

TIBERIU DUMITRESCU

ALGEBRA 1

București, 2006

PREFAȚĂ

Lucrarea se adresează studenților din anul I de la facultățile de matematică și informatică din universități. În cuprinsul ei sunt prezentate rezultate de bază referitoare la mulțimi, funcții, relații de echivalență, operații algebrice, monoizi, grupuri, inele, corpuri, inele de polinoame în una sau mai multe nedeterminate, rădăcini ale polinoamelor, aritmetica lui \mathbf{Z} și $K[X]$, polinoame simetrice, determinanți, spații vectoriale, sisteme de ecuații liniare, și teoria formei canonice Jordan. Urmând exemplul cărții [6] a lui Irving Kaplansky, materialul este prezentat ca un șir aproape neîntrerupt de teoreme. Numerotarea teoremelor e făcută în continuare fără a ține seama de trecerea dintr-un capitol în următorul. Definițiile și rezultatele sunt frecvent însoțite de exemple, aplicații sau comentarii. Fiecare capitol se termină cu o listă de exerciții de dificultate variabilă. Soluțiile complete ale acestor exerciții se găsesc la sfârșitul lucrării. Tot la sfârșit se află un index care facilitează găsirea în text a noțiunilor sau teoremelor importante.

Autorul

Cuprins

1	Mulțimi și funcții	9
1.1	Mulțimi	9
1.2	Funcții	12
1.3	Familii de mulțimi.	17
1.4	Relații de echivalență	19
1.5	Exerciții.	22
2	Operații algebrice, monoizi.	27
2.1	Operații algebrice	27
2.2	Monoizi	30
2.3	Exerciții	34
3	Grupuri	37
3.1	Exemple de grupuri	37
3.2	Morfisme de grupuri	39
3.3	Subgrupuri	40
3.4	Subgrupul generat de o mulțime	42
3.5	Congruențe modulo un subgrup	44
3.6	Ordinul unui element într-un grup	45
3.7	Subgrupuri normale	47
3.8	Grupul factor	48
3.9	Grupuri ciclice	49
3.10	Grupul permutărilor S_n	50
3.11	Ecuția claselor	53
3.12	Exerciții	55
4	Inele	61
4.1	Inel, subinel, ideal	61

4.2	Morfisme de inele	67
4.3	Inel factor	70
4.4	Corpuri	71
4.5	Inelul de polinoame $A[X]$	75
4.6	Rădăcini ale polinoamelor	78
4.7	Inelul de polinoame $A[X_1, \dots, X_n]$	80
4.8	Exerciții	83
5	Aritmetica lui \mathbf{Z} și $K[X]$	87
5.1	Teorema împărțirii cu rest	87
5.2	Numere prime, polinoame ireductibile	93
5.3	Complemente	97
5.4	Exerciții	98
6	Polinoame simetrice	101
6.1	Inelul polinoamelor simetrice	101
6.2	Teorema fundamentală	104
6.3	Exerciții	107
7	Determinanți	109
7.1	Proprietățile determinantilor	109
7.2	Dezvoltări ale determinantilor.	113
7.3	Aplicații	116
7.4	Exerciții	119
8	Spații vectoriale și sisteme liniare	123
8.1	Spații vectoriale	123
8.2	Sisteme de ecuații liniare	132
8.3	Rangul unei matrice	136
8.4	Exerciții	138
9	Forma canonică Jordan	143
9.1	Matricea unui endomorfism	143
9.2	Forma diagonal-canonică	146
9.3	Forma Jordan a unei matrice	151
9.4	Polinomul minimal	157
9.5	Cazul $K = \mathbf{C}$	160
9.6	Aplicații ale formei canonice Jordan.	165

<i>CUPRINS</i>	7
9.7 Exerciții	169
10 Soluțiile exercițiilor	175

Capitolul 1

Mulțimi și funcții

Acest capitol are caracter introductiv. Se trec în revistă conceptele de mulțime, apartenență, incluziune, operații cu mulțimi, mulțimea părților, produs cartezian, funcție, compunere, injectivitate, surjectivitate, echipotență, numărabilitate, familie de mulțimi, relație de echivalență, mulțime factor.

1.1 Mulțimi

Prin *mulțime* înțelegem o colecție de obiecte numite *elementele mulțimii*. Dacă x este un element al mulțimii A , atunci spunem că x *aparține* lui A și scriem $x \in A$; în caz contrar, spunem că x *nu aparține* lui A și scriem $x \notin A$. De exemplu, $1 \in \{1, 2, 3\}$ și $4 \notin \{1, 2, 3\}$, unde $\{1, 2, 3\}$ este mulțimea având elementele 1, 2 și 3.

Spunem că două mulțimi A, B sunt *egale* dacă au aceleași elemente, adică $A = B \Leftrightarrow (x \in A \Leftrightarrow x \in B)$. Cel mai simplu mod de a descrie o mulțime este specificând elementele sale. De exemplu, $\{1, 2\}$ este mulțimea cu elementele 1 și 2. Ordinea elementelor și repetițiile sunt irelevante. De exemplu, $\{1, 2\} = \{2, 1\} = \{1, 1, 1, 2\}$. O mulțime se poate descrie și prin precizarea unei proprietăți caracteristice a elementelor sale. De exemplu, $\{1, 2\} = \{x \in \mathbf{R} \mid x^2 - 3x + 2 = 0\}$.

Fie A, B două mulțimi. Spunem că A este o *submulțime* a lui B sau că A este *inclusă* în B , dacă orice element al lui A este și 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 *submulțime proprie* a lui B sau că A este *strict inclusă* în B și notăm $A \subset B$ sau $B \supset A$. Rezultă că $A = B \Leftrightarrow A \subseteq B$ și $B \subseteq A$.

Se vede imediat că egalitatea și incluziunea de mulțimi sunt tranzitive, adică, dacă A, B, C sunt mulțimi, atunci

- (a) $A \subseteq B$ și $B \subseteq C$ implică $A \subseteq C$,
- (b) $A = B$ și $B = C$ implică $A = C$.

Avem următoarele exemple importante de mulțimi. Mulțimea numerelor naturale $\mathbf{N} = \{0, 1, 2, \dots\}$, mulțimea numerelor întregi $\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, mulțimea numerelor raționale \mathbf{Q} , mulțimea numerelor reale \mathbf{R} și mulțimea 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} și \mathbf{C} se pot obține prin anumite construcții pornind de la \mathbf{N} (vezi exercițiile 24, 25 și 26). *Mulțimea vidă*, \emptyset , este mulțimea care nu are nici un element. Putem scrie

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

Mulțimea vidă este submulțime a oricărei mulțimi. Fie A o mulțime. Notăm cu $\mathcal{P}(A)$ și numim *mulțimea părților* lui A mulțimea ale cărei elemente sunt submulțimile lui A , adică

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

De exemplu, $\mathcal{P}(\emptyset) = \{\emptyset\}$ și $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$. Fie A, B două mulțimi. Se definesc următoarele operații:

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

$$A \cap B = \{x \mid x \in A \text{ și } x \in B\} \text{ (intersecția lui } A \text{ cu } B)$$

$$A \setminus B = \{x \in A \mid x \notin B\} \text{ (diferența dintre } A \text{ și } B).$$

De exemplu, $\{1, 2\} \cup \{1, 3\} = \{1, 2, 3\}$, $\{1, 2\} \cap \{1, 3\} = \{1\}$ și $\{1, 2\} \setminus \{1, 3\} = \{2\}$. Două mulțimi cu intersecția vidă se zic *disjuncte*. De exemplu, $\{1, 2\}$ și $\{3, 4\}$ sunt disjuncte. Cum se arată în teorema următoare, operațiile de reuniune și intersecție sunt comutative, asociative și fiecare dintre ele este distributivă față de cealaltă.

Teorema 1 Fie A, B, C trei mulțimi. Atunci

- (a) $A \cap B \subseteq A \subseteq A \cup B$,
- (b) $A \cup B = B \cup A$ și $A \cap B = B \cap A$,
- (c) $(A \cup B) \cup C = A \cup (B \cup C)$ și $(A \cap B) \cap C = A \cap (B \cap C)$,
- (d) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, și
- (e) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Demonstrație. Lăsăm demonstrația cititorului. Pentru exemplificare, probăm (e). Avem șirul de echivalențe: $x \in A \cup (B \cap C) \Leftrightarrow x \in A$ sau $x \in B \cap C \Leftrightarrow x \in A$ sau $(x \in B \text{ și } x \in C) \Leftrightarrow (x \in A \text{ sau } x \in B) \text{ și } (x \in A \text{ sau } x \in C) \Leftrightarrow x \in (A \cup B) \cap (A \cup C)$. •

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

Teorema 2 Fie X o mulțime și $A, B \subseteq X$. Atunci

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

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

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

Fie A, B două mulțimi și $a \in A$, $b \in B$. *Perechea ordonată* (a, b) se definește prin

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

Se vede ușor că două perechi (a, b) și (a', b') sunt egale dacă și numai dacă $a = a'$ și $b = b'$. *Produsul cartezian* $A \times B$ al mulțimilor A și B este mulțimea acestor perechi ordonate, adică

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

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 Funcții

Fie A și B două mulțimi. O *funcție* (sau *aplicație*) f de la A la B (notație $f : A \rightarrow B$) este o submulțime a produsului cartezian $A \times B$ cu proprietatea

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

Deci f asociază fiecărui element $x \in A$ un unic element $b_x \in B$ pe care-l vom nota cu $f(x)$. Așadar, pentru a defini o funcție $f : A \rightarrow B$ trebuie să precizăm mulțimea A numită *domeniul de definiție* al lui f , mulțimea B numită *codomeniul* sau *domeniul valorilor* lui f și asocierea $a \mapsto f(a)$. Mulțimea $\{(a, f(a)) \mid a \in A\} = f$ se mai numește și *graficul lui f*. Mulțimea tuturor funcțiilor $g : A \rightarrow B$ se notează cu B^A .

De exemplu, $f : \{1, 2\} \rightarrow \{1, 2, 3\}$, $f(n) = n + 1$ este o funcție cu graficul $\{(1, 2), (2, 3)\}$. Pe de altă parte, $g : \{0, 1, 2\} \rightarrow \mathbf{R}$, $g(x) = y$ unde $y \in \mathbf{R}$ și $x^2 + y^2 = 1$, nu este funcție, deoarece $g(0) = \pm 1$, deci $g(0)$ nu este unic determinat, iar $g(2)$ nu există. Cu alte cuvinte, submulțimea $\{(0, 1), (0, -1), (1, 0)\}$ a lui $\{0, 1, 2\} \times \mathbf{R}$ nu satisface condiția din definiția funcției.

Prin definiție, două funcții $f : A \rightarrow B$ și $g : C \rightarrow D$ sunt *egale* dacă $A = C$, $B = D$ și $f(x) = g(x)$ pentru orice $x \in A$. Fie două funcții $f : A \rightarrow B$ și $g : B \rightarrow C$. *Compunerea* gf dintre g și f este funcția $gf : A \rightarrow C$ definită prin

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

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

Teorema 3 Fie funcțiile $f : A \rightarrow B$, $g : B \rightarrow C$ și $h : C \rightarrow D$. Atunci $h(gf) = (hg)f$ (i.e., compunerea funcțiilor este asociativă).

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

O funcție $f : A \rightarrow B$ se numește *funcție injectivă* sau mai simplu *injectie*, 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 funcție $f : A \rightarrow B$ se numește *funcție surjectivă* sau mai simplu *surjectie*, dacă pentru orice $y \in B$ există $x \in A$ astfel încât $f(x) = y$. O funcție se numește *funcție bijectivă* sau mai simplu *bijectie*, dacă este simultan injectivă și surjectivă.

De exemplu, fie funcțiile $f, g, h, k : \mathbf{Z} \rightarrow \mathbf{Z}$ date prin: $f(m) = 2m$, $g(m) = \lfloor m/2 \rfloor$, $h(m) = m + 1$ și $k(m) = m^2$. Atunci f este injectivă și nesurjectivă, g este surjectivă și neinjectivă, h este bijectivă, iar k este neinjectivă și nesurjectivă.

Dacă A este o submulțime a lui B , atunci injectia $i : A \rightarrow B$, dată prin $i(x) = x$, se numește *funcția (aplicația) de incluziune a lui A în B* . Bijectia $I_A : A \rightarrow A$, dată prin $I_A(x) = x$, se numește *funcția (aplicația) identică a mulțimii A* . Se verifică imediat că pentru orice funcție $f : A \rightarrow B$ avem $I_B f = f$ și $f I_A = f$.

Dacă A, B sunt două mulțimi, atunci surjecțiile $p_A : A \times B \rightarrow A$ și $p_B : A \times B \rightarrow B$, date prin $p_A(x, y) = x$ și $p_B(x, y) = y$, se numesc *proiecțiile canonice* ale produsului cartezian $A \times B$ pe prima respectiv a doua componentă. O bijectie $s : A \rightarrow A$ se mai numește *permutare* a mulțimii A . De exemplu, $\sigma = \begin{pmatrix} a & b & c & d \\ b & c & a & d \end{pmatrix}$ este o permutare a mulțimii $\{a, b, c, d\}$.

Teorema 4 Fie funcțiile $f, f' : A \rightarrow B$ și $g, g' : B \rightarrow C$. Atunci au loc următoarele implicații

- (a) f, g injectii $\Rightarrow gf$ injectie,
- (b) f, g surjectii $\Rightarrow gf$ surjectie,
- (c) f, g bijectii $\Rightarrow gf$ bijectie,
- (d) gf injectie $\Rightarrow f$ injectie,
- (e) gf surjectie $\Rightarrow g$ surjectie,
- (f) gf bijectie $\Rightarrow f$ injectie și g surjectie,
- (g) $gf = gf'$ și g injectie $\Rightarrow f = f'$,
- (h) $gf = g'f$ și f surjectie $\Rightarrow g = g'$.

Demonstrație. (a). Fie $x, y \in A$ astfel încât $(gf)(x) = (gf)(y)$, adică $g(f(x)) = g(f(y))$. Cum g, f sunt injectii, obținem $f(x) = f(y)$ și apoi $x = y$. (b). Fie $z \in C$. Cum g, f sunt surjectii, există $y \in B$ cu $g(y) = z$ și apoi există $x \in A$ cu $f(x) = y$. Obținem $(gf)(x) = g(y) = z$.

(c) rezultă din (a) și (b).

(d). Fie $x, y \in A$ cu $f(x) = f(y)$. Aplicând pe g obținem $(gf)(x) = (gf)(y)$ și cum gf este injectie, rezultă $x = y$.

(e). Fie $z \in C$. Cum gf este surjecție, există $x \in A$ cu $(gf)(x) = z$. Deci $y = f(x) \in B$ și $g(y) = z$. (f) rezultă din (d) și (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 surjecție, există $x \in A$ cu $f(x) = y$. Deoarece $gf = g'f$, rezultă $g(y) = (gf)(x) = (g'f)(x) = g'(y)$. •

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

Teorema 5 Fie $f : A \rightarrow B$ o funcție. Atunci f este bijectivă dacă și numai dacă există o funcție $g : B \rightarrow A$ astfel încât $gf = I_A$ și $fg = I_B$. Dacă există, funcția g este unică; g se numește inversa lui f și se notează cu f^{-1} .

Demonstrație. Implicația \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 funcția $g : B \rightarrow A$ 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) și (h) ale teoremei 4. •

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

Fie $f : A \rightarrow B$ o funcție. Dacă $X \subseteq A$, atunci submulțimea lui B , $f(X) = \{f(x) \mid x \in X\}$ se numește *imagea (directă)* a lui X prin f . $f(A)$ se notează cu $\text{Im}(f)$ și se numește *imagea* lui f . E clar că f este surjectivă dacă și numai dacă $\text{Im}(f) = B$. De asemenea, dacă $Y \subseteq B$, atunci submulțimea lui A , $f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}$ se numește *pre-imagea* sau *imagea inversă* a lui Y prin f .

De exemplu, pentru funcția $h : \mathbf{N} \rightarrow \mathbf{Z}$, dată prin $h(n) = (-1)^n$, avem $\text{Im}(h) = \{1, -1\}$, $h(\{1, 3\}) = \{-1\}$, $h^{-1}(\{2\}) = \emptyset$ și $h^{-1}(\{1\}) =$ mulțimea numerelor naturale pare.

Teorema 6 Fie $f : A \rightarrow B$ o funcție, $X, W \subseteq A$ și $Y, Z \subseteq B$. 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).

Demonstrație. (a) și (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 și fie $y \in f(X) \cap f(W)$. Există $x \in X$ și $w \in W$ astfel încât $f(x) = f(w) = y$. Din injectivitatea lui f rezultă $x = w$, deci $y \in f(X \cap W)$.

(e). Avem șirul de echivalențe: $x \in f^{-1}(Y \cup Z) \Leftrightarrow f(x) \in Y \cup Z \Leftrightarrow f(x) \in Y$ 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). Relația $f(f^{-1}(Y)) \subseteq Y$ este evidentă. Presupunem că f este surjectivă și 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 mulțime. Afirmațiile următoare sunt echivalente:

- (a) A este finită,
- (b) orice injecție $f : A \rightarrow A$ este bijecție,
- (c) orice surjecție $f : A \rightarrow A$ este bijecție.

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

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

(b) \Rightarrow (a) și (c) \Rightarrow (a). Presupunem că A este infinită. Vom construi funcțiile $f, g : A \rightarrow A$, f injectivă nesurjectivă, g surjectivă neinjectivă. Fiind

infinită, A posedă o submulțime infinită $B = \{a_1, a_2, \dots, a_n, \dots\}$. Definim funcțiile $f, g : A \rightarrow A$ 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 $a_1 \notin \text{Im}(f)$, $g(a_1) = g(a_2)$ și $gf = I_A$, rezultă că f este injectivă dar nesurjectivă iar g este surjectivă dar neinjectivă. •

Proprietatea anterioară ne permite să definim mulțimile finite ca fiind mulțimile A cu proprietatea că orice injecție (surjecție) $f : A \rightarrow A$ este bijecție.

Teorema 8 Fie A, B mulțimi finite cu m respectiv n elemente. Atunci

- (a) numărul submulțimilor lui B este 2^n
- (b) numărul funcțiilor de la A la B este n^m
- (c) numărul permutărilor lui B este $n!$
- (d) dacă $m \leq n$, numărul injecțiilor de la A la B este $n!/(n-m)!$
- (e) dacă $m \geq n$, numărul surjecțiilor de la A la B este

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

Demonstrație. (a). Fie $0 \leq k \leq n$. Submulțimile lui B având k elemente sunt în număr de C_n^k . Deci B are $C_n^0 + C_n^1 + \dots + C_n^n = (1+1)^n = 2^n$ submulțimi. Pentru celelalte afirmații, vezi exercițiul 12. •

Spunem că două mulțimi A, B sunt *echipotente* sau că *au același cardinal* și notăm $A \simeq B$ sau $|A| = |B|$, dacă există o bijecție $f : A \rightarrow B$. E clar că două mulțimi finite sunt echipotente dacă și numai dacă au același număr de elemente. Din acest motiv, pentru o mulțime finită cu n elemente vom scrie $|A| = n$.

Pentru cazul mulțimilor arbitrare, se poate proba ușor că relația de echipotență posedă proprietățile reflexivitate ($A \simeq A$), simetrie ($A \simeq B \Rightarrow B \simeq A$) și tranzitivitate ($A \simeq B$ și $B \simeq C \Rightarrow A \simeq C$). O mulțime echipotentă cu \mathbf{N} se numește *mulțime numărabilă*. E clar că A este mulțime numărabilă dacă și numai dacă elementele lui A se pot așeza într-un șir infinit. Cum $\mathbf{Z} = \{0, \pm 1, \pm 2, \dots\}$, \mathbf{Z} este numărabilă. $\mathbf{N} \times \mathbf{N}$ este de asemenea numărabilă, deoarece avem bijecția

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

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

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

Demonstrație. Presupunem că \mathbf{R} este numărabilă. Atunci intervalul $(0, 1)$ este numărabil. Fie $\{a_1, \dots, a_n, \dots\}$ o înșiruire a numerelor din $(0, 1)$ și 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 și a_{nn} . Atunci numărul cu reprezentarea zecimală

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

apartține lui $(0, 1)$ dar nu se găsește în șirul $\{a_1, \dots, a_n, \dots\}$, contradicție. •

Fie A, B două mulțimi. Spunem că A are cardinal mai mic decât B și notăm $|A| \leq |B|$, dacă există o injecție $f : A \rightarrow B$. Dacă în plus, A, B nu sunt echipotente, notăm $|A| < |B|$. Au loc următoarele două rezultate remarcabile.

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

Demonstrație. Injecția $i : A \rightarrow \mathcal{P}(A)$, $i(x) = \{x\}$, ne arată că $|A| \leq |\mathcal{P}(A)|$. Presupunem că avem o bijecție $f : A \rightarrow \mathcal{P}(A)$. Se consideră mulțimea $B = \{a \in A \mid a \notin f(a)\}$. Cum f este surjectivă, există $b \in A$ cu $f(b) = B$. Dacă $b \in B$, atunci $b \notin f(b) = B$, contradicție; iar dacă $b \notin B$, atunci $b \in f(b) = B$, din nou contradicție. •

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

Demonstrație. Vezi exercițiul 9. •

1.3 Familii de mulțimi.

Fie M o mulțime nevidă. Un șir $(x_n)_{n \geq 1}$ de elemente ale lui M înseamnă, de fapt, o funcție $f : \mathbf{N}^* \rightarrow M$, $f(n) = x_n$. Mai general, dacă I este o mulțime, o

familie de elemente $(x_i)_{i \in I}$ din M indexată după mulțimea I înseamnă funcția $f : I \rightarrow M$, $f(i) = x_i$. I se numește *mulțimea 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 mulțimea $\{1, \dots, m\} \times \{1, \dots, n\}$.

Fie $(A_i)_{i \in I}$ o familie nevidă de mulțimi (adică, fiecare A_i este mulțime). Operațiile de reuniune/intersecție se pot defini pentru familii astfel

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

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

De exemplu, $\bigcup_{i=1}^n A_i = A_1 \cup \dots \cup A_n$, $\bigcup_{0 < x < 1} (0, x] = (0, 1)$ și $\bigcap_{i=1}^{\infty} (0, 1/n) = \emptyset$. Proprietățile reuniunii/intersecției din cazul a două mulțimi se extind ușor la cazul familiilor. De exemplu, o versiune generalizată a asociativității reuniunii este următoarea. Fie $((A_{i_k})_{i_k \in I_k})_{k \in K}$ o familie de familii mulțimi. Atunci

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

O versiune generalizată a distributivității intersecției față de reuniune este următoarea. Fie $(A_i)_{i \in I}$ și $(B_j)_{j \in J}$ familii de mulțimi. Atunci

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

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

Formulele lui De Morgan se exprimă astfel. Fie X o mulțime și fie $(A_i)_{i \in I}$ o familie de submulțimi 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, $x \in \overline{\bigcup_{i \in I} A_i} \Leftrightarrow x \in X \text{ și } x \notin \bigcup_{i \in I} A_i \Leftrightarrow x \in X \text{ și } x \notin A_i \text{ pentru orice } i \in I \Leftrightarrow x \in \bigcap_{i \in I} \overline{A_i}$.

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

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

Dacă A, I sunt mulțimi 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 mulțimea familiilor de elemente din A indexate după I , altfel spus, mulțimea funcțiilor $f : I \rightarrow A$. Dacă $I = \{1, \dots, n\}$, A^I se notează simplu cu A^n . În teoria axiomatică a mulțimilor, se admite următoarea axiomă:

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

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

1.4 Relații de echivalență

Fie A o mulțime nevidă. O *relație* " \sim " pe mulțimea A este o submulțime a produsului cartezian $A \times A$. Dacă $(a, b) \in \sim$, vom spune că *a este în relația \sim cu b* și vom folosi notația (mai comodă) $a \sim b$. De exemplu, $\rho = \{(1, 2)\}$ este o relație pe mulțimea $\{1, 2\}$ și $1\rho 2$. E clar că pe o mulțime cu n elemente sunt 2^{n^2} relații.

O relație \sim pe mulțimea A se numește *relație de echivalență* dacă \sim este simultan:

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

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

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

Exemple de relații de echivalență: relația de egalitate pe o mulțime nevidă, relația de paralelism pe mulțimea dreptelor din plan, relațiile de asemănare/congruență pe mulțimea triunghiurilor din plan. Relația de inegalitate \leq pe \mathbf{N} nu este relație de echivalență, nefiind simetrică. Dacă $f : A \rightarrow B$ este o funcție, atunci relația \sim_f pe A definită prin

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

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

Numim \sim_f relația de echivalență asociată lui f . De exemplu, pentru funcția $\alpha : \mathbf{R} \rightarrow \mathbf{C}$, $\alpha(x) = \cos(2\pi x) + i \sin(2\pi x)$, relația $x \sim_\alpha y$ înseamnă $x - y \in \mathbf{Z}$. Fie \sim o relație de echivalență pe mulțimea A . Dacă $a \in A$, mulțimea

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

se numește *clasa de echivalență* a elementului a . Mulțimea claselor de echivalență se numește *mulțimea factor a lui A modulo \sim* și se notează cu A/\sim . Deci $A/\sim = \{[a] \mid a \in A\}$. Surjecția

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

se numește *surjecția canonică*. Se vede că $\sim_p = \sim$. Pentru relația de egalitate pe o mulțime nevidă B , clasele de echivalență sunt submulțimile lui B cu câte un singur element. O *partiție* a unei mulțimi nevide A este o familie de submulțimi nevide disjuncte două câte două ale lui A a cărei reuniune este A . De exemplu, $(\{2n, 2n+1\})_{n \in \mathbf{Z}}$ este o partiție a lui \mathbf{Z} în timp ce $(\{n, n+1\})_{n \in \mathbf{Z}}$ și $(\{3n, 3n+1\})_{n \in \mathbf{Z}}$ nu sunt partiții.

Teorema 12 Fie \sim o relație de echivalență pe mulțimea A . Atunci

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

(b) Două clase de echivalență $[a]$ și $[b]$ sunt $\begin{cases} \text{egale} & \text{dacă } a \sim b \\ \text{disjuncte} & \text{dacă } a \not\sim b. \end{cases}$

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

(c) Mulțimea claselor de echivalență este o partiție a lui A .

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

Fie A o mulțime nevidă. Unei partiții $\mathcal{A} = (A_i)_{i \in I}$ a lui A , îi putem asocia relația pe A definită prin $x \sim_{\mathcal{A}} y \Leftrightarrow x, y$ se găsesc în același A_i . Se arată ușor că $\sim_{\mathcal{A}}$ este o relație de echivalență ale cărei clase de echivalență sunt chiar submulțimile A_i . Reciproc, dacă ρ este o relație de echivalență pe mulțimea A , atunci din teorema precedentă rezultă că A/ρ este o partiție a lui A și $\sim_{A/\rho} = \rho$. Am stabilit astfel următorul rezultat.

Teorema 13 Fie A o mulțime nevidă. Aplicațiile $\rho \mapsto A/\rho$ și $\mathcal{A} \mapsto \sim_{\mathcal{A}}$ sunt bijecții inverse una celeilalte între relațiile de echivalență pe A și partițiile lui A .

De exemplu, pe o mulțimea $\{1, 2, 3\}$ sunt cinci relații de echivalență deoarece $\{1, 2, 3\}$ are cinci partiții (vezi și exercițiul 16). Fie funcția $\alpha : \mathbf{R} \rightarrow \mathbf{C}$, $\alpha(x) = \cos(2\pi x) + i \sin(2\pi x)$. Clasele de echivalență ale relației \sim_{α} sunt submulțimile lui \mathbf{R} de forma $\{x + k \mid k \in \mathbf{Z}\}$ cu $0 \leq x < 1$. În fond, se vede ușor că pentru o funcție $f : A \rightarrow B$, clasele de echivalență ale relației \sim_f sunt submulțimile $f^{-1}(b)$ cu $b \in \text{Im}(f)$.

Fie \sim o relație de echivalență pe mulțimea A . O submulțime S a lui A se numește *sistem de reprezentanți* pentru \sim dacă S conține exact câte un element din fiecare clasă de echivalență. Deci, S este sistem de reprezentanți pentru \sim dacă și numai dacă S verifică condițiile

- (1) pentru orice $a \in A$ există $s_a \in S$ cu $a \sim s_a$, și
- (2) orice două elemente distincte ale lui S nu sunt în relația \sim .

$[0, 1)$ este un sistem de reprezentanți pentru relația \sim_{α} definită anterior. Pe mulțimea numerelor complexe (identificată cu planul complex), relația $z \sim w \Leftrightarrow |z| = |w|$ este o relație de echivalență (este chiar relația asociată funcției $d : \mathbf{C} \rightarrow \mathbf{R}$, $d(z) = |z|$). Clasele de echivalență sunt cercurile de centru 0, iar $[0, \infty)$ este un sistem de reprezentanți.

Fie n un număr natural fixat. Spunem că două numere întregi a, b sunt *congruente modulo n* și scriem $a \equiv b \pmod{n}$ dacă n divide $a - b$. Relația $\equiv \pmod{n}$ se numește *relația de congruență modulo n* pe \mathbf{Z} . De exemplu, $7 \equiv -5 \pmod{4}$ și $11 \not\equiv 4 \pmod{6}$. De asemenea, $a \equiv b \pmod{2} \Leftrightarrow a$ și b au aceeași paritate. Se vede imediat că relația de congruență modulo 0 este chiar egalitatea și că orice două numere sunt congruente modulo 1. Așadar, ne putem restrânge în cele ce urmează la cazul $n \geq 2$.

Teorema 14 Relația de congruență modulo n pe \mathbf{Z} este o relație de echivalență cu clasele de echivalență $\hat{0}, \hat{1}, \dots, \widehat{n-1}$, unde

$$\hat{r} = \{nq + r \mid q \in \mathbf{Z}\}.$$

Demonstrație. Fie $a, b \in \mathbf{Z}$. Împărțind pe fiecare cu rest la n , obținem $a = nq + r$, $b = ns + t$ cu $q, s \in \mathbf{Z}$ și $r, t \in \{0, 1, \dots, n-1\}$. Atunci $a \equiv b \pmod{n} \Leftrightarrow n \mid a - b \Leftrightarrow n \mid r - t \Leftrightarrow r = t$, deoarece $|r - t| \leq n - 1$. Așadar

$$a \equiv b \pmod{n} \Leftrightarrow a \text{ și } b \text{ dau același rest la împărțirea cu } n.$$

Cu această caracterizare se arată ușor că relația de congruență modulo n este o relație de echivalență și că are clasele de echivalență $\widehat{0}, \widehat{1}, \dots, \widehat{n-1}$. Într-adevăr, pentru $0 \leq r \leq n-1$, $\widehat{r} = \{nq+r \mid q \in \mathbf{Z}\}$ sunt exact numerele ce dau restul r la împărțirea cu n . Altfel spus, mulțimea resturilor $\{0, 1, \dots, n-1\}$ este un sistem de reprezentanți. •

Numim clasele de echivalență ale relației de congruență modulo n *clasele de resturi modulo n* , iar mulțimea lor o notăm cu \mathbf{Z}_n . Deci

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

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

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

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

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

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

$$(0, y) \approx (9, y) \text{ și } (x, 0) \approx (x, 1) \text{ pentru orice } (x, y) \in [0, 9] \times [0, 1],$$

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

Atunci mulțimea 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" și 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 Exerciții.

1. Fie M o mulțime, $A, B \subseteq M$ și fie funcția

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

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

2. Fie $f : A \rightarrow B$ o funcție. Considerăm funcțiile $f_* : \mathcal{P}(A) \rightarrow \mathcal{P}(B)$, $f^* : \mathcal{P}(B) \rightarrow \mathcal{P}(A)$, definite prin $f_*(X) = f(X)$ și $f^*(Y) = f^{-1}(Y)$. Arătați că f este injectivă (resp. surjectivă) $\Leftrightarrow f_*$ este surjectivă (resp. f^* injectivă).

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

4. Găsiți imaginea funcției $f : \mathbf{Z}^2 \rightarrow \mathbf{Z}$, $f(x, y) = x^2 - y^2$.

5. Scrieți elementele mulțimii $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$.

6. Fie $(A_n)_{n \geq 1}$ un șir mulțimi nevide finite și fie $f_n : A_{n+1} \rightarrow A_n$, $n \geq 1$, aplicații. Arătați că există un șir $(a_n)_{n \geq 1}$, $a_n \in A_n$, astfel încât $f_n(a_{n+1}) = a_n$ pentru $n \geq 1$.

7. Fie A o mulțime. Arătați că nu există o injecție $f : \mathcal{P}(A) \rightarrow A$. (Indicație: folosiți mulțimea $B = A \setminus \{f(C) \mid f(C) \in C\}$ și elementul $b = f(B)$.)

8. Fie $f : B \rightarrow A$ o funcție injectivă, unde A este o submulțime a lui B . Considerăm mulțimea $C = \{f^n(x) \mid x \in B \setminus A, n \geq 0\}$, unde $f^0(x) := x$ și $f^n = f \circ f^{n-1}$ pentru $n \geq 1$. Arătați că funcția $g : B \rightarrow A$ definită prin $g(x) = \begin{cases} f(x) & \text{dacă } x \in C \\ x & \text{dacă } x \notin C \end{cases}$ este bijectivă. Aplicație: calculați g pentru $f : [0, 1] \rightarrow [0, 1]$, $f(x) = x/2$.

9 Folosiți exercițiul precedent pentru a arăta că două mulțimi D, E sunt echipotente dacă între ele există injecții $u : D \rightarrow E$ și $v : E \rightarrow D$ (teorema Cantor-Schröder-Bernstein).

10. Fie A, B, C trei mulțimi nevide. Arătați că $(B \times C)^A \simeq B^A \times C^A$ și $(C^B)^A \simeq C^{A \times B}$.

11. (Principiul includerii și excluderii.) Fie X o mulțime finită nevidă și A_1, \dots, A_n submulțimi ale lui X . Arătați că:

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

12. Fie a, b două numere naturale, $A = \{1, 2, \dots, a\}$ și $B = \{1, 2, \dots, b\}$. Probați afirmațiile următoare.

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

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

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

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

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

(e) Numărul N_c al funcțiilor crescătoare de la A la B este C_{a+b-1}^a .

(Indicație. La (c), se numără non-surjecțiile folosind ex. 11, iar (e) se poate reduce la (d).)

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

14. Arătați că numărul permutărilor de grad n fără puncte fixe este $n!(1 - 1/1! + 1/2! - 1/3! + \dots + (-1)^n/n!)$. (Indicație. Folosiți ex. 11).

15. Pentru $n \geq 1$, fie $\varphi(n)$ numărul întregilor pozitivi $\leq n$ și primi cu n (funcția φ se numește *indicatorul lui Euler*). Arătați că

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

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

16. Numărați relațiile de echivalență pe o mulțime cu n elemente.

17. Arătați că relația de congruență modulo n este relație de echivalență folosind definiția.

18. Care dintre următoarele relații pe \mathbf{R} este relație de echivalență: (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} mulțimea relațiilor pe $\{1, 2, 3\}$. Considerăm axiomele de: (1) reflexivitate, (2) simetrie, (3) tranzitivitate, (4) antisimetrie. Calculați imaginea funcției următoare: $g : \mathcal{R} \rightarrow \{0, \dots, 15\}$, $g(\rho) = a_1 + 2a_2 + 4a_3 + 8a_4$ unde $a_i = 1$ (resp. $a_i = 0$) dacă ρ satisface (resp. nu satisface) axioma (i).

20. Fie A o mulțime infinită și F mulțimea funcțiilor $g : A \rightarrow A$. Pe F definim relația $f \sim g \Leftrightarrow$ mulțimea $D_{fg} = \{a \in A \mid f(a) \neq g(a)\}$ este finită. Arătați că \sim este o relație de echivalență.

21. Pe mulțimea \mathbf{C}^* (=planul complex fără 0) definim relația $z \sim w \Leftrightarrow z, w$ și 0 sunt coliniare. Arătați că \sim este relație de echivalență, determinați clasele de echivalență și un sistem de reprezentanți.

22. Pe mulțimea \mathbf{C} (=planul complex) definim relația $z \sim w \Leftrightarrow z - w \in \mathbf{R}$. Arătați că \sim este relație de echivalență, determinați clasele de echivalență și un sistem de reprezentanți.

23. Fie A o mulțime nevidă. Pe mulțimea H a funcțiilor de la A în A definim relația $f \sim g \Leftrightarrow$ există o bijecție $u \in H$ astfel încât $fu = ug$. Arătați că \sim este relație de echivalență.

24. (Construcția lui \mathbf{Z} .) Fie \sim relația pe $\mathbf{N} \times \mathbf{N}$ definită prin $(a, b) \sim (c, d)$ dacă $a + d = b + c$. Arătați că \sim este o relație de echivalență și că $\mathbf{N} \times \mathbf{N} / \sim$ se identifică în mod natural cu \mathbf{Z} .

25. (Construcția lui \mathbf{Q} .) Fie \sim relația pe $\mathbf{Z} \times \mathbf{N}^*$ definită prin $(a, b) \sim (c, d)$ dacă $ad = bc$. Arătați că \sim este o relație de echivalență și că $\mathbf{Z} \times \mathbf{N}^* / \sim$ se identifică în mod natural cu \mathbf{Q} .

26. (Construcția lui \mathbf{R} .) Fie \mathcal{C} mulțimea șirurilor Cauchy de numere raționale (un șir $(a_n)_{n \geq 1}$ se numește *șir 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 relația \sim definită prin $(a_n)_{n \geq 1} \sim (b_n)_{n \geq 1} \Leftrightarrow \lim_{n \rightarrow \infty} (a_n - b_n) = 0$. Arătați că \sim este o relație de echivalență și că \mathcal{C} / \sim se identifică în mod natural cu \mathbf{R} .

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

Capitolul 2

Operații algebrice, monoizi.

În acest capitol se introduce noțiunea de operație algebrică, noțiune fundamentală pentru înțelegerea tuturor capitolelor următoare. Sunt date apoi câteva proprietăți ale monoizilor.

2.1 Operații algebrice

Fie A o mulțimea nevidă. O *operație algebrică binară* $*$ pe mulțimea A (prescurtat, operație pe A) este o funcție $*$: $A \times A \rightarrow A$. Pentru comoditate, vom scrie $a * b$ în loc de $*(a, b)$. Deci, operația $*$ 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 operații pe \mathbf{R} .

Fie $*$ o operație pe mulțimea A . Operația $*$ se zice *asociativă* dacă

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

Operația $*$ se zice *comutativă* dacă

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

Un element $e \in A$ se numește *element neutru* pentru operația $*$ dacă

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

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

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

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

În acest caz, $*$ se restrânge la o operație pe H numită *operația indusă*. De exemplu, pe mulțimea \mathbf{N} , operația de adunare este asociativă, comutativă și are elementul neutru 0; în plus, $\mathbf{N} \setminus \{0, 1, 2, 4\}$ este parte stabilă. Operația de scădere pe \mathbf{Z} nu este nici asociativă nici comutativă și 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 numește *semigrup* dacă A este o mulțime nevidă și $*$ este operație asociativă pe A . Un *monoid* este un semigrup cu element neutru. A se numește *mulțimea subiacentă* a semigrupului/monoidului M . Semigrupul (monoidul) M se zice *comutativ* dacă $*$ este operație comutativă.

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

Fie B o mulțime nevidă. Pe mulțimea B^B a tuturor funcțiilor $f : B \rightarrow B$, operația de compunere determină o structură de monoid. Într-adevăr, compunerea funcțiilor este asociativă (cf. teoremei 3) și funcția identică I_B joacă rol de element neutru. Dacă B are cel puțin două elemente, monoidul B^B este necomutativ, după cum putem vedea compunând două aplicații constante diferite.

Fie $M = (A, *)$ un monoid cu elementul neutru e . Un element $a \in M$ se numește *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 $b \in A$ și $a * b = b * a = e$, atunci

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

Elementul a' se numește *inversul sau simetricul* lui a . Notăm cu $U(M)$ mulțimea elementelor inversabile ale monoidului M numită și *mulțimea unităților* lui M . Cum $e * e = e$, $e \in U(M)$.

Un monoid se numește *grup* dacă $U(M) = M$, adică orice element al său este inversabil. De exemplu, monoizii $(\mathbf{N}, +)$ și (\mathbf{Z}, \cdot) nu sunt grupuri,

deoarece $U(\mathbf{N}, +) = \{0\}$ și $U(\mathbf{Z}, \cdot) = \{1, -1\}$. Pe de altă parte, $(\mathbf{Z}, +)$ este grup; îl vom numi *grupul \mathbf{Z}* subînțelegând că operația grupală este adunarea.

Deosebim următoarele tipuri de notații. *Notăție generală*, caz în care operația 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} .

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

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

Pentru simplificarea scrierii, vom expune rezultatele teoretice referitoare la semigrupuri, monoizi și grupuri în notație multiplicativă. Concret, prin expresia “fie monoidul M ” vom înțelege că pe mulțimea nevidă M se consideră operația 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 înțelegere, cititorul e sfătuit să transcrie rezultatele în notație aditivă sau generală.

Fie M o mulțime împreună cu o operație neasociativă notată multiplicativ și 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 și ex. 30). Dacă operația este asociativă, toate cele cinci produse anterioare dau același 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 și $a_1, \dots, a_n \in M$, atunci valoarea produsului $a_1 \cdots a_n$ nu depinde de modul în care s-au pus parantezele.*

Demonstrație. Probăm afirmația prin inducție după n . Cazurile $n = 1$ și $n = 2$ sunt evidente, iar cazul $n = 3$ rezultă din asociativitate. Fie $n \geq 4$ și presupunem că afirmația a fost probată pentru produsele de lungime $< n$; deci pentru $b_1, \dots, b_k \in M$ și $k < n$, 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 inducție 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. Același rezultat se obține și 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 și $a_1, a_2, \dots, a_n \in M$ elemente permutabile două câte două. Atunci produsul $a_1 a_2 \cdots a_n$ nu depinde de ordinea factorilor.*

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

2.2 Monoizi

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

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

În particular, $U(M)$ este grup față de operația indusă.

Demonstrație. Avem

$$\begin{aligned} (a_1 a_2 \cdots a_n)(a_n^{-1} \cdots a_2^{-1} a_1^{-1}) &= (a_1 a_2 \cdots a_{n-1})(a_n a_n^{-1})(a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}) = \\ &= (a_1 a_2 \cdots a_{n-1})(a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}) = \dots = a_1 a_1^{-1} = 1. \end{aligned}$$

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 mulțimea $\mathbf{Z}_n = \{\widehat{0}, \widehat{1}, \dots, \widehat{n-1}\}$ a claselor de resturi modulo n definim o operație de adunare și una de înmulțire. Fie $\widehat{x}, \widehat{y} \in \mathbf{Z}_n$ cu $x, y \in \mathbf{Z}$. Definim $\widehat{x} + \widehat{y} = \widehat{x+y}$ și $\widehat{x}\widehat{y} = \widehat{xy}$.

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

Se verifică ușor că $(\mathbf{Z}_n, +)$ și (\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 subînțelegând că operația grupală este adunarea.

Considerăm acum monoidul (\mathbf{Z}_n, \cdot) . Atunci $U(\mathbf{Z}_n)$ este $\{\widehat{x} \mid x \in \mathbf{Z}, (x, n) = 1\}$. Într-adevăr, fie $x \in \mathbf{Z}$. Atunci $\widehat{x} \in U(\mathbf{Z}_n) \Leftrightarrow \exists y \in \mathbf{Z}$ cu $\widehat{xy} = \widehat{1} \Leftrightarrow \exists y, a \in \mathbf{Z}$ 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 $\leq n$ și primi cu n . Din teorema 17 obținem

Teorema 18 $U(\mathbf{Z}_n, \cdot) = \{\widehat{x} \mid x \in \mathbf{Z}, (x, n) = 1\}$ 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, $a \in M$ și $n \geq 1$. Definim *puterile lui a* prin: $a^0 = 1_M$, $a^n = aa \cdots a$ (n factori). Dacă a este inversabil, putem extinde definiția precedentă punând $a^{-n} = (a^{-1})^n$, $n \geq 1$. În cazul notației aditive egalitățile precedente se scriu $0a = 0_M$, $na = a + a + \cdots + a$ (n termeni), $0a = 0_M$ și $(-n)a = n(-a)$.

Teorema 19 (Reguli de calcul într-un monoid). Fie M un monoid și $a, b \in M$. (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).

Demonstrație. Pentru $m, n \geq 0$, afirmațiile sunt consecințe imediate ale definiției. 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 $m \geq 0$ și $n \leq 0$. 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 și B doi monoizi. O funcție $f : A \rightarrow B$ se numește *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 și B sunt monoizi, avem morfismele $x \mapsto 1_B : A \rightarrow B$ numit *morfismul trivial* și $I_A : A \rightarrow A$, $I_A(x) = x$, numit *morfismul identic*. $n \mapsto 2^n : (\mathbf{N}, +) \rightarrow (\mathbf{N}, \cdot)$, $x \mapsto |x| : (\mathbf{Z}, \cdot) \rightarrow (\mathbf{N}, \cdot)$ și $n \mapsto 2n : (\mathbf{N}, +) \rightarrow (\mathbf{N}, +)$ sunt exemple concrete de morfisme de monoizi.

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

Demonstrație. (a). Fie $f : A \rightarrow B$ și $g : B \rightarrow C$ 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 $f : A \rightarrow B$ este un izomorfism de monoizi. Fie $x, y \in B$ și $x' = f^{-1}(x)$, $y' = f^{-1}(y)$. 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 $f : A \rightarrow B$ un morfism de monoizi și $a \in A$. Atunci*

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

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

Demonstrație. Afirmția (a) rezultă din definiția morfismului. (b). Presupunem că $a \in U(A)$. Aplicând f șirului de egalități $aa^{-1} = a^{-1}a = 1_A$ se obține $f(a)f(a^{-1}) = f(a^{-1})f(a) = f(1_A) = 1_B$, deci $f(a) \in U(B)$ și $f(a)^{-1} = f(a^{-1})$. 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 și B sunt *izomorfi*, și scriem $A \simeq B$, dacă între ei există un izomorfism. Doi monoizi izomorfi au aceleași proprietăți monoidale, de aceea nu vom face distincție între ei. Din teorema 20, rezultă că relația de izomorfism între monoizi este reflexivă, simetrică și 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 $f : (\mathbf{N}, +) \rightarrow (\mathbf{N}^*, \cdot)$ este un izomorfism, ar rezulta că toate numerele naturale nenule sunt puteri ale lui $f(1)$.

Fie A o mulțime pe care o vom numi *alfabet* iar elementele sale *litere*. Vom numi *cuvânt* un șir finit $a_1a_2 \cdots a_n$ de litere, incluzând aici și *cuvântul vid* (cuvântul cu zero litere) notat cu \sqcup . Prin definiție, două cuvinte $a_1a_2 \cdots a_n$ și $b_1b_2 \cdots b_m$ sunt egale dacă $m = n$ și $a_1 = b_1, \dots, a_n = b_n$, adică dacă au același număr de litere și literele corespunzătoare sunt egale. Fie $W(A)$ mulțimea cuvintelor cu litere din A . Atunci $W(A)$ este monoid în raport cu operația 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 mulțimea A*. Elementul său neutru este cuvântul vid. De exemplu, dacă $B = \{b\}$, atunci $W(B) = \{\sqcup, b, bb, \dots, b^n, \dots\}$. Este clar că $W(B)$ este izomorf cu $(\mathbf{N}, +)$ prin izomorfismul $n \mapsto b^n : \mathbf{N} \rightarrow W(B)$. Dacă $D = \{a, b\}$, atunci monoidul $W(D) = \{\sqcup, a, b, ab, ba, abb, bab, aab, \dots\}$ este necomutativ, deoarece $ab \neq ba$.

Mesajul teoremei următoare este că morfismele de monoizi $W(A) \rightarrow M$ se pot defini “pe litere”. Demonstrația se face prin calcul.

Teorema 22 *Fie A o mulțime, M un monoid și $f : A \rightarrow M$ o funcție. Atunci funcția*

$$F : W(A) \rightarrow M, \quad F(a_1a_2 \cdots a_n) = f(a_1)f(a_2) \cdots f(a_n), \quad a_1, \dots, a_n \in A$$

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

2.3 Exerciții

28. Câte operații se pot defini pe o mulțime cu n elemente și câte dintre acestea sunt comutative, respectiv cu element neutru ?

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

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

32. Fie \mathcal{A} mulțimea operațiilor algebrice pe \mathbf{N} . Considerăm axiomele de: (1) asociativitate, (2) comutativitate, (3) existența elementului neutru. Calculați imaginea funcției următoare: $f : \mathcal{A} \rightarrow \{0, \dots, 7\}$, $f(\rho) = a_1 + 2a_2 + 4a_3$ unde $a_i = 1$ (resp. $a_i = 0$) dacă ρ satisface (resp. nu satisface) axioma (i). (Indicație: folosiți ex. precedent).

33. Dați exemple de operații algebrice care să arate că axiomele de asociativitate, comutativitate și de existență a elementului neutru sunt independente.

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

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

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

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

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

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

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

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

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

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

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

45. Descrieți atomii monoizilor multiplicativi $M_n = \{nk + 1 \mid k \in \mathbf{N}\}$ pentru $n = 2, 3$ și arătați că monoizii nu sunt izomorfi.

Capitolul 3

Grupuri

În acest capitol se introduc noțiunile de bază ale teoriei grupurilor: grup, morfism de grupuri, subgrup, sistem de generatori, congruențe 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, ecuația claselor de elemente conjugate și teorema lui Cauchy.

3.1 Exemple de grupuri

Reamintim că un grup este un monoid cu toate elementele inversabile. Așadar, un grup este o mulțime înzestrată cu o operație asociativă care are element neutru și astfel încât orice element este inversabil. Un grup se zice *grup abelian* sau *comutativ* dacă operația grupală este comutativă și se zice *finit* dacă mulțimea subiacentă este finită (numărul de elemente se numește *ordinul grupului*).

Mulțimile numerice \mathbf{Z} , \mathbf{Q} , \mathbf{R} și \mathbf{C} sunt grupuri abeliene în raport cu adunarea. De asemenea, \mathbf{Q}^* , \mathbf{R}^* și \mathbf{C}^* sunt grupuri abeliene în raport cu înmulțirea.

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

Conform teoremei 17, unitățile unui monoid formează grup în raport cu operația indusă. De exemplu, dacă A este o mulțime, mulțimea A^A a

funcțiilor de la A la A este monoid față de compunerea funcțiilor. $U(A^A)$ este grupul bijecțiilor $A \rightarrow A$, numit *grupul permutărilor mulțimii A* , grup notat cu S_A . Dacă $A = \{1, \dots, n\}$, S_A se notează mai simplu S_n și se numește *grupul permutărilor de grad n* .

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

Dacă G, H sunt grupuri, produsul cartezian $G \times H$ devine grup față de operația de “înmulțire pe componente” $(a, b)(a', b') := (aa', bb')$ pentru $a, a' \in G$ și $b, b' \in H$. Acest grup se numește *produsul direct al grupurilor G și 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 numește *grupul lui Klein*.

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

Se numește *izometrie* a planului euclidian \mathbf{R}^2 o funcție $f : \mathbf{R}^2 \rightarrow \mathbf{R}^2$ care păstrează distanțele, 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 și că mulțimea izometriilor $Izo(\mathbf{R}^2)$ este un grup față de compunere (vezi [3, pag. 213]). Orice izometrie este o translație, rotație, simetrie (față de o dreaptă) sau compunerea dintre o translație și o simetrie; în plus, orice izometrie se poate obține compunând cel mult trei simetrii (vezi [3, pag. 216]).

Fie acum o submulțime 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 $Sim(Y)$ și numit *grupul de simetrie al lui Y* . Într-adevăr, fie $f, g \in Sim(Y)$. Atunci $f(Y) = Y$ și $g(Y) = Y$, deci $g^{-1}(Y) = Y$ și rezultă că $(fg^{-1})(Y) = Y$.

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

Fie P un pătrat. $Sim(P)$ constă din transformarea identică, rotațiile de $\pi/2$, π , $3\pi/2$ radiani în jurul centrului pătratului și cele patru simetrii

față de mediatoarele laturilor și diagonale. Grupul este neabelian deoarece, de exemplu, simetriile față de diagonale nu comută. El este numit *grupul diedral al pătratului* și este notat cu D_4 (vezi și ex. 56).

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

3.2 Morfisme de grupuri

Fie G și H două grupuri. O funcție $f : G \rightarrow H$ se numește *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 $e^2 = e = e1_H$ și, prin amplificare la stânga cu e^{-1} , rezultă $e = 1_H$. Rezultă că $f(1_G) = 1_H$, deci f este și morfism de monoizi. Un morfism de grupuri bijectiv se numește *izomorfism de grupuri*. Un *automorfism* este un izomorfism de la un grup în el însuși.

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

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

Demonstrație. Rezultă din afirmațiile corespunzătoare pentru morfismele de monoizi (teorema 20). •

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

Se vede că dacă $f : G \rightarrow H$ 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 distincție între două grupuri izomorfe. De exemplu, fiecare dintre grupurile izomorfe $(\{\pm 1\} \times \{\pm 1\}, \cdot)$ și $(\mathbf{Z}_2 \times \mathbf{Z}_2, +)$ va fi numit grupul lui Klein.

Din teorema anterioară, rezultă că relația de izomorfism între grupuri este reflexivă, simetrică și tranzitivă.

O problemă importantă în teoria grupurilor finite este descrierea tuturor tipurilor de grupuri cu un număr dat n de elemente. Se poate vedea ușor că pentru $1 \leq n \leq 3$ există câte un singur tip de grup. Fie grupurile cu 4 elemente \mathbf{Z}_4 și $K = (\{\pm 1\}^2, \cdot)$ (grupul lui Klein). Se poate vedea că grupurile nu sunt izomorfe deoarece pentru orice $x \in K$ avem $x^2 = (1, 1)$, dar $2 \cdot 1 \neq \hat{0}$. 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 și anume \mathbf{Z}_p (vezi corolarul 46).

3.3 Subgrupuri

Fie G un grup. O submulțime nevidă H a lui G se numește *subgrup*, și 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 $xy \in H$ și $x^{-1} \in H$. Rezultă atunci că H este grup față de operația indusă. Într-adevăr, asociativitatea se transmite imediat la H , $1 \in H$ deoarece, dacă $y \in H$, atunci $y^{-1} \in H$ și $1 = yy^{-1}$, și orice element din H este inversabil. Printre subgrupurile lui G se găsesc $\{1\}$ numit *subgrupul trivial* și G numit *subgrupul impropriu*.

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

Demonstrație. Implicația directă este imediată: dacă $x, y \in H$, atunci $y^{-1} \in H$ și deci $xy^{-1} \in H$. Reciproc, să presupunem că $xy^{-1} \in H$ pentru orice $x, y \in H$. Cum H este nevidă, există $z \in H$ și 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 $Z(G) := \{a \in G \mid ax = xa \text{ pentru orice } x \in G\}$ este un subgrup al lui G numit *centrul lui G* . Într-adevăr, fie $a, b \in Z(G)$ și $x \in G$. Atunci $ax = xa$ și $bx = xb$, deci $abx = axb = xab$ și $a^{-1}x = xa^{-1}$, așadar $ab, a^{-1} \in H$.

Dacă $n \geq 1$, $U_n = \{z \in \mathbf{C} \mid z^n = 1\}$ 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 $n\mathbf{Z}$ mulțimea multiplilor întregi ai lui n , adică $n\mathbf{Z} = \{nk \mid k \in \mathbf{Z}\}$.

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

Demonstrație. Faptul că $n\mathbf{Z}$ este un subgrup al lui $(\mathbf{Z}, +)$ rezultă din faptul că diferența 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 și 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 $h \in H$ și fie $h = nq + r$, $q, r \in \mathbf{Z}$, $0 \leq r < n$ împărțirea 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 $h = nq \in n\mathbf{Z}$. •

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

Demonstrație. Dacă $x, y \in H \cap K$, atunci $x, y \in H$ și $x, y \in K$, deci $xy^{-1} \in H \cap K$. Afirmatia generală se probează analog. •

Teorema 27 *Fie $f : G \rightarrow G'$ 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 și f este injectiv $\Leftrightarrow \ker(f) = \{1\}$.*

Demonstrație. (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 $f(x), f(y) \in H'$ și $f(xy^{-1}) = f(x)f(y)^{-1} = f(x)f(y^{-1}) \in H'$. 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 $\ker(f) = \{1\}$ și 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 $f : \mathbf{Z}^2 \rightarrow \mathbf{Z}$, $f(x, y) = x - y$ este $\{(x, x) \mid x \in \mathbf{Z}\}$.

3.4 Subgrupul generat de o mulțime

Fie G un grup și A o submulțime a lui G . *Subgrupul lui G generat de A* este prin definiție

$$\langle A \rangle := \{a_1^{\pm 1} a_2^{\pm 1} \cdots a_n^{\pm 1} \mid a_1, \dots, a_n \in A, n \geq 0\}$$

altfel zis, mulțimea tuturor produselor de elemente din A și inverse ale acestora. Facem convenția ca un produs vid să însemne 1. E clar că $A \subseteq \langle A \rangle$. Se observă că $\langle \emptyset \rangle = \{1\}$ și $\langle G \rangle = G$. Dacă $a \in G$, atunci $\langle a \rangle = \{a^k \mid k \in \mathbf{Z}\}$. 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 și A o submulțime a sa. Atunci $\langle A \rangle$ este un subgrup al lui G conținut în orice subgrup al lui G care conține pe A (adică, $A \subseteq H \leq G$ implică $\langle A \rangle \subseteq H$).*

Demonstrație. Din definiția lui $\langle A \rangle$ rezultă că $\langle A \rangle$ este parte stabilă a lui G și că $1 \in \langle A \rangle$. Fie $x \in \langle A \rangle$. Atunci $x = a_1^{e_1} \cdots a_n^{e_n}$ cu $a_1, \dots, a_n \in A$, $e_1, \dots, e_n \in \{\pm 1\}$ și $n \geq 0$. Atunci $x^{-1} = a_n^{-e_n} \cdots a_1^{-e_1} \in \langle A \rangle$. Fie H un subgrup al lui G ce conține pe A . Dacă $x_1, \dots, x_n \in A$, atunci $x_1^{\pm 1} x_2^{\pm 1} \cdots x_n^{\pm 1} \in H$, din definiția subgrupului. Deci $\langle A \rangle \subseteq H$. •

Corolarul 29 *Fie G un grup și A o submulțime a lui G . Atunci subgrupul generat de A este intersecția tuturor subgrupurilor lui G care conțin pe A , adică*

$$\langle A \rangle = \bigcap_{A \subseteq H \leq G} H.$$

Expresia lui $\langle A \rangle$ din corolarul precedent poate fi luată drept definiție a lui $\langle A \rangle$.

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

$$\langle a_1, \dots, a_n \rangle = \{a_1^{k_1} \cdots a_n^{k_n} \mid k_1, \dots, k_n \in \mathbf{Z}\}.$$

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

Corolarul 31 Fie a, b, d, m numere naturale. Atunci

(a) $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z} \Leftrightarrow d = \text{cmmdc}(a, b)$.

(b) $a\mathbf{Z} \cap b\mathbf{Z} = m\mathbf{Z} \Leftrightarrow m = \text{cmmmc}(a, b)$.

Demonstrație. (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 și b . Fie f un divizor comun al lui a și b . Atunci $a, b \in f\mathbf{Z}$, deci $d\mathbf{Z} = a\mathbf{Z} + b\mathbf{Z} \subseteq f\mathbf{Z}$, și rezultă că f divide d . Afirmația (b) se probează analog. •

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

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

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

3.5 Congruențe modulo un subgrup

Conform teoremei 25, subgrupurile lui $(\mathbf{Z}, +)$ sunt submulțimile $n\mathbf{Z}$ 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 observație permite extinderea noțiunii de congruență la grupuri arbitrare. Fie G un grup și H un subgrup al lui G . Pe G definim următoarele relații: $x \equiv_s y(H) \Leftrightarrow x^{-1}y \in H$ numită *congruența la stânga modulo H* și $x \equiv_d y(H) \Leftrightarrow xy^{-1} \in H$ numită *congruența la dreapta modulo H* .

Teorema 32 *Fie G un grup și H un subgrup al lui G . Atunci cele două congruențe modulo H sunt relații de echivalență pe G . Clasele de echivalență ale congruenței la stânga sunt submulțimile lui G de forma $xH = \{xh \mid h \in H\}$ cu $x \in G$, numite clase la stânga modulo H . Clasele de echivalență ale congruenței la dreapta sunt submulțimile lui G de forma $Hx = \{hx \mid h \in H\}$ cu $x \in G$, numite clase la dreapta modulo H .*

Demonstrație. Demonstrăm afirmațiile doar pentru congruența la stânga modulo H , cele pentru congruența 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 $x \equiv_s y(H)$ și $y \equiv_s z(H)$. Rezultă că $x^{-1}y \in H$ și $y^{-1}z \in H$. Deci $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$, adică $x \equiv_s z(H)$. Am verificat așadar că $\equiv_s(H)$ este reflexivă, simetrică și tranzitivă. Clasa de echivalență 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. $(G/H)_d$) mulțimea claselor la stânga (resp. la dreapta) modulo H . Cele două relații de congruență coincid dacă și numai dacă au aceleași clase de echivalență, adică, dacă și 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, mulțimea $(G/H)_s = (G/H)_d$ se notează mai simplu cu G/H .

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

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

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

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

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

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

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

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

În particular, $|H|$ divide $|G|$.

Demonstrație. Fie C_1, \dots, C_s clasele la stânga modulo H . Conform definiției, $s = [G : H]$. Fie $a \in G$. Aplicația $x \mapsto ax : H \rightarrow aH$ este o bijecție cu inversa $y \mapsto a^{-1}y$. Deci $|C_i| = |H|$ pentru $i = 1, \dots, s$. Cum C_1, \dots, C_s este o partiție 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 și x un element al lui G . Ordinul lui x se definește prin

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

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

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

Demonstrație. 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 $k = nq + r$, $q, r \in \mathbf{Z}$, $0 \leq r < n$ împărțirea 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. definiției ordinului. •

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

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

Se vede că $\text{ord}(\theta_1) = n$. Mai general, $\text{ord}(\theta_k) = n/(k, n)$, unde $d = (k, n)$ este cmmdc al lui k și 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 și x un element al lui G . Atunci ordinul lui x este egal cu ordinul subgrupului generat de x .

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

Presupunem acum că $\text{ord}(x) = n < \infty$. Fie $k \in \mathbf{Z}$ și fie $k = nq + r$, $q, r \in \mathbf{Z}$, $0 \leq r < n$ împărțirea cu rest a lui k la n . Atunci $x^k = x^{nq+r} = (x^n)^q x^r = x^r$. Deci $\langle x \rangle = \{1, x, \dots, x^{n-1}\}$. 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 $1 \leq k-h \leq n-1$, contradicție, deoarece $\text{ord}(x) = n$. •

Corolarul 37 Fie G un grup finit cu n elemente și $x \in G$. Atunci $\text{ord}(x)$ divide n și $x^n = 1$.

Demonstrație. $\text{ord}(x) = |\langle x \rangle|$ divide G , cf. teoremei lui Lagrange. •

Reamintim că indicatorul lui Euler este funcția $\varphi : \mathbf{N}^* \rightarrow \mathbf{N}^*$, $\varphi(n) =$ 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 $U(\mathbf{Z}_n) = \{\bar{b} \in \mathbf{Z}_n \mid (b, n) = 1\}$. Aplicând corolarul precedent se obține

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

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

În cazul când n este număr prim se obține

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

$$a^{p-1} \equiv 1 \pmod{p}.$$

3.7 Subgrupuri normale

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

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

Demonstrație. \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 raționamentul pentru x^{-1} , se obține $Hx \subseteq xH$, deci $xH = Hx$. •

$H = \{I, (12)\}$ 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 $f : G \rightarrow G'$ 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.

Demonstrație. (a). Fie $x \in G$ și $y \in \ker(f)$. Atunci $f(xy x^{-1}) = f(x)f(y)f(x)^{-1} = f(x)f(x)^{-1} = 1$, deci $xy x^{-1} \in \ker(f)$.

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

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

3.8 Grupul factor

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

Operația este bine-definită, adică nu depinde de reprezentanții claselor. Într-adevăr, fie $x', y' \in G$ cu $\hat{x} = \hat{x}'$ și $\hat{y} = \hat{y}'$. Atunci $h = x^{-1}x'$ și $y^{-1}y'$ aparțin 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 și H un subgrup normal al lui G . Atunci în raport cu operația definită anterior G/H este grup numit grupul factor G modulo H . În plus, surjecția canonică $\pi : G \rightarrow G/H$ este morfism de grupuri.*

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

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 $S_3/A_3 = \{\hat{I}, \widehat{(12)}\}$ cu $\widehat{(12)}^2 = \hat{I}$.

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

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

Demonstrație. 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 funcția \bar{u} este bine-definită. Evident, \bar{u} este surjectivă. Fie $y, z \in G$. Atunci

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

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

Morfismul de grupuri $f : (\mathbf{R}, +) \rightarrow (\mathbf{C}^*, \cdot)$, $f(x) = \cos(2\pi x) + i \sin(2\pi x)$, are imaginea $U = \{z \in \mathbf{C} \mid |z| = 1\}$ (cercul unitate) și 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} și orice grup ciclic cu n elemente este izomorf cu \mathbf{Z}_n .*

Demonstrație. Fie $G = \langle a \rangle$ un grup ciclic. Considerăm morfismul surjectiv de grupuri $f : \mathbf{Z} \rightarrow G$, $f(k) = a^k$. Dacă G este infinit, rezultă că f este izomorfism. Presupunem acum că G are n elemente. Din teoremele 35 și 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.*

Demonstrație. E clar că un grup factor al unui grup ciclic este ciclic (dacă G este generat de a , atunci G/H este generat de \hat{a}). Conform teoremei anterioare, este suficient să demonstrăm afirmația referitoare la subgrupuri pentru grupurile \mathbf{Z} și \mathbf{Z}_n . În cazul \mathbf{Z} se aplică teorema 25. Considerăm cazul \mathbf{Z}_n . Fie $\pi : \mathbf{Z} \rightarrow \mathbf{Z}_n$ 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 conține pe $\ker(\pi) = n\mathbf{Z}$, deci $\pi^{-1}(H) = k\mathbf{Z}$ cu k divizor al lui n . Cum π este surjecție, avem $H = \pi(\pi^{-1}(H)) =$ subgrupul generat de \hat{k} . •

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

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

3.10 Grupul permutărilor S_n

Fie A o mulțime nevidă. Reamintim că S_A este grupul permutărilor mulțimii A , grup față de compunerea permutărilor. Dacă A și B sunt două mulțimi echipotente, atunci grupurile S_A și S_B sunt izomorfe, cf. exercițiului 53.

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

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

Grupul S_n este abelian dacă și numai dacă $n \leq 2$, deoarece S_1 și 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 .

Demonstrație. 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 aplicația $t_g : G \rightarrow G$, $t_g(x) = gx$. Dacă $g, h, x \in G$, atunci $(t_g t_h)(x) = ghx = t_{gh}(x)$. În particular, t_g este bijecție deoarece $t_g t_{g^{-1}} = I_G$. Aplicația $T : G \rightarrow S_G$, $T(g) = t_g$, este un morfism injectiv de grupuri. Într-adevăr, $T(g)T(h) = t_g t_h = t_{gh} = T(gh)$ și $\ker(T) = \{g \mid t_g = I_G\} = \{1\}$. Deci G este izomorf cu subgrupul $\text{Im}(T)$ al lui S_G . •

Morfismul injectiv T se numește *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 și β sunt *disjuncte* dacă pentru orice $i \in \{1, \dots, n\}$ rezultă $\alpha(i) = i$ sau $\beta(i) = i$. În particular, ciclurile (a_1, \dots, a_k) , (b_1, \dots, b_l) sunt disjuncte $\Leftrightarrow \{a_1, \dots, a_k\} \cap \{b_1, \dots, b_l\} = \emptyset$.

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 $\alpha^p = \beta^p = I$.

Demonstrație. (1), (2). Putem presupune că $\alpha, \beta \neq I$. Fie $i \in \{1, \dots, n\}$. Dacă $\alpha(i) = \beta(i) = i$, atunci $(\alpha\beta)(i) = i = (\beta\alpha)(i)$. Presupunem că $j = \alpha(i) \neq i$. Cum α este injecție, rezultă că $\alpha(j) \neq j$. Deoarece α, β sunt permutări disjuncte, $\beta(i) = i$ și $\beta(j) = j$. Deci $(\alpha\beta)(i) = \alpha(i) = j = \beta(j) = (\beta\alpha)(i)$. Rezultă și 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 $\beta(i) = i$ și $\beta^t(i) = i$. (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.

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

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

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

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.*

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

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

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

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

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

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

Demonstrație. Cum σ este bijectie, avem

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

Deci

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

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 transpoziția (12) este impară deoarece are o singură inversiune și anume $(1, 2)$.

Fie A_n mulțimea permutărilor pare din S_n .

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

Demonstrație. 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 obținem $S_n/A_n \simeq \{\pm 1\}$, deci $n! = |S_n| = |A_n||S_n/A_n| = 2|A_n|$. •

Așadar, produsul a două permutări de aceeași paritate este o permutare pară iar produsul a două permutări de parități diferite este o permutare impară.

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

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

3.11 Ecuația claselor

Fie G un grup și $x, y \in G$. Spunem că x, y sunt *conjugate* (notație $x \sim y$), dacă există $a \in G$ astfel încât $x = aya^{-1}$. Relația de conjugare este o relație

de echivalență. Într-adevăr, fie $x, y, z, a, b \in G$. Atunci $x = 1 \cdot x \cdot 1^{-1}$, $x = aya^{-1}$ implică $y = a^{-1}y(a^{-1})^{-1}$, și $x = aya^{-1}$ și $y = bzb^{-1}$ implică $x = abz(ab)^{-1}$.

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

Fie G un grup finit și $x \in G$. E ușor de văzut că $C(x) := \{a \in G \mid ax = xa\}$ este un subgrup al lui G numit *centralizatorul lui x* . Două elemente axa^{-1} și 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 partiție a lui G , rezultă că am demonstrat

Teorema 54 (Ecuația claselor de elemente conjugate). *Fie G un grup finit și fie x_1, \dots, x_n un sistem de reprezentanți pentru clasele de conjugare netriviale. Atunci*

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

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

Demonstrație. Facem inducție 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 $x \in G \setminus \{1\}$ și fie $H = \langle x \rangle$. 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 și $|G/H| < |G|$. Conform inducției, 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 $p = \text{ordinul lui } \hat{y} \text{ divide } na$, contradicție; deci $z \neq 1$. Pe de altă parte $z^p = (y^p)^{na} = 1$ deoarece $y^p \in H$ și $|H| = n$.

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 ecuația 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 inducția.

3.12 Exerciții

46. Arătați că un grup G în care $x^2 = 1$ pentru orice $x \in G$ este abelian.
47. Întocmiți tabla grupului lui Klein $\mathbf{Z}_2 \times \mathbf{Z}_2$.
48. Întocmiți tabla grupului permutărilor S_3 în funcție de $a = (123)$ și $b = (12)$.
49. Arătați că un grup cu 4 elemente este izomorf cu \mathbf{Z}_4 sau cu grupul lui Klein $\mathbf{Z}_2 \times \mathbf{Z}_2$. (Indicație: folosiți teorema lui Lagrange).
50. Fie G un grup și $a, b \in G$ elemente de ordin finit m resp. n . Presupunem că $ab = ba$ și că $(m, n) = 1$. Arătați că ab are ordinul mn .
51. Arătați că un grup cu 6 elemente este izomorf cu \mathbf{Z}_6 sau cu S_3 . (Indicație: folosiți teorema lui Cauchy).
52. Arătați 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. Arătați că dacă A și B sunt două mulțimi echipotente, atunci grupurile de permutări S_A și S_B sunt izomorfe.
54. Pe mulțimea $(-1, 1)$ considerăm operația $x * y = (x + y)/(1 + xy)$. Arătați că $((-1, 1), *)$ este un grup izomorf cu $((0, \infty), \cdot)$.
55. Fie G semigrupul cu tabla de înmulțire

\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) Arătați că G este grup neabelian generat de $\{a, d\}$.
- (b) Determinați clasele de conjugare și centrul lui G .
- (c) Determinați ordinul elementelor lui G .
- (d) Determinați subgrupurile (normale) ale lui G .
- (e) Arătați că $G / \langle b \rangle$ este izomorf cu grupul lui Klein.

56. Arătați că grupul G din exercițiul anterior este izomorf cu grupul diedral D_4 .

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

58. Arătați 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 înmulțirea definită prin $ij = k, ji = -k, jk = i, kj = -i, ki = j, ik = -j$ și $i^2 = j^2 = k^2 = -1$. Determinați subgrupurile lui Q și arătați că toate sunt subgrupuri normale. Q este numit *grupul cuaternionilor*.

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

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

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

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

64. Găsiți două grupuri neizomorfe G și H astfel încât există morfisme injective $G \rightarrow H$ și $H \rightarrow G$.

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

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

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

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

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

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

(c) Arătați că G nu este finit generat.

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

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

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

72. Descrieți morfismele de grupuri $\mathbf{Z}[X] \rightarrow \mathbf{Z}$.

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

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

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

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

- (a) dacă $a, b \in \mathbf{N}^*$ sunt prime între ele, atunci $\text{ord}(\widehat{a/b}) = b$,
- (b) orice subgrup finit generat este ciclic finit,
- (c) G nu este finit generat.

77. Determinați morfismele între grupurile aditive \mathbf{Z}_m și \mathbf{Z}_n .

78. Arătați că grupurile factor $(\mathbf{R}, +)/\mathbf{Z}$ și $(\mathbf{R}, +)/\langle \sqrt{2}, \sqrt{3} \rangle$ nu sunt izomorfe.

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

80. Fie G grupul aditiv al șirurilor de numere reale și H subgrupul lui G format din șirurile cu un număr finit de termeni nenuli. Arătați că G/H nu este izomorf cu G .

81. Arătați că automorfismele unui grup formează grup față de compunere și că grupul automorfismelor grupului lui Klein este izomorf cu S_3 .

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

83. Scrieți subgrupurile lui \mathbf{Z}_{12} și calculați grupurile factor ale lui \mathbf{Z}_{12} .

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

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

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

87. Calculați signatura și ordinul elementelor lui S_5 .

88. Determinați morfismele de grupuri $S_3 \rightarrow \{\pm 1, \cdot\}$.

89. Calculați elementele subgrupului D generat de (1234) și (13) în S_4 .

90. Calculați elementele subgrupului H generat de $(1234)(5678)$ și $(1537)(2846)$ în S_8 și arătați că H este izomorf cu grupul cuaternionilor (vezi ex. 59).

91. Arătați că S_n este generat de (a) transpozițiile $(12), (13), \dots, (1n)$, (b) transpozițiile $(12), (23), \dots, (n-1, n)$, (c) (12) și $(12\dots n)$.

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

93. Arătați că S_5 este generat de orice transpoziție și un ciclu de lungime 5.

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

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

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

97. Găsiți 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 $A = \{z \in \mathbf{C} \mid |z - i| \leq 1, \operatorname{Re}(z) \geq 0\}$ și fie $B = A \cup iA \cup -A \cup -iA$. Calculați grupul de simetrie al lui B .

99. Fie G grupul rotațiilor spațiului euclidian care invariază un tetraedru regulat. Descrieți elementele lui G și arătați că G este izomorf cu A_4 .

100. Fie G grupul rotațiilor spațiului euclidian care invariază un cub. Descrieți elementele lui G și arătați că G este izomorf cu S_4 .

101. Arătați că grupul G al rotațiilor spațiului euclidian care invariază un dodecaedru regulat are ordinul 60 și este izomorf cu A_5 .

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

Capitolul 4

Inele

În acest capitol se introduc noțiunile de bază ale teoriei inelelor: inel, corp, morfism de inele, subinel, ideal, sistem de generatori, caracteristica unui inel, inel factor. Se prezintă construcția inelelor de matrice, a inelelor de polinoame și construcția corpului cuaternionilor. Se demonstrează teoreme importante referitoare la aceste noțiuni și construcții.

4.1 Inel, subinel, ideal

Un *inel* este un triplet $(A, +, \cdot)$ format dintr-o mulțime nevidă A și două operații pe A , prima notată cu $+$ numită *adunare*, a doua notată cu \cdot numită *înmulțire*, astfel încât

- (1) $(A, +)$ este grup abelian
- (2) (A, \cdot) este monoid, și
- (3) înmulțirea este distributivă față de adunare, adică $a(b + c) = ab + ac$ și $(b + c)a = ba + ca$ pentru orice $a, b, c \in A$.

Elementul neutru al adunării se notează cu 0 și se numește *elementul nul*. Opusul unui element $a \in A$ (față de adunare) se notează cu $-a$. Elementul neutru al înmulțirii se notează cu 1 și se numește *elementul unitate*. Un element $a \in A$ se zice *inversabil* dacă este inversabil față de înmulțire; inversul său se notează cu a^{-1} . Mulțimea elementelor inversabile (încă zisă a unităților) lui A se notează cu $U(A)$. Inelul $\{0\}$ se numește inelul nul. Un inel se numește *inel comutativ* dacă înmulțirea este comutativă. Un inel nenul se numește *corp* dacă orice element nenul este inversabil. Grupul $(A, +)$ se numește *grupul aditiv subiacent al lui A*. Spunem că inelul A are divizori ai

lui zero dacă există $x, y \neq 0$ cu $xy = 0$.

\mathbf{Z} , \mathbf{Q} , \mathbf{R} , \mathbf{C} sunt inele comutative față de operațiile uzuale de adunare și înmulțire, ultimele trei fiind chiar corpuri. E clar că $U(\mathbf{Z}) = \{\pm 1\}$.

$\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$ 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 și $m, n \geq 1$. O *matrice cu m linii și 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}) . $a_{11}, a_{12}, \dots, a_{mn}$ se numesc *elementele matricei*. Matricea poate fi gândită ca fiind funcția $(i, j) \mapsto a_{ij} : \{1, \dots, m\} \times \{1, \dots, n\} \rightarrow R$. Dacă $m = n$, matricea se numește *matrice pătratică de ordinul n* . Vom nota cu $M_{m,n}(R)$ (resp. $M_n(R)$) mulțimea matricelor de tip (m, n) (resp. pătratice de ordinul n) cu elemente din R . Două matrice $A = (a_{ij})$ și $B = (b_{ij})$ sunt egale dacă sunt de același tip (m, n) și $a_{ij} = b_{ij}$ pentru $1 \leq i \leq m, 1 \leq j \leq n$. Așadar, $A = B$ dacă și numai dacă A și B privite ca funcții $\{1, \dots, m\} \times \{1, \dots, n\} \rightarrow R$ sunt egale.

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

Între anumite matrice se definește o operație de înmulțire. Fie $m, n, p \geq 1$. Fie $A = (a_{ij}) \in M_{m,n}(R)$ și $B = (b_{jk}) \in M_{n,p}(R)$. *Produsul AB* este prin definiție matricea $C = (c_{ik}) \in M_{m,p}(R)$ cu elementele $c_{ik} = \sum_{j=1}^n a_{ij}b_{jk}$. Așadar, 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 înmulțire se mai numește și “linii pe coloane”.

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

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

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

Fie $n \geq 1$. 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 numește *matricea unitate* de ordinul n . Dacă $A = (a_{ij}) \in M_{m,n}(R)$, atunci $AI_n = A$ și $I_n A = A$. 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 și $n \geq 1$. Față de operațiile de adunare și înmulțire ale matricelor, $M_n(R)$ este un inel numit inelul matricelor pătratice de ordinul n cu elemente din R . Dacă $n \geq 2$, inelul $M_n(R)$ este necomutativ și are divizori ai lui zero.*

Demonstrație. Faptul că $M_n(R)$ este un inel rezultă din proprietățile demonstrate anterior. Egalitățile

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

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

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

Date două inele B, C , produsul cartezian $B \times C$ împreună cu operațiile de adunare și înmulțire definite pe componente (adică, $(b_1, c_1) + (b_2, c_2) = (b_1 + b_2, c_1 + c_2)$, $(b_1, c_1)(b_2, c_2) = (b_1 b_2, c_1 c_2)$) este un inel numit *produsul direct* al inelelor B și C . Construcția produsului direct de inele se poate generaliza ușor pentru familii arbitrare de inele. De exemplu, $\mathbf{Z}^{\mathbf{N}}$ este inelul șirurilor 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 $n \geq 1$ și $a_1, \dots, a_k \in A$ astfel încât $a_i a_j = a_j a_i$ pentru orice i, j , atunci

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

Demonstrație. (1) Din $0 + 0 = 0$ se obține $a0 + a0 = a0$, deci, adunând $-a0$, rezultă $a0 = 0$. (2) $ab + a(-b) = a(b - b) = a0 = 0$, deci $a(-b) = -ab$. (3) Ținem seama de distributivitate și de comutativitatea elementelor a_i . Evaluăm produsul $(a_1 + \dots + a_k)^n$ desfășcând cele n paranteze și grupând monoamele asemenea. Fie $n_1, \dots, n_k \geq 0$ cu $n_1 + \dots + n_k = n$. Pentru a obține monomul $a_1^{n_1} a_2^{n_2} \dots a_k^{n_k}$ luăm a_1 din n_1 paranteze, și 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, ș.a.m.d. Deci monomul $a_1^{n_1} a_2^{n_2} \dots a_k^{n_k}$ apare de t ori, unde

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

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

Fie A un inel. Un element $a \in A$ se numește *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 $ab = 1$ și $xa = 0$ 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 numește *inel integru*. Un inel nenul comutativ integru se numește *domeniu (de integritate)*. Corpurile sunt inele integrale. \mathbf{Z} și $\mathbf{Z}[i]$ 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.*

Demonstrație. Fie a un non-divizor al lui zero al inelului finit A . Atunci aplicația $f : A \rightarrow A$, $f(x) = ax$ 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 față de operațiile de adunare și înmulțire definite după teorema 17. Într-adevăr, dacă $a, b \in \mathbf{Z}$, atunci $\widehat{a(\widehat{b} + \widehat{c})} = a(\widehat{b} + \widehat{c}) = \widehat{ab} + \widehat{ac} = \widehat{ab} + \widehat{ac}$. Îi vom spune simplu *inelul* \mathbf{Z}_n . Notăm cu $Z(\mathbf{Z}_n)$ mulțimea divizorilor lui zero din \mathbf{Z}_n .

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

Demonstrație. Primele două egalități rezultă din teoremele 18 și 58. În consecință, \mathbf{Z}_n este corp $\Leftrightarrow U(\mathbf{Z}_n, \cdot) = \mathbf{Z}_n \setminus \{\widehat{0}\} \Leftrightarrow$ numerele neprime cu n se divid cu $n \Leftrightarrow n$ este număr prim. •

Fie A un inel. O submulțime nevidă B a lui A se numește *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 înmulțirea, adică $xy \in A$ pentru orice $x, y \in A$, și
- (iii) $1 \in B$.

Dacă B este subinel al lui A , atunci B este inel față de operațiile de adunare și înmulțire induse de pe A . De exemplu, mulțimea $\mathbf{Z}_{(2)}$ a fracțiilor a/b cu a, b numere întregi și b impar este un subinel al lui \mathbf{Q} .

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

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

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

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

Dacă un ideal stâng sau drept I conține 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 și numai dacă idealele sale stângi (resp. drepte) sunt $\{0\}$ și A .*

Demonstrație. Dacă A este corp, atunci orice ideal I nenul conține un element inversabil, deci $I = A$. Reciproc, să presupunem că idealele stângi ale lui A sunt $\{0\}$ și A , și 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 inel comutativ orice ideal stâng este ideal drept și reciproc, motiv pentru care în acest caz vom spune simplu *ideal*.

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

Demonstrație. Facem demonstrația pentru o familie $(I_\alpha)_\alpha$ de ideale drepte, celelalte cazuri fiind similare. Fie $x, y \in \cap_\alpha I_\alpha$ și $a \in A$. 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 $n \geq 0$.*

Demonstrație. 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 $x \in n\mathbf{Z}$ și $a \in \mathbf{Z}$ 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 și X o submulțime a lui A . Mulțimea

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

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

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

Presupunem că A este inel comutativ. Atunci $AX = XA = AXA$ se numește *idealul generat de X* . Vom nota idealul generat de o mulțime $\{x_i\}_{i \in I} \subseteq A$ 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 $Ax = \{ax \mid a \in A\}$ se numește *idealul principal generat de x* . Un ideal se zice *finit generat* dacă poate fi generat de o mulțime 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 șirurilor de numere întregi, șirurile 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 și B două inele. O funcție $f : A \rightarrow B$ se numește *morfism de inele* dacă $f(x + y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$ pentru orice $x, y \in A$ și

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

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

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

Nu există morfisme de inele $\mathbf{Q} \rightarrow \mathbf{Z}$, deoarece singurul morfism de grupuri $(\mathbf{Q}, +) \rightarrow (\mathbf{Z}, +)$ 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 $f : A \rightarrow B$ un morfism de inele. Dacă $a \in U(A)$, atunci $f(a) \in U(B)$ și $f(a)^{-1} = f(a^{-1})$.*

Demonstrație. Se aplică teoremele 20 și 21. •

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

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

Fie $f : A \rightarrow B$ un morfism injectiv de inele. Atunci f stabilește un izomorfism între A și $Im(f)$. 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 $f : A \rightarrow B$ 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 și f este injectiv $\Leftrightarrow \ker(f) = \{0\}$.

(d) Dacă A este corp și 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 $a \in A$ și $x \in f^{-1}(J)$. Atunci $f(x) \in J$ și $f(ax) = f(a)f(x) \in J$. 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 $\{0\}$ și 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, $m, n \geq 1$, $b \in R$ și $A = (a_{ij}) \in M_{m,n}(R)$. Prin definiție, produsul bA dintre b și matricea A este matricea (ba_{ij}) . Similar, produsul Ab este matricea $(a_{ij}b)$. Injecția $b \mapsto bI_n : R \rightarrow M_n(R)$ este un morfism de inele, deoarece $(a+b)I_n = aI_n + bI_n$ și $(ab)I_n = (aI_n)(bI_n)$, pentru orice $a, b \in R$. Ca urmare, R se identifică cu subinelul $\{rI_n \mid r \in R\}$ al lui $M_n(R)$.

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

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

unde $\text{ord}(1)$ este ordinul lui 1 în grupul aditiv al lui A .

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

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

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

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 conține o copie izomorfă a corpului \mathbf{Q} și anume $\{a1/b1 \mid a, b \in \mathbf{Z}, b \neq 0\}$. Un corp finit are caracteristica număr prim.

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

Demonstrație. 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 $k!$ și $(p-k)!$ 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 $z \in A$ și s este un multiplu de p , atunci $sz = 0$, deoarece $\text{car}(A) = p$. Așadar $F(x+y) = (x+y)^p = X^p + C_p^1 x^{p-1}y + \dots + C_p^{p-1}xy^{p-1} + y^p = x^p + y^p = F(x) + F(y)$. •

4.3 Inel factor

Fie A un inel și 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 $\hat{x} = x + I$ cu $x \in A$. Pe A/I definim înmulțirea $\hat{x}\hat{y} = \widehat{xy}$ pentru $x, y \in A$. Această înmulțire e bine-definită (adică nu depinde de reprezentanții claselor). Într-adevăr, dacă $\hat{x} = \hat{x}'$ și $\hat{y} = \hat{y}'$, atunci $x' = x + i$ și $y' = y + j$ cu $i, j \in I$. Deci $x'y' = xy + xj + iy + ij \in xy + I$. Se probează ușor că față de această înmulțire grupul A/I devine un inel numit *inelul factor A modulo I* . În plus funcția $\pi : A \rightarrow A/I$, $\pi(x) = \hat{x}$ este un morfism surjectiv de inele numit *surjecția canonică*. De exemplu, $\mathbf{Z}/n\mathbf{Z}$ este chiar inelul \mathbf{Z}_n .

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

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

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

Demonstrație. Din teorema corespunzătoare de la grupuri (teorema 43) se știe că F este un izomorfism între grupurile aditive ale inelelor $A/\ker(f)$ și $\text{Im}(f)$. 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 ușor că $f : \mathbf{Z}[i] \rightarrow \mathbf{Z}_2$, $f(a + bi) = \widehat{a + b}$ 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 și I, J ideale ale lui A . Se verifică ușor că $I + J := \{i + j \mid i \in I, j \in J\}$ este un ideal al lui A numit *suma* idealelor i și J .

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

Demonstrație. Fie $p : A \rightarrow A/I$ și $q : A \rightarrow A/J$ proiecțiile canonice. Se vede ușor că aplicația $f : A \rightarrow A/I \times A/J$, $f(x) = (p(x), q(x))$, este un morfism de inele.

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

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

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

Demonstrație. Se aplică teorema anterioară și 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 corp se 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 rațional $c = a^2 - 2b^2 = (a + b\sqrt{2})(a - b\sqrt{2})$ 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, $\mathbf{Z}[i]/(3) = \{\widehat{a + bi} \mid 0 \leq a, b \leq 2\}$. 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 operațiile induse. De exemplu, \mathbf{Q} este subcorp al lui \mathbf{R} și orice corp de caracteristică zero conține un subcorp izomorf cu \mathbf{Q} .

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

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

Teorema 69 \mathbf{C} este un corp comutativ în raport cu adunarea și înmulțirea matricelor.

Demonstrație. 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 și înmulțirea:

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

și

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

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 $f : \mathbf{R} \rightarrow \mathbf{C}$, $f(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ 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

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

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

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

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

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

Teorema 71 *\mathbf{H} este un corp necomutativ în raport cu adunarea și înmulțirea matricelor.*

Demonstrație. E clar că matricea unitate se află în \mathbf{H} . Se arată prin calcul că \mathbf{H} este parte stabilă în raport cu adunarea și înmulțirea. Pentru înmulțire avem

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

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 egalitățile

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

rezultă că

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

Deci \mathbf{H} este corp necomutativ (necomutativitatea rezultă din calculele de mai jos). •

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

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = \begin{pmatrix} x + yi & z + ui \\ -z + ui & x - yi \end{pmatrix} = x + yi + zj + uk$$

și scrierea este unică. Obținem următoarea descriere a corpului cuaternionilor similară numerelor complexe.

Teorema 72 *Corpul cuaternionilor este*

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

împreună cu relațiile $ij = k$, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$, $ik = -j$ și $i^2 = j^2 = k^2 = -1$.

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

Reamintim că domeniu este un inel comutativ integru și nenul. Orice corp este domeniu, dar există domenii care nu sunt corpuri, de exemplu \mathbf{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 $K = \{a/b \mid a, b \in D, b \neq 0\}$. Pe K definim adunarea şi înmulţirea prin

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

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 $f : D \rightarrow K$, $f(a) = a/1$ 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.*

Demonstrație. $A^{(\mathbb{N})}$ este parte stabilă față de adunare și înmulțire: dacă $a_n = 0$, $b_n = 0$ pentru $n \geq N$, atunci $a_n + b_n = 0$ pentru $n \geq N$ și $\sum_{i+j=n} a_i b_j = 0$ pentru $n \geq 2N$.

Se arată ușor că $(A^{(\mathbb{N})}, +)$ este grup abelian cu elementul neutru șirul nul. Înmulțirea este asociativă deoarece

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

Șirul $(1, 0, 0, \dots)$ este elementul neutru al înmulțirii. E clar din definiție că înmulțirea este comutativă. Înmulțirea este distributivă față de adunare

$$\begin{aligned} ((a_n)_{n \geq 0} + (b_n)_{n \geq 0}) (c_n)_{n \geq 0} &= (a_n + b_n)_{n \geq 0} (c_n)_{n \geq 0} = \\ &= (\sum_{i+j=n} (a_i + b_i) c_j)_{n \geq 0} = (\sum_{i+j=n} a_i c_j)_{n \geq 0} + (\sum_{i+j=n} b_i c_j)_{n \geq 0} = \\ &= (a_n)_{n \geq 0} (c_n)_{n \geq 0} + (b_n)_{n \geq 0} (c_n)_{n \geq 0}. \bullet \end{aligned}$$

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

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

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

Inelul $A^{(\mathbb{N})}$ se notează cu $A[X]$ și se numește *inelul polinoamelor într-o nedeterminată* cu coeficienți în A .

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

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

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

(b) $\text{grad}(fg) \leq \text{grad}(f) + \text{grad}(g)$ cu egalitate dacă și numai dacă produsul coeficienților dominanți ai lui f și g este nenul.

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

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

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

Demonstrație. Prima afirmație 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 fracții al inelului de polinoame $L[X]$ se numește *corpul fracțiilor raționale peste L* și se notează cu $L(X)$. O *fracție rațională* este un cât de două polinoame P/Q cu $Q \neq 0$.

Teorema 77 Fie $u : A \rightarrow B$ un morfism de inele comutative și $x \in B$. Atunci funcția $v : A[X] \rightarrow B$,

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

este un morfism de inele.

Demonstrație. Fie $f = \sum_{i=0}^m a_i X^i$ și $g = \sum_{j=0}^n b_j X^j$, $f, g \in A[X]$. Avem

$$\begin{aligned} v(fg) &= v\left(\sum_{k=0}^{m+n} \sum_{i+j=k} a_i b_j\right) X^k = \sum_{k=0}^{m+n} \sum_{i+j=k} u(a_i) u(b_j) x^k = \\ &= \left(\sum_{i=0}^m u(a_i) x^i\right) \left(\sum_{j=0}^n u(b_j) x^j\right) = v(f)v(g). \end{aligned}$$

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

Fie A un subinel al inelului B și $x \in B$. 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 numește valoarea lui f în x . Funcția $\tilde{f} : B \rightarrow B$, $\tilde{f}(y) = f(y)$ se numește funcția polinomială asociată lui f . De exemplu, dacă $g = X^2 + X \in \mathbf{Z}_2[X]$, atunci \tilde{g} este funcția nulă.

4.6 Rădăcini ale polinoamelor

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

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

Polinoamele f, g, q, r se numesc deîmpărțit, împărțitor, cât și respectiv rest, iar egalitatea $f = gq + r$ se numește identitatea împărțirii.

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

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

Fie A un inel comutativ nenul, $f \in A[X]$ și $\alpha \in A$. 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, $f \in A[X]$ și $\alpha \in A$. Atunci restul împărțirii lui f la $X - \alpha$ este $f(\alpha)$. În particular, α este rădăcină a lui $f \Leftrightarrow X - \alpha$ divide f .*

Demonstrație. Există $q \in A[X]$ și $r \in A$ cu $f = (X - \alpha)q + r$. Făcând $X = \alpha$ obținem $r = f(\alpha)$. •

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

Demonstrație. Rezultă din teorema lui Bézout. •

Dacă f satisface condițiile 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, $0 \neq f \in D[X]$, $\alpha_1, \dots, \alpha_s \in D$ rădăcini distincte ale lui f respectiv de ordin n_1, \dots, n_s . Atunci f se poate scrie sub forma

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

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

Demonstrație. Afirmatia 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 $h \in D[X]$ și $h(\alpha_1) \neq 0$. 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 $p \in D[X]$ și $p(\alpha_2) \neq 0$. Deci $f = (X - \alpha_1)^{n_1} (X - \alpha_2)^k p$ și din corolarul precedent rezultă $k = n_2$. Așadar, $f = (X - \alpha_1)^{n_1} (X - \alpha_2)^{n_2} p$. 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 și 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 esențială, 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 (Relațiile lui Viète.) Fie D un domeniu și $f = a_0 + a_1X + \cdots + a_nX^n \in D[X]$ un polinom de grad $n \geq 1$. Presupunem că f are n rădăcini $\alpha_1, \dots, \alpha_n \in D$. Atunci

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

În plus, în corpul de fracții al lui D , au loc așa-numitele relațiile ale lui Viète

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

Demonstrație. Procedăm prin inducție 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 $X_1 = X$ și $X_2 = Y$. 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 $j = 0, \dots, n$. Rezultă că

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

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 , $\sum_{j=0}^n \left(\sum_{i=0}^m a_{ij} X^i \right) Y^j = \sum_{j=0}^n \left(\sum_{i=0}^m b_{ij} X^i \right) Y^j$ rezultă că $\sum_{i=0}^m a_{ij} X^i = \sum_{i=0}^m b_{ij} X^i$ pentru $j = 0, \dots, n$, deci $a_{ij} = b_{ij}$ pentru orice i și j . •

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

Gradul unui polinom este maximul gradelor monoamelor sale. Gradul polinomului nul se ia $-\infty$. Un polinom se numește polinom omogen dacă toate monoamele sale au același grad. Prin *componenta omogenă* de grad k , f_k , a unui polinom f înțelegem suma monoamelor de grad k din f . De exemplu, polinomul $f = 1 + XY + YZ + XZ + XYZ$ are gradul 3 și componentele omogene $f_0 = 1$, $f_1 = 0$, $f_2 = XY + YZ + XZ$ și $f_3 = XYZ$. Proprietățile gradului din cazul polinoamelor într-o nedeterminată se extind ușor 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 coeficienților lor este nul sau nenul. De asemenea, se vede ușor 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, $n \geq 1$ și $f, g \in A[X_1, \dots, X_n]$. Atunci

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

Demonstrație. (a) este evidentă. (b). Putem presupune că f și g sunt nenule, altfel afirmația este banală. Fie $k = \text{grad}(f)$ și $l = \text{grad}(g)$. Scriem pe f și g ca sumă de componente omogene: $f = f_0 + f_1 + \dots + f_k$ și $g = g_0 + g_1 + \dots + g_l$ 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 $\text{grad}(fg) \leq k + l$. Dacă, în plus, A este domeniu, atunci $f_k g_l$ este un polinom omogen de grad $k + l$ și $\text{grad}(f_i g_j) < k + l$ pentru orice $(i, j) \neq (k, l)$. Deci $\text{grad}(fg) = k + l$. •

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

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

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

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

De asemenea,

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

$$\begin{aligned}
&= \sum_{i,j=0}^p (f_i(b_1, \dots, b_{n-1})g_j(b_1, \dots, b_{n-1}))b_n^{i+j} = \\
&= \left(\sum_{i=0}^p f_i(b_1, \dots, b_{n-1})b_n^i\right)\left(\sum_{j=0}^p g_j(b_1, \dots, b_{n-1})b_n^j\right) = f(b_1, \dots, b_n)g(b_1, \dots, b_n). \bullet
\end{aligned}$$

4.8 Exerciții

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

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

105. Determinați unitățile inelului $\mathbf{Z}_{(2)} = \{a/b \mid a, b \in \mathbf{Z}, b \text{ impar}\}$.

106. Fie S o mulțime de numere prime (eventual vidă) și fie \mathbf{Z}_S mulțimea fracțiilor a/b cu a, b numere întregi și $b \neq 0$ cu toți factorii primi în S . Arătați că \mathbf{Z}_S este un subinel al lui \mathbf{Q} și că orice subinel al lui \mathbf{Q} este de această formă.

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

108. Arătați 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 mulțimea matricelor cu toate elementele multipli de n . În plus, $M_2(\mathbf{Z})/M_2(n\mathbf{Z}) \simeq M_2(\mathbf{Z}_n)$. Generalizare.

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

110. Fie A inelul al cărui grup abelian este $\mathbf{Z} \times \mathbf{Q}$ și are înmulțirea definită prin $(a, x)(b, y) = (ab, ay + bx)$. Arătați 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. Calculați tablele adunării/înmulțirii pentru următoarele inele factor: $\mathbf{Z}_2[X]/(X^2 + X + \hat{1})$, $\mathbf{Z}_2[X]/(X^2 + X)$, $\mathbf{Z}_2[X]/(X^2 + \hat{1})$ și $\mathbf{Z}_2[X]/(X^2)$.

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

113. Descrieți elementele inelului $\mathbf{Z}[i]/(3)$ și explicitați endomorfismul lui Frobenius.

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

(a) f este nilpotent dacă și numai dacă f are toți coeficienții nilpotenți (un element x al unui inel se zice nilpotent dacă există n cu $x^n = 0$).

(b) f este inversabil dacă și numai dacă f are termenul liber inversabil și ceilalți coeficienți nilpotenți.

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

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

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

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

118. Fie A inelul șirurilor de numere reale. Arătați că mulțimea I a șirurilor 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 $f(0) \in \mathbf{Z}$. Arătați că idealul $X\mathbf{Q}[X]$ nu este finit generat.

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

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

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

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

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

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

127. Arătați 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. Arătați 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. Explicitați corpul de fracții al domeniului $\mathbf{R}[X, Y]/(X^2 + Y^2)$.

130. Arătați 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. Decideți dacă inelele factor $\mathbf{Z}[X, Y]/(X - 1, Y - 2)$, $\mathbf{Q}[X, Y]/(X^2 + 1, Y^2 - 2)$ și $\mathbf{R}[X, Y]/(X^2 + 1, Y^2 + 1)$ sunt domenii.

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

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

134. Determinați mulțimile $A = \{Im(f) \mid f \text{ morfism de inele } \mathbf{Z}[X] \rightarrow \mathbf{Q}\}$ și $B = \{Im(f) \mid f \text{ morfism de inele } \mathbf{Z}[X, Y] \rightarrow \mathbf{Q}\}$.

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

136. Fie A un inel comutativ. Notăm cu $A^{\mathbf{N}}$ mulțimea șirurilor $(a_n)_{n \geq 0}$ cu elemente din A . Pe $A^{\mathbf{N}}$ definim două operații: adunarea $(a_n)_{n \geq 0} + (b_n)_{n \geq 0} = (a_n + b_n)_{n \geq 0}$ și înmulțirea $(a_n)_{n \geq 0} (b_n)_{n \geq 0} = (c_n)_{n \geq 0}$ unde $c_n = \sum_{i+j=n} a_i b_j$. Arătați că față de aceste două operații, $A^{\mathbf{N}}$ este un inel comutativ și că orice element al său se scrie unic sub forma $\sum_{n=0}^{\infty} a_n X^n$ cu $a_n \in A$, unde $X = (0, 1, 0, \dots)$. Acest inel se notează cu $A[[X]]$ și se numește *inelul seriilor formale cu coeficienți în A* .

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

138. Determinați morfismele de inele $\mathbf{Z}[[X]] \rightarrow \mathbf{Z}$.

Capitolul 5

Aritmetica lui \mathbf{Z} și $K[X]$

În acest capitol se studiază comparativ diferite proprietăți aritmetice ale inelelor \mathbf{Z} și $K[X]$, K corp comutativ. Se expun mai întâi rezultate referitoare la teorema împărțirii cu rest, cel mai mare divizor comun și 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 înțelegem un corp comutativ.

5.1 Teorema împărțirii cu rest

Fie K un corp. Reamintim următorul rezultat stabilit anterior.

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

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

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

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

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

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

Numerele/polinoamele a, b, q, r se numesc deîmpărțit, împărțitor, cât și respectiv rest, iar egalitatea $a = bq + r$ se numește identitatea împărțirii.

Demonstrație. Cazul $D = \mathbf{Z}$. Demonstrăm mai întâi existența lui q și 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 $0 \leq a - b(q + \text{sgn}(b)) < a - bq$, contradicție. Probăm unicitatea lui q și r . Fie $q', r' \in \mathbf{Z}$ astfel încât $a = bq' + r'$ și $0 \leq r' < |b|$. Scăzând cele două expresii ale lui a rezultă $b(q - q') = r' - r$, deci $r' - r = 0$ deoarece $|r' - r| < |b|$. Așadar $r' = r$ și 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 împărțiri 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 și $f \in K[X]$ un polinom de grad $n \geq 1$. Atunci elementele inelului factor $K[X]/(f)$ se reprezintă unic sub forma $a_0 + a_1X + \dots + a_{n-1}X^{n-1} + (f)$ cu $a_0, a_1, \dots, a_{n-1} \in K$. În particular, dacă K este finit cu q elemente, atunci $K[X]/(f)$ are q^n elemente.

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

Fie $D = \mathbf{Z}$ sau $K[X]$ și fie $a, b \in D$. Spunem că b divide a și 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 împărțirii lui a la b este zero.

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

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

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

- (a) $a \mid b$ dacă și numai dacă $aD \supseteq bD$.
- (b) Dacă $a \mid b$ și $b \mid c$, atunci $a \mid c$.
- (c) Dacă $a \mid b$ și $a \mid c$, atunci $a \mid bb' + cc'$ pentru orice $b', c' \in D$.
- (d) Dacă $a \mid b$, atunci

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

- (e) Elementele a, b sunt asociate dacă și numai dacă

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

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

Demonstrație.

- (a). Avem șirul de echivalențe $a \mid b \Leftrightarrow b \in aD \Leftrightarrow aD \supseteq bD$.
- (b). Cf. (a), $aD \supseteq bD \supseteq cD$, deci $a \mid c$.
- (c). Fie $b', c' \in D$. Cum $a \mid b$ și $a \mid c$, 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 $f \mid g$ și $g \mid f$. Reciproc, să presupunem că $f \mid g$ și $g \mid f$. Deci există $u, v \in K[X]$ cu $g = fu$ și $f = gv$. Rezultă $f = fuv$. Dacă $f = 0$, atunci $g = fu = 0$ și putem scrie $f = 1g$. Dacă $f \neq 0$, atunci $uv = 1$, deci $u, v \in K^*$. •

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

Fie $D = \mathbf{Z}$ sau $K[X]$ și fie $a, b, d, m \in D$. Spunem d este un *cel mai mare divizor comun* (cmmdc) al perechii a, b dacă $d \mid a$, $d \mid b$ și 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 $a \mid m$, $b \mid m$ și m divide orice alt multiplu comun al elementelor a, b . În acest caz vom scrie $m = [a, b]$. Evident, dacă $a \mid b$, atunci $(a, b) = a$ și $[a, b] = b$. Vom arăta că în \mathbf{Z} și $K[X]$ orice pereche de elemente are cmmdc și cmmmc.

Fie $a, b, d, d' \in D$ astfel încât atât d cât și d' joacă rol de cmmdc pentru perechea a, b . Din definiție rezultă că d și 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*. Considerații similare se pot face pentru cmmmc. De exemplu, în \mathbf{Z} , $(-18, 24) = 6$; în $\mathbf{Q}[X]$, $(2X - 1, -3X^2) = 1$.

În \mathbf{Z} și $K[X]$ orice pereche de elemente are cmmdc și acesta se poate calcula cu algoritmul lui Euclid.

Teorema 93 (Algoritmul lui Euclid.) *Fie D egal cu \mathbf{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 împărțirea cu rest: $a = bq + r$ cu $q, r \in D$ (cf. Teoremei 89);

$a := b$; $b := r$;

end;

$d := a$;

Demonstrație. E suficient să observăm următoarele. Conform pct. (c) din teorema 91, perechile $(a = bq + r, b)$ și (b, r) au aceeași divizori comuni, deci același cel mai mare divizor comun. Așadar 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 puțin o unitate. Deci algoritmul se termină după un număr finit de pași cu o pereche de forma $(a, 0)$, care are cmmdc egal cu a . •

Să considerăm exemplul $D = \mathbf{Z}$, $a = 18$ și $b = 24$. În timpul desfășurării 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.

Demonstrație. Afirmația este clară în cazul idealului nul. Fie I un ideal nenul și 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 împărțire cu rest, există $q, r \in D$ astfel încât $f = gq + r$ cu $0 \leq r < |g|$ în cazul $D = \mathbf{Z}$, respectiv $\text{grad}(r) < \text{grad}(g)$ 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 $K[X]$ și fie $a, b \in D$. Atunci (a, b) și $[a, b]$ există și au loc relațiile:

- (a) $aD + bD = (a, b)D$,
- (b) $aD \cap bD = [a, b]D$, și
- (c) elementele $(a, b)[a, b]$ și ab sunt asociate.

Demonstrație. (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 $a \mid m$ și $b \mid m$. Fie $n \in D$ un multiplu comun al lui a și b . Rezultă că $n \in aD \cap bD = mD$, deci $m \mid n$.

(c). Punem $d = (a, b)$ și $m = [a, b]$. Dacă $a = 0$ sau $b = 0$, afirmația e clară. Presupunem că a, b sunt nenule, deci d, m sunt nenule. Elementul $ab/d \in D$ se divide cu a și 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 și b . Deci $(ab/m) \mid d$, adică $ab \mid dm$. Așadar ab și dm sunt asociate. •

Teorema următoare cuprinde câteva proprietăți ale celui mai mare divizor comun.

Teorema 96 Fie $D = \mathbf{Z}$ sau $K[X]$ și 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 și 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) și $(a, b)c$ sunt asociate.
- (e) Dacă a, b sunt prime cu c , atunci ab este prim cu c .
- (f) Dacă $a \mid bc$ și a este prim cu b , atunci $a \mid c$.

Demonstrație. Afirmația (a) rezultă din pct. (a) al Teoremei 95, (b) rezultă din (a), iar (c) rezultă din (a) și (b).

(d). Fie $d = (a, b)$. Cf. Teoremei 95, $aD + bD = dD$. De aici rezultă ușor 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 $u, u', v, v' \in D$. Înmulțind aceste relații avem $1 = ab(uu') + c(bu'v + auv' + cvv')$, deci ab este prim cu c , cf. (b).

(f). Din (d) rezultă că (ac, bc) și c sunt asociate. Cum $a \mid ac$ și $a \mid bc$, deducem că $a \mid c$. •

Fie $D = \mathbf{Z}$ sau $K[X]$. Definiția cmmdc/cmmmc dată înaintea Teoremei 93, se poate extinde cu ușurință de la două elemente la un număr finit de elemente din D . Fie $a_1, \dots, a_n, d \in D$, $n \geq 2$. Spunem d este un cmmdc al elementelor a_1, \dots, a_n dacă $d \mid a_i$ pentru $i = 1, \dots, n$ și d se divide cu orice alt divizor comun al elementelor a_1, \dots, a_n . În acest caz vom scrie $d = (a_1, \dots, a_n)$.

De asemenea, m este un cmmmc al elementelor a_1, \dots, a_n dacă $a_i \mid m$ pentru $i = 1, \dots, n$ și m divide cu orice alt multiplu comun al elementelor a_1, \dots, a_n . În acest caz vom scrie $m = [a_1, \dots, a_n]$.

Teorema 95 se poate extinde în modul următor.

Teorema 97 Fie $D = \mathbf{Z}$ sau $K[X]$ și fie $a_1, \dots, a_n \in D$ cu $n \geq 2$. Atunci (a_1, \dots, a_n) și $[a_1, \dots, a_n]$ există și au loc egalitățile:

- (a) $a_1D + \dots + a_nD = (a_1, \dots, a_n)D$,
- (b) $a_1D \cap \dots \cap a_nD = [a_1, \dots, a_n]D$, și
- (c) $(a_1, \dots, a_n) = (a_1, (a_2, \dots, a_n))$.

Demonstrație. Pentru (a) și (b) se adaptează demonstrația Teoremei 95. Vom ilustra demonstrația lui (c) pe cazul $n = 3$. Fie $a, b, c, d, e \in D$ astfel încât $d = (b, c)$ și $e = (a, d)$. Arătăm că $e = (a, b, c)$. Din relațiile $e \mid a$, $e \mid d$,

$d \mid b$ și $d \mid c$, 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 $f \mid d$ și $f \mid a$, deci $f \mid e$. •

5.2 Numere prime, polinoame ireductibile

Un număr întreg $p \neq 0, \pm 1$ se numește *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 $\pm 1, \pm p$. Un număr întreg diferit de $0, \pm 1$ și neprim se numește *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 numește *polinom ireductibil* dacă f nu se poate scrie ca produs de două polinoame neconstante, alfel zis, dacă f nu are decât divizorii a și af cu $a \in K^*$. Un polinom neconstant non-ireductibil se numește *polinom reductibil*. De exemplu, în $\mathbf{Q}[X]$, X este ireductibil, X^2 este reductibil iar problema (i)reductibilității 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 , și*
- (c) *un polinom de grad 2 sau 3 este ireductibil dacă și numai dacă nu are rădăcini în K .*

Demonstrație. (a) este evidentă. (b) și (c) rezultă din următoarele observații. Un polinom are un factor $aX + b$ de gradul 1 dacă și numai dacă are rădăcina $-b/a \in K$. Pe de altă parte, un polinom de grad 2 sau 3 este reductibil dacă și 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+1 , X^3+X+1 și X^3+X^2+1 . X^4+X+1 este ireductibil în $\mathbf{Z}_2[X]$ deoarece nu are rădăcini și nu este pătratul lui X^2+X+1 .

Fie $D = \mathbf{Z}$ resp. $K[X]$, $p \in D$ un număr prim resp. polinom ireductibil și $a \in D$. Din definiții, rezultă că $p \mid a$ sau $(a, p) = 1$.

Teorema 99 Fie $D = \mathbf{Z}$ sau $K[X]$ și $p \in D$ un element nenul și neinvertibil. Atunci p este prim în cazul $D = \mathbf{Z}$ resp. ireductibil în cazul $D = K[X]$ dacă și numai dacă satisface condiția:

$$a, b \in D \text{ și } p \mid ab \Rightarrow p \mid a \text{ sau } p \mid b.$$

Demonstrație. 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 $a, b \in \mathbf{Z}$ și $1 < |a|, |b| < |p|$. Atunci $p \mid ab$ dar $p \nmid a$ și $p \nmid b$. De asemenea, să presupunem că $p \in K[X]$ este polinom reductibil. Deci $p = ab$ cu $a, b \in K[X]$ și $0 < \text{grad}(a), \text{grad}(b) < \text{grad}(p)$. Atunci $p \mid ab$ dar $p \nmid a$ și $p \nmid b$. •

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) și (b) sunt unice (vezi Teorema 102).

Demonstrație. (a). Presupunem că există întregi diferiți 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 și b se pot scrie ca produs de numere prime. Dar atunci și $N = ab$ este produs de prime, contradicție.

(b). Adaptăm demonstrația de la (a). Presupunem că există polinoame 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 și g se pot scrie ca produs de polinoame ireductibile. Dar atunci și $H = fg$ este produs de polinoame ireductibile, contradicție. •

Din teorema precedentă rezultă că $a, b \in \mathbf{Z}$ sunt prime între ele dacă și numai dacă nu au un divizor prim comun. O afirmație similară are loc în $K[X]$.

Teorema 101 (Euclid)

- (a) Mulțimea numerelor naturale prime este infinită.
- (b) Mulțimea polinoamelor unitare ireductibile din $K[X]$ este infinită.

Demonstrație. (a). Negăm. Fie p_1, \dots, p_n mulțimea numerelor naturale prime. Considerăm numărul $N = p_1 \cdots p_n + 1$. Atunci N nu se divide cu nici un număr prim p_i , contradicție.

(b). Dacă K este corp infinit, putem folosi polinoamele ireductibile $X - a$ cu $a \in K$. În cazul K corp finit se reiterează raționamentul 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, \dots, p_s sunt numere prime pozitive distincte și $\alpha_1, \dots, \alpha_s \geq 1$.

(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, \dots, π_s sunt polinoame ireductibile unitare distincte și $\alpha_1, \dots, \alpha_s \geq 1$.

Demonstrație.

(a) Existența 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, \dots, q_t numere prime pozitive distincte și $\beta_1, \dots, \beta_t \geq 1$. Facem inducție după $M = \alpha_1 + \cdots + \alpha_s$ afirmația fiind evidentă pentru $M = 1$. Presupunem $M > 1$. Cum $p_s \mid N$ și $N = \pm q_1 \cdots q_t$, 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 $p_1^{\alpha_1} \cdots p_s^{\alpha_s} = q_1^{\beta_1} \cdots q_t^{\beta_t}$ obținem $p_1^{\alpha_1} \cdots p_s^{\alpha_s-1} = q_1^{\beta_1} \cdots q_t^{\beta_t-1}$. Din ipoteza de inducție rezultă că $s = t$, și, după o eventuală renumerotare, $p_i = q_i$ și $\alpha_i = \beta_i$ pentru $i = 1, \dots, s-1$, și $\alpha_s - 1 = \beta_s - 1$. Deci $\alpha_s = \beta_s$.

(b) Se adaptează raționamentul precedent. •

Teorema următoare este numită Teorema Fundamentală a Algebrei.

Teorema 103 (D'Alembert-Gauss) Orice polinom neconstant $f \in \mathbf{C}[X]$ are cel puțin o rădăcină în \mathbf{C} .

O demonstrație 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 și cele de gradul doi fără rădăcini reale.*

Demonstrație. $f \in \mathbf{R}[X]$ de grad ≥ 3 și 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 și rădăcina $\bar{\alpha}$. Atunci f se divide în $\mathbf{C}[X]$ și $\mathbf{R}[X]$ (observația 92) cu $(X - \alpha)(X - \bar{\alpha})$, deci f este reductibil. •

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 $a \in \mathbf{C}$, $\alpha_1, \dots, \alpha_s \in \mathbf{C}$ distincte, și $m_1, \dots, m_s \geq 1$.*

(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 $a \in \mathbf{R}$, $\alpha_1, \dots, \alpha_s \in \mathbf{R}$ distincte, $\pi_1, \dots, \pi_t \in \mathbf{R}[X]$ sunt polinoame unitare de gradul doi distincte fără rădăcini reale și $m_1, \dots, m_s, n_1, \dots, n_t \geq 1$.*

În \mathbf{Z} și $K[X]$ cmmdc și 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, \dots, p_s sunt numere prime pozitive distincte și $\alpha_i \geq 1$ pentru $i = 1, \dots, s$. 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 $i = 1, \dots, s$.*

Demonstrație. Fie $a = bc$ o factorizare a lui a cu $b, c \in \mathbf{Z}$. Din Teorema 102, factorii primi din descompunerea lui b și c sunt dintre p_1, \dots, p_s . Deci putem scrie $b = \pm p_1^{\beta_1} \cdots p_s^{\beta_s}$ și $c = \pm p_1^{\gamma_1} \cdots p_s^{\gamma_s}$. Din $a = bc$ obținem $p_1^{\alpha_1} \cdots p_s^{\alpha_s} = p_1^{\beta_1 + \gamma_1} \cdots p_s^{\beta_s + \gamma_s}$. Din Teorema 102 rezultă că $\alpha_i = \beta_i + \gamma_i$ pentru $i = 1, \dots, s$. •

Se poate demonstra o leamnă analogă pentru $K[X]$.

Teorema 107 *Fie $a = \pm p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ și $b = \pm p_1^{\beta_1} \cdots p_s^{\beta_s}$ unde p_1, \dots, p_s sunt numere prime pozitive distincte iar $\alpha_i, \beta_i \geq 1$, pentru $i = 1, \dots, s$. Atunci*

$$(a) (a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdots p_s^{\min(\alpha_s, \beta_s)} \text{ și}$$

$$(b) [a, b] = p_1^{\max(\alpha_1, \beta_1)} \cdots p_s^{\max(\alpha_s, \beta_s)}.$$

Demonstrație. (a). Cf. lemei anterioare, divizorii comuni ai lui a și b au forma $\pm p_1^{\gamma_1} \cdots p_s^{\gamma_s}$ cu $\gamma_i \leq \min(\alpha_i, \beta_i)$ pentru $i = 1, \dots, s$. 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 $f = a\pi_1^{\alpha_1} \cdots \pi_s^{\alpha_s}$ și $g = b\pi_1^{\beta_1} \cdots \pi_s^{\beta_s}$ unde $a, b \in K^*$, π_1, \dots, π_s sunt polinoame ireductibile unitare distincte din $K[X]$ și $\alpha_i, \beta_i \geq 1$ pentru $i = 1, \dots, s$. Atunci

- (a) $(f, g) = \pi_1^{\min(\alpha_1, \beta_1)} \cdots \pi_s^{\min(\alpha_s, \beta_s)}$ și
 (b) $[f, g] = \pi_1^{\max(\alpha_1, \beta_1)} \cdots \pi_s^{\max(\alpha_s, \beta_s)}$.

Demonstrație. Se adaptează demonstrația precedentă. •

5.3 Complemente

Teorema 109 Fie K un corp și $f \in K[X]$ un polinom ireductibil. Atunci inelul factor $k[X]/(f)$ este corp.

Demonstrație. 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 $\alpha : K \rightarrow K[X]/(f)$, $\alpha(a) = \widehat{a}$, 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 și $f \in K[X]$ un polinom de grad ≥ 1 . Atunci există un corp L care îl conține pe K astfel încât f are o rădăcină în L .

Demonstrație. 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 toți coeficienții lui h , cu excepția coeficientului dominant, iar p^2 nu divide termenul liber al lui h . Atunci h este ireductibil în $\mathbf{Q}[X]$.*

Demonstrație. 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 $ab \neq 1$ și 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 obținute din af resp. bg prin reducerea coeficienților 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 toți coeficienții lui af , deci și coeficientul dominant a , sunt divizibili cu q , deci $(a/q)f \in \mathbf{Z}[X]$, în contradicție cu alegerea lui a . Rezultă că $a = b = 1$, deci $f, g \in \mathbf{Z}[X]$.

Fie $\overline{f}, \overline{g}$ polinoamele obținute din f resp. g prin reducerea coeficienților modulo p . Rezultă că $\overline{f}\overline{g} = X^n$ în $\mathbf{Z}_p[X]$, unde n este gradul lui h . Deducem că $\overline{f} = X^s$ și $\overline{g} = X^t$, unde s, t sunt gradele lui f resp. g . Deci termenii liberi ai lui f și g se divid cu p . În consecință, termenul liber al lui h se divide cu p^2 , contradicție. •

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 Exerciții

139. Calculați $(24, 54)$ în \mathbf{Z} cu ajutorul algoritmului lui Euclid.

140. Fie $a, b \in \mathbf{N}$ și $d = (a, b)$. Arătați că $(X^a - 1, X^b - 1) = X^d - 1$ în $K[X]$, unde K este un corp.

141. Calculați $f = (X^{23} + X^{22} + \dots + X + 1, X^{53} + X^{52} + \dots + X + 1)$ în $\mathbf{Q}[X]$.

142. Calculați $(X^4 - 4X^3 + 1, X^3 - 3X^2 + 1)$ în $\mathbf{R}[X]$.

143. Calculați $(2^m - 1, 2^n - 1)$ în \mathbf{Z} .

144. Fie $a, b, c, d \in \mathbf{Z} \setminus \{0\}$ astfel încât $ab = cd$. Arătați că există $x, y, u, v \in \mathbf{Z}$ astfel încât $xy = c$, $uv = d$, $xu = a$ și $yv = b$.

145. Fie A un domeniu și $0 \neq a, b \in A$ astfel încât $Aa + Ab = Ad$. Arătați că $d = (a, b)$.

146. Fie K un corp și $0 \neq f, g \in K[X]$ astfel încât $f \mid g^2 \mid f^3 \mid g^4 \mid \dots$. Arătați că f, g sunt asociate.

147. Arătați că numerele $F_n = 2^{2^n} + 1$ (numite *numerele Fermat*) sunt relativ prime două câte două. Deduceți că există o infinitate de numere prime. (Indicație. $F_0 F_1 F_2 \dots F_{n-1} = F_n - 2$).

148. Arătați că $F_n = 2^{2^n} + 1$ este număr prim pentru $n = 0, 1, 2, 3$ și compus pentru $n = 5$. (Indicație. Folosind egalitățile $641 = 5 \cdot 2^7 + 1 = 5^4 + 2^4$, rezultă că F_5 se divide cu 641).

149. Calculați $(X^2 - 1)\mathbf{Q}[X] \cap (X^3 - 1)\mathbf{Q}[X]$ și $(X^2 - 1)\mathbf{Q}[X] + (X^3 - 1)\mathbf{Q}[X]$.

150. Calculați (f, g) și $[f, g]$ în $\mathbf{Q}[X]$ pentru $f = (X - 1)(X^2 - 1)(X^3 - 1)(X^4 - 1)$ și $g = (X + 1)(X^2 + 1)(X^3 + 1)(X^4 + 1)$.

151. Descompuneți 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 $X^4 + X^2 + 1$? (Indicație. Descompuneți polinomul $X^4 + X^2 + 1$.)

153. Găsiți polinoamele ireductibile de grad ≤ 5 din $\mathbf{Z}_2[X]$.

154. Descompuneți polinomul $X^{15} + \hat{1}$ în produs de polinoame ireductibile în $\mathbf{Z}_2[X]$.

155. Descompuneți polinomul $X^{56} - X^{49} - X^7 + \hat{1}$ în produs de polinoame ireductibile în $\mathbf{Z}_7[X]$. (Indicație. Folosiți morfismul lui Frobenius.)

156. Găsiți polinoamele ireductibile de grad ≤ 2 din $K[X]$, unde K este corpul $\{0, 1, z, z + 1\}$, unde $1 + 1 = 0$ și $z^2 = z + 1$.

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 și $f, g, h \in K[X]$ polinoame. Arătați că

$$[f, g, h]^2(f, g)(g, h)(f, h) = (f, g, h)^2[f, g][g, h][f, h].$$

159. Arătați 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 și n un număr natural nenul. Arătați că polinomul $X^n - k$ este ireductibil în $\mathbf{Q}[X]$.

161. Fie K un corp, $f \in K[X]$ un polinom neconstant și $a, b \in K$, $a \neq 0$. Arătați că f este ireductibil $\Leftrightarrow f(aX + b)$ este ireductibil.

162. Fie n un număr natural nenul. Arătați că polinomul $f = X^{2^n} + 1$ este ireductibil în $\mathbf{Q}[X]$. (Indicație. Se consideră $f(X + 1)$.)

163. Fie p un număr natural prim. Arătați că polinomul $f = X^{p-1} + X^{p-2} + \dots + X + 1$ este ireductibil în $\mathbf{Q}[X]$. (Indicație. Se consideră $f(X + 1)$.)

Capitolul 6

Polinoame simetrice

În acest capitol se prezintă teorema fundamentală a polinoamelor simetrice.

6.1 Inelul polinoamelor simetrice

Fie A un inel comutativ și $n \geq 1$. Un polinom $f \in A[X_1, \dots, X_n]$ se numește *polinom simetric* dacă f rămâne neschimbat după orice permutare a nedeterminatelor X_1, \dots, X_n , adică

$$f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = f(X_1, \dots, X_n) \text{ pentru orice } \sigma \in S_n.$$

Polinoamele constante sunt evident simetrice. Deoarece orice permutare din S_n este un produs de transpoziții (teorema 51), rezultă că un polinom este simetric dacă și numai dacă f este invariant la orice transpoziție (X_i, X_j) a nedeterminatelor X_1, \dots, X_n . Polinoamele

$$\begin{aligned} s_1 &= X_1 + \dots + X_n \\ s_2 &= X_1X_2 + X_1X_3 + \dots + X_{n-1}X_n \\ &\vdots \\ s_n &= X_1 \dots X_n \end{aligned}$$

sunt simetrice deoarece s_k este suma tuturor produselor de k nedeterminate distincte din mulțimea X_1, \dots, 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 își schimbă semnul. Deci g este simetric dacă și numai dacă inelul A este de caracteristică 2.

Teorema 112 *Mulțimea polinoamelor simetrice formează un subinel al inelului $A[X_1, \dots, X_n]$.*

Demonstrație. Fie f, g polinoame simetrice. Avem de arătat că $f + g$ și fg sunt de asemenea simetrice. Fie $\sigma \in S_n$. Atunci $(fg)(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})g(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = fg$. Deci fg este simetric și la fel se arată că $f + g$ este simetric. •

În consecință, $g(s_1, s_2, \dots, s_n)$ este polinom simetric pentru orice $g \in A[Y_1, \dots, Y_n]$. Vom arăta că orice polinom simetric se poate scrie astfel și că scrierea este unică. De exemplu, $X_1^2 + X_2^2 + \dots + X_n^2 = s_1^2 - 2s_2$. Sunt necesare unele pregătiri.

Definim *ordinea lexicografică* pe mulțimea monoamelor din $A[X_1, \dots, X_n]$. Fie $M = aX_1^{i_1} \dots X_n^{i_n}$ și $N = bX_1^{j_1} \dots X_n^{j_n}$ două monoame nenule. Spunem că M este *strict mai mare ca N în ordinea lexicografică*, și scriem $M > N$, dacă există k , $1 \leq k < n$, astfel încât $i_1 = j_1, \dots, i_k = j_k$ și $i_{k+1} > j_{k+1}$. Altfel spus, $M > N$ dacă prima componentă nenulă a vectorului $(i_1 - j_1, \dots, i_n - j_n)$ 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 dicționar: e ca și cum am compara cuvintele (i_1, \dots, i_n) și (j_1, \dots, j_n) .

De exemplu, $X_1^k \geq X_1^l \Leftrightarrow k \geq l$ și $X_1^2 > X_1X_2 > X_1X_3 > X_2^2 > X_2X_3 > X_3^2$.

Teorema 113 *Fie M, N, P, Q patru monoame nenule. Atunci*

- (a) $M \geq N$ sau $N \geq M$.
- (b) Dacă $M \geq N$ și $N \geq P$, atunci $M \geq P$.
- (c) Dacă $M \geq N$ și $N \geq M$, atunci M și N sunt asemenea.
- (d) Dacă $M \geq N$, $P \geq Q$ și $MP, NQ \neq 0$, atunci $MP \geq NQ$.

La (b) și (d), dacă una din inegalitățile din ipoteză este strictă, atunci și inegalitatea din concluzie este strictă.

Demonstrație. (a) și (c) rezultă din definiție. Fie $M = aX_1^{i_1} \dots X_n^{i_n}$, $N = bX_1^{j_1} \dots X_n^{j_n}$, $P = cX_1^{k_1} \dots X_n^{k_n}$ și $Q = dX_1^{l_1} \dots X_n^{l_n}$. (b). Putem presupune că $M > N$ și $N > P$ altfel afirmația e clară. Atunci vectorii $(i_1 - j_1, \dots, i_n - j_n)$ și $(j_1 - k_1, \dots, j_n - k_n)$ au prima componentă nenulă > 0 . Rezultă că și suma lor $(i_1 - k_1, \dots, i_n - k_n)$ are prima componentă nenulă > 0 ,

deci $M > P$. (d). Tratăm cazul $M > N$ și $P > Q$, celelalte se probează analog. Atunci vectorii $(i_1 - j_1, \dots, i_n - j_n)$ și $(k_1 - l_1, \dots, k_n - l_n)$ au prima componentă nenulă > 0 , deci și suma lor $(i_1 + j_1 - k_1 - l_1, \dots, i_n + j_n - k_n - l_n)$ are prima componentă nenulă > 0 , adică $MN > PQ$. •

În anumite privințe, ordinea lexicografică se comportă similar relației de ordine pe mulțimea numerelor naturale.

Teorema 114 *Orice șir strict descrescător de monoame din $A[X_1, \dots, X_n]$ este finit.*

Demonstrație. Facem inducție după n , pentru $n = 1$ proprietatea fiind clară. Fie $n \geq 2$ și presupunem că există un șir infinit strict descrescător de monoame $M_1 > M_2 > M_3 > \dots$. Izolând în fiecare monom M_j nedeterminata X_1 , obținem $X_1^{i_1} N_1 > X_1^{i_2} N_2 > X_1^{i_3} N_3 > \dots$, unde N_j sunt monoame în nedeterminatele X_2, \dots, X_n . Rezultă că $i_1 \geq i_2 \geq i_3 \geq \dots$, deci există s astfel încât $i_k = i_s$ pentru orice $k \geq s$. Rezultă șirul infinit $N_s > N_{s+1} > N_{s+2} > \dots$, în contradicție cu ipoteza de inducție. •

Fie f un polinom nenul. Numim *termen principal* al lui f , și-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 $aX_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$ este termenul principal al unui polinom simetric, atunci $i_1 \geq i_2 \geq \dots \geq i_n$.*

Demonstrație. Fie f un polinom simetric și $N = bX_1^{j_1} X_2^{j_2} \dots X_n^{j_n}$ un monom nenul al său. Fiind simetric, f conține odată cu N toate monoamele $bX_1^{j_{\sigma(1)}} X_2^{j_{\sigma(2)}} \dots X_n^{j_{\sigma(n)}}$, $\sigma \in S_n$. Între acestea, cel mai mare în ordinea lexicografică este cel pentru care $j_{\sigma(1)} \geq j_{\sigma(2)} \geq \dots \geq j_{\sigma(n)}$. •

În particular, pentru polinoamele simetrice fundamentale avem $T(s_k) = X_1 \dots X_k$, $1 \leq k \leq n$.

Teorema 116 *Fie $f, g \in A[X_1, \dots, X_n]$ două polinoame nenule. Dacă $T(f)T(g) \neq 0$ (e.g., dacă A este domeniu), atunci $T(fg) = T(f)T(g)$.*

Demonstrație. Scriem $f = M_0 + M_1 + \dots + M_k$ și $g = N_0 + N_1 + \dots + N_l$ unde $M_0 = T(f)$ și $N_0 = T(g)$, M_1, \dots, M_k sunt monoame strict mai mici ca $T(f)$ și N_1, \dots, 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 toți ceilalți termeni $M_i N_j$, cf. teoremei 113. Deci $T(fg) = T(f)T(g)$. •

6.2 Teorema fundamentală

Teorema 117 (Teoremă fundamentală a polinoamelor simetrice.) *Orice polinom simetric $f \in A[X_1, \dots, X_n]$ se scrie în mod unic ca expresie polinomială cu coeficienți în A de polinoamele simetrice fundamentale s_1, \dots, s_n , adică există și este unic un polinom $g \in A[Y_1, \dots, Y_n]$ astfel încât $f = g(s_1, \dots, s_n)$.*

Existența lui g rezultă din următorul algoritm (unicitatea lui g va fi probată ulterior).

Algoritmul 118 (Exprimarea unui polinom simetric în funcție de polinoamele simetrice fundamentale).

Input: $f \in A[X_1, \dots, X_n]$ polinom simetric.

Output: $g \in A[Y_1, \dots, Y_n]$ astfel încât $f = g(s_1, \dots, s_n)$.

$g := 0; h := f;$

while ($h \neq 0$) *do*

begin

$aX_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$ = termenul principal al lui h ;

$h := h - a s_1^{i_1-i_2} s_2^{i_2-i_3} \dots s_{n-1}^{i_{n-1}-i_n} s_n^{i_n};$

$g := g + a Y_1^{i_1-i_2} Y_2^{i_2-i_3} \dots Y_{n-1}^{i_{n-1}-i_n} Y_n^{i_n};$

end.

Corectitudinea algoritmului rezultă din următoarele observații. Cf. teoremei 112, h rămâne simetric în timpul desfășurării algoritmului. Rezultă că $T(h) = aX_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$ are proprietatea $i_1 \geq i_2 \geq \dots \geq i_n$, cf. teoremei 115. Deci, au sens expresiile $a s_1^{i_1-i_2} s_2^{i_2-i_3} \dots s_{n-1}^{i_{n-1}-i_n} s_n^{i_n}$ și $a Y_1^{i_1-i_2} Y_2^{i_2-i_3} \dots Y_{n-1}^{i_{n-1}-i_n} Y_n^{i_n}$. Cf. teoremei 116, $a s_1^{i_1-i_2} s_2^{i_2-i_3} \dots s_{n-1}^{i_{n-1}-i_n} s_n^{i_n}$ are termenul principal

$$aX_1^{i_1-i_2} (X_1 X_2)^{i_2-i_3} \dots (X_1 \dots X_{n-1})^{i_{n-1}-i_n} (X_1 \dots X_n)^{i_n} = aX_1^{i_1} X_2^{i_2} \dots X_n^{i_n}.$$

Deci la fiecare parcurgere a buclei *while*, $T(h)$ scade strict. În consecință, bucla *while* se parcurge doar de un număr finit de ori, cf. teoremei 114. În fine, se observă că după inițializările $g := 0$, $h := f$, avem $f = h + g(s_1, \dots, s_n)$, egalitate ce se păstrează după fiecare parcurgere a buclei *while*. La sfârșit vom avea $h = 0$, deci $f = g(s_1, \dots, s_n)$. •

De exemplu, pentru $f = X_1^2 + \dots + X_n^2$, variabilele algoritmului iau valorile următoare: $h = f$, $-2s_1$, 0 , $T(h) = X_1^2$, $-2X_1X_2$ și $g = 0$, Y_1^2 , $Y_1^2 - 2Y_2$. Adică $f = s_1^2 - 2s_2$.

Demonstrația unicității lui g . Fie $g, g' \in A[Y_1, \dots, Y_n]$ distincte; deci $G := g - g' \neq 0$. E suficient să arătăm că $G(s_1, \dots, s_n) \neq 0$. Fie $G = \sum_{i=1}^k M_i$ scrierea canonică a lui G ca sumă de monoame. Atunci $G(s_1, \dots, s_n) = \sum_{i=1}^k M_i(s_1, \dots, s_n) \neq 0$, deoarece polinoamele $M_i(s_1, \dots, s_n)$ au termenii principali monoame neasemenea două câte două. Într-adevăr, fie

$$M = aY_1^{i_1}Y_2^{i_2} \dots Y_n^{i_n}, \quad N = bY_1^{j_1}Y_2^{j_2} \dots Y_n^{j_n}$$

două monoame nenule neasemenea astfel încât $M(s_1, \dots, s_n)$ și $N(s_1, \dots, s_n)$ au termenii principali monoame asemenea. Cum $M(s_1, \dots, s_n) = as_1^{i_1}s_2^{i_2} \dots s_n^{i_n}$ are termenul principal

$$aX_1^{i_1}(X_1X_2)^{i_2} \dots (X_1 \dots X_n)^{i_n} = aX_1^{i_1+\dots+i_n}X_2^{i_2+\dots+i_n} \dots X_{n-1}^{i_{n-1}+\dots+i_n}X_n^{i_n}$$

iar $N(s_1, \dots, s_n)$ are termenul principal

$$bX_1^{j_1+\dots+j_n}X_2^{j_2+\dots+j_n} \dots X_{n-1}^{j_{n-1}+\dots+j_n}X_n^{j_n}$$

rezultă că $i_n = i_n$, $i_{n-1} = j_{n-1}, \dots, i_1 = j_1$, deci monoamele M , N sunt asemenea, contradicție.

Teorema 119 *Componentele omogene ale unui polinom simetric sunt polinoame simetrice.*

Demonstrație. Fie $f \in A[X_1, \dots, X_n]$ un polinom simetric și fie f_0, \dots, f_k componentele sale omogene. Dacă $\sigma \in S_n$ și notăm $f_j(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ cu f_j^σ , obținem $f^\sigma = f_0^\sigma + f_1^\sigma + \dots + f_k^\sigma$. Cum f_j^σ este polinom omogen de grad j și $f = f^\sigma$, deducem că $f_j^\sigma = f_j$ pentru orice j și 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 și omogen de grad k . Se observă că, în timpul desfășurării 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 $i_1 + \cdots + i_n = k$, $i_1 \geq i_2 \geq \cdots \geq i_n$ și $X_1^{i_1} \cdots X_n^{i_n} \leq T(f)$. Coeficienții a_α pot fi determinați dând valori particulare nedeterminatelor X_1, \dots, X_n .

De exemplu, fie $f = (X_1 + X_2)(X_1 + X_3)(X_2 + X_3)$. f este simetric și omogen de grad 3 și $T(f) = X_1^2 X_2$. Tripletele (i_1, i_2, i_3) ce verifică condițiile precedente sunt $(2, 1, 0)$ și $(1, 1, 1)$. Deci $f = s_1^{2-1} s_2^{1-0} s_3^0 + a s_1^{1-1} s_2^{1-1} s_3^1 = s_1 s_2 + a s_3$. Făcând $X_1 = X_2 = X_3 = 1$, găsim $9 + a = 8$, adică $a = -1$. Deci $f = s_1 s_2 - s_3$.

Lema 120 Fie $f \in A[X_1, \dots, X_n]$ un polinom omogen și simetric de grad k cu $1 \leq k < n$. Atunci $f(X_1, \dots, X_k, 0, \dots, 0) \neq 0$.

Demonstrație. Fie $M = a X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ termenul principal al lui f . Atunci $i_1 \geq i_2 \geq \cdots \geq i_n$, cf. teoremei 115. Cum $i_1 + \cdots + i_n = k$ și $k < n$, rezultă $i_{k+1} = \cdots = i_n = 0$. Deci M rămâne nenul după anularea nedeterminatelor X_{k+1}, \dots, X_n , adică $f(X_1, \dots, X_k, 0, \dots, 0) \neq 0$. •

Teorema 121 (Formulele lui Newton). Fie polinoamele

$$p_k = X_1^k + X_2^k + \cdots + X_n^k, \quad k \geq 1$$

și fie $s_1, \dots, s_n \in A[X_1, \dots, X_n]$ polinoamele simetrice fundamentale. Atunci

$$p_k - s_1 p_{k-1} + s_2 p_{k-2} - \cdots + (-1)^n s_n p_{k-n} = 0 \text{ pentru } k \geq n \quad (6.1)$$

și

$$p_k - s_1 p_{k-1} + \cdots + (-1)^{k-1} s_{k-1} p_1 + (-1)^k k s_k = 0 \text{ pentru } 1 \leq k \leq n-1. \quad (6.2)$$

Demonstrație. Fie $k \geq n$ și fie $g \in A[X_1, \dots, X_n, Y]$, $g = (Y - X_1)(Y - X_2) \cdots (Y - X_n)$. Din relațiile lui Viète

$$g = Y^n - s_1 Y^{n-1} + s_2 Y^{n-2} - \cdots + (-1)^n s_n.$$

Cum fiecare X_i este rădăcină a lui g , deducem că

$$X_i^n - s_1 X_i^{n-1} + s_2 X_i^{n-2} - \dots + (-1)^n s_n = 0.$$

Prin înmulțire cu X_i^{n-k} rezultă

$$X_i^k - s_1 X_i^{k-1} + s_2 X_i^{k-2} - \dots + (-1)^n s_n X_i^{n-k} = 0.$$

Adunând aceste relații pentru i de la 1 la n obținem formula (6.1). Pentru $k = n$ obținem în $A[X_1, \dots, X_k]$

$$p_k - s_1 p_{k-1} + s_2 p_{k-2} - \dots + (-1)^k k s_k = 0. \quad (6.3)$$

Fie acum $1 \leq k \leq n-1$ și presupunem că polinomul

$$h = p_k - s_1 p_{k-1} + \dots + (-1)^{k-1} s_{k-1} p_1 + (-1)^k k s_k$$

este nenul. Atunci h este simetric și omogen de grad k . Din formula (6.3) rezultă că $h(X_1, \dots, X_k, 0, \dots, 0) = 0$, contradicție, 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 Exerciții

164. Fie $n \geq 1$ și $t_k = \varepsilon_1^k + \dots + \varepsilon_n^k$, unde $\varepsilon_1, \dots, \varepsilon_n$ sunt rădăcinile complexe de ordinul n ale unității. Arătați că $t_k = 0$ dacă n nu divide k și $t_k = n$ dacă n divide k .

165. Calculați suma cuburilor rădăcinilor ecuației $x^4 + x^3 + 2x^2 + x + 1 = 0$.

166. Calculați sumele $p_k = x_1^k + \dots + x_n^k$, $1 \leq k \leq n$, unde x_1, \dots, x_n sunt rădăcinile ecuației $x^n + x^{n-1}/1! + x^{n-2}/2! + \dots + x/(n-1)! + 1/n! = 0$.

167. Aranjați 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 mulțimi ordonate A și B sunt izomorfe dacă există o bijecție crescătoare $f : A \rightarrow B$ cu inversa f^{-1} crescătoare. Este mulțimea monoamelor unitare în nedeterminatele X, Y ordonată lexicografic izomorfă cu (\mathbb{N}, \leq) ?

169. "Rulați" algoritmul din teorema fundamentală a polinoamelor simetrice pentru $f = X^3 + Y^3 + Z^3$.

170. Exprimați polinomul $f = (X_1 - X_2)^2(X_2 - X_3)^2(X_1 - X_3)^2$ în funcție de polinoamele simetrice fundamentale folosind metoda coeficienților nedeterminați.

171. Exprimați polinoamele $f_1 = \sum X_1^2 X_2 X_3$, $f_2 = \sum X_1^2 X_2^2$, $f_3 = \sum X_1^3 X_2$ și $f_4 = \sum X_1^3 X_2^2$ în funcție de polinoamele simetrice fundamentale.

172. Fie x_1, x_2, x_3 rădăcinile ecuației $x^3 + px + q = 0$. Calculați discriminantul ecuației $D = (x_1 - x_2)^2(x_2 - x_3)^2(x_1 - x_3)^2$.

173. Fie x_1, x_2, x_3 rădăcinile ecuației $x^3 + px + q = 0$ și fie $\varepsilon = (-1 + i\sqrt{3})/2$. Găsiți ecuația de gradul doi cu rădăcinile $y_1 = (x_1 + \varepsilon x_2 + \varepsilon^2 x_3)^3$ și $y_2 = (x_1 + \varepsilon^2 x_2 + \varepsilon x_3)^3$. Rezolvați ecuația $x^3 + px + q = 0$. Aplicație: $x^3 + 6x + 2 = 0$.

174. Fie $A \subseteq \mathbf{R}[X, Y]$ subinelul polinoamelor simetrice. Arătați că inelul factor $A/(X^2 + Y^2)$ este izomorf cu $\mathbf{R}[X]$.

Capitolul 7

Determinanți

În acest capitol se definește determinantul unei matrice pătratice cu elemente dintr-un inel comutativ și se trec în revistă proprietățile determinantilor. Se demonstrează rezultate importante precum regula lui Laplace, regula lui Cramer sau formula Binet-Cauchy.

7.1 Proprietățile determinantilor

Fie R un inel comutativ, $n \geq 1$ și 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 definiție, *determinantul* matricei A este elementul lui R

$$|A| := \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}. \quad (7.1)$$

Expresia anterioară se mai numește *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) și (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 $\sigma(i) \geq i$, $i = 1, \dots, n$, 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 înțelege linia (coloana) i a matricei A .

Teorema 122 (Proprietăți ale determinantilor).

- (a) O matrice are același determinant cu transpusa sa.
- (b) Un determinant cu o linie nulă este nul.
- (c) Dacă înmulțim o linie a unui determinant cu un element $\lambda \in R$, determinantul se înmulțește cu λ .
- (d) Dacă o linie a unui determinant $|A|$ are forma $(b_1 + c_1, \dots, b_n + c_n)$, atunci $|A| = |B| + |C|$, unde $|B|$ resp. $|C|$ sunt determinanții obținuți din $|A|$ înlocuind linia respectivă cu (b_1, \dots, b_n) resp. (c_1, \dots, c_n) .
- (e) Un determinant cu două linii proporționale (e.g., egale) este nul.
- (f) Dacă într-un determinant permutăm două linii, atunci determinantul își schimbă semnul.
- (g) Un determinant nu se schimbă dacă la o linie adunăm o altă linie înmulțită cu un element $\lambda \in R$.
- (h) Proprietățile (b) – (f) au loc și pentru coloane.

Demonstrație. 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: $a_{\sigma^{-1}(1)1}a_{\sigma^{-1}(2)2} \cdots a_{\sigma^{-1}(n)n}$. Ținând seama că o permutare are aceeași semnătură cu inversa sa, avem

$$\begin{aligned} |A| &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma^{-1}) a_{\sigma^{-1}(1)1} a_{\sigma^{-1}(2)2} \cdots a_{\sigma^{-1}(n)n} = \\ &= \sum_{\tau \in S_n} \operatorname{sgn}(\tau) a_{\tau(1)1} a_{\tau(2)2} \cdots a_{\tau(n)n} = |{}^t A|. \end{aligned}$$

(b) și (c) rezută din faptul că fiecare termen din (7.1) conține exact un factor din linia i și anume $a_{i\sigma(i)}$.

$$\begin{aligned} (d). |A| &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{i-1\sigma(i-1)} (b_{\sigma(i)} + c_{\sigma(i)}) a_{i+1\sigma(i+1)} \cdots a_{n\sigma(n)} = \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{i-1\sigma(i-1)} b_{\sigma(i)} a_{i+1\sigma(i+1)} \cdots a_{n\sigma(n)} + \\ &+ \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{i-1\sigma(i-1)} c_{\sigma(i)} a_{i+1\sigma(i+1)} \cdots a_{n\sigma(n)} = |B| + |C|. \end{aligned}$$

(e). Cf. lui (c), e suficient să tratăm cazul a două linii egale, și fie acestea, pentru simplitate, primele două. Cum $S_n = A_n \cup A_n(12)$ este o partiție 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 și fie D matricea astfel obținută. Remarcăm că funcția $\sigma \mapsto \sigma(12) : S_n \rightarrow S_n$ este bijectivă. Deci putem înlocui în formula (7.1), σ cu $\sigma(12)$ și obținem

$$|A| = - \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(2)} a_{2\sigma(1)} \cdots a_{n\sigma(n)} = -|D|.$$

(g). Fie B matricea obținută din A prin adunarea la linia i a elementelor liniei j înmulțite cu un element $\lambda \in R$. Aplicând proprietatea (d) pentru linia i a matricei B obținem $|B| = |A| + \Delta$, unde Δ este un determinant cu două linii proporționale, deci $\Delta = 0$, cf. (e).

(h) rezultă din (a). •

Corolarul 123 *Dacă una din liniile (resp. coloanele) unui determinant este combinație liniară de celelalte linii (resp. coloane), atunci determinantul este nul. În particular, dacă R este corp și $|A| \neq 0$, atunci liniile lui A (resp. coloanele lui A) constituie o bază a R -spațiului vectorial R^n .*

Demonstrație. Prima afirmație rezultă din pct. (b), (d) și (h) ale teoremei. A doua rezultă din faptul că n vectori din R^n formează o R -bază a lui R^n dacă și numai dacă nici unul din ei nu este combinație liniară de ceilalți. •

Teorema 124 *Fie $A = (a_{ij})_{1 \leq i, j \leq n}$ o matrice pătratică de ordinul n cu elemente din inelul comutativ R și $\varphi : R \rightarrow S$ un morfism de inele. Aplicând φ fiecărui element al lui A obținem matricea $B = (\varphi(a_{ij}))_{1 \leq i, j \leq n}$. Atunci $\varphi(|A|) = |B|$.*

Demonstrație.

$$\begin{aligned} \varphi(|A|) &= \varphi\left(\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}\right) = \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \varphi(a_{1\sigma(1)}) \varphi(a_{2\sigma(2)}) \cdots \varphi(a_{n\sigma(n)}) = |B|. \bullet \end{aligned}$$

Teorema 125 (Determinantul Vandermonde.) *Fie R un inel comutativ și $a_1, \dots, a_n \in R$. Atunci*

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{vmatrix} = \prod_{1 \leq j < i \leq n} (a_i - a_j).$$

Demonstrație. Fie f determinantul din enunț (determinantul Vandermonde). E suficient să dăm demonstrația în cazul inelului de polinoame $T = \mathbf{Z}[X_1, X_2, \dots, X_n]$ pentru $a_i = X_i$, $i = 1, \dots, n$. Aceasta rezultă din teorema anterioară aplicată morfismului de inele $P(X_1, \dots, X_n) \mapsto P(a_1, \dots, a_n) : T \rightarrow R$. Privit ca polinom în nedeterminata X_n , f are rădăcinile X_1, \dots, 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 același raționament, vedem că f_1 , privit ca polinom în nedeterminata X_{n-1} , are rădăcinile X_1, \dots, 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 obținem

$$f = b \prod_{1 \leq j < i \leq n} (X_i - X_j).$$

Cum atât f cât și $h = \prod_{1 \leq j < i \leq n} (X_i - X_j)$ 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 și h cu coeficientul 1, rezultă că $b = 1$. •

7.2 Dezvoltări ale determinanților.

Fie R un inel comutativ, $n \geq 1$ și 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 subdeterminant al lui $|A|$ aflat la intersecția a m linii și m coloane ale lui $|A|$. Mai concret, m -minorul definit de liniile $1 \leq k_1 < k_2 < \dots < k_m \leq n$ și coloanele $1 \leq l_1 < l_2 < \dots < l_m \leq n$ este

$$M = \begin{vmatrix} a_{k_1 l_1} & \dots & a_{k_1 l_m} \\ \vdots & \ddots & \vdots \\ a_{k_m l_1} & \dots & a_{k_m l_m} \end{vmatrix}.$$

Prin definiție, *minorul complementar al lui M* este $(n - m)$ -minorul \overline{M} al lui A obținut din $|A|$ prin tăierea liniilor $1 \leq k_1 < k_2 < \dots < k_m \leq n$ și coloanelor $1 \leq l_1 < l_2 < \dots < l_m \leq n$ (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 definiție $(-1)^s \overline{M}$, unde $s = k_1 + \dots + k_m + l_1 + \dots + l_m$. 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 numește *complementul algebric al elementului a_{ij}* . Acesta este $A_{ij} := (-1)^{i+j} D$, unde D este minorul obținut din $|A|$ prin tăierea liniei i și 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 $1 \leq k_1 < k_2 < \dots < k_m \leq n$. Fie Γ mulțimea m -minorilor lui A cu elemente din liniile fixate k_1, k_2, \dots, k_m . Atunci

$$|A| = \sum_{M \in \Gamma} M M'$$

altfel zis, $|A|$ este egal cu suma tuturor produselor dintre M și complementul său algebric, când M parcurge mulțimea 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 obținem

$$\begin{vmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \\ 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{vmatrix} = (-1)^6 \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} \begin{vmatrix} 3 & 4 \\ 7 & 8 \end{vmatrix} + (-1)^8 \begin{vmatrix} 1 & 0 \\ 0 & 2 \end{vmatrix} \begin{vmatrix} 2 & 3 \\ 6 & 7 \end{vmatrix} +$$

$$+(-1)^8 \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} \begin{vmatrix} 1 & 4 \\ 5 & 8 \end{vmatrix} + (-1)^{10} \begin{vmatrix} 1 & 0 \\ 0 & 2 \end{vmatrix} \begin{vmatrix} 1 & 2 \\ 5 & 6 \end{vmatrix} = -4 - 8 + 12 - 8 = -8.$$

Vom demonstra teorema ulterior. În cazul $m = 1$ obținem 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, obținem 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 obținute 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 $A = (a_{ij})_{1 \leq i, j \leq n}$ o matrice pătratică cu elemente din inelul comutativ R și fie $1 \leq k, l \leq n$ fixate. Atunci

$$a_{k1}A_{l1} + a_{k2}A_{l2} + \cdots + a_{kn}A_{ln} = \delta_{kl}|A|$$

și

$$a_{1k}A_{1l} + a_{2k}A_{2l} + \cdots + a_{nk}A_{nl} = \delta_{kl}|A|$$

unde A_{ij} este complementul algebric al elementului a_{ij} iar δ_{kl} este simbolul lui Kronecker. În particular

$$AA^* = A^*A = |A|I_n.$$

Demonstrație. Probăm prima relație. Cazul $k = l$ a fost explicitat mai sus, deci putem presupune $k \neq l$. $d = a_{k1}A_{l1} + a_{k2}A_{l2} + \cdots + a_{kn}A_{ln}$ reprezintă dezvoltarea după linia l a determinantului obținut din $|A|$ prin înlocuirea liniei l cu linia k , deci $d = 0$ (determinant cu două linii egale). A doua afirmație rezultă analog. Ultima afirmație rezultă din primele două și din definiția matricei adjuncte. •

Pentru demonstrația teoremei 126 avem nevoie de următoarea leamnă. Fie M un m -minor al lui A și M' complementul său algebric. Fie $M = M_1 + \dots + M_m!$ și $M' = N_1 + \dots + N_{(n-m)!}$ 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 $M_i N_j$ este un termen din dezvoltarea lui $|A|$.

Demonstrație. Pentru început, presupunem că M este m -minorul “stânga-sus”, adică cel definit de primele m linii și m coloane ale lui A . Atunci M' este chiar minorul complementar al lui M , deoarece $1 + \dots + m + 1 + \dots + m = 2m$ este număr par. Fie $(-1)^\alpha a_{1t_1} a_{2t_2} \dots a_{mt_m}$ resp. $(-1)^\beta a_{m+1t_{m+1}} a_{m+2t_{m+2}} \dots a_{mt_n}$ un termen din dezvoltarea lui M resp. M' unde α resp. β este numărul de inversiuni ale permutării $\begin{pmatrix} 1 & \dots & m \\ t_1 & \dots & t_m \end{pmatrix}$ resp. $\begin{pmatrix} m+1 & \dots & n \\ t_{m+1} & \dots & t_n \end{pmatrix}$. E suficient să observăm că permutarea $\begin{pmatrix} 1 & \dots & m & m+1 & \dots & n \\ t_1 & \dots & t_m & t_{m+1} & \dots & t_n \end{pmatrix}$ are $\alpha + \beta$ inversiuni, deoarece $t_1, \dots, t_m \in \{1, \dots, m\}$ și $t_{m+1}, \dots, t_n \in \{m+1, \dots, n\}$.

Presupunem acum că M este m -minorul definit de liniile $1 \leq k_1 < k_2 < \dots < k_m \leq n$ și coloanele $1 \leq l_1 < l_2 < \dots < l_m \leq n$. 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, ș.a.m.d. Continuăm pe coloane. Procedând astfel aducem minorul M în poziția stânga-sus S prin $k_1 + \dots + k_m - (1 + \dots + m)$ permutări de linii vecine și $l_1 + \dots + l_m - (1 + \dots + m)$ permutări de coloane vecine. Făcând astfel, ordinea liniilor și coloanelor din M și M' se păstrează iar $|A|$ se înmulțește cu $(-1)^w$ cu $w = k_1 + \dots + k_m + l_1 + \dots + l_m$. Ne-am redus astfel la cazul analizat anterior deoarece $M' = (-1)^w \overline{M}$, unde \overline{M} este minorul complementar al lui M . •

Demonstrația teoremei 126. Fie M, N doi m -minori distincți cu elemente din liniile k_1, \dots, k_m . Atunci dezvoltările lui MM' și NN' nu au termeni comuni, deoarece M, N au cel puțin 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 toți. •

7.3 Aplicații

Teorema 129 Fie A, B două matrice pătratice de ordinul n cu elemente din inelul comutativ R . Atunci $|AB| = |A||B|$.

Demonstrație. Fie C matricea pătratică 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 și 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 $1, \dots, n$ înmulțite respectiv cu b_{1k}, \dots, b_{nk} . În urma acestei operații, primele n elemente de pe coloana k a lui C vor fi $(a_{i1}b_{1k} + \dots + a_{in}b_{nk})_{1 \leq i \leq n}$. Se obține $|C| = \begin{vmatrix} A & AB \\ -I_n & 0 \end{vmatrix}$. Dezvoltând din nou cu regula lui Laplace pe primele n linii, găsim $|C| = (-1)^w | -I_n | |AB|$, unde $w = 1 + \dots + n + (n+1) + \dots + 2n = n(2n+1)$. Deci $|C| = (-1)^{2n^2+2n} |AB| = |AB|$. •

Reamintim că o matrice $A \in M_n(R)$, R inel comutativ, se numește *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 și 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 .

Demonstrație. 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 și 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 $AB = I_m$ și $BA = I_n$, atunci $m = n$.

Demonstrație. Presupunem că $m > n$. Considerăm matricele pătratice de ordinul m , $C = \begin{pmatrix} A & 0_{m(m-n)} \end{pmatrix}$ și $D = \begin{pmatrix} B \\ 0_{(m-n)m} \end{pmatrix}$. Se observă că $CD = I_m$, deci $0 = |C||D| = |CD| = 1$, contradicție. •

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 și $b_1, \dots, b_n \in R$. Dacă $|A|$ este un element inversabil în R , atunci sistemul de ecuații liniare

$$\sum_{j=1}^n a_{ij}x_j = b_i, \quad i = 1, \dots, n$$

este compatibil determinat cu soluția unică $(\Delta_1|A|^{-1}, \dots, \Delta_n|A|^{-1})$, unde Δ_j este determinantul obținut din $|A|$ prin înlocuirea coloanei j cu vectorul termenilor liberi $\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$.

Demonstrație. Scris matriceal, sistemul este $Ax = b$ unde $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ și $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$. Deci el are soluția unică $s = A^{-1}b = \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}$. Fie c_1, \dots, c_n coloanele lui A . Rezultă că $b = s_1c_1 + \dots + s_nc_n$. Notând cu $|b \ c_2 \ \dots \ c_n|$ determinantul cu coloanele b, c_2, \dots, c_n , avem

$$\Delta_1 = |b \ c_2 \ \dots \ c_n| = |b - s_2c_2 - \dots - s_nc_n \ c_2 \ \dots \ c_n| = s_1|A|.$$

Deci $s_1 = \Delta_1|A|^{-1}$ și la fel se arată că $s_j = \Delta_j|A|^{-1}$, $j = 2, \dots, n$.

Altă demonstrație. Fie A_{ij} complementul algebric al lui a_{ij} în matricea A . Înmulțind cu A^* egalitatea $Ax = b$ se obține $|A|x = A^*b$. Pentru $k = 1, \dots, n$, deducem că $|A|x_k = A_{1k}b_1 + A_{2k}b_2 + \dots + A_{nk}b_k$ care este dezvoltarea după coloana k a determinantului matricei obținute din A prin înlocuirea coloanei k cu vectorul b ; deci $x_k = \Delta_k|A|^{-1}$. •

Un sistem de ecuații liniare căruia i se poate aplica regula lui Cramer se numește *sistem Cramer*. De exemplu, sistemul de ecuații 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 și are soluția

$$(c-d)(c-b)(b-d)/\delta, (c-a)(c-d)(d-a)/\delta, (d-a)(d-b)(b-a)/\delta$$

unde $\delta = (c-a)(c-b)(b-a)$, cf. teoremei 125.

Vom folosi următoarea notație. Fie A o matrice de tip (n, p) , $m \leq n, p$ și $I \subseteq \{1, \dots, n\}$, $J \subseteq \{1, \dots, p\}$ mulțimi cu m elemente. Notăm cu A_I^J m -minorul lui A cu format cu liniile cu indici din I și coloanele cu indici din J .

Teorema 133 (Formula Binet-Cauchy). *Fie A și B matrice de tip (n, p) și respectiv (p, q) , și fie $m \leq n, p, q$. Fie $I \subseteq \{1, \dots, n\}$ și $K \subseteq \{1, \dots, q\}$ două submulțimi cu m elemente. Atunci*

$$(AB)_I^K = \sum_J A_I^J B_J^K$$

suma făcându-se după toate submulțimile $J \subseteq \{1, \dots, p\}$ cu m elemente.

Demonstrație. Fie $C = AB$, $I = \{i_1, i_2, \dots, i_m\}$ și $K = \{k_1, k_2, \dots, k_m\}$ cu $i_1 < i_2 < \dots < i_m$ și $k_1 < k_2 < \dots < k_m$. Punem $A = (a_{ij})$, $B = (b_{jk})$ și $C = (c_{ik})$. Fie s_1, \dots, s_m o permutare a numerelor k_1, \dots, k_m , adică $\{s_1, \dots, s_m\} = \{k_1, \dots, k_m\}$. Atunci signatura permutării $\begin{pmatrix} k_1 & k_2 & \dots & k_m \\ s_1 & s_2 & \dots & s_m \end{pmatrix}$ este $(-1)^{Inv(s_1, \dots, s_m)}$ unde $Inv(s_1, \dots, s_m)$ este numărul perechilor (u, v) , $1 \leq u < v \leq m$, cu $s_u > s_v$. Avem

$$\begin{aligned} C_I^K &= C_{i_1, \dots, i_m}^{k_1, \dots, k_m} = \sum_{\{s_1, \dots, s_m\} = \{k_1, \dots, k_m\}} (-1)^{Inv(s_1, \dots, s_m)} c_{i_1 s_1} \cdots c_{i_m s_m} = \\ &= \sum_{\{s_1, \dots, s_m\} = \{k_1, \dots, k_m\}} (-1)^{Inv(s_1, \dots, s_m)} \left(\sum_{t_1=1}^p a_{i_1 t_1} b_{t_1 s_1} \right) \cdots \left(\sum_{t_m=1}^p a_{i_m t_m} b_{t_m s_m} \right) = \end{aligned}$$

$$\begin{aligned}
&= \sum_{t_1=1}^p \cdots \sum_{t_m=1}^p a_{i_1 t_1} \cdots a_{i_m t_m} \sum_{\{s_1, \dots, s_m\}=\{k_1, \dots, k_m\}} (-1)^{Inv(s_1, \dots, s_m)} b_{t_1 s_1} \cdots b_{t_m s_m} = \\
&= \sum_{t_1=1}^p \cdots \sum_{t_m=1}^p a_{i_1 t_1} \cdots a_{i_m t_m} B_{t_1, \dots, t_m}^{k_1, \dots, k_m}
\end{aligned}$$

unde $B_{t_1, \dots, t_m}^{k_1, \dots, k_m}$ desemnează m -minorul lui B cu liniile t_1, \dots, t_m și 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

$$\begin{aligned}
C_I^K &= \sum_{1 \leq j_1 < \dots < j_m \leq p} \sum_{\{t_1, \dots, t_m\}=\{j_1, \dots, j_m\}} a_{i_1 t_1} \cdots a_{i_m t_m} (-1)^{Inv(t_1, \dots, t_m)} B_{j_1, \dots, j_m}^{k_1, \dots, k_m} = \\
&= \sum_{1 \leq j_1 < \dots < j_m \leq p} B_{j_1, \dots, j_m}^{k_1, \dots, k_m} \sum_{\{t_1, \dots, t_m\}=\{j_1, \dots, j_m\}} (-1)^{Inv(t_1, \dots, t_m)} a_{i_1 t_1} \cdots a_{i_m t_m} = \\
&= \sum_{1 \leq j_1 < \dots < j_m \leq p} B_{j_1, \dots, j_m}^{k_1, \dots, k_m} A_{i_1, \dots, i_m}^{j_1, \dots, j_m} = \sum_J A_I^J B_J^K. \bullet
\end{aligned}$$

Cazul $m = 1$ al formulei Binet-Cauchy este chiar regula de înmulțire a două matrice, iar în cazul $m = n = p = q$ se obține $|AB| = |A||B|$, deci o nouă demonstrație a teoremei 129.

7.4 Exerciții

175. Calculați determinanții

$$\begin{vmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{vmatrix}, \quad \begin{vmatrix} a & b & c \\ b & c & a \\ c & a & b \end{vmatrix}, \quad \begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix}, \quad \begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^3 & b^3 & c^3 \end{vmatrix}, \quad \begin{vmatrix} 1 & 1 & 1 \\ a^2 & b^2 & c^2 \\ a^3 & b^3 & c^3 \end{vmatrix}.$$

176. Fie x_1, x_2, x_3 rădăcinile ecuației $x^3 + px + q = 0$. Calculați discriminantul ecuației, 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 funcție de p și q .

177. Calculați determinanții

$$\begin{vmatrix} a & b & b & b \\ b & a & b & b \\ b & b & a & b \\ b & b & b & a \end{vmatrix}, \quad \begin{vmatrix} 0 & x & y & z \\ x & 0 & z & y \\ y & z & 0 & x \\ z & y & x & 0 \end{vmatrix}, \quad \begin{vmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{vmatrix}.$$

178. Calculați determinantul

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ a_1^{i-1} & a_2^{i-1} & \cdots & a_n^{i-1} \\ a_1^{i+1} & a_2^{i+1} & \cdots & a_n^{i+1} \\ \vdots & \vdots & \cdots & \vdots \\ a_1^n & a_2^n & \cdots & a_n^n \end{vmatrix}.$$

179. Calculați determinantul $\Delta =$

$$\begin{vmatrix} a_1 & x & x & \cdots & x \\ x & a_2 & x & \cdots & x \\ x & x & a_3 & \cdots & x \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ x & x & x & \cdots & a_n \end{vmatrix}.$$

180. Calculați determinantul următor prin dezvoltare Laplace pe liniile 1 și 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. Calculați determinantul $D_n =$

$$\begin{vmatrix} 5 & 3 & 0 & 0 & \cdots & 0 & 0 \\ 2 & 5 & 3 & 0 & \cdots & 0 & 0 \\ 0 & 2 & 5 & 3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 2 & 5 \end{vmatrix}.$$

182. Fie polinomul $f = a_1 + a_2X + \cdots + a_nX^{n-1}$ și matricele

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-3} & a_{n-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ a_2 & a_3 & a_4 & \cdots & a_n & a_1 \end{pmatrix} \text{ și } B = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_n \\ \varepsilon_1^2 & \varepsilon_2^2 & \cdots & \varepsilon_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ \varepsilon_1^{n-1} & \varepsilon_2^{n-1} & \cdots & \varepsilon_n^{n-1} \end{pmatrix}$$

unde $\varepsilon_1, \dots, \varepsilon_n$ sunt rădăcinile de ordinul n ale unității. Arătați că $|AB| = f(\varepsilon_1) \cdots f(\varepsilon_n)|B|$ și calculați $|A|$.

183. Arătați că grupurile abeliene \mathbf{Z}^2 și \mathbf{Z}^3 nu sunt izomorfe.

184. Găsiți un inel necomutativ R și două matrice A resp. B matrice de tip $(1, 2)$ resp. $(2, 1)$ cu elemente din R astfel încât $AB = I_1$ și $BA = I_2$.

185. Numărați matricele inversabile de ordin 3 cu elemente din \mathbf{Z}_2 . Generalizare.

186. Numărați matricele inversabile de ordin 3 cu elemente din \mathbf{Z}_4 .

187. Calculați 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. Calculați inversa matricei $U = \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 0 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 1 & 0 \end{pmatrix}.$

189. Calculați inversa matricei $B = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_n \\ \varepsilon_1^2 & \varepsilon_2^2 & \cdots & \varepsilon_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ \varepsilon_1^{n-1} & \varepsilon_2^{n-1} & \cdots & \varepsilon_n^{n-1} \end{pmatrix}$, unde $\varepsilon_1, \dots, \varepsilon_n$

sunt rădăcinile de ordinul n ale unității.

Capitolul 8

Spații vectoriale și sisteme liniare

În acest capitol se introduc noțiunile de bază referitoare la spații vectoriale. Apoi, se prezintă metoda eliminării a lui Gauss de rezolvare a sistemelor de ecuații liniare și se studiază noțiunea de rang al unei matrice.

În acest capitol, prin corp vom înțelege corp comutativ.

8.1 Spații vectoriale

Fie K un corp. Un *spațiu vectorial* peste corpul K (pe scurt, K -*spațiu vectorial*) este un grup abelian $(V, +)$ împreună cu o operație externă $K \times V \rightarrow V$, $(a, x) \mapsto ax$, numită *înmulțire cu scalari*, care verifică următoarele condiții pentru orice $a, b \in K$ și $x, y \in V$

- (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 notația ${}_K V$ vom înțelege că V este un K -spațiu vectorial. Vom nota cu 0_K scalarul nul și cu 0_V vectorul nul (când nu este pericol de confuzie, vom suprima indicii K și V).

Teorema 134 Fie ${}_K V$ un spațiu vectorial, $a \in K$ și $x \in V$. Atunci

- (a) $ax = 0_V$ dacă și numai dacă $a = 0_K$ sau $x = 0_V$.
 (b) $(-a)x = a(-x) = -ax$.

Demonstrație. (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 $ax = 0_V$ și $a \neq 0_K$, atunci a este inversabil în K și rezultă $x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}0_V = 0_V$.

(b) rezultă din egalitățile $0_V = (a - a)x = ax + (-a)x$ și $0_V = a(x - x) = ax + a(-x)$. •

Exemple. 1. Dacă $n \geq 1$, atunci K^n are o structură de K -spațiu vectorial obținută definind adunarea vectorilor prin $(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$ și înmulțirea cu scalari prin $\alpha(a_1, \dots, a_n) = (\alpha a_1, \dots, \alpha a_n)$, pentru $\alpha, a_1, \dots, a_n, b_1, \dots, b_n \in K$. K^n se numește *spațiul vectorial standard de dimensiune n* .

2. Dacă ${}_K V_1, \dots, {}_K V_n$ sunt spații vectoriale, atunci produsul cartezian $V_1 \times \dots \times V_n$ are o structură de spațiu vectorial obținută definind adunarea vectorilor prin $(v_1, \dots, v_n) + (w_1, \dots, w_n) = (v_1 + w_1, \dots, v_n + w_n)$ și înmulțirea cu scalari prin $\alpha(v_1, \dots, v_n) = (\alpha v_1, \dots, \alpha v_n)$, pentru $\alpha \in K$ și $v_i, w_i \in V_i$, $i = 1, \dots, n$. $V_1 \times \dots \times V_n$ se numește *produsul direct al spațiilor vectoriale V_1, \dots, V_n* .

3. Dacă K este subcorp al inelului L , atunci grupul aditiv al lui L are o structură de K -spațiu vectorial în care înmulțirea cu scalari este chiar înmulțirea din L (dacă $a \in K$ și $x \in L$, ax este produsul dintre a și x în L). De exemplu, \mathbf{R} , \mathbf{C} și $\mathbf{Q}(\sqrt{2})$ sunt \mathbf{Q} -spații vectoriale. De asemenea, $M_n(K)$, $K[X]$ și $K(X)$ sunt K -spații vectoriale.

4. Fie p un număr prim și $(G, +)$ un grup abelian. Se vede ușor că G are o structură de \mathbf{Z}_p -spațiu vectorial dacă și numai dacă $px = 0$ pentru orice $x \in G$. În acest caz, înmulțirea cu scalari se definește prin $\hat{a}x = ax$, pentru $a \in \mathbf{Z}$ și $x \in G$. Definiția 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 -spații vectoriale. O funcție $f : V \rightarrow W$ se numește *morfism de spații vectoriale* sau *aplicație liniară* dacă $f(ax + by) = af(x) + bf(y)$ pentru orice $a, b \in K$ și $x, y \in V$. f este în particular morfism de grupuri abeliene, deci $f(0) = 0$, $f(-x) = -f(x)$ pentru orice $x \in V$ și f este injecție dacă și numai dacă $\ker(f) = \{0\}$, unde $\ker(f) = \{x \in V \mid f(x) = 0\}$

este nucleul lui f . Un morfism $f : V \rightarrow V$ se numește *endomorfism* al lui V .

Fie V, W două K -spații vectoriale. Morfismul $x \mapsto 0 : V \rightarrow W$ este numit *morfismul trivial*, iar $I_V : V \rightarrow V$, $I_V(x) = x$ este numit *morfismul identic*. Dacă $a \in K$, atunci endomorfismul $x \mapsto ax : V \rightarrow V$ este numit *omotetia* definită de a .

Un morfism de spații vectoriale bijectiv se numește *izomorfism* iar două spații vectoriale se zic *izomorfe* dacă există un izomorfism între ele.

Teorema 135 (a) *Compunerea a două morfisme de spații vectoriale este un morfism de spații vectoriale.*

(b) *Inversul unui izomorfism de spații vectoriale este tot un izomorfism.*

Demonstrație. (a). Fie $f : V \rightarrow V'$ și $g : V' \rightarrow V''$ morfisme de K -spații vectoriale și 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 $f : V \rightarrow V'$ un izomorfism și fie $x, y \in V'$, $a, b \in K$. Notăm $x' = f^{-1}(x)$ și $y' = f^{-1}(y)$. 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 submulțime nevidă W a unui spațiu vectorial ${}_K V$ este *subspațiu al lui V* (și notăm $W \leq V$) dacă $ax + by \in W$ pentru orice $a, b \in K$ și $x, y \in W$. Dacă $W \leq V$, atunci W este K -spațiu vectorial față de operațiile de adunare a vectorilor și înmulțire cu scalari induse din V . Pentru orice spațiu vectorial ${}_K V$, $\{0\}$ și V sunt subspații numite *subspațiul trivial* respectiv *subspațiul impropriu*. Subspațiul nul $\{0\}$ se mai notează simplu cu 0 .

Fie $a, b \in \mathbf{R}$ cu $a^2 + b^2 \neq 0$. Atunci dreapta $\{(x, y) \mid ax + by = 0\}$ este un subspațiu al lui ${}_R \mathbf{R}^2$.

Teorema 136 *Fie $f : V \rightarrow W$ o aplicație 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 și imaginea lui f sunt subspații.

Demonstrație. (a). Fie $x, y \in V'$ și $a, b \in K$. Atunci $ax + by \in V'$, deci $af(x) + bf(y) = f(ax + by) \in W$. (b). Fie $x, y \in f^{-1}(W')$ și $a, b \in K$. 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 ${}_K V$ un spațiu vectorial și $(V_i)_{i \in I}$ o familie de subspații ale lui V , atunci intersecția subspațiilor V_i este de asemenea un subspațiu al lui V , deoarece dacă $a, b \in K$ și $x, y \in \cap_{i \in I} V_i$, atunci $ax + by$ este în fiecare V_i , deci $ax + by \in \cap_{i \in I} V_i$.

Dacă ${}_K V$ un spațiu vectorial și V_1, \dots, V_n subspații ale lui V , atunci

$$V_1 + \dots + V_n = \{x_1 + \dots + x_n \mid x_i \in V_i, i = 1, \dots, n\}$$

este de asemenea un subspațiu al lui V , numit *suma subspațiilor* V_1, \dots, V_n . Într-adevăr, dacă $x_i, y_i \in V_i, i = 1, \dots, n$, și $a, b \in K$, atunci $a(x_1 + \dots + x_n) + b(y_1 + \dots + y_n) = (ax_1 + by_1) + \dots + (ax_n + by_n) \in V_1 + \dots + V_n$, deoarece $ax_i + by_i \in V_i$ pentru orice i . Mai general, suma unei familii F de subspații se definește ca reuniunea sumelor tuturor subfamiliilor finite ale lui F .

În ${}_R \mathbf{R}^3$, suma subspațiilor

$$V_1 = \{(x, y, 0) \mid x, y \in \mathbf{R}\}, \quad V_2 = \{(0, x, y) \mid x, y \in \mathbf{R}\}$$

este \mathbf{R}^3 iar intersecția lor este $\{(0, x, 0) \mid x \in \mathbf{R}\}$.

Spunem că spațiu vectorial ${}_K V$ este *suma directă* a subspațiilor V_1 și V_2 , și notăm $V = V_1 \oplus V_2$ dacă $V = V_1 + V_2$ și $V_1 \cap V_2 = 0$. De exemplu, ${}_R \mathbf{R}^3$ este suma directă a subspațiilor $V_1 = \{(x, y, 0) \mid x, y \in \mathbf{R}\}$ și $V_2 = \{(0, 0, z) \mid z \in \mathbf{R}\}$.

Fie ${}_K V$ un spațiu vectorial și $v_1, \dots, v_n \in V$. Notăm cu $\langle v_1, \dots, v_n \rangle$ mulțimea tuturor *combinațiilor liniare* ale elementelor v_1, \dots, v_n , adică a sumelor $a_1 v_1 + \dots + a_n v_n$ cu $a_1, \dots, a_n \in K$. $\langle v_1, \dots, v_n \rangle$ este un subspațiu al lui V numit *subspațiul generat de* v_1, \dots, v_n .

Într-adevăr, dacă $c, d, a_1, \dots, a_n, b_1, \dots, b_n \in K$, atunci $c(a_1 v_1 + \dots + a_n v_n) + b(a_1 v_1 + \dots + a_n v_n) = (ca_1 + db_1)v_1 + \dots + (ca_n + db_n)v_n$.

E clar că dacă W este un subspațiu al lui V care conține elementele v_1, \dots, v_n , atunci $\langle v_1, \dots, v_n \rangle \subseteq W$. Deci $\langle v_1, \dots, v_n \rangle$ este intersecția tuturor subspațiilor lui V care conțin elementele v_1, \dots, v_n .

În general, subspațiul generat de o submulțime nu neapărat finită G a lui V se definește ca mulțimea tuturor combinațiilor liniare ale submulțimilor finite ale lui G , $\langle G \rangle := \{a_1 v_1 + \dots + a_n v_n \mid a_1, \dots, a_n \in K, v_1, \dots, v_n \in G, n \geq 0\}$.

Spunem că un spațiu vectorial ${}_K V$ este *finit generat* dacă există o mulțime de vectori v_1, \dots, v_n astfel încât $V = \langle v_1, \dots, v_n \rangle$.

Spunem că o mulțime de vectori v_1, \dots, v_n ai spațiului vectorial ${}_K V$ este *liniar independentă* (sau că vectorii v_1, \dots, v_n sunt *liniar independenți*), dacă singura combinație liniară nulă a vectorilor v_1, \dots, v_n este cea trivială, adică dacă $a_1, \dots, a_n \in K$ și $a_1 v_1 + \dots + a_n v_n = 0$ implică $a_1 = \dots = a_n = 0$. Mulțimea vidă este *liniar independentă*.

În general, spunem că o submulțime nu neapărat finită G a lui V este *liniar independentă* dacă orice submulțime finită alui G este *liniar independentă*. O submulțime T a lui V se zice *liniar dependentă* dacă nu este *liniar independentă*.

E clar că o submulțime a unei mulțimi *liniar independente* este *liniar independentă* și că o mulțime *liniar independentă* nu conține vectorul nul (deoarece $1 \cdot 0_V = 0_V$).

Teorema 137 *Fie ${}_K V$ un spațiu vectorial și $v_1, \dots, v_n \in V$. Afirmațiile următoare sunt echivalente.*

- (a) *Vectorii v_1, \dots, v_n sunt liniar independenți.*
- (b) *Nici unul dintre vectorii v_1, \dots, v_n nu este o combinație liniară a celorlalți.*
- (c) *$v_1 \neq 0$, $v_2 \notin \langle v_1 \rangle$, ..., $v_n \notin \langle v_1, \dots, v_{n-1} \rangle$.*

Demonstrație. Implicația (b) \Rightarrow (c) este clară.

(c) \Rightarrow (a). Presupunem că vectorii v_1, \dots, v_n sunt *liniar dependenți*. Atunci există $a_1, \dots, a_j \in K$, $a_j \neq 0$, astfel încât $a_1 v_1 + \dots + a_j v_j = 0$. Deci $v_j = -(a_1/a_j)v_1 - \dots - (a_{j-1}/a_j)v_{j-1} \in \langle v_1, \dots, v_{j-1} \rangle$.

(a) \Rightarrow (b). Dacă vectorul v_i este combinație liniară a celorlalți, să zicem, $v_i = a_1 v_1 + \dots + a_{i-1} v_{i-1} + a_{i+1} v_{i+1} + \dots + a_n v_n$, atunci $a_1 v_1 + \dots + a_{i-1} v_{i-1} - v_i + a_{i+1} v_{i+1} + \dots + a_n v_n = 0$, deci vectorii v_1, \dots, v_n sunt *liniar dependenți*. •

Teorema 138 (Teorema schimbului.) *Fie ${}_K V$ un spațiu vectorial finit generat, w_1, \dots, w_n un sistem de generatori al lui V și $v_1, \dots, v_m \in V$ vectori liniar independenți. Atunci $m \leq n$ și după o renumerotare a vectorilor w_1, \dots, w_n , $\langle v_1, \dots, v_m, w_{m+1}, \dots, w_n \rangle = V$.*

Demonstrație. Facem inducție după m . Pentru $m = 0$ afirmația e clară. Fie $m \geq 1$. Din ipoteza de inducție, putem renumera vectorii w_1, \dots, w_n astfel încât $\langle v_1, \dots, v_{m-1}, w_m, \dots, w_n \rangle = V$. Deci putem scrie pe v_m ca o

combinație liniară $v_m = a_1v_1 + \dots + a_{m-1}v_{m-1} + a_mw_m + \dots + a_nw_n$ cu $a_i \in K$. Cum v_1, \dots, v_m sunt liniar independenți, rezultă că $n \geq m$ și nu toți scalarii a_m, \dots, a_n sunt nuli; renumerotând vectorii w_m, \dots, w_n , putem presupune că $a_m \neq 0$. Rezultă că $w_m = -(a_1/a_m)v_1 - \dots - (a_{m-1}/a_m)v_{m-1} + (1/a_m)v_m - (a_{m+1}/a_m)w_{m+1} - \dots - (a_n/a_m)w_n$. Deci $V = \langle v_1, \dots, v_{m-1}, w_m, \dots, w_n \rangle \subseteq \langle v_1, \dots, v_m, w_{m+1}, \dots, w_n \rangle$, adică $\langle v_1, \dots, v_m, w_{m+1}, \dots, w_n \rangle = V$.

Fie ${}_K V$ un spațiu vectorial. O *bază* a lui V este o submulțime a lui V care este simultan liniar independentă și sistem de generatori pentru V . Vectorii $e_1 = (1, \dots, 0)$, $e_2 = (0, 1, \dots, 0)$, ..., $e_n = (0, 0, \dots, 0, 1)$ formează o bază a lui K^n numită *baza canonică*. Verificarea se face ușor folosind egalitatea $(a_1, \dots, a_n) = a_1e_1 + \dots + a_ne_n$, pentru $a_1, \dots, a_n \in K$. De asemenea, $\{1, X, X^2, \dots\}$ este o K -bază a lui $K[X]$.

Teorema 139 *Dacă e_1, e_2, \dots, e_n este o bază a spațiului vectorial V , atunci orice element $x \in V$ se scrie în mod unic sub forma*

$$x = x_1e_1 + x_2e_2 + \dots + x_ne_n \text{ cu } x_i \in K$$

(x_1, x_2, \dots, x_n se numesc coordonatele lui x în baza e_1, e_2, \dots, e_n).

Demonstrație. Scrierea din enunț există pentru că e_1, e_2, \dots, e_n îl generează pe V . Dacă x se mai scrie și sub forma $x = y_1e_1 + y_2e_2 + \dots + y_ne_n$ cu $y_i \in K$, atunci, scăzând cele două exprimări ale lui x , obținem $0 = (x_1 - y_1)e_1 + (x_2 - y_2)e_2 + \dots + (x_n - y_n)e_n$, deci $x_1 = y_1$, $x_2 = y_2$, ..., $x_n = y_n$, deoarece vectorii e_1, e_2, \dots, e_n sunt liniar independenți. •

De exemplu, în baza canonică a lui K^n , coordonatele vectorului (a_1, a_2, \dots, a_n) sunt chiar a_1, a_2, \dots, a_n ; coordonatele aceluiași vector în baza $(1, 0, 0, \dots, 0)$, $(1, 1, 0, \dots, 0)$, ..., $(1, 1, 1, \dots, 1)$ sunt $a_1 - a_2, a_2 - a_3, \dots, a_{n-1} - a_n, a_n$.

Teorema 140 *Orice spațiu vectorial ${}_K V$ finit generat admite o bază finită și orice două baze au același număr de elemente. Cardinalul comun al tuturor bazelor se numește dimensiunea lui V și se notează cu $\dim(V)$.*

Demonstrație. Fie G un sistem finit de generatori al lui V și $S \subseteq G$ o submulțime liniar independentă (eventual $S = \emptyset$). Fie B o mulțime liniar independentă maximală cu proprietatea $S \subseteq B \subseteq G$. Atunci $\langle B \rangle = V$,

deoarece dacă $y \in G \setminus \langle B \rangle$, atunci $B \cup \{y\}$ este liniar independentă, contradicție. Deci B bază.

Arătăm acum că orice două baze au același număr de elemente. Fie B o bază cu m elemente și C o altă bază cu n elemente. Cum B este mulțime liniar independentă și C sistem de generatori, din teorema schimbului rezultă că $m \leq n$. Inversând rolurile lui B și C rezultă că $n \leq m$, deci $m = n$. •

Folosind baza canonică $e_1 = (1, \dots, 0)$, $e_2 = (0, 1, \dots, 0), \dots, e_n = (0, 0, \dots, 0, 1)$ vedem că spațiul vectorial standard K^n are dimensiunea n . Din demonstrația precedentă și din teorema schimbului, rezultă

Corolarul 141 *Fie ${}_K V$ un spațiu vectorial n -dimensional. Atunci din orice sistem de generatori se poate extrage o bază și orice mulțime liniar independentă se poate extinde la o bază. În particular, orice mulțime cu n elemente care este liniar independentă sau sistem de generatori este bază.*

Teorema 140 este adevărată și pentru spații care nu sunt finit generate (vezi [5, teorema V.4.3]). Din acest motiv vom numi spațiile finit generate spații *finit dimensionale*, iar pe cele care nu sunt finit generate spații *infini dimensionale*. De exemplu, ${}_K K^n$ este n -dimensional, iar ${}_K K[X]$ este infinit dimensional.

Teorema 142 *Fie ${}_K V$ un spațiu vectorial finit generat și W un subspațiu al lui V . Atunci W este finit generat și $\dim(W) \leq \dim(V)$. În plus, $W = V$ dacă și numai dacă $\dim(W) = \dim(V)$.*

Demonstrație. Fie $n = \dim(V)$. Din teorema schimbului, orice submulțime liniar independentă a lui W are cel mult n elemente. Din teorema 137 rezultă că W este finit generat și $\dim(W) \leq \dim(V)$. Dacă $\dim(W) = \dim(V)$, atunci orice bază a lui W este și o bază a lui V , cf. corolarului 141. •

Teorema 143 *Fie V un K -spațiu vectorial n -dimensional și fie $E = \{e_1, \dots, e_n\}$, $F = \{f_1, \dots, f_n\}$ baze ale lui V . Exprimăm fiecare vector f_j în baza E ,*

$$f_j = \sum_{i=1}^n a_{ij} e_i, \quad j = 1, \dots, n.$$

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, \dots, x_n și în baza F coordonatele y_1, y_2, \dots, y_n , atunci

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = A \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}.$$

Demonstrație. Fie $B = (b_{ij})_{1 \leq i, j \leq n}$ matricea de trecere de la F la E . Pentru $k = 1, \dots, n$ avem

$$e_k = \sum_{j=1}^n b_{jk} f_j = \sum_{j=1}^n b_{jk} \sum_{i=1}^n a_{ij} e_i = \sum_{i=1}^n \left(\sum_{j=1}^n a_{ij} b_{jk} \right) e_i.$$

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,

$$x = \sum_{j=1}^n y_j f_j = \sum_{j=1}^n y_j \sum_{i=1}^n a_{ij} e_i = \sum_{i=1}^n \left(\sum_{j=1}^n a_{ij} y_j \right) e_i. \quad \bullet$$

Teorema 144 Fie V și W două spații vectoriale. Presupunem că e_1, e_2, \dots, e_n este o bază a lui V și $f_1, f_2, \dots, f_n \in W$. Atunci există și este unică o aplicație liniară $\alpha : V \rightarrow W$ cu proprietatea $\alpha(e_i) = f_i$, $i = 1, \dots, n$. În plus, f_1, f_2, \dots, f_n este bază a lui W dacă și numai dacă α este izomorfism.

Demonstrație. Fie $\alpha : V \rightarrow W$ o aplicație liniară cu proprietatea $\alpha(e_i) = f_i$, $i = 1, \dots, n$. Dacă $a_1, \dots, a_n \in K$, 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 aplicația $\alpha : V \rightarrow W$ dată prin $\alpha(\sum_{i=1}^n a_i e_i) = \sum_{i=1}^n a_i f_i$. E ușor de văzut că α este aplicație liniară și $\alpha(e_i) = f_i$, $i = 1, \dots, n$.

E clar că dacă α este izomorfism, atunci f_1, f_2, \dots, f_n este bază a lui W . Reciproc, presupunem că f_1, f_2, \dots, f_n este bază a lui W . Conform primei părți, există și este unică o aplicație liniară $\beta : W \rightarrow V$ cu proprietatea $\beta(f_i) = e_i$, $i = 1, \dots, n$. Atunci $\beta\alpha$ este un endomorfism al lui V cu proprietatea $\beta\alpha(e_i) = e_i$, $i = 1, \dots, n$. Din prima parte rezultă că $\beta\alpha = I$. \bullet

Corolarul 145 *Un spațiu vectorial n -dimensional este izomorf cu spațiul standard K^n . În particular, două spații vectoriale finit dimensionale sunt izomorfe dacă și numai dacă au aceeași dimensiune.*

Corolarul 146 *Fie K un corp finit de caracteristică p . Atunci K are p^n elemente.*

Demonstrație. K se poate organiza ca spațiu vectorial peste corpul \mathbf{Z}_p definind înmulțirea cu scalari prin $\hat{a}x = ax$ 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 $f : V \rightarrow W$ un morfism de K -spații vectoriale. Dimensiunea $\dim(\text{Im}(f))$ a imaginii lui f se numește *rangul* lui f și se notează $\text{rang}(f)$. De asemenea, dimensiunea $\dim(\ker(f))$ a nucleului lui f se numește *defectul* lui f și se notează $\text{defect}(f)$; deci morfismele injective sunt cele de defect nul.

De exemplu, dacă V este un spațiu vectorial n -dimensional, atunci morfismul trivial are rangul 0 și defectul n , iar morfismul identic are rangul n și defectul 0.

Teorema 147 (Teorema rang-defect.) *Fie $f : V \rightarrow W$ un morfism de K -spații vectoriale finit dimensionale. Atunci $\dim(V) = \text{rang}(f) + \text{defect}(f)$.*

Demonstrație. Fie $E = \{e_1, \dots, e_k, e_{k+1}, \dots, e_n\}$ unde e_1, \dots, e_k este o bază a lui $\ker(u)$ iar $u(e_{k+1}), \dots, u(e_n)$ este o bază a lui $\text{Im}(u)$. Deci $\dim_K(\ker(u)) = k$ și $\dim_K(\text{Im}(u)) = n - k$. 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, \dots, e_k și $u(e_{k+1}), \dots, u(e_n)$ sunt mulțimi liniar independente, avem $\sum_{i=k+1}^n a_i u(e_i) = 0$, deci $a_{k+1} = \dots = a_n = 0$, apoi $\sum_{i=1}^k a_i e_i = 0$, deci $a_1 = \dots = a_k = 0$.

Fie $x \in V$. Putem scrie $u(x) = \sum_{i=k+1}^n b_i u(e_i)$ cu $b_{k+1}, \dots, b_n \in K$. Deci $u(x) - \sum_{i=k+1}^n b_i u(e_i) \in \ker(u)$, deci putem scrie $x - \sum_{i=k+1}^n b_i e_i = \sum_{i=1}^k b_i e_i$, $b_1, \dots, b_k \in K$. Deci $x = \sum_{i=1}^n b_i e_i$. •

Teorema 148 *Fie V și W două spații vectoriale finit generat și W un subspațiu al lui V . Atunci $\dim(V \times W) = \dim(V) + \dim(W)$.*

Demonstrație. Fie $\{e_1, \dots, e_m\}$ o bază a lui V și $\{f_1, \dots, f_n\}$ o bază a lui W . Se arată că $B = \{(e_1, 0), \dots, (e_m, 0), (0, f_1), \dots, (0, f_n)\}$ o bază a lui $V \times W$.

Într-adevăr, fie $(x, y) \in V \times W$. Există $a_1, \dots, a_m, b_1, \dots, b_n \in K$ astfel încât $x = \sum_{i=1}^m a_i e_i$ și $y = \sum_{j=1}^n b_j f_j$. 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 $a_1, \dots, a_m, b_1, \dots, b_n \in K$ 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 $a_1, \dots, a_m, b_1, \dots, b_n$ sunt toți nuli.

O demonstrație mai scurtă se obține aplicând teorema rang-defect proiecției $p_V : V \times W \rightarrow V$, $p_V(x, y) = x$, deoarece $\ker(p_V) = 0 \times W$ este izomorf cu W . •

Teorema precedentă se extinde ușor la cazul produselor directe finite: dacă ${}_K V_1, \dots, {}_K V_n$ sunt spații vectoriale, atunci $\dim(V_1 \times \dots \times V_n) = \dim(V_1) + \dots + \dim(V_n)$.

Teorema 149 (Teorema lui Grassmann.) *Fie Y un spațiu vectorial și V, W subspații finit dimensionale ale lui Y . Atunci $\dim(V + W) = \dim(V) + \dim(W) - \dim(V \cap W)$.*

Demonstrație. Morfismul surjectiv $\pi : V \times W \rightarrow V + W$, $\pi(x, y) = x - y$ are nucleul $T = \{(x, x) \mid x \in V \cap W\}$. Avem izomorfismul $x \mapsto (x, x) : V \cap W \rightarrow T$, deci $\text{defect}(\pi) = \dim(V \cap W)$. Cum π e surjectiv, $\text{rang}(\pi) = \dim(V + W)$. Din teorema 148, $\dim(V \times W) = \dim(V) + \dim(W)$. Se aplică teorema rang-defect. •

8.2 Sisteme de ecuații liniare

Fie K un corp (comutativ) și $m, n \geq 1$. Considerăm sistemul de ecuații liniare

$$\sum_{j=1}^n a_{ij} x_j = b_i, \quad i = 1, \dots, m$$

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 și $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ este vectorul termenilor liberi. O

soluție 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 numește *incompatibil* dacă nu admite nici o soluție, *compatibil determinat* dacă admite o soluție unică și *compatibil nedeterminat* dacă admite cel puțin două soluții. Două sisteme se zic *echivalente* dacă au aceleași soluții.

Se vede ușor că următoarele transformări nu afectează mulțimea soluțiilor unui sistem, deci produc sisteme echivalente cu cel dat.

- a. Adunarea la o ecuație a altei ecuații înmulțite cu un element din K .
- b. Permutarea a două ecuații.
- c. Înmulțirea unei ecuații 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 înmulțite cu un element din K .
2. Permutarea a două linii.
3. Înmulțirea 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 același tip sunt *echivalente pe linii* dacă A se obține din B printr-o succesiune de transformări elementare pe linii. E clar că “echivalența pe linii” este o relație de echivalență pe mulțimea matricelor de același 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 transformările elementare 1 – 3 și $f(C)$ este matricea obținută 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 înmulțită cu elementul $a \in K$.
2. P_{ij} = matricea unitate cu liniile i și j permutate.
3. $D_i(u)$ = matricea unitate cu linia i înmulțită 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 eșalon (pe linii)* o matrice de forma

$$\begin{pmatrix} 0 & \cdots & 0 & 1 & * & \cdots & * & 0 & * & \cdots & * & 0 & * & \cdots & * \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & * & \cdots & * & 0 & * & \cdots & * \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & * & \cdots & * \\ \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \end{pmatrix}.$$

Mai precis o matrice eșalon este o matrice ce verifică următoarele condiții.

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 sfârșit.

Teorema 151 *O matrice eșalon inversabilă este egală cu matricea unitate.*

Demonstrație. O matricea eșalon este superior triunghiulară. Dacă este și inversabilă, atunci pivoții apar pe diagonala principală, deci este matricea unitate. •

Teorema 152 *Orice matrice A cu elemente din K este echivalentă pe linii cu o matrice eșalon unică numită forma eșalon a lui A .*

Demonstrație. Dacă $A = 0$, atunci A este matrice eșalon. 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 și apoi, împărțind prima linie la b , facem $b = 1$, obținând astfel un pivot în poziția $(1, j)$. Prin transformări de tip 1, anulăm elementele aflate dedesubt pe coloana pivotului. Apoi, se aplică același algoritm submatricei obținute din A eliminând linia 1 și primele j coloane. La sfârșit, prin transformări de tip 1, anulăm elementele aflate deasupra pe coloana fiecărui pivot.

Demonstrația unicității, deși în principiu simplă, este destul de laborioasă. De aceea o omitem. •

Corolarul 153 *Dacă A este o matrice, atunci există matricele elementare E_1, \dots, E_k astfel încât $E_k \cdots E_1 A$ este matrice eșalon.*

Corolarul 154 *O matrice pătratică este inversabilă dacă și numai dacă ea este produs de matrice elementare.*

Demonstrație. Fie A o matrice pătratică inversabilă de ordin n . Cf. corolarului precedent, există matricele elementare E_1, \dots, E_k astfel încât $C = E_k \cdots E_1 A$ este matrice eșalon. Conform teoremei 151, $C = I_n$, deci $A = E_1^{-1} \cdots E_k^{-1}$. Reciproca este evidentă. •

Cu notațiile precedente, $A^{-1} = E_k \cdots E_1$, deci A^{-1} se poate obține făcând asupra lui I_n secvența de transformări elementare ce duce pe A în I_n . Deci, eșalonând matricea $(A \ I_n)$ se obține matricea $(I_n \ A^{-1})$. Obținem astfel un algoritm de calcul al inversei unei matrice prin transformări elementare.

Din teorema 152 și comentariile anterioare referitoare la sistemele de ecuații liniare rezultă

Teorema 155 *Orice sistem de ecuații liniare este echivalent cu un sistem având matricea extinsă o matrice eșalon.*

Presupunem că sistemul de ecuații liniare

$$\sum_{j=1}^n a_{ij} x_j = b_i, \quad i = 1, \dots, m$$

are matricea extinsă B matrice eșalon. Observăm că dacă apare un pivot în ultima coloană a lui B , atunci sistemul are o ecuație de forma $0 = 1$, deci este incompatibil. În continuare presupunem că B nu are pivoți pe ultima coloană. Fie p_1, \dots, p_k coloanele ce au pivoți. Numim necunoscutele x_{p_1}, \dots, x_{p_k} *necunoscute principale*, celelalte necunoscute x_{s_1}, \dots, x_{s_l} fiind numite *necunoscute secundare*. Trecând necunoscutele secundare în membrul drept și neglijând ecuațiile de forma $0 = 0$, sistemul devine

$$x_{p_i} = b_i - \sum_{j=1}^l a_{is_j} x_{s_j}, \quad i = 1, \dots, k.$$

Deci sistemul este compatibil, necunoscutele secundare, dacă există, putând lua valori arbitrare. Rezultă următoarea teoremă.

Teorema 156 *Fie un sistem de ecuații liniare cu matricea extinsă B matrice eșalon. Sistemul este compatibil dacă și numai dacă B nu are pivoți pe ultima coloană. Dacă este compatibil, sistemul este compatibil determinat dacă și numai dacă nu există necunoscute secundare, adică matricea sistemului are câte un pivot pe fiecare coloană.*

Metoda de rezolvare a unui sistem de ecuații liniare prin eșalonarea matricei extinse poartă numele de *metoda eliminării a lui Gauss*.

8.3 Rangul unei matrice

Fie K un corp și $A \in M_{mn}(K)$. Prin definiție, *rangul lui A* este numărul, notat $\text{rang}(A)$, egal cu ordinul maxim al unui minor nenul al lui A . Matricea nulă are rangul zero.

Deci $\text{rang}(A) = r$ înseamnă că A are un r -minor nenul și toți minorii de ordin $\geq r + 1$ sunt nuli. Din regula lui Laplace, vedem că $\text{rang}(A) = r$ dacă și numai dacă A are un r -minor nenul și toți minorii de ordin $r + 1$ sunt nuli. Din definiția rangului și din faptul că A și tA au aceeași minori, rezultă că

$$0 \leq \text{rang}(A) \leq \min(m, n) \text{ și } \text{rang}(A) = \text{rang}({}^tA).$$

Dacă $A \in M_n(K)$, atunci $\text{rang}(A) = n$ dacă și numai dacă $|A| \neq 0$.

Teorema 157 *Fie $A \in M_{mn}(K)$ și $B \in M_{np}(K)$. Atunci $\text{rang}(AB) \leq \min(\text{rang}(A), \text{rang}(B))$.*

Demonstrație. Din formula Binet-Cauchy (teorema 133), rezultă că un r -minor al lui AB este combinație liniară de r -minori ai lui A resp. B . •

Corolarul 158 *Fie $A \in M_{mn}(K)$, $U \in GL_m(K)$ și $V \in GL_n(K)$. Atunci*

$$\text{rang}(UA) = \text{rang}(AV) = \text{rang}(A).$$

În particular, două matrice echivalente pe linii au același rang.

Demonstrație. Din teorema precedentă,

$$\text{rang}(UA) \leq \text{rang}(A) \text{ și } \text{rang}(A) = \text{rang}(U^{-1}UA) \leq \text{rang}(UA)$$

deci $\text{rang}(UA) = \text{rang}(A)$. Cealaltă egalitate se probează analog. •

Teorema 159 (Kronecker). *Fie $A \in M_{mn}(K)$. Atunci $\text{rang}(A)$ este egal cu dimensiunea peste K a subspațiului generat de liniile lui A și de asemenea egal cu dimensiunea peste K a subspațiului generat de coloanele lui A .*

Demonstrație. Fie $l(A)$ respectiv $c(A)$ dimensiunea subspațiului generat de liniile respectiv coloanele lui A . Arătăm că $\text{rang}(A) = l(A)$. Se vede ușor că transformările elementare nu afectează $l(A)$. Conform corolarului 158, putem presupune că A este matrice eșalon. Fie p numărul de pivoti ai lui A . E ușor 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 pivotii pe diagonala principală), deci $\text{rang}(A) = p$. În final, $\text{rang}(A) = \text{rang}(^t A) = l(^t A) = c(A)$. •

Din demonstrație rezultă că $\text{rang}(A)$ este egal cu numărul de pivoti ai formei eșalon a lui A .

Corolarul 160 *Fie $A = (a_{ij}) \in M_{mn}(K)$. Presupunem că A are un r -minor nenul M astfel încât toți $(r+1)$ -minorii obținuți din M prin bordare cu elemente din A sunt nuli. Atunci $\text{rang}(A) = r$.*

Demonstrație. Fără a micșora generalitatea, putem presupune că M constă din primele r linii și r coloane ale lui A . Notăm liniile lui A cu A_1, \dots, A_m . Cum M este un r -minor nenul, $\text{rang}(A) \geq r$ și liniile A_1, \dots, A_r sunt liniar independente.

Presupunem că $\text{rang}(A) \geq r+1$. Din teorema precedentă, putem presupune că liniile A_1, \dots, A_{r+1} sunt liniar independente. Pentru $j = 1, \dots, n$,

considerăm $(r+1)$ -minorul $M_j = \begin{vmatrix} a_{11} & \cdots & a_{1r} & a_{1j} \\ \vdots & \ddots & \vdots & \vdots \\ a_{r1} & \cdots & a_{rr} & a_{rj} \\ a_{r+11} & \cdots & a_{r+1r} & a_{r+1j} \end{vmatrix}$. M_j este nul,

deoarece pentru $j = 1, \dots, r$, M_j are două coloane egale, iar pentru $j = r+1, \dots, n$ se aplică ipoteza. Complementii algebrici $d_1, \dots, d_r, d_{r+1} = M$ ai elementelor de pe coloana $r+1$ nu depind de j . Dezvoltând M_j pe coloana $r+1$, obținem $0 = d_1 a_{1j} + \cdots + d_r a_{rj} + M a_{r+1j}$ pentru $j = 1, \dots, n$. Deci $d_1 A_1 + \cdots + d_r A_r + M A_{r+1} = 0$, cu $M \neq 0$. Rezultă că liniile A_1, \dots, A_{r+1} sunt liniar dependente, contradicție. •

Teorema 161 (Kronecker-Capelli). *Un sistem de ecuații liniare este compatibil dacă și numai dacă rangul matricei sistemului este egal cu rangul matricei extinse.*

Demonstrație. Fie A matricea sistemului și B matricea extinsă. Conform teoremei 155 și corolarului 158, putem presupune că B (deci și A) este matrice eșalon. Condiția din enunț este echivalentă cu faptul B nu are pivoți în ultima coloană. Se aplică teorema 156.

Altă demonstrație. Fie c_1, \dots, c_n coloanele lui A , b vectorul termenilor liberi și $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. Sistemul $Ax = b$ se scrie sub forma $x_1 c_1 + \dots + x_n c_n = b$.

Deci sistemul $Ax = b$ este compatibil dacă și numai dacă b este combinație liniară de c_1, \dots, c_n dacă și numai dacă $\text{rang}(A) = \dim \langle c_1, \dots, c_n \rangle = \dim \langle c_1, \dots, c_n, b \rangle = \text{rang}(B)$. •

8.4 Exerciții

190. Fie A o mulțime finită și $\mathcal{P}(A)$ mulțimea părților lui A . $\mathcal{P}(A)$ este grup față de operația de diferență simetrică Δ . Arătați că acest grup o structură de \mathbf{Z}_2 -spațiu vectorial și găsiți o bază a sa.

191. Fie K un corp, V un grup abelian și $\text{End}(V)$ mulțimea endomorfismelor lui V . Arătați că $\text{End}(V)$ este inel față de operațiile de adunare și compunere, și că V împreună cu operația externă $K \times V \rightarrow V$, $(a, x) \mapsto ax$, este un spațiu vectorial dacă și numai dacă aplicația $f : K \rightarrow \text{End}(V)$, dată prin $f(a)(x) = ax$, pentru $a \in K$ și $x \in V$, este un morfism de inele.

192. Arătați că grupul aditiv \mathbf{Z} nu poate fi organizat ca spațiu vectorial (peste nici un corp).

193. Care din submulțimile următoare sunt subspații ale \mathbf{Q} -spațiului vectorial $\mathbf{Q}[X]$, $(a) \{f; f(a) = f(-a) \forall a \in \mathbf{Q}\}$,

$(b) \{f; f \text{ unitar, i.e. are coeficientul dominant} = 1\}$,

$(c) \{f; f \text{ neunitar}\}$,

$(d) \{f; f \text{ de grad impar}\}$,

$(e) \{f; f \text{ de grad} \leq 10\}$,

$(f) \{f; f(0) = f(1)\}$?

194. Fie subspațiile $U = \langle (2, 3, 1), (1, 2, 0) \rangle$ și $W = \langle (1, 1, 1), (0, -1, -1) \rangle$ ale lui ${}_{\mathbf{R}}\mathbf{R}^3$. Calculați $U + W$ și $U \cap W$.

195. Fie V \mathbf{R} -spațiul vectorial $M_3(\mathbf{R})$ și fie S (resp. A) mulțimea matricelor simetrice (resp. antisimetrice). Arătați că S și A sunt subspații și determinați dimensiunea lor. Este V suma directă a lui S cu A ?

196. Fie V \mathbf{R} -spațiul vectorial al șirurilor de numere reale $(x_n)_{n \geq 0}$ care verifică relația de recurență $x_n = x_{n-1} - x_{n-2}$, pentru $n \geq 2$. Arătați că șirurile $(\sin(n\pi/3))_{n \geq 0}$, $(\cos(n\pi/3))_{n \geq 0}$ constituie o bază a lui V .

197. Fie $f = a_0 + a_1X + \dots + a_{n-1}X^{n-1} + X^n \in \mathbf{Q}[X]$ un polinom ireductibil și $y \in \mathbf{C}$ o rădăcină alui f . Arătați că mulțimea $1, y, \dots, y^{n-1}$ este o bază a \mathbf{Q} -subspațiului vectorial generat de toate puterile lui y .

198. Fie W subspațiul lui ${}_{\mathbf{Q}}\mathbf{R}$ generat de $\{\cos(20^\circ n); n \geq 0\}$. Găsiți o bază a lui W . (Indicație. $\cos(20^\circ)$ este rădăcina polinomului ireductibil $8X^3 - 6X - 1$).

199. Arătați că orice spațiu vectorial V admite o bază.

200. Fie V \mathbf{R} -spațiul vectorial al polinoamelor de grad ≤ 4 cu coeficienți reali. Calculați matricele de trecere între bazele $E = \{1, X, X^2, X^3, X^4\}$ și $F = \{1, X - 1, (X - 1)^2, (X - 1)^3, (X - 1)^4\}$.

201. Cu notațiile din exercițiul anterior, fie $D : V \rightarrow V$ operatorul de derivare. Arătați că D este aplicație liniară și calculați matricele lui D în bazele E , F și $G = \{1, X/1!, X^2/2!, X^3/3!, X^4/4!\}$.

202. Cu notațiile din exercițiul anterior, găsiți baze în $\text{Im}(D)$ și $\text{ker}(D)$.

Fie $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbf{Q}\}$.

203. Arătați că $\mathbf{Q}(\sqrt{2}, \sqrt{3}) \leq {}_{\mathbf{Q}}\mathbf{R}$ și că $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ este o bază a sa.

204. Arătați că $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ este un subcorp al lui \mathbf{R} .

205. Fie Q -spațiul vectorial ${}_{\mathbf{Q}}V = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. Arătați că $T : V \rightarrow V$, $T(x) = (\sqrt{2} + \sqrt{3})x$, este un endomorfism al lui V și determinați matricea sa în baza $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$.

206. Cu notațiile din exercițiul anterior, arătați că $1, \sqrt{2} + \sqrt{3}, (\sqrt{2} + \sqrt{3})^2, (\sqrt{2} + \sqrt{3})^3$ este o bază a lui V și determinați matricea lui T în aceasta bază.

207. Fie V \mathbf{R} -spațiul vectorial al matricelor 2×2 cu intrări reale și fie $A \in V$ fixată. Arătați că aplicația $T : V \rightarrow V$, $T(Y) = AY + YA$ este liniară. Determinați matricea lui T în baza canonică a lui V .

208. Arătați că vectorii $(2, 2, 3)$, $(1, -1, 0)$, $(-1, 2, 1)$ constituie o bază F a lui \mathbf{R}^3 peste \mathbf{R} . Calculați matricele de trecere între F și baza canonică, și coordonatele lui $(1, 1, 1)$ în baza F .

209. Calculați inversa matricei $A = \begin{pmatrix} 1+a & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1+a & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1+a & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 1 & 1+a \end{pmatrix}$ prin eșalonare.

210. Calculați inversa matricei $B = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 0 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$ prin eșalonare.

211. Listați matricele eșalon 2×4 cu elemente din \mathbf{Z}_2 .

212. Eșalonați matricea

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

și găsiți baze în subspațiile generate de liniile resp. coloanele matricei.

213. Rezolvați sistemul de ecuații 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. Rezolvați sistemul de ecuații liniare $\begin{cases} x + y - 3z = -1 \\ 2x + y - 2z = 1 \\ x + y + z = 3 \\ x + 2y - 3z = 1. \end{cases}$

215. Calculați inversa matricei următoare prin eșalonare $\begin{pmatrix} 2 & 1 & 0 & 0 \\ 3 & 2 & 0 & 0 \\ 1 & 1 & 3 & 4 \\ 2 & -1 & 2 & 3 \end{pmatrix}$.

216. Calculați 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 . Arătați că A poate fi adusă prin transformări elementare pe linii și pe coloane la forma $\begin{pmatrix} I_p & 0 \\ 0 & 0 \end{pmatrix}$.

218. Fie $A, B \in M_n(K)$. Arătați că $\text{rang}(AB) \geq \text{rang}(A) + \text{rang}(B) - n$.

Capitolul 9

Forma canonică Jordan

În acest capitol se prezintă teoria formei canonice Jordan. Trecând prin conceptele de matrice caracteristică, forma diagonal-canonice, factori invarianti, 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 înțelege corp comutativ.

9.1 Matricea unui endomorfism

Fie K un corp. Fie V un K -spațiu vectorial finit dimensional și fie u, v endomorfisme ale lui V . Fie $E = \{e_1, \dots, e_n\}$ o bază a lui V . Exprimând vectorii $u(e_1), \dots, u(e_n)$ în baza E

$$u(e_j) = \sum_{i=1}^n a_{ij} e_i, \quad j = 1, \dots, n \quad \text{cu} \quad a_{ij} \in K$$

obținem 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 $x \in V$ și fie x_1, \dots, x_n (resp. y_1, \dots, y_n) coordonatele lui x (resp. $u(x)$) în baza E . Atunci

$$u(x) = u\left(\sum_{j=1}^n x_j e_j\right) = \sum_{j=1}^n x_j u(e_j) = \sum_{j=1}^n x_j \sum_{i=1}^n a_{ij} e_i = \sum_{i=1}^n \left(\sum_{j=1}^n a_{ij} x_j\right) e_i.$$

Deci coordonatele lui $u(x)$ în baza E se pot obține înmulțind 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 față de dreapta $y = x \operatorname{tg} t$. 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 notațiile 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 $d \in K$.

Demonstrație. Vom proba (b), celelalte afirmații arătându-se analog. Fie $M_E(u) = (a_{ij})$ și $M_E(v) = (b_{ij})$. Pentru $k = 1, \dots, n$ avem

$$(vu)(e_k) = v\left(\sum_{j=1}^n a_{jk}e_j\right) = \sum_{j=1}^n a_{jk}v(e_j) = \sum_{j=1}^n a_{jk} \sum_{i=1}^n b_{ij}e_i = \sum_{i=1}^n \left(\sum_{j=1}^n b_{ij}a_{jk}\right)e_i.$$

Așadar $M_E(vu) = M_E(v)M_E(u)$. •

Fie V un K -spațiu vectorial finit dimensional. Pe mulțimea $\operatorname{End}(V)$ a endomorfismelor lui V definim o operație de adunare prin $(u+v)(x) = u(x) + v(x)$ și o operație de înmulțire cu scalari prin $(au)(x) = au(x)$ pentru orice $u, v \in \operatorname{End}(V)$, $a \in K$ și $x \in V$. Se arată ușor că față de adunare și compunere $\operatorname{End}(V)$ este un inel, iar față de adunare și înmulțire cu scalari, $\operatorname{End}(V)$ este un spațiu vectorial.

Teorema 163 *Fie V un K -spațiu vectorial finit dimensional și $E = \{e_1, \dots, e_n\}$ o bază a lui V . Aplicația $M_E : \operatorname{End}(V) \rightarrow M_n(K)$, $u \mapsto M_E(u)$, este un izomorfism de inele și spații vectoriale.*

Demonstrație. Din teorema precedentă rezultă că M_E este un morfism de inele și spații vectoriale. Asociem fiecărei matrice $A = (a_{ij}) \in M_n(K)$ endomorfismul u_A al lui V definit pe baza E prin

$$u_A(e_j) = \sum_{i=1}^n a_{ij} e_i, \quad j = 1, \dots, n.$$

Obținem aplicația $\alpha : M_n(K) \rightarrow \text{End}(V)$, $\alpha(A) = u_A$. Se arată ușor că aplicațiile M_E și α sunt inverse una celeilalte. •

În particular, u este izomorfism dacă și numai dacă $M_E(u)$ este matrice inversabilă.

Teorema 164 Fie V un K -spațiu vectorial finit dimensional, u un endomorfism al lui V , E, F baze ale lui V și C matricea de trecere de la E la F . Atunci $M_F(u) = C^{-1} M_E(u) C$.

Demonstrație. Fie $E = \{e_1, \dots, e_n\}$, $F = \{f_1, \dots, f_n\}$, $M_E(u) = (a_{ij})$, $M_F(u) = (b_{ij})$ și $C = (c_{ij})$. Avem

$$u(f_k) = \sum_{j=1}^n b_{jk} f_j = \sum_{j=1}^n b_{jk} \sum_{i=1}^n c_{ij} e_i = \sum_{i=1}^n \left(\sum_{j=1}^n c_{ij} b_{jk} \right) e_i.$$

Pe de altă parte

$$u(f_k) = u\left(\sum_{j=1}^n c_{jk} e_j\right) = \sum_{j=1}^n c_{jk} u(e_j) = \sum_{j=1}^n c_{jk} \sum_{i=1}^n a_{ij} e_i = \sum_{i=1}^n \left(\sum_{j=1}^n a_{ij} c_{jk} \right) e_i.$$

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 $C M_F(u) = M_E(u) C$. •

Spunem că două matrice $A, B \in M_n(K)$ sunt *asemenea*, și notăm $A \approx B$, dacă există o matrice inversabilă $U \in M_n(K)$ astfel încât $A = U^{-1} B U$. Relația de asemănare este o relație de echivalență pe $M_n(K)$. Într-adevăr, fie $A, B, C \in M_n(K)$ și $U, V \in GL_n(K)$. Atunci $A = I^{-1} A I$, $A = U^{-1} B U$ implică $B = U A U^{-1}$, iar dacă $A = U^{-1} B U$ și $B = V^{-1} C V$, atunci rezultă că $A = (V U)^{-1} C (V U)$.

Teorema 165 Fie V un K -spațiu vectorial finit dimensional, u un endomorfism al lui V și E o bază a lui V . Atunci $\{M_F(u) \mid F \text{ bază a lui } V\}$ este exact mulțimea matricelor asemenea cu $M_E(u)$.

Demonstrație. Incluziunea \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, \dots, f_n definită prin $f_j = \sum_{i=1}^n c_{ij}e_i$, $j = 1, \dots, n$, unde $C = (c_{ij})$ și $E = \{e_1, \dots, e_n\}$. Din teorema precedentă, rezultă că $M_F(u) = B$. •

9.2 Forma diagonal-canonice

Împreună 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 $f = B_m X^m + \dots + B_1 X + B_0$ cu coeficienții $B_i \in M_n(K)$, înmulțirea monoamelor făcându-se după regula $(AX^i)(BX^j) = ABX^{i+j}$.

Teorema 166 Între inelele $M_n(K)[X]$ și $M_n(K[X])$ există un izomorfism natural.

Demonstrație. Elementele lui $M_n(K)[X]$ au forma $\sum_{k=0}^p A_k X^k$ cu $A_k = (a_{ijk})_{1 \leq i, j \leq n} \in M_n(K)$. Se arată ușor că aplicația

$$\varphi : M_n(K)[X] \rightarrow M_n(K[X]), \quad \varphi\left(\sum_{k=0}^p A_k X^k\right) = \left(\sum_{i=0}^p a_{ijk} X^k\right)_{1 \leq i, j \leq n}$$

este un izomorfism de inele. •

În continuare vom identifica inelele $M_n(K)[X]$ și $M_n(K[X])$ 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 numește *matricea caracteristică* a lui A iar $P_A = |XI - A|$ se numește *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 $X^3 - 12X^2 + 21X - 10 = (X-1)^2(X-10)$ și valorile proprii 1 și 10.

Fie $f = B_m X^m + \dots + B_1 X + B_0 \in M_n(K)[X]$ și $A \in M_n(K)$. Matricea $f_d(A) := B_m A^m + \dots + B_1 A + B_0$ se numește *valoarea la dreapta a lui f în A* , iar matricea $f_s(A) := A^m B_m + \dots + A B_1 + B_0$ se numește *valoarea la stânga a lui f în A* .

Teorema 167 (Teorema lui Bézout generalizată.) Fie $f \in M_n(K)[X]$ și $A \in M_n(K)$. Atunci există $q \in M_n(K)[X]$, astfel încât $f = q(IX - A) + f_d(A)$ și aceasta este unica scriere a lui f sub forma $f = q'(IX - A) + r$ cu $q' \in M_n(K)[X]$ și $r \in M_n(K)$.

Analog, există $q \in M_n(K)[X]$, astfel încât $f = (IX - A)q + f_s(A)$ și aceasta este unica scriere a lui f sub forma $f = (IX - A)q' + r$ cu $q' \in M_n(K)[X]$ și $r \in M_n(K)$.

Demonstrație. Fie $f = B_m X^m + \dots + B_1 X + B_0$. Atunci $f_d(A) = B_m A^m + \dots + B_1 A + B_0$. Deci

$$f - f_d(A) = B_m(IX^m - A^m) + \dots + B_1(IX - A)$$

și e suficient să observăm că

$$IX^k - A^k = (IX - A)(IX^{k-1} + \dots + A^{k-1}).$$

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 $q = q'$ și $r = r'$, altfel polinomul $(q - q')(IX - A)$ are gradul ≥ 1 . •

Fie $A \in M_n(K)$ o matrice și $f = b_p X^p + b_{p-1} X^{p-1} + \dots + b_1 X + b_0 \in K[X]$ un polinom. Matricea $f(A) = b_p A^p + b_{p-1} A^{p-1} + \dots + b_1 A + b_0 I \in M_n(K)$, se numește *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 $P_A(A) = 0$.

Demonstrație. 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*, și notăm $A \sim B$, dacă există două matrice inversabile $U, V \in M_n(K[X])$ astfel încât $A = UBV$.

Aceasta este o relație de echivalență pe $M_n(K[X])$. Într-adevăr, fie $A, B, C \in M_n(K[X])$ și $U, V, U', V' \in GL_n(K[X])$. Atunci $A = IAI$, $A = UBV$ implică $B = U^{-1}AU^{-1}$, iar dacă $A = UBV$ și $B = U'CV'$, atunci rezultă că $A = UU'CV'V$.

Teorema 169 Fie $A, B \in M_n(K)$. Atunci $A \approx B$ dacă și numai dacă $IX - A \sim IX - B$.

Demonstrație. Implicația 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 $f(IX - A) = (IX - B)g^{-1}$ și $(IX - A)g = f^{-1}(IX - B)$. Din teorema lui Bézout generalizată, există $f_1, g_1 \in M_n(K)[X]$ și $F, G \in M_n(K)$ astfel încât

$$f = (IX - B)f_1 + F \quad \text{și} \quad g = g_1(IX - B) + G.$$

Notăm $\alpha = IX - A$ și $\beta = IX - B$. Combinând relațiile 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

$$\begin{aligned} \beta - F\alpha G &= f\alpha g_1\beta + \beta f_1\alpha G = f\alpha g_1\beta + \beta f_1\alpha(g - g_1\beta) = \\ &= f\alpha g_1\beta + \beta f_1\alpha g - \beta f_1\alpha g_1\beta = \beta g^{-1}g_1\beta + \beta f_1f^{-1}\beta - \beta f_1\alpha g_1\beta. \end{aligned}$$

Așadar

$$IX - B - F(IX - A)G = (IX - B)(g^{-1}g_1 + f_1f^{-1} - f_1(IX - A)g_1)(IX - B).$$

Privite ca polinoame, membrul stâng are gradul ≤ 1 , deci membrul drept este nul, altfel are gradul ≥ 2 . Rezultă că $FG = I$ și $B = FAG$. •

Dacă $d_1, \dots, d_n \in K[X]$, notăm cu $\text{diag}(d_1, \dots, d_n)$ matricea cu elementele d_1, \dots, d_n pe diagonala principală și zero în rest.

Teorema 170 Fie $C \in M_n(K[X])$ cu $|C| \neq 0$. Atunci există și sunt unice polinoamele unitare $d_1, \dots, d_n \in K[X]$ astfel încât $d_1 \mid d_2 \mid \dots \mid d_n$ și $C \sim \text{diag}(d_1, \dots, d_n)$. (Matricea $\text{diag}(d_1, \dots, d_n)$ se numește forma *diagonal-canonică* a lui C .)

Demonstrație. Existența. Vom arăta mai mult și anume că C se poate aduce prin transformări elementare pe linii și coloane la forma $\text{diag}(d_1, \dots, d_n)$ cu d_1, \dots, d_n polinoame unitare astfel încât $d_1 \mid d_2 \mid \dots \mid d_n$.

Este suficient să arătăm că prin transformări elementare pe linii și coloane, putem aduce matricea C la forma următoare.

(*) Elementul c_{11} este polinom unitar, toate celelalte elemente de pe prima linie și prima coloană ale lui C sunt nule și c_{11} divide toate elementele matricei.

Într-adevăr, fie C' matricea obținută din C tăind prima linie și prima coloană. Cum $|C| \neq 0$, rezultă că $|C'| \neq 0$. Raționând prin inducție după n , putem presupune că C' se poate aduce prin transformări elementare pe liniile și coloanele $2, \dots, n$ la forma $C' \sim \text{diag}(d_2, \dots, d_n)$ cu d_2, \dots, d_n polinoame unitare astfel încât $d_2 \mid d_3 \mid \dots \mid d_n$. Cum c_{11} divide toate elementele matricei C' , rezultă că c_{11} divide d_2 , și afirmația este probată.

La forma (*) se ajunge prin intermediul algoritmului următor.

do

Prin permutări de linii și coloane, se aduce în poziția $(1, 1)$ 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 împărțirea cu rest $c_{1j} = qc_{11} + r$;

Se scade coloana 1 înmulțită cu q din coloana j ;

Se permută coloanele 1 și j ;

end

for $j=2$ *to* n *do*

Se scade coloana 1 înmulțită 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 împărțirea cu rest  $c_{i1} = qc_{11} + r$ ;
    Se scade linia 1 înmulțită cu  $q$  din linia  $i$ ;
    Se permută liniile 1 și  $i$ ;
end
for  $i=2$  to  $n$  do
    Se scade linia 1 înmulțită cu  $c_{i1}/c_{11}$  din linia  $i$ ;
    if  $c_{11}$  nu divide un element  $c_{\alpha\beta}$  then se adună linia  $\alpha$  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 înlocuiește cu restul unei împărțiri la c_{11} , deci gradul lui c_{11} scade strict. După parcurgerea celor două bucle *while*, cu excepția lui c_{11} , toate celelalte elemente de pe prima linie și 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 pași. E clar că la terminarea algoritmului matricea C verifică condițiile (*). •

Pregătim demonstrația unicității. 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 combinație liniară de p -minori, rezultă că

$$\Delta_1(C) \mid \Delta_2(C) \mid \dots \mid \Delta_n(C).$$

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, \dots, X^n .

Lema 171 Fie $C, D \in M_n(K[X])$ cu $|C| \neq 0$ și $|D| \neq 0$. Dacă $C \sim D$, atunci $\Delta_p(C) = \Delta_p(D)$, pentru $p = 1, \dots, n$.

Demonstrație. 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 $\Delta_p(D) \mid \Delta_p(C)$ și, datorită simetriei, $\Delta_p(C) \mid \Delta_p(D)$. Cum $\Delta_p(C)$, $\Delta_p(D)$ sunt polinoame unitare, ele sunt egale. •

Demonstrația teoremei 170 (unicitatea). Fie $C \in M_n(K[X])$ și $d_1, \dots, d_n \in K[X]$ polinoame unitare astfel încât $d_1 \mid d_2 \mid \dots \mid d_n$ și $C \sim \text{diag}(d_1, \dots, d_n)$. Notăm $D = \text{diag}(d_1, \dots, d_n)$. Conform lemei precedente, $\Delta_p(C) = \Delta_p(D)$ pentru $p = 1, 2, \dots, n$. Fie $1 \leq p \leq n$. p -minorii nenuli ai lui D sunt produsele de p elemente d_i . Cum $d_1 \mid d_2 \mid \dots \mid d_n$, 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 $p = 1, 2, \dots, n$. Atunci $d_1 = \Delta_1(C)$, $d_2 = \Delta_2(C)/\Delta_1(C), \dots, d_n = \Delta_n(C)/\Delta_{n-1}(C)$. Așadar polinoamele d_i sunt unic determinate. •

Observația 172 *Din demonstrația precedentă rezultă că, pentru o matrice $C \in M_n(K[X])$ cu $|C| \neq 0$, elementele formei diagonal-canonică $\text{diag}(d_1, d_2, \dots, d_n)$ se pot calcula prin $d_1 = \Delta_1(C)$, $d_2 = \Delta_2(C)/\Delta_1(C), \dots, d_n = \Delta_n(C)/\Delta_{n-1}(C)$.*

Din teorema 170 și observația 172 rezultă

Teorema 173 *Fie $C, D \in M_n(K[X])$ cu $|C| \neq 0$ și $|D| \neq 0$. Atunci $C \sim D \Leftrightarrow C, D$ au aceeași formă diagonal-canonică $\Leftrightarrow \Delta_p(C) = \Delta_p(D)$, pentru $p = 1, \dots, n$.*

9.3 Forma Jordan a unei matrice

Fie $A \in M_n(K)$ și presupunem că matricea caracteristică $XI_n - A$ a lui A are forma diagonal-canonică $\text{diag}(1, \dots, 1, d_1, d_2, \dots, d_r)$, unde d_1, d_2, \dots, d_r sunt polinoame unitare de grad ≥ 1 . Polinoamele d_1, d_2, \dots, d_r poartă numele de *factorii invarianți* ai matricei A . Așadar, factorii invarianți ai matricei $A \in M_n(K)$ sunt polinoamele de grad ≥ 1 ale formei diagonal-canonică a lui $XI - A$. Altfel spus, factorii invarianți ai lui A sunt polinoamele neconstante de forma $\Delta_i(XI - A)/\Delta_{i-1}(XI - A)$, $i = 1, \dots, n$, cf. observației 172.

De exemplu, matricea nulă are factorii invarianți X, X, \dots, X , iar matricea $\text{diag}(1, 2, \dots, n)$ are factorul invariant $(X - 1)(X - 2) \cdots (X - n)$.

Teorema 174 *Produsul factorilor invariante ai unei matrice $A \in M_n(K)$ este egal cu polinomul caracteristic al lui A .*

Demonstrație. Deoarece $XI_n - A \sim \text{diag}(1, \dots, 1, d_1, d_2, \dots, d_r)$, există $U, V \in GL_n(K[X])$ astfel încât $XI_n - A = U \text{diag}(1, \dots, 1, d_1, d_2, \dots, d_r) V$. Deci

$$P_A = |XI_n - A| = |U| |\text{diag}(1, \dots, 1, d_1, d_2, \dots, d_r)| |V| = |U| |V| d_1 \cdots d_r.$$

Cum P_A și $d_1 \cdots d_r$ sunt polinoame unitare și $|U|, |V| \in K^*$, rezultă că $|U| |V| = 1$. •

Din teoremele 173 și 169 rezultă

Teorema 175 *Două matrice $A, B \in M_n(K)$ sunt asemenea dacă și numai dacă au aceiași factori invariante.*

Unui polinom unitar $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$, îi asociem matricea $C_f \in M_n(K)$

$$C_f = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & 0 & -a_2 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & -a_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

numită *matricea companion a lui f* sau *companionul lui f* . De exemplu, $C_{X+3} = (-3)$ și $C_{X^2-X+5} = \begin{pmatrix} 0 & -5 \\ 1 & 1 \end{pmatrix}$.

Teorema 176 *Polinomul caracteristic al companionului lui f este chiar f , adică $|XI_n - C_f| = f$. În particular, $f(C_f) = 0$.*

Demonstrație. Păstrând notațiile anterioare, avem

$$P_{C_f} = |XI - C_f| = \begin{vmatrix} X & 0 & \cdots & 0 & 0 & a_0 \\ -1 & X & \cdots & 0 & 0 & a_1 \\ 0 & -1 & \cdots & 0 & 0 & a_2 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & X & a_{n-2} \\ 0 & 0 & \cdots & 0 & -1 & X + a_{n-1} \end{vmatrix}.$$

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 obținem $P_{C_f} = X|XI - C_g| + a_0$, unde $g = X^{n-1} + a_{n-1}X^{n-2} + \cdots + a_2X + a_1$ și se face inducție 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 și anume f . Altfel spus,*

$$XI - C_f \sim \text{diag}(1, \dots, 1, f).$$

Demonstrație. Fie

$$B = XI - C_f = \begin{pmatrix} X & 0 & \cdots & 0 & 0 & a_0 \\ -1 & X & \cdots & 0 & 0 & a_1 \\ 0 & -1 & \cdots & 0 & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & X & a_{n-2} \\ 0 & 0 & \cdots & 0 & -1 & X + a_{n-1} \end{pmatrix}.$$

Din teorema precedentă, $\Delta_n(B) = P_{C_f} = f$. $(n-1)$ -minorul lui B obținut tăind prima linie și 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 observația 172. •

Fie matricele $C_i \in M_{p_i}(K[X])$, $i = 1, \dots, t$. Matricea

$$C_1 \oplus C_2 \oplus \cdots \oplus C_t := \text{diag}(C_1, C_2, \dots, C_t) = \begin{pmatrix} C_1 & & & \\ & C_2 & & \\ & & \ddots & \\ & & & C_t \end{pmatrix}$$

se numește *suma directă* a matricelor C_1, \dots, C_t . Afirmatiile următoarei leme se probează ușor.

Lema 178 *Fie matricele $C_i, D_i \in M_{p_i}(K[X])$, $i = 1, \dots, t$.*

$$(a) (C_1 \oplus \cdots \oplus C_t) + (D_1 \oplus \cdots \oplus D_t) = (C_1 + D_1) \oplus \cdots \oplus (C_t + D_t).$$

$$(b) (C_1 \oplus \cdots \oplus C_t)(D_1 \oplus \cdots \oplus D_t) = (C_1 D_1) \oplus \cdots \oplus (C_t D_t).$$

$$(c) \text{ Dacă } C_i \sim D_i \text{ pentru } i = 1, \dots, t, \text{ atunci } C_1 \oplus \cdots \oplus C_t \sim D_1 \oplus \cdots \oplus D_t.$$

$$(d) \text{ Dacă } C_i, D_i \text{ sunt matrice constante și } C_i \approx D_i \text{ pentru } i = 1, \dots, t, \text{ atunci } C_1 \oplus \cdots \oplus C_t \approx D_1 \oplus \cdots \oplus D_t.$$

Teorema 179 Dacă matricea $A \in M_n(K)$ are factorii invarianți d_1, \dots, d_r , atunci

$$A \approx C_{d_1} \oplus \dots \oplus C_{d_r}.$$

Demonstrație. Cf. teoremei 177, avem

$$XI - (C_{d_1} \oplus \dots \oplus C_{d_r}) = (XI - C_{d_1}) \oplus \dots \oplus (XI - C_{d_r}) \sim$$

$$\sim \text{diag}(1, \dots, 1, d_1) \oplus \dots \oplus \text{diag}(1, \dots, 1, d_r) \sim \text{diag}(1, \dots, 1, d_1, \dots, d_r).$$

Cum $d_1 \mid d_2 \mid \dots \mid d_r$, deducem că d_1, \dots, d_r sunt factorii invarianți ai matricei $C_{d_1} \oplus \dots \oplus C_{d_r}$. Se aplică teorema 175. •

Fie $d_1, \dots, d_r \in K[X]$ factorii invarianți ai matricei $A \in M_n(K)$ și fie $\pi_1, \dots, \pi_s \in K[X]$ divizorii lor ireductibili (unitari). Putem scrie

$$d_i = \pi_1^{k_{i1}} \pi_2^{k_{i2}} \dots \pi_s^{k_{is}}, \quad i = 1, \dots, r \quad \text{cu } 0 \leq k_{1j} \leq k_{2j} \leq \dots \leq k_{rj}, \quad j = 1, \dots, s.$$

Polinoamele

$$\{\pi_i^{k_{ij}} \mid k_{ij} \geq 1, \quad i = 1, \dots, r, \quad j = 1, \dots, s\}$$

se numesc *divizorii elementari* ai lui A . Deci divizorii elementari sunt puteri de polinoame ireductibile unitare din $K[X]$. Egalitățile anterioare permit recuperarea factoriilor invarianți 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 $A, B \in M_n(K)$. Afirmățiile următoare sunt echivalente:

- (a) $A \approx B$,
- (b) A, B au aceeași factori invarianți,
- (c) A, B au aceeași divizori elementari.

Teorema 182 Fie $f, g \in K[X]$ două polinoame unitare neconstante prime între ele. Atunci $C_{fg} \approx C_f \oplus C_g$.

Demonstrație. 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 și anume fg . Avem

$$\begin{aligned} XI - (C_f \oplus C_g) &= (XI_p - C_f) \oplus (XI_q - C_g) \sim \text{diag}(1, \dots, 1, f) \oplus \text{diag}(1, \dots, 1, g) \sim \\ &\sim \text{diag}(1, \dots, 1, fg) \sim \text{diag}(1, \dots, 1, fg). \end{aligned}$$

Ultima echivalență rezultă din faptul că $(n - 1)$ -minorii nenuli ai matricei $\text{diag}(1, \dots, 1, fg)$ sunt egali cu f, g sau fg , deci $\Delta_{n-1}(\text{diag}(1, \dots, 1, fg)) = 1$.

•

Fie $\pi \in K[X]$ un polinom ireductibil unitar de grad s și $k \geq 1$. 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 $N = \begin{pmatrix} & 1 \\ & & \ddots \\ & & & 1 \end{pmatrix}$, elementele omise în $J_k(\pi)$ și N fiind nule.

O sumă directă de celule Jordan se numește *matrice Jordan*.

Pentru $k = 1$ avem $J_1(\pi) = C_\pi$. Fie $\lambda \in K$. Pentru celula Jordan

$$J_k(X - \lambda) = \begin{pmatrix} \lambda & & & \\ 1 & \lambda & & \\ & 1 & \lambda & \\ & & \ddots & \ddots \\ & & & 1 & \lambda \end{pmatrix} \text{ vom utiliza și notația mai simplă } J_k(\lambda).$$

$$X^2 + X + 1 \text{ este ireductibil peste } \mathbf{R} \text{ și } J_2(X^2 + X + 1) = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

Teorema 183 Dacă $\pi \in K[X]$ un polinom ireductibil și $k \geq 1$, atunci

$$C_{\pi^k} \approx J_k(\pi).$$

Demonstrație. Cf. teoremelor 175 și 177, e suficient să vedem că $J_k(\pi)$ are un singur factor invariant și anume π^k . Fie D matricea caracteristică a lui $J_k(\pi)$ și fie $n = sk$, unde s este gradul lui π . $(n-1)$ -minorul lui D obținut tăind prima linie și 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 și anume π^k . •

Enunțăm teorema centrală a teoriei formei Jordan.

Teorema 184 (Forma Jordan a unei matrice). *Dacă matricea $A \in M_n(K)$ are divizorii elementari $\pi_1^{k_1}, \dots, \pi_s^{k_s}$, atunci*

$$A \approx J_{k_1}(\pi_1) \oplus \dots \oplus J_{k_s}(\pi_s).$$

Mai puțin o permutare a celulelor, $J_{k_1}(\pi_1) \oplus \dots \oplus J_{k_s}(\pi_s)$ este unica matrice Jordan asemenea cu A . Ea se numește forma Jordan a lui A .

Demonstrație. Fie d unul dintre factorii invariante ai lui A și $d = \rho_1^{l_1} \dots \rho_t^{l_t}$ descompunerea lui d în produs de factori ireductibili. Cf. teoremei 182,

$$C_{\rho_1^{l_1} \dots \rho_t^{l_t}} \approx C_{\rho_1^{l_1}} \oplus C_{\rho_2^{l_2} \dots \rho_t^{l_t}} \approx \dots \approx C_{\rho_1^{l_1}} \oplus \dots \oplus C_{\rho_t^{l_t}}.$$

Folosind acest fapt și teoremele 175, 183, rezultă că

$$A \approx C_{d_1} \oplus \dots \oplus C_{d_r} \approx C_{\pi_1^{k_1}} \oplus \dots \oplus C_{\pi_s^{k_s}} \approx J_{k_1}(\pi_1) \oplus \dots \oplus J_{k_s}(\pi_s).$$

Unicitatea formei Jordan rezultă din faptul că matricea Jordan $J_{k_1}(\pi_1) \oplus \dots \oplus J_{k_s}(\pi_s)$ are divizorii elementari $\pi_1^{k_1}, \dots, \pi_s^{k_s}$. •

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 invariante X , $X(X-3)$, deci divizorii elementari X , X , $X-3$. Rezultă că $A \approx J_1(X) \oplus J_1(X) \oplus J_1(X-3) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 3 \end{pmatrix}$. Aceași 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 și teorema 165 rezultă

Teorema 185 (Forma Jordan a unui endomorfism). *Pentru orice endomorfism u al unui K -spațiu vectorial finit-dimensional, există o bază în care matricea lui u este matrice Jordan. Această matrice este unică până la o permutare a celulelor și se numește forma Jordan a lui u .*

Recapitulăm conceptele ce conduc la forma Jordan: matrice constantă, asemănare de matrice constante, matrice caracteristică, echivalență de matrice polinomiale, formă diagonal-canonice a unei matrice polinomiale, factori invarianți, 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 , $\lambda_1, \lambda_2, \dots, \lambda_n \in K$, atunci*

$$A \approx \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n).$$

În particular, dacă un endomorfism u al unui K -spațiu vectorial n -dimensional are n valori proprii distincte, atunci u este diagonalizabil.

Demonstrație. Cum produsul divizorilor elementari ai lui A este $P_A = (X - \lambda_1) \cdots (X - \lambda_n)$, rezultă că aceștia sunt exact $X - \lambda_1, X - \lambda_2, \dots, X - \lambda_n$. •

9.4 Polinomul minimal

Fie $A \in M_n(K)$ o matrice și $f = b_p X^p + b_{p-1} X^{p-1} + \cdots + b_1 X + b_0 \in K[X]$ 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 numește *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 ușor că aplicația

$$\varphi_A : K[X] \rightarrow M_n(K), \quad \varphi_A(f) = f(A)$$

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 numește *polinomul minimal al lui A*. Reamintim că μ_A este polinomul unitar de grad minim în $\ker(\varphi_A)$, cf. demonstrației teoremei 94.

Teorema 187 Fie $A \in M_n(K)$ o matrice și $g \in K[X]$ un polinom. Următoarele afirmații sunt echivalente.

- (a) $g = \mu_A$,
- (b) g este unitar, $g(A) = 0$ și g este de grad minim între polinoamele cu aceste proprietăți,
- (c) g este unitar, $g(A) = 0$ și g divide toate polinoamele $h \in K[X]$ cu proprietatea $h(A) = 0$.

Demonstrație. Echivalența (a) \Leftrightarrow (b) a fost justificată mai sus, iar implicațiile (a) \Rightarrow (c) și (c) \Rightarrow (b) sunt clare. •

Exemple 188 (a) Dacă $a \in K$, atunci $\mu_A = X - a$ dacă și numai dacă $A = aI$.

(b) Fie $A = \begin{pmatrix} 0 & -2 \\ 1 & 3 \end{pmatrix}$ și $f = X^2 - 3X + 2 = (X - 1)(X - 2)$. 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 $\mu_{C_f} = f$.

Demonstrație. Fie $f = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$ și fie e_1, \dots, 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 $i = 1, \dots, n-1$, deci $C_f^i e_1 = e_{i+1}$. Dacă $g = c_{n-1}X^{n-1} + \dots + c_1X + c_0 \in K[X]$ are proprietatea $g(C_f) = 0$, atunci

$$0 = g(C_f)e_1 = c_{n-1}e_n + \dots + c_1e_2 + c_0e_1 = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix}$$

deci $g = 0$. Se aplică teoremele 176 și 187. •

Teorema 190 Fie $A \in M_n(K)$. Atunci polinomul minimal al lui A este ultimul factor invariant al lui A . Altfel spus,

$$\mu_A = \frac{P_A}{\Delta_{n-1}(XI - A)}.$$

Demonstrație. Fie $d_1 \mid \cdots \mid d_r$ factorii invarianți 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 și numai dacă $g(C_{d_i}) = 0$, $i = 1, \dots, r$. Din teorema precedentă, $\mu_{C_{d_i}} = d_i$. Ținând seama că $d_1 \mid \cdots \mid d_r$, rezultă că $g(A) = 0$ dacă și 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 și μ_A au aceeași factori ireductibili în $K[X]$.

Demonstrație. Fie $d_1 \mid \cdots \mid d_r$ factorii invarianți ai lui A . Cum $P_A = d_1 \cdots d_r$ și $d_1 \mid \cdots \mid d_r$, rezultă că P_A și d_r au aceeași 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 și numai dacă μ_A are toate rădăcinile în K și acestea sunt distincte.

Demonstrație. Are loc șirul de echivalențe. 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 și acestea sunt distincte \Leftrightarrow ultimul factor invariant (adică μ_A) are toate rădăcinile în K și acestea sunt distincte. •

Fie $A \in M_n(K)$. Interpretăm pe A ca endomorfismul spațiului 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, $\text{rang}(A) + \text{defect}(A) = n$.

Teorema 193 Fie $A \in M_n(K)$ și $\lambda \in K$. Afirmațiile următoare sunt echivalente.

- (a) $P_A(\lambda) = 0$ (adică λ este valoare proprie a lui A),
- (b) matricea $A - \lambda I$ este neinvertibilă,
- (c) $\text{defect}(A - \lambda I) \geq 1$,
- (d) Există $0 \neq v \in M_{n,1}(K)$ astfel încât $Av = \lambda v$.

Demonstrație. Avem șirul de echivalențe. $0 = P_A(\lambda) = |\lambda I - A| \Leftrightarrow$ matricea $A - \lambda I$ este neinvertibilă $\Leftrightarrow \text{rang}(A - \lambda I) \leq n - 1 \Leftrightarrow \text{defect}(A - \lambda I) \geq 1 \Leftrightarrow$ are loc (d). •

Un vector $0 \neq v \in M_{n,1}(K)$ astfel încât $Av = \lambda v$ se numește *vector propriu* al lui A corespunzător valorii proprii λ iar $\ker(A - \lambda I) = \{v \in M_{n,1}(K) \mid Av = \lambda v\}$ se numește *spațiul 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

$$J_k(\lambda) = \begin{pmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & 1 & \lambda & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda \end{pmatrix} \text{ cu } \lambda \in \mathbf{C} \text{ și } k \geq 1.$$

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 numește *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 și este numită *forma canonică Jordan a lui A* . $\lambda_1, \dots, \lambda_s \in \mathbf{C}$ sunt valorile proprii ale lui A .

Demonstrație. Se aplică teorema 184. În plus, rezultă că $P_A = (X - \lambda_1)^{k_1} \cdots (X - \lambda_s)^{k_s}$. Deci $\lambda_1, \dots, \lambda_s$ sunt valorile proprii ale lui A . •

Așadar forma canonică Jordan a unei matrice A este determinată de valorile proprii ale lui A și, pentru fiecare valoare proprie λ , de numărul și ordinul λ -celulelor.

Observația 195 În ipotezele și cu notațiile 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 $\lambda \in \mathbf{C}$, $f \in \mathbf{C}[X]$ și $k \geq 1$. Atunci

$$f(J_k(\lambda)) = \begin{pmatrix} f(\lambda) & & & & \\ \frac{f'(\lambda)}{1!} & f(\lambda) & & & \\ \frac{f''(\lambda)}{2!} & \frac{f'(\lambda)}{1!} & f(\lambda) & & \\ \vdots & \vdots & \vdots & \ddots & \\ \frac{f^{(k-1)}(\lambda)}{(k-1)!} & \cdots & \frac{f''(\lambda)}{2!} & \frac{f'(\lambda)}{1!} & f(\lambda) \end{pmatrix}$$

elementele de deasupra diagonalei principale fiind nule.

Demonstrație. 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

$$J_k^2(0) = \begin{pmatrix} 0 & & & & \\ 0 & 0 & & & \\ 1 & 0 & 0 & & \\ & \ddots & \ddots & \ddots & \\ & & 1 & 0 & 0 \end{pmatrix}, \dots, J_k^{k-1}(0) = \begin{pmatrix} & & & & \\ & & & & \\ & & & & \\ & & & & \\ 1 & & & & \end{pmatrix}, J_k^k(0) = 0.$$

Aplicând formula binomului lui Newton pentru $J_k^m(\lambda) = (\lambda I + J_k(0))^m$, obținem formula din enunț, deoarece $(X^p)^{(m)}/m! = C_p^m X^{p-m}$. •

Fie $a_0, a_1, \dots, a_{p-1} \in \mathbf{C}$, $a_0 \neq 0$. Considerăm șirul definit prin relația de recurență $x_n = a_{p-1}x_{n-1} + a_{p-2}x_{n-2} + \dots + a_0x_{n-p}$ cu x_0, \dots, x_{p-1} date. Avem relația matriceală $(x_{n-p+1}, \dots, x_n) = (x_{n-p}, \dots, x_{n-1})A$, unde A este companionul matriceal al polinomului $f = X^p - a_{p-1}X^{p-1} - \dots - a_1X - a_0$ ($f = 0$ se numește *ecuația caracteristică* a relației de recurență). Rezultă că

$$(x_{n-p+1}, \dots, x_n) = (x_0, \dots, x_{p-1})A^n. \quad (9.1)$$

Fie $f = (X - \lambda_1)^{k_1} \dots (X - \lambda_s)^{k_s}$ cu $\lambda_1, \dots, \lambda_s$ distincte. Rezultă că $A \approx J_{k_1}(\lambda_1) \oplus J_{k_2}(\lambda_2) \oplus \dots \oplus J_{k_s}(\lambda_s)$, deci $A^n \approx J_{k_1}^n(\lambda_1) \oplus J_{k_2}^n(\lambda_2) \oplus \dots \oplus J_{k_s}^n(\lambda_s)$. Din relația 9.1 și teorema 196, rezultă că termenul general al șirului are forma

$$x_n = (b_{10} + b_{11}n + \dots + b_{1k_1-1}n^{k_1-1})\lambda_1^n + \dots + (b_{s0} + b_{s1}n + \dots + b_{sk_s-1}n^{k_s-1})\lambda_s^n$$

cu coeficienții $b_{ij} \in \mathbf{C}$.

De exemplu, termenul general al șirului definit prin relația de recurență $x_n = 2x_{n-1} + x_{n-2} - 2x_{n-3} - x_{n-4}$ are forma $x_n = (a + bn)(1/2 + \sqrt{5}/2)^n + (c + dn)(1/2 - \sqrt{5}/2)^n$.

Fie $A \in M_n(\mathbf{C})$ și λ o valoare proprie a lui A . Multiplicitatea $m_a(\lambda)$ a lui λ ca rădăcină a lui P_A se numește *multiplicitatea algebrică* a lui λ . Numărul

$$m_g(\lambda) = \text{defect}(A - \lambda I)$$

adică dimensiunea subspațiului vectorilor proprii corespunzător lui λ , se numește *multiplicitatea geometrică* a lui λ .

Dacă $A \approx B$, atunci $P_A = P_B$, deci A, B au aceleași valori proprii și cu aceleași multiplicități algebrice.

Teorema 197 Dacă $A \approx B$ și 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 .

Demonstrație. Fie $S \in GL_n(K)$ astfel încât $B = SAS^{-1}$. Avem $\text{defect}(B - \lambda I) = \text{defect}(SAS^{-1} - \lambda I) = \text{defect } S(A - \lambda I)S^{-1} = \text{defect}(A - \lambda I)$. •

Dacă $A = J_k(\lambda)$, atunci $P_A = (X - \lambda)^k$. Deci $m_a(\lambda) = k$ și $m_g(\lambda) = \text{defect}(A - \lambda I) = k - \text{rang}(J_k(0)) = 1$.

Teorema 198 Fie $A \in M_n(\mathbf{C})$ și 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, $m_a(\lambda) \geq m_g(\lambda)$.

Demonstrație. Ultima afirmație 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 aceeași multiplicitate algebrică (resp. geometrică) în A și 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 afirmație. Apoi,

$$\begin{aligned} m_g(\lambda) &= \text{defect}(A - \lambda I) = \\ &= \text{defect}(J_{k_1}(\lambda_1 - \lambda) \oplus J_{k_2}(\lambda_2 - \lambda) \oplus \cdots \oplus J_{k_s}(\lambda_s - \lambda)) = \\ &= \text{defect}(J_{k_1}(\lambda_1 - \lambda)) + \text{defect}(J_{k_2}(\lambda_2 - \lambda)) + \cdots + \text{defect}(J_{k_s}(\lambda_s - \lambda)). \end{aligned}$$

În final folosim faptul că

$$\text{defect}(J_k(\alpha)) = \begin{cases} 0 & \text{dacă } \alpha \neq 0 \\ 1 & \text{dacă } \alpha = 0 \end{cases} \bullet$$

Corolarul 199 O matrice $A \in M_n(\mathbf{C})$ este diagonalizabilă dacă și numai dacă toate valorile proprii ale lui A au multiplicitatea algebrică egală cu multiplicitatea geometrică.

Demonstrație. Folosim teoremă precedentă. Afirmația rezultă din faptul că A este diagonalizabilă dacă și numai dacă toate celulele Jordan ale sale au ordinul 1. \bullet

Lema 200 Dacă $\lambda \in \mathbf{C}$ și $k, p \geq 1$, atunci

$$\text{defect}(J_k^p(0)) = \min(k, p).$$

Demonstrație. Pentru $p \geq k$, $J_k^p(0) = 0$, deci $\text{defect}(J_k^p(0)) = k$. Pentru $p \leq k - 1$, $J_k^p(0)$ are o diagonală formată din $k - p$ elemente egale cu 1 și toate celelalte elemente nule. Deci $\text{defect}(J_k^p(0)) = p$. \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 și $p \geq 1$. Atunci numărul λ -celulelor Jordan ale lui A de ordin $\geq p$ este

$$\text{defect}((A - \lambda I)^p) - \text{defect}((A - \lambda I)^{p-1}).$$

Demonstrație. 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

$$\begin{aligned} & \text{defect}((A - \lambda I)^p) = \\ &= \text{defect}(J_{k_1}^p(\lambda_1 - \lambda) \oplus J_{k_2}^p(\lambda_2 - \lambda) \oplus \cdots \oplus J_{k_s}^p(\lambda_s - \lambda)) = \\ &= \text{defect}(J_{k_1}^p(\lambda_1 - \lambda)) + \text{defect}(J_{k_2}^p(\lambda_2 - \lambda)) + \cdots + \text{defect}(J_{k_s}^p(\lambda_s - \lambda)). \end{aligned}$$

Folosind faptul că $\text{defect}(J_k^p(\alpha)) = 0$ dacă $\alpha \neq 0$ și lema anterioară, avem

$$\text{defect}((A - \lambda I)^p) = \sum_{j=1}^s \sum_{\lambda_j=\lambda} \min(k_j, p).$$

Formula are loc și dacă înlocuim p cu $p - 1$. Rezultă că

$$\begin{aligned} & \text{defect}((A - \lambda I)^p) - \text{defect}((A - \lambda I)^{p-1}) = \\ &= \sum_{j=1}^s \sum_{\lambda_j=\lambda} (\min(k_j, p) - \min(k_j, p-1)) = \sum_{j=1}^s \sum_{\lambda_j=\lambda, k_j \geq p} 1. \bullet \end{aligned}$$

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

$$f_p = \text{defect}((A - \lambda I)^p) - \text{defect}((A - \lambda I)^{p-1}), \quad 1 \leq p \leq m_a(\lambda) + 1.$$

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 și aceea are ordinul 1. Avem $A - 4I = \begin{pmatrix} 0 & 0 & 0 \\ 2 & -3 & 3 \\ 5 & 0 & 0 \end{pmatrix}$ și $(A - 4I)^2 = \begin{pmatrix} 1 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Deci $f_1 = \text{defect}(A - 4I) = 1$ și $f_2 = \text{defect}(A - 4I)^2 - \text{defect}(A - 4I) = 2 - 1 = 1$. 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 Aplicații ale formei canonice Jordan.

Fie $A \in M_n(\mathbf{C})$ o matrice cu forma canonică Jordan $J = J_{k_1}(\lambda_1) \oplus J_{k_2}(\lambda_2) \oplus \dots \oplus J_{k_s}(\lambda_s)$. Ne interesează găsirea unei matrice inversabile U astfel încât $A = UJU^{-1}$ (U se numește *matrice de asemănare* între A și J sau mai simplu *matrice de asemănare pentru A*). Pentru $B \in M_n(\mathbf{C})$ și $u, v \in M_{n,1}(\mathbf{C})$, vom scrie $u \xrightarrow{B} v$, dacă $Bu = v$.

Fie $U \in M_n(\mathbf{C})$. Notăm coloanele lui U prin $u_{11}, \dots, u_{1k_1}, \dots, u_{s1}, \dots, u_{sk_s}$. Atunci coloanele matricei AU sunt

$$Au_{11}, \dots, Au_{1k_1}, \dots, Au_{s1}, \dots, Au_{sk_s}.$$

Pe de altă parte, coloanele matricei UJ sunt

$$\lambda_1 u_{11} + u_{12}, \dots, \lambda_1 u_{1k_1-1} + u_{1k_1}, \lambda_1 u_{1k_1}, \dots, \lambda_s u_{s1} + u_{s2}, \dots, \lambda_s u_{sk_s}.$$

Deci egalitatea $AU = UJ$ este echivalentă cu setul de relații

$$\begin{aligned} u_{11} &\xrightarrow{A-\lambda_1 I} u_{12} \xrightarrow{A-\lambda_1 I} \dots \xrightarrow{A-\lambda_1 I} u_{1k_1} \xrightarrow{A-\lambda_1 I} 0 \\ &\dots \\ u_{s1} &\xrightarrow{A-\lambda_s I} u_{s2} \xrightarrow{A-\lambda_s I} \dots \xrightarrow{A-\lambda_s I} u_{sk_s} \xrightarrow{A-\lambda_s I} 0. \end{aligned} \quad (9.2)$$

Fie $\text{Spec}(A) = \{\lambda_1, \dots, \lambda_s\}$, mulțimea valorilor proprii ale lui A . Fie $F = \{u_{1k_1}, u_{2k_2}, \dots, u_{sk_s}\}$ și pentru fiecare $\lambda \in \text{Spec}(A)$, fie $F_\lambda = \{u_{ik_i} \in F \mid \lambda_i = \lambda\}$.

Dăm, fără demonstrație, următoarea teoremă.

Teorema 202 (Filippov.) *Matricea U este o matrice de asemănare între A și J dacă și numai dacă coloanele lui U verifică relațiile (9.2) și mulțimea F_λ este liniar independentă pentru orice $\lambda \in \text{Spec}(A)$.*

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 $P_A = X^4$ și

$\text{defect}(A) = 1$, deci $A \approx J_4(0)$. U este matrice de asemănare dacă și numai dacă coloanele sale, u_1, \dots, u_4 , verifică:

$$u_1 \xrightarrow{A} u_2 \xrightarrow{A} u_3 \xrightarrow{A} u_4 \xrightarrow{A} 0 \text{ și } u_4 \neq 0.$$

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

$$\text{din } I, A, A^2, A^3: U = \begin{pmatrix} 1 & 3 & 2 & 1 \\ 0 & 2 & 1 & 1 \\ 0 & 3 & 2 & 1 \\ 0 & 3 & 2 & 1 \end{pmatrix}.$$

Putem proceda și astfel. Rezolvând prin eliminare gaussiană sistemul cu

$$\text{matricea extinsă } \begin{pmatrix} 3 & -1 & -1 & -1 & a \\ 2 & -1 & 0 & -1 & b \\ 2 & -1 & -1 & 0 & c \\ 3 & -1 & -1 & -1 & d \end{pmatrix}, \text{ găsim}$$

$$\begin{pmatrix} 1 & 0 & 0 & -1 & a-c \\ 0 & 1 & 0 & -1 & 2a-b-2c \\ 0 & 0 & 1 & -1 & b-c \\ 0 & 0 & 0 & 0 & d-a \end{pmatrix}, \text{ de unde obținem soluția } \begin{pmatrix} a-c+\lambda \\ 2a-b-2c+\lambda \\ b-c+\lambda \\ \lambda \end{pmatrix}$$

și condiția de compatibilitate $d = a$. În final, dând lui λ succesiv valorile

$$1, 0, 0, 0 \text{ găsim } U = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & -1 & 1 \\ 2 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

(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 $P_A = (X - 2)^2 X^2$,

$\text{defect}(A - 2I) = 1$ și $\text{defect}(A) = 1$, 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 și numai dacă coloanele sale, u_1, \dots, u_4 , verifică:

$$u_1 \xrightarrow{A-2I} u_2 \xrightarrow{A-2I} 0, \quad u_3 \xrightarrow{A} u_4 \xrightarrow{A} 0 \text{ și } u_2, u_4 \neq 0.$$

$A - 2I = \begin{pmatrix} -2 & -1 & 2 & 1 \\ -2 & -1 & 2 & 1 \\ -1 & -1 & 0 & 2 \\ 0 & -1 & 2 & -1 \end{pmatrix}$. Subspațiul 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 $A^t(1, 1, 0, 1) = 0$ și $A^t(1, 1, 1, 0) = {}^t(1, 1, 0, 1)$. 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 $P_A = (X - 1)^4$. $A -$

$I = \begin{pmatrix} 2 & -1 & 0 & -1 \\ 2 & -1 & 0 & -1 \\ 1 & -1 & 0 & 0 \\ 2 & -1 & 0 & -1 \end{pmatrix}$ și $(A - I)^2 = 0$. Rezultă că $\text{defect}(A - I) = 2$ și

$\text{defect}(A - I)^2 = 4$, 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 și numai dacă coloanele sale, u_1, \dots, u_4 , verifică:

$$u_1 \xrightarrow{A-I} u_2 \xrightarrow{A-I} 0, \quad u_3 \xrightarrow{A-I} u_4 \xrightarrow{A-I} 0 \text{ și } u_2, u_4 \text{ liniar independente.}$$

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 ecuații diferențiale cu coeficienți constanți $y' = Ay$. Prin definiție, o soluție a acestui sistem este o funcție vectorială derivabilă $f : \mathbf{R} \rightarrow \mathbf{C}^n$, astfel încât $f'(t) = Af(t)$ pentru orice t .

În teoria ecuațiilor diferențiale cu coeficienți constanți se arată că soluția generală a acestui sistem de ecuații este $y = e^{tA}C$ cu $C \in M_{n1}(\mathbf{C})$, unde matricea e^{tA} , numită *exponențiala lui A*, se definește prin formula $e^{tA} = \sum_{n=0}^{\infty} (tA)^n/n!$. În aplicații, explicitarea soluției se face prin intermediul formei canonice Jordan.

Fie $B \in M_n(\mathbf{C})$, $S \in GL_n(\mathbf{C})$ și $C \in M_p(\mathbf{C})$. Din definiție rezultă că

$$e^{tSBS^{-1}} = S\left(\sum_{n=0}^{\infty} (tB)^n/n!\right)S^{-1} = Se^{tB}S^{-1}$$

și

$$e^{t(B \oplus C)} = \sum_{n=0}^{\infty} t^n (B \oplus C)^n/n! = e^{tB} \oplus e^{tC}.$$

De aici rezultă că putem reduce calculul lui e^{tA} la cazul celulelor Jordan. Pentru acestea avem

Teorema 203

$$e^{tJ_k(\lambda)} = e^{\lambda t} \begin{pmatrix} 1 & & & & \\ & \frac{t}{1!} & & & \\ & & 1 & & \\ & \frac{t^2}{2!} & \frac{t}{1!} & & \\ & \dots & & & \\ & \frac{t^{k-1}}{(k-1)!} & \dots & \frac{t^2}{2!} & \frac{t}{1!} & 1 \end{pmatrix}.$$

Demonstrație.

$$\begin{aligned} e^{tJ_k(\lambda)} &= \sum_{n=0}^{\infty} \frac{t^n J_k^n(\lambda)}{n!} = \\ &= \sum_{n=0}^{\infty} \begin{pmatrix} \frac{(t\lambda)^n}{n!} & & & & \\ \frac{t}{1!} \frac{(t\lambda)^{n-1}}{(n-1)!} & \frac{(t\lambda)^n}{n!} & & & \\ \frac{t^2}{2!} \frac{(t\lambda)^{n-2}}{(n-2)!} & \frac{t}{1!} \frac{(t\lambda)^{n-1}}{(n-1)!} & \frac{(t\lambda)^n}{n!} & & \\ \dots & & & & \\ \frac{t^{k-1}}{(k-1)!} \frac{(t\lambda)^{n-k+1}}{(n-k+1)!} & \dots & \frac{t^2}{2!} \frac{(t\lambda)^{n-2}}{(n-2)!} & \frac{t}{1!} \frac{(t\lambda)^{n-1}}{(n-1)!} & \frac{(t\lambda)^n}{n!} \end{pmatrix} = \end{aligned}$$

$$= e^{\lambda t} \begin{pmatrix} 1 & & & & \\ \frac{t}{1!} & 1 & & & \\ \frac{t^2}{2!} & \frac{t}{1!} & 1 & & \\ \dots & & & & \\ \frac{t^{k-1}}{(k-1)!} & \dots & \frac{t^2}{2!} & \frac{t}{1!} & 1 \end{pmatrix} \cdot \bullet$$

Exemplu. Fie sistemul de ecuații diferențiale cu coeficienți constanți $y' = Ay$, 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, $A =$

$$U(J_2(2) \oplus J_2(0))U^{-1}, \text{ unde } U = \begin{pmatrix} 0 & 1 & 1 & 0 \\ -1 & 1 & 0 & -2 \\ 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \text{ Rezultă că soluția}$$

generală a ecuației diferențiale $y' = Ay$ 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 Exerciții

În exercițiile următoare K este un corp comutativ.

219. Găsiți clasele de asemănare ale matricelor din $M_2(\mathbf{Z}_2)$. (Indicație. Dacă matricea nu este scalară, atunci ea are un singur factor invariant.)

220. Numărați clasele de asemănare ale matricelor din $M_2(K)$, unde K este un corp cu q elemente.

221. Calculați factorii invariante ai matricelor următoare cu transformări elementare și cu ajutorul polinoamelor Δ . Pentru fiecare matrice, scrieți forma Jordan peste \mathbf{Q} , \mathbf{R} și \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. Descrieți matricele $A \in M_2(\mathbf{C})$ nediazonalizabile.

223. Fie $\alpha, \beta, \gamma \in \mathbf{C}$ distincte și $A \in M_3(\mathbf{C})$. Determinați forma canonică Jordan a lui A în cazurile următoare: (1) $\text{Spec}(A) = \{\alpha, \beta, \gamma\}$. (2) $\text{Spec}(A) = \{\alpha, \beta\}$, $m_a(\alpha) = 2$, $m_g(\alpha) = 2$. (3) $\text{Spec}(A) = \{\alpha, \beta\}$, $m_a(\alpha) = 2$, $m_g(\alpha) = 1$. (4) $\text{Spec}(A) = \{\alpha\}$, $m_g(\alpha) = 3$. (5) $\text{Spec}(A) = \{\alpha\}$, $m_g(\alpha) = 2$. (6) $\text{Spec}(A) = \{\alpha\}$, $m_g(\alpha) = 1$.

224. Determinați forma canonică Jordan și o matrice de asemănare pentru

$$\text{matricea } A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \in M_n(\mathbf{C}).$$

225. Calculați factorii invariante ai matricelor următoare cu transformări elementare și cu ajutorul polinoamelor Δ .

$$\begin{pmatrix} \hat{1} & \hat{1} & \hat{0} & \hat{1} \\ \hat{0} & \hat{0} & \hat{0} & \hat{1} \\ \hat{1} & \hat{1} & \hat{1} & \hat{0} \\ \hat{0} & \hat{1} & \hat{0} & \hat{0} \end{pmatrix} \in M_4(\mathbf{Z}_2) \text{ și } \begin{pmatrix} \hat{1} & \hat{0} & \hat{0} & \hat{0} \\ \hat{0} & \hat{2} & \hat{2} & \hat{2} \\ \hat{0} & \hat{1} & \hat{0} & \hat{0} \\ \hat{0} & \hat{0} & \hat{1} & \hat{0} \end{pmatrix} \in M_4(\mathbf{Z}_3).$$

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 $A \in M_{10}(\mathbf{Q})$. Găsiți forma canonică Jordan a lui A știind că printre divizorii elementari ai lui A peste \mathbf{C} se găsesc $X - i$, $(X - i)^2$, $X + \sqrt{2}$ și $X + \sqrt{3}$.

229. Fie $a, b, c \in \mathbf{C}$ astfel încât a^2, b^2, c^2 sunt distincte. Găsiți 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 $\sigma \in S_n$. Găsiți forma canonică Jordan a matricei $A_\sigma = (a_{ij})_{1 \leq i, j \leq n}$ unde $a_{ij} = \delta_{i\sigma(j)}$. Aplicație: $\sigma = (1943)(852)$. Deduceți că două permutări $\alpha, \beta \in S_n$ sunt conjugate dacă și numai dacă $A_\alpha \approx A_\beta$.

231. Fie V un K -spațiu vectorial cu baza e_1, \dots, e_n , n număr par. Găsiți forma Jordan a endomorfismului u al lui V definit prin $u(e_i) = e_{n+1-i}$.

232. Găsiți forma Jordan a unei matrice $A \in M_n(K)$ de rang 1. Aplicați rezultatul pentru $B = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{pmatrix}$ și $C = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ -3 & -3 & -3 \end{pmatrix}$.

233. Găsiți forma Jordan a unei matrice $A \in M_n(K)$ cu toate elementele egale cu 1.

234. Fie matricea $A = \begin{pmatrix} 5 & 4 & 2 \\ 4 & 5 & 2 \\ 2 & 2 & 2 \end{pmatrix}$. Calculați:

- (a) polinomul caracteristic al lui A ,
- (b) inversa matricei A folosind teorema Hamilton-Cayley,
- (c) valorile proprii și subspațiile proprii corespunzătoare,
- (d) forma Jordan a lui A și o matrice de asemănare.

235. Determinați forma canonică Jordan și o matrice de asemănare pentru matricea $A = \begin{pmatrix} 3 & -1 & 0 & -1 \\ 2 & 0 & 0 & -1 \\ 1 & -1 & 1 & 0 \\ 2 & -1 & 0 & 0 \end{pmatrix} \in M_4(\mathbf{C})$. Calculați puterile lui A .

236. Determinați 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. Determinați forma canonică Jordan și 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. Determinați forma canonică Jordan și 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. Determinați 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. Arătați că o matrice $A \in M_n(K)$ este nilpotentă $\Leftrightarrow P_A = X^n \Leftrightarrow A^n = 0$. Pentru $n = 4$, scrieți toate matricele Jordan nilpotente.

241. Fie $A \in M_n(K)$ astfel încât $P_A = \pi_1\pi_2 \cdots \pi_k$ cu $\pi_1, \pi_2, \dots, \pi_k \in K[X]$ polinoame ireductibile unitare distincte. Arătați că $A \approx J_1(\pi_1) \oplus \cdots \oplus J_1(\pi_k)$.

242. Arătați 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 $n = 4$, scrieți toate matricele Jordan idempotente.

243. Fie matricea $A = \begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 1 \end{pmatrix}$. Arătați că $A = A^2$ și determinați forma Jordan a lui A .

244. Găsiți forma Jordan a lui $J_n^2(0)$.

245. Arătați că $J_5^2(0) \approx J_2^2(0) \oplus J_3^2(0)$ folosind transformări elementare de tip P_{ij} .

246. Dați un exemplu de două matrice nilpotente neasemenea având același rang, polinom caracteristic și polinom minimal.

247. Fie $A, B \in M_n(K)$. Arătați că $Tr(A + B) = Tr(A) + Tr(B)$ și $Tr(AB) = Tr(BA)$.

248. Arătați 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. Arătați că o matrice $A \in M_n(\mathbf{C})$ are urma nulă dacă și numai dacă A se poate scrie sub forma $XY - YX$ cu $X, Y \in M_n(\mathbf{C})$.

250. Fie K un corp, $n \geq 1$, $A \in M_n(K)$ și $b_1, \dots, b_n \in K$ elemente distincte. Arătați că A comută cu $diag(b_1, \dots, b_n) \Leftrightarrow$ este A este matrice diagonală. În particular, dacă $A^k = diag(b_1, \dots, b_n)$, atunci $A = diag(a_1, \dots, a_n)$ cu $a_i^k = b_i$, $i = 1, \dots, n$.

251. Fie $A, B \in M_n(\mathbf{C})$ că $AB = BA$ astfel încât A are valorile proprii distincte. Arătați că există $S \in GL_n(\mathbf{C})$ astfel încât SAS^{-1} și SBS^{-1} sunt matrice diagonale.

252. Fie $A \in M_n(\mathbf{C})$ și $k \geq 2$. Arătați că $2rang(A^k) \leq rang(A^{k-1}) + rang(A^{k+1})$. În particular, dacă $rang(A^k) = rang(A^{k-1})$, atunci $rang(A^{k+1}) = rang(A^k)$.

253. Găsiți forma canonică Jordan a unei matrice $A \in M_7(\mathbf{C})$ cu $\mu_A = X(X - 1)^3$ și $Tr(A) = 4$.

254. Găsiți termenul general al șirurilor date prin relațiile de recurență: (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. Determinați termenul general al șirurilor $(a_n)_n$, $(b_n)_n$, $(c_n)_n$ definite prin relațiile de recurență $a_{n+1} = (b_n + c_n)/2$, $b_{n+1} = (a_n + c_n)/2$, $c_{n+1} = (a_n + b_n)/2$, a_0, b_0, c_0 date.

256. Arătați că pentru $n \geq 2$, ecuația matriceală $Z^2 = J_n(0)$ nu are soluții.

257. Fie K un corp de caracteristică $\neq 2$ și $n \geq 1$. Arătați, prin inducție după n , că ecuația matriceală $Z^2 = J_n(1)$ are soluții.

258. Fie $A = (a_{ij})_{1 \leq i, j \leq n} \in M_n(K)$ o inferior triunghiulară cu $a_{11} = a_{22} = \dots = a_{nn} = \alpha$ și $a_{12}a_{23} \cdots a_{n-1n} \neq 0$. Determinați forma Jordan a lui A și aplicați rezultatul pentru $J_n^k(\alpha)$, $\alpha \in K^*$.

259. Fie $a \in \mathbf{C}^*$ și $k, n \geq 1$. Arătați că ecuația matriceală $Z^k = J_n(a)$ are soluții în $M_n(\mathbf{C})$.

260. Fie matricele $A = \begin{pmatrix} 2 & -1 & 0 & -1 \\ 2 & -1 & 0 & -1 \\ 1 & -1 & 0 & 0 \\ 2 & -1 & 0 & -1 \end{pmatrix}$ și $B = \begin{pmatrix} 3 & -1 & -1 & -1 \\ 2 & -1 & 0 & -1 \\ 2 & -1 & -1 & 0 \\ 3 & -1 & -1 & -1 \end{pmatrix}$.

Au ecuațiile $Y^2 = A$, $Z^2 = B$ soluție în $M_4(\mathbf{C})$?

261. Rezolvați în $M_3(\mathbf{C})$ ecuația $Y^2 = A$, unde $A = \begin{pmatrix} 5 & 2 & 3 \\ 4 & 5 & -4 \\ 6 & 4 & -4 \end{pmatrix}$.

262. Calculați A^n și e^A pentru $A = \begin{pmatrix} 0 & 2 \\ -3 & 5 \end{pmatrix}$.

263. Calculați A^n și e^A pentru $A = \begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix}$.

264. Fie $A \in M_n(\mathbf{C})$. Arătați că $|e^A| = e^{\text{Tr}(A)}$.

265. Calculați 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*. Prentice Hall, New Jersey 1990.
- [2] D. Faddeev, I. Sominski, *Recueil d'exercices d'algèbre supérieure*. Editions MIR, Moscou 1972.
- [3] G. Galbură, F. Radó, *Geometrie*. Editura Didactică și Pedagogică, București 1979.
- [4] P. Halmos, *Naive Set Theory*. Springer, New York, Berlin 1974.
- [5] Ion D. Ion, N. Radu, *Algebră*. Editura Didactică și Pedagogică, București 1991.
- [6] I. Kaplansky *Commutative Rings*. The University of Chicago Press, Chicago and London 1974.
- [7] C. Năstăsescu, C. Niță, C. Vraciu, *Bazele Algebrei*. Editura Academiei Române, București 1986.
- [8] I. Proskouriakov, *Recueil de problèmes d'algèbre linéaire*. Editions MIR, Moscou 1989.
- [9] I. Tomescu, *Probleme de combinatorică și teoria grafurilor*. Editura Didactică și Pedagogică, București 1981.

Index

- adunare modulo n , 30
- aplicația identică, 13
- asociere în divizibilitate, 88
- atom, 35
- automorfism interior, 39
- axioma alegerii, 19

- bază, 128
- baza canonică, 128
- bijecție, 13

- caracteristica unui inel, 69
- celulă Jordan, 155
- centrul unui grup, 41
- ciclu, 38
- clasă de resturi, 22
- clasă la dreapta, 44
- clasă la stânga, 44
- clasa de echivalență, 20
- cmmdc, 89
- cmmmc, 89
- codomeniu, 12
- coeficient, 76, 80
- coeficient dominant, 76
- combinație liniară, 126
- complement algebric, 113
- complementară, 11
- componenta omogenă, 81
- compunerea funcțiilor, 12
- congruență modulo n , 21
- congruențe modulo un subgrup, 44
- conjugare într-un grup, 53
- coordonate, 128
- corp, 61
- corpul cuaternionilor, 73
- corpul de fracții, 75
- corpul fracțiilor raționale, 77

- defectul unui morfism, 131
- determinant, 109
- determinant Vandermonde, 112
- dezvoltarea determinantului după o linie, 114
- dimensiunea unui spațiu vectorial, 128
- divizor al lui zero, 64
- divizori elementari, 154
- domeniu, 65
- domeniu de definiție, 12

- ecuația claselor de elemente conjugate, 54
- ecuație caracteristică, 162
- element inversabil, 28
- element neutru, 27
- eliminarea gaussiană, 136
- exponențiala unei matrice, 168

- factori invariante, 151
- familie de mulțimi, 18
- familie de elemente, 18
- forma canonică Jordan, 160
- forma diagonal-canonică, 149

- forma eşalon, 134
- forma Jordan a unei matrice, 156
- forma Jordan a unui endomorfism, 157
- formula Binet-Cauchy, 118
- formulele De Morgan, 11
- formulele lui Newton, 106
- funcție, 12
- funcții egale, 12

- grad, 76, 80
- grafic, 12
- grup, 28
- grup abelian, 37
- grup ciclic, 43
- grup de simetrie, 38
- grup factor, 48
- grup finit, 37
- grup finit generat, 43
- grup simplu, 59
- grupul \mathbf{Z}_n , 31
- grupul aditiv al unui inel, 61
- grupul diedral D_4 , 39
- grupul diedral D_n , 39
- grupul general liniar, 64
- grupul lui Klein, 38
- grupul permutărilor S_A , 38
- grupul permutărilor S_n , 50
- grupul rotațiilor cubului, 59
- grupul rotațiilor dodecaedrului, 59
- grupul rotațiilor tetraedrului, 59
- grupuri izomorfe, 39

- ideal, 66
- ideal principal, 67
- ideal finit generat, 67
- idealele lui \mathbf{Z} , 66
- idealul generat de o mulțime, 67
- imaginea directă a unei mulțimi, 14

- indicatorul lui Euler, 24, 46
- inel, 61
- inel factor, 70
- inel integru, 65
- inelul \mathbf{Z}_n , 65
- inelul întregilor lui Gauss, 62
- inelul de polinoame în n nedeterminate, 80
- inelul matricelor, 63
- inelul polinoamelor într-o nedeterminată, 76
- inelul seriilor formale, 85
- injectie, 13
- înmulțire cu scalari, 123
- înmulțirea matricelor, 62
- intersecție, 10
- inversa unei funcții, 14
- inversiune, 52
- izometrie, 38
- izomorfism de grupuri, 39
- izomorfism de inele, 68
- izomorfism de monoizi, 32
- izomorfism de spații vectoriale, 125

- Lema chineză a resturilor, 71
- lema lui Kronecker, 97
- liniar independentă, 127

- matrice, 62
- matrice adjuncă, 114
- matrice asemenea, 145
- matrice caracteristică, 146
- matrice companion, 152
- matrice de asemănare, 165
- matrice diagonalizabilă, 159
- matrice eşalon, 134
- matrice echivalente, 148
- matrice echivalente pe linii, 133

- matrice elementare, 133
- matrice inversabilă, 116
- matrice Jordan, 155
- matrice pătratică, 62
- matrice polinomială, 146
- matricea caracteristică, 146
- matricea de trecere, 130
- matricea unui endomorfism, 143
- minor, 113
- minor complementar, 113
- monoame asemenea, 80
- monoid, 28
- monoidul liber, 33
- monom, 76, 80
- morfism de corpuri, 68
- morfism de grupuri, 39
- morfism de inele, 67
- morfism de monoizi, 32
- morfism de spații vectoriale, 124
- morfismul lui Frobenius, 70
- mulțime, 9
- mulțime factor, 20
- mulțime numărabilă, 16
- mulțimea părților, 10
- mulțimea vidă, 10
- mulțimi disjuncte, 10
- mulțimi echipotente, 16
- multiplicitate algebrică, 162
- multiplicitate geometrică, 162
- multiplicitatea unei rădăcini, 79
- necunoscute principale, 135
- necunoscute secundare, 135
- notație aditivă, 29
- notație multiplicativă, 29
- nucleul unui morfism de grupuri, 41
- nucleul unui morfism de inele, 69
- număr prim, 93
- omotetie, 125
- operație comutativă, 27
- operație algebrică, 27
- operație asociativă, 27
- ordinea lexicografică, 102
- ordinul unui grup, 37
- parte stabilă, 28
- partiție, 20
- pereche ordonată, 11
- permutări disjuncte, 51
- permutare, 13
- permutare impară, 53
- permutare pară, 53
- pivot, 134
- polinoamele simetrice fundamentale, 101
- polinom ireductibil, 93
- polinom matriceal, 146
- polinom simetric, 101
- polinom unitar, 76
- polinomul caracteristic, 146
- polinomul minimal, 158
- pre-imaginea a unei mulțimi, 14
- produs cartezian, 11, 19
- produs direct de grupuri, 38
- produs direct de inele, 64
- produsul direct de spații vectoriale, 124
- proiecție canonică, 13
- rădăcină, 78
- rangul unei matrice, 136
- rangul unui morfism, 131
- regula lui Cramer, 117
- regula lui Laplace, 113
- relație, 19
- relație de echivalență, 19

- relațiile lui Viète, 79
 reuniune, 10
 scalari, 123
 semigrup, 28
 semnatura unei permutări, 52
 sistem compatibil determinat, 133
 sistem compatibil nedeterminat, 133
 sistem Cramer, 118
 sistem de reprezentanți, 21
 sistem incompatibil, 133
 sisteme echivalente, 133
 spațiu vectorial, 123
 spațiu vectorial finit generat, 126
 spațiul vectorial standard, 124
 structura grupurilor ciclice, 49
 subcorp, 72
 subgrup, 40
 subgrup ciclic, 42
 subgrup generat de o mulțime, 42
 subgrup normal, 44
 subgrupul impropriu, 40
 subgrupul trivial, 40
 subinel, 65
 subinel prim, 69
 submulțime, 9
 subspațiu, 125
 subspațiul generat de o mulțime, 126
 sumă directă de matrice, 153
 sumă de ideale, 71
 suma de subspații, 126
 suma directă, 126
 surjecție, 13
 teoremă fundamentală a polinoamelor
 simetrice, 104
 teorema Cantor-Schröder-Bernstein, 17
 teorema de izomorfism pentru inele,
 70
 teorema împărțirii cu rest, 78
 teorema Bézout generalizată, 147
 teorema de izomorfism pentru grupuri,
 48
 teorema formei Jordan, 156
 teorema Fundamentală a Algebrei, 95
 teorema Hamilton-Cayley, 148
 teorema Kronecker-Capelli, 137
 teorema lui Bézout, 78
 teorema lui Cantor, 17
 teorema lui Cauchy, 54
 teorema lui Cayley, 50
 teorema lui Euler, 47
 teorema lui Filippov, 166
 teorema lui Frobenius, 159
 teorema lui Grassman, 132
 teorema lui Kronecker, 137
 teorema lui Lagrange, 45
 teorema lui Wilson, 80
 teorema mică Fermat, 47
 teorema rang-defect, 131
 teorema schimbului, 127
 teoremele lui Euclid, 94
 termen principal, 103
 transformări elementare, 133
 transpoziție, 38
 valori proprii, 147
 valoarea la dreapta, 147
 vector propriu, 160
 vectori, 123