot)$ şi $(\mathbf{Z}_2 \times \mathbf{Z}_2, +)$ va fi numit grupul lui Klein.

Din teorema anterioară, rezultă că relaţia de izomorfism între grupuri este reflexivă, simetrică şi tranzitivă.

O problemă importantă în teoria grupurilor finite este descrierea tuturor tipurilor de grupuri cu un număr dat n de elemente. Se poate vedea uşor că pentru $1 \leq n \leq 3$ există câte un singur tip de grup. Fie grupurile cu 4 elemente $\mathbf{Z}_4$ şi $K = (\{\pm 1\}^2, \cdot)$ (grupul lui Klein). Se poate vedea că grupurile nu sunt izomorfe deoarece pentru orice $x \in K$ avem $x^2 = (1, 1)$, dar $2 \cdot \hat{1} \neq \hat{0}$. Mai mult, orice grup cu 4 elemente este izomorf cu $\mathbf{Z}_4$ sau cu K (vezi ex. 49). Deci sunt două tipuri de grupuri cu 4 elemente. Vom arăta că dacă p este număr prim, atunci există doar un tip de grup cu p elemente şi anume $\mathbf{Z}_p$ (vezi corolarul 46).

3.3 Subgrupuri

Fie G un grup. O submulţime nevidă H a lui G se numeşte *subgrup* , şi notăm $H \leq G$, dacă H este o parte stabilă a lui G închisă la luarea inversului, adică pentru orice $x, y \in H$ rezultă $xy \in H$ şi $x^{-1} \in H$. Rezultă atunci că H este grup faţă de operaţia indusă. Într-adevăr, asociativitatea se transmite imediat la H, $1 \in H$ deoarece, dacă $y \in H$, atunci $y^{-1} \in H$ şi $1 = yy^{-1}$, şi orice element din H este inversabil. Printre subgrupurile lui G se găsesc $\{1\}$ numit *subgrupul trivial* şi G numit *subgrupul impropriu.*

Teorema 24 *Fie G un grup. O submulţime nevidă H a lui G este subgrup dacă şi numai dacă $xy^{-1} \in H$ pentru orice $x, y \in H$*

Demonstraţie. Implicaţia directă este imediată: dacă $x, y \in H$, atunci $y^{-1} \in H$ şi deci $xy^{-1} \in H$. Reciproc, să presupunem că $xy^{-1} \in H$ pentru orice $x, y \in H$. Cum H este nevidă, există $z \in H$ şi rezultă că $1 = zz^{-1} \in H$. Fie acum $x, y \in H$. Deducem că $y^{-1} = 1 \cdot y^{-1} \in H$, deci $xy = x(y^{-1})^{-1} \in H$.•

Dacă G este un grup, atunci $Z(G) := \{a \in G|\ ax = xa$ pentru orice $x \in G\}$ este un subgrup al lui G numit *centrul lui* G. Într-adevăr, fie $a, b \in Z(G)$ şi $x \in G$. Atunci $ax = xa$ şi $bx = xb$, deci $abx = axb = xab$ şi $a^{-1}x = xa^{-1}$, aşadar $ab, a^{-1} \in H$.

Dacă $n \geq 1$, $U_n = \{z \in \mathbf{C}|\ z^n = 1\}$ este un subgrup al lui $\mathbf{C}^*$. Într-adevăr, dacă $x, y \in U_n$, atunci $(xy^{-1})^n = x^n(y^n)^{-1} = 1$, deci $xy^{-1} \in U_n$.

Pentru fiecare $n \in \mathbf{N}$, notăm cu $n\mathbf{Z}$ mulţimea multiplilor întregi ai lui n, adică $n\mathbf{Z} = \{nk|\ k \in \mathbf{Z}\}$.

Teorema 25 *Subgrupurile lui* $(\mathbf{Z}, +)$ *sunt submulţimile* $n\mathbf{Z}$, $n \in \mathbf{N}$.

Demonstraţie. Faptul că $n\mathbf{Z}$ este un subgrup al lui $(\mathbf{Z}, +)$ rezultă din faptul că diferenţa a doi multipli de n este tot un multiplu de n. Reciproc, fie H un subgrup al lui $(\mathbf{Z}, +)$. Dacă $H = \{0\}$, atunci $H = 0\mathbf{Z}$. Presupunem că $H \neq \{0\}$. Deoarece $m \in H$ implică $-m \in H$, rezultă că în H există numere naturale nenule şi fie n cel mai mic dintre acestea. Arătăm că $H = n\mathbf{Z}$. Incluziunea $n\mathbf{Z} \subseteq H$ rezultă din faptul că $n \in H$. Reciproc, fie $h \in H$ şi fie $h = nq + r$, $q, r \in \mathbf{Z}$, $0 \leq r < n$ împărţirea lui cu rest a lui h la n. Cum $h, n \in H$, rezultă că $r = h - nq \in H$, deci $r = 0$, altfel se contrazice alegerea lui n. Deci $h = nq \in n\mathbf{Z}$. $\bullet$

Teorema 26 *Fie* G *un grup. Dacă* H, K *sunt subgrupuri ale lui* G, *atunci şi* $H \cap K$ *este subgrup. Mai general, intersecţia unei familii de subgrupuri este tot un subgrup.*

Demonstraţie. Dacă $x, y \in H \cap K$, atunci $x, y \in H$ şi $x, y \in K$, deci $xy^{-1} \in H \cap K$. Afirmaţia generală se probează analog. $\bullet$

Teorema 27 *Fie* $f : G \to G'$ *un morfism de grupuri.*

(a) *Dacă* H *este un subgrup al lui* G, *atunci* $f(H)$ *este un subgrup al lui* G' *numit* imaginea directă *a lui* H.

(b) *Dacă* H' *este un subgrup al lui* G', *atunci* $f^{-1}(H')$ *este un subgrup al lui* G *numit* pre-imaginea *sau* imaginea inversă *a lui* H'.

(c) $ker(f) := f^{-1}(1)$ *este un subgrup al lui* G' *numit* nucleul lui f *şi* f *este injectiv* $\Leftrightarrow ker(f) = \{1\}$.

Demonstraţie. (a). Fie $x, y \in H$. Atunci $f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(H)$. (b). Fie $x, y \in f^{-1}(H')$. Atunci $f(x), f(y) \in H'$ şi $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} \in H'$. Deci $xy^{-1} \in f^{-1}(H')$. (c).

$ker(f)$ este pre-imaginea subgrupului trivial al lui G', deci este subgrup al lui G cf. (b). E clar că dacă f este injectiv atunci $ker(f) = \{1\}$. Reciproc, presupunem că $ker(f) = \{1\}$ şi fie $x, y \in G$ cu $f(x) = f(y)$. Atunci $1 = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$, adică $xy^{-1} \in ker(f) = \{1\}$, deci $x = y$. •

De exemplu, nucleul morfismului de grupuri $f : \mathbf{Z}^2 \to \mathbf{Z}$, $f(x, y) = x - y$ este $\{(x, x) |\ x \in \mathbf{Z}\}$.

3.4 Subgrupul generat de o mulţime

Fie G un grup şi A o submulţime a lui G. *Subgrupul lui G generat de A* este prin definiţie

$$< A >:= \{a_1^{\pm 1} a_2^{\pm 1} \cdots a_n^{\pm 1} |\ a_1, ..., a_n \in A, n \geq 0\}$$

altfel zis, mulţimea tuturor produselor de elemente din A şi inverse ale acestora. Facem convenţia ca un produs vid să însemne 1. E clar că $A \subseteq < A >$. Se observă că $< \emptyset >= \{1\}$ şi $< G >= G$. Dacă $a \in G$, atunci $< a >= \{a^k |\ k \in \mathbf{Z}\}$. Un subgrup de această formă e numit *subgrup ciclic*. Teorema 25 afirmă că toate subgrupurile lui $(\mathbf{Z}, +)$ sunt ciclice.

Teorema 28 *Fie G un grup şi A o submulţime a sa. Atunci $< A >$ este un subgrup al lui G conţinut în orice subgrup al lui G care conţine pe A (adică, $A \subseteq H \leq G$ implică $< A >\subseteq H$).*

Demonstraţie. Din definiţia lui $< A >$ rezultă că $< A >$ este parte stabilă a lui G şi că $1 \in< A >$. Fie $x \in< A >$. Atunci $x = a_1^{e_1} \cdots a_n^{e_n}$ cu $a_1, ..., a_n \in A$, $e_1, ..., e_n \in \{\pm 1\}$ şi $n \geq 0$. Atunci $x^{-1} = a_n^{-e_n} \cdots a_1^{-e_1} \in< A >$. Fie H un subgrup al lui G ce conţine pe A. Dacă $x_1, ..., x_n \in A$, atunci $x_1^{\pm 1} x_2^{\pm 1} \cdots x_n^{\pm 1} \in H$, din definiţia subgrupului. Deci $< A >\subseteq H$. •

Corolarul 29 *Fie G un grup şi A o submulţime a lui G. Atunci subgrupul generat de A este intersecţia tuturor subgrupurilor lui G care conţin pe A, adică*

$$< A >= \bigcap_{A \subseteq H \leq G} H.$$

Expresia lui $< A >$ din corolarul precedent poarte fi luată drept definiţie a lui $< A >$.

Corolarul 30 *Fie G un grup şi $a_1, ..., a_n \in G$ astfel încât $a_i a_j = a_j a_i$ pentru orice i, j (e.g., dacă G este abelian). Atunci*

$$< a_1, ..., a_n >= \{a_1^{k_1} \cdots a_n^{k_n} |\ k_1, ..., k_n \in \mathbf{Z}\}.$$

De exemplu, dacă $a, b \in (\mathbf{Z}, +)$, atunci $< a, b >= a\mathbf{Z} + b\mathbf{Z}$.

Corolarul 31 *Fie a, b, d, m numere naturale. Atunci*
(a) $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z} \Leftrightarrow d = cmmdc(a, b)$.
(b) $a\mathbf{Z} \cap b\mathbf{Z} = m\mathbf{Z} \Leftrightarrow m = cmmmc(a, b)$.

Demonstraţie. (a). Conform teoremei, există $d \in \mathbf{N}$ astfel încât $a\mathbf{Z}+b\mathbf{Z} = d\mathbf{Z}$. Deci $a, b \in d\mathbf{Z}$, adică d este divizor comun al lui a şi b. Fie f un divizor comun al lui a şi b. Atunci $a, b \in f\mathbf{Z}$, deci $d\mathbf{Z} = a\mathbf{Z} + b\mathbf{Z} \subseteq f\mathbf{Z}$, şi rezultă că f divide d. Afirmaţia (b) se probează analog. $\bullet$

Spunem că grupul G este *generat de submulţimea* A, sau că A este un *sistem de generatori pentru* G, dacă $G =< A >$. Un grup se zice *ciclic* dacă este generat de o submulţime cu un singur element. De exemplu, $\mathbf{Z}$ este ciclic. Un grup ciclic este abelian. Într-adevăr, dacă $G =< a >$, atunci elementele lui G sunt de forma a^k şi $a^k a^l = a^{k+l} = a^l a^k$.

Grupul permutărilor S_3 este generat de (12) şi (13), deoarece (23) = (12)(13)(12), (123) = (13)(12) şi (132) = (12)(13). Cum S_3 nu este abelian, el nu este ciclic. Grupul $(\mathbf{Z}^2, +)$ este generat de $(1, 0)$ şi $(0, 1)$ deoarece $(a, b) = a(1, 0) + b(0, 1)$. Pe de altă parte, el nu este ciclic. Într-adevăr, dacă $\mathbf{Z}^2 =< (c, d) >$, atunci există m, n întregi astfel încât $(1, 0) = m(c, d)$ şi $(0, 1) = n(c, d)$. Rezultă că $c = d = 0$, contradicţie.

Un grup G se zice *finit generat* dacă poate fi generat de o submulţime finită a sa. Evident că un grup finit este finit generat. Grupul $(\mathbf{Q}, +)$ nu este finit generat. Într-adevăr, să presupunem că $\mathbf{Q} =< a_1/b_1, ..., a_k/b_k >$ cu $a_i, b_i \in \mathbf{Z}$, $b_i > 0$. Fie $n = max(b_1, ..., b_k)$. Cum $a_i/b_i \in< 1/n! >$, rezultă că $\mathbf{Q} =< 1/n! >$. Dar $1/(n + 1)! \notin< 1/n! >$, deoarece $1/(n + 1)! = a/n!$ cu a întreg implică $a = 1/(n + 1)$, contradicţie.

3.5 Congruenţe modulo un subgrup

Conform teoremei 25, subgrupurile lui $(\mathbf{Z},+)$ sunt submulţimile $n\mathbf{Z}$ cu n număr natural. Dacă $a,b\in\mathbf{Z}$, atunci $a\equiv b(n)\Leftrightarrow n\mid a-b\Leftrightarrow a-b\in n\mathbf{Z}$.

Această observaţie permite extinderea noţiunii de congruenţă la grupuri arbitrare. Fie G un grup şi H un subgrup al lui G. Pe G definim următoarele relaţii: $x\equiv_s y(H)\Leftrightarrow x^{-1}y\in H$ numită *congruenţa la stânga modulo H* şi $x\equiv_d y(H)\Leftrightarrow xy^{-1}\in H$ numită *congruenţa la dreapta modulo H*.

Teorema 32 *Fie G un grup şi H un subgrup al lui G. Atunci cele două congruenţe modulo H sunt relaţii de echivalenţă pe G. Clasele de echivalenţă ale congruenţei la stânga sunt submulţimile lui G de forma $xH=\{xh|\ h\in H\}$ cu $x\in G$, numite* clase la stânga modulo H. *Clasele de echivalenţă ale congruenţei la dreapta sunt submulţimile lui G de forma $Hx=\{hx|\ h\in H\}$ cu $x\in G$, numite* clase la dreapta modulo H.

Demonstraţie. Demonstrăm afirmaţiile doar pentru congruenţa la stânga modulo H, cele pentru congruenţa la dreapta probându-se analog. Fie $x,y,z\in G$. Avem $x\equiv_s x(H)$ deoarece $x^{-1}x=1\in H$. Dacă $x\equiv_s y(H)$, atunci $x^{-1}y\in H$, deci $y^{-1}x=(x^{-1}y)^{-1}\in H$, adică $y\equiv_s x(H)$. Presupunem că $x\equiv_s y(H)$ şi $y\equiv_s z(H)$. Rezultă că $x^{-1}y\in H$ şi $y^{-1}z\in H$. Deci $x^{-1}z=(x^{-1}y)(y^{-1}z)\in H$, adică $x\equiv_s z(H)$. Am verificat aşadar că $\equiv_s(H)$ este reflexivă, simetrică şi tranzitivă. Clasa de echivalenţă a lui x constă din toate elementele y cu $x\equiv_s y(H)$. Dar $x\equiv_s y(H)\Leftrightarrow x^{-1}y\in H\Leftrightarrow y\in xH$. •

Vom nota cu $(G/H)_s$ (resp. $(G/H)_d$) mulţimea claselor la stânga (resp. la dreapta) modulo H. Cele două relaţii de congruenţă coincid dacă şi numai dacă au aceleaşi clase de echivalenţă, adică, dacă şi numai dacă $xH=Hx$ pentru orice $x\in G$. În acest caz se spune că H este un *subgrup normal* al lui G. Este clar că toate subgrupurile unui grup abelian sunt normale. Când H este subgrup normal, mulţimea $(G/H)_s=(G/H)_d$ se notează mai simplu cu G/H.

Teorema 33 *Fie G un grup şi H un subgrup al lui său. Atunci mulţimile $(G/H)_s$ şi $(G/H)_d$ sunt echipotente. Cardinalul comun al celor două mulţimi se numeşte indicele lui H în G şi se notează cu $[G:H]$.*

Demonstraţie. Fie $f:G\to G$, $f(x)=x^{-1}$. E clar că $ff=I_G$, deci f este bijecţie. Dacă $h\in H$ şi $a\in G$, rezultă că $f(ah)=h^{-1}a^{-1}$. Deci

$f(aH) = Ha^{-1}$ pentru orice $a \in G$. Cum $(G/H)_s$ şi $(G/H)_d$ sunt partiţii ale lui G, rezultă că aplicaţia $aH \mapsto Ha^{-1} : (G/H)_s \to (G/H)_d$ este bijectivă. •

În S_3 considerăm subgrupul $H = \{I, (12)\}$. Clasele la stânga modulo H sunt $1 \cdot H = H$, $(13)H = \{(13), (123)\}$ şi $(23)H = \{(23), (132)\}$ în timp ce clasele la dreapta modulo H sunt $H \cdot 1 = H$, $H(13) = \{(13), (132)\}$ şi $H(23) = \{(23), (123)\}$. Deci $[S_3 : H] = 3$ şi cele două congruenţe modulo H sunt diferite, adică H nu este subgrup normal al lui S_3.

Fie $n \geq 1$. Cum clasele de congruenţă modulo n sunt $\{\widehat{0}, ..., \widehat{n-1}\}$, deducem că $[\mathbf{Z} : n\mathbf{Z}] = n$.

Pe de altă parte $[\mathbf{Q} : \mathbf{Z}] = \infty$. Într-adevăr, dacă $\mathbf{Q}/\mathbf{Z} = \{x_1 + \mathbf{Z}, ..., x_n + \mathbf{Z}\}$, atunci $\mathbf{Q} =< x_1, ..., x_n, 1 >$, contradicţie.

Teorema 34 (Teorema lui Lagrange). *Fie G un grup finit şi H un subgrup al lui său. Atunci*

$$|G| = |H|[G : H].$$

În particular, $|H|$ divide $|G|$.

Demonstraţie. Fie C_1,...,C_s clasele la stânga modulo H. Conform definiţiei, $s = [G : H]$. Fie $a \in G$. Aplicaţia $x \mapsto ax : H \to aH$ este o bijecţie cu inversa $y \mapsto a^{-1}y$. Deci $|C_i| = |H|$ pentru $i = 1, ..., s$. Cum C_1,...,C_s este o partiţie a lui G, rezultă

$$|G| = \sum_{i=1}^{s} |C_i| = \sum_{i=1}^{s} |H| = |H|[G : H]. \quad \bullet$$

3.6 Ordinul unui element într-un grup

Fie G un grup şi x un element al lui G. Ordinul lui x se defineşte prin

$$ord(x) = \begin{cases} \infty & \text{dacă } \ x^n \neq 1 \text{ pentru orice } n \geq 1 \\ min\{n \in \mathbf{N}^* |\ x^n = 1\} & \text{dacă } \ \text{există } n \geq 1 \text{ cu } x^n = 1. \end{cases}$$

E clar că 1_G are ordinul 1. În grupul multiplicativ $\{\pm 1, \pm i\}$, avem $ord(i) = 4$ deoarece $i \neq 1$, $i^2 = -1$, $i^3 = -i$ şi $i^4 = 1$. De asemenea, orice element nenul al grupului $(\mathbf{Z}, +)$ are ordinul infinit.

Teorema 35 *Fie G un grup şi x un element al lui G de ordin finit $= n$. Dacă $k \in \mathbf{Z}$, atunci $x^k = 1$ dacă şi numai dacă n divide k.*

Demonstraţie. Dacă n divide k, atunci $k = nq$ cu $q \in \mathbf{Z}$, deci $x^k = (x^n)^q = 1$, deoarece $x^n = 1$. Reciproc, presupunem că $x^k = 1$. Fie $k = nq+r$, $q, r \in \mathbf{Z}$, $0 \leq r < n$ împărţirea cu rest a lui k la n. Atunci $1 = x^k = x^{nq+r} = (x^n)^q x^r = x^r$, deci $r = 0$, cf. definiţiei ordinului. •

În grupul $(\mathbf{C}^*, \cdot)$, elementele de ordin finit sunt rădăcinile unităţii, adică rădăcinile ecuaţiilor de forma $z^n = 1$, $n \geq 1$. Pentru n fixat, ele se pot reprezenta sub formă trigonometrică

$$\theta_k = cos(2k\pi/n) + i\sin(2k\pi/n), \qquad 0 \leq k \leq n-1.$$

Se vede că $ord(\theta_1) = n$. Mai general, $ord(\theta_k) = n/(k, n)$, unde $d = (k, n)$ este cmmdc al lui k şi n. Într-adevăr, $\theta_k^s = 1 \Leftrightarrow \theta_1^{sk} = 1 \Leftrightarrow n \mid sk \Leftrightarrow n/d \mid sk/d$ $\Leftrightarrow n/d \mid s$, deoarece $(n/d, k/d) = 1$.

Teorema 36 *Fie G un grup şi x un element al lui G. Atunci ordinul lui x este egal cu ordinul subgrupului generat de x.*

Demonstraţie. Presupunem că $ord(x) = \infty$. Atunci pentru orice numere întregi $h < k$, rezultă $x^k \neq x^h$, altfel $x^{k-h} = 1$. Deci subgrupul $< x >= \{x^k \mid k \in \mathbf{Z}\}$ este infinit.

Presupunem acum că $ord(x) = n < \infty$. Fie $k \in \mathbf{Z}$ şi fie $k = nq + r$, $q, r \in \mathbf{Z}$, $0 \leq r < n$ împărţirea cu rest a lui k la n. Atunci $x^k = x^{nq+r} = (x^n)^q x^r = x^r$. Deci $< x >= \{1, x, ..., x^{n-1}\}$. Mai mult, aceste elemente sunt distincte deoarece din $x^k \neq x^h$ cu $0 \leq h < k \leq n-1$, rezultă $x^{k-h} = 1$ cu $1 \leq k - h \leq n - 1$, contradicţie, deoarece $ord(x) = n$. •

Corolarul 37 *Fie G un grup finit cu n elemente şi $x \in G$. Atunci $ord(x)$ divide n şi $x^n = 1$.*

Demonstraţie. $ord(x) = | < x > |$ divide G, cf. teoremei lui Lagrange. •

Reamintim că *indicatorul lui Euler* este funcţia $\varphi : \mathbf{N}^* \to \mathbf{N}^*$, $\varphi(n) =$ numărul întregilor $1 \leq k \leq n$ primi cu n (vezi ex. 15). De exemplu, $\varphi(12) = |\{1, 5, 7, 11\}| = 4$. $\varphi(n)$ este egal cu ordinul grupului multiplicativ $U(\mathbf{Z}_n) = \{\widehat{b} \in \mathbf{Z}_n \mid (b, n) = 1\}$. Aplicând corolarul precedent se obţine

Corolarul 38 (Teorema lui Euler). *Fie $a, n \geq 1$ numere naturale relativ prime. Atunci*

$$a^{\varphi(n)} \equiv 1 \ (mod\ n).$$

În cazul când n este număr prim se obţine

Corolarul 39 (Mica teoremă a lui Fermat). *Fie p un număr prim şi a un număr natural nedivizibil cu p. Atunci*

$$a^{p-1} \equiv 1 \ (mod\ p).$$

3.7 Subgrupuri normale

Fie G un grup şi H un subgrup al lui G. Reamintim că H se numeşte subgrup normal al lui G dacă $xH = Hx$ pentru orice $x \in G$.

Teorema 40 *Fie G un grup şi H un subgrup al lui său. Atunci H este un subgrup normal al lui G dacă şi numai dacă $xhx^{-1} \in H$ pentru orice $x \in G$ şi $h \in H$ (adică, $xHx^{-1} \subseteq H$ pentru orice $x \in G$).*

Demonstraţie. $\Rightarrow$. Fie $x \in H$. Cum H este normal, rezultă că $xH = Hx$, deci $xHx^{-1} \subseteq H$. $\Leftarrow$. Fie $x \in H$. Din ipoteza, rezultă că $xHx^{-1} \subseteq H$, deci $xH \subseteq Hx$. Refăcând raţionamentul pentru x^{-1}, se obţine $Hx \subseteq xH$, deci $xH = Hx$. $\bullet$

$H = \{I, (12)\}$ nu este subgrup normal al lui S_3 deoarece $(13)(12)(13)^{-1} = (23)$. $K = \{I, (12)(34), (13)(24), (14)(23)\}$ este subgrup normal al lui S_4 deoarece $\sigma\alpha\sigma^{-1} \in K$ pentru orice $\sigma \in S_4$, de exemplu $\sigma(12)(34)\sigma^{-1} = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4)) \in K$.

Alte exemple de subgrupuri normale sunt date de rezultatul următor.

Teorema 41 *Fie G un grup. (a) Dacă $f : G \to G'$ este un morfism de grupuri, atunci $ker(f)$ este un subgrup normal al lui G.*

(b) Orice subgrup al lui $Z(G)$ este un subgrup normal al lui G.

(c) Orice subgrup de indice 2 este normal.

Demonstraţie. (a). Fie $x \in G$ şi $y \in ker(f)$. Atunci $f(xyx^{-1}) = f(x)f(y)f(x)^{-1} = f(x)f(x)^{-1} = 1$, deci $xyx^{-1} \in ker(f)$.

(b). Fie H un subgrup al lui $Z(G)$, $x \in H$ şi $y \in ker(f)$. Atunci $xyx^{-1} = xx^{-1}y = y \in H$.

(c). Fie H un subgrup de indice 2 al lui G. Cum $[G : H] = 2$, atât clasele la stânga modulo H cât şi cele la dreapta sunt H şi $G \setminus H$. •

3.8 Grupul factor

Fie G un grup şi H un subgrup normal al lui G. Dacă $x \in G$, notăm $\widehat{x} = xH = Hx$ clasa lui x modulo H. Notăm $G/H = \{\widehat{x}|\ x \in G\}$. Pe G/H introducem operaţia definită prin $\widehat{x}\widehat{y} = \widehat{xy}$ pentru orice $x, y \in G$.

Operaţia este bine-definită, adică nu depinde de reprezentanţii claselor. Într-adevăr, fie $x', y' \in G$ cu $\widehat{x} = \widehat{x'}$ şi $\widehat{y} = \widehat{y'}$. Atunci $h = x^{-1}x'$ şi $y^{-1}y'$ aparţin lui H. Cum $y'H = Hy'$, există $h' \in H$ cu $hy' = y'h'$. Deci $(xy)^{-1}(x'y') = y^{-1}x^{-1}x'y' = y^{-1}hy' = y^{-1}y'h' \in H$. Rezultă că $\widehat{xy} = \widehat{x'y'}$.

Teorema 42 *Fie G un grup şi H un subgrup normal al lui G. Atunci în raport cu operaţia definită anterior G/H este grup numit* grupul factor G modulo H. *În plus, surjecţia canonică $\pi : G \to G/H$ este morfism de grupuri.*

Demonstraţie. Faptul că G/H este grup rezultă din egalităţile Fie $x, y, z \in G$. Atunci $(\widehat{x}\widehat{y})\widehat{z} = \widehat{xy}\widehat{z} = \widehat{xyz} = \widehat{x}\widehat{yz} = \widehat{x}(\widehat{y}\widehat{z})$, probând astfel asociativitatea. De asemenea, $\widehat{x}\widehat{1} = \widehat{x1} = \widehat{x} = \widehat{1}\widehat{x}$, deci $\widehat{1}$ este element neutru. Apoi, $\widehat{x}\widehat{x^{-1}} = \widehat{xx^{-1}} = \widehat{1} = \widehat{x^{-1}}\widehat{x}$, deci orice element al lui G/H este inversabil. În fine, $\pi(x)\pi(y) = \widehat{x}\widehat{y} = \widehat{xy} = \pi(xy)$. •

Fie $n \geq 1$. Grupul factor $\mathbf{Z}/n\mathbf{Z}$ este chiar grupul $\mathbf{Z}_n$ definit după teorema 17. În S_3, $A_3 = \{I, (123), (132)\}$ este un subgrup de indice 2, deci normal cf. teoremei 41. Avem $S_3/A_3 = \{\widehat{I}, \widehat{(12)}\}$ cu $\widehat{(12)}^2 = \widehat{I}$.

Teorema 43 (Teorema fundamentală de izomorfism.) *Fie $u : G \to H$ un morfism de grupuri. Atunci grupul factor $G/ker(u)$ este izomorf cu $Im(u)$. Mai precis, avem izomorfismul de grupuri*

$$\bar{u} : G/ker(u) \to Im(u), \quad \bar{u}(\hat{x}) = u(x), \quad x \in G.$$

Demonstraţie. Verificăm mai întâi buna definire a lui $\bar{u}$. Fie $x, y \in G$ cu $\hat{x} = \hat{y}$. Atunci există $k \in ker(u)$ astfel încât $x = ky$. Rezultă că $u(x) = u(ky) = u(k)u(y) = u(y)$. Deci funcţia $\bar{u}$ este bine-definită. Evident, $\bar{u}$ este surjectivă. Fie $y, z \in G$. Atunci

$$\bar{u}(\widehat{y}\widehat{z}) = \bar{u}(\widehat{yz}) = u(yz) = u(y)u(z) = \bar{u}(\widehat{y})\bar{u}(\widehat{z})$$

deci $\bar{u}$ este morfism de grupuri. În fine, din $\widehat{x} \in ker(\bar{u})$, rezultă $1 = \bar{u}(\widehat{x}) = u(x)$, deci $x \in ker(u)$, adică $\widehat{x} = \widehat{1}$. Deci $\bar{u}$ este morfism injectiv, cf. teoremei 27. •

Morfismul de grupuri $f : (\mathbf{R}, +) \to (\mathbf{C}^*, \cdot)$, $f(x) = \cos(2\pi x) + i\,\sin(2\pi x)$, are imaginea $U = \{z \in \mathbf{C} |\ |z| = 1\}$ (cercul unitate) şi nucleul $ker(f) = \mathbf{Z}$, deci $\mathbf{R}/\mathbf{Z}$ este izomorf cu U, cf. teoremei fundamentale de izomorfism.

3.9 Grupuri ciclice

Teorema 44 (Teorema de structură a grupurilor ciclice.) *Orice grup ciclic infinit este izomorf cu* $\mathbf{Z}$ *şi orice grup ciclic cu n elemente este izomorf cu* $\mathbf{Z}_n$.

Demonstraţie. Fie $G =< a >$ un grup ciclic. Considerăm morfismul surjectiv de grupuri $f : \mathbf{Z} \to G$, $f(k) = a^k$. Dacă G este infinit, rezultă că f este izomorfism. Presupunem acum că G are n elemente. Din teoremele 35 şi 36 rezultă că $ker(f) = n\mathbf{Z}$, deci G este izomorf cu $\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}_n$, cf. teoremei fundamentale de izomorfism. •

Corolarul 45 *Orice subgrup sau grup factor al unui grup ciclic este de asemenea grup ciclic.*

Demonstraţie. E clar că un grup factor al unui grup ciclic este ciclic (dacă G este generat de a, atunci G/H este generat de $\widehat{a}$). Conform teoremei anterioare, este suficient să demonstrăm afirmaţia referitoare la subgrupuri pentru grupurile $\mathbf{Z}$ şi $\mathbf{Z}_n$. În cazul $\mathbf{Z}$ se aplică teorema 25. Considerăm cazul $\mathbf{Z}_n$. Fie $\pi : \mathbf{Z} \to \mathbf{Z}_n$ morfismul canonic. Fie H este un subgrup al lui $\mathbf{Z}_n$. Atunci $\pi^{-1}(H)$ este un subgrup al lui $\mathbf{Z}$ care-l conţine pe $ker(\pi) = n\mathbf{Z}$, deci $\pi^{-1}(H) = k\mathbf{Z}$ cu k divizor al lui n. Cum π este surjecţie, avem $H = \pi(\pi^{-1}(H))$ = subgrupul generat de $\widehat{k}$. •

Corolarul 46 *Fie p un număr prim. Atunci orice grup finit de ordin p este ciclic, deci izomorf cu $\mathbf{Z}_p$.*

Demonstraţie. Fie G un grup de ordin p, fie $x \in G \setminus \{1\}$ şi $H =< x >$. Atunci $|H| > 1$ şi se divide cu p, deci $G =< x >$. Se aplică teorema 44. •

3.10 Grupul permutărilor S_n

Fie A o mulţime nevidă. Reamintim că S_A este grupul permutărilor mulţimii A, grup faţă de compunerea permutărilor. Dacă A şi B sunt două mulţimi echipotente, atunci grupurile S_A şi S_B sunt izomorfe, cf. exerciţiului 53.

În particular, grupul permutărilor unei mulţimi finite cu n elemente este izomorf cu grupul permutărilor mulţimii $\{1, 2, ..., n\}$, grup pe care îl notăm cu S_n şi-l numim *grupul permutărilor de grad n*. Conform exerciţiului 12 (b), S_n are $n!$ elemente.

Fie $n \geq 1$ şi $a_1, ..., a_k$ numere distincte între 1 şi n. Reamintim că ciclul $(a_1, ..., a_k)$ este permutarea din S_n definită prin $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_n \mapsto a_1$ şi $x \mapsto x$ pentru $x \neq a_i$. Numărul k se numeşte *lungimea ciclului.* Ciclurile de lungime 1 se numesc *cicluri triviale* iar cele de lungime 2 *transpoziţii.*

Grupul S_n este abelian dacă şi numai dacă $n \leq 2$, deoarece S_1 şi S_2 sunt grupuri abeliene, iar dacă $n \geq 3$, atunci $(12)(13) = (132) \neq (123) = (13)(12)$.

Teorema 47 (Cayley.) *Orice grup cu n elemente este izomorf cu un subgrup al grupului permutărilor S_n.*

Demonstraţie. Fie G un grup cu n elemente. Deoarece S_n este izomorf cu S_G, este suficient să arătăm că G este izomorf cu un subgrup al grupului permutărilor S_G. Pentru fiecare $g \in G$, considerăm aplicaţia $t_g : G \to G$, $t_g(x) = gx$. Dacă $g, h, x \in G$, atunci $(t_g t_h)(x) = ghx = t_{gh}(x)$. În particular, t_g este bijecţie deoarece $t_g t_{g^{-1}} = I_G$. Aplicaţia $T : G \to S_G$, $T(g) = t_g$, este un morfism injectiv de grupuri. Într-adevăr, $T(g)T(h) = t_g t_h = t_{gh} = T(gh)$ şi $ker(T) = \{g |\ t_g = I_G\} = \{1\}$. Deci G este izomorf cu subgrupul $Im(T)$ al lui S_G. •

Morfismul injectiv T se numeşte *scufundarea Cayley* a lui G în S_G. Pentru grupul lui Klein $K = \{1, a, b, c\}$ scufundarea Cayley este $T(1) = I$, $T(a) = \begin{pmatrix} 1 & a & b & c \\ a & 1 & c & b \end{pmatrix}$, $T(b) = \begin{pmatrix} 1 & a & b & c \\ b & c & 1 & a \end{pmatrix}$, $T(c) = \begin{pmatrix} 1 & a & b & c \\ c & b & a & 1 \end{pmatrix}$.

Spunem că două permutări α şi β sunt *disjuncte* dacă pentru orice $i \in \{1, ..., n\}$ rezultă $\alpha(i) = i$ sau $\beta(i) = i$. În particular, ciclurile $(a_1, ..., a_k)$, $(b_1, ..., b_l)$ sunt disjuncte $\Leftrightarrow \{a_1, ..., a_k\} \cap \{b_1, ..., b_l\} = \emptyset$.

Lema 48 *Fie $\alpha, \beta \in S_n$ permutări disjuncte. Atunci*
(1) $\alpha\beta = \beta\alpha$.
(2) *Dacă $\alpha\beta = I$, atunci $\alpha = \beta = I$.*
(3) *α^s, β^t sunt disjuncte pentru orice $s, t \geq 1$.*
(4) *Dacă $(\alpha\beta)^p = 1$, atunci $\alpha^p = \beta^p = I$.*

Demonstraţie. (1), (2). Putem presupune că $\alpha, \beta \neq I$. Fie $i \in \{1, ..., n\}$. Dacă $\alpha(i) = \beta(i) = i$, atunci $(\alpha\beta)(i) = i = (\beta\alpha)(i)$. Presupunem că $j = \alpha(i) \neq i$. Cum α este injecţie, rezultă că $\alpha(j) \neq j$. Deoarece α, β sunt permutări disjuncte, $\beta(i) = i$ şi $\beta(j) = j$. Deci $(\alpha\beta)(i) = \alpha(i) = j = \beta(j) = (\beta\alpha)(i)$. Rezultă şi că $\alpha\beta \neq I$. Cazul $\beta(i) \neq i$ se tratează analog. (3). Dacă $\alpha^s(i) \neq i$, atunci $\alpha(i) \neq i$, deci $\beta(i) = i$ şi $\beta^t(i) = i$. (4) rezultă din punctele anterioare. •

Teorema 49 *Orice permutare $\sigma \in S_n$ se scrie ca produs de cicluri disjuncte, scrierea fiind unică până la ordinea ciclurilor.*

Demonstraţie. Fie $\sigma \in S_n$. Pe mulţimea $\{1, ..., n\}$ considerăm relaţia de echivalenţă $x \sim y$ dacă există k întreg cu $\sigma^k(x) = y$. Clasele de echivalenţă $\{a_{11}, ..., a_{1k_1}\}$, $\{a_{21}, ..., a_{2k_2}\}$, ..., $\{a_{s1}, ..., a_{sk_s}\}$, numite şi *orbitele lui σ*, formează o partiţie a mulţimii $\{1, ..., n\}$. Dacă $x \in \{1, ..., n\}$ şi k este cel mai mic întreg ≥ 1 astfel încât $\sigma^k(x) = x$, atunci orbita lui x este $\{x, \sigma(x), ..., \sigma^{k-1}(x)\}$ (elemente distincte, altfel se contrazice minimalitatea lui k).

Rezultă că, schimbând eventual notaţia în interiorul fiecărei orbite, putem presupune că $a_{i1} = \sigma^{k_i}(a_{ik_i})$ şi $a_{ij} = \sigma(a_{ij-1})$ pentru $2 \leq j \leq k_i$ şi $1 \leq i \leq s$. Rezultă că $\sigma = (a_{11}, ..., a_{1k_1}) \cdots (a_{s1}, ..., a_{sk_s})$.

Probăm acum unicitatea. Fie $\sigma = (b_{11}, ..., b_{1p_1}) \cdots (b_{t1}, ..., b_{tp_t})$ o altă scriere a lui σ ca produs cicluri disjuncte. Rezultă că $\{b_{11}, ..., b_{1p_1}\}$,...,$\{b_{t1}, ..., b_{tp_t}\}$ sunt orbitele lui σ, deci $s = t$. Conform lemei precedente ciclurile disjuncte comută, deci putem presupune că $\{a_{11}, ..., a_{1k_1}\} = \{b_{11}, ..., b_{1p_1}\}$,..., $\{a_{s1}, ..., a_{sk_s}\} = \{b_{s1}, ..., b_{sp_s}\}$ şi că $a_{11} = b_{11}$,...,$a_{s1} = b_{s1}$. Rezultă atunci că $(a_{11}, ..., a_{1k_1}) = (b_{11}, ..., b_{1p_1})$,..., $(a_{s1}, ..., a_{sk_s}) = (b_{s1}, ..., b_{sp_s})$. •

De exemplu, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 2 & 1 & 9 & 3 & 5 & 7 & 8 \end{pmatrix} = (14)(263)(5987).$

Teorema 50 *Ordinul unei permutări $\sigma \in S_n$ este cel mai mic multiplu comun al lungimii ciclurilor componente.*

Demonstraţie. Dacă σ este un ciclu de lungime k, $\sigma = (a_1, ..., a_k)$, atunci $\sigma^k \neq I$ pentru $p < k$, deoarece $\sigma^k(a_1) = a_{k+1}$, şi $\sigma^p = I$, deci ordinul lui σ este k. Fie acum $\sigma = (a_{11}, ..., a_{1k_1}) \cdots (a_{s1}, ..., a_{sk_s})$ produs de cicluri disjuncte. Fie $p \geq 1$. Cum ciclurile disjuncte comută, avem $\sigma^p = (a_{11}, ..., a_{1k_1})^p \cdots (a_{s1}, ..., a_{sk_s})^p$. Conform lemei 48, $\sigma^p = I$ dacă şi numai dacă $(a_{11}, ..., a_{1k_1})^p = \cdots = (a_{s1}, ..., a_{sk_s})^p = I$, deoarece permutările $(a_{11}, ..., a_{1k_1})^p$,...,$(a_{s1}, ..., a_{sk_s})^p$ sunt disjuncte. Rezultă că $\sigma^p = I$ dacă şi numai dacă p se divide cu k_1,...,k_s. Deci ordinul lui σ este cel mai mic multiplu comun al numerelor k_1,...,k_s. •

De exemplu, ordinul permutării (14)(263)(5987) este $[2, 3, 4] = 12$.

Teorema 51 *Orice permutare $\sigma \in S_n$ se scrie ca produs de transpoziţii, altfel spus, grupul S_n este generat de mulţimea transpoziţiilor.*

Demonstraţie. Conform teoremei 49, este suficient să observăm că ciclurile se scriu ca produs de transpoziţii, de exemplu, $(a_1, a_2, ..., a_k) = (a_1, a_2)$ $(a_2, a_3) \cdots (a_{k-1}, a_k) = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_3)(a_1, a_2)$. •

Fie $\sigma \in S_n$, unde $n \geq 2$. Definim *signatura lui σ* prin

$$sgn(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}. \tag{3.1}$$

O pereche (i, j), $1 \leq i < j \leq n$ cu $\sigma(i) > \sigma(j)$ se numeşte *inversiune a lui σ*. Fie $Inv(\sigma)$ numărul inversiunilor lui σ.

Teorema 52 *Dacă $\sigma \in S_n$, $n \geq 2$, atunci $sgn(\sigma) = (-1)^{Inv(\sigma)} \in \{\pm 1\}$.*

Demonstraţie. Cum σ este bijecţie, avem

$$\prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i)) = (-1)^{Inv(\sigma)} \prod_{1 \leq i < j \leq n} |\sigma(j) - \sigma(i)| = (-1)^{Inv(\sigma)} \prod_{1 \leq i < j \leq n} (j - i).$$

Deci

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

Permutările cu signatura 1 se numesc *permutări pare* iar cele cu signatura -1 se numesc *permutări impare*. De exemplu, permutarea identică este pară deoarece nu are inversiuni, în timp ce transpoziţia (12) este impară deoarece are o singură inversiune şi anume $(1,2)$.

Fie A_n mulţimea permutărilor pare din S_n.

Teorema 53 *Fie $n \geq 2$. Aplicaţia $sgn : S_n \to \{\pm 1\}$ este un morfism surjectiv de grupuri. În particular, A_n este un subgrup normal al lui S_n, numit* subgrupul altern de grad n, *şi S_n/A_n este izomorf cu $\{\pm 1\}$, deci $|A_n| = n!/2$.*

Demonstraţie. Fie $\sigma, \tau \in S_n$. Avem

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

deoarece

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

Deci σ este un morfism surjectiv de grupuri, deoarece $\sigma(12) = -1$. Aplicând teorema fundamentală de izomorfism obţinem $S_n/A_n \simeq \{\pm 1\}$, deci $n! = |S_n| = |A_n||S_n/A_n| = 2|A_n|$. •

Aşadar, produsul a două permutări de aceeaşi paritate este o permutare pară iar produsul a două permutări de parităţi diferite este o permutare impară.

Transpoziţiile sunt permutări impare, deoarece pentru $1 \leq i < j \leq n$ putem scrie $(ij) = (1i)(2j)(12)(2j)(1i)$ şi aplicând sgn avem $sgn(ij) = (sgn(1i))^2(sgn(2j))^2 sgn(12) = -1$.

Un ciclu de lungime k, $(a_1, a_2, ..., a_k)$ are signatura $(-1)^{k-1}$, deoarece $(a_1, a_2, ..., a_k) = (a_1, a_2)(a_2, a_3)\cdots(a_{k-1}, a_k)$.

3.11 Ecuaţia claselor

Fie G un grup şi $x, y \in G$. Spunem că x, y sunt *conjugate* (notaţie $x \sim y$), dacă există $a \in G$ astfel încât $x = aya^{-1}$. Relaţia de conjugare este o relaţie de echivalenţă. Într-adevăr, fie $x, y, z, a, b \in G$. Atunci $x = 1 \cdot x \cdot 1^{-1}$, $x = aya^{-1}$ implică $y = a^{-1}y(a^{-1})^{-1}$, şi $x = aya^{-1}$ şi $y = bzb^{-1}$ implică $x = abz(ab)^{-1}$.

Clasele de echivalenţă se numesc *clasele de conjugare* ale lui G. Clasa de conjugare a $[x]$ lui x este $\{axa^{-1}|\ a \in G\}$. O clasă de conjugare $[x]$ constă dintr-un singur element (numindu-se în acest caz *trivială*) dacă şi numai dacă $x = axa^{-1}$ pentru orice $a \in G$, adică $x \in Z(G)$.

Fie G un grup finit şi $x \in G$. E uşor de văzut că $C(x) := \{a \in G|\ ax = xa\}$ este un subgrup al lui G numit *centralizatorul lui* x. Două elemente axa^{-1} şi bxb^{-1} ale lui $[x]$ sunt egale $\Leftrightarrow b^{-1}ax = xb^{-1}a \Leftrightarrow b^{-1}a \in C(x) \Leftrightarrow a, b$ sunt congruente la stânga modulo $C(x)$. Deci clasa de conjugare $[x]$ a lui x are exact $[G : C(x)]$ elemente.

Cum clasele de conjugare constituie o partiţie a lui G, rezultă că am demonstrat

Teorema 54 (Ecuaţia claselor de elemente conjugate). *Fie G un grup finit şi fie x_1,...,x_n un sistem de reprezentanţi pentru clasele de conjugare netriviale. Atunci*

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots [G : C(x_n)].$$

Teorema 55 (Teorema lui Cauchy). *Fie G un grup finit şi p un număr prim divizor al ordinului lui G. Atunci G conţine un element de ordin p.*

Demonstraţie. Facem inducţie după $|G|$. Dacă $|G| = p$, atunci orice element $x \in G \setminus \{1\}$ are ordinul p, cf. teoremei 36. Analizăm mai întâi cazul când G este abelian. Fie $x \in G \setminus \{1\}$ şi fie $H =< x >$. Dacă ordinul n al lui x se divide cu p, atunci $x^{n/p}$ este un element de ordin p. Presupunem că n nu se divide cu p, deci există a, b întregi cu $na + pb = 1$. Din teoremei lui Lagrange, ordinul grupului factor G/H se divide cu p şi $|G/H| < |G|$. Conform inducţiei, există un element $\hat{y} \in G/H$ de ordinul p. Fie $z = y^{na}$. Dacă $z = 1$, atunci $\hat{y}^{na} = \hat{1}$, deci $p =$ ordinul lui $\hat{y}$ divide na, contradicţie; deci $z \neq 1$. Pe de altă parte $z^p = (y^p)^{na} = 1$ deoarece $y^p \in H$ şi $|H| = n$.

Tratăm acum cazul general. Dacă p divide $|Z(G)|$, atunci problema se reduce la cazul anterior, deoarece $Z(G)$ este grup abelian. Presupunem că p nu divide $|Z(G)|$. Din ecuaţia claselor grupului G, rezultă că există $a \in G \setminus Z(G)$ astfel încât p nu divide $[G : C(a)]$. Din teoremei lui Lagrange rezultă că p divide $|C(a)|$. În plus, $|C(a)| < |G|$, deoarece $a \notin Z(G)$. Se aplică inducţia.

3.12 Exerciţii

46. Arătaţi că un grup G în care $x^2 = 1$ pentru orice $x \in G$ este abelian.

47. Întocmiţi tabla grupului lui Klein $\mathbf{Z}_2 \times \mathbf{Z}_2$.

48. Întocmiţi tabla grupului permutărilor S_3 în funcţie de $a = (123)$ şi $b = (12)$.

49. Arătaţi că un grup cu 4 elemente este izomorf cu $\mathbf{Z}_4$ sau cu grupul lui Klein $\mathbf{Z}_2 \times \mathbf{Z}_2$. (Indicaţie: folosiţi teorema lui Lagrange).

50. Fie G un grup şi $a, b \in G$ elemente de ordin finit m resp. n. Presupunem că $ab = ba$ şi că $(m, n) = 1$. Arătaţi că ab are ordinul mn.

51. Arătaţi că un grup cu 6 elemente este izomorf cu $\mathbf{Z}_6$ sau cu S_3. (Indicaţie: folosiţi teorema lui Cauchy).

52. Arătaţi că un grup cu 8 elemente este izomorf cu $\mathbf{Z}_8$, $\mathbf{Z}_2 \times \mathbf{Z}_4$, $\mathbf{Z}_2^3$, D_4 (grupul diedral) sau Q (grupul cuaternionilor).

53. Arătaţi că dacă A şi B sunt două mulţimi echipotente, atunci grupurile de permutări S_A şi S_B sunt izomorfe.

54. Pe mulţimea $(-1, 1)$ considerăm operaţia $x * y = (x + y)/(1 + xy)$. Arătaţi că $((-1, 1), *)$ este un grup izomorf cu $((0, \infty), \cdot)$.

55. Fie G semigrupul cu tabla de înmulţire

$\cdot$	1	a	b	c	d	e	f	g
1	1	a	b	c	d	e	f	g
a	a	b	c	1	e	f	g	d
b	b	c	1	a	f	g	d	e
c	c	1	a	b	g	d	e	f
d	d	g	f	e	1	c	b	a
e	e	d	g	f	a	1	c	b
f	f	e	d	g	b	a	1	c
g	g	f	e	d	c	b	a	1.

(a) Arătaţi că G este grup neabelian generat de $\{a, d\}$.
(b) Determinaţi clasele de conjugare şi centrul lui G.
(c) Determinaţi ordinul elementelor lui G.
(d) Determinaţi subgrupurile (normale) ale lui G.
(e) Arătaţi că $G/<b>$ este izomorf cu grupul lui Klein.

56. Arătaţi că grupul G din exerciţiul anterior este izomorf cu grupul diedral D_4.

57. Arătaţi că grupul diedral D_3 este izomorf cu S_3.

58. Arătaţi că grupul diedral D_{12} nu este izomorf cu S_4.

59. Fie Q grupul de ordinul 8, $Q = \{\pm 1, \pm i, \pm j, \pm k\}$, cu înmulţirea definită prin $ij = k$, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$, $ik = -j$ şi $i^2 = j^2 = k^2 = -1$. Determinaţi subgrupurile lui Q şi arătaţi că toate sunt subgrupuri normale. Q este numit *grupul cuaternionilor.*

60. Pe mulţimea $G = \mathbf{Z} \times \{\pm 1\}$ considerăm operaţia $(x, a)(y, b) = (x + ay, ab)$. Arătaţi că $(G, \cdot)$ este grup. Găsiţi două elemente de ordin finit $u, v \in G$ cu uv de ordin infinit.

61. Arătaţi că singurul morfism de grupuri $(\mathbf{Q}, +) \to (\mathbf{Z}, +)$ este cel nul.

62. Arătaţi că grupurile $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$ şi $(\mathbf{Q}^*, \cdot)$ sunt două câte două neizomorfe.

63. Arătaţi că orice subgrup finit generat al grupului $(\mathbf{Q}, +)$ este ciclic.

64. Găsiţi două grupuri neizomorfe G şi H astfel încât există morfisme injective $G \to H$ şi $H \to G$.

65. Arătaţi că $G = \mathbf{Z} \times \{\pm 1\}$ este grup faţă de operaţia $(a, b) * (a', b') = (a + a', bb')$. Este G grup ciclic ?

66. Fie $(p_n)_n$ şirul numerelor prime. Arătaţi că pentru orice subgrup nenul H al grupului $(\mathbf{Q}, +)$, există $q \in \mathbf{Q}^*$ şi un şir $(s_n)_n$ cu elemente din $\mathbf{N}^* \cup \{\infty\}$ astfel încât qH este subgrupul generat de mulţimea $\{1/p_n^{k_n} |\ k_n < s_n,\ n \geq 1\}$.

67. Fie p un număr prim şi fie $\mathbf{Z}[1/p]$ subgrupul lui $(\mathbf{Q},+)$ constând din toate fracţiile cu numitor putere de p. Considerăm grupul factor $\mathbf{Z}_{p^\infty} := \mathbf{Z}[1/p]/\mathbf{Z}$. Arătaţi că subgrupurile nenule şi proprii ale lui $\mathbf{Z}_{p^\infty}$ sunt ciclice de forma $<\widehat{1/p^n}>$. În plus, $\mathbf{Z}_{p^\infty}/<\widehat{1/p^n}>\simeq \mathbf{Z}_{p^\infty}$.

68. Arătaţi că $u : (\mathbf{Z}[i],\cdot) \to (\mathbf{Z}_5 \times \mathbf{Z}_5,\cdot)$, $u(a+bi) = (\widehat{a+2b}, \widehat{a-2b})$, este morfism de monoizi. Calculaţi $u((2 \pm i)^n)$, $n \geq 1$.

69. Considerăm grupul factor $G = (\mathbf{C}^*,\cdot)/\mathbf{Q}^*$. (a) Calculaţi ordinul elementelor $\widehat{1+i}$ şi $\widehat{2+i}$.

(b) Arătaţi că $arctg(1/2)/\pi \notin \mathbf{Q}^*$ şi că subgrupul generat de $\widehat{1+i}$ şi $\widehat{2+i}$ nu este ciclic.

(c) Arătaţi că G nu este finit generat.

70. Arătaţi că orice subgrup al lui $(\mathbf{Z}^2,+)$ este generat de două elemente.

71. Daţi un exemplu de grup G astfel încât $G \times G \simeq G$.

În următoarele patru exerciţii, $\mathbf{Z}[[X]]$ (resp. $\mathbf{Z}[X]$) desemnează grupul aditiv al seriilor formale (resp. polinoamelor).

72. Descrieţi morfismele de grupuri $\mathbf{Z}[X] \to \mathbf{Z}$.

73. Fie $u : \mathbf{Z}[[X]] \to \mathbf{Z}$ un morfism de grupuri. Arătaţi că există N cu $u(X^n) = 0$ pentru $n \geq N$.

74. Fie $u : \mathbf{Z}[[X]] \to \mathbf{Z}$ un morfism de grupuri care se anulează pe $\mathbf{Z}[X]$. Arătaţi că $u = 0$.

75. Pentru fiecare $i \geq 0$, fie $\pi_i : \mathbf{Z}[[X]] \to \mathbf{Z}$ morfismul de grupuri definit prin $\pi_i(\sum_n a_n X^n) = a_i$. Arătaţi că orice morfism de grupuri $u : \mathbf{Z}[[X]] \to \mathbf{Z}$ este o combinaţie liniară cu coeficienţi întregi de morfismele π_i.

76. Fie G grupul factor $(\mathbf{Q},+)/\mathbf{Z}$. Arătaţi că:

(a) dacă $a, b \in \mathbf{N}^*$ sunt prime între ele, atunci $ord(\widehat{a/b}) = b$,

(b) orice subgrup finit generat este ciclic finit,

(c) G nu este finit generat.

77. Determinaţi morfismele între grupurile aditive $\mathbf{Z}_m$ şi $\mathbf{Z}_n$.

78. Arătaţi că grupurile factor $(\mathbf{R},+)/\mathbf{Z}$ şi $(\mathbf{R},+)/<\sqrt{2},\sqrt{3}>$ nu sunt izomorfe.

79. Arătaţi că grupul factor $(\mathbf{Z}^2,+)/<(2,3)>$ este ciclic infinit iar grupul factor $(\mathbf{Z}^2,+)/<(2,2)>$ nu este ciclic.

80. Fie G grupul aditiv al şirurilor de numere reale şi H subgrupul lui G format din şirurile cu un număr finit de termeni nenuli. Arătaţi că G/H nu este izomorf cu G.

81. Arătaţi că automorfismele unui grup formează grup faţă de compunere şi că grupul automorfismelor grupului lui Klein este izomorf cu S_3.

82. Fie G un grup şi $x \in G$ un element de ordin finit n. Arătaţi că pentru orice k natural, ordinul lui x^k este $n/(n,k)$.

83. Scrieţi subgrupurile lui $\mathbf{Z}_{12}$ şi calculaţi grupurile factor ale lui $\mathbf{Z}_{12}$.

84. Arătaţi că subgrupurile finite ale lui $(\mathbf{C}^*,\cdot)$ sunt ciclice.

85. Fie G subgrupul grupului permutărilor lui $\mathbf{R}$ generat de T şi D, unde $T(x)=x+1$ şi $D(x)=2x$. Arătaţi că G posedă un subgrup care nu este finit generat.

86. Arătaţi că $S_4/H \simeq S_3$ unde $H=\{I,(12)(34),(13)(24),(14)(23)\}$.

87. Calculaţi signatura şi ordinul elementelor lui S_5.

88. Determinaţi morfismele de grupuri $S_3 \to \{\pm 1,\cdot\}$.

89. Calculaţi elementele subgrupului D generat de (1234) şi (13) în S_4.

90. Calculaţi elementele subgrupului H generat de (1234)(5678) şi (1537) (2846) în S_8 şi arătaţi că H este izomorf cu grupul cuaternionilor (vezi ex. 59).

91. Arătaţi că S_n este generat de (a) transpoziţiile (12), (13), ...,($1n$), (b) transpoziţiile (12), (23), ...,($n-1$ n), (c) (12) şi (12...n).

92. Arătaţi că A_n este generat de (a) ciclurile de lungime 3, (b) (123), (234), ...,($n-2$ $n-1$ n).

93. Arătaţi că S_5 este generat de orice transpoziţie şi un ciclu de lungime 5.

94. Arătaţi că A_4 nu posedă subgrupuri de indice 2.

95. Arătaţi că A_5 nu posedă subgrupuri normale diferite de $\{I\}$ şi A_5 (un grup cu această proprietate se numeşte grup simplu).

96. Fie $k_1, k_2, ..., k_n$ numere naturale cu $1k_1 + 2k_2 + \cdots + nk_n = n$. Spunem că o permutare $\sigma \in S_n$ are tipul $(k_1, k_2, ..., k_n)$ dacă în descompunerea lui σ ca produs de cicluri disjuncte există k_i cicluri de lungime i, $1 \leq i \leq n$. Arătaţi că două permutări $\alpha, \beta \in S_n$ sunt conjugate dacă şi numai dacă au acelaşi tip. Număraţi permutările de tip $(k_1, k_2, ..., k_n)$.

97. Găsiţi un subgrup H al lui S_6 izomorf cu S_3 astfel încât orice permutare diferită de I din H nu are puncte fixe.

98 Fie semidiscul din planul complex $A = \{z \in \mathbf{C} |\ |z - i| \leq 1, Re(z) \geq 0\}$ şi fie $B = A \cup iA \cup -A \cup -iA$. Calculaţi grupul de simetrie al lui B.

99. Fie G grupul rotaţiilor spaţiului euclidian care invariază un tetraedru regulat. Descrieţi elementele lui G şi arătaţi că G este izomorf cu A_4.

100. Fie G grupul rotaţiilor spaţiului euclidian care invariază un cub. Descrieţi elementele lui G şi arătaţi că G este izomorf cu S_4.

101. Arătaţi că grupul G al rotaţiilor spaţiului euclidian care invariază un dodecaedru regulat are ordinul 60 şi este izomorf cu A_5.

102. Fie G un grup. Arătaţi că dacă $G/Z(G)$ este ciclic, atunci G este abelian (adică $|G/Z(G)| = 1$). Folosind acest rezultat, arătaţi că orice grup cu p^2 elemente, p prim, este abelian.

Capitolul 4

Inele

În acest capitol se introduc noţiunile de bază ale teoriei inelelor: inel, corp, morfism de inele, subinel, ideal, sistem de generatori, caracteristica unui inel, inel factor. Se prezintă construcţia inelelor de matrice, a inelelor de polinoame şi construcţia corpului cuaternionilor. Se demonstrează teoreme importante referitoare la aceste noţiuni şi construcţii.

4.1 Inel, subinel, ideal

Un *inel* este un triplet $(A, +, \cdot)$ format dintr-o mulţime nevidă A şi două operaţii pe A, prima notată cu $+$ numită *adunare*, a doua notată cu $\cdot$ numită *înmulţire*, astfel încât

(1) $(A, +)$ este grup abelian

(2) $(A, \cdot)$ este monoid, şi

(3) înmulţirea este distributivă faţă de adunare, adică $a(b + c) = ab + ac$ şi $(b + c)a = ba + ca$ pentru orice $a, b, c \in A$.

Elementul neutru al adunării se notează cu 0 şi se numeşte *elementul nul*. Opusul unui element $a \in A$ (faţă de adunare) se notează cu $-a$. Elementul neutru al înmulţirii se notează cu 1 şi se numeşte *elementul unitate*. Un element $a \in A$ se zice *inversabil* dacă este inversabil faţă de înmulţire; inversul său se notează cu a^{-1}. Mulţimea elementelor inversabile (încă zisă a unităţilor) lui A se notează cu $U(A)$. Inelul $\{0\}$ se numeşte inelul nul. Un inel se numeşte *inel comutativ* dacă înmulţirea este comutativă. Un inel nenul se numeşte *corp* dacă orice element nenul este inversabil. Grupul $(A, +)$ se numeşte *grupul aditiv subiacent al lui A*. Spunem că inelul A are divizori ai lui zero dacă există $x, y \neq 0$ cu $xy = 0$.

Z, **Q**, **R**, **C** sunt inele comutative faţă de operaţiile uzuale de adunare şi înmulţire, ultimele trei fiind chiar corpuri. E clar că $U(\mathbf{Z}) = \{\pm 1\}$.

$\mathbf{Z}[i] = \{a + bi |\ a, b \in \mathbf{Z}\}$ este un inel comutativ numit *inelul întregilor lui Gauss.* $U(\mathbf{Z}[i]) = \{\pm 1, \pm i\}$, deoarece dacă $(a + bi)(c + di) = 1$, atunci $1 = |(a + bi)(c + di)|^2 = (a^2 + b^2)(c^2 + d^2)$, deci $a + bi \in \{\pm 1, \pm i\}$.

Fie R un inel şi $m, n \geq 1$. O *matrice cu m linii şi n* coloane (sau *matrice de tip* (m, n)) cu elemente din R este un tablou de forma

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

unde toate elementele a_{ij} sunt din R. Vom nota matricea precedentă cu $(a_{ij})_{1\leq i\leq m, 1\leq j\leq n}$ sau mai simplu cu (a_{ij}). a_{11}, a_{12}, ...,a_{mn} se numesc *elementele matricei.* Matricea poate fi gândită ca fiind funcţia $(i, j) \mapsto a_{ij} : \{1, ..., m\} \times \{1, ..., n\} \to R$. Dacă $m = n$, matricea se numeşte *matrice pătratică de ordinul n.* Vom nota cu $M_{m,n}(R)$ (resp. $M_n(R)$) mulţimea matricelor de tip (m, n) (resp. pătratice de ordinul n) cu elemente din R. Două matrice $A = (a_{ij})$ şi $B = (b_{ij})$ sunt egale dacă sunt de acelaşi tip (m, n) şi $a_{ij} = b_{ij}$ pentru $1 \leq i \leq m$, $1 \leq j \leq n$. Aşadar, $A = B$ dacă şi numai dacă A şi B privite ca funcţii $\{1, ..., m\} \times \{1, ..., n\} \to R$ sunt egale.

Pe mulţimea $M_{m,n}(R)$ definim o operaţie de adunare indusă de adunarea din R. Concret, dacă $A = (a_{ij})$ şi $B = (b_{ij})$ sunt din $M_{m,n}(R)$, atunci $A + B$ este prin definiţie matricea $(a_{ij} + b_{ij})$. Se vede imediat că $(M_{m,n}(R), +)$ este un grup abelian. Într-adevăr, asociativitatea rezultă din egalităţile $[(a_{ij}) + (b_{ij})] + (c_{ij}) = (a_{ij} + b_{ij} + c_{ij}) = (a_{ij}) + [(b_{ij}) + (c_{ij})]$, elementul neutru este matricea cu toate elementele nule numită *matricea nulă* şi notată cu 0_{mn}, iar opusă matricei $A = (a_{ij})$ este matricea $-A = (-a_{ij})$.

Între anumite matrice se defineşte o operaţie de înmulţire. Fie $m, n, p \geq 1$. Fie $A = (a_{ij}) \in M_{m,n}(R)$ şi $B = (b_{jk}) \in M_{n,p}(R)$. *Produsul AB* este prin definiţie matricea $C = (c_{ik}) \in M_{m,p}(R)$ cu elementele $c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}$. Aşadar, produsul AB este definit doar dacă numărul coloanelor lui A este egal cu numărul liniilor lui B, iar elementul c_{ik} este suma produselor dintre elementele liniei i din A cu elementele corespunzătoare de pe coloana k din B. Din acest motiv, regula de înmulţire se mai numeşte şi "linii pe coloane".

Înmulţirea matricelor este asociativă, adică dacă $A = (a_{ij}) \in M_{m,n}(R)$, $B = (b_{jk}) \in M_{n,p}(R)$ şi $C = (c_{kl}) \in M_{p,q}(R)$, atunci $(AB)C = A(BC)$.

Într-adevăr, fie $AB = (d_{ik})$ şi $(AB)C = (e_{il})$. Atunci $d_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}$ şi $e_{il} = \sum_{k=1}^{p} d_{ik}c_{kl}$. Deci $e_{il} = \sum_{k=1}^{p}(\sum_{j=1}^{n} a_{ij}b_{jk})c_{kl} = \sum_{k=1}^{p}\sum_{j=1}^{n} a_{ij}b_{jk}c_{kl}$. Fie $A(BC) = (f_{il})$. Un calcul similar arată că $f_{il} = e_{il}$. Deci $(AB)C = A(BC)$.

Înmulţirea matricelor este distributivă la stânga faţă de adunare, mai precis, dacă $A = (a_{ij}) \in M_{m,n}(R)$, $B = (b_{jk}) \in M_{n,p}(R)$ şi $C = (c_{jk}) \in M_{n,p}(R)$, atunci $A(B + C) = AB + AC$. Într-adevăr, fie $A(B + C) = (d_{ik})$ şi $AB + AC = (e_{il})$. Folosind distributivitatea înmulţirii faţă de adunare în inelul R, obţinem $d_{ik} = \sum_{j=1}^{n} a_{ij}(b_{jk} + c_{jk}) = \sum_{j=1}^{n} a_{ij}b_{jk} + \sum_{j=1}^{n} a_{ij}c_{jk} = e_{ik}$ pentru $1 \le i \le m$, $1 \le k \le p$. Distributivitatea la dreapta se probează analog.

Fie $n \ge 1$. Matricea pătratică de ordinul n

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

se numeşte *matricea unitate* de ordinul n. Dacă $A = (a_{ij}) \in M_{m,n}(R)$, atunci $AI_n = A$ şi $I_mA = A$. Într-adevăr, fie $AI_n = (b_{ik})$. Cum $I_n = (\delta_{ij})$, unde δ_{ij} este simbolul lui Kronecker, rezultă că $b_{ik} = \sum_{j=1}^{n} a_{ij}\delta_{jk} = a_{ik}$. Cealaltă egalitate se probează similar.

Teorema 56 *Fie R un inel nenul şi $n \ge 1$. Faţă de operaţiile de adunare şi înmulţire ale matricelor, $M_n(R)$ este un inel numit* inelul matricelor pătratice de ordinul n cu elemente din R. *Dacă $n \ge 2$, inelul $M_n(R)$ este necomutativ şi are divizori ai lui zero.*

Demonstraţie. Faptul că $M_n(R)$ este un inel rezultă din proprietăţile demonstrate anterior. Egalităţile

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

arată că inelul $M_2(R)$ este necomutativ şi are divizori ai lui zero. Cazul $n \ge 3$ se probează analog. •

Unităţile inelului $M_n(R)$ se numesc *matrice inversabile*. Conform teoremei 17, ele formează grup faţă de înmulţirea matricelor. Acest grup este notat cu $GL_n(R)$ şi este numit *grupul general liniar* de ordin n peste R.

Date două inele B, C, produsul cartezian $B \times C$ împreună cu operaţiile de adunare şi înmulţire definite pe componente (adică, $(b_1, c_1) + (b_2, c_2) = (b_1 + b_2, c_1 + c_2)$, $(b_1, c_1)(b_2, c_2) = (b_1b_2, c_1c_2)$) este un inel numit *produsul direct* al inelelor B şi C. Construcţia produsului direct de inele se poate generaliza uşor pentru familii arbitrare de inele. De exemplu, $\mathbf{Z}^{\mathbf{N}}$ este inelul şirurilor de numere întregi.

Teorema 57 (Reguli de calcul într-un inel.) *Fie A un inel.*
(1) *$a0 = 0a = 0$ pentru orice $a \in A$.*
(2) *$a(-b) = (-a)b = -ab$ pentru orice $a, b \in A$.*
(3) *Dacă $n \geq 1$ şi $a_1, ..., a_k \in A$ astfel încât $a_ia_j = a_ja_i$ pentru orice i, j, atunci*

$$(a_1 + \cdots + a_k)^n = \sum_{n_1+\cdots+n_k=n} \frac{n!}{n_1!n_2!\cdots n_k!} a_1^{n_1}a_2^{n_2}\cdots a_k^{n_k}.$$

Demonstraţie. (1) Din $0 + 0 = 0$ se obţine $a0 + a0 = a0$, deci, adunând $-a0$, rezultă $a0 = 0$. (2) $ab + a(-b) = a(b - b) = a0 = 0$, deci $a(-b) = -ab$. (3) Ţinem seama de distributivitate şi de comutativitatea elementelor a_i. Evaluăm produsul $(a_1 + \cdots + a_k)^n$ desfăcând cele n paranteze şi grupând monoamele asemenea. Fie $n_1, ..., n_k \geq 0$ cu $n_1 + \cdots + n_k = n$. Pentru a obţine monomul $a_1^{n_1}a_2^{n_2}\cdots a_k^{n_k}$ luăm a_1 din n_1 paranteze, şi acest lucru se poate face în $C_n^{n_1}$ moduri, luăm a_2 din n_2 paranteze, în $C_{n-n_1}^{n_2}$ moduri, ş.a.m.d. Deci monomul $a_1^{n_1}a_2^{n_2}\cdots a_k^{n_k}$ apare de t ori, unde

$$t = C_n^{n_1}C_{n-n_1}^{n_2}\cdots C_{n-n_1-n_2-\cdots-n_{k-1}}^{n_k} = \frac{n!}{n_1!n_2!\cdots n_k!}.$$

Pentru $k = 2$ se obţine formula binomului lui Newton. •

Fie A un inel. Un element $a \in A$ se numeşte *divizor al lui zero* dacă există $x \in A$, $x \neq 0$, astfel încât $ax = 0$ sau $xa = 0$. În orice inel nenul, 0 este divizor al lui zero. Un element inversabil nu este divizor al lui zero, deoarece $ab = 1$ şi $xa = 0$ implică $0 = xab = x$.

Un inel în care zero este singurul divizor al lui zero (adică în care $ab = 0$ implică $a = 0$ sau $b = 0$) se numeşte *inel integru*. Un inel nenul comutativ integru se numeşte *domeniu (de integritate)*. Corpurile sunt inele integre. $\mathbf{Z}$ şi $\mathbf{Z}[i]$ sunt domenii; $\mathbf{Z} \times \mathbf{Z}$ nu este integru deoarece $(1, 0)(0, 1) = (0, 0)$.

Teorema 58 *Într-un inel finit orice element este inversabil sau divizor al lui zero.*

Demonstraţie. Fie a un non-divizor al lui zero al inelului finit A. Atunci aplicaţia $f : A \to A$, $f(x) = ax$ este injectivă, deci surjectivă, deoarece A este finit. Deci există $b \in A$ cu $ab = 1$. Analog, există $c \in A$ cu $ca = 1$. Rezultă $c = cab = b$. •

Dacă $n \geq 2$, atunci $\mathbf{Z}_n$ este inel comutativ faţă de operaţiile de adunare şi înmulţire definite după teorema 17. Într-adevăr, dacă $a, b, \in \mathbf{Z}$, atunci $\widehat{a}(\widehat{b} + \widehat{c}) = a\widehat{(b + c)} = \widehat{ab + ac} = \widehat{a}\widehat{b} + \widehat{a}\widehat{c}$. Ii vom spune simplu *inelul* $\mathbf{Z}_n$. Notăm cu $Z(\mathbf{Z}_n)$ mulţimea divizorilor lui zero din $\mathbf{Z}_n$.

Corolarul 59 $U(\mathbf{Z}_n) = \{\widehat{x} |\ x \in \mathbf{Z},\ (x, n) = 1\}$, $Z(\mathbf{Z}_n) = \{\widehat{x} |\ x \in \mathbf{Z},\ (x, n) \neq 1\}$ *şi* $\mathbf{Z}_n$ *este corp* $\Leftrightarrow$ n *este număr prim.*

Demonstraţie. Primele două egalităţi rezultă din teoremele 18 şi 58. În consecinţă, $\mathbf{Z}_n$ este corp $\Leftrightarrow U(\mathbf{Z}_n, \cdot) = \mathbf{Z}_n \setminus \{\hat{0}\} \Leftrightarrow$ numerele neprime cu n se divid cu $n \Leftrightarrow n$ este număr prim. •

Fie A un inel. O submulţime nevidă B a lui A se numeşte *subinel* al lui A dacă

(i) A este subgrup al grupului aditiv al lui A, adică $x - y \in A$ pentru orice $x, y \in A$,

(ii) A este parte stabilă lui B în raport cu înmulţirea, adică $xy \in A$ pentru orice $x, y \in A$, şi

(iii) $1 \in B$.

Dacă B este subinel al lui A, atunci B este inel faţă de operaţiile de adunare şi înmulţire induse de pe A. De exemplu, mulţimea $\mathbf{Z}_{(2)}$ a fracţiilor a/b cu a, b numere întregi şi b impar este un subinel al lui $\mathbf{Q}$.

Fie A un inel. O submulţime nevidă I a lui A se numeşte *ideal stâng* (resp. *ideal drept*) dacă

(i) $x - y \in I$ pentru orice $x, y \in I$, şi

(ii) $ax \in I$ (resp. $xa \in I$) pentru orice $x \in I$ şi $a \in A$.

Un ideal stâng şi drept se numeşte *ideal bilateral.* $\{0\}$ şi A sunt ideale bilaterale numite *idealul trivial* respectiv *idealul impropriu.*

Dacă un ideal stâng sau drept I conţine un element inversabil x, atunci $I = A$, deoarece, dacă $a \in A$, atunci $a = xx^{-1}a \in I$.

Teorema 60 *Un inel nenul A este corp dacă şi numai dacă idealele sale stângi (resp. drepte) sunt $\{0\}$ şi A.*

Demonstraţie. Dacă A este corp, atunci orice ideal I nenul conţine un element inversabil, deci $I = A$. Reciproc, să presupunem că idealele stângi ale lui A sunt $\{0\}$ şi A, şi fie $x \neq 0$. Rezultă că $Ax = A$, deci există $y \in A$ cu $xy = 1$. Repetând argumentul pentru y, există $z \in A$ cu $yz = 1$. Rezultă că $x = x(yz) = (xy)z = z$. Deci x este inversabil. Varianta cu ideale drepte se probează analog. •

În cazul unui inelul comutativ orice idel stâng este ideal drept şi reciproc, motiv pentru care în acest caz vom spune simplu *ideal.*

Teorema 61 *Fie A un inel. Atunci o intersecţie de subinele (resp. ideale stângi, drepte, bilaterale) este tot un subinel (resp. ideal stâng, drept, bilateral).*

Demonstraţie. Facem demonstraţia pentru o familie $(I_\alpha)_\alpha$ de ideale drepte, celelalte cazuri fiind similare. Fie $x, y \in \cap_\alpha I_\alpha$ şi $a \in A$. Atunci $x, y \in I_\alpha$ pentru orice α. Cum fiecare I_α este ideal drept, rezultă că $x - y, xa \in I_\alpha$ pentru orice α. Deci $x - y, xa \in \cap_\alpha I_\alpha$.

Teorema 62 *Idealele lui* $\mathbf{Z}$ *sunt* $n\mathbf{Z}$ *cu* $n \geq 0$.

Demonstraţie. Idealele sunt subgrupuri ale grupului aditiv, deci au forma $n\mathbf{Z}$ cu $n \geq 0$, cf. teoremei 25. Reciproc, fiecare $n\mathbf{Z}$ este ideal, deoarece $x \in n\mathbf{Z}$ şi $a \in \mathbf{Z}$ implică $ax \in n\mathbf{Z}$. •

În inelul matricelor $M_2(\mathbf{Z})$, matricele cu linia a doua nulă formează un ideal drept care nu e ideal stâng. Într-adevăr, pentru orice $a, b, c, d, e, f \in \mathbf{Z}$, $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c & d \\ e & f \end{pmatrix} = \begin{pmatrix} ac+be & ad+bf \\ 0 & 0 \end{pmatrix}$, dar $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

Pentru $n \geq 0$ fixat, matricele $K \in M_2(\mathbf{Z})$ cu toate elementele multipli de n formează un ideal bilateral al lui $M_2(\mathbf{Z})$. Mai mult, toate idealele bilaterale ale lui $M_2(\mathbf{Z})$ au această formă, cf. ex. 108.

Fie A un inel şi X o submulţime a lui A. Mulţimea

$$AX := \{a_1x_1 + \cdots + a_nx_n |\ a_i \in A, x_i \in X, n \geq 0\}$$

este un idealul stâng al lui A numit *idealul stâng generat de* X. Într-adevăr, e clar că diferenţa a două elemente din AX este tot în AX, iar dacă $y = a_1x_1 + \cdots + a_nx_n \in AX$ şi $b \in A$, atunci $by = ba_1x_1 + \cdots + ba_nx_n \in AX$. Se vede imediat că $X \subseteq AX$ şi că $AX \subseteq I$ pentru orice ideal stâng al lui A care conţine X.

În mod analog, se arată că $XA := \{x_1a_1 + \cdots + x_na_n |\ a_i \in A, x_i \in X, n \geq 0\}$ este un idealul drept al lui A numit *idealul drept generat de* X şi că $AXA := \{a_1x_1b_1 + \cdots + a_nx_nb_n |\ a_i, b_i \in A, x_i \in X, n \geq 0\}$ este un idealul bilateral al lui A numit *idealul bilateral generat de* X.

Presupunem că A este inel comutativ. Atunci $AX = XA = AXA$ se numeşte *idealul generat de* X. Vom nota idealul generat de o mulţime $\{x_i\}_{i\in I} \subseteq A$ cu $(x_i;\ i \in I)$ sau $\sum_{i\in I} Ax_i$ sau încă $\sum_{i\in I} x_iA$.

Dacă $x \in A$, atunci $Ax = \{ax|\ a \in A\}$ se numeşte *idealul principal generat de* x. Un ideal se zice *finit generat* dacă poate fi generat de o mulţime finită.

Toate idealele lui $\mathbf{Z}$ sunt principale, cf. teoremei 62. Idealul $(2, X)\mathbf{Z}[X]$ nu este principal, cf. ex. 116. În inelul şirurilor de numere întregi, şirurile cu un număr finit de termeni nenuli formează un ideal care nu este finit generat, cf. ex. 118.

4.2 Morfisme de inele

Fie A şi B două inele. O funcţie $f : A \to B$ se numeşte *morfism de inele* dacă $f(x + y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$ pentru orice $x, y \in A$ şi

$f(1_A) = 1_B$. Rezultă că f este morfism de inele dacă şi numai dacă f este morfism de grupuri $(A, +) \to (B, +)$ şi morfism de monoizi $(A, \cdot) \to (B, \cdot)$.

Un *morfism de corpuri* este un morfism de inele între două corpuri. Un morfism de inele (corpuri) bijectiv se numeşte *izomorfism de inele (corpuri)* şi dacă în plus $A = B$, atunci se numeşte *automorfism*.

Fie A un inel (corp). Aplicaţia identică $I_A : A \to A$ este un automorfism. Există un singur morfism de inele $f : \mathbf{Z} \to A$ şi anume cel dat de $k \mapsto k \cdot 1_A$. Aplicaţia de incluziune $\mathbf{Q} \hookrightarrow \mathbf{R}$ şi cea de conjugare $\mathbf{C} \to \mathbf{C}$ sunt morfisme de corpuri.

Nu există morfisme de inele $\mathbf{Q} \to \mathbf{Z}$, deoarece singurul morfism de grupuri $(\mathbf{Q}, +) \to (\mathbf{Z}, +)$ este cel nul, cf. ex. 61.

Teorema 63 (a) *Compunerea a două morfisme de inele este un morfism de inele.* (b) *Inversul unui izomorfism de inele este tot un izomorfism de inele.* (c) *Fie $f : A \to B$ un morfism de inele. Dacă $a \in U(A)$, atunci $f(a) \in U(B)$ şi $f(a)^{-1} = f(a^{-1})$.*

Demonstraţie. Se aplică teoremele 20 şi 21. •

Spunem că inelele A şi B sunt sunt izomorfe, şi scriem $A \simeq B$, dacă există există un izomorfism de inele $f : A \to B$. Se vede că orice proprietate ce ţine de structura de inel a lui A se poate transporta prin f în B. De aceea, nu vom face distinţie între două inele izomorfe. Din teorema anterioară, rezultă că relaţia de izomorfism între inele este reflexivă, simetrică şi tranzitivă.

Se poate arăta (vezi ex. 112) că inelele $\mathbf{Z}_4$, $\mathbf{Z}_2 \times \mathbf{Z}_2$, $\mathbf{Z}_2[X]/X^2\mathbf{Z}_2[X]$ şi $\mathbf{Z}_2[X]/(X^2 + X + \hat{1})\mathbf{Z}_2[X]$ sunt mutual neizomorfe şi că orice inel cu 4 elemente este izomorf cu unul dintre acestea. Se spune că sunt 4 tipuri de inele cu 4 elemente.

Fie $f : A \to B$ un morfism injective de inele. Atunci f stabileşte un izomorfism între A şi $Im(f)$. Putem atunci să gândim pe A ca subinel al lui B prin identificarea fiecărui $a \in A$ cu $f(a)$. De exemplu, putem identifica fiecare număr real a cu numărul complex $a + 0i$.

Teorema 64 *Fie $f : A \to B$ un morfism de inele.*

(a) *Dacă C este un subinel al lui A, atunci $f(C)$ este un subinel al lui B. În particular, $Im(f)$ este un subinel al lui B.*

(b) *Dacă J este un subinel (resp. ideal stâng, drept, bilateral) al lui B, atunci $f^{-1}(J)$ este un subinel (resp. ideal stâng, drept, bilateral) al lui A numit* pre-imaginea *sau* imaginea inversă *a lui J.*

(c) $ker(f) := f^{-1}(0)$ *este un ideal bilateral al lui* A *numit* nucleul lui f *şi* f *este injectiv* $\Leftrightarrow ker(f) = \{0\}$.

(d) *Dacă* A *este corp şi* B *inel nenul, atunci* f *este injectiv.*

(a). Din teorema 27, $f(C)$ este un subgrup al lui $(B, +)$. Fie $x, y \in C$. Atunci $f(x)f(y) = f(xy) \in f(C)$. În plus, $1 = f(1) \in f(C)$.

(b). Presupunem că J este un ideal stâng al lui B. Din teorema 27, $f^{-1}(J)$ este un subgrup al lui $(A, +)$. Fie $a \in A$ şi $x \in f^{-1}(J)$. Atunci $f(x) \in J$ şi $f(ax) = f(a)f(x) \in J$. Deci $ax \in f^{-1}(J)$. Celelalte cazuri se probează analog.

(c). $ker(f)$ este pre-imaginea idealului trivial al lui B, deci este ideal bilateral al lui B, cf. (b). Se aplică teorema 27.

(d). A nu are decât idealele $\{0\}$ şi A, deoarece este corp. Cum $f(1) = 1 \neq 0$, rezultă $ker(f) \neq A$, deci $ker(f) = \{0\}$, adică f este morfism injectiv.

•

Fie R un inel, $m, n \geq 1$, $b \in R$ şi $A = (a_{ij}) \in M_{m,n}(R)$. Prin definiţie, produsul bA dintre b şi matricea A este matricea (ba_{ij}). Similar, produsul Ab este matricea $(a_{ij}b)$. Injecţia $b \mapsto bI_n : R \to M_n(R)$ este un morfism de inele, deoarece $(a + b)I_n = aI_n + bI_n$ şi $(ab)I_n = (aI_n)(bI_n)$, pentru orice $a, b \in R$. Ca urmare, R se identifică cu subinelul $\{rI_n |\ r \in R\}$ al lui $M_n(R)$.

Fie A un inel nenul. *Caracteristica lui* A este numărul natural definit prin

$$car(A) = \begin{cases} ord(1) & \text{dacă } ord(1) < \infty \\ 0 & \text{dacă } ord(1) = \infty. \end{cases}$$

unde $ord(1)$ este ordinul lui 1 în grupul aditiv al lui A.

Aşadar, $car(A) = 0$ însemnă că toate sumele de forma $1 + 1 + \cdots + 1$ sunt nenule, iar $car(A) = n > 0$ însemnă că n este cel mai mic număr natural nenul cu $n1_A = 0$. E clar că un subinel are aceeaşi caracteristică cu inelul. Exemple: $car(\mathbf{Z}) = 0$, $car(\mathbf{Q}) = 0$, $car(\mathbf{Z}_n) = n$.

Fie A un inel. Dacă $car(A) = 0$, atunci A conţine o copie izomorfă a inelului $\mathbf{Z}$ şi anume subinelul $P = \{k1_A |\ k \in \mathbf{Z}\}$, iar dacă $car(A) = n > 0$, atunci A conţine o copie a inelului $\mathbf{Z}_n$ şi anume subinelul $P = \{k1 |\ 0 \leq k \leq n-1\}$. În ambele cazuri P se numeşte *subinelul prim al lui* A.

De exemplu, subinelul prim al inelului $M_2(\mathbf{Z})$ este $\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} |\ a \in \mathbf{Z}\}$.

Deoarece un subinel al unui inel integru este tot inel integru, rezultă că subinelul prim al unui inel integru este izomorf cu $\mathbf{Z}$ sau cu $\mathbf{Z}_p$ cu p număr prim. Cu alte cuvinte, caracteristica unui inel integru (în particular, caracteristica unui corp) este zero sau un număr prim. Se observă că un corp K de caracteristică zero conţin o copie izomorfă a corpului $\mathbf{Q}$ şi anume $\{a1/b1|\ a, b \in \mathbf{Z}, b \neq 0\}$. Un corp finit are caracteristica număr prim.

Teorema 65 (Morfismul lui Frobenius.) *Fie A un inel comutativ de caracteristică p număr prim. Atunci funcţia $F : A \to A$, $F(x) = x^p$ este un morfism de inele.*

Demonstraţie. Fie $x, y \in A$. $F(xy) = (xy)^p = x^p y^p = F(x)F(y)$. Fie $1 \leq k \leq p-1$. Atunci $k!$ şi $(p-k)!$ nu se divid cu p, deci numărul $C_p^k = p!/k!(p-k)!$ se divide cu p, deoarece numărătorul $p!$ se divide cu p. Dacă $z \in A$ şi s este un multiplu de p, atunci $sz = 0$, deoarece $car(A) = p$. Aşadar $F(x+y) = (x+y)^p = X^p + C_p^1 x^{p-1} y + \cdots + C_p^{p-1} x y^{p-1} + y^p = x^p + y^p = F(x) + F(y)$. •

4.3 Inel factor

Fie A un inel şi I un ideal bilateral al lui A. Cum I este subgrup (normal) al grupului $(A, +)$, putem considera grupul factor A/I. Elementele lui A/I sunt de forma $\widehat{x} = x + I$ cu $x \in A$. Pe A/I definim înmulţirea $\widehat{x}\widehat{y} = \widehat{xy}$ pentru $x, y \in A$. Această înmulţire e bine-definită (adică nu depinde de reprezentanţii claselor). Într-adevăr, dacă $\widehat{x} = \widehat{x'}$ şi $\widehat{y} = \widehat{y'}$, atunci $x' = x + i$ şi $y' = y + j$ cu $i, j \in I$. Deci $x'y' = xy + xj + iy + ij \in xy + I$. Se probează uşor că faţă de această înmulţire grupul A/I devine un inel numit *inelul factor A modulo I*. În plus funcţia $\pi : A \to A/I$, $\pi(x) = \widehat{x}$ este un morfism surjectiv de inele numit *surjecţia canonică.* De exemplu, $\mathbf{Z}/n\mathbf{Z}$ este chiar inelul $\mathbf{Z}_n$.

Teorema 66 (Teorema fundamentală de izomorfism pentru inele.) *Fie $f : A \to B$ un morfism de inele. Atunci aplicaţia*

$$F : A/ker(f) \to B, \quad F(\widehat{x}) = f(x), \quad x \in A$$

este un izomorfism de inele. Deci $A/ker(f) \simeq Im(f)$.

Demonstraţie. Din teorema corespunzătoare de la grupuri (teorema 43) se ştie că F este un izomorfism între grupurile aditive ale inelelor $A/ker(f)$ şi $Im(f)$. Dacă $a, b \in A$, atunci $F(\widehat{ab}) = f(ab) = f(a)f(b) = F(\widehat{a})F(\widehat{b})$. În plus, $F(\widehat{1}) = f(1) = 1_B$. Deci F este izomorfism de inele. •

Se verifică uşor că $f : \mathbf{Z}[i] \to \mathbf{Z}_2$, $f(a+bi) = \widehat{a+b}$ este un morfism surjectiv de inele cu nucleul $(1+i)\mathbf{Z}[i]$. Deci $\mathbf{Z}[i]/(1+i)\mathbf{Z}[i] \simeq \mathbf{Z}_2$.

Fie A un inel comutativ şi I, J ideale ale lui A. Se verifică uşor că $I+J := \{i+j |\ i \in I, j \in J\}$ este un ideal al lui A numit *suma* idealelor i şi J.

Teorema 67 (Lema chineză a resturilor.) *Fie A un inel comutativ şi I, J ideale ale lui A astfel încât $I + J = A$. Atunci inelul factor $A/(I \cap J)$ este izomorf cu $A/I \times A/J$.*

Demonstraţie. Fie $p : A \to A/I$ şi $q : A \to A/J$ proiecţiile canonice. Se vede uşor că aplicaţia $f : A \to A/I \times A/J$, $f(x) = (p(x), q(x))$, este un morfism de inele.

Avem $ker(f) = \{x \in A|\ p(x) = 0 \text{ şi } q(x) = 0\} = I \cap J$.

Cum $I + J = A$, există $i \in I$ şi $j \in J$ cu $i + j = 1$. Rezultă că $p(i) = 0$, $p(j) = 1$, $q(i) = 1$ şi $q(j) = 0$. Dacă $x, y \in A$, atunci $f(jx + iy) = (p(jx), q(iy)) = (p(x), q(y))$, deci f este surjecţie. Se aplică teorema fundamentală de izomorfism. •

Corolarul 68 *Fie $m, n \geq 2$ numere întregi prime între ele. Atunci inelele $\mathbf{Z}_{mn}$ şi $\mathbf{Z}_m \times \mathbf{Z}_n$ sunt izomorfe.*

Demonstraţie. Se aplică teorema anterioară şi corolarul 31 •

4.4 Corpuri

Reamintim că un *corp* este un inel cu $1 \neq 0$ în care orice element nenul este inversabil. Cum elementele inversabile sunt nondivizori ai lui zero, rezultă că un corp este inel integru.

Exemple de corpuri: $\mathbf{Q}$, $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{R}$, $\mathbf{C}$. Justificarea faptului că $\mathbf{Q}(\sqrt{2})$ este corpse poate face în felul următor. E clar că $\mathbf{Q}(\sqrt{2})$ este subinel al lui $\mathbf{R}$. Fie $0 \neq a + b\sqrt{2} \in \mathbf{Q}(\sqrt{2})$. Atunci numărul raţional $c = a^2 - 2b^2 = (a+b\sqrt{2})(a-b\sqrt{2})$ este nenul. Atunci $1/(a+b\sqrt{2}) = a/c-(b/c)\sqrt{2} \in \mathbf{Q}(\sqrt{2})$.

$\mathbf{Z}[i]/(3)$ este corp cu 9 elemente. Într-adevăr, $\mathbf{Z}[i]/(3) = \{\widehat{a+bi} |\ 0 \leq a, b \leq 2\}$. Se observă că dacă $\widehat{a+bi} \neq \widehat{0}$ atunci $\widehat{a^2+b^2} = (\widehat{a+bi})(\widehat{a-bi}) \neq 0$. Se continuă ca în exemplul referitor la $\mathbf{Q}(\sqrt{2})$.

Un *corp finit* este un corp cu un număr finit de elemente. O celebră teoremă a lui Wedderburn afirmă că orice corp finit este comutativ (vezi [5, teorema X.2.5]).

Inelele: $\mathbf{Z}$, $\mathbf{Z}(i)$, $\mathbf{Q}[X]$, $\mathbf{R}[[X]]$ sunt domenii nu sunt corpuri. În general, un inel de polinoame sau de serii formale nu este niciodată corp.

Un *subcorp* al unui inel L este un subinel care este corp în raport cu operaţiile induse. De exemplu, $\mathbf{Q}$ este subcorp al lui $\mathbf{R}$ şi orice corp de caracteristică zero conţine un subcorp izomorf cu $\mathbf{Q}$.

Reamintim varianta matriceală a contrucţiei corpului $\mathbf{C}$ al numerelor complexe pornind de la $\mathbf{R}$. Fie

$$\mathbf{C} = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbf{R}\}.$$

Teorema 69 $\mathbf{C}$ *este un corp comutativ în raport cu adunarea şi înmulţirea matricelor.*

Demonstraţie. E clar că matricea unitate se află în $\mathbf{C}$. $\mathbf{C}$ este parte stabilă a lui $M_2(\mathbf{R})$ în raport cu adunarea şi înmulţirea:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}$$

şi

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Deci $\mathbf{C}$ este subinel comutativ al lui $M_2(\mathbf{R})$. Fie $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ o matrice nenulă din $\mathbf{C}$. Deci $a^2 + b^2 \neq 0$. Din egalitatea

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} a^2+b^2 & 0 \\ 0 & a^2+b^2 \end{pmatrix}$$

rezultă că $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = (a^2+b^2)^{-1}\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Deci $\mathbf{C}$ este corp comutativ. •

Morfismul injectiv de inele $f : \mathbf{R} \to \mathbf{C}$, $f(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ ne permite să gândim pe $\mathbf{R}$ ca un subcorp al lui $\mathbf{C}$ prin identificarea fiecărui $a \in \mathbf{R}$ cu $f(a)$. Notăm $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ cu i. Rezultă că $i^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -1$.

Dacă $a, b \in \mathbf{R}$, atunci

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = a + bi$$

şi scrierea este unică. Rezultă că $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$. Obţinem următorea descriere a corpului numerelor complexe.

Teorema 70 *Corpul numerelor complexe este* $\mathbf{C} = \{a + bi|\ a, b \in \mathbf{R}\}$, *scrierea sub forma* $a+bi$ *fiind unică, cu adunarea şi înmulţirea definite prin* $(a+bi)+(c+di) = (a+c)+(b+d)i$ *şi* $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$.

Vom descrie un exemplu de corp necomutativ *corpul cuaternionilor* construit pentru prima dată de Hamilton în 1843. Fie

$$\mathbf{H} = \{\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in \mathbf{C}\}.$$

Teorema 71 $\mathbf{H}$ *este un corp necomutativ în raport cu adunarea şi înmulţirea matricelor.*

Demonstraţie. E clar că matricea unitate se află în $\mathbf{H}$. Se arată prin calcul că $\mathbf{H}$ este parte stabilă în raport cu adunarea şi înmulţirea. Pentru înmulţire avem

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}\begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix} = \begin{pmatrix} ac-b\bar{d} & ad+b\bar{c} \\ -\overline{(ad+b\bar{c})} & \overline{ac-b\bar{d}} \end{pmatrix}.$$

Deci $\mathbf{H}$ este subinel al lui $M_2(\mathbf{C})$. Fie $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ o matrice nenulă din $\mathbf{H}$. Deci $|a|^2+|b|^2 \neq 0$. Din egalităţile

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}\begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix} = \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix}\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = \begin{pmatrix} |a|^2+|b|^2 & 0 \\ 0 & |a|^2+|b|^2 \end{pmatrix}$$

rezultă că

$$\left(\begin{array}{cc} a & b \\ -\bar{b} & \bar{a} \end{array}\right)^{-1} = (|a|^2 + |b|^2)^{-1} \left(\begin{array}{cc} \bar{a} & -b \\ \bar{b} & a \end{array}\right).$$

Deci **H** este corp necomutativ (necomutativitatea rezultă din calculele de mai jos). •

Numim elementele lui **H** *cuaternioni*. Morfismul injectiv de corpuri $f : \mathbf{C} \to \mathbf{H}$, $f(a) = \left(\begin{array}{cc} a & 0 \\ 0 & \bar{a} \end{array}\right)$ ne permite să gândim pe **C** ca un subcorp al lui **H** prin identificarea fiecărui $a \in \mathbf{C}$ cu $f(a)$. În particular, numărul real a se identifică cu $\left(\begin{array}{cc} a & 0 \\ 0 & a \end{array}\right)$ iar i se identifică cu $\left(\begin{array}{cc} i & 0 \\ 0 & -i \end{array}\right)$. Considerăm şi cuaternionii $j = \left(\begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array}\right)$ şi $k = \left(\begin{array}{cc} 0 & i \\ i & 0 \end{array}\right)$. Prin calcul rezultă că $ij = k$, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$ şi $ik = -j$ (se reamarca analogia cu produsul vectorial al versorilor unui sistem de axe rectangular tridimensional). În plus, $i^2 = j^2 = k^2 = -1$. Fie $a, b \in \mathbf{C}$ şi $a = x + yi$, $b = z + ui$ cu x, y, z, u reale. Atunci

$$\left(\begin{array}{cc} a & b \\ -\bar{b} & \bar{a} \end{array}\right) = \left(\begin{array}{cc} x + yi & z + ui \\ -z + ui & x - yi \end{array}\right) = x + yi + zj + uk$$

şi scrierea este unică. Obţinem următoarea descriere a corpului cuaternionilor similară numerelor complexe.

Teorema 72 *Corpul cuaternionilor este*

$$\mathbf{H} = \{x + yi + zj + uk \ (\textit{scriere unică}) \mid x, y, z, u \in \mathbf{R}\}$$

împreună cu relaţiile $ij = k$, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$, $ik = -j$ *şi* $i^2 = j^2 = k^2 = -1$.

Corolarul 73 *Cuaternionii* $\{\pm 1, \pm i, \pm j, \pm k\}$ *formează în raport cu înmulţirea un grup necomutativ numit grupul cuaternionilor.*

Reamintim că domeniu este un inel comutativ integru şi nenul. Orice corp este domeniu, dar există domenii care nu sunt corpuri, de exemplu **Z** sau $\mathbf{Q}[X]$.

Fie D un domeniu. Lui D îi putem ataşa în mod natural un corp care îl conţine pe D ca subinel, numit corpul de fracţii al lui D. Construcţia corpului de fracţii generalizează construcţia numerelor raţionale pornind de la numerele întregi.

Numim *fracţie* o pereche de elemente $a, b \in D$ cu $b \neq 0$ scrisă sub forma a/b. Definim egalitatea fracţiilor prin $a/b = c/d \Leftrightarrow ad = bc$. Egalitatea fracţiilor este reflexivă, simetrică şi tranzitivă. Într-adevăr, reflexivitatea şi simetria sunt evidente. Dacă $a/b = c/d$ şi $c/d = e/f$, atunci $ad = bc$ şi $cf = de$, deci $adf = bde$, de unde $af = be$, deoarece D este domeniu şi $d \neq 0$. Deci $a/b = e/f$. Fie $K = \{a/b|\ a, b \in D, b \neq 0\}$. Pe K definim adunarea şi înmulţirea prin

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{şi} \qquad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

Aceste operaţii sunt corect definite, adică nu depind de reprezentarea fracţiilor. Într-adevăr, să presupunem că $a/b = a'/b'$ şi $c/d = c'/d'$. Deducem că $ab' = a'b$ şi $cd' = c'd$, de unde rezultă că $(ad + bc)b'd' = (a'd' + b'c')bd$ şi $acb'd' = a'c'bd$. Se verifică uşor că, faţă de aceste operaţii, K este corp. K poartă numele de *corpul de fracţii al lui* D şi se notează cu $Q(D)$.

Morfismul injectiv de corpuri $f : D \to K$, $f(a) = a/1$ ne permite să gândim pe D ca subinel al lui K prin identificarea lui a cu $a/1$.

De exemplu, corpul de fracţii al lui $\mathbf{Z}$ este $\mathbf{Q}$, iar corpul de fracţii al lui $\mathbf{Z}[i]$ este $\mathbf{Q}(i)$.

4.5 Inelul de polinoame $A[X]$

Fie A un inel comutativ. Notăm cu $A^{(\mathbf{N})}$ mulţimea şirurilor $(a_n)_{n\geq 0}$ cu elemente din A cu un număr finit de termeni nenuli. Pe $A^{(\mathbf{N})}$ definim două operaţii: adunarea

$$(a_n)_{n\geq 0} + (b_n)_{n\geq 0} = (a_n + b_n)_{n\geq 0}$$

şi înmulţirea

$$(a_n)_{n\geq 0}(b_n)_{n\geq 0} = (c_n)_{n\geq 0} \text{ unde } c_n = \sum_{i+j=n} a_i b_j.$$

Teorema 74 *Faţă de aceste două operaţii,* $A^{(\mathbf{N})}$ *este un inel comutativ.*

Demonstraţie. $A^{(\mathbf{N})}$ este parte stabilă faţă de adunare şi înmulţire: dacă $a_n = 0$, $b_n = 0$ pentru $n \geq N$, atunci $a_n + b_n = 0$ pentru $n \geq N$ şi $\sum_{i+j=n} a_i b_j = 0$ pentru $n \geq 2N$.

Se arată uşor că $(A^{(\mathbf{N})}, +)$ este grup abelian cu elementul neutru şirul nul. Înmulţirea este asociativă deoarece

$$((a_n)_{n\geq 0}(b_n)_{n\geq 0})(c_n)_{n\geq 0} = ((\sum_{i+j=n} a_i b_j)_{n\geq 0})(c_n)_{n\geq 0} =$$

$$= (\sum_{i+j+k=n} a_i b_j c_k)_{n\geq 0} = (a_n)_{n\geq 0}((b_n)_{n\geq 0}(c_n)_{n\geq 0}).$$

Şirul $(1, 0, 0, ...)$ este elementul neutru al înmulţirii. E clar din definiţie că înmulţirea este comutativă. Înmulţirea este distributivă faţă de adunare

$$((a_n)_{n\geq 0} + (b_n)_{n\geq 0})(c_n)_{n\geq 0} = (a_n + b_n)_{n\geq 0}(c_n)_{n\geq 0} =$$

$$= (\sum_{i+j=n} (a_i + b_i)c_j)_{n\geq 0} = (\sum_{i+j=n} a_i c_j)_{n\geq 0} + (\sum_{i+j=n} b_i c_j)_{n\geq 0} =$$

$$= (a_n)_{n\geq 0}(c_n)_{n\geq 0} + (b_n)_{n\geq 0}(c_n)_{n\geq 0}. \bullet$$

Morfismul injectiv de inele $\varphi : \mathbf{A} \to A^{(\mathbf{N})}$, $\varphi(a) = (a, 0, 0, ...)$ ne permite să gândim pe A ca un subinel al lui $A^{(\mathbf{N})}$ prin identificarea fiecărui $a \in A$ cu $\varphi(a)$.

Notăm cu X şirul $(0, 1, 0, ...)$ şi îl numim *nedeterminată*. Se vede prin calcul că $X^n = (0, 0, 0, ..., 0, 1, 0, ...)$, unde 1 este precedat de n zerouri. Avem scrierea unică

$$(a_0, a_1, ..., a_n, 0, ...) = a_0 + a_1 X + \cdots + a_n X^n.$$

Inelul $A^{(\mathbf{N})}$ se notează cu $A[X]$ şi se numeşte *inelul polinoamelor într-o nedeterminată* cu coeficienţi în A.

Fie $f = a_0 + a_1 X + \cdots + a_n X^n$. Termenii $a_i X^i$ se numesc *monoame*, iar $a_0, a_1, ..., a_n$ *coeficienţii* polinomului. Numim *gradul lui* f (notat cu $grad(f)$), cel mai mare număr natural k cu $a_k \neq 0$. Gradul polinomului nul se ia $-\infty$. Dacă $f = a_0 + a_1 X + \cdots + a_n X^n$ are gradul n, atunci a_n se numeşte *coeficientul dominant* al lui f. Un polinom cu coeficientul dominant egal cu 1 se numeşte *polinom unitar*.

Teorema 75 *Fie A un inel comutativ şi $f, g \in A[X] \setminus \{0\}$. Atunci*

(a) $grad(f + g) \leq max(grad(f), grad(g))$.

(b) $grad(fg) \leq grad(f)+grad(g)$ cu egalitate dacă şi numai dacă produsul coeficienţilor dominanţi ai lui f şi g este nenul.

(c) Dacă f are coeficientul dominant non-divizor al lui zero (e.g. dacă A este domeniu), atunci $grad(fg) = grad(f) + grad(g)$ şi f este non-divizor al lui zero.

Demonstraţie. (a) este evidentă. (b). Fie $f = a_0 + a_1X + \cdots + a_nX^n$ şi $g = b_0 + b_1X + \cdots + b_mX^m$ cu $a_n, b_m \neq 0$. Deci $grad(f) = n$ şi $grad(g) = m$. Dacă $k > m + n$ atunci $\sum_{i+j=k} a_ib_j = 0$ deoarece $i + j = k$ implică $i > n$ sau $j > m$. Deci $grad(fg) \leq grad(f) + grad(g)$. $grad(fg) = m + n$ dacă şi numai dacă coeficientul a_nb_m al lui X^{m+n} este nenul. (c) rezultă din (b). •

Corolarul 76 *Fie A un domeniu. Atunci $A[X]$ este domeniu şi $U(A[X]) = U(A)$.*

Demonstraţie. Prima afirmaţie rezultă din punctul (c) al teoremei anterioare. Fie $f, g \in A[X]$ cu $fg = 1$. Din teorema precedentă, rezultă că f, g sunt polinoame constante (i.e. de grad zero). •

Fie L un corp comutativ. Corpul de fracţii al inelului de polinoame $L[X]$ se numeşte *corpul fracţiilor raţionale peste* L şi se notează cu $L(X)$. O *fracţie raţională* este un cât de două polinoame P/Q cu $Q \neq 0$.

Teorema 77 *Fie $u : A \to B$ un morfism de inele comutative şi $x \in B$. Atunci funcţia $v : A[X] \to B$,*

$$v(a_0 + a_1X + \cdots + a_nX^n) = u(a_0) + u(a_1)x + \cdots + u(a_n)x^n$$

este un morfim de inele.

Demonstraţie. Fie $f = \sum_{i=0}^{m} a_iX^i$ şi $g = \sum_{j=0}^{n} b_jX^j$, $f, g \in A[X]$. Avem

$$v(fg) = v(\sum_{k=0}^{m+n} \sum_{i+j=k} a_ib_j)X^k = \sum_{k=0}^{m+n} \sum_{i+j=k} u(a_i)u(b_j))x^k =$$

$$= (\sum_{i=0}^{m} u(a_i)x^i)(\sum_{j=0}^{n} u(b_j)x^j) = v(f)v(g).$$

Verificarea egalităţii $v(f + g) = v(f) + v(g)$ se face analog. •

Fie A un subinel al inelului B şi $x \in B$. Dacă $f = a_0+a_1X+\cdots+a_nX^n \in A[X]$ atunci $f(x) = a_0 + a_1x + \cdots + a_nx^n$ se numeşte valoarea lui f în x. Funcţia $\tilde{f} : B \to B$, $\tilde{f}(y) = f(y)$ se numeşte funcţia polinomială asociată lui f. De exemplu, dacă $g = X^2 + X \in \mathbf{Z}_2[X]$, atunci $\tilde{g}$ este funcţia nulă.

4.6 Rădăcini ale polinoamelor

Teorema 78 (Teorema împărţirii cu rest.) *Fie A un inel comutativ şi fie $f, g \in A[X]$ astfel încât g este polinom nenul cu coeficientul dominant inversabil (e.g. g unitar). Atunci există şi sunt unice polinoamele $q, r \in A[X]$ astfel încât*

$$f = gq + r \quad cu \quad grad(r) < grad(g).$$

Polinoamele f, g, q, r se numesc deîmpărţit, împărţitor, cât şi repectiv rest, iar egalitatea $f = gq + r$ se numeşte identitatea împărţirii.

Demonstraţie. Fie $r = f - gq$ polinomul de grad cel mai mic între toate polinoamele de forma $f - gw$ cu $w \in D[X]$. Dacă $grad(f - gq) \geq grad(g)$, atunci fie αX^n monomul conducător al lui $f - gq$ şi βX^m monomul conducător al lui g. Atunci $f - gq - \alpha\beta^{-1}X^{n-m}g$ este un polinom de grad $< grad(f - gq)$, contradicţie.

Probăm unicitatea lui q şi r. Fie $q', r' \in D[X]$ astfel încât $f = gq' + r'$ şi $grad(r') < grad(g)$. Scăzând cele două expresii ale lui f rezultă $g(q - q') = r' - r$ şi $grad(r' - r) < grad(g)$. Aplicăm teorema 75. Cum g are coeficientul dominant inversabil, rezultă că $r' - r = 0$, altfel $grad(r' - r) = grad(g(q - q')) \geq grad(g)$. Aşadar $r' = r$ şi din egalitatea $g(q - q') = 0$ rezultă $q' = q$, din nou pentru că g are coeficientul dominant inversabil. •

Fie A un inel comutativ nenul, $f \in A[X]$ şi $\alpha \in A$. Spunem că α este *rădăcină* a lui f dacă $f(\alpha)$=0. De exemplu, $X^2 - 1 \in \mathbf{R}[X]$ are rădăcinile ± 1.

Corolarul 79 (teorema lui Bézout.) *Fie A un inel comutativ, $f \in A[X]$ şi $\alpha \in A$. Atunci restul împărţirii lui f la $X - \alpha$ este $f(\alpha)$. În particular, α este rădăcină a lui $f \Leftrightarrow X - \alpha$ divide f.*

Demonstraţie. Există $q \in A[X]$ şi $r \in A$ cu $f = (X - \alpha)q + r$. Făcând $X = \alpha$ obţinem $r = f(\alpha)$. •

Corolarul 80 *Fie D un domeniu, $0 \neq f \in D[X]$, $\alpha \in D$ o rădăcină a lui f şi $n \geq 1$. Atunci $(X - \alpha)^n$ divide f şi $(X - \alpha)^{n+1}$ nu divide $f \Leftrightarrow f$ se scrie $f = (X - \alpha)^n g$ cu $g \in D[X]$, $g(\alpha) \neq 0$.*

Demonstraţie. Rezultă din teorema lui Bézout. •

Dacă f satisface condiţiile echivalente din corolarul precedent, spunem că α este rădăcină a lui f cu *ordinul de multiplicitate* n. De exemplu, 2 este rădăcină de ordin 3 (triplă) a polinomului $X^5 - 5X^4 + 7X^3 - 2X^2 + 4X - 8$.

Teorema 81 *Fie D un domeniu, $0 \neq f \in D[X]$, $\alpha_1, ..., \alpha_s \in D$ rădăcini distincte ale lui f respectiv de ordin $n_1, ..., n_s$. Atunci f se poate scrie sub forma*

$$f = (X - \alpha_1)^{n_1} \cdots (X - \alpha_s)^{n_s} g$$

unde $g \in D[X]$ şi $\alpha_1, ..., \alpha_s$ nu sunt rădăcini ale lui g.

Demonstraţie. Afirmaţia e clară dacă $s = 1$. Presupunem că $s \geq 2$. Deoarece α_1 este rădăcină a lui f de ordin n_1, putem scrie $f = (X - \alpha_1)^{n_1} h$ cu $h \in D[X]$ şi $h(\alpha_1) \neq 0$. Deducem că $0 = f(\alpha_2) = (\alpha_2 - \alpha_1)^{n_1} h(\alpha_2)$, deci $h(\alpha_2) = 0$. Scriem $h = (X - \alpha_2)^k p$ cu $p \in D[X]$ şi $p(\alpha_2) \neq 0$. Deci $f = (X - \alpha_1)^{n_1}(X - \alpha_2)^k p$ şi din corolarul precedent rezultă $k = n_2$. Aşadar, $f = (X - \alpha_1)^{n_1}(X - \alpha_2)^{n_2} p$. În continuare, se repetă argumentul precedent. •

Vom număra rădăcinile unui polinom numărând fiecare rădăcină de atâtea ori cât este ordinul ei de multiplicitate. De exemplu, polinomul $(X - 1)^3(X - 2)$ are 4 rădăcini şi anume $1, 1, 1, 2$. Din teorema precedentă rezultă

Corolarul 82 *Fie D un domeniu. Un polinom de grad $n \geq 1$ din $D[X]$ are cel mult n rădăcini în D.*

Ipoteza că inelul D este integru este esenţială, de exemplu, polinomul $(1, 0)X \in (\mathbf{Z} \times \mathbf{Z})[X]$ are o infinitate de rădăcini, $(0, a)$, $a \in \mathbf{Z}$.

Teorema 83 (Relaţiile lui Viétè.) *Fie D un domeniu şi $f = a_0 + a_1 X + \cdots + a_n X^n \in D[X]$ un polinom de grad $n \geq 1$. Presupunem că f are n rădăcini $\alpha_1, ..., \alpha_n \in D$. Atunci*

$$f = a_n(X - \alpha_1) \cdots (X - \alpha_n).$$

În plus, în corpul de fracţii al lui D, au loc aşa-numitele relaţiile ale lui Viétè

$$\begin{cases} \alpha_1 + \alpha_2 + \cdots + \alpha_n = -a_{n-1}/a_n \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n = a_{n-2}/a_n \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \alpha_1\alpha_2\cdots\alpha_n = (-1)^n a_0/a_n. \end{cases}$$

Demonstraţie. Din teorema 81, $f = b(X-\alpha_1)\cdots(X-\alpha_n)$ cu b polinom constant nenul. Identificând coeficienţii dominanţi, rezultă $b = a_n$. Relaţiile lui Viétè se obţin din identificarea celorlalţi coeficienţi. •

Corolarul 84 (Teorema lui Wilson.) *Dacă p este un număr prim, atunci*

$$(p-1)! \equiv -1 \ (mod\ p).$$

Demonstraţie. Considerăm corpul $\mathbf{Z}_p$. Grup său multiplicativ $\mathbf{Z}_p^*$ are $p-1$ elemente, deci $a^{p-1} = \widehat{1}$ pentru orice $a \in \mathbf{Z}_p^*$. Altfel spus, polinomul $X^{p-1} - \widehat{1} \in \mathbf{Z}_p[X]$ are rădăcinile $\widehat{1}$, ..., $\widehat{p-1}$. Din ultima relaţie Viétè rezultă că $(\widehat{p-1})! = -\widehat{1}$, deci $(p-1)! \equiv -1$ $(mod\ p)$. •

4.7 Inelul de polinoame $A[X_1, ..., X_n]$

Fie A un inel comutativ. Construcţia inelului de polinoame $A[X]$ a fost prezentată anterior. *Inelul de polinoame în n nedeterminate (variabile) cu coeficienţi în A* se defineşte inductiv prin egalitatea

$$A[X_1, ..., X_n] = A[X_1, ..., X_{n-1}][X_n] \text{ pentru } n \geq 2.$$

De exemplu, $A[X, Y] = A[X][Y]$. Deci elementele lui $A[X, Y]$ sunt polinoame în Y cu coeficienţi în $A[X]$. Elementele lui $A[X_1, ..., X_n]$ se numesc *polinoame în nedeterminatele $X_1, ..., X_n$ cu coeficienţi în A.*

Polinoamele de forma $M = aX_1^{i_1}\cdots X_n^{i_n}$ cu $a \in A$ se numesc *monoame.* a se numeşte coeficientul lui M, iar dacă $a \neq 0$, numărul $i_1 + \cdots i_n$ se numeşte *gradul* lui M. Monoamele nenule $M = aX_1^{i_1}\cdots X_n^{i_n}$ şi $N = bX_1^{j_1}\cdots X_n^{j_n}$ se zic *monoame asemenea* dacă $i_1 = j_1$,...,$i_n = j_n$. De exemplu, monoamele unitare (i.e. cu coeficientul 1) de gradul 3 în nedeterminatele X, Y sunt X^3, X^2Y, XY^2 şi Y^3.

Teorema 85 *Orice polinom din $f \in A[X_1, ..., X_n]$ se scrie în mod unic ca sumă de monoame (mutual neasemenea). Această scriere se numeşte forma canonică lui f.*

Demonstraţie. Procedăm prin inducţie după n, cazul $n = 1$ fiind cunoscut. Deoarece pasul inductiv se face în spiritul cazului $n = 2$, preferăm, din motive de claritate, să prezentăm doar acest caz. Renotăm $X_1 = X$ şi $X_2 = Y$. Fie $f \in A[X, Y]$. Atunci $f = \sum_{j=0}^{n} f_j Y^j$ cu $f_j = \sum_{i=0}^{m} a_{ij} X^i$, $a_{ij} \in A$, pentru $j = 0, ..., n$. Rezultă că

$$f = \sum_{j=0}^{n} (\sum_{i=0}^{m} a_{ij} X^i) Y^j = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{ij} X^i Y^j$$

deci f se scrie ca sumă de monoame. Pentru a proba unicitatea scrierii, fie $f = \sum_{i=0}^{m} \sum_{j=0}^{n} b_{ij} X^i Y^j$, $b_{ij} \in A$, o altă reprezentare a lui f ca sumă de monoame. Din egalitatea de polinoame în Y, $\sum_{j=0}^{n} (\sum_{i=0}^{m} a_{ij} X^i) Y^j = \sum_{j=0}^{n} (\sum_{i=0}^{m} b_{ij} X^i) Y^j$ rezultă că $\sum_{i=0}^{m} a_{ij} X^i = \sum_{i=0}^{m} b_{ij} X^i$ pentru $j = 0, ..., n$, deci $a_{ij} = b_{ij}$ pentru orice i şi j. $\bullet$

Folosind corolarul 76, se arată inductiv că dacă A este domeniu (e.g., dacă A este corp), atunci $A[X_1, ..., X_n]$ este domeniu pentru orice n.

Gradul unui polinom este maximul gradelor monoamelor sale. Gradul polinomului nul se ia $-\infty$. Un polinom se numeşte polinom omogen dacă toate monoamele sale au acelaşi grad. Prin *componenta omogenă* de grad k, f_k, a unui polinom f înţelegem suma monoamelor de grad k din f. De exemplu, polinomul $f = 1 + XY + YZ + XZ + XYZ$ are gradul 3 şi componentele omogene $f_0 = 1$, $f_1 = 0$, $f_2 = XY + YZ + XZ$ şi $f_3 = XYZ$. Proprietăţile gradului din cazul polinoamelor într-o nedeterminată se extind uşor la polinoamele în mai multe nedeterminate.

Este clar că produsul a două monoame de grad m respectiv n este monomul nul sau un monom de grad $m + n$ după cum produsul coeficienţilor lor este nul sau nenul. De asemenea, se vede uşor că produsul a două polinoame omogene de grad m respectiv n este polinomul nul sau un polinom omogen de grad $m + n$.

Teorema 86 *Fie A un inel comutativ, $n \geq 1$ şi $f, g \in A[X_1, ..., X_n]$. Atunci*

(*a*) *grad*$(f+g) \leq$ *max*(*grad*(f), *grad*(g)),
(*b*) *grad*$(fg) \leq$ *grad*(f) + *grad*(g) *cu egalitate dacă* A *este domeniu.*

Demonstraţie. (*a*) este evidentă. (*b*). Putem presupune că f şi g sunt nenule, altfel afirmaţia este banală. Fie $k = grad(f)$ şi $l = grad(g)$. Scriem pe f şi g ca sumă de componente omogene: $f = f_0 + f_1 + \cdots f_k$ şi $g = g_0 + g_1 + \cdots g_l$ cu f_k, g_l nenule. Atunci $fg = \sum_{i=1}^{k} \sum_{j=1}^{l} f_i g_j$, unde fiecare termen nenul $f_i g_j$ este un polinom omogen de grad $i + j \leq k + l$. Deci $grad(fg) \leq k + l$. Dacă, în plus, A este domeniu, atunci $f_k g_l$ este un polinom omogen de grad $k + l$ şi $grad(f_i g_j) < k + l$ pentru orice $(i, j) \neq (k, l)$. Deci $grad(fg) = k + l$. •

Fie $A \subseteq B$ o extindere de inele şi $b_1, ..., b_n \in B$ elemente fixate. Dacă $f \in A[X_1, ..., X_n]$, numim valoarea lui f în $b_1, ..., b_n$ elementul $f(b_1, ..., b_n) \in B$ obţinut din f prin înlocuirea fiecărei nedeterminate X_i cu b_i. Altfel zis, dacă $f = \sum a_{i_1 \ldots i_n} X_1^{i_1} \cdots X_n^{i_n}$, atunci $f(b_1, ..., b_n) = \sum a_{i_1 \ldots i_n} b_1^{i_1} \cdots b_n^{i_n}$. De exemplu, dacă $f = X_1^3 + \cdots X_n^3$, atunci $f(1, ..., n) = n^2(n+1)^2/4$.

Teorema 87 *Cu notaţiile anterioare, funcţia* $\pi : A[X_1, ..., X_n] \to B$, $\pi(f) = f(b_1, ..., b_n)$, *este un morfism de inele.*

Demonstraţie. Procedăm prin inducţie după n, cazul $n = 1$ fiind cunoscut din teorem 77. Presupunem că $n \geq 2$ şi fie $f, g \in A[X_1, ..., X_n]$. Scriem f, g ca polinoame în X_n cu coeficienţi în $A[X_1, ..., X_{n-1}]$, $f = \sum_{i=0}^{p} f_i X_n^i$ şi $g = \sum_{j=0}^{p} g_j X_n^j$. Atunci $f + g = \sum_{i=0}^{p} (f_i + g_i) X_n^i$ şi $fg = \sum_{i,j=0}^{p} (f_i g_j) X_n^{i+j}$. Folosind ipoteza de inducţie obţinem

$$(f+g)(b_1, ..., b_n) = \sum_{i=0}^{p} (f_i + g_i)(b_1, ..., b_{n-1}) b_n^i =$$

$$= \sum_{i=0}^{p} (f_i(b_1, ..., b_{n-1}) + g_i(b_1, ..., b_{n-1})) b_n^i =$$

$$= \sum_{i=0}^{p} f_i(b_1, ..., b_{n-1}) b_n^i + \sum_{i=0}^{p} g_i(b_1, ..., b_{n-1}) b_n^i = f(b_1, ..., b_n) + g(b_1, ..., b_n).$$

De asemenea,

$$(fg)(b_1, ..., b_n) = \sum_{i,j=0}^{p} (f_i g_j)(b_1, ..., b_{n-1}) b_n^{i+j} =$$

$$= \sum_{i,j=0}^{p} (f_i(b_1, ..., b_{n-1}) g_i(b_1, ..., b_{n-1})) b_n^{i+j} =$$

$$= (\sum_{i=0}^{p} f_i(b_1, ..., b_{n-1}) b_n^i)(\sum_{j=0}^{p} g_j(b_1, ..., b_{n-1}) b_n^j) = f(b_1, ..., b_n) g(b_1, ..., b_n). \bullet$$

4.8 Exerciţii

103. Fie K un corp. Arătaţi că grupul aditiv $(K, +)$ nu este izomorf cu grupul multiplicativ $(K^*, \cdot)$.

104. Fie A un inel şi $a, b \in A$. Arătaţi că dacă $1 - ab$ este inversabil, atunci $1 - ba$ este inversabil.

105. Determinaţi unităţile inelului $\mathbf{Z}_{(2)} = \{a/b |\ a, b \in \mathbf{Z},\ b \text{ impar}\}$.

106. Fie S o mulţime de numere prime (eventual vidă) şi fie $\mathbf{Z}_S$ mulţimea fracţiilor a/b cu a, b numere întregi şi $b \neq 0$ cu toţi factorii primi în S. Arătaţi că $\mathbf{Z}_S$ este un subinel al lui $\mathbf{Q}$ şi că orice subinel al lui $\mathbf{Q}$ este de această formă.

107. Fie A o mulţime. Arătaţi că inelele $\mathbf{Z}_2^A$ şi $(\mathcal{P}(A), \Delta, \cap)$ sunt izomorfe.

108. Arătaţi că idealele bilaterale ale inelului $M_2(\mathbf{Z})$ sunt $M_2(n\mathbf{Z})$, $n \geq 0$, unde $M_2(n\mathbf{Z})$ este mulţimea matricelor cu toate elementele multipli de n. In plus, $M_2(\mathbf{Z})/M_2(n\mathbf{Z}) \simeq M_2(\mathbf{Z}_n)$. Generalizare.

109. Fie A şi B două inele comutative. Arătaţi că idealele inelului produs direct $A \times B$ sunt de forma $I \times J$ cu I ideal al lui A şi J ideal al lui B. In plus, $(A \times B)/(I \times J) \simeq A/I \times B/J$.

110. Fie A inelul al cărui grup abelian este $\mathbf{Z} \times \mathbf{Q}$ şi are înmulţirea definită prin $(a, x)(b, y) = (ab, ay + bx)$. Arătaţi că idealele lui A sunt de forma $n\mathbf{Z} \times \mathbf{Q}$, $n \in \mathbf{N}$, sau $\{0\} \times H$ cu H subgrup al lui $\mathbf{Q}$.

111. Calculaţi tablele adunării/înmulţirii pentru următoarele inele factor: $\mathbf{Z}_2[X]\ /(X^2 + X + \hat{1})$, $\mathbf{Z}_2[X]/(X^2 + X)$, $\mathbf{Z}_2[X]/(X^2 + \hat{1})$ şi $\mathbf{Z}_2[X]/(X^2)$.

112. Arătaţi că inelele $\mathbf{Z}_4$, $\mathbf{Z}_2 \times \mathbf{Z}_2$, $\mathbf{Z}_2[X]/X^2\mathbf{Z}_2[X]$ şi $\mathbf{Z}_2[X]/(X^2 + X + \hat{1})\mathbf{Z}_2[X]$ sunt două câte două neizomorfe şi că orice inel cu 4 elemente este izomorf cu unul dintre acestea.

113. Descrieţi elementele inelului $\mathbf{Z}[i]/(3)$ şi explicitaţi endomorfismul lui Frobenius.

114. Fie A un inel comutativ şi fie $f \in A[X]$. Arătaţi că:

(a) f este nilpotent dacă şi numai dacă f are toţi coeficienţii nilpotenţi (un element x al unui inel se zice nilpotent dacă există n cu $x^n = 0$).

(b) f este inversabil dacă şi numai dacă f are termenul liber inversabil şi ceilalţi coeficienţi nilpotenţi.

(c) f este divizor al lui zero dacă şi numai dacă $af = 0$ pentru un a nenul din A.

115. Listaţi idealele inelului $A = \mathbf{Z}_2[X]/(X^2)$.

116. Arătaţi că idealul I generat de 2 şi X în $\mathbf{Z}[X]$ nu este principal.

117. Fie A un domeniu. Arătaţi că idealul generat de X şi Y în $A[X, Y]$ nu este principal.

118. Fie A inelul şirurilor de numere reale. Arătaţi că mulţimea I a şirurilor cu un număr finit de termeni nenuli formează un ideal al lui A care nu este finit generat.

119. Fie $\mathbf{Z} + X\mathbf{Q}[X]$ subinelul lui $\mathbf{Q}[X]$ format din polinoamele f cu $f(0) \in \mathbf{Z}$. Arătaţi că idealul $X\mathbf{Q}[X]$ nu este finit generat.

120. Arătaţi că inelul factor $\mathbf{Z}[i]/(1 + i)\mathbf{Z}[i]$ este izomorf cu $\mathbf{Z}_2$.

121. Arătaţi că au loc izomorfismele de inele $\mathbf{Z}[i]/(2 + i)\mathbf{Z}[i] \simeq \mathbf{Z}_5$ şi $\mathbf{Z}[i]/5\mathbf{Z}[i] \simeq \mathbf{Z}_5 \times \mathbf{Z}_5$.

122. Arătaţi că inelul factor $\mathbf{Z}[X]/(X^2 - X)$ este izomorf cu $\mathbf{Z} \times \mathbf{Z}$.

123. Arătaţi că inelul factor $\mathbf{Q}[X]/(X^2 - 1)$ este izomorf cu $\mathbf{Q} \times \mathbf{Q}$, dar că $\mathbf{Z}[X]/(X^2 - 1)$ nu este izomorf cu $\mathbf{Z} \times \mathbf{Z}$.

124. Arătaţi că inelul factor $\mathbf{Z}[X]/(X^2-1)$ este izomorf cu $A = \{(x,y) \in \mathbf{Z}^2 |\ x-y \text{ par}\}$.

125. Fie K un corp comutativ, $a_1, ..., a_n \in K$ distincte şi $f = (X - a_1)\cdots(X-a_n)$. Arătaţi că inelul factor $K[X]/(f)$ este izomorf cu K^n.

126. Arătaţi că inelul factor $\mathbf{Z}[X]/(2)$ este izomorf cu $\mathbf{Z}_2[X]$.

127. Arătaţi că inelul factor $\mathbf{Q}[X,Y]/(Y^2-X^3)$ este izomorf cu subinelul A al lui $\mathbf{Q}[T]$ format din polinoamele ce nu au monom de gradul 1.

128. Arătaţi că inelul factor $\mathbf{R}[X,Y]/(X^2+Y^2)$ este izomorf cu subinelul A al lui $\mathbf{C}[T]$ format din polinoamele f cu $f(0)$ real.

129. Explicitaţi corpul de fracţii al domeniului $\mathbf{R}[X,Y]/(X^2+Y^2)$.

130. Arătaţi că inelul factor $\mathbf{R}[X]/(X^2+bX+c)$ este izomorf cu $\mathbf{R}\times\mathbf{R}$, $\mathbf{R}[X]/(X^2)$ sau $\mathbf{C}$ după cum $\Delta = b^2-4c$ este >0, $=0$, resp. <0.

131. Decideţi dacă inelele factor $\mathbf{Z}[X,Y]/(X-1,Y-2)$, $\mathbf{Q}[X,Y]/(X^2+1, Y^2-2)$ şi $\mathbf{R}[X,Y]/(X^2+1,Y^2+1)$ sunt domenii.

132. Fie A un inel comutativ şi $a \in A$. Arătaţi că inelul factor $A[X]/(X-a)$ este izomorf cu A. Generalizare.

133. Arătaţi că nu există un morfism surjectiv de inele $\pi : \mathbf{Z}[X,Y] \to \mathbf{Q}$.

134. Determinaţi mulţimile $A = \{Im(f)|\ f \text{ morfism de inele } \mathbf{Z}[X] \to \mathbf{Q}\}$ şi $B = \{Im(f)|\ f \text{ morfism de inele } \mathbf{Z}[X,Y] \to \mathbf{Q}\}$.

135. Arătaţi că inelele $\mathbf{Z}[X]$ şi $\mathbf{Z}[X,Y]$ nu sunt izomorfe.

136. Fie A un inel comutativ. Notăm cu $A^{\mathbf{N}}$ mulţimea şirurilor $(a_n)_{n\geq 0}$ cu elemente din A. Pe $A^{\mathbf{N}}$ definim două operaţii: adunarea $(a_n)_{n\geq0} + (b_n)_{n\geq0} = (a_n+b_n)_{n\geq0}$ şi înmulţirea $(a_n)_{n\geq0}(b_n)_{n\geq0} = (c_n)_{n\geq0}$ unde $c_n = \sum_{i+j=n} a_ib_j$. Arătaţi că faţă de aceste două operaţii, $A^{\mathbf{N}}$ este un inel comutativ şi că orice element al său se scrie unic sub forma $\sum_{n=0}^{\infty} a_nX^n$ cu $a_n \in A$, unde $X = (0,1,0,...)$. Acest inel se notează cu $A[[X]]$ şi se numeşte *inelul seriilor formale cu coeficienţi în A*.

137. Fie A un inel comutativ. Arătaţi că unităţile inelului $A[[X]]$ sunt seriile formale $\sum_{n=0}^{\infty} a_nX^n$ cu a_0 inversabil în A.

138. Determinaţi morfismele de inele $\mathbf{Z}[[X]] \to \mathbf{Z}$.

Capitolul 5

Aritmetica lui $\mathbf{Z}$ şi $K[X]$

În aceast capitol se studiază comparativ diferite proprietăţi aritmetice ale inelelor $\mathbf{Z}$ şi $K[X]$, K corp comutativ. Se expun mai întâi rezultate referitoare la teorema împărţirii cu rest, cel mai mare divizor comun şi cel mai mic multiplu comun. Se dau apoi rezultatele fundamentale referitoare la descompunerea unui număr întreg/polinom în produs de numere prime/polinoame ireductibile.

În acest capitol, prin corp înţelegem un corp comutativ.

5.1 Teorema împărţirii cu rest

Fie K un corp. Reamintim următorul rezultat stabilit anterior.

Teorema 88 (a) $K[X]$ *este domeniu de integritate.*

(b) *Pentru orice* $f, g \in K[X] \setminus \{0\}$, $grad(f+g) \leq max(grad(f), grad(g))$ *şi* $grad(fg) = grad(f) + grad(g)$.

(c) *Elementele inversabile ale inelului* $K[X]$ *sunt polinoamele constante nenule, altfel spus,* $U(K[X]) = K^*$.

Atât în $\mathbf{Z}$ cât şi în $K[X]$ este valabilă teorema împărţirii cu rest.

Teorema 89 (Teorema împărţirii cu rest pentru $\mathbf{Z}$ şi $K[X]$.) *Fie* $D = \mathbf{Z}$ *sau* $K[X]$. *Atunci pentru orice* $a, b \in D$, $b \neq 0$, *există şi sunt unice* $q, r \in D$ *astfel încât*

$$a = bq + r \quad cu \quad \begin{cases} 0 \leq r < |b| & dac\breve{a} \quad D = \mathbf{Z} \\ grad(r) < grad(b) & dac\breve{a} \quad D = K[X]. \end{cases}$$

Numerele/polinoamele a, b, q, r se numesc deîmpărţit, împărţitor, cât şi repectiv rest, iar egalitatea $a = bq + r$ se numeşte identitatea împărţirii.

Demonstraţie. Cazul $D = \mathbf{Z}$. Demonstrăm mai întâi existenţa lui q şi r. Fie $r = a - bq$ cel mai mic număr întreg ≥ 0 de forma $a - bx$ cu $x \in \mathbf{Z}$. Dacă $a - bq \geq |b|$, atunci $0 \leq a - b(q + \mathrm{sgn}(b)) < a - bq$, contradicţie. Probăm unicitatea lui q şi r. Fie $q', r' \in \mathbf{Z}$ astfel încât $a = bq' + r'$ şi $0 \leq r' < |b|$. Scăzând cele două expresii ale lui a rezultă $b(q - q') = r' - r$, deci $r' - r = 0$ deoarece $|r' - r| < |b|$. Aşadar $r' = r$ şi din egalitatea $b(q - q') = 0$ rezultă $q' = q$ deoarece $b \neq 0$. Cazul $D = K[X]$ a fost demonstrat în teorema 78.•

Exemple de împărţiri cu rest: în $\mathbf{Z}$, $-15 = 2 \cdot (-8) + 1$, în $\mathbf{Q}[X]$, $X^3 + X + 1 = (X^2 + X + 1)(X - 1) + X + 2$.

Din teorema 89 rezultă imediat

Corolarul 90 *Fie K un corp şi $f \in K[X]$ un polinom de grad $n \geq 1$. Atunci elementele inelului factor $K[X]/(f)$ se reprezintă unic sub forma $a_0 + a_1X + \cdots + a_{n-1}X^{n-1}) + (f)$ cu $a_0, a_1, ..., a_{n-1} \in K$. În particular, dacă K este finit cu q elemente, atunci $K[X]/(f)$ are q^n elemente.*

Demonstraţie. Fie $g \in K[X]$. Dacă $g = qf + a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$ este împărţirea cu rest a lui g la f, atunci $g + (f) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + (f)$. În plus, dacă $a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + (f) = b_0 + b_1X + \cdots + b_{n-1}X^{n-1} + (f)$ cu $a_i, b_i \in K$, atunci f divide $h = (a_0 - b_0) + (a_1 - b_1)X + \cdots + (a_{n-1} - b_{n-1})X^{n-1}$, deci $h = 0$, deoarece $grad(f) = n$. •

Fie $D = \mathbf{Z}$ sau $K[X]$ şi fie $a, b \in D$. Spunem că b *divide* a şi notăm $b \mid a$ dacă există $c \in D$ cu $a = bc$. Se mai spune că b este un divizor (factor) al lui a sau că a este multiplu de b. Dacă $b \neq 0$, atunci $b \mid a \Leftrightarrow$ restul împărţirii lui a la b este zero.

Pentru orice $a \in D$, $a \mid 0$ (deoarece $0 = a.0$), $a \mid a$ şi $1 \mid a$ (deoarece $a = a.1$). În $K[X]$, $c \mid f$ pentru orice $c \in K^*$ şi $f \in K[X]$, deoarece $f = c(c^{-1}f)$.

Elementele $a, b \in D$ se zic *asociate (în divizibilitate)*, dacă $a \mid b$ şi $b \mid a$. Divizibilitatea are următoarele proprietăţi.

Teorema 91 *Fie $D = \mathbf{Z}$ sau $K[X]$ şi fie $a, b, c \in D$. Atunci*

(a) $a \mid b$ dacă şi numai dacă $aD \supseteq bD$.

(b) Dacă $a \mid b$ şi $b \mid c$, atunci $a \mid c$.

(c) Dacă $a \mid b$ şi $a \mid c$, atunci $a \mid bb' + cc'$ pentru orice $b', c' \in D$.

(d) Dacă $a \mid b$, atunci

$$\begin{cases} |a| \leq |b| & \text{dacă} \quad D = \mathbf{Z} \\ grad(a) \leq grad(b) & \text{dacă} \quad D = K[X]. \end{cases}$$

(e) Elementele a, b sunt asociate dacă şi numai dacă

$$\begin{cases} a = \pm b & \text{dacă} \quad D = \mathbf{Z} \\ a = db \text{ cu } d \in K^* & \text{dacă} \quad D = K[X]. \end{cases}$$

Deci a, b sunt asociate dacă şi numai dacă există $u \in U(D)$ astfel încât $a = ub$.

Demonstraţie.

(a). Avem şirul de echivalenţe $a \mid b \Leftrightarrow b \in aD \Leftrightarrow aD \supseteq bD$.

(b). Cf. (a), $aD \supseteq bD \supseteq cD$, deci $a \mid c$.

(c). Fie $b', c' \in D$. Cum $a \mid b$ şi $a \mid c$, rezultă că $b, c \in aD$, deci $bb' + cc' \in aD$, deoarece aD este ideal.

(d) este evidentă.

(e). Cazul $D = \mathbf{Z}$ e clar. Presupunem că $D = K[X]$. Dacă $f = dg$ cu $d \in K^*$, atunci $g = d^{-1}f$, deci $f \mid g$ şi $g \mid f$. Reciproc, să presupunem că $f \mid g$ şi $g \mid f$. Deci există $u, v \in K[X]$ cu $g = fu$ şi $f = gv$. Rezultă $f = fuv$. Dacă $f = 0$, atunci $g = fu = 0$ şi putem scrie $f = 1g$. Dacă $f \neq 0$, atunci $uv = 1$, deci $u, v \in K^*$. •

Observaţia 92 Fie $K \subseteq L$ o extindere de corpuri şi $f, g \in K[X] \setminus \{0\}$. Atunci $f \mid g$ în $K[X] \Leftrightarrow f \mid g$ în $L[X]$. Aceasta rezultă din faptul că identitatea împărţirii lui g la f este aceeaşi în $K[X]$ şi $L[X]$.

Fie $D = \mathbf{Z}$ sau $K[X]$ şi fie $a, b, d, m \in D$. Spunem d este un *cel mai mare divizor comun* (cmmdc) al perechii a, b dacă $d \mid a$, $d \mid b$ şi d se divide cu orice alt divizor comun al elementelor a, b. În acest caz vom scrie $d = (a, b)$. Dacă $(a, b) = 1$, se zice că a, b sunt *relativ prime* sau că a este prim cu b. Dual, spunem că m este un *cel mai mic multiplu comun* (cmmmc) al perechii a, b

dacă $a \mid m$, $b \mid m$ şi m divide orice alt multiplu comun al elementelor a, b. În acest caz vom scrie $m = [a, b]$. Evident, dacă $a \mid b$, atunci $(a, b) = a$ şi $[a, b] = b$. Vom arăta că în **Z** şi $K[X]$ orice pereche de elemente are cmmdc şi cmmmc.

Fie $a, b, d, d' \in D$ astfel încât atât d cât şi d' joacă rol de cmmdc pentru perechea a, b. Din definiţie rezultă că d şi d' sunt asociate. Din teorema 91 pct. (e), rezultă că (a, b) este determinat până la semn în cazul $D = \mathbf{Z}$, resp. până la o multiplicare cu o constantă nenulă din K în cazul $D = K[X]$. Convenim să alegem pe $(a, b) \geq 0$ în primul caz, resp. un polinom unitar sau zero în cel de-al doilea caz. Aceste alegeri se numesc *alegerile canonice*. Consideraţii similare se pot face pentru cmmmc. De exemplu, în **Z**, $(-18, 24) = 6$; în $\mathbf{Q}[X]$, $(2X - 1, -3X^2) = 1$.

În **Z** şi $K[X]$ orice pereche de elemente are cmmdc şi acesta se poate calcula cu algoritmul lui Euclid.

Teorema 93 (Algoritmul lui Euclid.) *Fie D egal cu* **Z** *sau $K[X]$. Următorul algoritm furnizează cel mai mare divizor comun al unei perechi de elemente $a, b \in D$.*

input: $a, b \in D$
output: $d = (a, b)$

while $b \neq 0$ do
begin
  se face împărţirea cu rest: $a = bq + r$ cu $q, r \in D$ (cf. Teoremei 89);
  $a := b$; $b := r$;
end;
$d := a$;

Demonstraţie. E suficient să observăm următoarele. Conform pct. (c) din teorema 91, perechile $(a = bq + r, b)$ şi (b, r) au aceeaşi divizori comuni, deci acelaşi cel mai mare divizor comun. Aşadar putem înlocui perechea (a, b) cu perechea (b, r). La fiecare parcurgere a buclei *while* modulul lui b dacă $D = \mathbf{Z}$ (resp. gradul lui b dacă $D = K[X]$) scade cu cel puţin o unitate. Deci algoritmul se termină după un număr finit de paşi cu o pereche de forma $(a, 0)$, care are cmmdc egal cu a. •

Să considerăm exemplul $D = \mathbf{Z}$, $a = 18$ şi $b = 24$. În timpul desfăşurării algoritmului lui Euclid, variabilele a, b, r iau succesiv valorile: $a = 18, 24, 18, 6$, $b = 24, 18, 6, 0$, $r = 18, 6, 0$. Deci $(18, 24) = 6$.

Teorema 94 *Fie $D = \mathbf{Z}$ sau $K[X]$. Atunci orice ideal al lui D este principal.*

Demonstraţie. Afirmaţia este clară în cazul idealului nul. Fie I un ideal nenul şi fie $g \in I \setminus \{0\}$, g de modul minim în cazul $D = \mathbf{Z}$ resp. g de grad minim în cazul $D = K[X]$. Arătăm că $I = gD$. Incluziunea $\supseteq$ e clară. Pentru a proba incluziunea $\subseteq$, fie $f \in I$. Conform teoremei de împărţire cu rest, există $q, r \in D$ astfel încât $f = gq + r$ cu $0 \leq r < |g|$ în cazul $D = \mathbf{Z}$, respectiv $grad(r) < grad(g)$ în cazul $D = K[X]$. Cum $r = f - gq \in I$, r nu poate fi decât nul, altfel contrazicem alegerea lui g. Deci $f = gq \in gD$. •

Conform pct. (e) din teorema 91, generatorul g al idealului nenul I este determinat până la semn în cazul $D = \mathbf{Z}$, resp. până la o multiplicare cu o constantă nenulă din K în cazul $D = K[X]$.

Teorema 95 *Fie $D = \mathbf{Z}$ sau $K[X]$ şi fie $a, b \in D$. Atunci (a, b) şi $[a, b]$ există şi au loc relaţiile:*
(a) $aD + bD = (a, b)D$,
(b) $aD \cap bD = [a, b]D$, şi
(c) elementele $(a, b)[a, b]$ şi ab sunt asociate.

Demonstraţie. (a) Cf. Teoremei 94, există $d \in D$ astfel încât $aD + bD = dD$. Atunci $dD = aD + bD \subseteq eD$, deci $e \mid d$.

(b). Cf. Teoremei 94, există $m \in D$ astfel încât $aD \cap bD = mD$. Deoarece $m \in aD \cap bD$, rezultă că $a \mid m$ şi $b \mid m$. Fie $n \in D$ un multiplu comun al lui a şi b. Rezultă că $n \in aD \cap bD = mD$, deci $m \mid n$.

(c). Punem $d = (a, b)$ şi $m = [a, b]$. Dacă $a = 0$ sau $b = 0$, afirmaţia e clară. Presupunem că a, b sunt nenule, deci d, m sunt nenule. Elementul $ab/d \in D$ se divide cu a şi b. Rezultă că $m \mid (ab/d)$, deci dm divide ab. Evident $m \mid ab$, deci $ab/m \in D$. În plus ab/m este un divizor comun al lui a şi b. Deci $(ab/m) \mid d$, adică $ab \mid dm$. Aşadar ab şi dm sunt asociate. •

Teorema următoare cuprinde câteva proprietăţi ale celui mai mare divizor comun.

Teorema 96 *Fie* $D = \mathbf{Z}$ *sau* $K[X]$ *şi fie* $a, b, c \in D \setminus \{0\}$.

(a) *Dacă* $d = (a, b)$, *atunci există* $a', b' \in D$ *astfel încât* $d = aa' + bb'$.

(b) a, b *sunt relativ prime dacă şi numai dacă există* $a', b' \in D$ *astfel încât* $1 = aa' + bb'$.

(c) *Dacă* $d = (a, b)$, *atunci* a/d, b/d *sunt relativ prime.*

(d) (ac, bc) *şi* $(a, b)c$ *sunt asociate.*

(e) *Dacă* a, b *sunt prime cu* c, *atunci* ab *este prim cu* c.

(f) *Dacă* $a \mid bc$ *şi* a *este prim cu* b, *atunci* $a \mid c$.

Demonstraţie. Afirmaţia (a) rezultă din pct. (a) al Teoremei 95, (b) rezultă din (a), iar (c) rezultă din (a) şi (b).

(d). Fie $d = (a, b)$. Cf. Teoremei 95, $aD + bD = dD$. De aici rezultă uşor că $acD + bcD = cdD$, deci $cd = (ac, bc)$.

(e). Cum a, b sunt prime cu c, putem scrie $1 = au + cv$, $1 = bu' + cv'$ cu $u, u', v, v' \in D$. Înmulţind aceste relaţii avem $1 = ab(uu') + c(bu'v + auv' + cvv')$, deci ab este prim cu c, cf. (b).

(f). Din (d) rezultă că (ac, bc) şi c sunt asociate. Cum $a \mid ac$ şi $a \mid bc$, deducem că $a \mid c$. •

Fie $D = \mathbf{Z}$ sau $K[X]$. Definiţia cmmdc/cmmmc dată înaintea Teoremei 93, se poate extinde cu uşurinţă de la două elemente la un număr finit de elemente din D. Fie $a_1, ..., a_n, d \in D$, $n \geq 2$. Spunem d este un cmmdc al elementelor $a_1, ..., a_n$ dacă $d \mid a_i$ pentru $i = 1, ..., n$ şi d se divide cu orice alt divizor comun al elementelor $a_1, ..., a_n$. În acest caz vom scrie $d = (a_1, ..., a_n)$.

De asemenea, m este un cmmmc al elementelor $a_1, ..., a_n$ dacă $a_i \mid m$ pentru $i = 1, ..., n$ şi m divide cu orice alt multiplu comun al elementelor $a_1, ..., a_n$. În acest caz vom scrie $m = [a_1, ..., a_n]$.

Teorema 95 se poate extinde în modul următor.

Teorema 97 *Fie* $D = \mathbf{Z}$ *sau* $K[X]$ *şi fie* $a_1, ..., a_n \in D$ *cu* $n \geq 2$. *Atunci* $(a_1, ..., a_n)$ *şi* $[a_1, ..., a_n]$ *există şi au loc egalităţile:*

(a) $a_1D + \cdots + a_nD = (a_1, ..., a_n)D$,

(b) $a_1D \cap \cdots \cap a_nD = [a_1, ..., a_n]D$, *şi*

(c) $(a_1, ..., a_n) = (a_1, (a_2, ..., a_n))$.

Demonstraţie. Pentru (a) şi (b) se adaptează demonstraţia Teoremei 95. Vom ilustra demonstraţia lui (c) pe cazul $n = 3$. Fie $a, b, c, d, e \in D$ astfel încât $d = (b, c)$ şi $e = (a, d)$. Arătăm că $e = (a, b, c)$. Din relaţiile $e \mid a$, $e \mid d$,

$d \mid b$ şi $d \mid c$, rezultă că e este un divizor comun al elementelor a, b, c. Acum fie f un divizor comun al elementelor a, b, c. Deducem că $f \mid d$ şi $f \mid a$, deci $f \mid e$. •

5.2 Numere prime, polinoame ireductibile

Un număr întreg $p \neq 0, \pm 1$ se numeşte *număr prim* dacă p nu se poate scrie ca produsul a două numere întregi diferite de ± 1, alfel zis, dacă p nu are decât divizorii ± 1, $\pm p$. Un număr întreg diferit de 0, ± 1 şi neprim se numeşte *număr compus*. De exemplu, 3, -7, 17 sunt numere prime în timp ce -21, 15, 60 sunt compuse.

Conceptul omolog în $K[X]$ celui de număr prim este cel de polinom ireductibil. Un polinom neconstant (adică de grad ≥ 1) $f \in K[X]$ se numeşte *polinom ireductibil* dacă f nu se poate scrie ca produs de două polinoame neconstante, alfel zis, dacă f nu are decât divizorii a şi af cu $a \in K^*$. Un polinom neconstant non-ireductibil se numeşte *polinom reductibil*. De exemplu, în $\mathbf{Q}[X]$, X este ireductibil, X^2 este reductibil iar problema (i)reductibilităţii lui 3 nu se poate pune.

Teorema 98 *În $K[X]$,*

(a) *polinoamele de gradul* 1 *sunt ireductibile,*

(b) *un polinom ireductibil de grad ≥ 2 nu are rădăcini în K, şi*

(c) *un polinom de grad* 2 *sau* 3 *este ireductibil dacă şi numai dacă nu are rădăcini în K.*

Demonstraţie. (a) este evidentă. (b) şi (c) rezultă din următoarele observaţii. Un polinom are un factor $aX + b$ de gradul 1 dacă şi numai dacă are rădăcina $-b/a \in K$. Pe de altă parte, un polinom de grad 2 sau 3 este reductibil dacă şi numai dacă are un factor de gradul 1. •

De exemplu, $X^2 - 2$ este polinom ireductibil în $\mathbf{Q}[X]$ neavând rădăcini în $\mathbf{Q}$, dar reductibil în $\mathbf{R}[X]$, $X^2 - 2 = (X + \sqrt{2})(X - \sqrt{2})$. Polinomul $(X^2+1)(X^2+2)$ este reductibil în $\mathbf{Q}[X]$ dar nu are rădăcini în $\mathbf{Q}$. Polinoamele de grad 2 sau 3 ireductibile din $\mathbf{Z}_2[X]$ sunt cele fără rădăcini în $\mathbf{Z}_2$: $X^2+X+\hat{1}$, $X^3 + X + \hat{1}$ şi $X^3 + X^2 + \hat{1}$. $X^4 + X + \hat{1}$ este ireductibil în $\mathbf{Z}_2[X]$ deoarece nu are rădăcini şi nu este pătratul lui $X^2 + X + \hat{1}$.

Fie $D = \mathbf{Z}$ resp. $K[X]$, $p \in D$ un număr prim resp. polinom ireductibil şi $a \in D$. Din definiţii, rezultă că $p \mid a$ sau $(a,p) = 1$.

Teorema 99 *Fie $D = \mathbf{Z}$ sau $K[X]$ şi $p \in D$ un element nenul şi neinversabil. Atunci p este prim în cazul $D = \mathbf{Z}$ resp. ireductibil în cazul $D = K[X]$ dacă şi numai dacă satisface condiţia:*

$$a, b \in D \text{ şi } p \mid ab \Rightarrow p \mid a \text{ sau } p \mid b.$$

Demonstraţie. Presupunem că p este prim în cazul $D = \mathbf{Z}$ resp. ireductibil în cazul $D = K[X]$. În plus, presupunem că p nu divide pe a. Cum p este număr prim resp. polinom ireductibil, rezultă că $(p,a) = 1$. Cf. teoremei 96, $p \mid b$. Reciproc, să presupunem că p este număr compus. Deci $p = ab$ cu $a, b \in \mathbf{Z}$ şi $1 < |a|, |b| < |p|$. Atunci $p \mid ab$ dar $p \not| \, a$ şi $p \not| \, b$. De asemenea, să presupunem că $p \in K[X]$ este polinom reductibil. Deci $p = ab$ cu $a, b \in K[X]$ şi $0 < grad(a), grad(b) < grad(p)$. Atunci $p \mid ab$ dar $p \not| \, a$ şi $p \not| \, b$. •

Teorema 100 (Euclid)
(a) *Orice număr întreg diferit de* 0, ± 1 *se poate scrie ca produs de numere prime.*
(b) *Orice polinom neconstant $f \in K[X]$ se poate scrie ca produs de polinoame ireductibile.*
Descompunerile de la (a) *şi* (b) *sunt unice (vezi Teorema 102).*

Demonstraţie. (a). Presupunem că există întregi diferiţi de 0, ± 1 care nu se pot scrie ca produs de numere prime. Fie N cel mai mic întreg pozitiv cu această proprietate. Cum N nu este prim, putem scrie $N = ab$ cu $1 < a, b < N$. Datorită alegerii lui N, numerele a şi b se pot scrie ca produs de numere prime. Dar atunci şi $N = ab$ este produs de prime, contradicţie.

(b). Adaptăm demonstraţia de la (a). Presupunem că există polinome neconstante care nu se pot scrie ca produs de polinoame ireductibile. Fie H un astfel de polinom de grad minim. Cum H nu este ireductibil, putem scrie $H = fg$ cu f, g polinoame neconstante de grade strict mai mici decât gradul lui f. Datorită alegerii lui H, polinoamele f şi g se pot scrie ca produs de polinoame ireductibile. Dar atunci şi $H = fg$ este produs de polinoame ireductibile, contradicţie. •

Din teorema precedentă rezultă că $a, b \in \mathbf{Z}$ sunt prime între ele dacă şi numai dacă nu au un divizor prim comun. O afirmaţie similară are loc în $K[X]$.

Teorema 101 (Euclid)
(a) *Mulţimea numerelor naturale prime este infinită.*
(b) *Mulţimea polinoamelor unitare ireductibile din $K[X]$ este infinită.*

Demonstraţie. (a). Negăm. Fie $p_1, ..., p_n$ mulţimea numerelor naturale prime. Considerăm numărul $N = p_1 \cdots p_n + 1$. Atunci N nu se divide cu nici un număr prim p_i, contradicţie.
(b). Dacă K este corp infinit, putem folosi polinoamele ireductibile $X - a$ cu $a \in K$. În cazul K corp finit se reiterează raţionamentul de la (a). •

Teorema 102 (a) *Orice număr întreg N diferit de 0, ± 1 se scrie în mod unic sub forma $N = \pm p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ unde p_1,...,p_s sunt numere prime pozitive distincte şi α_1,...,$\alpha_s \geq 1$.*
(b) *Orice polinom neconstant $F \in K[X]$ se scrie în mod unic sub forma $F = a\pi_1^{\alpha_1} \cdots \pi_s^{\alpha_s}$ unde $a \in K^*$, π_1,...,π_s sunt polinoame ireductibile unitare distincte şi α_1,...,$\alpha_s \geq 1$.*

Demonstraţie.
(a) Existenţa scrierii a fost demonstrată în teorema 100. Probăm unicitatea. E clar că semnul $''\pm''$ este unic determinat fiind semnul lui N. Fie $N = \pm q_1^{\beta_1} \cdots q_t^{\beta_t}$ o altă scriere a lui N cu q_1,...,q_t numere prime pozitive distincte şi β_1,...,$\beta_s \geq 1$. Facem inducţie după $M = \alpha_1 + \cdots \alpha_s$ afirmaţia fiind evidentă pentru $M = 1$. Presupunem $M > 1$. Cum $p_s \mid N$ şi $N = \pm q_1 \cdots q_t$, din teorema 99 rezultă că p_s divide unul dintre prime numerele q_i, să zicem pe q_t. Deci $p_s = q_t$. Simplificând p_s din egalitatea $p_1^{\alpha_1} \cdots p_s^{\alpha_s} = q_1^{\beta_1} \cdots q_t^{\beta_t}$ obţinem $p_1^{\alpha_1} \cdots p_s^{\alpha_s - 1} = q_1^{\beta_1} \cdots q_t^{\beta_t - 1}$. Din ipoteza de inducţie rezultă că $s = t$, şi, după o eventuală renumerotare, $p_i = q_i$ şi $\alpha_i = \beta_i$ pentru $i = 1, ..., s - 1$, şi $\alpha_s - 1 = \beta_s - 1$. Deci $\alpha_s = \beta_s$.
(b) Se adaptează raţionamentul precedent. •

Teorema următoare este numită Teorema Fundamentală a Algebrei.

Teorema 103 (D'Alembert-Gauss) *Orice polinom neconstant $f \in \mathbf{C}[X]$ are cel puţin o rădăcină în $\mathbf{C}$.*

O demonstraţie se poate găsi în [5, teorema IX.3.4]. Din teoremă rezultă că polinoamele ireductibile din $\mathbf{C}[X]$ sunt polinoamele de gradul 1.

Corolarul 104 *Polinoamele ireductibile din* $\mathbf{R}[X]$ *sunt polinoamele de gradul 1 şi cele de gradul doi fără rădăcini reale.*

Demonstraţie. $f \in \mathbf{R}[X]$ de grad ≥ 3 şi fie $\alpha \in \mathbf{C}$ o rădăcină a lui f. Dacă $\alpha \in \mathbf{R}$ atunci f este reductibil. Dacă nu, rezultă că f are şi rădăcina $\overline{\alpha}$. Atunci f se divide în $\mathbf{C}[X]$ şi $\mathbf{R}[X]$ (observaţia 92) cu $(X-\alpha)(X-\overline{\alpha})$, deci f este reductibil. $\bullet$

Deducem următorul corolar.

Corolarul 105 (a) *Orice polinom neconstant* $f \in \mathbf{C}[X]$ *se scrie în mod unic sub forma* $f = a(X-\alpha_1)^{m_1}\cdots(X-\alpha_s)^{m_s}$ *cu* $a \in \mathbf{C}$, $\alpha_1,\ldots,\alpha_s \in \mathbf{C}$ *distincte, şi* $m_1,\ldots,m_s \geq 1$.

(b) *Orice polinom neconstant* $f \in \mathbf{R}[X]$ *se scrie în mod unic sub forma* $f = a(X-\alpha_1)^{m_1}\cdots(X-\alpha_s)^{m_s}\pi_1^{n_1}\cdots\pi_t^{n_t}$ *cu* $a \in \mathbf{R}$, $\alpha_1,\ldots,\alpha_s \in \mathbf{R}$ *distincte,* $\pi_1,\ldots,\pi_t \in \mathbf{R}[X]$ *sunt polinoame unitare de gradul doi distincte fără rădăcini reale şi* $m_1,\ldots,m_s,\ n_1,\ldots,n_t \geq 1$.

În **Z** şi $K[X]$ cmmdc şi cmmmc se pot calcula cu ajutorul descompunerii în produs de factori primi (ireductibili).

Lema 106 *Fie* $a = \pm p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ *unde* $p_1,\ldots,p_s$ *sunt numere prime pozitive distincte şi* $\alpha_i \geq 1$ *pentru* $i = 1,\ldots,s$. *Atunci divizorii întregi ai lui* a *sunt de numerele forma* $c = \pm p_1^{\gamma_1}\cdots p_s^{\gamma_s}$ *unde* $0 \leq \gamma_i \leq \alpha_i$ *pentru* $i = 1,\ldots,s$.

Demonstraţie. Fie $a = bc$ o factorizare a lui a cu $b, c \in \mathbf{Z}$. Din Teorema 102, factorii primi din descompunerea lui b şi c sunt dintre $p_1,\ldots,p_s$. Deci putem scrie $b = \pm p_1^{\beta_1}\cdots p_s^{\beta_s}$ şi $c = \pm p_1^{\gamma_1}\cdots p_s^{\gamma_s}$. Din $a = bc$ obţinem $p_1^{\alpha_1}\cdots p_s^{\alpha_s} = p_1^{\beta_1+\gamma_1}\cdots p_s^{\beta_s+\gamma_s}$. Din Teorema 102 rezultă că $\alpha_i = \beta_i + \gamma_i$ pentru $i = 1,\ldots,s$. $\bullet$

Se poate demonstra o lemă analogă pentru $K[X]$.

Teorema 107 *Fie* $a = \pm p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ *şi* $b = \pm p_1^{\beta_1}\cdots p_s^{\beta_s}$ *unde* $p_1,\ldots,p_s$ *sunt numere prime pozitive distincte iar* $\alpha_i, \beta_i \geq 1$, *pentru* $i = 1,\ldots,s$. *Atunci*

(a) $(a,b) = p_1^{min(\alpha_1,\beta_1)}\cdots p_s^{min(\alpha_s,\beta_s)}$ *şi*

(b) $[a,b] = p_1^{max(\alpha_1,\beta_1)}\cdots p_s^{max(\alpha_s,\beta_s)}$.

Demonstraţie. (a). Cf. lemei anterioare, divizorii comuni ai lui a şi b au forma $\pm p_1^{\gamma_1}\cdots p_s^{\gamma_s}$ cu $\gamma_i \leq min(\alpha_i, \beta_i)$ pentru $i = 1, ..., s$. De aici rezultă (a).

(b). Din teorema 95, $[a, b] = \pm ab/(a, b)$. Folosind (a), deducem $[a, b] = p_1^{max(\alpha_1,\beta_1)}\cdots p_s^{max(\alpha_s,\beta_s)}$, deoarece, pentru orice $\alpha, \beta \in \mathbf{N}$, $min(\alpha, \beta)+max(\alpha, \beta) = \alpha + \beta$. •

Proprietatea analogă pentru $K[X]$ este

Teorema 108 *Fie* $f = a\pi_1^{\alpha_1}\cdots\pi_s^{\alpha_s}$ *şi* $g = b\pi_1^{\beta_1}\cdots\pi_s^{\beta_s}$ *unde* $a, b \in K^*$, π_1,...,π_s *sunt polinoame ireductibile unitare distincte din* $K[X]$ *şi* $\alpha_i, \beta_i \geq 1$ *pentru* $i = 1, ..., s$. *Atunci*

(a) $(f, g) = \pi_1^{min(\alpha_1,\beta_1)}\cdots\pi_s^{min(\alpha_s,\beta_s)}$ *şi*

(b) $[f, g] = \pi_1^{max(\alpha_1,\beta_1)}\cdots\pi_s^{max(\alpha_s,\beta_s)}$.

Demonstraţie. Se adaptează demonstraţia precedentă. •

5.3 Complemente

Teorema 109 *Fie* K *un corp şi* $f \in K[X]$ *un polinom ireductibil. Atunci inelul factor* $k[X]/(f)$ *este corp.*

Demonstraţie. Un element nenul din $K[X]/(f)$ se scrie sub forma $\widehat{g}$ cu $g \in K[X]$ nedivizibil cu f. Cum f este ireductibil, rezultă că f, g sunt relativ prime. Cf. teoremei 96, putem scrie $ff_1 + gg_1 = 1$ cu $f_1, g_1 \in K[X]$. Deci $\widehat{g}\widehat{g_1} = \widehat{1}$. •

Morfismul (injectiv) de corpuri $\alpha : K \to K[X]/(f)$, $\alpha(a) = \widehat{a}$, ne permite să identificăm pe K cu un subcorp al lui $K[X]/(f)$ prin identificarea fiecărui $a \in K$ cu $\widehat{a}$. Dacă $f = a_0 + a_1X + \cdots + a_nX^n$, atunci $f(\widehat{X}) = a_0 + a_1\widehat{X} + \cdots + a_n\widehat{X}^n = \widehat{a_0} + \widehat{a_1}\widehat{X} + \cdots + \widehat{a_n}\widehat{X}^n = \widehat{f} = \widehat{0}$. Deci este $\widehat{X}$ o rădăcină a lui f în corpul $K[X]/(f)$.

Teorema 110 (Lema lui Kronecker). *Fie* K *un corp şi* $f \in K[X]$ *un polinom de grad* ≥ 1. *Atunci există un corp* L *care îl conţine pe* K *astfel încât* f *are o rădăcină în* L.

Demonstraţie. Înlocuind pe f cu un factor ireductibil al său, putem presupune că f este ireductibil. În acest caz teorema a fost deja demonstrată în paragraful anterior teoremei. •

$\mathbf{Q}[X]$ posedă polinoame ireductibile de orice grad. De exemplu, polinomul $X^n - 2$ este ireductibil, pentru orice $n \geq 1$, după cum rezultă din următorul criteriu de ireductibilitate.

Teorema 111 (Criteriul lui Eisenstein). *Fie $h \in \mathbf{Z}[X]$ un polinom neconstant unitar. Presupunem că există un număr prim p astfel încât p divide toţi coeficienţii lui h, cu excepţia coeficientului dominant, iar p^2 nu divide termenul liber al lui h. Atunci h este ireductibil în $\mathbf{Q}[X]$.*

Demonstraţie. Negăm. Deci există $f, g \in \mathbf{Q}[X]$ polinoame unitare neconstante astfel încât $fg = h$. Arătăm că $f, g \in \mathbf{Z}[X]$. Fie a, b numere naturale nenule minime cu proprietatea $af, bg \in \mathbf{Z}[X]$. Presupunem că $ab \neq 1$ şi fie q un divizor prim al lui ab. Deoarece $h \in \mathbf{Z}[X]$, q divide abh în $\mathbf{Z}[X]$. Fie $\overline{af}$, $\overline{bg}$ polinoamele obţinute din af resp. bg prin reducerea coeficienţilor modulo q. Rezultă că $(\overline{af})(\overline{bg}) = \overline{0}$ în $\mathbf{Z}_q[X]$. Cum $\mathbf{Z}_q[X]$ este domeniu, unul din factori, să zicem $\overline{af}$, este nul. Rezultă că toţi coeficienţii lui af, deci şi coeficientul dominant a, sunt divizibili cu q, deci $(a/q)f \in \mathbf{Z}[X]$, în contradicţie cu alegerea lui a. Rezultă că $a = b = 1$, deci $f, g \in \mathbf{Z}[X]$.

Fie $\overline{f}$, $\overline{g}$ polinoamele obţinute din f resp. g prin reducerea coeficienţilor modulo p. Rezultă că $\overline{f}\overline{g} = X^n$ în $\mathbf{Z}_p[X]$, unde n este gradul lui h. Deducem că $\bar{f} = X^s$ şi $\bar{g} = X^t$, unde s, t sunt gradele lui f resp. g. Deci termenii liberi ai lui f şi g se divid cu p. În consecinţă, termenul liber al lui h se divide cu p^2, contradicţie. •

Fie polinomul $f = (X^5 - 1)/(X - 1) = X^4 + X^3 + X^2 + X + 1$. Aplicând criteriul lui Eisenstein polinomului $g = f(X+1) = X^4+5X^3+10X^2+10X+5$, pentru $p = 5$, deducem că g este ireductibil în $\mathbf{Q}[X]$. Deci f este ireductibil în $\mathbf{Q}[X]$.

5.4 Exerciţii

139. Calculaţi $(24, 54)$ în **Z** cu ajutorul algoritmului lui Euclid.

140. Fie $a, b \in \mathbf{N}$ şi $d = (a, b)$. Arătaţi că $(X^a - 1, X^b - 1) = X^d - 1$ în $K[X]$, unde K este un corp.

141. Calculaţi $f = (X^{23} + X^{22} + \cdots + X + 1, X^{53} + X^{52} + \cdots + X + 1)$ în $\mathbf{Q}[X]$.

142. Calculaţi $(X^4 - 4X^3 + 1, X^3 - 3X^2 + 1)$ în $\mathbf{R}[X]$.

143. Calculaţi $(2^m - 1, 2^n - 1)$ în $\mathbf{Z}$.

144. Fie $a, b, c, d \in \mathbf{Z} \setminus \{0\}$ astfel încât $ab = cd$. Arătaţi că există $x, y, u, v \in \mathbf{Z}$ astfel încât $xy = c$, $uv = d$, $xu = a$ şi $yv = b$.

145. Fie A un domeniu şi $0 \neq a, b \in A$ astfel încât $Aa + Ab = Ad$. Arătaţi că $d = (a, b)$.

146. Fie K un corp şi $0 \neq f, g \in K[X]$ astfel încât $f \mid g^2 \mid f^3 \mid g^4 \mid \ldots$. Arătaţi că f, g sunt asociate.

147. Arătaţi că numerele $F_n = 2^{2^n} + 1$ (numite *numerele Fermat*) sunt relativ prime două câte două. Deduceţi că există o infinitate de numere prime. (Indicaţie. $F_0 F_1 F_2 \cdots F_{n-1} = F_n - 2$).

148. Arătaţi că $F_n = 2^{2^n} + 1$ este număr prim pentru $n = 0, 1, 2, 3$ şi compus pentru $n = 5$. (Indicaţie. Folosind egalităţile $641 = 5 \cdot 2^7 + 1 = 5^4 + 2^4$, rezultă că F_5 se divide cu 641).

149. Calculaţi $(X^2 - 1)\mathbf{Q}[X] \cap (X^3 - 1)\mathbf{Q}[X]$ şi $(X^2 - 1)\mathbf{Q}[X] + (X^3 - 1)\mathbf{Q}[X]$.

150. Calculaţi (f, g) şi $[f, g]$ în $\mathbf{Q}[X]$ pentru $f = (X - 1)(X^2 - 1)(X^3 - 1)(X^4 - 1)$ şi $g = (X + 1)(X^2 + 1)(X^3 + 1)(X^4 + 1)$.

151. Descompuneţi polinomul $X^n - 1$, $1 \leq n \leq 6$, în produs de polinoame ireductibile în $\mathbf{Q}[X]$, $\mathbf{R}[X]$, $\mathbf{C}[X]$.

152. În ce caz este polinomul $X^{3m} + X^{3n+1} + X^{3p+2} \in \mathbf{Q}[X]$ divizibil cu $X^4 + X^2 + 1$? (Indicaţie. Descompuneţi polinomul $X^4 + X^2 + 1$.)

153. Găsiţi polinoamele ireductibile de grad ≤ 5 din $\mathbf{Z}_2[X]$.

154. Descompuneţi polinomul $X^{15}+\hat{1}$ în produs de polinoame ireductibile în $\mathbf{Z}_2[X]$.

155. Descompuneţi polinomul $X^{56}-X^{49}-X^7+\hat{1}$ în produs de polinoame ireductibile în $\mathbf{Z}_7[X]$. (Indicaţie. Folosiţi morfismul lui Frobenius.)

156. Găsiţi polinoamele ireductibile de grad ≤ 2 din $K[X]$, unde K este corpul $\{0,1,z,z+1\}$, unde $1+1=0$ şi $z^2=z+1$.

157. Sunt corpurile $\mathbf{Z}_2[X]/(X^3+X+\hat{1})$, $\mathbf{Z}_2[X]/(X^3+X^2+\hat{1})$ izomorfe ?

158. Fie K un corp şi $f,g,h\in K[X]$ polinoame. Arătaţi că

$$[f,g,h]^2(f,g)(g,h)(f,h)=(f,g,h)^2[f,g][g,h][f,h].$$

159. Arătaţi că pentru orice număr prim p, polinomul $f=X^p-X+\hat{1}\in\mathbf{Z}_p[X]$ este ireductibil.

160. Fie k un număr întreg $\neq 0,\pm 1$ liber de pătrate şi n un număr natural nenul. Arătaţi că polinomul X^n-k este ireductibil în $\mathbf{Q}[X]$.

161. Fie K un corp, $f\in K[X]$ un polinom neconstant şi $a,b\in K$, $a\neq 0$. Arătaţi că f este ireductibil $\Leftrightarrow$ $f(aX+b)$ este ireductibil.

162. Fie n un număr natural nenul. Arătaţi că polinomul $f=X^{2^n}+1$ este ireductibil în $\mathbf{Q}[X]$. (Indicaţie. Se consideră $f(X+1)$.)

163. Fie p un număr natural prim. Arătaţi că polinomul $f=X^{p-1}+X^{p-2}+\ldots+X+1$ este ireductibil în $\mathbf{Q}[X]$. (Indicaţie. Se consideră $f(X+1)$.)

Capitolul 6

Polinoame simetrice

În aceast capitol se prezintă teorema fundamentală a polinoamelor simetrice.

6.1 Inelul polinoamelor simetrice

Fie A un inel comutativ şi $n \geq 1$. Un polinom $f \in A[X_1, ..., X_n]$ se numeşte *polinom simetric* dacă f rămâne neschimbat după orice permutare a nedeterminatelor $X_1, ..., X_n$, adică

$$f(X_{\sigma(1)}, ..., X_{\sigma(n)}) = f(X_1, ..., X_n) \text{ pentru orice } \sigma \in S_n.$$

Polinoamele constante sunt evident simetrice. Deoarece orice permutare din S_n este un produs de transpoziţii (teorema 51), rezultă că un polinom este simetric dacă şi numai dacă f este invariant la orice transpoziţie (X_i, X_j) a nedeterminatelor $X_1, ..., X_n$. Polinoamele

$$\begin{aligned} s_1 &= X_1 + \cdots + X_n \\ s_2 &= X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n \\ &\vdots \\ s_n &= X_1 \cdots X_n \end{aligned}$$

sunt simetrice deoarece s_k este suma tuturor produselor de k nedeterminate distincte din mulţimea X_1,...,X_n. Ele se numesc *polinoamele simetrice fundamentale*. Polinomul $f = X_1 + X_2^2$ nu este simetric deoarece $f(X_2, X_1) = X_1^2 + X_2 \neq f$. Dacă schimbăm între ele două nedeterminate în polinomul $g = (X_1 - X_2)(X_2 - X_3)(X_3 - X_1)$, atunci g îşi schimbă semnul. Deci g este simetric dacă şi numai dacă inelul A este de caracteristică 2.

Teorema 112 *Mulţimea polinoamelor simetrice formează un subinel al inelului* $A[X_1, ..., X_n]$.

Demonstraţie. Fie f, g polinoame simetrice. Avem de arătat că $f + g$ şi fg sunt de asemenea simetrice. Fie $\sigma \in S_n$. Atunci $(fg)(X_{\sigma(1)}, ..., X_{\sigma(n)}) = f(X_{\sigma(1)}, ..., X_{\sigma(n)})g(X_{\sigma(1)}, ..., X_{\sigma(n)}) = fg$. Deci fg este simetric şi la fel se arată că $f - g$ este simetric. •

În consecinţă, $g(s_1, s_2, ..., s_n)$ este polinom simetric pentru orice $g \in A[Y_1, ..., Y_n]$. Vom arăta că orice polinom simetic se poate scrie astfel şi că scrierea este unică. De exemplu, $X_1^2 + X_2^2 + \cdots + X_n^2 = s_1^2 - 2s_2$. Sunt necesare unele pregătiri.

Definim *ordinea lexicografică* pe mulţimea monoamelor din $A[X_1, ..., X_n]$. Fie $M = aX_1^{i_1} \cdots X_n^{i_n}$ şi $N = bX_1^{j_1} \cdots X_n^{j_n}$ două monoame nenule. Spunem că M este *strict mai mare ca* N *în ordinea lexicografică*, şi scriem $M > N$, dacă există k, $1 \leq k < n$, astfel încât $i_1 = j_1$,...,$i_k = j_k$ şi $i_{k+1} > j_{k+1}$. Altfel spus, $M > N$ dacă prima componentă nenulă a vectorului $(i_1 - j_1, ..., i_n - j_n)$ este > 0. Vom scrie $M \geq N$ dacă $M > N$ sau M este asemenea cu N.

Se observă analogia cu modul de ordonare a cuvintelor într-un dicţionar: e ca şi cum am compara cuvintele $(i_1, ..., i_n)$ şi $(j_1, ..., j_n)$.

De exemplu, $X_1^k \geq X_1^l \Leftrightarrow k \geq l$ şi $X_1^2 > X_1X_2 > X_1X_3 > X_2^2 > X_2X_3 > X_3^2$.

Teorema 113 *Fie* M, N, P, Q *patru monoame nenule. Atunci*

(a) $M \geq N$ *sau* $N \geq M$.

(b) Dacă $M \geq N$ *şi* $N \geq P$, *atunci* $M \geq P$.

(c) Dacă $M \geq N$ *şi* $N \geq M$, *atunci* M *şi* N *sunt asemenea.*

(d) Dacă $M \geq N$, $P \geq Q$ *şi* $MP, NQ \neq 0$, *atunci* $MP \geq NQ$.

La (b) şi (d), dacă una din inegalităţile din ipoteză este strictă, atunci şi inegalitatea din concluzie este strictă.

Demonstraţie. (a) şi (c) rezultă din definiţie. Fie $M = aX_1^{i_1} \cdots X_n^{i_n}$, $N = bX_1^{j_1} \cdots X_n^{j_n}$, $P = cX_1^{k_1} \cdots X_n^{k_n}$ şi $Q = dX_1^{l_1} \cdots X_n^{l_n}$. (b). Putem presupune că $M > N$ şi $N > P$ altfel afirmaţia e clară. Atunci vectorii $(i_1 - j_1, ..., i_n - j_n)$ şi $(j_1 - k_1, ..., j_n - k_n)$ au prima componentă nenulă > 0. Rezultă că şi suma lor $(i_1 - k_1, ..., i_n - k_n)$ are prima componentă nenulă > 0, deci $M > P$. (d). Tratăm cazul $M > N$ şi $P > Q$, celelalte se probează analog. Atunci vectorii $(i_1 - j_1, ..., i_n - j_n)$ şi $(k_1 - l_1, ..., k_n - l_n)$ au prima componentă nenulă > 0, deci şi suma lor $(i_1 + j_1 - k_1 - l_1, ..., i_n + j_n - k_n - l_n)$ are prima componentă nenulă > 0, adică $MN > PQ$. •

În anumite privinţe, ordinea lexicografică se comportă similar relaţiei de ordine pe mulţimea numerelor naturale.

Teorema 114 *Orice şir strict descrescător de monoame din* $A[X_1, ..., X_n]$ *este finit.*

Demonstraţie. Facem inducţie după n, pentru $n = 1$ proprietatea fiind clară. Fie $n \geq 2$ şi presupunem că există un şir infinit strict descrescător de monoame $M_1 > M_2 > M_3 > \cdots$. Izolând în fiecare monom M_j nedeterminata X_1, obţinem $X_1^{i_1}N_1 > X_1^{i_2}N_2 > X_1^{i_3}N_3 > \cdots$, unde N_j sunt monoame în nedeterminatele $X_2, ..., X_n$. Rezultă că $i_1 \geq i_2 \geq i_3 \geq \cdots$, deci există s astfel încât $i_k = i_s$ pentru orice $k \geq s$. Rezultă şirul infinit $N_s > N_{s+1} > N_{s+2} > \cdots$, în contradicţie cu ipoteza de inducţie. •

Fie f un polinom nenul. Numim *termen principal* al lui f, şi-l notăm $T(f)$, cel mai mare monom al lui f în ordinea lexicografică. De exemplu, $T(s_1) = X_1$. Pentru polinoame într-o singură nedeterminată, termenul principal este chiar monomul dominant.

Teorema 115 *Dacă* $aX_1^{i_1}X_2^{i_2} \cdots X_n^{i_n}$ *este temenul principal al unui polinon simetric, atunci* $i_1 \geq i_2 \geq \cdots \geq i_n$.

Demonstraţie. Fie f un polinom simetric şi $N = bX_1^{j_1}X_2^{j_2} \cdots X_n^{j_n}$ un monom nenul al său. Fiind simetric, f conţine odată cu N toate monoamele $bX_1^{j_{\sigma(1)}}X_2^{j_{\sigma(2)}} \cdots X_n^{j_{\sigma(n)}}$, $\sigma \in S_n$. Între acestea, cel mai mare în ordinea lexicografică este cel pentru care $j_{\sigma(1)} \geq j_{\sigma(2)} \geq \cdots \geq j_{\sigma(n)}$. •

În particular, pentru polinoamele simetrice fundamentale avem $T(s_k) = X_1 \cdots X_k$, $1 \leq k \leq n$.

Teorema 116 *Fie* $f, g \in A[X_1, ..., X_n]$ *două polinoame nenule. Dacă* $T(f)T(g) \neq 0$ *(e.g., dacă* A *este domeniu), atunci* $T(fg) = T(f)T(g)$.

Demonstraţie. Scriem $f = M_0 + M_1 + \cdots + M_k$ şi $g = N_0 + N_1 + \cdots + N_l$ unde $M_0 = T(f)$ şi $N_0 = T(g)$, $M_1, ..., M_k$ sunt monoame strict mai mici ca $T(f)$ şi $N_1, ..., N_l$ sunt monoame strict mai mici ca $T(g)$. Rezultă $fg = \sum_{i,j} M_i N_j$ sumă în care $M_0 N_0 = T(f)T(g)$ este strict mai mare decât toţi ceilalţi termeni $M_i N_j$, cf. teoremei 113. Deci $T(fg) = T(f)T(g)$. •

6.2 Teorema fundamentală

Teorema 117 (Teorem fundamentală a polinoamelor simetrice.) *Orice polinom simetric $f \in A[X_1, ..., X_n]$ se scrie în mod unic ca expresie polinomială cu coeficienţi în A de polinoamele simetrice fundamentale $s_1, ..., s_n$, adică există şi este unic un polinom $g \in A[Y_1, ..., Y_n]$ astfel încât $f = g(s_1, ..., s_n)$.*

Existenţa lui g rezultă din următorul algoritm (unicitatea lui g va fi probată ulterior).

Algoritmul 118 *(Exprimarea unui polinom simetric în funcţie de polinoamele simetrice fundamentale).*

Input: $f \in A[X_1, ..., X_n]$ polinom simetric.
Output: $g \in A[Y_1, ..., Y_n]$ astfel încât $f = g(s_1, ..., s_n)$.

$g := 0$; $h := f$;
while($h \neq 0$ *) do*
begin
  $aX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ = termenul principal al lui h;
  $h := h - as_1^{i_1-i_2}s_2^{i_2-i_3}\cdots s_{n-1}^{i_{n-1}-i_n}s_n^{i_n}$;
  $g := g + aY_1^{i_1-i_2}Y_2^{i_2-i_3}\cdots Y_{n-1}^{i_{n-1}-i_n}Y_n^{i_n}$;
end.

Corectitudinea algoritmului rezultă din următoarele observaţii. Cf. teoremei 112, h rămâne simetric în timpul desfăşurării algoritmului. Rezultă că $T(h) = aX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ are proprietatea $i_1 \geq i_2 \geq \cdots \geq i_n$, cf. teoremei 115. Deci, au sens expresiile $as_1^{i_1-i_2}s_2^{i_2-i_3}\cdots s_{n-1}^{i_{n-1}-i_n}s_n^{i_n}$ şi $aY_1^{i_1-i_2}Y_2^{i_2-i_3}\cdots Y_{n-1}^{i_{n-1}-i_n}Y_n^{i_n}$. Cf. teoremei 116, $as_1^{i_1-i_2}s_2^{i_2-i_3}\cdots s_{n-1}^{i_{n-1}-i_n}s_n^{i_n}$ are termenul principal

$$aX_1^{i_1-i_2}(X_1X_2)^{i_2-i_3}\cdots(X_1\cdots X_{n-1})^{i_{n-1}-i_n}(X_1\cdots X_n)^{i_n} = aX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}.$$

Deci la fiecare parcurgere a buclei *while*, $T(h)$ scade strict. În consecinţă, bucla *while* se parcurge doar de un număr finit de ori, cf. teoremei 114. În fine, se observă că după iniţializările $g := 0$, $h := f$, avem $f = h+g(s_1, ..., s_n)$, egalitate ce se păstrează după fiecare parcurgere a buclei *while*. La sfârşit vom avea $h = 0$, deci $f = g(s_1, ..., s_n)$. •

De exemplu, pentru $f = X_1^2 + \cdots + X_n^2$, variabilele algoritmului iau valorile următoare: $h = f, -2s_1, 0$, $T(h) = X_1^2, -2X_1X_2$ şi $g = 0, Y_1^2, Y_1^2 - 2Y_2$. Adică $f = s_1^2 - 2s_2$.

Demonstraţia unicităţii lui g. Fie $g, g' \in A[Y_1, ..., Y_n]$ distincte; deci $G := g - g' \neq 0$. E suficient să arătăm că $G(s_1, ..., s_n) \neq 0$. Fie $G = \sum_{i=1}^{k} M_i$ scrierea canonică a lui G ca sumă de monoame. Atunci $G(s_1, ..., s_n) = \sum_{i=1}^{k} M_i(s_1, ..., s_n) \neq 0$, deoarece polinoamele $M_i(s_1, ..., s_n)$ au termenii principali monoame neasemenea două câte două. Într-adevăr, fie

$$M = aY_1^{i_1}Y_2^{i_2} \cdots Y_n^{i_n}, \ N = bY_1^{j_1}Y_2^{j_2} \cdots Y_n^{j_n}$$

două monoame nenule neasemenea astfel încât $M(s_1, ..., s_n)$ şi $N(s_1, ..., s_n)$ au termenii principali monoame asemenea. Cum $M(s_1, ..., s_n) = as_1^{i_1}s_2^{i_2} \cdots s_n^{i_n}$ are termenul principal

$$aX_1^{i_1}(X_1X_2)^{i_2} \cdots (X_1 \cdots X_n)^{i_n} = aX_1^{i_1+\cdots+i_n}X_2^{i_2+\cdots+i_n} \cdots X_{n-1}^{i_n+i_{n-1}}X_n^{i_n}$$

iar $N(s_1, ..., s_n)$ are termenul principal

$$bX_1^{j_1+\cdots+j_n}X_2^{j_2+\cdots+j_n} \cdots X_{n-1}^{j_n+j_{n-1}}X_n^{j_n}$$

rezultă că $i_n = i_n$, $i_{n-1} = j_{n-1}$,...,$i_1 = j_1$, deci monoamele M, N sunt asemenea, contradicţie.

Teorema 119 *Componentele omogene ale unui polinom simetric sunt polinoame simetrice.*

Demonstraţie. Fie $f \in A[X_1, ..., X_n]$ un polinom simetric şi fie $f_0, ..., f_k$ componentele sale omogene. Dacă $\sigma \in S_n$ şi notăm $f_j(X_{\sigma(1)}, ..., X_{\sigma(n)})$ cu f_j^σ, obţinem $f^\sigma = f_0^\sigma + f_1^\sigma + \cdots + f_n^\sigma$. Cum f_j^σ este polinom omogen de grad j şi $f = f^\sigma$, deducem că $f_j^\sigma = f_j$ pentru orice j şi orice permutare σ. Deci fiecare componentă omogenă f_j este polinom simetric. •

Rezultă că algoritmul 118 poate fi ”rulat” separat pentru fiecare componentă omogenă a unui polinom simetric. Presupunem că în algoritmul 118, f este simetric şi omogen de grad k. Se observă că, în timpul desfăşurării algoritmului, h este omogen de grad k sau nul. Mai mult, termenul principal al lui h este mai mic decât termenul principal al lui f. Deci f este o sumă de ”monoame” de tipul $a_\alpha s_1^{i_1-i_2}s_2^{i_2-i_3}\cdots s_{n-1}^{i_{n-1}-i_n}s_n^{i_n}$ cu $i_1+\cdots+i_n=k$, $i_1\geq i_2\geq\cdots\geq i_n$ şi $X_1^{i_1}\cdots X_n^{i_n}\leq T(f)$. Coeficienţii a_α pot fi determinaţi dând valori paticulare nedeterminatelor $X_1,...,X_n$.

De exemplu, fie $f=(X_1+X_2)(X_1+X_3)(X_2+X_3)$. f este simetric şi omogen de grad 3 şi $T(f)=X_1^2X_2$. Tripletele (i_1,i_2,i_3) ce verifică condiţiile precedente sunt $(2,1,0)$ şi $(1,1,1)$. Deci $f=s_1^{2-1}s_2^{1-0}s_3^0+as_1^{1-1}s_2^{1-1}s_3^1=s_1s_2+as_3$. Făcând $X_1=X_2=X_3=1$, găsim $9+a=8$, adică $a=-1$. Deci $f=s_1s_2-s_3$.

Lema 120 *Fie $f\in A[X_1,...,X_n]$ un polinom omogen şi simetric de grad k cu $1\leq k<n$. Atunci $f(X_1,...,X_k,0,...,0)\neq 0$.*

Demonstraţie. Fie $M=aX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ termenul principal al lui f. Atunci $i_1\geq i_2\geq\cdots\geq i_n$, cf. teoremei 115. Cum $i_1+\cdots+i_n=k$ şi $k<n$, rezultă $i_{k+1}=\cdots=i_n=0$. Deci M rămâne nenul după anularea nedeterminatelor X_{k+1},...,X_n, adică $f(X_1,...,X_k,0,...,0)\neq 0$. •

Teorema 121 (Formulele lui Newton). *Fie polinoamele*

$$p_k=X_1^k+X_2^k+\cdots+X_n^k,\ k\geq 1$$

şi fie s_1,...,$s_n\in A[X_1,...,X_n]$ polinoamele simetrice fundamentale. Atunci

$$p_k-s_1p_{k-1}+s_2p_{k-2}-\cdots+(-1)^ns_np_{k-n}=0 \text{ pentru } k\geq n \tag{6.1}$$

şi

$$p_k-s_1p_{k-1}+\cdots+(-1)^{k-1}s_{k-1}p_1+(-1)^kks_k=0 \text{ pentru } 1\leq k\leq n-1. \tag{6.2}$$

Demonstraţie. Fie $k\geq n$ şi fie $g\in A[X_1,...,X_n,Y]$, $g=(Y-X_1)(Y-X_2)\cdots(Y-X_n)$. Din relaţiile lui Viete

$$g=Y^n-s_1Y^{n-1}+s_2Y^{n-2}-\cdots+(-1)^ns_n.$$

Cum fiecare X_i este rădăcină a lui g, deducem că

$$X_i^n - s_1 X_i^{n-1} + s_2 X_i^{n-2} - \cdots + (-1)^n s_n = 0.$$

Prin înmulţire cu X_i^{n-k} rezultă

$$X_i^k - s_1 X_i^{k-1} + s_2 X_i^{k-2} + \cdots + (-1)^n s_n X_i^{n-k} = 0.$$

Adunând aceste relaţii pentru i de la 1 la n obţinem formula (6.1). Pentru $k = n$ obţinem în $A[X_1, ..., X_k]$

$$p_k - s_1 p_{k-1} + s_2 p_{k-2} - \cdots + (-1)^k k s_k = 0. \tag{6.3}$$

Fie acum $1 \leq k \leq n-1$ şi presupunem că polinomul

$$h = p_k - s_1 p_{k-1} + \cdots + (-1)^{k-1} s_{k-1} p_1 + (-1)^k k s_k$$

este nenul. Atunci h este simetric şi omogen de grad k. Din formula (6.3) rezultă că $h(X_1, ..., X_k, 0, ..., 0) = 0$, contradicţie, cf. lemei 120. •

Din formulele lui Newton rezultă $p_2 = s_1^2 - 2s_2$, $p_3 = s_1^3 - 3s_1 s_2 + 3s_3$, $p_4 = s_1^4 - 4s_1^2 s_2 + 2s_2^2 + 4s_1 s_3 - 4s_4$.

6.3 Exerciţii

164. Fie $n \geq 1$ şi $t_k = \varepsilon_1^k + \cdots \varepsilon_n^k$, unde ε_1,...,ε_n sunt rădăcinile complexe de ordinul n ale unităţii. Arătaţi că $t_k = 0$ dacă n nu divide k şi $t_k = n$ dacă n divide k.

165. Calculaţi suma cuburilor rădăcinilor ecuaţiei $x^4 + x^3 + 2x^2 + x + 1 = 0$.

166. Calculaţi sumele $p_k = x_1^k + \cdots + x_n^k$, $1 \leq k \leq n$, unde x_1,...,x_n sunt rădăcinile ecuaţiei $x^n + x^{n-1}/1! + x^{n-2}/2! + \cdots + x/(n-1)! + 1/n! = 0$.

167. Aranjaţi în ordine lexicografică monoamele de grad 6, $X_1^{i_1} X_2^{i_2} X_3^{i_3}$ cu $i_1 \geq i_2 \geq i_3$.

168. Spunem că două mulţimi ordonate A şi B sunt izomorfe dacă există o bijecţie crescătoare $f : A \to B$ cu inversa f^{-1} crescătoare. Este mulţimea monoamelor unitare în nedeterminatele X, Y ordonată lexicografic izomorfă cu $(\mathbf{N}, \leq)$?

169. "Rulaţi" algoritmul din teorema fundamentală a polinoamelor simetrice pentru $f = X^3 + Y^3 + Z^3$.

170. Exprimaţi polinomul $f = (X_1 - X_2)^2(X_2 - X_3)^2(X_1 - X_3)^2$ în funcţie de polinoamele simetrice fundamentale folosind metoda coeficienţilor nedeterminaţi.

171. Exprimaţi polinoamele $f_1 = \sum X_1^2X_2X_3$, $f_2 = \sum X_1^2X_2^2$, $f_3 = \sum X_1^3X_2$ şi $f_4 = \sum X_1^3X_2^2$ în funcţie de polinoamele simetrice fundamentale.

172. Fie x_1, x_2, x_3 rădăcinile ecuaţiei $x^3 + px + q = 0$. Calculaţi discriminantul ecuaţiei $D = (x_1 - x_2)^2(x_2 - x_3)^2(x_1 - x_3)^2$.

173. Fie x_1, x_2, x_3 rădăcinile ecuaţiei $x^3+px+q = 0$ şi fie $\varepsilon = (-1+i\sqrt{3})/2$. Găsiţi ecuaţia de gradul doi cu rădăcinile $y_1 = (x_1 + \varepsilon x_2 + \varepsilon^2 x_3)^3$ şi $y_2 = (x_1+\varepsilon^2 x_2+\varepsilon x_3)^3$. Rezolvaţi ecuaţia $x^3+px+q = 0$. Aplicaţie: $x^3+6x+2 = 0$.

174. Fie $A \subseteq \mathbf{R}[X, Y]$ subinelul polinoamelor simetrice. Arătaţi că inelul factor $A/(X^2 + Y^2)$ este izomorf cu $\mathbf{R}[X]$.

Capitolul 7

Determinanţi

În acest capitol se defineşte determinantul unei matrice pătratice cu elemente dintr-un inel comutativ şi se trec în revistă proprietăţile determinanţilor. Se demonstrează rezultate importante precum regula lui Laplace, regula lui Cramer sau formula Binet-Cauchy.

7.1 Proprietăţile determinanţilor

Fie R un inel comutativ, $n \geq 1$ şi fie $A = (a_{ij})_{1 \leq i,j \leq n} \in M_n(R)$ o matrice pătratică de ordinul n cu elemente din R. Prin definiţie, *determinantul* matricei A este elementul lui R

$$|A| := \sum_{\sigma \in S_n} sgn(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}. \tag{7.1}$$

Expresia anterioară se mai numeşte *dezvoltarea lui* $|A|$. Pentru $n = 1$, $|A| = a_{11}$, iar pentru $n = 2$, $|A| = a_{11}a_{22} - a_{12}a_{21}$. Cazul $n = 3$. Permutările de grad 3 sunt I, (123), (132) (permutări pare) şi (12), (13), (23) (permutări impare), deci

$$|A| = a_{11}a_{12}a_{13} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31} + a_{11}a_{23}a_{32}.$$

Fie $B = (b_{ij})_{1 \leq i,j \leq n} \in M_n(R)$ o matrice superior triunghiulară, adică $b_{ij} = 0$ pentru $j < i$. Atunci $b_{1\sigma(1)} b_{2\sigma(2)} \cdots b_{n\sigma(n)} \neq 0$ implică $\sigma(i) \geq i$, $i = 1, ..., n$, deci $\sigma = I$. Deci $|A| = a_{11}a_{22} \cdots a_{nn}$. Un rezultat similar are loc pentru matricele inferior triunghiulare, în particular pentru cele diagonale.

Pentru simplificarea limbajului, prin linia (coloana) i a determinantului $|A|$, vom înţelege linia (coloana) i a matricei A.

Teorema 122 (Proprietăţi ale determinanţilor).

(a) *O matrice are acelaşi determinant cu transpusa sa.*

(b) *Un determinant cu o linie nulă este nul.*

(c) *Dacă înmulţim o linie a unui determinant cu un element $\lambda \in R$, determinantul se înmulţeşte cu λ.*

(d) *Dacă o linie a unui determinant $|A|$ are forma $(b_1 + c_1, ..., b_n + c_n)$, atunci $|A| = |B| + |C|$, unde $|B|$ resp. $|C|$ sunt determinanţii obţinuţi din $|A|$ înlocuind linia respectivă cu $(b_1, ..., b_n)$ resp. $(c_1, ..., c_n)$.*

(e) *Un determinant cu două linii proporţionale (e.g., egale) este nul.*

(f) *Dacă într-un determinant permutăm două linii, atunci determinantul îşi schimbă semnul.*

(g) *Un determinant nu se schimbă dacă la o linie adunăm o altă linie înmulţită cu un element $\lambda \in R$.*

(h) *Proprietăţile $(b) - (f)$ au loc şi pentru coloane.*

Demonstraţie. Fie $A = (a_{ij})_{1 \leq i,j \leq n} \in M_n(R)$.

(a). Inelul R fiind comutativ, putem ordona produsele $a_{1\sigma(1)}a_{2\sigma(2)} \cdots a_{n\sigma(n)}$ după indicele de coloană: $a_{\sigma^{-1}(1)1}a_{\sigma^{-1}(2)2} \cdots a_{\sigma^{-1}(n)n}$. Ţinând seama că o permutare are aceeaşi signatură cu inversa sa, avem

$$|A| = \sum_{\sigma \in S_n} sgn(\sigma^{-1})a_{\sigma^{-1}(1)1}a_{\sigma^{-1}(2)2} \cdots a_{\sigma^{-1}(n)n} =$$

$$= \sum_{\tau \in S_n} sgn(\tau)a_{\tau(1)1}a_{\tau(2)2} \cdots a_{\tau(n)n} = |{}^tA|.$$

(b) şi (c) rezută din faptul că fiecare termen din (7.1) conţine exact un factor din linia i şi anume $a_{i\sigma(i)}$.

$$(d).\ |A| = \sum_{\sigma \in S_n} sgn(\sigma)a_{1\sigma(1)} \cdots a_{i-1\sigma(i-1)}(b_{\sigma(i)} + c_{\sigma(i)})a_{i+1\sigma(i+1)} \cdots a_{n\sigma(n)} =$$

$$= \sum_{\sigma \in S_n} sgn(\sigma)a_{1\sigma(1)} \cdots a_{i-1\sigma(i-1)}b_{\sigma(i)}a_{i+1\sigma(i+1)} \cdots a_{n\sigma(n)}+$$

$$+ \sum_{\sigma \in S_n} sgn(\sigma)a_{1\sigma(1)} \cdots a_{i-1\sigma(i-1)}c_{\sigma(i)}a_{i+1\sigma(i+1)} \cdots a_{n\sigma(n)} = |B| + |C|.$$

(e). Cf. lui (c), e suficient să tratăm cazul a două linii egale, şi fie acestea, pentru simplitate, primele două. Cum $S_n = A_n \cup A_n(12)$ este o partiţie a lui S_n, avem

$$|A| = \sum_{\sigma \in A_n} a_{1\sigma(1)}a_{2\sigma(2)} \cdots a_{n\sigma(n)} - \sum_{\sigma \in A_n} a_{1\sigma(2)}a_{2\sigma(1)} \cdots a_{n\sigma(n)} = 0$$

deoarece primele două linii sunt egale.

(f). Pentru simplitate, considerăm cazul când se permută primele două linii ale matricei A şi fie D matricea astfel obţinută. Remarcăm că funcţia $\sigma \mapsto \sigma(12) : S_n \to S_n$ este bijectivă. Deci putem înlocui în formula (7.1), σ cu $\sigma(12)$ şi obţinem

$$|A| = -\sum_{\sigma \in S_n} sgn(\sigma) a_{1\sigma(2)}a_{2\sigma(1)} \cdots a_{n\sigma(n)} = -|D|.$$

(g). Fie B matricea obţinută din A prin adunarea la linia i a elementelor liniei j înmulţite cu un element $\lambda \in R$. Aplicând proprietatea (d) pentru linia i a matricei B obţinem $|B| = |A| + \Delta$, unde Δ este un determinant cu două linii proporţionale, deci $\Delta = 0$, cf. (e).

(h) rezultă din (a). •

Corolarul 123 *Dacă una din liniile (resp. coloanele) unui determinant este combinaţie liniară de celelalte linii (resp. coloane), atunci determinantul este nul. În particular, dacă R este corp şi $|A| \neq 0$, atunci liniile lui A (resp. coloanele lui A) constituie o bază a R-spaţiului vectorial R^n.*

Demonstraţie. Prima afirmaţie rezultă din pct. (b), (d) şi (h) ale teoremei. A doua rezultă din faptul că n vectori din R^n formează o R-bază a lui R^n dacă şi numai dacă nici unul din ei nu este combinaţie liniară de ceilalţi. •

Teorema 124 *Fie $A = (a_{ij})_{1 \le i,j \le n}$ o matrice pătratică de ordinul n cu elemente din inelul comutativ R şi $\varphi : R \to S$ un morfism de inele. Aplicând φ fiecărui element al lui A obţinem matricea $B = (\varphi(a_{ij}))_{1 \le i,j \le n}$. Atunci $\varphi(|A|) = |B|$.*

Demonstraţie.

$$\varphi(|A|) = \varphi(\sum_{\sigma \in S_n} sgn(\sigma) a_{1\sigma(1)}a_{2\sigma(2)} \cdots a_{n\sigma(n)}) =$$

$$= \sum_{\sigma \in S_n} sgn(\sigma) \varphi(a_{1\sigma(1)}) \varphi(a_{2\sigma(2)}) \cdots \varphi(a_{n\sigma(n)}) = |B|. \bullet$$

Teorema 125 (Determinantul Vandermonde.) *Fie R un inel comutativ şi $a_1, ..., a_n \in R$. Atunci*

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ . & . & \cdots & . \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{vmatrix} = \prod_{1\leq j<i\leq n} (a_i - a_j).$$

Demonstraţie. Fie f determinantul din enunţ (determinantul Vandermonde). E suficient să dăm demonstraţia în cazul inelului de polinoame $T = \mathbf{Z}[X_1, X_2, ..., X_n]$ pentru $a_i = X_i$, $i = 1, ..., n$. Aceasta rezultă din teorema anterioară aplicată morfismului de inele $P(X_1, ..., X_n) \mapsto P(a_1, ..., a_n) : T \to R$. Privit ca polinom în nedeterminata X_n, f are rădăcinile X_1,...,X_{n-1}, deoarece un determinant cu două coloane egale este nul. Conform teoremei 81, putem scrie $f = (X_n - X_1) \cdots (X_n - X_{n-1})f_1$ cu $f_1 \in T$. Cu acelaşi raţionament, vedem că f_1, privit ca polinom în nedeterminata X_{n-1}, are rădăcinile X_1,...,X_{n-2}. Putem scrie $f = (X_n - X_1) \cdots (X_n - X_{n-1})(X_{n-1} - X_1) \cdots (X_{n-1} - X_{n-2})f_2$ cu $f_2 \in T$. Continuând astfel obţinem

$$f = b \prod_{1\leq j<i\leq n} (X_i - X_j).$$

Cum atât f cât şi $h = \prod_{1\leq j<i\leq n}(X_i - X_j)$ sunt polinoame omogene de grad $1 + 2 + \cdots + n - 1 = n(n - 1)/2 = C_n^2$, rezultă că $b \in \mathbf{Z}$. Deoarece monomul $X_2 X_3^2 \cdots X_n^{n-1}$ apare în f şi h cu coeficientul 1, rezultă că $b = 1$. •

7.2 Dezvoltări ale determinanţilor.

Fie R un inel comutativ, $n \geq 1$ şi fie $A = (a_{ij})_{1\leq i,j\leq n} \in M_n(R)$ o matrice pătratică de ordinul n cu elemente din R. Fie $1 \leq m \leq n$. Un *minor de ordinul* m (pe scurt, m-minor) al matricei A (al lui $|A|$) este un sub-determinant al lui $|A|$ aflat la intersecţia a m linii şi m coloane ale lui $|A|$. Mai concret, m-minorul definit de liniile $1 \leq k_1 < k_2 < \cdots < k_m \leq n$ şi coloanele $1 \leq l_1 < l_2 < \cdots < l_m \leq n$ este

$$M = \begin{vmatrix} a_{k_1 l_1} & \cdots & a_{k_1 l_m} \\ . & \cdots & . \\ a_{k_m l_1} & \cdots & a_{k_m l_m} \end{vmatrix}.$$

Prin definiţie, *minorul complementar al lui* M este $(n-m)$-minorul $\overline{M}$ al lui A obţinut din $|A|$ prin tăierea liniilor $1 \leq k_1 < k_2 < \cdots < k_m \leq n$ şi coloanelor $1 \leq l_1 < l_2 < \cdots < l_m \leq n$ (convenim ca determinantul vid să însemne 1). Se vede că M este atunci minorul complementar al lui $\overline{M}$. *Complementul algebric* M' al lui M este prin definiţie $(-1)^s\overline{M}$, unde $s = k_1 + \cdots + k_m + l_1 + \cdots + l_m$. Fie $(-1)^t M$ complementul algebric al lui $\overline{M}$. Cum $s + t = n(n+1) =$ număr par, rezultă că $\overline{M}$ are complementul algebric $(-1)^s M$. Complementul algebric al unui 1-minor $|a_{ij}|$ se mai numeşte *complementul algebric al elementului* a_{ij}. Acesta este $A_{ij} := (-1)^{i+j}D$, unde D este minorul obţinut din $|A|$ prin tăierea liniei i şi coloanei j.

Teorema 126 (Regula lui Laplace de dezvoltare a unui determinant).
În matricea pătratică $A = (a_{ij})_{1\leq i,j\leq n}$ cu elemente din inelul comutativ R, fixăm liniile $1 \leq k_1 < k_2 < \cdots < k_m \leq n$. Fie Γ mulţimea m-minorilor lui A cu elemente din liniile fixate $k_1, k_2, \ldots, k_m$. Atunci

$$|A| = \sum_{M\in\Gamma} MM'$$

altfel zis, $|A|$ este egal cu suma tuturor produselor dintre M şi complementul său algebric, când M parcurge mulţimea m-minorilor lui A cu elemente din liniile fixate. Un rezultat similar are loc pentru coloanele lui A.

De exemplu, dezvoltând determinantul următor după primele două linii obţinem

$$\begin{vmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \\ 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{vmatrix} = (-1)^6 \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} \begin{vmatrix} 3 & 4 \\ 7 & 8 \end{vmatrix} + (-1)^8 \begin{vmatrix} 1 & 0 \\ 0 & 2 \end{vmatrix} \begin{vmatrix} 2 & 3 \\ 6 & 7 \end{vmatrix} +$$

$$+(-1)^8 \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} \begin{vmatrix} 1 & 4 \\ 5 & 8 \end{vmatrix} + (-1)^{10} \begin{vmatrix} 1 & 0 \\ 0 & 2 \end{vmatrix} \begin{vmatrix} 1 & 2 \\ 5 & 6 \end{vmatrix} = -4 - 8 + 12 - 8 = -8.$$

Vom demonstra teorema ulterior. În cazul $m = 1$ obţinem exprimarea

$$|A| = a_{k1}A_{k1} + a_{k2}A_{k2} + \cdots + a_{kn}A_{kn}$$

numită *dezvoltarea determinantului după linia* k, unde A_{ij} este complementul algebric al elementului a_{ij}. Analog, obţinem exprimarea

$$|A| = a_{1k}A_{1k} + a_{2k}A_{2k} + \cdots + a_{nk}A_{nk}$$

numită *dezvoltarea determinantului după coloana* k.

Matricea adjunctă a lui A, notată A^*, este transpusa matricei obţinute din A prin înlocuirea fiecărui element a_{ij} cu complementul său algebric A_{ij}. De exemplu, adjuncta lui $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ este $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, iar adjuncta lui $\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ este $\begin{pmatrix} ei - fh & -(bi - ch) & bf - ce \\ -(di - fg) & ai - cg & -(af - cd) \\ dh - eg & -(ah - bg) & ae - bd \end{pmatrix}$.

Teorema 127 *Fie* $A = (a_{ij})_{1 \le i,j \le n}$ *o matrice pătratică cu elemente din inelul comutativ* R *şi fie* $1 \le k, l \le n$ *fixate. Atunci*

$$a_{k1}A_{l1} + a_{k2}A_{l2} + \cdots + a_{kn}A_{ln} = \delta_{kl}|A|$$

şi

$$a_{1k}A_{1l} + a_{2k}A_{2l} + \cdots + a_{nk}A_{nl} = \delta_{kl}|A|$$

unde A_{ij} *este complementul algebric al elementului* a_{ij} *iar* δ_{kl} *este simbolul lui Kronecker. În particular*

$$AA^* = A^*A = |A|I_n.$$

Demonstraţie. Probăm prima relaţie. Cazul $k = l$ a fost explicitat mai sus, deci putem presupunem $k \neq l$. $d = a_{k1}A_{l1} + a_{k2}A_{l2} + \cdots + a_{kn}A_{ln}$ reprezintă dezvoltarea după linia l a determinantului obţinut din $|A|$ prin înlocuirea liniei l cu linia k, deci $d = 0$ (determinant cu două linii egale). A doua afirmaţie rezultă analog. Ultima afirmaţie rezultă din primele două şi din definiţia matricei adjuncte. •

Pentru demonstraţia teoremei 126 avem nevoie de următoarea lemă. Fie M un m-minor al lui A şi M' complementul său algebric. Fie $M = M_1 + \cdots + M_{m!}$ şi $M' = N_1 + \cdots + N_{(n-m)!}$ dezvoltările celor doi minori (vezi egalitatea 7.1). Deci $MM' = \sum_{i=1}^{m!} \sum_{j=1}^{(n-m)!} M_i N_j$.

Lema 128 *În contextul anterior, fiecare produs M_iN_j este un termen din dezvoltarea lui $|A|$.*

Demonstraţie. Pentru început, presupunem că M este m-minorul "stânga-sus", adică cel definit de primele m linii şi m coloane ale lui A. Atunci M' este chiar minorul complementar al lui M, deoarece $1 + \cdots + m + 1 \cdots + m = 2m$ este număr par. Fie $(-1)^\alpha a_{1t_1} a_{2t_2} \cdots a_{mt_m}$ resp. $(-1)^\beta a_{m+1t_{m+1}} a_{m+2t_{m+2}} \cdots a_{mt_n}$ un termen din dezvoltarea lui M resp. M' unde α resp. β este numărul de inversiuni ale permutării $\begin{pmatrix} 1 & \cdots & m \\ t_1 & \cdots & t_m \end{pmatrix}$ resp. $\begin{pmatrix} m+1 & \cdots & n \\ t_{m+1} & \cdots & t_n \end{pmatrix}$. E suficient să observăm că permutarea $\begin{pmatrix} 1 & \cdots & m & m+1 & \cdots & n \\ t_1 & \cdots & t_m & t_{m+1} & \cdots & t_n \end{pmatrix}$ are $\alpha+\beta$ inversiuni, deoarece $t_1, ..., t_m \in \{1, ..., m\}$ şi $t_{m+1}, ..., t_n \in \{m+1, ..., n\}$.

Presupunem acum că M este m-minorul definit de definit de liniile $1 \leq k_1 < k_2 < \cdots < k_m \leq n$ şi coloanele $1 \leq l_1 < l_2 < \cdots < l_m \leq n$. Prin $k_1 - 1$ permutări de linii vecine, aducem elementele liniei k_1 pe prima linie, apoi aducem, prin $k_2 - 2$ permutări de linii vecine, elementele liniei k_2 pe a doua linie, ş.a.m.d. Continuăm pe coloane. Procedând astfel aducem minorul M în poziţia stânga-sus S prin $k_1 + \cdots + k_m - (1 + \cdots + m)$ permutări de linii vecine şi $l_1 + \cdots + l_m - (1 + \cdots + m)$ permutări de coloane vecine. Făcând astfel, ordinea liniilor şi coloanelor din M şi M' se păstrează iar $|A|$ se înmulţeşte cu $(-1)^w$ cu $w = k_1 + \cdots + k_m + l_1 + \cdots + l_m$. Ne-am redus astfel la cazul analizat anterior deoarece $M' = (-1)^w \overline{M}$, unde $\overline{M}$ este minorul complementar al lui M. •

Demonstraţia teoremei 126. Fie M, N doi m-minori distincţi cu elemente din liniile $k_1, ..., k_m$. Atunci dezvoltările lui MM' şi NN' nu au termeni comuni, deoarece M, N au cel puţin o coloană diferită. Deci, cf. lemei, în suma din teoremă se găsesc $C_n^m m!(n-m)! = n!$ termeni din dezvoltarea lui $|A|$, adică toţi. •

7.3 Aplicaţii

Teorema 129 *Fie A, B două matrice pătratice de ordinul n cu elemente din inelul comutativ R. Atunci $|AB| = |A||B|$.*

Demonstraţie. Fie C matricea pătratice de ordinul $2n$, $C = \begin{pmatrix} A & 0 \\ -I_n & B \end{pmatrix}$. Dezvoltând cu regula lui Laplace pe primele n linii, găsim $|C| = |A||B|$. Pe de altă parte, calculăm $|C|$ în modul următor. Prin amplificări convenabile ale primelor n coloane şi adunarea lor la următoarele n coloane, facem 0 în locul lui B. Fie $1 \leq k \leq n$. Pentru a anula coloana k a lui B adunăm la coloana $n+k$ a lui C coloanele $1,\ldots,n$ înmulţite respectiv cu $b_{1k},\ldots,b_{nk}$. În urma acestei operaţii, primele n elemente de pe coloana k a lui C vor fi $(a_{i1}b_{1k}+\cdots+a_{in}b_{nk})_{1\leq i\leq n}$. Se obţine $|C| = \begin{vmatrix} A & AB \\ -I_n & 0 \end{vmatrix}$. Dezvoltând din nou cu regula lui Laplace pe primele n linii, găsim $|C| = (-1)^w|-I_n||AB|$, unde $w = 1+\cdots+n+(n+1)+\cdots+2n = n(2n+1)$. Deci $|C| = (-1)^{2n^2+2n}|AB| = |AB|$. •

Reamintim că o matrice $A \in M_n(R)$, R inel comutativ, se numeşte *matrice inversabilă* dacă există o matrice $B \in M_n(R)$ astfel încât $AB = BA = I_n$.

Teorema 130 *Fie A o matrice pătratică de ordinul n cu elemente din inelul comutativ R. Atunci A este inversabilă dacă şi numai dacă $|A|$ este un element inversabil în R. În acest caz, inversa lui A este $|A|^{-1}A^*$, unde A este adjuncta lui A.*

Demonstraţie. Dacă $AB = I_n$, atunci $1 = |I_n| = |AB| = |A||B|$, deci $|A| \in U(R)$, cf. teoremei 129. Reciproc, să presupunem că $|A| \in U(R)$. Atunci $A(|A|^{-1}A^*) = (|A|^{-1}A^*)A = I_n$, cf. teoremei 127. •

În particular, dacă R este corp, A este inversabilă dacă şi numai dacă $|A| \neq 0$.

Teorema 131 *Fie A, B matrice de tip (m,n) respectiv (n,m) cu elemente din inelul comutativ R. Dacă $AB = I_m$ şi $BA = I_n$, atunci $m = n$.*

Demonstraţie. Presupunem că $m > n$. Condiderăm matricele pătratice de ordinul m, $C = \begin{pmatrix} A & 0_{m(m-n)} \end{pmatrix}$ şi $D = \begin{pmatrix} B \\ 0_{(m-n)m} \end{pmatrix}$. Se observă că $CD = I_m$, deci $0 = |C||D| = |CD| = 1$, contradicţie. •

Teorema 132 (Regula lui Cramer.) *Fie $A = (a_{ij})_{1\leq i,j\leq n}$ o matrice pătratică de ordinul n cu elemente din inelul comutativ R şi $b_1, ..., b_n \in R$. Dacă $|A|$ este un element inversabil în R, atunci sistemul de ecuaţii liniare*

$$\sum_{j=1}^{n} a_{ij}x_j = b_i, \qquad i = 1, ..., n$$

este compatibil determinat cu soluţia unică $(\Delta_1|A|^{-1},...,\Delta_n|A|^{-1})$, unde Δ_j este determinantul obţinut din $|A|$ prin înlocuirea coloanei j cu vectorul termenilor liberi $\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$.

Demonstraţie. Scris matriceal, sistemul este $Ax = b$ unde $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ şi $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$. Deci el are soluţia unică $s = A^{-1}b = \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}$. Fie c_1,...,c_n coloanele lui A. Rezultă că $b = s_1c_1 + \cdots + s_nc_n$. Notând cu $|b\ c_2\ \cdots\ c_n|$ determinantul cu coloanele b, c_2, ..., c_n, avem

$$\Delta_1 = |b\ c_2\ \cdots\ c_n| = |b - s_2c_2 - \cdots - s_nc_n\ c_2\ \cdots\ c_n| = s_1|A|.$$

Deci $s_1 = \Delta_1|A|^{-1}$ şi la fel se arată că $s_j = \Delta_j|A|^{-1}$, $j = 2, ..., n$.

Altă demonstraţie. Fie A_{ij} complementul algebric al lui a_{ij} în matricea A. Înmulţind cu A^* egalitatea $Ax = b$ se obţine $|A|x = A^*b$. Pentru $k = 1, ..., n$, deducem că $|A|x_k = A_{1k}b_1 + A_{2k}b_2 + \cdots + A_{nk}b_k$ care este dezvoltarea după coloana k a determinantului matricei obţinute din A prin înlocuirea coloanei k cu vectorul b; deci $x_k = \Delta_k|A|^{-1}$. •

Un sistem de ecuaţii liniare căruia i se poate aplica regula lui Cramer se numeşte *sistem Cramer*. De exemplu, sistemul de ecuaţii liniare

$$\begin{cases} x & + & y & + & z & = & 1 \\ ax & + & by & + & cz & = & d \\ ax^2 & + & b^2y & + & c^2z & = & d^2 \\ a^3x & + & b^3y & + & c^3z & = & d^3 \end{cases}$$

unde a, b, c, d sunt numere reale, a, b, c distincte, este sistem Cramer şi are soluţia

$$(c-d)(c-b)(b-d)/\delta,\ (c-a)(c-d)(d-a)/\delta,\ (d-a)(d-b)(b-a)/\delta$$

unde $\delta = (c-a)(c-b)(b-a)$, cf. teoremei 125.

Vom folosi următoarea notaţie. Fie A o matrice de tip (n, p), $m \leq n, p$ şi $I \subseteq \{1, ..., n\}$, $J \subseteq \{1, ..., p\}$ mulţimi cu m elemente. Notăm cu A_I^J m-minorul lui A cu format cu liniile cu indici din I şi coloanele cu indici din J.

Teorema 133 (Formula Binet-Cauchy). *Fie A şi B matrice de tip (n, p) şi respectiv (p, q), şi fie $m \leq n, p, q$. Fie $I \subseteq \{1, ..., n\}$ şi $K \subseteq \{1, ..., q\}$ două submulţimi cu m elemente. Atunci*

$$(AB)_I^K = \sum_J A_I^J B_J^K$$

suma făcându-se după toate submulţimile $J \subseteq \{1, ..., p\}$ cu m elemente.

Demonstraţie. Fie $C = AB$, $I = \{i_1, i_2, ..., i_m\}$ şi $K = \{k_1, k_2, ..., k_m\}$ cu $i_1 < i_2 < \cdots < i_m$ şi $k_1 < k_2 < \cdots < k_m$. Punem $A = (a_{ij})$, $B = (b_{jk})$ şi $C = (c_{ik})$. Fie $s_1, ..., s_m$ o permutare a numerelor $k_1, ..., k_m$, adică $\{s_1, ..., s_m\} = \{k_1, ..., k_m\}$. Atunci signatura permutării $\begin{pmatrix} k_1 & k_2 & ... & k_m \\ s_1 & s_2 & ... & s_m \end{pmatrix}$ este $(-1)^{Inv(s_1,...,s_m)}$ unde $Inv(s_1, ..., s_m)$ este numărul perechilor (u, v), $1 \leq u < v \leq m$, cu $s_u > s_v$. Avem

$$C_I^K = C_{i_1,...,i_m}^{k_1,...,k_m} = \sum_{\{s_1,...,s_m\}=\{k_1,...,k_m\}} (-1)^{Inv(s_1,...,s_m)} c_{i_1 s_1} \cdots c_{i_m s_m} =$$

$$= \sum_{\{s_1,...,s_m\}=\{k_1,...,k_m\}} (-1)^{Inv(s_1,...,s_m)} (\sum_{t_1=1}^{p} a_{i_1 t_1} b_{t_1 s_1}) \cdots (\sum_{t_m=1}^{p} a_{i_m t_m} b_{t_m s_m}) =$$

$$= \sum_{t_1=1}^{p} \cdots \sum_{t_m=1}^{p} a_{i_1 t_1} \cdots a_{i_m t_m} \sum_{\{s_1,\dots,s_m\}=\{k_1,\dots,k_m\}} (-1)^{Inv(s_1,\dots,s_m)} b_{t_1 s_1} \cdots b_{t_m s_m} =$$

$$= \sum_{t_1=1}^{p} \cdots \sum_{t_m=1}^{p} a_{i_1 t_1} \cdots a_{i_m t_m} B^{k_1,\dots,k_m}_{t_1,\dots,t_m}$$

unde $B^{k_1,\dots,k_m}_{t_1,\dots,t_m}$ desemnează m-minorul lui B cu liniile $t_1, \dots, t_m$ şi coloanele $k_1, \dots, k_m$ în această ordine. Acest minor este nul dacă numerele $t_1, \dots, t_m$ nu sunt distincte. Deci putem scrie

$$C_I^K = \sum_{1 \le j_1 < \cdots < j_m \le p} \sum_{\{t_1,\dots,t_m\}=\{j_1,\dots,j_m\}} a_{i_1 t_1} \cdots a_{i_m t_m} (-1)^{Inv(t_1,\dots,t_m)} B^{k_1,\dots,k_m}_{j_1,\dots,j_m} =$$

$$= \sum_{1 \le j_1 < \cdots < j_m \le p} B^{k_1,\dots,k_m}_{j_1,\dots,j_m} \sum_{\{t_1,\dots,t_m\}=\{j_1,\dots,j_m\}} (-1)^{Inv(t_1,\dots,t_m)} a_{i_1 t_1} \cdots a_{i_m t_m} =$$

$$= \sum_{1 \le j_1 < \cdots < j_m \le p} B^{k_1,\dots,k_m}_{j_1,\dots,j_m} A^{j_1,\dots,j_m}_{i_1,\dots,i_m} = \sum_J A_I^J B_J^K. \bullet$$

Cazul $m = 1$ al formulei Binet-Cauchy este chiar regula de înmulţire a două matrice, iar în cazul $m = n = p = q$ se obţine $|AB| = |A||B|$, deci o nouă demonstraţie a teoremei 129.

7.4 Exerciţii

175. Calculaţi determinanţii

$$\begin{vmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{vmatrix}, \quad \begin{vmatrix} a & b & c \\ b & c & a \\ c & a & b \end{vmatrix}, \quad \begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix}, \quad \begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^3 & b^3 & c^3 \end{vmatrix}, \quad \begin{vmatrix} 1 & 1 & 1 \\ a^2 & b^2 & c^2 \\ a^3 & b^3 & c^3 \end{vmatrix}.$$

176. Fie x_1, x_2, x_3 rădăcinile ecuaţiei $x^3 + px + q = 0$. Calculaţi discriminantul ecuaţiei, adică $\begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{vmatrix}^2$, în funcţie de p şi q.

177. Calculaţi determinanţii

$$\begin{vmatrix} a & b & b & b \\ b & a & b & b \\ b & b & a & b \\ b & b & b & a \end{vmatrix}, \quad \begin{vmatrix} 0 & x & y & z \\ x & 0 & z & y \\ y & z & 0 & x \\ z & y & x & 0 \end{vmatrix}, \quad \begin{vmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{vmatrix}.$$

178. Calculaţi determinantul $\begin{vmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ . & . & \cdots & . \\ a_1^{i-1} & a_2^{i-1} & \cdots & a_n^{i-1} \\ a_1^{i+1} & a_2^{i+1} & \cdots & a_n^{i+1} \\ . & . & \cdots & . \\ a_1^n & a_2^n & \cdots & a_n^n \end{vmatrix}$.

179. Calculaţi determinantul $\Delta = \begin{vmatrix} a_1 & x & x & \cdots & x \\ x & a_2 & x & \cdots & x \\ x & x & a_3 & \cdots & x \\ . & . & . & \cdots & . \\ x & x & x & \cdots & a_n \end{vmatrix}$.

180. Calculaţi determinantul următor prin dezvoltare Laplace pe liniile 1 şi 2

$$\begin{vmatrix} 5 & 3 & 0 & 0 & 0 \\ 2 & 5 & 3 & 0 & 0 \\ 0 & 2 & 5 & 3 & 0 \\ 0 & 0 & 2 & 5 & 3 \\ 0 & 0 & 0 & 2 & 5 \end{vmatrix}.$$

181. Calculaţi determinantul $D_n = \begin{vmatrix} 5 & 3 & 0 & 0 & \cdots & 0 & 0 \\ 2 & 5 & 3 & 0 & \cdots & 0 & 0 \\ 0 & 2 & 5 & 3 & \cdots & 0 & 0 \\ . & . & . & . & \cdots & . & . \\ 0 & 0 & 0 & 0 & \cdots & 2 & 5 \end{vmatrix}$.

182. Fie polinomul $f = a_1 + a_2X + \cdots + a_nX^{n-1}$ şi matricele

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-3} & a_{n-2} \\ . & . & . & \cdots & . & . \\ a_2 & a_3 & a_4 & \cdots & a_n & a_1 \end{pmatrix} \text{ şi } B = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_n \\ \varepsilon_1^2 & \varepsilon_2^2 & \cdots & \varepsilon_n^2 \\ . & . & \cdots & . \\ \varepsilon_1^{n-1} & \varepsilon_2^{n-1} & \cdots & \varepsilon_n^{n-1} \end{pmatrix}$$

unde ε_1,...,ε_n sunt rădăcinile de ordinul n ale unităţii. Arătaţi că $|AB| = f(\varepsilon_1)\cdots f(\varepsilon_n)|B|$ şi calculaţi $|A|$.

183. Arătaţi că grupurile abeliene $\mathbf{Z}^2$ şi $\mathbf{Z}^3$ nu sunt izomorfe.

184. Găsiţi un inel necomutativ R şi două matrice A resp. B matrice de tip $(1,2)$ resp. $(2,1)$ cu elemente din R astfel încât $AB = I_1$ şi $BA = I_2$.

185. Număraţi matricele inversabile de ordin 3 cu elemente din $\mathbf{Z}_2$. Generalizare.

186. Număraţi matricele inversabile de ordin 3 cu elemente din $\mathbf{Z}_4$.

187. Calculaţi inversele matricelor

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}, \begin{pmatrix} \sin\alpha & \cos\alpha \\ \cos\alpha & -\sin\alpha \end{pmatrix}, \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}.$$

188. Calculaţi inversa matricei $U = \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 0 & \cdots & 1 & 1 \\ . & . & . & \cdots & . & . \\ 1 & 1 & 1 & \cdots & 1 & 0 \end{pmatrix}$.

189. Calculaţi inversa matricei $B = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_n \\ \varepsilon_1^2 & \varepsilon_2^2 & \cdots & \varepsilon_n^2 \\ . & . & \cdots & . \\ \varepsilon_1^{n-1} & \varepsilon_2^{n-1} & \cdots & \varepsilon_n^{n-1} \end{pmatrix}$, unde $\varepsilon_1,...,\varepsilon_n$ sunt rădăcinile de ordinul n ale unităţii.

Capitolul 8

Spaţii vectoriale şi sisteme liniare

În acest capitol se introduc noţiunile de bază referitoare la spaţii vectoriale. Apoi, se prezintă metoda eliminării a lui Gauss de rezolvare a sistemelor de ecuaţii liniare şi se studiază noţiunea de rang al unei matrice.

În acest capitol, prin corp vom înţelege corp comutativ.

8.1 Spaţii vectoriale

Fie K un corp. Un *spaţiu vectorial* peste corpul K (pe scurt, K-*spaţiu vectorial*) este un grup abelian $(V, +)$ împreună cu o operaţie externă $K \times V \to V$, $(a, x) \mapsto ax$, numită *înmulţire cu scalari*, care verifică următoarele condiţii pentru orice $a, b \in K$ şi $x, y \in V$

(1) $a(x + y) = ax + ay$,
(2) $(a + b)x = ax + bx$,
(3) $(ab)x = a(bx)$,
(4) $1x = x$.

Elementele lui K se numesc *scalari* iar cele din V *vectori*. Prin notaţia ${}_KV$ vom înţelege că V este un K-spaţiu vectorial. Vom nota cu 0_K scalarul nul şi cu 0_V vectorul nul (când nu este pericol de confuzie, vom suprima indicii K şi V).

Teorema 134 *Fie ${}_KV$ un spaţiu vectorial, $a \in K$ şi $x \in V$. Atunci*

(a) $ax = 0_V$ dacă şi numai dacă $a = 0_K$ sau $x = 0_V$.
(b) $(-a)x = a(-x) = -ax$.

Demonstraţie. (a) Avem $0_K x = (0_K + 0_K)x = 0_K x + 0_K x$, deci, scăzând din ambii membri $0_K x$, rezultă $0_K x = 0_V$. La fel se arată că $a0_V = 0_V$. Reciproc, dacă $ax = 0_V$ şi $a \neq 0_K$, atunci a este inversabil în K şi rezultă $x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}0_V = 0_V$.

(b) rezultă din egalităţile $0_V = (a-a)x = ax + (-a)x$ şi $0_V = a(x-x) = ax + a(-x)$. •

Exemple. 1. Dacă $n \geq 1$, atunci K^n are o structură de K-spaţiu vectorial obţinută definind adunarea vectorilor prin $(a_1, ..., a_n) + (b_1, ..., b_n) = (a_1 + b_1, ..., a_n + b_n)$ şi înmulţirea cu scalari prin $\alpha(a_1, ..., a_n) = (\alpha a_1, ..., \alpha a_n)$, pentru $\alpha, a_1, ..., a_n, b_1, ..., b_n \in K$. K^n se numeşte *spaţiul vectorial standard de dimensiune n.*

2. Dacă ${}_KV_1$,..., ${}_KV_n$ sunt spaţii vectoriale, atunci produsul cartezian $V_1 \times \cdots \times V_n$ are o structură de spaţiu vectorial obţinută definind adunarea vectorilor prin $(v_1, ..., v_n) + (w_1, ..., w_n) = (v_1 + w_1, ..., v_n + w_n)$ şi înmulţirea cu scalari prin $\alpha(v_1, ..., v_n) = (\alpha v_1, ..., \alpha v_n)$, pentru $\alpha \in K$ şi $v_i, w_i \in V_i$, $i = 1, ...n$. $V_1 \times \cdots \times V_n$ se numeşte *produsul direct al spaţiilor vectoriale* V_1,..., V_n.

3. Dacă K este subcorp al inelului L, atunci grupul aditiv al lui L are o structură de K-spaţiu vectorial în care înmulţirea cu scalari este chiar înmulţirea din L (dacă $a \in K$ şi $x \in L$, ax este produsul dintre a şi x în L). De exemplu, $\mathbf{R}$, $\mathbf{C}$ şi $\mathbf{Q}(\sqrt{2})$ sunt $\mathbf{Q}$-spaţii vectoriale. De asemenea, $M_n(K)$, $K[X]$ şi $K(X)$ sunt K-spaţii vectoriale.

4. Fie p un număr prim şi $(G, +)$ un grup abelian. Se vede uşor că G are o structură de $\mathbf{Z}_p$-spaţiu vectorial dacă şi numai dacă $px = 0$ pentru orice $x \in G$. În acest caz, înmulţirea cu scalari se defineşte prin $\hat{a}x = ax$, pentru $a \in \mathbf{Z}$ şi $x \in G$. Definiţia este corectă. Într-adevăr, fie $a, b \in \mathbf{Z}$ cu $\hat{a} = \hat{b}$. Atunci $a - b = pc$ cu $c \in \mathbf{Z}$, deci $ax - bx = (a-b)x = pcx = 0$, adică $ax = bx$.

Fie V, W două K-spaţii vectoriale. O funcţie $f : V \to W$ se numeşte *morfism de spaţii vectoriale* sau *aplicaţie liniară* dacă $f(ax + by) = af(x) + bf(y)$ pentru orice $a, b \in K$ şi $x, y \in V$. f este în particular morfism de grupuri abeliene, deci $f(0) = 0$, $f(-x) = -f(x)$ pentru orice $x \in V$ şi f este injecţie dacă şi numai dacă $ker(f) = \{0\}$, unde $ker(f) = \{x \in V |\ f(x) = 0\}$

este nucleul lui f. Un morfism $f: V \to V$ se numeşte *endomorfism* al lui V.

Fie V, W două K-spaţii vectoriale. Morfismul $x \mapsto 0 : V \to W$ este numit *morfismul trivial)*, iar $I_V : V \to V$, $I_V(x) = x$ este numit *morfismul identic*. Dacă $a \in K$, atunci endomorfismul $x \mapsto ax : V \to V$ este numit *omotetia* definită de a.

Un morfism de spaţii vectoriale bijectiv se numeşte *izomorfism* iar două spaţii vectoriale se zic *izomorfe* dacă există un izomorfism între ele.

Teorema 135 (a) *Compunerea a două morfisme de spaţii vectoriale este un morfism de spaţii vectoriale.*

(b) *Inversul unui izomorfism de spaţii vectoriale este tot un izomorfism.*

Demonstraţie. (a). Fie $f : V \to V'$ şi $g : V' \to V''$ morfisme de K-spaţii vectoriale şi fie $x, y \in V$, $a, b \in K$. Rezultă că $(gf)(ax + by) = g(af(x) + bf(y)) = a(gf)(x) + b(gf)(y)$. Deci gf este morfism. (b). Fie $f : V \to V'$ un izomorfism şi fie $x, y \in V'$, $a, b \in K$. Notăm $x' = f^{-1}(x)$ şi $y' = f^{-1}(y)$. Atunci $f^{-1}(ax+by) = f^{-1}(af(x')+bf(y')) = f^{-1}(f(ax'+by')) = ax' + by' = af^{-1}(x) + bf^{-1}(y)$. •

Spunem că o submulţime nevidă W a unui spaţiu vectorial ${}_KV$ este *subspaţiu al lui* V (şi notăm $W \leq V$) dacă $ax + by \in W$ pentru orice $a, b \in K$ şi $x, y \in W$. Dacă $W \leq V$, atunci W este K-spaţiu vectorial faţă de operaţiile de adunare a vectorilor şi înmulţire cu scalari induse din V. Pentru orice spaţiu vectorial ${}_KV$, $\{0\}$ şi V sunt subspaţii numite *subspaţiul trivial* respectiv *subspaţiul impropriu*. Subspaţiul nul $\{0\}$ se mai notează simplu cu 0.

Fie $a, b \in \mathbf{R}$ cu $a^2 + b^2 \neq 0$. Atunci dreapta $\{(x, y) |\ ax + by = 0\}$ este un subspaţiu al lui ${}_{\mathbf{R}}\mathbf{R}^2$.

Teorema 136 *Fie* $f : V \to W$ *o aplicaţie liniară.*

(a). *Dacă* $V' \leq V$, *atunci* $f(V') \leq W$.

(b). *Dacă* $W' \leq W$, *atunci* $f^{-1}(W') \leq V$.

În particular, nucleul şi imaginea lui f *sunt subspaţii.*

Demonstraţie. (a). Fie $x, y \in V'$ şi $a, b \in K$. Atunci $ax + by \in V'$, deci $af(x)+bf(y) = f(ax+by) \in V'$. (b). Fie $x, y \in f^{-1}(W')$ şi $a, b \in K$. Atunci $f(x), f(y) \in W'$, deci $f(ax + by) = af(x) + bf(y) \in W'$, de unde rezultă că $ax + by \in f^{-1}(W')$. •

Dacă ${}_KV$ un spaţiu vectorial şi $(V_i)_{i\in I}$ o familie de subspaţii ale lui V, atunci intersecţia subspaţiilor V_i este de asemenea un subspaţiu al lui V, deoarece dacă $a, b \in K$ şi $x, y \in \cap_{i\in I} V_i$, atunci $ax + by$ este în fiecare V_i, deci $ax + by \in \cap_{i\in I} V_i$.

Dacă ${}_KV$ un spaţiu vectorial şi V_1, ..., V_n subspaţii ale lui V, atunci

$$V_1 + \cdots + V_n = \{x_1 + \cdots + x_n |\ x_i \in V_i, i = 1, ..., n\}$$

este de asemenea un subspaţiu al lui V, numit *suma subspaţiilor* V_1, ..., V_n. Într-adevăr, dacă $x_i, y_i \in V_i, i = 1, ..., n$, şi $a, b \in K$, atunci $a(x_1 + \cdots + x_n) + b(y_1 + \cdots + y_n) = (ax_1 + by_1) + \cdots + (ax_n + by_n) \in V_1 + \cdots + V_n$, deoarece $ax_i + by_i \in V_i$ pentru orice i. Mai general, suma unei familii F de subspaţii se defineşte ca reuniunea sumelor tuturor subfamiliilor finite ale lui F.

În ${}_{\mathbf{R}}\mathbf{R}^3$, suma subspaţiilor

$$V_1 = \{(x, y, 0)|\ x, y \in \mathbf{R}\},\ V_2 = \{(0, x, y)|\ x, y \in \mathbf{R}\}$$

este $\mathbf{R}^3$ iar intersecţia lor este $\{(0, x, 0)|\ x \in \mathbf{R}\}$.

Spunem că spaţiu vectorial ${}_KV$ este *suma directă* a subspaţiilor V_1 şi V_2, şi notăm $V = V_1 \oplus V_2$ dacă $V = V_1 + V_2$ şi $V_1 \cap V_2 = 0$. De exemplu, ${}_{\mathbf{R}}\mathbf{R}^3$ este suma directă a subspaţiilor $V_1 = \{(x, y, 0)|\ x, y \in \mathbf{R}\}$ şi $V_2 = \{(0, 0, z)|\ z \in \mathbf{R}\}$.

Fie ${}_KV$ un spaţiu vectorial şi $v_1, ..., v_n \in V$. Notăm cu $< v_1, ..., v_n >$ mulţimea tuturor *combinaţiilor liniare* ale elementelor $v_1, ..., v_n$, adică a sumelor $a_1v_1 + \cdots + a_nv_n$ cu $a_1, ..., a_n \in K$. $< v_1, ..., v_n >$ este un subspaţiu al lui V numit *subspaţiul generat de* $v_1, ..., v_n$.

Într-adevăr, dacă $c, d, a_1, ..., a_n, b_1, ..., b_n \in K$, atunci $c(a_1v_1 + \cdots + a_nv_n) + b(a_1v_1 + \cdots + a_nv_n) = (ca_1 + db_1)v_1 + \cdots + (ca_n + db_n)v_n$.

E clar că dacă W este un subspaţiu al lui V care conţine elementele $v_1, ..., v_n$, atunci $< v_1, ..., v_n >\subseteq W$. Deci $< v_1, ..., v_n >$ este intersecţia tuturor subspaţiilor lui V care conţin elementele $v_1, ..., v_n$.

În general, subspaţiul generat de o submulţime nu neapărat finită G a lui V se defineşte ca mulţimea tuturor combinaţiilor liniare ale submulţimilor finite ale lui G, $< G >:= \{a_1v_1 + \cdots + a_nv_n|\ a_1, ..., a_n \in K,\ v_1, ..., v_n \in G,\ n \geq 0\}$.

Spunem că un spaţiu vectorial ${}_KV$ este *finit generat* dacă există o mulţime de vectori $v_1, ..., v_n$ astfel încât $V =< v_1, ..., v_n >$

Spunem că o mulţime de vectori $v_1, ..., v_n$ ai spaţiului vectorial ${}_KV$ este *liniar independentă* (sau că vectorii $v_1, ..., v_n$ sunt liniar independenţi), dacă singura combinatie liniară nulă a vectorilor $v_1, ..., v_n$ este cea trivială, adică dacă $a_1, ..., a_n \in K$ şi $a_1v_1 + \cdots + a_nv_n = 0$ implică $a_1 = \cdots = a_n = 0$. Mulţimea vidă este liniar independentă.

În general, spunem că o submulţime nu neapărat finită G a lui V este *liniar independentă* dacă orice submulţime finită alui G este liniar independentă. O submulţime T a lui V se zice *liniar dependentă* dacă nu este liniar independentă.

E clar că o submulţime a unei mulţimi liniar independente este liniar independentă şi că o mulţime liniar independentă nu conţine vectorul nul (deoarece $1 \cdot 0_V = 0_V$).

Teorema 137 *Fie ${}_KV$ un spaţiu vectorial şi $v_1, ..., v_n \in V$. Afirmaţiile următoare sunt echivalente.*

(a) *Vectorii $v_1, ..., v_n$ sunt liniar independenţi.*

(b) *Nici unul dintre vectorii $v_1, ..., v_n$ nu este o combinaţie liniară a celorlalţi.*

(c) *$v_1 \neq 0$, $v_2 \notin < v_1 >$, ..., $v_n \notin < v_1, ..., v_{n-1} >$.*

Demonstraţie. Implicaţia $(b) \Rightarrow (c)$ este clară.

$(c) \Rightarrow (a)$. Presupunem că vectorii $v_1, ..., v_n$ sunt liniar dependenţi. Atunci există $a_1, ..., a_j \in K$, $a_j \neq 0$, astfel încât $a_1v_1 + \cdots + a_jv_j = 0$. Deci $v_j = -(a_1/a_j)v_1 - \cdots - (a_{j-1}/a_j)v_{j-1} \in < v_1, ..., v_{j-1} >$.

$(a) \Rightarrow (b)$. Dacă vectorul v_i este combinaţie liniară a celorlalţi, să zicem, $v_i = a_1v_1 + \cdots + a_{i-1}v_{i-1} + a_{i+1}v_{i+1} \cdots + a_nv_n$, atunci $a_1v_1 + \cdots + a_{i-1}v_{i-1} - v_i + a_{i+1}v_{i+1} \cdots + a_nv_n = 0$, deci vectorii $v_1, ..., v_n$ sunt liniar dependenţi. •

Teorema 138 (Teorema schimbului.) *Fie ${}_KV$ un spaţiu vectorial finit generat, $w_1, ..., w_n$ un sistem de generatori al lui V şi $v_1, ..., v_m \in V$ vectori liniar independenţi. Atunci $m \leq n$ şi după o renumerotare a vectorilor $w_1, ..., w_n$, $< v_1, ..., v_m, w_{m+1}, ..., w_n >= V$.*

Demonstraţie. Facem inducţie după m. Pentru $m = 0$ afirmaţia e clară. Fie $m \geq 1$. Din ipoteza de inducţie, putem renumerota vectorii $w_1, ..., w_n$ astfel încât $< v_1, ..., v_{m-1}, w_m, ..., w_n >= V$. Deci putem scrie pe v_m ca o combinaţie liniară $v_m = a_1v_1+\cdots+a_{m-1}v_{m-1}+a_mw_m+\cdots+a_nw_n$ cu $a_i \in K$. Cum $v_1, ..., v_m$ sunt liniar independenţi, rezultă că $n \geq m$ şi nu toţi scalarii a_m, ..., a_n sunt nuli; renumerotând vectorii w_m, ..., w_n, putem presupune că $a_m \neq 0$. Rezultă că $w_m = -(a_1/a_m)v_1 - \cdots - (a_{m-1}/a_m)v_{m-1} + (1/a_m)v_m - (a_{m+1}/a_m)w_{m+1} - \cdots - (a_n/a_m)w_n$. Deci $V =< v_1, ..., v_{m-1}, w_m, ..., w_n >\subseteq< v_1, ..., v_m, w_{m+1}, ..., w_n >$, adică $< v_1, ..., v_m, w_{m+1}, ..., w_n >= V$.

Fie ${}_KV$ un spaţiu vectorial. O *bază* a lui V este o submulţime a lui V care este simultan liniar independentă şi sistem de generatori pentru V. Vectorii $e_1 = (1, ..., 0)$, $e_2 = (0, 1, ..., 0)$,...,$e_n = (0, 0, ..., 0, 1)$ formează o bază a lui K^n numită *baza canonică*. Verificarea se face uşor folosind egalitatea $(a_1, ..., a_n) = a_1e_1 + \cdots + a_ne_n$, pentru $a_1, ..., a_n \in K$. De asemenea, $\{1, X, X^2, ...\}$ este o K-bază a lui $K[X]$.

Teorema 139 *Dacă $e_1, e_2, ..., e_n$ este o bază a spaţiului vectorial V, atunci orice element $x \in V$ se scrie în mod unic sub forma*

$$x = x_1e_1 + x_2e_2 + ... + x_ne_n \text{ cu } x_i \in K$$

($x_1, x_2, ..., x_n$ se numesc coordonatele lui x în baza $e_1, e_2, ..., e_n$).

Demonstraţie. Scrierea din enunţ există pentru că $e_1, e_2, ..., e_n$ îl generează pe V. Dacă x se mai scrie şi sub forma $x = y_1e_1 + y_2e_2 + ... + y_ne_n$ cu $y_i \in K$, atunci, scăzând cele două exprimări ale lui x, obţinem $0 = (x_1 - y_1)e_1 + (x_2 - y_2)e_2 + ... + (x_n - y_n)e_n$, deci $x_1 = y_1$, $x_2 = y_2$,...,$x_n = y_n$, deoarece vectorii $e_1, e_2, ..., e_n$ sunt liniar independenţi. •

De exemplu, în baza canonică a lui K^n, coordonatele vectorului $(a_1, a_2, ..., a_n)$ sunt chiar $a_1, a_2, ..., a_n$; coordonatele aceluieaşi vector în baza $(1, 0, 0, ..., 0)$, $(1, 1, 0, ..., 0)$, ..., $(1, 1, 1, ..., 1)$ sunt $a_1 - a_2$, $a_2 - a_3$, ..., $a_{n-1} - a_n$, a_n.

Teorema 140 *Orice spaţiu vectorial ${}_KV$ finit generat admite o bază finită şi orice două baze au acelaşi număr de elemente. Cardinalul comun al tuturor bazelor se numeşte* dimensiunea lui V *şi se notează cu dim*(V).

Demonstraţie. Fie G un sistem finit de generatori al lui V şi $S \subseteq G$ o submulţime liniar independentă (eventual $S = \emptyset$). Fie B o mulţime liniar independentă maximală cu proprietatea $S \subseteq B \subseteq G$. Atunci $< B >= V$, deoarece dacă $y \in G\setminus < B >$, atunci $B \cup \{y\}$ este liniar independentă, contradicţie. Deci B bază.

Arătăm acum că orice două baze au acelaşi număr de elemente. Fie B o bază cu m elemente şi C o altă bază cu n elemente. Cum B este mulţime liniar independentă şi C sistem de generatori, din teorema schimbului rezultă că $m \leq n$. Inversând rolurile lui B şi C rezultă că $n \leq m$, deci $m = n$. •

Folosind baza canonică $e_1 = (1, ..., 0)$, $e_2 = (0, 1, ..., 0)$,...,$e_n = (0, 0, ..., 0, 1)$ vedem că spaţiul vectorial standard K^n are dimensiunea n. Din demonstraţia precedentă şi din teorema schimbului, rezultă

Corolarul 141 *Fie ${}_KV$ un spaţiu vectorial n-dimensional. Atunci din orice sistem de generatori se poate extrage o bază şi orice mulţime liniar independentă se poate extinde la o bază. În particular, orice mulţime cu n elemente care este liniar independentă sau sistem de generatori este bază.*

Teorema 140 este adevărată şi pentru spaţii care nu sunt finit generate (vezi [5, teorema V.4.3]). Din acest motiv vom numi spaţiile finit generate spaţii *finit dimensionale*, iar pe cele care nu sunt finit generate spaţii *infinit dimensionale*. De exemplu, ${}_KK^n$ este n-dimensional, iar ${}_KK[X]$ este infinit dimensional.

Teorema 142 *Fie ${}_KV$ un spaţiu vectorial finit generat şi W un subspaţiu al lui V. Atunci W este finit generat şi $dim(W) \leq dim(V)$. În plus, $W = V$ dacă şi numai dacă $dim(W) = dim(V)$.*

Demonstraţie. Fie $n = dim(V)$. Din teorema schimbului, orice submulţime liniar independentă a lui W are cel mult n elemente. Din teorema 137 rezultă că W este finit generat şi $dim(W) \leq dim(V)$. Dacă $dim(W) = dim(V)$, atunci orice bază a lui W este şi o bază a lui V, cf. corolarului 141. •

Teorema 143 *Fie V un K-spaţiu vectorial n-dimensional şi fie $E = \{e_1,..., e_n\}$, $F = \{f_1, ..., f_n\}$ baze ale lui V. Exprimăm fiecare vector f_j în baza E,*

$$f_j = \sum_{i=1}^{n} a_{ij} e_i, \quad j = 1, ..., n.$$

Atunci matricea $A = (a_{ij})_{1\leq i,j\leq n} \in M_n(K)$*, numită* matricea de trecere de la baza E la baza F*, este matrice inversabilă cu inversa matricea de trecere de la* F *la* E*. În plus, dacă vectorul* $x \in V$ *are în baza* E *coordonatele* $x_1, x_2, ..., x_n$ *şi în baza* F *coordonatele* $y_1, y_2, ..., y_n$*, atunci*

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = A \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}.$$

Demonstraţie. Fie $B = (b_{ij})_{1\leq i,j\leq n}$ matricea de trecere de la F la E. Pentru $k = 1, ..., n$ avem

$$e_k = \sum_{j=1}^{n} b_{jk} f_j = \sum_{j=1}^{n} b_{jk} \sum_{i=1}^{n} a_{ij} e_i = \sum_{i=1}^{n} (\sum_{j=1}^{n} a_{ij} b_{jk}) e_i.$$

Rezultă că $\sum_{j=1}^{n} a_{ij} b_{jk} = \delta_{ik}$ pentru $1 \leq i, k \leq n$. Deci $BA = I_n$. În plus,

$$x = \sum_{j=1}^{n} y_j f_j = \sum_{j=1}^{n} y_j \sum_{i=1}^{n} a_{ij} e_i = \sum_{i=1}^{n} (\sum_{j=1}^{n} a_{ij} y_j) e_i. \quad \bullet$$

Teorema 144 *Fie* V *şi* W *două spaţii vectoriale. Presupunem că* $e_1, e_2, ..., e_n$ *este o bază a lui* V *şi* $f_1, f_2, ..., f_n \in W$*. Atunci există şi este unică o aplicaţie liniară* $\alpha : V \to W$ *cu proprietatea* $\alpha(e_i) = f_i$*,* $i = 1, ..., n$*. În plus,* $f_1, f_2, ..., f_n$ *este bază a lui* W *dacă şi numai dacă* α *este izomorfism.*

Demonstraţie. Fie $\alpha : V \to W$ o aplicaţie liniară cu proprietatea $\alpha(e_i) = f_i$, $i = 1, ..., n$. Dacă $a_1, ..., a_n \in K$, atunci $\alpha(\sum_{i=1}^{n} a_i e_i) = \sum_{i=1}^{n} a_i \alpha(e_i) = \sum_{i=1}^{n} a_i f_i$, de unde rezultă unicitatea lui α. Fie acum aplicaţia $\alpha : V \to W$ dată prin $\alpha(\sum_{i=1}^{n} a_i e_i) = \sum_{i=1}^{n} a_i f_i$. E uşor de văzut că α este aplicaţie liniară şi $\alpha(e_i) = f_i$, $i = 1, ..., n$.

E clar că dacă α este izomorfism, atunci $f_1, f_2, ..., f_n$ este bază a lui W. Reciproc, presupunem că $f_1, f_2, ..., f_n$ este bază a lui W. Conform primei părţi, există şi este unică o aplicaţie liniară $\beta : W \to V$ cu proprietatea $\alpha(f_i) = e_i$, $i = 1, ..., n$. Atunci $\beta\alpha$ este un endomorfism al lui V cu proprietatea $\beta\alpha(e_i) = e_i$, $i = 1, ..., n$. Din prima parte rezultă că $\beta\alpha = I$. $\bullet$

Corolarul 145 *Un spaţiu vectorial n-dimensional este izomorf cu spaţiul standard K^n. În particular, două spaţii vectoriale finit dimensionale sunt izomorfe dacă şi numai dacă au aceeaşi dimensiune.*

Corolarul 146 *Fie K un corp finit de caracteristică p. Atunci K are p^n elemente.*

Demonstraţie. K se poate organiza ca spaţiu vectorial peste corpul $\mathbf{Z}_p$ definind înmulţirea cu scalari prin $\widehat{a}x = ax$ pentru $a \in \mathbf{Z}$. Fie n dimensiunea lui K peste $\mathbf{Z}_p$. Atunci $K \simeq \mathbf{Z}_p^n$, deci K are p^n elemente. •

Fie $f : V \to W$ un morfism de K-spaţii vectoriale. Dimensiunea $dim(Im(f))$ a imaginii lui f se numeşte *rangul* lui f şi se notează $rang(f)$. De asemenea, dimensiunea $dim(ker(f))$ a nucleului lui f se numeşte *defectul* lui f şi se notează $defect(f)$; deci morfismele injective sunt cele de defect nul.

De exemplu, dacă V este un spaţiu vectorial n-dimensional, atunci morfismul trivial are rangul 0 şi defectul n, iar morfismul identic are rangul n şi defectul 0.

Teorema 147 (Teorema rang-defect.) *Fie $f : V \to W$ un morfism de K-spaţii vectoriale finit dimensionale. Atunci $dim(V) = rang(u) + defect(u)$.*

Demonstraţie. Fie $E = \{e_1, ..., e_k, e_{k+1}, .., e_n\}$ unde $e_1, ..., e_k$ este o bază a lui $ker(u)$ iar $u(e_{k+1}), .., u(e_n)$ este o bază a lui $Im(u)$. Deci $dim_K(ker(u)) = k$ şi $dim_K(Im(u)) = n - k$. E suficient să arătăm că E este o bază a lui V. Fie $\sum_{i=1}^n a_i e_i = 0$ cu $a_i \in K$. Cum $e_1, ..., e_k$ şi $u(e_{k+1}), .., u(e_n)$ sunt mulţimi liniar independente, avem $\sum_{i=k+1}^n a_i u(e_i) = 0$, deci $a_{k+1} = \cdots = a_n = 0$, apoi $\sum_{i=1}^k a_i e_i = 0$, deci $a_1 = \cdots = a_k = 0$.

Fie $x \in V$. Putem scrie $u(x) = \sum_{i=k+1}^n b_i u(e_i)$ cu $b_{k+1}, ..., b_n \in K$. Deci $u(x) - \sum_{i=k+1}^n a_i e_i \in ker(u)$, deci putem scrie $x - \sum_{i=k+1}^n b_i e_i = \sum_{i=1}^k b_i e_i$, $b_1, ..., b_k \in K$. Deci $x = \sum_{i=1}^n b_i e_i$. •

Teorema 148 *Fie V şi W două spaţii vectoriale finit generat şi W un subspaţiu al lui V. Atunci $dim(V \times W) = dim(V) + dim(W)$.*

Demonstraţie. Fie $\{e_1, ..., e_m\}$ o bază a lui V şi $\{f_1, ..., f_n\}$ o bază a lui W. Se arată că $B = \{(e_1, 0), ..., (e_m, 0), (0, f_1), ..., (0, f_n)\}$ o bază a lui $V \times W$.

Întra-devăr, fie $(x,y) \in V \times W$. Există $a_1,...,a_m,b_1,...,b_n \in K$ astfel încât $x = \sum_{i=1}^m a_i e_i$ şi $y = \sum_{j=1}^n b_j f_j$. Rezultă că $(x,y) = \sum_{i=1}^m a_i(e_i,0) + \sum_{j=1}^n b_j(0,f_j)$. Deci B este sistem de generatori. Fie $a_1,...,a_m,b_1,...,b_n \in K$ astfel încât $\sum_{i=1}^m a_i(e_i,0) + \sum_{j=1}^n b_j(0,f_j) = (0,0)$. Rezultă că $(\sum_{i=1}^m a_i e_i, \sum_{j=1}^n b_j f_j) = (0,0)$. Deci $a_1,...,a_m,b_1,...,b_n$ sunt toţi nuli.

O demonstraţie mai scurtă se obţine aplicând teorema rang-defect proiecţiei $p_V : V \times W \to V$, $p_V(x,y) = x$, deoarece $ker(p_V) = 0 \times W$ este izomorf cu W. •

Teorema precedentă se extinde uşor la cazul produselor directe finite: dacă ${}_KV_1$,..., ${}_KV_n$ sunt spaţii vectoriale, atunci $dim(V_1 \times \cdots \times V_n) = dim(V_1) + \cdots + dim(V_n)$.

Teorema 149 (Teorema lui Grassmann.) *Fie Y un spaţiu vectorial şi V, W subspaţii finit dimensionale ale lui Y. Atunci $dim(V+W) = dim(V) + dim(W) - dim(V \cap W)$.*

Demonstraţie. Morfismul surjectiv $\pi : V \times W \to V + W$, $\pi(x,y) = x - y$ are nucleul $T = \{(x,x) |\ x \in V \cap W\}$. Avem izomorfismul $x \mapsto (x,x) : V \cap W \to T$, deci $defect(\pi) = dim(V \cap W)$. Cun π e surjectiv, $rang(\pi) = dim(V+W)$. Din teorema 148, $dim(V \times W) = dim(V) + dim(W)$. Se aplică teorema rang-defect. •

8.2 Sisteme de ecuaţii liniare

Fie K un corp (comutativ) şi $m, n \geq 1$. Considerăm sistemul de ecuaţii liniare

$$\sum_{j=1}^{n} a_{ij} x_j = b_i, \qquad i = 1,...,m$$

unde $a_{ij}, b_i \in K$. Scris matriceal, sistemul este $Ax = b$, unde A este matricea de tip (m,n) cu elementele a_{ij} numită matricea sistemului, $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ este vectorul necunoscutelor şi $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ este vectorul termenilor liberi. O soluţie a sistemului este un vector coloană $c = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ cu elemente din K astfel încât $Ac = b$. Sistemul se numeşte *incompatibil* dacă nu admite nici o soluţie, *compatibil determinat* dacă admite o soluţie unică şi *compatibil nedeterminat* dacă admite cel puţin două soluţii. Două sisteme se zic *echivalente* dacă au aceleaşi soluţii.

Se vede uşor că următoarele transformări nu afectează mulţimea soluţiilor unui sistem, deci produc sisteme echivalente cu cel dat.

a. Adunarea la o ecuaţie a altei ecuaţii înmulţite cu un element din K.

b. Permutarea a două ecuaţii.

c. Înmulţirea unei ecuaţii cu un element nenul din K.

Fie $B = (A\ b)$ matricea extinsă a sistemului, adică matricea sistemului la care am adăugat vectorul coloană al termenilor liberi. Transformările a, b, c de mai sus produc asupra matricei B următoarele transformări numite *transformări elementare pe linii*.

1. Adunarea la o linie a altei linii înmulţite cu un element din K.
2. Permutarea a două linii.
3. Înmulţirea unei linii cu un element nenul din K.

Observăm că fiecare din cele trei transformări posedă o transformare inversă. Spunem că două matrice A, B de acelaşi tip sunt *echivalente pe linii* dacă A se obţine din B printr-o succesiune de transformări elementare pe linii. E clar că "echivalenţa pe linii" este o relaţie de echivalenţă pe mulţimea matricelor de acelaşi tip. Prin calcul direct putem proba următorul rezultat.

Teorema 150 *Fie C o matrice de tip (p, q) cu elemente din K. Dacă f este una din tranformările elementare $1 - 3$ şi $f(C)$ este matricea obţinută din C prin efectuarea transformării f, atunci $f(C) = f(I_p)C$, unde I_p este matricea unitate.*

Apar astfel următoarele matrice numite *matrice elementare*.

1. $T_{ij}(a)$ = matricea unitate în care la linia j s-a adunat linia i înmulţită cu elementul $a \in K$.
2. P_{ij} = matricea unitate cu liniile i şi j permutate.
3. $D_i(u)$ = matricea unitate cu linia i înmulţită cu elementul $u \in K^*$.

Vedem că

$$T_{ij}(a)T_{ij}(-a) = I_p, \quad P_{ij}^2 = I_p, \quad D_i(u)D_i(u^{-1}) = I_p.$$

deci matricele elementare sunt inversabile.

Numim *matrice eşalon (pe linii)* o matrice de forma

$$\begin{pmatrix} 0 & \cdots & 0 & 1 & * & \cdots & * & 0 & * & \cdots & * & 0 & * & \cdots & * \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & * & \cdots & * & 0 & * & \cdots & * \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & * & \cdots & * \\ . & \cdots & . & . & . & \cdots & . & . & . & \cdots & . & . & . & \cdots & . \end{pmatrix}.$$

Mai precis o matrice eşalon este o matrice ce verifică următoarele condiţii.

1. Primul element nenul din fiecare linie, numit *pivot*, este egal cu 1.
2. Pivotul de pe linia $i+1$ este la dreapta pivotului de pe linia i.
3. Pivotul este singurul element nenul de pe coloana sa.
4. Eventualele linii nule apar la sfârşit.

Teorema 151 *O matrice eşalon inversabilă este egală cu matricea unitate.*

Demonstraţie. O matricea eşalon este superior triunghiulară. Dacă este şi inversabilă, atunci pivoţii apar pe diagonala principală, deci este matricea unitate. •

Teorema 152 *Orice matrice A cu elemente din K este echivalentă pe linii cu o matrice eşalon unică numită* forma eşalon *a lui A.*

Demonstraţie. Dacă $A = 0$, atunci A este matrice eşalon. Presupunem că $A \neq 0$. Procedăm astfel. Găsim prima coloană cu elemente nenule, să zicem coloana j. Prin permutări de linii, aducem un element nenul b al ei pe prima linie şi apoi, împărţind prima linie la b, facem $b = 1$, obţinând astfel un pivot în poziţia $(1, j)$. Prin transformări de tip 1, anulăm elementele aflate dedesubt pe coloana pivotului. Apoi, se aplică acelaşi algoritm submatricei obţinute din A eliminând linia 1 şi primele j coloane. La sfârşit, prin transformări de tip 1, anulăm elementele aflate deasupra pe coloana fiecărui pivot.

Demonstraţia unicităţii, deşi în principiu simplă, este destul de laborioasă. De aceea o omitem. •

Corolarul 153 *Dacă A este o matrice, atunci există matricele elementare E_1, ..., E_k astfel încât $E_k \cdots E_1 A$ este matrice eşalon.*

Corolarul 154 *O matrice pătratică este inversabilă dacă şi numai dacă ea este produs de matrice elementare.*

Demonstraţie. Fie A o matrice pătratică inversabilă de ordin n. Cf. corolarului precedent, există matricele elementare E_1, ..., E_k astfel încât $C = E_k \cdots E_1 A$ este matrice eşalon. Conform teoremei 151, $C = I_n$, deci $A = E_1^{-1} \cdots E_k^{-1}$. Reciproca este evidentă. •

Cu notaţiile precedente, $A^{-1} = E_k \cdots E_1$, deci A^{-1} se poate obţine făcând asupra lui I_n secvenţa de transformări elementare ce duce pe A în I_n. Deci, eşalonând matricea $(A\ I_n)$ se obţine matricea $(I_n\ A^{-1})$. Obţinem astfel un algoritm de calcul al inversei unei matrice prin transformări elementare.

Din teorema 152 şi comentariile anterioare referitoare la sistemele de ecuaţii liniare rezultă

Teorema 155 *Orice sistem de ecuaţii liniare este echivalent cu un sistem având matricea extinsă o matrice eşalon.*

Presupunem că sistemul de ecuaţii liniare

$$\sum_{j=1}^{n} a_{ij} x_j = b_i, \quad i = 1, ..., m$$

are matricea extinsă B matrice eşalon. Observăm că dacă apare un pivot în ultima coloană a lui B, atunci sistemul are o ecuaţie de forma $0 = 1$, deci este incompatibil. În continuare presupunem că B nu are pivoţi pe ultima coloană. Fie p_1,...,p_k coloanele ce au pivoţi. Numim necunoscutele x_{p_1},...,x_{p_k} *necunoscute principale*, celelalte necunoscute x_{s_1},...,x_{s_l} fiind numite *necunoscute secundare*. Trecând necunoscutele secundare în membrul drept şi neglijând ecuaţiile de forma $0 = 0$, sistemul devine

$$x_{p_i} = b_i - \sum_{j=1}^{l} a_{is_j} x_{s_j}, \quad i = 1, ..., k.$$

Deci sistemul este compatibil, necunoscutele secundare, dacă există, putând lua valori arbitrare. Rezultă următoarea teoremă.

Teorema 156 *Fie un sistem de ecuaţii liniare cu matricea extinsă B matrice eşalon. Sistemul este compatibil dacă şi numai dacă B nu are pivoţi pe ultima coloană. Dacă este compatibil, sistemul este compatibil determinat dacă şi numai dacă nu există necunoscute secundare, adică matricea sistemului are câte un pivot pe fiecare coloană.*

Metoda de rezolvare a unui sistem de ecuaţii liniare prin eşalonarea matricei extinse poartă numele de *metoda eliminării a lui Gauss*.

8.3 Rangul unei matrice

Fie K un corp şi $A \in M_{mn}(K)$. Prin definiţie, *rangul lui* A este numărul, notat $rang(A)$, egal cu ordinul maxim al unui minor nenul al lui A. Matricea nulă are rangul zero.

Deci $rang(A) = r$ înseamnă că A are un r-minor nenul şi toţi minorii de ordin $\geq r + 1$ sunt nuli. Din regula lui Laplace, vedem că $rang(A) = r$ dacă şi numai dacă A are un r-minor nenul şi toţi minorii de ordin $r + 1$ sunt nuli. Din definiţia rangului şi din faptul că A şi ${}^tA$ au aceeaşi minori, rezultă că

$$0 \leq rang(A) \leq min(m, n) \text{ şi } rang(A) = rang({}^tA).$$

Dacă $A \in M_n(K)$, atunci $rang(A) = n$ dacă şi numai dacă $|A| \neq 0$.

Teorema 157 *Fie* $A \in M_{mn}(K)$ *şi* $A \in M_{np}(K)$. *Atunci* $rang(AB) \leq min(rang(A),\ rang(B))$.

Demonstraţie. Din formula Binet-Cauchy (teorema 133), rezultă că un r-minor al lui AB este combinaţie liniară de r-minori ai lui A resp. B. •

Corolarul 158 *Fie* $A \in M_{mn}(K)$, $U \in GL_m(K)$ *şi* $V \in GL_n(K)$. *Atunci*

$$rang(UA) = rang(AV) = rang(A).$$

În particular, două matrice echivalente pe linii au acelaşi rang.

Demonstraţie. Din teorema precedentă,

$$rang(UA) \leq rang(A) \text{ şi } rang(A) = rang(U^{-1}UA) \leq rang(UA)$$

deci $rang(UA) = rang(A)$. Cealaltă egalitate se probează analog. •

Teorema 159 (Kronecker). *Fie $A \in M_{mn}(K)$. Atunci $rang(A)$ este egal cu dimensiunea peste K a subspaţiului generat de liniile lui A şi de asemenea egal cu dimensiunea peste K a subspaţiului generat de coloanele lui A.*

Demonstraţie. Fie $l(A)$ respectiv $c(A)$ dimensiunea subspaţiului generat de liniile respectiv coloanele lui A. Arătăm că $rang(A) = l(A)$. Se vede uşor că transformările elementare nu afectează $l(A)$. Conform corolarului 158, putem presupune că A este matrice eşalon. Fie p numărul de pivoţi ai lui A. E uşor de văzut că primele p linii sunt liniar independente iar celelalte sunt nule. Deci $l(A) = p$. Totodată A are un p-minor egal cu 1 (cel având pivoţii pe diagonala principală), deci $rang(A) = p$. În final, $rang(A) = rang({}^tA) = l({}^tA) = c(A)$. •

Din demonstraţie rezultă că $rangul(A)$ este egal cu numărul de pivoţi ai formei eşalon a lui A.

Corolarul 160 *Fie $A = (a_{ij}) \in M_{mn}(K)$. Presupunem că A are un r-minor nenul M astfel încât toţi $(r+1)$-minorii obţinuţi din M prin bordare cu elemente din A sunt nuli. Atunci $rang(A) = r$.*

Demonstraţie. Fără a micşora generalitatea, putem presupune că M constă din primele r linii şi r coloane ale lui A. Notăm liniile lui A cu A_1,...,A_m. Cum M este un r-minor nenul, $rang(A) \geq r$ şi liniile A_1,...,A_r sunt liniar independente.

Presupunem că $rang(A) \geq r + 1$. Din teorema precedentă, putem presupune că liniile A_1,...,A_{r+1} sunt liniar independente. Pentru $j = 1, ..., n$, considerăm $(r+1)$-minorul $M_j = \begin{vmatrix} a_{11} & \cdots & a_{1r} & a_{1j} \\ . & \cdots & . & . \\ a_{r1} & \cdots & a_{rr} & a_{rj} \\ a_{r+11} & \cdots & a_{r+1r} & a_{r+1j} \end{vmatrix}$. M_j este nul, deoarece pentru $j = 1, ..., r$, M_j are două coloane egale, iar pentru $j = r+1, ..., n$ se aplică ipoteza. Complemenţii algebrici d_1,...,d_r,$d_{r+1} = M$ ai elementelor de pe coloana $r+1$ nu depind de j. Dezvoltând M_j pe coloana $r+1$, obţinem $0 = d_1a_{1j} + \cdots + d_ra_{rj} + Ma_{r+1j}$ pentru $j = 1, ..., n$. Deci $d_1A_1 + \cdots + d_rA_r + MA_{r+1} = 0$, cu $M \neq 0$. Rezultă că liniile A_1,...,A_{r+1} sunt liniar dependente, contradicţie. •

Teorema 161 (Kronecker-Capelli). *Un sistem de ecuaţii liniare este compatibil dacă şi numai dacă rangul matricei sistemului este egal cu rangul matricei extinse.*

Demonstraţie. Fie A matricea sistemului şi B matricea extinsă. Conform teoremei 155 şi corolarului 158, putem presupune că B (deci şi A) este matrice eşalon. Condiţia din enunţ este echivalentă cu faptul B nu are pivoţi în ultima coloană. Se aplică teorema 156.

Altă demonstraţie. Fie c_1,...,c_n coloanele lui A, b vectorul termenilor liberi şi $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. Sistemul $Ax = b$ se scrie sub forma $x_1c_1 + \cdots + x_nc_n = b$. Deci sistemul $Ax = b$ este compatibil dacă şi numai dacă b este combinaţie liniară de c_1,...,c_n dacă şi numai dacă $rang(A) = dim < c_1, ..., c_n >= dim < c_1, ..., c_n, b >= rang(B)$. •

8.4 Exerciţii

190. Fie A o mulţime finită şi $\mathcal{P}(A)$ mulţimea părţilor lui A. $\mathcal{P}(A)$ este grup faţă de operaţia de diferenţă simetrică Δ. Arătaţi că acest grup o structură de $\mathbf{Z}_2$-spaţiu vectorial şi găsiţi o bază a sa.

191. Fie K un corp, V un grup abelian şi $End(V)$ mulţimea endomorfismelor lui V. Arătaţi că $End(V)$ este inel faţa de operaţiile de adunare şi compunere, şi că V împreună cu operaţia externă $K \times V \to V$, $(a, x) \mapsto ax$, este un spaţiu vectorial dacă şi numai dacă aplicaţia $f : K \to End(V)$, dată prin $f(a)(x) = ax$, pentru $a \in K$ şi $x \in V$, este un morfism de inele.

192. Arătaţi că grupul aditiv $\mathbf{Z}$ nu poate fi organizat ca spaţiu vectorial (peste nici un corp).

193. Care din submulţimile următoare sunt subspaţii ale $\mathbf{Q}$-spaţiului vectorial $\mathbf{Q}[X]$, (a) $\{f;\ f(a) = f(-a)\ \forall\ a \in \mathbf{Q}\}$,

(b) $\{f;\ f$ unitar, i.e. are coeficientul dominant $= 1\}$,

(c) $\{f;\ f$ neunitar$\}$,

(d) $\{f;\ f$ de grad impar$\}$,

(e) $\{f;\ f$ de grad $\leq 10\}$,

(f) $\{f;\ f(0) = f(1)\}$?

194. Fie subspaţiile $U =< (2, 3, 1), (1, 2, 0) >$ şi $W =< (1, 1, 1), (0, -1, -1) >$ ale lui ${}_{\mathbf{R}}\mathbf{R}^3$. Calculaţi $U + W$ şi $U \cap W$.

195. Fie V $\mathbf{R}$-spaţiul vectorial $M_3(\mathbf{R})$ şi fie S (resp. A) mulţimea matricelor simetrice (resp. antisimetrice). Arătaţi că S şi A sunt subspaţii şi determinaţi dimensiunea lor. Este V suma directă a lui S cu A ?

196. Fie V $\mathbf{R}$-spaţiul vectorial al şirurilor de numere reale $(x_n)_{n\geq 0}$ care verifică relaţia de recurenţă $x_n = x_{n-1} - x_{n-2}$, pentru $n \geq 2$. Arătaţi că şirurile $(sin(n\pi/3))_{n\geq 0}$, $(cos(n\pi/3))_{n\geq 0}$ constituie o bază a lui V.

197. Fie $f = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n \in \mathbf{Q}[X]$ un polinom ireductibil şi $y \in \mathbf{C}$ o rădăcină alui f. Arătaţi că mulţimea $1, y, ..., y^{n-1}$ este o bază a $\mathbf{Q}$-subspaţiului vectorial generat de toate puterile lui y.

198. Fie W subspaţiul lui ${}_{\mathbf{Q}}\mathbf{R}$ generat de $\{cos(20°n);\ n \geq 0\}$. Găsiţi o bază a lui W. (Indicaţie. $cos(20°)$ este rădăcina polinomului ireductibil $8X^3 - 6X - 1$).

199. Arătaţi că orice spaţiu vectorial V admite o bază.

200. Fie V $\mathbf{R}$-spaţiul vectorial al polinoamelor de grad ≤ 4 cu coeficienţi reali. Calculaţi matricele de trecere între bazele $E = \{1, X, X^2, X^3, X^4\}$ şi $F = \{1, X-1, (X-1)^2, (X-1)^3, (X-1)^4\}$.

201. Cu notaţiile din exerciţiul anterior, fie $D : V \to V$ operatorul de derivare. Arătaţi că D este aplicaţie liniară şi calculaţi matricele lui D în bazele E, F şi $G = \{1, X/1!, X^2/2!, X^3/3!, X^4/4!\}$.

202. Cu notaţiile din exerciţiul anterior, găsiţi baze în $Im(D)$ şi $ker(D)$.

Fie $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}|\ a, b, c, d \in \mathbf{Q}\}$.

203. Arătaţi că $\mathbf{Q}(\sqrt{2}, \sqrt{3}) \leq\ {}_{\mathbf{Q}}\mathbf{R}$ şi că $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ este o bază a sa.

204. Arătaţi că $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ este un subcorp al lui $\mathbf{R}$.

205. Fie Q-spaţiul vectorial ${}_{\mathbf{Q}}V = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. Arătaţi că $T : V \to V$, $T(x) = (\sqrt{2} + \sqrt{3})x$, este un endomorfism al lui V şi determinaţi matricea sa în baza $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$.

206. Cu notaţiile din exerciţiul anterior, arătaţi că 1, $\sqrt{2}+\sqrt{3}$, $(\sqrt{2}+\sqrt{3})^2$, $(\sqrt{2}+\sqrt{3})^3$ este o bază a lui V şi determinaţi matricea lui T în aceasta bază.

207. Fie V $\mathbf{R}$-spaţiul vectorial al matricelor 2×2 cu intrări reale şi fie $A \in V$ fixată. Arătaţi că aplicaţia $T : V \to V$, $T(Y) = AY + YA$ este liniară. Determinaţi matricea lui T în baza canonică a lui V.

208. Arătaţi că vectorii $(2, 2, 3)$, $(1, -1, 0)$, $(-1, 2, 1)$ constituie o bază F a lui $\mathbf{R}^3$ peste $\mathbf{R}$. Calculaţi matricele de trecere între F şi baza canonică, şi coordonatele lui $(1, 1, 1)$ în baza F.

209. Calculaţi inversa matricei $A = \begin{pmatrix} 1+a & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1+a & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1+a & \cdots & 1 & 1 \\ . & . & . & \cdots & . & . \\ 1 & 1 & 1 & \cdots & 1 & 1+a \end{pmatrix}$ prin eşalonare.

210.. Calculaţi inversa matricei $B = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 0 & 1 & \cdots & 1 & 1 \\ . & . & . & \cdots & . & . \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$ prin eşalonare.

211. Listaţi matricele eşalon 2×4 cu elemente din $\mathbf{Z}_2$.

212. Eşalonaţi matricea

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

şi găsiţi baze în subspaţiile generate de liniile resp. coloanele matricei.

213. Rezolvaţi sistemul de ecuaţii liniare $\begin{cases} x - 2y + z + t = 1 \\ x - 2y + z - t = -1 \\ x - 2y + z + 5t = 5 \end{cases}$ prin metoda eliminării a lui Gauss.

214. Rezolvaţi sistemul de ecuaţii liniare $\begin{cases} x + y - 3z = -1 \\ 2x + y - 2z = 1 \\ x + y + z = 3 \\ x + 2y - 3z = 1. \end{cases}$

215. Calculaţi inversa matricei următoare prin eşalonare $\begin{pmatrix} 2 & 1 & 0 & 0 \\ 3 & 2 & 0 & 0 \\ 1 & 1 & 3 & 4 \\ 2 & -1 & 2 & 3 \end{pmatrix}$.

216. Calculaţi rangul matricei $\begin{pmatrix} a & b & c \\ b & c & a \\ c & a & b \end{pmatrix}$.

217. Fie $A \in M_{m,n}(K)$ o matrice de rang p. Arătaţi că A poate fi adusă prin transformări elementare pe linii şi pe coloane la forma $\begin{pmatrix} I_p & 0 \\ 0 & 0 \end{pmatrix}$.

218. Fie $A, B \in M_n(K)$. Arătaţi că $rang(AB) \geq rang(A) + rang(B) - n$.

Capitolul 9

Forma canonică Jordan

În acest capitol se prezintă teoria formei canonice Jordan. Trecând prin conceptele de matrice caracteristică, forma diagonal-canonică, factori invarianţi, divizori elementari, se arată că orice matrice pătratică cu elemente dintr-un corp comutativ este asemenea cu o matrice Jordan.

Pe întreg parcursul acestui capitol, prin corp vom înţelege corp comutativ.

9.1 Matricea unui endomorfism

Fie K un corp. Fie V un K-spaţiu vectorial finit dimensional şi fie u, v endomorfisme ale lui V. Fie $E = \{e_1, ..., e_n\}$ o bază a lui V. Exprimând vectorii $u(e_1)$,...,$u(e_n)$ în baza E

$$u(e_j) = \sum_{i=1}^{n} a_{ij}e_i, \qquad j = 1, ..., n \quad \text{cu} \quad a_{ij} \in K$$

obţinem matricea $M_E(u) := (a_{ij})_{1\leq i,j\leq n} \in M_n(K)$ numită *matricea lui u în baza E*. Fie vectorul $x \in V$ şi fie x_1,...,x_n (resp. y_1,...,y_n) coordonatele lui x (resp. $u(x)$) în baza E. Atunci

$$u(x) = u(\sum_{j=1}^{n} x_je_j) = \sum_{j=1}^{n} x_ju(e_j) = \sum_{j=1}^{n} x_j \sum_{i=1}^{n} a_{ij}e_i = \sum_{i=1}^{n}(\sum_{j=1}^{n} a_{ij}x_j)e_i.$$

Deci coordonatele lui $u(x)$ în baza E se pot obţine înmulţind matricea lui u cu coordonatele lui x, adică

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = M_E(u) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

De exemplu, fie σ simetria plană faţă de dreapta $y = x\, tg\, t$. Atunci matricea lui S în baza canonică este $\begin{pmatrix} cos\ 2t & sin\ 2t \\ sin\ 2t & -cos\ 2t \end{pmatrix}$, iar matricea lui σ în baza $(cos\ t, sin\ t)$, $(-sin\ t, cos\ t)$ este $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Teorema 162 *Cu notaţiile de mai sus avem:*
(*a*) $M_E(u + v) = M_E(u) + M_E(v)$,
(*b*) $M_E(vu) = M_E(v)M_E(u)$,
(*c*) $M_E(du) = dM_E(u)$ *pentru orice* $d \in K$.

Demonstraţie. Vom proba (*b*), celelalte afirmaţii arătându-se analog. Fie $M_E(u) = (a_{ij})$ şi $M_E(v) = (b_{ij})$. Pentru $k = 1, ..., n$ avem

$$(vu)(e_k) = v(\sum_{j=1}^{n} a_{jk}e_j) = \sum_{j=1}^{n} a_{jk}v(e_j) = \sum_{j=1}^{n} a_{jk} \sum_{i=1}^{n} b_{ij}e_i = \sum_{i=1}^{n}(\sum_{j=1}^{n} b_{ij}a_{jk})e_i.$$

Aşadar $M_E(vu) = M_E(v)M_E(u)$. •

Fie V un K-spaţiu vectorial finit dimensional Pe mulţimea $End(V)$ a endomorfismelor lui V definim o operaţie de adunare prin $(u+v)(x) = u(x)+v(x)$ şi o operaţie de înmulţire cu scalari prin $(au)(x) = au(x)$ pentru orice $u, v \in End(V)$, $a \in K$ şi $x \in V$. Se arată uşor că faţă de adunare şi compunere $End(V)$ este un inel, iar faţă de adunare şi înmulţire cu scalari, $End(V)$ este un spaţiu vectorial.

Teorema 163 *Fie V un K-spaţiu vectorial finit dimensional şi $E = \{e_1, ..., e_n\}$ o bază a lui V. Aplicaţia $M_E : End(V) \to M_n(K)$, $u \mapsto M_E(u)$, este un izomorfism de inele şi spaţii vectoriale.*

Demonstraţie. Din teorema precedentă rezultă că M_E este un morfism de inele şi spaţii vectoriale. Asociem fiecărei matrice $A = (a_{ij}) \in M_n(K)$ endomorfismul u_A al lui V definit pe baza E prin

$$u_A(e_j) = \sum_{i=1}^{n} a_{ij}e_i, \qquad j = 1, ..., n.$$

Obţinem aplicaţia $\alpha : M_n(K) \to End(V)$, $\alpha(A) = u_A$. Se arată uşor că aplicaţiile M_E şi α sunt inverse una celeilalte. •

În particular, u este izomorfism dacă şi numai dacă $M_E(u)$ este matrice inversabilă.

Teorema 164 *Fie V un K-spaţiu vectorial finit dimensional, u un endomorfism al lui V, E, F baze ale lui V şi C matricea de trecere de la E la F. Atunci $M_F(u) = C^{-1}M_E(u)C$.*

Demonstraţie. Fie $E = \{e_1, ..., e_n\}$, $F = \{f_1, ..., f_n\}$, $M_E(u) = (a_{ij})$, $M_F(u) = (b_{ij})$ şi $C = (c_{ij})$. Avem

$$u(f_k) = \sum_{j=1}^{n} b_{jk}f_j = \sum_{j=1}^{n} b_{jk} \sum_{i=1}^{n} c_{ij}e_i = \sum_{i=1}^{n}(\sum_{j=1}^{n} c_{ij}b_{jk})e_i.$$

Pe de altă parte

$$u(f_k) = u(\sum_{j=1}^{n} c_{jk}e_j) = \sum_{j=1}^{n} c_{jk}u(e_j) = \sum_{j=1}^{n} c_{jk} \sum_{i=1}^{n} a_{ij}e_i = \sum_{i=1}^{n}(\sum_{j=1}^{n} a_{ij}c_{jk})e_i.$$

Rezultă că $\sum_{j=1}^{n} c_{ij}b_{jk} = \sum_{j=1}^{n} a_{ij}c_{jk}$ pentru $1 \leq i, k \leq n$, deci $CM_F(u) = M_E(u)C$. •

Spunem că două matrice $A, B \in M_n(K)$ sunt *asemenea*, şi notăm $A \approx B$, dacă există o matrice inversabilă $U \in M_n(K)$ astfel încât $A = U^{-1}BU$. Relaţia de asemănare este o relaţie de echivalenţă pe $M_n(K)$. Într-adevăr, fie $A, B, C \in M_n(K)$ şi $U, V \in GL_n(K)$. Atunci $A = I^{-1}AI$, $A = U^{-1}BU$ implică $B = UAU^{-1}$, iar dacă $A = U^{-1}BU$ şi $B = V^{-1}CV$, atunci rezultă că $A = (VU)^{-1}C(VU)$.

Teorema 165 *Fie V un K-spaţiu vectorial finit dimensional, u un endomorfism al lui V şi E o bază a lui V. Atunci $\{M_F(u) \mid F$ bază a lui $V\}$ este exact mulţimea matricelor asemenea cu $M_E(u)$.*

Demonstraţie. Încluziunea $\subseteq$ rezultă din teorema precedentă. Reciproc, fie $B, C \in M_n(K)$, C inversabilă astfel încât $B = C^{-1}M_E(u)C$. Fie F baza $f_1,...,f_n$ definită prin $f_j = \sum_{i=1}^n c_{ij}e_i$, $j = 1,...,n$, unde $C = (c_{ij})$ şi $E = \{e_1, ..., e_n\}$. Din teorema precedentă, rezultă că $M_F(u) = B$. •

9.2 Forma diagonal-canonică

Impreună cu inelul matricelor polinomiale $M_n(K[X])$ putem considera inelul polinoamelor matriceale $M_n(K)[X]$. Elementele lui $M_n(K)[X]$ sunt polinoame $f = B_mX^m + \cdots + B_1X + B_0$ cu coeficienţii $B_i \in M_n(K)$, înmulţirea monoamelor făcându-se după regula $(AX^i)(BX^j) = ABX^{i+j}$.

Teorema 166 *Între inelele $M_n(K)[X]$ şi $M_n(K[X])$ există un izomorfism natural.*

Demonstraţie. Elementele lui $M_n(K)[X]$ au forma $\sum_{k=0}^p A_kX^k$ cu $A_k = (a_{ijk})_{1\le i,j\le n} \in M_n(K)$. Se arată uşor că aplicaţia

$$\varphi : M_n(K)[X] \to M_n(K[X]), \quad \varphi(\sum_{k=0}^{p} A_kX^k) = (\sum_{i=0}^{p} a_{ijk}X^k)_{1\le i,j\le n}$$

este un izomorfism de inele. •

În continuare vom identifica inelele $M_n(K)[X]$ şi $M_n(K[X])$ prin intermediul izomorfismului precedent. De exemplu, vom identifica polinomul matriceal $\begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix} X^2 + \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix} X + \begin{pmatrix} 3 & 3 \\ 0 & -3 \end{pmatrix}$ cu matricea polinomială $\begin{pmatrix} X^2+2X+3 & -X^2+3 \\ X & X^2+X-3 \end{pmatrix}$. Matricele din $M_n(K)$ vor fi numite matrice constante.

Fie $A \in M_n(K)$. Matricea $XI-A$ se numeşte *matricea caracteristică* a lui A iar $P_A = |XI-A|$ se numeşte *polinom caracteristic* al lui A. Rădăcinile lui

P_A se numesc *valorile proprii* ale lui A. De exemplu, matricea $\begin{pmatrix} 5 & 4 & 2 \\ 4 & 5 & 2 \\ 2 & 2 & 2 \end{pmatrix}$ are matricea caracteristică $\begin{pmatrix} X-5 & -4 & -2 \\ -4 & X-5 & -2 \\ -2 & -2 & X-2 \end{pmatrix}$, polinomul caracteristic $X^3 - 12X^2 + 21X - 10 = (X-1)^2(X-10)$ şi valorile proprii 1 şi 10.

Fie $f = B_m X^m + \cdots + B_1 X + B_0 \in M_n(K)[X]$ şi $A \in M_n(K)$. Matricea $f_d(A) := B_m A^m + \cdots + B_1 A + B_0$ se numeşte *valoarea la dreapta a lui f în A*, iar matricea $f_s(A) := A^m B_m + \cdots + AB_1 + B_0$ se numeşte *valoarea la stânga a lui f în A*.

Teorema 167 (Teorema lui Bézout generalizată.) *Fie $f \in M_n(K)[X]$ şi $A \in M_n(K)$. Atunci există $q \in M_n(K)[X]$, astfel încât $f = q(IX-A)+f_d(A)$ şi aceasta este unica scriere a lui f sub forma $f = q'(IX-A) + r$ cu $q' \in M_n(K)[X]$ şi $r \in M_n(K)$.*

Analog, există $q \in M_n(K)[X]$, astfel încât $f = (IX-A)q + f_s(A)$ şi aceasta este unica scriere a lui f sub forma $f = (IX-A)q' + r$ cu $q' \in M_n(K)[X]$ şi $r \in M_n(K)$.

Demonstraţie. Fie $f = B_m X^m + \cdots + B_1 X + B_0$. Atunci $f_d(A) = B_m A^m + \cdots + B_1 A + B_0$. Deci

$$f - f_d(A) = B_m(IX^m - A^m) + \cdots + B_1(IX - A)$$

şi e suficient să observăm că

$$IX^k - A^k = (IX - A)(IX^{k-1} + \cdots + A^{k-1}).$$

Unicitatea. Fie $f = q(IX-A) + r = q'(IX-A) + r'$ cu $q, q' \in M_n(K)[X]$, $r, r' \in M_n(K)$. Atunci $(q-q')(IX-A) + r - r' = 0$, deci $q = q'$ şi $r = r'$, altfel polinomul $(q-q')(IX-A)$ are gradul ≥ 1. •

Fie $A \in M_n(K)$ o matrice şi $f = b_p X^p + b_{p-1} X^{p-1} + \cdots + b_1 X + b_0 \in K[X]$ un polinom. Matricea $f(A) = b_p A^p + b_{p-1} A^{p-1} + \cdots + b_1 A + b_0 I \in M_n(K)$, se numeşte *valoarea lui f în A*. Se vede că $(If)(A)_d = (If)(A)_s = f(A)$. De exemplu, valoarea lui $f = X^2 + X + 1$ în $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ este matricea nulă.

Teorema 168 (Hamilton-Cayley.) *Fie $A \in M_n(K)$. Atunci $P_A(A) = 0$.*

Demonstraţie. Fie $(IX - A)^*$ matricea adjunctă a matricei caracteristice $IX - A$. Din teorema 127 rezultă că $IP_A = I|IX - A| = (IX - A)^*(IX - A)$. Din teorema lui Bézout generalizată deducem că $0 = (IP_A)_d(A) = P_A(A)$. •

Spunem că două matrice polinomiale $A, B \in M_n(K[X])$ sunt *echivalente*, şi notăm $A \sim B$, dacă există două matrice inversabile $U, V \in M_n(K[X])$ astfel încât $A = UBV$.

Aceasta este o relaţie de echivalenţă pe $M_n(K[X])$. Într-adevăr, fie $A, B, C \in M_n(K[X])$ şi $U, V, U', V' \in GL_n(K[X])$. Atunci $A = IAI$, $A = UBV$ implică $B = U^{-1}AV^{-1}$, iar dacă $A = UBV$ şi $B = U'CV'$, atunci rezultă că $A = UU'CV'V$.

Teorema 169 *Fie $A, B \in M_n(K)$. Atunci $A \approx B$ dacă şi numai dacă $IX - A \sim IX - B$.*

Demonstraţie. Implicaţia directă este imediată: dacă $A = SBS^{-1}$ cu $S \in GL_n(K)$, atunci $IX - A = S(IX - B)S^{-1}$.

Reciproc, presupunem că $IX - A \sim IX - B$. Deci există $f, g \in M_n(K)[X]$ inversabile astfel încât

$$IX - B = f(IX - A)g.$$

Rezultă că $f(IX - A) = (IX - B)g^{-1}$ şi $(IX - A)g = f^{-1}(IX - B)$. Din teorema lui Bézout generalizată, există $f_1, g_1 \in M_n(K)[X]$ şi $F, G \in M_n(K)$ astfel încât

$$f = (IX - B)f_1 + F \quad \text{şi} \quad g = g_1(IX - B) + G.$$

Notăm $\alpha = IX - A$ şi $\beta = IX - B$. Combinând relaţiile anterioare găsim

$$\beta = f\alpha g = f\alpha(g_1\beta + G) = f\alpha g_1\beta + f\alpha G = f\alpha g_1\beta + (\beta f_1 + F)\alpha G.$$

Deci

$$\beta - F\alpha G = f\alpha g_1\beta + \beta f_1\alpha G = f\alpha g_1\beta + \beta f_1\alpha(g - g_1\beta) =$$
$$= f\alpha g_1\beta + \beta f_1\alpha g - \beta f_1\alpha g_1\beta = \beta g^{-1}g_1\beta + \beta f_1 f^{-1}\beta - \beta f_1\alpha g_1\beta.$$

Aşadar

$$IX - B - F(IX - A)G = (IX - B)(g^{-1}g_1 + f_1f^{-1} - f_1(IX - A)g_1)(IX - B).$$

Privite ca polinoame, membrul stâng are gradul ≤ 1, deci membrul drept este nul, altfel are gradul ≥ 2. Rezultă că $FG = I$ şi $B = FAG$. •

Dacă $d_1, ..., d_n \in K[X]$, notăm cu $diag(d_1, ..., d_n)$ matricea cu elementele $d_1, ..., d_n$ pe diagonala principală şi zero în rest.

Teorema 170 *Fie* $C \in M_n(K[X])$ *cu* $|C| \neq 0$. *Atunci există şi sunt unice polinoamele unitare* $d_1, ..., d_n \in K[X]$ *astfel încât* $d_1 \mid d_2 \mid ... \mid d_n$ *şi* $C \sim diag(d_1, ..., d_n)$. (Matricea $diag(d_1, ..., d_n)$ se numeşte forma *diagonal-canonică* a lui C.)

Demonstraţie. Existenţa. Vom arăta mai mult şi anume că C se poate aduce prin transformări elementare pe linii şi coloane la forma $diag(d_1, ..., d_n)$ cu $d_1, ..., d_n$ polinoame unitare astfel încât $d_1 \mid d_2 \mid ... \mid d_n$.

Este suficient să arătăm că prin transformări elementare pe linii şi coloane, putem aduce matricea C la forma următoare.

$(*)$ Elementul c_{11} este polinom unitar, toate celelalte elemente de pe prima linie şi prima coloană ale lui C sunt nule şi c_{11} divide toate elementele matricei.

Într-adevăr, fie C' matricea obţinută din C tăind prima linie şi prima coloană. Cum $|C| \neq 0$, rezultă că $|C'| \neq 0$. Raţionând prin inducţie după n, putem presupune că C' se poate aduce prin transformări elementare pe liniile şi coloanele $2, ..., n$ la forma $C \sim diag(d_2, ..., d_n)$ cu $d_2, ..., d_n$ polinoame unitare astfel încât $d_2 \mid d_2 \mid ... \mid d_n$. Cum c_{11} divide toate elementele matricei C', rezultă că c_{11} divide d_2, şi afirmaţia este probată.

La forma $(*)$ se ajunge prin intemediul algoritmului următor.

do
    Prin permutări de linii şi coloane, se aduce în poziţia $(1, 1)$ un polinom nenul de grad minim;
    while c_{11} nu divide toate elementele de pe prima linie *do*
    begin
        Se alege un element c_{1j} nedivizibil cu c_{11};
        Se face împărţirea cu rest $c_{1j} = qc_{11} + r$;
        Se scade coloana 1 înmulţită cu q din coloana j;
        Se permută coloanele 1 şi j;
    end
    for j=2 *to* n *do*
        Se scade coloana 1 înmulţită cu c_{1j}/c_{11} din coloana j;

while c_{11} nu divide toate elementele de pe prima coloană *do*
begin
Se alege un element c_{i1} nedivizibil cu c_{11};
Se face împărţirea cu rest $c_{i1} = qc_{11} + r$;
Se scade linia 1 înmulţită cu q din linia i;
Se permută liniile 1 şi i;
end
for i=2 *to* n *do*
Se scade linia 1 înmulţită cu c_{i1}/c_{11} din linia i;
if c_{11} nu divide un element $c_{\alpha\beta}$ *then* se adună linia α la linia 1;
until c_{11} divide toate elementele matricei;
se împarte prima linie la coeficientul dominant al lui c_{11}.

Se observă că la fiecare parcurgerea unei bucle *while* c_{11} se înlocuieşte cu restul unei împărţiri la c_{11}, deci gradul lui c_{11} scade strict. După parcurgerea celor două bucle *while*, cu excepţia lui c_{11}, toate celelalte elemente de pe prima linie şi prima coloană ale lui C sunt nule. Rezultă că după fiecare parcurgerea a buclei *do-until*, gradul lui c_{11} scade strict (exceptând eventual prima parcurgere). Deci algoritmul se termină după un număr finit de paşi. E clar că la terminarea algoritmului matricea C verifică condiţiile $(*)$. •

Pregătim demonstraţia unicităţii. Fie $C \in M_n(K[X])$ cu $|C| \neq 0$. Pentru fiecare $1 \leq p \leq n$, fie $\Delta_p(C)$ polinomul unitar egal cu *cmmdc* al p-minorilor lui C. Astfel $\Delta_1(C)$ este *cmmdc* al elementelor lui C, iar $\Delta_n(C) = a^{-1}|C|$, unde a este coeficientul dominant al lui $|C|$. Cum orice $(p+1)$-minor e combinaţie liniară de p-minori, rezultă că

$$\Delta_1(C) \mid \Delta_2(C) \mid ... \mid \Delta_n(C).$$

În particular, dacă C este matricea caracteristică a unei matrice $A \in M_n(K)$, $\Delta_n(C) = P_A$. De exemplu, pentru matricea XI_n, polinoamele Δ sunt $X, X^2, ..., X^n$.

Lema 171 *Fie $C, D \in M_n(K[X])$ cu $|C| \neq 0$ şi $|D| \neq 0$. Dacă $C \sim D$, atunci $\Delta_p(C) = \Delta_p(D)$, pentru $p = 1, ..., n$.*

Demonstraţie. Cum $C \sim D$, există $U, V \in GL_n(K[X])$ cu $C = UDV$. Fie $1 \leq p \leq n$. Din formula Binet-Cauchy vedem că $\Delta_p(D)$ divide orice p-minor al lui UD, deci $\Delta_p(D) \mid \Delta_p(UD)$. La fel se vede că $\Delta_p(UD) \mid \Delta_p(UDV)$. Deci $\Delta_p(D) \mid \Delta_p(C)$ şi, datorită simetriei, $\Delta_p(C) \mid \Delta_p(D)$. Cum $\Delta_p(C)$, $\Delta_p(D)$ sunt polinoame unitare, ele sunt egale. •

Demonstraţia teoremei 170 (unicitatea). Fie $C \in M_n(K[X])$ şi $d_1, ..., d_n \in K[X]$ polinoame unitare astfel încât $d_1 \mid d_2 \mid ... \mid d_n$ şi $C \sim diag(d_1, ..., d_n)$. Notăm $D = diag(d_1, ..., d_n)$. Conform lemei precedente, $\Delta_p(C) = \Delta_p(D)$ pentru $p = 1, 2, ..., n$. Fie $1 \leq p \leq n$. p-minorii nenuli ai lui D sunt produsele de p elemente d_i. Cum $d_1 \mid d_2 \mid ... \mid d_n$, rezultă $\Delta_p(D) = d_1 d_2 \cdots d_p$. Cf. lemei precedente, $\Delta_p(C) = \Delta_p(D) = d_1 d_2 \cdots d_p$ pentru $p = 1, 2, ..., n$. Atunci $d_1 = \Delta_1(C)$, $d_2 = \Delta_2(C)/\Delta_1(C)$,..., $d_n = \Delta_n(C)/\Delta_{n-1}(C)$. Aşadar polinoamele d_i sunt unic determinate. •

Observaţia 172 *Din demonstraţia precedentă rezultă că, pentru o matrice $C \in M_n(K[X])$ cu $|C| \neq 0$, elementele formei diagonal-canonice $diag(d_1, d_2, ..., d_n)$ se pot calcula prin $d_1 = \Delta_1(C)$, $d_2 = \Delta_2(C)/\Delta_1(C)$,..., $d_n = \Delta_n(C)/\Delta_{n-1}(C)$.*

Din teorema 170 şi observaţia 172 rezultă

Teorema 173 *Fie $C, D \in M_n(K[X])$ cu $|C| \neq 0$ şi $|D| \neq 0$. Atunci $C \sim D \Leftrightarrow C, D$ au aceeaşi formă diagonal-canonică $\Leftrightarrow \Delta_p(C) = \Delta_p(D)$, pentru $p = 1, ..., n$.*

9.3 Forma Jordan a unei matrice

Fie $A \in M_n(K)$ şi presupunem că matricea caracteristică $XI_n - A$ a lui A are forma diagonal-canonică $diag(1, ..., 1, d_1, d_2, ..., d_r)$, unde $d_1, d_2, ..., d_r$ sunt polinoame unitare de grad ≥ 1. Polinoamele $d_1, d_2, ..., d_r$ poartă numele de *factorii invarianţi* ai matricei A. Aşadar, factorii invarianţi ai matricei $A \in M_n(K)$ sunt polinoamele de grad ≥ 1 ale formei diagonal-canonice a lui $XI - A$. Altfel spus, factorii invarianţi ai lui A sunt polinoamele neconstante de forma $\Delta_i(IX - A)/\Delta_{i-1}(IX - A)$, $i = 1, ..., n$, cf. observaţiei 172.

De exemplu, matricea nulă are factorii invarianţi $X, X, ..., X$, iar matricea $diag(1, 2, ..., n)$ are factorul invariant $(X - 1)(X - 2) \cdots (X - n)$.

Teorema 174 *Produsul factorilor invarianţi ai unei matrice $A \in M_n(K)$ este egal cu polinomul caracteristic al lui A.*

Demonstraţie. Deoarece $XI_n - A \sim diag(1, ..., 1, d_1, d_2, ..., d_r)$, există $U, V \in GL_n(K[X])$ astfel încât $XI_n - A = U\,diag(1, ..., 1, d_1, d_2, ..., d_r)V$. Deci

$$P_A = |XI_n - A| = |U||diag(1, ..., 1, d_1, d_2, ..., d_r)||V| = |U||V|d_1 \cdots d_r.$$

Cum P_A şi $d_1 \cdots d_r$ sunt polinoame unitare şi $|U|, |V| \in K^*$, rezultă că $|U||V| = 1$. •

Din teoremele 173 şi 169 rezultă

Teorema 175 *Două matrice $A, B \in M_n(K)$ sunt asemenea dacă şi numai dacă au aceeaşi factori invarianţi.*

Unui polinom unitar $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$, îi asociem matricea $C_f \in M_n(K)$

$$C_f = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & 0 & -a_2 \\ . & . & \cdots & . & . & . \\ 0 & 0 & \cdots & 1 & 0 & -a_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

numită *matricea companion a lui f* sau *companionul lui f*. De exemplu, $C_{X+3} = (-3)$ şi $C_{X^2-X+5} = \begin{pmatrix} 0 & -5 \\ 1 & 1 \end{pmatrix}$.

Teorema 176 *Polinomul caracteristic al companionului lui f este chiar f, adică $|XI_n - C_f| = f$. În particular, $f(C_f) = 0$.*

Demonstraţie. Păstrând notaţiile anterioare, avem

$$P_{C_f} = |XI - C_f| = \begin{vmatrix} X & 0 & \cdots & 0 & 0 & a_0 \\ -1 & X & \cdots & 0 & 0 & a_1 \\ 0 & -1 & \cdots & 0 & 0 & a_2 \\ . & . & \cdots & . & . & . \\ 0 & 0 & \cdots & -1 & X & a_{n-2} \\ 0 & 0 & \cdots & 0 & -1 & X + a_{n-1} \end{vmatrix}.$$

Dezvoltând după ultima coloană rezultă

$$P_{C_f} = a_0 + a_1X + \cdots a_{n-2}X^{n-2} + (X + a_{n-1})X^{n-1} = f.$$

Alternativ, dezvoltând după prima linie obţinem $P_{C_f} = X|XI - C_g| + a_0$, unde $g = X^{n-1} + a_{n-1}X^{n-2} + \cdots + a_2X + a_1$ şi se face inducţie după n. Egalitatea $f(C_f) = 0$ rezultă din teorema Hamilton-Cayley. •

Teorema 177 *Companionul matriceal C_f al unui polinom unitar $f \in K[X]$ are un singur factor invariant şi anume f. Altfel spus,*

$$XI - C_f \sim diag(1, ..., 1, f).$$

Demonstraţie. Fie

$$B = XI - C_f = \begin{pmatrix} X & 0 & \cdots & 0 & 0 & a_0 \\ -1 & X & \cdots & 0 & 0 & a_1 \\ 0 & -1 & \cdots & 0 & 0 & a_2 \\ . & . & \cdots & . & . & . \\ 0 & 0 & \cdots & -1 & X & a_{n-2} \\ 0 & 0 & \cdots & 0 & -1 & X + a_{n-1} \end{pmatrix}.$$

Din teorema precedentă, $\Delta_n(B) = P_{C_f} = f$. $(n-1)$-minorul lui B obţinut tăind prima linie şi ultima coloană are valoarea $(-1)^{n-1}$, deci $\Delta_{n-1}(B) = 1$. Pentru $1 \leq i \leq n-2$, $\Delta_i(B)$ divide $\Delta_{n-1}(B)$, deci $\Delta_i(B) = 1$. Se aplică observaţia 172. •

Fie matricele $C_i \in M_{p_i}(K[X])$, $i = 1, ..., t$. Matricea

$$C_1 \oplus C_2 \oplus \cdots \oplus C_t := diag(C_1, C_2, ..., C_t) = \begin{pmatrix} C_1 & & & \\ & C_2 & & \\ & & \ddots & \\ & & & C_t \end{pmatrix}$$

se numeşte *suma directă* a matricelor C_1,...,C_t. Afirmaţiile următoarei leme se probează uşor.

Lema 178 *Fie matricele $C_i, D_i \in M_{p_i}(K[X])$, $i = 1, ..., t$.*

(*a*) $(C_1 \oplus \cdots \oplus C_t) + (D_1 \oplus \cdots \oplus D_t) = (C_1 + D_1) \oplus \cdots \oplus (C_t + D_t)$.

(*b*) $(C_1 \oplus \cdots \oplus C_t)(D_1 \oplus \cdots \oplus D_t) = (C_1D_1) \oplus \cdots \oplus (C_tD_t)$.

(*c*) *Dacă $C_i \sim D_i$ pentru $i = 1, ..., t$, atunci $C_1 \oplus \cdots \oplus C_t \sim D_1 \oplus \cdots \oplus D_t$.*

(*d*) *Dacă C_i, D_i sunt matrice constante şi $C_i \approx D_i$ pentru $i = 1, ..., t$, atunci $C_1 \oplus \cdots \oplus C_t \approx D_1 \oplus \cdots \oplus D_t$.*

Teorema 179 *Dacă matricea $A \in M_n(K)$ are factorii invarianţi $d_1, ..., d_r$, atunci*
$$A \approx C_{d_1} \oplus \cdots \oplus C_{d_r}.$$

Demonstraţie. Cf. teoremei 177, avem

$$XI - (C_{d_1} \oplus \cdots \oplus C_{d_r}) = (XI - C_{d_1}) \oplus \cdots \oplus (XI - C_{d_r}) \sim$$

$$\sim diag(1, ..., 1, d_1) \oplus \cdots \oplus diag(1, ..., 1, d_r) \sim diag(1, ..., 1, d_1, ..., d_r).$$

Cum $d_1 \mid d_2 \mid \cdots \mid d_r$, deducem că $d_1, ..., d_r$ sunt factorii invarianţi ai matricei $C_{d_1} \oplus \cdots \oplus C_{d_r}$. Se aplică teorema 175. •

Fie $d_1, ..., d_r \in K[X]$ factorii invarianţi ai matricei $A \in M_n(K)$ şi fie π_1,...,$\pi_s \in K[X]$ divizorii lor ireductibili (unitari). Putem scrie

$$d_i = \pi_1^{k_{i1}} \pi_2^{k_{i2}} \cdots \pi_s^{k_{is}},\ i = 1, ..., r \ \text{ cu } 0 \le k_{1j} \le k_{2j} \le \cdots \le k_{rj},\ j = 1, ..., s.$$

Polinoamele
$$\{\pi_i^{k_{ij}} \mid k_{ij} \ge 1,\ i = 1, ..., r,\ j = 1, ..., s\}$$
se numesc *divizorii elementari* ai lui A. Deci divizorii elementari sunt puteri de polinoame ireductibile unitare din $K[X]$. Egalităţile anterioare permit recuperarea factoriilor invarianţi din divizorii elementari. Din teorema 174 rezultă

Teorema 180 *Produsul divizorilor elementari ai unei matrice $A \in M_n(K)$ este egal cu polinomul caracteristic al lui A.*

Din teorema 175 rezultă

Teorema 181 *Fie două matrice $A, B \in M_n(K)$. Afirmaţiile următoare sunt echivalente:*
(a) $A \approx B$,
(b) *A, B au aceeaşi factori invarianţi,*
(c) *A, B au aceeaşi divizori elementari.*

Teorema 182 *Fie $f, g \in K[X]$ două polinoame unitare neconstante prime între ele. Atunci $C_{fg} \approx C_f \oplus C_g$.*

Demonstraţie. Fie $n = p + q$, unde p este gradul lui f iar q este gradul lui g. Cf. teoremei 181, e suficient să arătăm că $C_f \oplus C_g$ are un singur factor invariant şi anume fg. Avem

$$XI-(C_f \oplus C_g) = (XI_p - C_f) \oplus (XI_q - C_g) \sim diag(1, ..., 1, f) \oplus diag(1, ..., 1, g) \sim$$

$$\sim diag(1, ..., 1, f, g) \sim diag(1, ..., 1, 1, fg).$$

Ultima echivalenţă rezultă din faptul că $(n-1)-$minorii nenuli ai matricei $diag(1, ..., 1, f, g)$ sunt egali cu f, g sau fg, deci $\Delta_{n-1}(diag(1, ..., 1, f, g)) = 1$.
•

Fie $\pi \in K[X]$ un polinom ireductibil unitar de grad s şi $k \geq 1$. Definim *celula Jordan* corespunzătoare lui π^k prin

$$J_k(\pi) = \begin{pmatrix} C_\pi & & & & \\ N & C_\pi & & & \\ & N & C_\pi & & \\ & & & \ddots & \\ & & & N & C_\pi \end{pmatrix} \in M_{sk}(K)$$

unde companionul C_π apare de k ori iar matricea $N \in M_s(K)$, care apare de $k-1$ ori, are forma $N = \begin{pmatrix} & 1 \\ & \end{pmatrix}$, elementele omise în $J_k(\pi)$ şi N fiind nule. O sumă directă de celule Jordan se numeşte *matrice Jordan*.

Pentru $k = 1$ avem $J_1(\pi) = C_\pi$. Fie $\lambda \in K$. Pentru celula Jordan $J_k(X-\lambda) = \begin{pmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & 1 & \lambda & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda \end{pmatrix}$ vom utiliza şi notaţia mai simplă $J_k(\lambda)$.

X^2+X+1 este ireductibil peste $\mathbf{R}$ şi $J_2(X^2+X+1) = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$.

Teorema 183 *Dacă $\pi \in K[X]$ un polinom ireductibil şi $k \geq 1$, atunci*

$$C_{\pi^k} \approx J_k(\pi).$$

Demonstraţie. Cf. teoremelor 175 şi 177, e suficient să vedem că $J_k(\pi)$ are un singur factor invariant şi anume π^k. Fie D matricea caracteristică a lui $J_k(\pi)$ şi fie $n = sk$, unde s este gradul lui π. $(n-1)$-minorul lui D obţinut tăind prima linie şi ultima coloană are valoarea ± 1. Rezultă că $\Delta_{n-1}(D) = 1$, deci $\Delta_i(D) = 1$ pentru $1 \leq i \leq n-1$. Pe de altă parte, cu regula lui Laplace, vedem că $\Delta_n(D) = \pi^k$. Deci $J_k(\pi)$ are un singur factor invariant şi anume π^k. •

Enunţăm teorema centrală a teoriei formei Jordan.

Teorema 184 (Forma Jordan a unei matrice). *Dacă matricea $A \in M_n(K)$ are divizorii elementari $\pi_1^{k_1}$,...,$\pi_s^{k_s}$, atunci*

$$A \approx J_{k_1}(\pi_1) \oplus \cdots \oplus J_{k_s}(\pi_s).$$

Mai puţin o permutare a celulelor, $J_{k_1}(\pi_1) \oplus \cdots \oplus J_{k_s}(\pi_s)$ este unica matrice Jordan asemenea cu A. Ea se numeşte forma Jordan a lui A.

Demonstraţie. Fie d unul dintre factorii invarianţi ai lui A şi $d = \rho_1^{l_1} \cdots \rho_t^{l_t}$ descompunerea lui d în produs de factori ireductibili. Cf. teoremei 182,

$$C_{\rho_1^{l_1} \cdots \rho_t^{l_t}} \approx C_{\rho_1^{l_1}} \oplus C_{\rho_2^{l_2} \cdots \rho_t^{l_t}} \approx \cdots \approx C_{\rho_1^{l_1}} \oplus \cdots \oplus C_{\rho_t^{l_t}}.$$

Folosind acest fapt şi teoremele 175,183, rezultă că

$$A \approx C_{d_1} \oplus \cdots \oplus C_{d_r} \approx C_{\pi_1^{k_1}} \oplus \cdots \oplus C_{\pi_s^{k_s}} \approx J_{k_1}(\pi_1) \oplus \cdots \oplus J_{k_s}(\pi_s).$$

Unicitatea formei Jordan rezultă din faptul că matricea Jordan $J_{k_1}(\pi_1) \oplus \cdots \oplus J_{k_s}(\pi_s)$ are divizorii elementari $\pi_1^{k_1}$,...,$\pi_s^{k_s}$. •

De exemplu, se poate arăta că matricea $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \in M_3(K)$, K corp de caracteristică $\neq 3$, are factorii invarianţi X, $X(X-3)$, deci divizorii elementari X, X, $X-3$. Rezultă că $A \approx J_1(X) \oplus J_1(X) \oplus J_1(X-3) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 3 \end{pmatrix}$. Aceeaşi matrice are peste un corp de caracteristică 3 divizorii elementari X, X^2, deci forma Jordan $J_1(X) \oplus J_2(X) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

Din teorema anterioară şi teorema 165 rezultă

Teorema 185 (Forma Jordan a unui endomorfism). *Pentru orice endomorfism u al unui K-spaţiu vectorial finit-dimensional, există o bază în care matricea lui u este matrice Jordan. Această matrice este unică până la o permutare a celulelor şi se numeşte* forma Jordan a lui u.

Recapitulăm conceptele ce conduc la forma Jordan: matrice constantă, asemănare de matrice constante, matrice caracteristică, echivalenţă de matrice polinomiale, formă diagonal-canonică a unei matrice polinomiale, factori invarianţi, divizori elementari, companion matriceal, celulă Jordan, matrice Jordan.

Corolarul 186 *Dacă o matrice $A \in M_n(K)$ are n valori proprii distincte în K, $\lambda_1, \lambda_2, ..., \lambda_n \in K$, atunci*

$$A \approx diag(\lambda_1, \lambda_2, ..., \lambda_n).$$

În particular, dacă un endomorfism u al unui K-spaţiu vectorial n-dimensional are n valori proprii distincte, atunci u este diagonalizabil.

Demonstraţie. Cum produsul divizorilor elementari ai lui A este $P_A = (X-\lambda_1)\cdots(X-\lambda_n)$, rezultă că aceştia sunt exact $X-\lambda_1$, $X-\lambda_2$, ..., $X-\lambda_n$. •

9.4 Polinomul minimal

Fie $A \in M_n(K)$ o matrice şi $f = b_pX^p + b_{p-1}X^{p-1} + \cdots + b_1X + b_0 \in K[X]$ un polinom. Matricea $f(A) = b_pA^p + b_{p-1}A^{p-1} + \cdots + b_1A + b_0I \in M_n(K)$, se numeşte *valoarea lui f în A*. De exemplu, valoarea lui $f = X^2 + X + 1$ în $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ este matricea nulă.

Fie $A \in M_n(K)$ o matrice fixată. Se verifică uşor că aplicaţia

$$\varphi_A : K[X] \to M_n(K), \quad \varphi_A(f) = f(A)$$

este un morfism de inele. Nucleul său $ker(\varphi_A)$ este un ideal nenul deoarece, potrivit teoremei Hamilton-Cayley, $P_A(A) = 0$, deci $P_A \in ker(\varphi_A)$. Unicul generator polinom unitar μ_A al idealului $ker(\varphi_A)$ se numeşte *polinomul minimal al lui A*. Reamintim că μ_A este polinomul unitar de grad minim în $ker(\varphi_A)$, cf. demonstraţiei teoremei 94.

Teorema 187 *Fie $A \in M_n(K)$ o matrice şi $g \in K[X]$ un polinom. Următoarele afirmaţii sunt echivalente.*

(a) $g = \mu_A$,

(b) g este unitar, $g(A) = 0$ şi g este de grad minim între polinoamele cu aceste proprietăţi,

(c) g este unitar, $g(A) = 0$ şi g divide toate polinomele $h \in K[X]$ cu proprietatea $h(A) = 0$.

Demonstraţie. Echivalenţa $(a) \Leftrightarrow (b)$ a fost justificată mai sus, iar implicaţiile $(a) \Rightarrow (c)$ şi $(c) \Rightarrow (b)$ sunt clare. •

Exemple 188 *(a) Dacă $a \in K$, atunci $\mu_A = X - a$ dacă şi numai dacă $A = aI$.*

(b) Fie $A = \begin{pmatrix} 0 & -2 \\ 1 & 3 \end{pmatrix}$ şi $f = X^2 - 3X + 2 = (X-1)(X-2)$. Deoarece $f(A) = 0$, μ_A poate fi f, $X - 1$ sau $X - 2$. Cum $A \neq I$, $2I$, rămâne că $\mu_A = f$.

Teorema 189 *Fie $f \in K[X]$ un polinom unitar. Atunci polinomul minimal al companionului lui f este chiar f, adică $\mu_{C_f} = f$.*

Demonstraţie. Fie $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ şi fie $e_1,...,e_n$ baza canonică a lui $M_{n,1}(K)$, adică coloanele matricei I_n. Vedem că $C_f e_i = e_{i+1}$ pentru $i = 1, ..., n-1$, deci $C_f^i e_i = e_{i+1}$. Dacă $g = c_{n-1}X^{n-1} + \cdots + c_1X + c_0 \in K[X]$ are proprietatea $g(C_f) = 0$, atunci

$$0 = g(C_f)e_1 = c_{n-1}e_n + \cdots + c_1e_2 + c_0e_1 = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix}$$

deci $g = 0$. Se aplică teoremele 176 şi 187. •

Teorema 190 *Fie $A \in M_n(K)$. Atunci polinomul minimal al lui A este ultimul factor invariant al lui A. Altfel spus,*

$$\mu_A = \frac{P_A}{\Delta_{n-1}(XI - A)}.$$

Demonstraţie. Fie $d_1 \mid \cdots \mid d_r$ factorii invarianţi ai lui A. Cf. teoremei 179, există $S \in GL_n(K)$ astfel încât

$$SAS^{-1} = C_{d_1} \oplus \cdots \oplus C_{d_r}.$$

Dacă $g \in K[X]$, atunci

$$Sg(A)S^{-1} = g(SAS^{-1}) = g(C_{d_1}) \oplus \cdots \oplus g(C_{d_r}).$$

Deci $g(A) = 0$ dacă şi numai dacă $g(C_{d_i}) = 0$, $i = 1, ..., r$. Din teorema precedentă, $\mu_{C_{d_i}} = d_i$. Ţinând seama că $d_1 \mid \cdots \mid d_r$, rezultă că $g(A) = 0$ dacă şi numai dacă $d_r \mid g$. Deci $\mu_A = d_r$. •

Teorema 191 (Teorema lui Frobenius.) *Fie $A \in M_n(K)$. Atunci P_A şi μ_A au aceeaşi factori ireductibili în $K[X]$.*

Demonstraţie. Fie $d_1 \mid \cdots \mid d_r$ factorii invarianţi ai lui A. Cum $P_A = d_1 \cdots d_r$ şi $d_1 \mid \cdots \mid d_r$, rezultă că P_A şi d_r au aceeaşi factori reductibili. Dar $d_r = \mu_A$, cf. teoremei precedente. •

O matrice $A \in M_n(K)$ se zice *diagonalizabilă* dacă A este asemenea cu o matrice diagonală.

Teorema 192 *O matrice $A \in M_n(K)$ este diagonalizabilă dacă şi numai dacă μ_A are toate rădăcinile în K şi acestea sunt distincte.*

Demonstraţie. Are loc şirul de echivalenţe. A este diagonalizabilă $\Leftrightarrow$ divizorii elementari ai lui A sunt de forma $X - a$ cu $a \in K$ $\Leftrightarrow$ fiecare factor invariant al lui A are toate rădăcinile în K şi acestea sunt distincte $\Leftrightarrow$ ultimul factor invariant (adică μ_A) are toate rădăcinile în K şi acestea sunt distincte. •

Fie $A \in M_n(K)$. Interpretăm pe A ca endomorfismul spaţiului vectorial $M_{n,1}(K) \simeq K^n$ dat prin $v \mapsto Av$. Putem atunci vorbi de defectul lui A = dimensiunea nucleului acestui endomorfism. Din teorema rang-defect, rang$(A) + defect(A) = n$.

Teorema 193 *Fie $A \in M_n(K)$ şi $\lambda \in K$. Afirmaţiile următoare sunt echivalente.*
(a) $P_A(\lambda) = 0$ *(adică λ este valoare proprie a lui A),*
(b) *matricea $A - \lambda I$ este neinversabilă,*
(c) $defect(A - \lambda I) \geq 1$,
(d) *Există $0 \neq v \in M_{n,1}(K)$ astfel încât $Av = \lambda v$.*

Demonstraţie. Avem şirul de echivalenţe. $0 = P_A(\lambda) = |\lambda I - A| \Leftrightarrow$ matricea $A - \lambda I$ este neinversabilă $\Leftrightarrow$ rang$(A - \lambda I) \leq n-1 \Leftrightarrow defect(A - \lambda I) \geq 1$ $\Leftrightarrow$ are loc (d). •

Un vector $0 \neq v \in M_{n,1}(K)$ astfel încât $Av = \lambda v$ se numeşte *vector propriu* al lui A corespunzător valorii proprii λ iar $ker(A - \lambda I) = \{v \in M_{n,1}(K) |\ Av = \lambda v\}$ se numeşte *spaţiul vectorilor proprii corespunzător valorii proprii* λ.

9.5 Cazul $K = \mathbf{C}$

În continuare, vom lucra numai în cazul $K = \mathbf{C}$. Deoarece peste $\mathbf{C}$ polinoamele ireductibile unitare sunt de forma $X - \lambda$, rezultă că toate celulele Jordan sunt de forma

$$J_k(\lambda) = \begin{pmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & 1 & \lambda & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda \end{pmatrix} \quad \text{cu } \lambda \in \mathbf{C} \text{ şi } k \geq 1.$$

Vom numi o astfel de matrice λ-*celulă Jordan de ordin* k. Forma Jordan a unei matrice $A \in M_n(\mathbf{C})$ se mai numeşte *forma canonică Jordan.*

Teorema 184 capătă forma următoare.

Teorema 194 (Forma canonică Jordan a unei matrice). *Orice matrice $A \in M_n(\mathbf{C})$ este asemenea cu o matrice de forma*

$$J = J_{k_1}(\lambda_1) \oplus J_{k_2}(\lambda_2) \oplus \cdots \oplus J_{k_s}(\lambda_s).$$

Matricea J este unic determinată până la o permutare a celulelor Jordan şi este numită forma canonică Jordan a lui A. $\lambda_1, ..., \lambda_s \in \mathbf{C}$ sunt valorile proprii ale lui A.

Demonstraţie. Se aplică teorema 184. În plus, rezultă că $P_A = (X - \lambda_1)^{k_1} \cdots (X - \lambda_s)^{k_s}$. Deci $\lambda_1, ..., \lambda_s$ sunt valorile proprii ale lui A. •

Aşadar forma canonică Jordan a unei matrice A este determinată de valorile proprii ale lui A şi, pentru fiecare valoare proprie λ, de numărul şi ordinul λ-celulelor.

Observaţia 195 În ipotezele şi cu notaţiile din teorema precedentă, dacă $f \in \mathbf{C}[X]$, atunci

$$f(A) \approx f(J_{k_1}(\lambda_1)) \oplus f(J_{k_2}(\lambda_2)) \oplus \cdots \oplus f(J_{k_s}(\lambda_s)).$$

Se poate aplica teorema următoare.

Teorema 196 *Fie $\lambda \in \mathbf{C}$, $f \in \mathbf{C}[X]$ şi $k \geq 1$. Atunci*

$$f(J_k(\lambda)) = \begin{pmatrix} f(\lambda) & & & & \\ \frac{f'(\lambda)}{1!} & f(\lambda) & & & \\ \frac{f''(\lambda)}{2!} & \frac{f'(\lambda)}{1!} & f(\lambda) & & \\ \cdots & & & & \\ \frac{f^{(k-1)}(\lambda)}{(k-1)!} & \cdots & \frac{f''(\lambda)}{2!} & \frac{f'(\lambda)}{1!} & f(\lambda) \end{pmatrix}$$

elementele de deasupra diagonalei principale fiind nule.

Demonstraţie. Ne putem reduce la cazul $f = X^m$. Vedem prin calcul că puterile succesive ale celulei Jordan $J_k(0) = \begin{pmatrix} 0 & & & & \\ 1 & 0 & & & \\ & 1 & 0 & & \\ & & \ddots & \ddots & \\ & & & 1 & 0 \end{pmatrix}$ sunt

$$J_k^2(0) = \begin{pmatrix} 0 & & & & \\ 0 & 0 & & & \\ 1 & 0 & 0 & & \\ & \ddots & \ddots & \ddots & \\ & & 1 & 0 & 0 \end{pmatrix}, \cdots, J_k^{k-1}(0) = \begin{pmatrix} & & & \\ & & & \\ & & & \\ & & & \\ 1 & & & \end{pmatrix}, J_k^k(0) = 0.$$

Aplicând formula binomului lui Newton pentru $J_k^m(\lambda) = (\lambda I + J_k(0))^m$, obţinem formula din enunţ, deoarece $(X^p)^{(m)}/m! = C_p^m X^{p-m}$. •

Fie a_0, a_1,...,$a_{p-1} \in \mathbf{C}$, $a_0 \neq 0$. Considerăm şirul definit prin relaţia de recurenţă $x_n = a_{p-1}x_{n-1} + a_{p-2}x_{n-2} + \cdots + a_0x_{n-p}$ cu x_0,...,x_{p-1} date. Avem relaţia matriceală $(x_{n-p+1}, ..., x_n) = (x_{n-p}, ..., x_{n-1})A$, unde A este companionul matriceal al polinomului $f = X^p - a_{p-1}X^{p-1} - \cdots - a_1X - a_0$ ($f = 0$ se numeşte *ecuaţia caracteristică* a relaţiei de recurenţă). Rezultă că

$$(x_{n-p+1}, ..., x_n) = (x_0, ..., x_{p-1})A^n. \tag{9.1}$$

Fie $f = (X - \lambda_1)^{k_1} \cdots (X - \lambda_s)^{k_s}$ cu $\lambda_1, ..., \lambda_s$ distincte. Rezultă că $A \approx J_{k_1}(\lambda_1) \oplus J_{k_2}(\lambda_2) \oplus \cdots \oplus J_{k_s}(\lambda_s)$, deci $A^n \approx J^n_{k_1}(\lambda_1) \oplus J^n_{k_2}(\lambda_2) \oplus \cdots \oplus J^n_{k_s}(\lambda_s)$. Din relaţia 9.1 şi teorema 196, rezultă că termenul general al şirului are forma

$$x_n = (b_{10} + b_{11}n + \cdots + b_{1k_1-1}n^{k_1-1})\lambda_1^n + \cdots + (b_{s0} + b_{s1}n + \cdots + b_{sk_s-1}n^{k_s-1})\lambda_s^n$$

cu coeficienţii $b_{ij} \in \mathbf{C}$.

De exemplu, termenul general al şirului definit prin relaţia de recurenţă $x_n = 2x_{n-1} + x_{n-2} - 2x_{n-3} - x_{n-4}$ are forma $x_n = (a + bn)(1/2 + \sqrt{5}/2)^n + (c + dn)(1/2 - \sqrt{5}/2)^n$.

Fie $A \in M_n(\mathbf{C})$ şi λ o valoare proprie a lui A. Multiplicitatea $m_a(\lambda)$ a lui λ ca rădăcină a lui P_A se numeşte *multiplicitatea algebrică* a lui λ. Numărul

$$m_g(\lambda) = \text{defect}(A - \lambda I)$$

adică dimensiunea subspaţiului vectorilor proprii corespunzător lui λ, se numeşte *multiplicitatea geometrică* a lui λ.

Dacă $A \approx B$, atunci $P_A = P_B$, deci A, B au aceleaşi valori proprii şi cu aceleaşi multiplicităţi algebrice.

Teorema 197 *Dacă $A \approx B$ şi λ este o valoare proprie a lui A, atunci multiplicitatea geometrică a lui λ în A este egală cu multiplicitatea geometrică a lui λ în B.*

Demonstraţie. Fie $S \in GL_n(K)$ astfel încât $B = SAS^{-1}$. Avem $defect(B-\lambda I) = defect(SAS^{-1} - \lambda I) = defect\ S(A - \lambda I)S^{-1} = defect(A - \lambda I)$. •

Dacă $A = J_k(\lambda)$, atunci $P_A = (X - \lambda)^k$. Deci $m_a(\lambda) = k$ şi $m_g(\lambda) = \text{defect}(A - \lambda I) = k - \text{rang}(J_k(0)) = 1$.

Teorema 198 *Fie $A \in M_n(\mathbf{C})$ şi λ o valoare proprie a lui A. Atunci multiplicitatea algebrică a lui λ în A este suma ordinelor λ-celulelor lui A, iar multiplicitatea geometrică a lui λ în A este numărul λ-celulelor lui A. În particular, $m_a(\lambda) \geq m_g(\lambda)$.*

Demonstraţie. Ultima afirmaţie rezultă din celelalte. Fie $J = J_{k_1}(\lambda_1) \oplus J_{k_2}(\lambda_2) \oplus \cdots \oplus J_{k_s}(\lambda_s)$ forma canonică Jordan a lui A. Cum $A \approx J$, λ are aceeaşi multiplicitate algebrică (resp. geometrică) în A şi J. Deci putem presupune că $A = J$. Avem $P_A = (X - \lambda_1)^{k_1} \cdots (X - \lambda_s)^{k_s}$, de unde rezultă prima afirmaţie. Apoi,

$$m_g(\lambda) = \text{defect}(A - \lambda I) =$$

$$= \text{defect}(J_{k_1}(\lambda_1 - \lambda) \oplus J_{k_2}(\lambda_2 - \lambda) \oplus \cdots \oplus J_{k_s}(\lambda_s - \lambda)) =$$

$$= \text{defect}(J_{k_1}(\lambda_1 - \lambda)) + \text{defect}(J_{k_2}(\lambda_2 - \lambda)) + \cdots + \text{defect}(J_{k_s}(\lambda_s - \lambda)).$$

În final folosim faptul că

$$\text{defect}(J_k(\alpha)) = \begin{cases} 0 & \text{dacă} \quad \alpha \neq 0 \\ 1 & \text{dacă} \quad \alpha = 0 \end{cases} \quad \bullet$$

Corolarul 199 *O matrice $A \in M_n(\mathbf{C})$ este diagonalizabilă dacă şi numai dacă toate valorile proprii ale lui A au multiplicitatea algebrică egală cu multiplicitatea geometrică.*

Demonstraţie. Folosim teorem precedentă. Afirmaţia rezultă din faptul că A este diagonalizabilă dacă şi numai dacă toate celulele Jordan ale sale au ordinul 1. $\bullet$

Lema 200 *Dacă $\lambda \in \mathbf{C}$ şi $k, p \geq 1$, atunci*

$$\textit{defect}(J_k^p(0)) = \textit{min}(k, p).$$

Demonstraţie. Pentru $p \geq k$, $J_k^p(0) = 0$, deci defect$(J_k^p(0)) = k$. Pentru $p \leq k - 1$, $J_k^p(0)$ are o diagonală formată din $k - p$ elemente egale cu 1 şi toate celelalte elemente nule. Deci defect$(J_k^p(0)) = p$. $\bullet$

Teorema următoare permite un calcul direct al formei canonice Jordan a unei matrice de numere complexe.

Teorema 201 *Fie $A \in M_n(\mathbf{C})$, λ o valoare proprie a lui A şi $p \geq 1$. Atunci numărul λ-celulelor Jordan ale lui A de ordin $\geq p$ este*

$$\mathit{defect}((A-\lambda I)^p) - \mathit{defect}((A-\lambda I)^{p-1}).$$

Demonstraţie. Fie $J = J_{k_1}(\lambda_1) \oplus J_{k_2}(\lambda_2) \oplus \cdots \oplus J_{k_s}(\lambda_s)$ forma canonică Jordan a lui A. Cum A, J sunt matrice asemenea, putem presupune că $A = J$. Atunci

$$\mathrm{defect}((A-\lambda I)^p) =$$

$$= \mathrm{defect}(J^p_{k_1}(\lambda_1-\lambda) \oplus J^p_{k_2}(\lambda_2-\lambda) \oplus \cdots \oplus J^p_{k_s}(\lambda_s-\lambda)) =$$

$$= \mathrm{defect}(J^p_{k_1}(\lambda_1-\lambda)) + \mathrm{defect}(J^p_{k_2}(\lambda_2-\lambda)) + \cdots + \mathrm{defect}(J^p_{k_s}(\lambda_s-\lambda)).$$

Folosind faptul că $\mathrm{defect}(J^p_k(\alpha)) = 0$ dacă $\alpha \neq 0$ şi lema anterioară, avem

$$\mathrm{defect}((A-\lambda I)^p) = \sum_{j=1}^{s} \sum_{\lambda_j=\lambda} \min(k_j, p).$$

Formula are loc şi dacă înlocuim p cu $p-1$. Rezultă că

$$\mathrm{defect}((A-\lambda I)^p) - \mathrm{defect}((A-\lambda I)^{p-1}) =$$

$$= \sum_{j=1}^{s} \sum_{\lambda_j=\lambda} (\min(k_j, p) - \min(k_j, p-1)) = \sum_{j=1}^{s} \sum_{\lambda_j=\lambda, k_j \geq p} 1. \bullet$$

Din teorema anterioară rezultă următorul algoritm de calcul direct al formei canonice Jordan a unei matrice de numere complexe A.

1. Se calculează valorile proprii ale lui A, adică rădăcinile lui P_A.
2. Pentru fiecare valoare proprie λ, se calculează numerele

$$f_p = \mathrm{defect}((A-\lambda I)^p) - \mathrm{defect}((A-\lambda I)^{p-1}), \quad 1 \leq p \leq m_a(\lambda) + 1.$$

Pentru $1 \leq p \leq m_a(\lambda)$, numărul λ-celulelor Jordan ale lui A de ordin p este $f_p - f_{p+1}$.

De exemplu, fie $A = \begin{pmatrix} 4 & 0 & 0 \\ 2 & 1 & 3 \\ 5 & 0 & 4 \end{pmatrix}$. Găsim $P_A = (X-4)^2(X-1)$. E clar că A are o singură 1-celulă Jordan şi aceea are ordinul 1. Avem $A - 4I = \begin{pmatrix} 0 & 0 & 0 \\ 2 & -3 & 3 \\ 5 & 0 & 0 \end{pmatrix}$ şi $(A-4I)^2 = \begin{pmatrix} 1 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Deci $f_1 = \text{defect}(A-4I) = 1$ şi $f_2 = \text{defect}(A-4I)^2 - \text{defect}(A-4I) = 2 - 1 = 1$. Deducem că A are o 4-celulă de ordinul doi. Deci forma canonică Jordan a lui A este $J_1(1) \oplus J_2(4) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 1 & 4 \end{pmatrix}$.

9.6 Aplicaţii ale formei canonice Jordan.

Fie $A \in M_n(\mathbf{C})$ o matrice cu forma canonică Jordan $J = J_{k_1}(\lambda_1) \oplus J_{k_2}(\lambda_2) \oplus \cdots \oplus J_{k_s}(\lambda_s)$. Ne interesează găsirea unei matrice inversabile U astfel încât $A = UJU^{-1}$ (U se numeşte *matrice de asemănare* între A şi J sau mai simplu *matrice de asemănare pentru* A). Pentru $B \in M_n(\mathbf{C})$ şi $u, v \in M_{n,1}(\mathbf{C})$, vom scrie $u \stackrel{B}{\to} v$, dacă $Bu = v$.

Fie $U \in M_n(\mathbf{C})$. Notăm coloanele lui U prin u_{11},...,u_{1k_1},...,u_{s1},...,u_{sk_s}. Atunci coloanele matricei AU sunt

$$Au_{11}, ..., Au_{1k_1}, ..., Au_{s1}, ..., Au_{sk_s}.$$

Pe de altă parte, coloanele matricei UJ sunt

$$\lambda_1 u_{11} + u_{12}, ..., \lambda_1 u_{1k_1-1} + u_{1k_1}, \lambda_1 u_{1k_1}, ..., \lambda_s u_{s1} + u_{s2}, ..., \lambda_s u_{sk_s}.$$

Deci egalitatea $AU = UJ$ este echivalentă cu setul de relaţii

$$\begin{gathered} u_{11} \stackrel{A-\lambda_1 I}{\to} u_{12} \stackrel{A-\lambda_1 I}{\to} \cdots \stackrel{A-\lambda_1 I}{\to} u_{1k_1} \stackrel{A-\lambda_1 I}{\to} 0 \\ \cdots \\ u_{s1} \stackrel{A-\lambda_s I}{\to} u_{s2} \stackrel{A-\lambda_s I}{\to} \cdots \stackrel{A-\lambda_s I}{\to} u_{sk_s} \stackrel{A-\lambda_s I}{\to} 0. \end{gathered} \tag{9.2}$$

Fie $Spec(A) = \{\lambda_1, ..., \lambda_s\}$, mulţimea valorilor proprii ale lui A. Fie $F = \{u_{1k_1}, u_{2k_2}, ..., u_{sk_s}\}$ şi pentru fiecare $\lambda \in Spec(A)$, fie $F_\lambda = \{u_{ik_i} \in F | \ \lambda_i = \lambda\}$.

Dăm, fără demonstraţie, următoarea teoremă.

Teorema 202 (Filippov.) *Matricea U este o matrice de asemănare între A şi J dacă şi numai dacă coloanele lui U verifică relaţiile* (9.2) *şi mulţimea F_λ este liniar independentă pentru orice $\lambda \in Spec(A)$.*

În particular, dacă valorile proprii ale lui A sunt distincte, atunci U este o matrice ale cărei coloane sunt vectori proprii ai lui A (câte unul pentru fiecare valoare proprie).

Exemple. (1). Fie matricea $A = \begin{pmatrix} 3 & -1 & -1 & -1 \\ 2 & -1 & 0 & -1 \\ 2 & -1 & -1 & 0 \\ 3 & -1 & -1 & -1 \end{pmatrix}$. Avem $P_A = X^4$ şi $defect(A) = 1$, deci $A \approx J_4(0)$. U este matrice de asemănare dacă şi numai dacă coloanele sale, u_1,..., u_4, verifică:

$$u_1 \xrightarrow{A} u_2 \xrightarrow{A} u_3 \xrightarrow{A} u_4 \xrightarrow{A} 0 \text{ şi } u_4 \neq 0.$$

Calculăm puterile lui A: $A^2 = \begin{pmatrix} 2 & 0 & -1 & -1 \\ 1 & 0 & -1 & 0 \\ 2 & 0 & -1 & -1 \\ 2 & 0 & -1 & -1 \end{pmatrix}$, $A^3 = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \end{pmatrix}$.

Putem lua $u_1 =^t (1, 0, 0, 0)$, adică U să fie matricea formată cu prima coloană din I, A, A^2, A^3: $U = \begin{pmatrix} 1 & 3 & 2 & 1 \\ 0 & 2 & 1 & 1 \\ 0 & 3 & 2 & 1 \\ 0 & 3 & 2 & 1 \end{pmatrix}$.

Putem proceda şi astfel. Rezolvând prin eliminare gaussiană sistemul cu matricea extinsă $\begin{pmatrix} 3 & -1 & -1 & -1 & a \\ 2 & -1 & 0 & -1 & b \\ 2 & -1 & -1 & 0 & c \\ 3 & -1 & -1 & -1 & d \end{pmatrix}$, găsim

$\begin{pmatrix} 1 & 0 & 0 & -1 & a-c \\ 0 & 1 & 0 & -1 & 2a-b-2c \\ 0 & 0 & 1 & -1 & b-c \\ 0 & 0 & 0 & 0 & d-a \end{pmatrix}$, de unde obţinem soluţia $\begin{pmatrix} a-c+\lambda \\ 2a-b-2c+\lambda \\ b-c+\lambda \\ \lambda \end{pmatrix}$

şi condiţia de compatibilitate $d = a$. În final, dând lui λ succesiv valorile $1, 0, 0, 0$ găsim $U = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & -1 & 1 \\ 2 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

(2). Fie matricea $A = \begin{pmatrix} 0 & -1 & 2 & 1 \\ -2 & 1 & 2 & 1 \\ -1 & -1 & 2 & 2 \\ 0 & -1 & 2 & 1 \end{pmatrix}$. Avem $P_A = (X-2)^2X^2$, $defect(A-2I) = 1$ şi $defect(A) = 1$, deci $A \approx J_2(2) \oplus J_2(0)$. U este matrice de asemănare (adică $A = U(J_2(2) \oplus J_2(0))U^{-1}$) dacă şi numai dacă coloanele sale, u_1,..., u_4, verifică:

$$u_1 \overset{A-2I}{\rightarrow} u_2 \overset{A-2I}{\rightarrow} 0,\ u_3 \overset{A}{\rightarrow} u_4 \overset{A}{\rightarrow} 0 \text{ şi } u_2, u_4 \neq 0.$$

$A - 2I = \begin{pmatrix} -2 & -1 & 2 & 1 \\ -2 & -1 & 2 & 1 \\ -1 & -1 & 0 & 2 \\ 0 & -1 & 2 & -1 \end{pmatrix}$. Subspaţiul 2-vectorilor proprii ai lui A este generat de vectorul ${}^t(1,1,1,1)$. Se vede că $(A-2I)^t(0,-1,0,0) =^t (1,1,1,1)$. Analog observăm că $A^t(1,1,0,1) = 0$ şi $A^t(1,1,1,0) =^t (1,1,0,1)$. Deci o matrice de asemănare este $U = \begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$.

(3). Fie matricea $A = \begin{pmatrix} 3 & -1 & 0 & -1 \\ 2 & 0 & 0 & -1 \\ 1 & -1 & 1 & 0 \\ 2 & -1 & 0 & 0 \end{pmatrix}$. Avem $P_A = (X-1)^4$. $A - I = \begin{pmatrix} 2 & -1 & 0 & -1 \\ 2 & -1 & 0 & -1 \\ 1 & -1 & 0 & 0 \\ 2 & -1 & 0 & -1 \end{pmatrix}$ şi $(A-I)^2 = 0$. Rezultă că $defect(A-I) = 2$ şi $defect(A-I)^2 = 4$, deci $A \approx J_2(1) \oplus J_2(1)$. U este matrice de asemănare (adică, $A = U(J_2(1) \oplus J_2(1))U^{-1}$) dacă şi numai dacă coloanele sale, u_1,..., u_4, verifică:

$$u_1 \overset{A-I}{\rightarrow} u_2 \overset{A-I}{\rightarrow} 0,\ u_3 \overset{A-I}{\rightarrow} u_4 \overset{A-I}{\rightarrow} 0 \text{ şi } u_2, u_4 \text{ liniar independente.}$$

Putem lua $U = \begin{pmatrix} 1 & 2 & 0 & -1 \\ 0 & 2 & 1 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 2 & 0 & -1 \end{pmatrix}$.

Fie $A \in M_n(\mathbf{C})$. Considerăm sistemul de ecuaţii diferenţiale cu coeficienţi constanţi $y' = Ay$. Prin definiţie, o soluţie a acestui sistem este o funcţie vectorială derivabilă $f : \mathbf{R} \to \mathbf{C}^n$, astfel încât $f'(t) = Af(t)$ pentru orice t.

În teoria ecuaţiilor diferenţiale cu coeficienţi constanţi se arată că soluţia generală a acestui sistem de ecuaţii este $y = e^{tA}C$ cu $C \in M_{n1}(\mathbf{C})$, unde matricea e^{tA}, numită *exponenţiala lui A*, se defineşte prin formula $e^{tA} = \sum_{n=0}^{\infty}(tA)^n/n!$. În aplicaţii, explicitarea soluţiei se face prin intermediul formei canonice Jordan.

Fie $B \in M_n(\mathbf{C})$, $S \in GL_n(\mathbf{C})$ şi $C \in M_p(\mathbf{C})$. Din definiţie rezultă că

$$e^{tSBS^{-1}} = S(\sum_{n=0}^{\infty}(tB)^n/n!)S^{-1} = Se^{tB}S^{-1}$$

şi

$$e^{t(B \oplus C)} = \sum_{n=0}^{\infty} t^n (B \oplus C)^n/n! = e^{tB} \oplus e^{tC}.$$

De aici rezultă că putem reduce calculul lui e^{tA} la cazul celulelor Jordan. Pentru acestea avem

Teorema 203

$$e^{tJ_k(\lambda)} = e^{\lambda t} \begin{pmatrix} 1 & & & & \\ \frac{t}{1!} & 1 & & & \\ \frac{t^2}{2!} & \frac{t}{1!} & 1 & & \\ \cdots & & & & \\ \frac{t^{k-1}}{(k-1)!} & \cdots & \frac{t^2}{2!} & \frac{t}{1!} & 1 \end{pmatrix}.$$

Demonstraţie.

$$e^{tJ_k(\lambda)} = \sum_{n=0}^{\infty} \frac{t^n J_k^n(\lambda)}{n!} =$$

$$= \sum_{n=0}^{\infty} \begin{pmatrix} \frac{(t\lambda)^n}{n!} & & & & \\ \frac{t}{1!}\frac{(t\lambda)^{n-1}}{(n-1)!} & \frac{(t\lambda)^n}{n!} & & & \\ \frac{t^2}{2!}\frac{(t\lambda)^{n-2}}{(n-2)!} & \frac{t}{1!}\frac{(t\lambda)^{n-1}}{(n-1)!} & \frac{(t\lambda)^n}{n!} & & \\ \cdots & & & & \\ \frac{t^{k-1}}{(k-1)!}\frac{(t\lambda)^{n-k+1}}{(n-k+1)!} & \cdots & \frac{t^2}{2!}\frac{(t\lambda)^{n-2}}{(n-2)!} & \frac{t}{1!}\frac{(t\lambda)^{n-1}}{(n-1)!} & \frac{(t\lambda)^n}{n!} \end{pmatrix} =$$

$$= e^{\lambda t}\begin{pmatrix} 1 & & & & \\ \frac{t}{1!} & 1 & & & \\ \frac{t^2}{2!} & \frac{t}{1!} & 1 & & \\ \cdots & & & & \\ \frac{t^{k-1}}{(k-1)!} & \cdots & \frac{t^2}{2!} & \frac{t}{1!} & 1 \end{pmatrix}. \bullet$$

Exemplu. Fie sistemul de ecuaţii diferenţiale cu coeficienţi constanţi $y' = Ay$, unde $A = \begin{pmatrix} 0 & -1 & 2 & 1 \\ -2 & 1 & 2 & 1 \\ -1 & -1 & 2 & 2 \\ 0 & -1 & 2 & 1 \end{pmatrix}$. Cum am văzut mai sus, $A = U(J_2(2) \oplus J_2(0))U^{-1}$, unde $U = \begin{pmatrix} 0 & 1 & 1 & 0 \\ -1 & 1 & 0 & -2 \\ 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$. Rezultă că soluţia generală a ecuaţiei diferenţiale $y' = Ay$ este

$$f(t) = e^{tA}C = e^{tU(J_2(2)\oplus J_2(0))U^{-1}}C = Ue^{tJ_2(2)\oplus tJ_2(0)}U^{-1}C$$

cu $C \in M_{41}(\mathbf{C})$. Conform teoremei anterioare,

$$e^{tJ_2(2)\oplus tJ_2(0)} = e^{tJ_2(2)} \oplus e^{tJ_2(0)} = \begin{pmatrix} e^{2t} & 0 & 0 & 0 \\ te^{2t} & e^{2t} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & t & 1 \end{pmatrix}.$$

9.7 Exerciţii

În exerciţiile următoare K este un corp comutativ.

219. Găsiţi clasele de asemănare ale matricelor din $M_2(\mathbf{Z}_2)$. (Indicaţie. Dacă matricea nu este scalară, atunci ea are un singur factor invariant.)

220. Număraţi clasele de asemănare ale matricelor din $M_2(K)$, unde K este un corp cu q elemente.

221. Calculaţi factorii invarianţi ai matricelor următoare cu transformări elementare şi cu ajutorul polinoamelor Δ. Pentru fiecare matrice, scrieţi forma Jordan peste $\mathbf{Q}$, $\mathbf{R}$ şi $\mathbf{C}$.

$$\begin{pmatrix} 4 & 5 & -2 \\ -2 & -2 & 1 \\ -1 & -1 & 1 \end{pmatrix}, \begin{pmatrix} -3 & -1 & 3 \\ 22 & 9 & -27 \\ 5 & 2 & -6 \end{pmatrix}, \begin{pmatrix} 0 & 4 & 2 \\ -1 & -4 & -1 \\ 0 & 0 & -2 \end{pmatrix}, \begin{pmatrix} 2 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 2 & 1 \\ 1 & -1 & 1 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 3 & 0 & 0 \\ a & 3 & 0 \\ b & 0 & -2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

222. Descrieţi matricele $A \in M_2(\mathbf{C})$ nediagonalizabile.

223. Fie $\alpha, \beta, \gamma \in \mathbf{C}$ distincte şi $A \in M_3(\mathbf{C})$. Determinaţi forma canonică Jordan a lui A în cazurile următoare: (1) $Spec(A) = \{\alpha, \beta, \gamma\}$. (2) $Spec(A) = \{\alpha, \beta\}$, $m_a(\alpha) = 2$, $m_g(\alpha) = 2$. (3) $Spec(A) = \{\alpha, \beta\}$, $m_a(\alpha) = 2$, $m_g(\alpha) = 1$. (4) $Spec(A) = \{\alpha\}$, $m_g(\alpha) = 3$. (5) $Spec(A) = \{\alpha\}$, $m_g(\alpha) = 2$. (6) $Spec(A) = \{\alpha\}$, $m_g(\alpha) = 1$.

224. Determinaţi forma canonică Jordan şi o matrice de asemănare pentru matricea $A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \in M_n(\mathbf{C})$.

225. Calculaţi factorii invarianţi ai matricelor următoare cu transformări elementare şi cu ajutorul polinoamelor Δ.

$$\begin{pmatrix} \hat{1} & \hat{1} & \hat{0} & \hat{1} \\ \hat{0} & \hat{0} & \hat{0} & \hat{1} \\ \hat{1} & \hat{1} & \hat{1} & \hat{0} \\ \hat{0} & \hat{1} & \hat{0} & \hat{0} \end{pmatrix} \in M_4(\mathbf{Z}_2) \text{ şi } \begin{pmatrix} \hat{1} & \hat{0} & \hat{0} & \hat{0} \\ \hat{0} & \hat{2} & \hat{2} & \hat{2} \\ \hat{0} & \hat{1} & \hat{0} & \hat{0} \\ \hat{0} & \hat{0} & \hat{1} & \hat{0} \end{pmatrix} \in M_4(\mathbf{Z}_3).$$

226. Este matricea $A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$ asemenea cu o matrice diagonală ?

227. Cum poate arăta forma Jordan a unei matrice cu polinomul caracteristic $(X-2)^2(X-3)^3$?

228. Fie $A \in M_{10}(\mathbf{Q})$. Găsiţi forma canonică Jordan a lui A ştiind că printre divizorii elementari ai lui A peste $\mathbf{C}$ se găsesc $X-i$, $(X-i)^2$, $X+\sqrt{2}$ şi $X+\sqrt{3}$.

229. Fie $a, b, c \in \mathbf{C}$ astfel încât a^2, b^2, c^2 sunt distincte. Găsiţi forma canonică Jordan a matricei $A = \begin{pmatrix} 0 & a & b & c \\ a & 0 & c & b \\ b & c & 0 & a \\ c & b & a & 0 \end{pmatrix}$.

230. Fie $\sigma \in S_n$. Găsiţi forma canonică Jordan a matricei $A_\sigma = (a_{ij})_{1 \leq i,j \leq n}$ unde $a_{ij} = \delta_{i\sigma(j)}$ Aplicaţie: $\sigma = (1943)(852)$. Deduceţi că două permutări $\alpha, \beta \in S_n$ sunt conjugate dacă şi numai dacă $A_\alpha \approx A_\beta$.

231. Fie V un K-spaţiu vectorial cu baza e_1,..., e_n, n număr par. Găsiţi forma Jordan a endomorfismului u al lui V definit prin $u(e_i) = e_{n+1-i}$.

232. Găsiţi forma Jordan a unei matrice $A \in M_n(K)$ de rang 1. Aplicaţi rezultatul pentru $B = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{pmatrix}$ şi $C = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ -3 & -3 & -3 \end{pmatrix}$

233. Găsiţi forma Jordan a unei matrice $A \in M_n(K)$ cu toate elementele egale cu 1.

234. Fie matricea $A = \begin{pmatrix} 5 & 4 & 2 \\ 4 & 5 & 2 \\ 2 & 2 & 2 \end{pmatrix}$. Calculaţi:

(a) polinomul caracteristic al lui A,
(b) inversa matricei A folosind teorema Hamilton-Cayley,
(c) valorile proprii şi subspaţiile proprii corespunzătoare,
(d) forma Jordan a lui A şi o matrice de asemănare.

235. Determinaţi forma canonică Jordan şi o matrice de asemănare pentru matricea $A = \begin{pmatrix} 3 & -1 & 0 & -1 \\ 2 & 0 & 0 & -1 \\ 1 & -1 & 1 & 0 \\ 2 & -1 & 0 & 0 \end{pmatrix} \in M_4(\mathbf{C})$. Calculaţi puterile lui A.

236. Determinaţi forma canonică Jordan a matricei $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \varepsilon & \varepsilon^2 \\ 1 & \varepsilon^2 & \varepsilon \end{pmatrix}$ unde $\varepsilon = (-1 + i\sqrt{3})/2$.

237. Determinaţi forma canonică Jordan şi o matrice de asemănare pentru matricea $A = \begin{pmatrix} 0 & 0 & 8 \\ 1 & 0 & -12 \\ 0 & 1 & 6 \end{pmatrix} \in M_3(\mathbf{C})$.

238. Determinaţi forma canonică Jordan şi o matrice de asemănare pentru matricea $A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & -2 \\ 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$.

239. Determinaţi forma canonică Jordan a matricei $A = \begin{pmatrix} a & 0 & b \\ a & a+b & 0 \\ b & 0 & a \end{pmatrix}$ unde $a, b \in \mathbf{C}^*$.

240. Arătaţi că o matrice $A \in M_n(K)$ este nilpotentă $\Leftrightarrow P_A = X^n \Leftrightarrow A^n = 0$. Pentru $n = 4$, scrieţi toate matricele Jordan nilpotente.

241. Fie $A \in M_n(K)$ astfel încât $P_A = \pi_1\pi_2\cdots\pi_k$ cu $\pi_1, \pi_2, ..., \pi_k \in K[X]$ polinoame ireductibile unitare distincte. Arătaţi că $A \approx J_1(\pi_1)\oplus\cdots\oplus J_1(\pi_k)$.

242. Arătaţi că o matrice $A \in M_n(K)$ este idempotentă (i.e. $A^2 = A$) $\Leftrightarrow$ A are divizorii elementari forma X sau $X - 1$. Pentru $n = 4$, scrieţi toate matricele Jordan idempotente.

243. Fie matricea $A = \begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 1 \end{pmatrix}$. Arătaţi că $A = A^2$ şi determinaţi forma Jordan a lui A.

244. Găsiţi forma Jordan a lui $J_n^2(0)$.

245. Arătaţi că $J_5^2(0) \approx J_2^2(0) \oplus J_3^2(0)$ folosind transformări elementare de tip P_{ij}.

246. Daţi un exemplu de două matrice nilpotente neasemenea având acelaşi rang, polinom caracteristic şi polinom minimal.

247. Fie $A, B \in M_n(K)$. Arătaţi că $Tr(A+B) = Tr(A) + Tr(B)$ şi $Tr(AB) = Tr(BA)$.

248. Arătaţi că o matrice $A \in M_n(\mathbf{C})$ cu urma nulă este asemenea cu o matrice având elementele de pe diagonala principală nule.

249. Arătaţi că o matrice $A \in M_n(\mathbf{C})$ are urma nulă dacă şi numai dacă A se poate scrie sub forma $XY - YX$ cu $X, Y \in M_n(\mathbf{C})$.

250. Fie K un corp, $n \geq 1$, $A \in M_n(K)$ şi $b_1, ..., b_n \in K$ elemente distincte. Arătaţi că A comută cu $diag(b_1, ..., b_n) \Leftrightarrow$ este A este matrice diagonală. În particular, dacă $A^k = diag(b_1, ..., b_n)$, atunci $A = diag(a_1, ..., a_n)$ cu $a_i^k = b_i$, $i = 1, ..., n$.

251. Fie $A, B \in M_n(\mathbf{C})$ că $AB = BA$ astfel încât A are valorile proprii distincte. Arătaţi că există $S \in GL_n(\mathbf{C})$ astfel încât SAS^{-1} şi SBS^{-1} sunt matrice diagonale.

252. Fie $A \in M_n(\mathbf{C})$ şi $k \geq 2$. Arătaţi că $2\,rang(A^k) \leq rang(A^{k-1}) + rang(A^{k+1})$. În particular, dacă $rang(A^k) = rang(A^{k-1})$, atunci $rang(A^{k+1}) = rang(A^k)$.

253. Găsiţi forma canonică Jordan a unei matrice $A \in M_7(\mathbf{C})$ cu $\mu_A = X(X-1)^3$ şi $Tr(A) = 4$.

254. Găsiţi termenul general al şirurilor date prin relaţiile de recurenţă: (a) $x_n = -x_{n-1} - x_{n-2}$, $x_0 = 2$, $x_1 = -1$. (b) $x_n = 10x_{n-2} + 20x_{n-3} + 15x_{n-4} + 4x_{n-5}$, $x_0 = 2$, $x_1 = 1$, $x_2 = 29$, $x_3 = 27$, $x_4 = 337$.

255. Determinaţi termenul general al şirurilor $(a_n)_n$, $(b_n)_n$, $(c_n)_n$ definite prin relaţiile de recurenţă $a_{n+1} = (b_n + c_n)/2$, $b_{n+1} = (a_n + c_n)/2$, $c_{n+1} = (a_n + b_n)/2$, a_0, b_0, c_0 date.

256. Arătaţi că pentru $n \geq 2$, ecuaţia matriceală $Z^2 = J_n(0)$ nu are soluţii.

257. Fie K un corp de caracteristică $\neq 2$ şi $n \geq 1$. Arătaţi, prin inducţie după n, că ecuaţia matriceală $Z^2 = J_n(1)$ are soluţii.

258. Fie $A = (a_{ij})_{1\leq i,j\leq n} \in M_n(K)$ o inferior triunghiulară cu $a_{11} = a_{22} = ... = a_{nn} = \alpha$ şi $a_{12}a_{23}\cdots a_{n-1n} \neq 0$. Determinaţi forma Jordan a lui A şi aplicaţi rezultatul pentru $J_n^k(\alpha)$, $\alpha \in K^*$.

259. Fie $a \in \mathbf{C}^*$ şi $k, n \geq 1$. Arătaţi că ecuaţia matriceală $Z^k = J_n(a)$ are soluţii în $M_n(\mathbf{C})$.

260. Fie matricele $A = \begin{pmatrix} 2 & -1 & 0 & -1 \\ 2 & -1 & 0 & -1 \\ 1 & -1 & 0 & 0 \\ 2 & -1 & 0 & -1 \end{pmatrix}$ şi $B = \begin{pmatrix} 3 & -1 & -1 & -1 \\ 2 & -1 & 0 & -1 \\ 2 & -1 & -1 & 0 \\ 3 & -1 & -1 & -1 \end{pmatrix}$.
Au ecuaţiile $Y^2 = A$, $Z^2 = B$ soluţie în $M_4(\mathbf{C})$?

261. Rezolvaţi în $M_3(\mathbf{C})$ ecuaţia $Y^2 = A$, unde $A = \begin{pmatrix} 5 & 2 & 3 \\ 4 & 5 & -4 \\ 6 & 4 & -4 \end{pmatrix}$.

262. Calculaţi A^n şi e^A pentru $A = \begin{pmatrix} 0 & 2 \\ -3 & 5 \end{pmatrix}$.

263. Calculaţi A^n şi e^A pentru $A = \begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix}$.

264. Fie $A \in M_n(\mathbf{C})$. Arătaţi că $|e^A| = e^{Tr(A)}$.

265. Calculaţi e^{tA} unde $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix}$.

Bibliografie

[1] M. Artin, *Algebra.* Prentince Hall, New Jersey 1990.

[2] D. Faddéev, I. Sominski, *Recueil d'exercises d'algèbre supérieure.* Editions MIR, Mouscou 1972.

[3] G. Galbură, F. Radó, *Geometrie.* Editura Didactică şi Pedagogică, Bucureşti 1979.

[4] P. Halmos, *Naive Set Theory.* Springer, New York, Berlin 1974.

[5] Ion D. Ion, N. Radu, *Algebră.* Editura Didactică şi Pedagogică, Bucureşti 1991.

[6] I. Kaplansky *Commutative Rings.* The University of Chicago Press, Chicago and London 1974.

[7] C. Năstăsescu, C. Niţă, C. Vraciu, *Bazele Algebrei.* Editura Academiei Române, Bucureşti 1986.

[8] I. Proskouriakov, *Recueil de problèmes d'algebre linéaire.* Editions MIR, Mouscou 1989.

[9] I. Tomescu, *Probleme de combinatorică şi teoria grafurilor.* Editura Didactică şi Pedagogică, Bucureşti 1981.

Index