

TIBERIU DUMITRESCU

ALGEBRA 1

București, 2006

Profesorului meu
NICOLAE RADU

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. 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* . Bijecția $I_A : A \rightarrow A$, 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 bijecție $s : A \rightarrow A$ 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 surjectie, 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 surjectie, 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 *imaginea (directă)* a lui X prin f . $f(A)$ se notează cu $\text{Im}(f)$ și se numește *imaginea* 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-imaginea* sau *imaginea 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 endomorfisme monoiziilor $(\mathbf{N}, +)$, (\mathbf{N}, \max) și morfisme 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 $xy^{-1} \in H \cap K$. Afirmția 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 . Afirmția (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 $xy x^{-1} = xx^{-1}y = y \in H$.

(c). Fie H un subgrup de indice 2 al lui G . Cum $[G : H] = 2$, atât clasele la stânga modulo H cât 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 $a_{ij} = \sigma(a_{ij-1})$ 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.

