1. MULŢIMI

Definiţia mulţimii.

Definiţia 1.1. (Cantor) Prin *mulţime* înţelegem o colecţie de obiecte bine determinate şi distincte. Obiectele din care este constituită mulţimea se numesc *elementele* mulţimii. Două mulţimi sunt *egale* dacă ele sunt formate din exact aceleaşi elemente.

Notaţia 1.2. Dacă x este un obiect şi A este o mulţime, vom nota

- $x \in A$ dacă x este element al lui A;
- $x \notin A$ dacă x nu este element al lui A.

Observaţia 1.3. Două mulţimi A şi B sunt egale dacă şi numai dacă are loc echivalenţa $(x \in A \Leftrightarrow x \in B)$.

Moduri de a defini o mulţime:

- *sintetic*, prin enumerarea elementelor mulţimii, e.g. $A = \{0, 1\}$;
- *analitic*, cu ajutorul unei proprietăţi ca caracterizează elementele mulţimii:

$$A = \{x \mid x \text{ are proprietatea P}\}$$

e.g. $A = \{x \mid x \in \mathbb{N},\ x < 2\} = \{x \in \mathbb{R} \mid x^2 = x\}$.

Mulţimi importante.

- Mulţimea numerelor naturale:

$$\mathbb{N} = \{0, 1, 2, \ldots, n, n+1, \ldots\}$$

$$\mathbb{N}^* = \{1, 2, \ldots, n, n+1, \ldots\}$$

- Mulţimea numerelor întregi

$$\mathbb{Z} = \{\ldots, -n-1, -n, \ldots, -2, -1, 0, 1, 2, \ldots, n, n+1, \ldots\}$$

- Mulţimea numerelor raţionale

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0,\ \left(\frac{a}{b} = \frac{p}{q} \Leftrightarrow aq = pb \right) \right\}$$

- Mulţimea numerelor reale: $\mathbb{R}$
- Mulţimea numerelor complexe: $\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\}$
- Mulţimea vidă $\varnothing = \{x \mid x \neq x\}$.

Incluziunea mulţimilor.

Definiţia 1.4. Dacă A şi B sunt mulţimi, spunem că A este *submulţime* a mulţimii B dacă toate elementele lui A sunt şi elemente ale lui B.

Notaţia 1.5. Notăm $A \subseteq B$ faptul că A este o submulţime a mulţimii B.

Observaţia 1.6. Următoarele afirmaţii sunt adevărate, oicare ar fi mulţimile A, B şi C.
i) $A \subseteq B \Leftrightarrow (\forall x \in A, x \in B) \Leftrightarrow (x \in A \Rightarrow x \in B)$.
ii) $A = B \Leftrightarrow (A \subseteq B$ şi $B \subseteq A)$ (antisimetria).
iii) $A \subseteq B$ şi $B \subseteq C \Rightarrow A \subseteq C$.
iv) $A \subseteq A$.
v) $\varnothing \subseteq A$.

Operaţii cu mulţimi.

- *intersecţia*: $A \cap B = \{x \mid x \in A$ şi $x \in B\}$
- *reuniunea*: $A \cup B = \{x \mid x \in A$ sau $x \in B\}$
- *diferenţa*: $A \setminus B = \{x \mid x \in A$ şi $x \notin B\}$
- *complementara*: Dacă $A \subseteq E$, atunci $\complement_E(A) = E \setminus A$.

Propoziţia 1.7. *Următoarele afirmaţii sunt adevărate pentru orice mulţii A, B, C şi E.*

(as) $A \cap (B \cap C) = (A \cap B) \cap C$; $A \cup (B \cup C) = (A \cup B) \cup C$; *(asociativitatea operaţiilor $\cap$ şi $\cup$)*
(com) $A \cap B = B \cap A$; $A \cup B = B \cup A$; *(comutativitatea operaţiilor $\cap$ şi $\cup$)*
(dis) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$; *(distributivitatea operaţiei $\cap$ faţă de $\cup$, respectiv a operaţiei $\cup$ faţă de $\cap$)*
(abs) $A \cap (A \cup B) = A$; $A \cup (A \cap B) = A$; *(absorţia)*
(dM) $\complement_E(A \cap B) = \complement_E A \cup \complement_E B$; $\complement_E(A \cup B) = \complement_E A \cap \complement_E B$ *(formulele lui de Morgan).*

2. Funcţii

Definiţia funcţiei.

Definiţia 2.1. Fie A şi B două mulţimi. Prin *funcţie* (*aplicaţie*) de *domeniu* A şi *codomeniu* B (funcţie definită pe A cu valori în B) înţelegem o coresponenţă f care asociază fiecărui element $a \in A$ un singur element din B, notat $f(a)$, numit *valoarea lui f în punctul* (*argumentul*) a.

Notaţia 2.2. Notăm o funcţie de domeniu A şi codomeniu B prin $f : A \to B$ sau $A \xrightarrow{f} B$. Legea de corespondenţă se mai notează $a \mapsto f(a)$.

Notaţia 2.3. Notaţie $B^A = \{f \mid f : A \to B\}$.

Observaţia 2.4. Fie $f : A \to B$ şi $g : C \to D$ funcţii. Are loc

$$f = g \Leftrightarrow A = C,\ B = D,\ \text{şi } (\forall a \in A, f(a) = g(a)).$$

Example 2.5. $x \mapsto x^2$

Funcţiile pot fi reprezentate cu ajutorul diagramelor Euler-Ven:

Example 2.6.

Definiţia 2.7. Fie A o mulţime, $C \subseteq A$.

- Funcţia $1_A : A \to A$, $\forall a \in A$, $1_A(a) = a$ senumeşte *funcţia identică*.
- Dacă $f : A \to B$ este o funcţie, atunci $f_{|C} : C \to B$, $f_{|C}(c) = f(c)$, $\forall c \in C$, se numeşte *restricţia lui f la C*.
- Funţia $i_{CA} = (1_A)_{|C}$ s.n. aplicaţia de incluziune a lui C în A.

Imagine (inversă).

Definiţia 2.8. Fie $f : A \to B$ o funcţie.

a) Dacă $X \subseteq A$, mulţimea

$$f(X) = \{f(x) \mid x \in X\} = \{y \in B \mid \exists x \in X \text{ a.î. } f(x) = y\}$$

se numeşte *imaginea (directă) lui X prin f*.

b) Mulţimea lui $\mathrm{Im}(f) \overset{\text{not.}}{=} f(A)$ se numeşte *imaginea funcţiei f*.

c) Dacă $Y \subseteq B$, mulţimea

$$f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}$$

se numeşte *imaginea inversă* (*contraimaginea*) lui Y prin f.

Example 2.9.

2.10. Fie $f : A \to B$ o funcţie. Să se arate că:

a) $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$, oricare ar fi $X_1, X_2 \subseteq A$;
b) $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$, oricare ar fi $X_1, X_2 \subseteq A$;
c) La b) nu poate fi demonstrată egalitatea.

2.11. Fie $f : A \to B$ o funcţie. Să se arate că:

a) $f(Y_1 \cup Y_2) = f(Y_1) \cup f(Y_2)$, oricare ar fi $Y_1, Y_2 \subseteq B$;
b) $f(Y_1 \cap Y_2) = f(Y_1) \cap f(Y_2)$, oricare ar fi $Y_1, Y_2 \subseteq B$;

Compunerea funcţiilor.

Definiţia 2.12. Fie $f : A \to B$ şi $g : B \to C$ funcţii. Funcţia $g \circ f : A \to C$, $(g \circ f)(a) = g(f(a))$ s.n. *compusa funcţiilor f şi g.*

Example 2.13. a) $f \circ 1_A = f = 1_B \circ f$.
b) Dacă $C \subseteq A$ şi $f : A \to B$, atunci $f_A = f \circ i_{CA}$.

Teorema 2.14. *Compunerea funcţiilor este asociativă:*

$$f : A \to B,\ g : B \to C,\ h : C \to D \Rightarrow (h \circ g) \circ f = h \circ (g \circ f).$$

Demonstraţie. □

Funcţii injective, surjective, bijective.

Definiţia 2.15. Fie $f : A \to B$ o funcţie. Spunem că funcţia f este

- *injectivă* dacă are loc implicaţia:

$$a_1, a_2 \in A,\ a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2);$$

- *surjectivă* dacă este adevărată propoziţia:

$$\forall b \in B,\ \exists a \in A \text{ a.î. } f(a) = b;$$

- *bijectivă* dacă f este injectivă şi surjectivă.

Observaţia 2.16. Fie $f : A \to B$ o funcţie. Următoarele afirmaţii sunt echivalente:

a) f este injectivă;
b) $a_1, a_2 \in A,\ f(a_1) = f(a_2) \Rightarrow a_1 = a_2$;
c) $\forall b \in B$, ecuaţia $f(x) = b$ are cel mult o soluţie.

Observaţia 2.17. Fie $f : A \to B$ o funcţie. Următoarele afirmaţii sunt echivalente:

a) f este surjectivă;
b) $\mathrm{Im}(f) = B$;
c) $\forall b \in B$, ecuaţia $f(x) = b$ are cel puţin o soluţie.

Observaţia 2.18. Fie $f : A \to B$ o funcţie. Următoarele afirmaţii sunt echivalente:

a) f este bijectivă;
b) $\forall b \in B,\ \exists! a \in A$ a.î. $f(a) = b$;
c) $\forall b \in B$, ecuaţia $f(x) = b$ are exact o soluţie.

Propoziţia 2.19. *Fie $f : A \to B$ şi $g : B \to C$ funcţii. Sunt adevărate implicaţiile:*

i) *f şi g injective $\Rightarrow g \circ f$ este injectivă;*
ii) *$g \circ f$ injectivă $\Rightarrow f$ este injectivă;*
iii) *f şi g surjective $\Rightarrow g \circ f$ este surjectivă;*
iv) *$g \circ f$ surjectivă $\Rightarrow f$ este surjectivă;*
v) *f şi g bijective $\Rightarrow g \circ f$ este bijectivă;*

Demonstraţie.

$\square$

Funcţii inversabile.

Definiţia 2.20. Spunem că o funcţie $f : A \to B$ este inversabilă dacă există $g : B \to A$ astfel încât $g \circ f = 1_A$ şi $f \circ g = 1_B$.

Teorema 2.21. *O funcţie f este inversabilă dacă şi numai dacă ea este bijectivă. În aceste condiţii funcţia g din definiţia 2.20 este unică.*

Demonstraţie.

$\square$

Definiţia 2.22. Funcţia g fin definiţia 2.20 se numeşte *inversa* funcţiei f şi se notează cu f^{-1}.

Propoziţia 2.23. *a) Dacă funcţia $f : A \to B$ este bijectivă, atunci f^{-1} este bijectivă şi $(f^{-1})^{-1} = f$.*

b) Dacă $f : A \to B$ şi $g : B \to C$ sunt funcţii bijective, atunci $g \circ f : A \to C$ este bijectivă şi $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Demonstraţie. TEMA $\square$

Teorema 2.24. ***(Teorema alternativei)*** *Fie A o mulţime finită şi $f : A \to A$ o funcţie. Următoarele afirmaţii sunt echivalente:*

a) *f este bijectivă;*
b) *f este injectivă;*
c) *f este surjectivă.*

Demonstraţie.

$\square$

Familii. În anumite contexte,

Definiţia 2.25. Dacă I şi A sunt mulţimi, o funcţie $\varphi : I \to A$ se numeşte *familie* de elemente din A. Dacă elementele mulţimii A sunt mulţimi, spunem că φ este o *familie de mulţimi*.

Notaţia 2.26. 1) Dacă $\varphi : I \to A$ este o familie de elemente din A, şi $\forall i \in I,\ \varphi(i) = a_i$, atunci notăm $\varphi = (a_i)_{i\in I} = (a_i)$.

2) Dacă $I = \{1, \dots, n\}$, atunci notăm $\varphi = (a_1, \dots, a_n)$ şi numim această famlie *n-uplu*.

Definiţia 2.27. Fie $(A_i)_{i\in I}$ o familie de mulţimi. Atunci

$$\bigcap_{i\in I} A_i = \{x \mid \forall i \in I :\ x \in A_i\}$$

se numeşte reuniunea familiei $(A_i)_{i\in I}$, iar

$$\bigcup_{i\in I} A_i = \{x \mid \exists i \in I :\ x \in A_i\}$$

se numeşte intersecţia familiei $(A_i)_{i\in I}$,

Definiţia 2.28. Fie $(A_i)_{i\in I}$ o familie de mulţimi. Mulţimea

$$\prod_{i\in I} A_i = \{\varphi : I \to \bigcup_{i\in I} A_i \mid \forall i \in I,\ \varphi(i) \in A_i\}$$

se numeşte *produsul cartezian* al familiei $(A_i)_{i\in I}$. Dacă $j \in I$, atunci funcţia $p_j : \prod_{i\in I} A_i \to A_j,\ p_j)(\varphi) = \varphi(j)$ s.n. proiecţia a j-a a produsului cartezian.

Example 2.29. 1) $A_1 \times A_2$

2) $A_1 \times \cdots \times A_n$

3) cazul general:

Observaţia 2.30. Dacă $\forall i \in I,\ A_i \neq \varnothing$, atunci toate proiecţiie canonice sunt funcţii surjective.

3. Relaţii de echivalenţă

Definiţia relaţiei de echivalenţă.

Definiţia 3.1. Fie A o mulţime. O submulţime $\rho \subseteq A \times A$ s.n. *relaţie omogenă pe* A. Dacă $(a, b) \in \rho$, atunci vom spune că *a se află în relaţia ρ cu b*.

Notaţia 3.2. Notă $(a, b) \in \rho$ cu $a\rho b$ şi cu $a\not\rho b$ dacă $(a, b) \notin \rho$.

Example 3.3. 1)

2) δ_A

Definiţia 3.4. Fie ρ o relaţie de echivalenţă definită pe mulţimea A. Spunem că ρ este:

(r) *reflexivă* dacă $\forall a \in A,\ a\rho a$;
(t) *tranzitivă* dacă $(a, b, c \in A,\ a\rho b,\ b\rho c \Rightarrow a\rho c)$;
(s) *simetrică* dacă $(a, b \in A,\ a\rho b \Rightarrow b\rho a)$;

Definiţia 3.5. Spunem că o relaţie omogenă este o *relaţie de echivalenţă* dacă ea este reflexivă, tranzitivă şi simetică.

Example 3.6.

Mulţime factor.

Definiţia 3.7. Dacă ρ este o relaţie de echivalenţă pe A şi $a \in A$, atunci mulţimea $\rho\langle a\rangle = \{b \in A \mid a\rho b\}$ s.n. *clasa e echivalenţă* a lui A. Mulţimea

$$A/\rho = \{\rho\langle a\rangle \mid a \in A\}$$

s.n. *mulţimea factor* (*cât*) indusă de ρ.

Notaţia 3.8. Clasele de echivalenţă se notează de obicei cu $\widehat{a}$, $\overline{a}$, $[a]$ etc.

Teorema 3.9. *Fie $A \neq \varnothing$ o mulţime şi ρ o relaţie de echivalenţă pe A. Atunci:*
a) $\forall a \in A,\ a \in \rho\langle a\rangle$;
b) $a\rho b \Leftrightarrow \rho\langle a\rangle = \rho\langle b\rangle$;
c) $a \not\rho\, b \Leftrightarrow \rho\langle a\rangle \neq \rho\langle b\rangle \Leftrightarrow \rho\langle a\rangle \cap \rho\langle b\rangle = \varnothing$;
d) $A = \bigcup_{a\in A} \rho\langle a\rangle$.

Demonstraţie.

□

Example 3.10. 1)
2) Nucleul unei funcţii

Relaţia de congruenţă modulo n.

Teorema 3.11. *Fie $n > 1$ un număr natural. Considerăm relaţia omogenă pe $\mathbb{Z}$, definită de*

$$x \equiv y (\text{mod } n) \Leftrightarrow n | y - x.$$

Sunt adevărate afirmaţiile:

(a) *Relaţia $\equiv \pmod n$ este o relaţie de echivalenţă.*
(b) *$x \equiv y (\text{mod } n)$ dacă şi numai dacă x şi y dau acelaşi rest prin împărţirea la n.*
(c) *Mulţimea factor indusă este:*

$$\mathbb{Z}_n = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\},$$

unde $r + n\mathbb{Z} = \{r + nk \mid k \in \mathbb{Z}\}$.

Demonstraţie. TEMĂ. □

Definiţia 3.12. Relaţia definită în teorema 3.11 se numeşte *relaţia de congruenţă modulo n*.

Funcţii cu domeniul mulţimi cât.

Observaţia 3.13. Dacă A este o mulţime şi ρ este o relaţie de echivalenţă pe A. Dacă definim o funcţie $f : A/\rho \to B$ de o lege $f(\rho\langle x\rangle) = F(x)$, atunci această definiţie trebuie să fie *independentă de alegerea reprezentaţilor*, i.e.

$$\rho\langle x\rangle = \rho\langle y\rangle \Rightarrow F(x) = F(y).$$

Example 3.14.

4. Exerciţii

4.1. Să se arate că au loc egalităţile:

a) $X \setminus (Y \cup Z) = (X \setminus Y) \setminus Z$;
b) $X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$;
c) $(X \cup Y) \setminus Z = (X \setminus Z) \cup (Y \setminus Z)$
d) $(X \cap Y) \setminus Z = X \cap (Y \setminus Z)$.

pentru orice mulţimi X, Y şi Z.

4.2. Două mulţimi A şi B sunt egale dacă şi numai dacă există o mulţime C astfel încât $A \cap C = B \cap C$ şi $A \cup C = B \cup C$.

4.3. Fie A şi B două mulţimi. Mulţimea

$$A\triangle B = (A\setminus B) \cup (B\setminus A).$$

se numeşte *diferenţă simetrică* a mulţimilor A şi B.

a) Fie A, $B \subseteq E$. Diferenţa simetrică se mai exprimă şi prin:

$$A\triangle B = (A \cap \complement_E(B)) \cup (B \cap \complement(A)).$$

b) Oricare ar fi mulţimile A, B, C, avem:

(i) $A\triangle A = \emptyset$;

(ii) $A\triangle B = B\triangle A$ (comutativitatea diferenţei simetrice);

(iii) $(A\triangle B)\triangle C = A\triangle(B\triangle C)$ (asociativitatea diferenţei simetrice);

(iv) $A\triangle\varnothing = A = \varnothing\triangle A$ ($\varnothing$ este element neutru în raport cu diferenţa simetrică);

(v) $A \cap (B\triangle C) = (A \cap B)\triangle(A \cap C)$ (distributivitatea $\cap$ faţă de $\triangle$).

4.4. Dacă $X \subseteq \mathbb{R}$, atunci notăm $X^* = \{a \in \mathbb{R} \mid \exists x \in X,\ a = |x + 1|\}$. Să se arate că:

a) $(X \cup Y)^* = X^* \cup Y^*$, oricare ar fi $X, Y \subseteq \mathbb{R}$;
b) $(X \cap Y)^* \subseteq X^* \cap Y^*$, oricare ar fi $X, Y \subseteq \mathbb{R}$;
c) la punctul b) nu putem demonstra egalitatea;
d) $(X \cap Y)^* = X^* \cap Y^*$, oricare ar fi $X, Y \subseteq [-1, \infty)$.

5. Operaţii binare; Monoizi; Grupuri

Operaţii binare.

Definiţia 5.1. Fie A o mulţime. O funcţie $\varphi : A \times A \to A$ s.n. *operaţie binară* (*lege de compoziţie*) pe A.

Notaţia 5.2. De obicei, o operaţie binară se notează cu $\cdot$, $+$, $\star$, $\perp$ etc. În loc de $\cdot(x, y) = x \cdot y (= xy)$.

Observaţia 5.3. O operaţie binară pe o mulţime finită poate fi reprezentată cu ajutorul unei matrici, numită "tabla lui Cayley".

Example 5.4. a) $x \star y = x^y$
b) $-$
c) (tabla)

Definiţia 5.5. Fie A o mulţime şi $\star$ o operaţie binară pe A. Spunem că opraţia $\star$

- este *asociativă* dacă $\forall x, y, z \in A,\ (x \star y) \star z = x \star (y \star z)$;
- este *comutativă* dacă $\forall x, y \in A,\ x \star y = y \star x$;
- are *element neutru* dacă $\exists e \in A$ a.î. $\forall x \in A, x \star e = e \star x = x$.

Example 5.6.

Observaţia 5.7. O operaţie are cel mult un element neutru.

Definiţia 5.8. Fie A o mulţime şi $\star$ o operaţie binară pe A care are elementul neutru e. Spunem că $a \in A$ este *inversabil* dacă

$$\exists a' \in A \text{ a.î } a \star a' = a' \star a = e.$$

În aceste condiţii a' s.n. *inversul* (*simetricul*) lui A

Example 5.9. a) $(\mathbb{N}, +)$
b) $(\mathbb{Z}, \cdot)$
c) $(\mathbb{Q}^*, :)$
d) tabla

Observaţia 5.10. Dacă A este o mulţime şi $\star$ este o operaţie binară asociativă pe A care admite un element neutru, atunci orice element din A are cel mult un invers (în A).

5.1. **Semigrupuri şi monoizi.**

Definiţia 5.11. Fie A o mulţime şi $\star$ o operaţie binară pe A.

(a) Perechea $(A, \star)$ s.n. *grupoid*.
(b) Dacă $\star$ este asociativă, spunem că $(A, \star)$ este un *semigrup*.
(c) Dacă $\star$ este asociativă şi are element neutru, spunem că $(A, \star)$ este un *monoid*.

Dacă, în plus $\star$ este comutativă, atunci avem grupoid, semigrup sau monoid *comutativ*.

Observaţia 5.12. Un monoid este un semigrup cu element neutru.

Notaţia 5.13. În general vom nota cu $\cdot$ operaţia unui semigrup sau monoid. Această notaţie s.n. *multiplicativă*.

Dacă $(A, \cdot)$ este un monoid, atunci

- 1 reprezintă elementul neutru şi este numit *unitate*;
- a^{-1} este inversul lui $a \in A$;
- $a^1 = a$, $a^{n+1} = a^n \cdot a$, $foralln \in \mathbb{N}^*$ (notaţie valabilă şi pentru semigrupuri);

- $a^0 = 1$.

Observaţia 5.14. Pentru uşurarea expunerii, ne vom referi doar la *mulţimea suport* A, atunci când discutăm despre un monoid in notaţie multiplicativă: "monoidul A"≡"monoidul $(A, \cdot)$".

Notaţia 5.15. Pentru monoizi comutativi se foloseşte de obicei notaţia *aditivă* $(A, +)$. Dacă $(A, +)$ este un monoid, atunci

- 0 reprezintă elementul neutru şi este numit *zero*;
- $-a$ este imetricul lui $a \in A$;
- $1a = a$, $(n + 1)a = na + a$, $\forall n \in \mathbb{N}^*$ (notaţie valabilă şi pentru semigrupuri);
- $0a = 0$.

Propoziţia 5.16. *Dacă A este un monoid, atunci*

(a) *Pentru orice $a \in A$ şi orice $m, n \in \mathbb{N}$ au loc egalităţile*

$$a^m a^n = a^{m+n}, \ (a^m)^n = a^{mn};$$

(b) *Dacă $a, b \in A$ sunt elemente inversabile, atunci ab este iversabil şi $(ab)^{-1} = b^{-1}a^{-1}$;*

(c) *Dacă $a, b \in A$ sunt elemente care comută (i.e. $ab = ba$), atunci $(ab)^m = a^m b^m$ pentru orice $m \in \mathbb{N}$.*

Demonstraţie. a) şi c) prin inducţie
b) verificare directă. □

Example 5.17. a) $(\mathbb{N}, +)$
b) $(\mathbb{N}^*, +)$
c) $(\mathbb{Z}, \cdot)$
d) M mulţime, $(M^M, \circ)$.

Grupuri.

Definiţia 5.18. Spunem că monoidul $(G, \cdot)$ este un *grup* dacă toate elementele sale sunt inversabile. Dacă, în plus, $\cdot$ este comutativă, atunci $(G, \cdot)$ este *grup comutativ* (*abelian*).

Example 5.19. 1) $(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$
2) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, ...
3) $(\mathbb{Q}, \cdot)$, ...
4) $(\mathbb{Q}^*, \cdot)$, ...
5) Orice mulţime cu un element este grup: $(\{1\}, \star)$, $1 \star 1 = 1$.

Propoziţia 5.20. *Fie $(A, \cdot)$ un monoid. Notă cu $U(A)$ mulţimea elementelor inversabile ale lui A. Atunci restricţia operaţiei $\cdot$ la $U(A)$ este o operaţie pe $U(A)$ şi $(U(A), \cdot)$ este un grup.*

Demonstraţie. Temă. □

Example 5.21. a) Dacă M este o mulţime, şi $S(M) = \{f : M \to M \mid f \text{ este bijectivă}\}$, atunci $(S(M), \circ)$ este un grup, numit *grupul permutărilor mulţimii* M.

b) Dacă $n \in \mathbb{N}^*$ şi $M_n(\mathbb{R})$ reprezintă mulţimea matriilor pătratice de tipul $n \times n$ cu coeficienţi în R, iar $GL_n(\mathbb{R})$ este mulţimea matricilor inversabile cu coeficienţi în $\mathbb{R}$, atunci $(M_n(\mathbb{R}), \cdot)$ este un monoid, iar $(GL_n(\mathbb{R}), \cdot)$ este un grup, numit *grupul general liniar* cu coeficienţi reali.

Teorema 5.22. *Un semigrup $(G, \cdot)$ este grup dacă şi numai dacă oricare ar fi $a, b \in G$, ecuaţiile $ax = b$ şi $xa = b$ au soluţii în G. În aceste condiţii soluţiile ecuaţiilor sunt unice.*

Demonstraţie.

□

Corolarul 5.23. *Un semigrup $(G, \cdot)$ este grup dacă şi numai dacă pntru orice $a \in A$ translaţiile $t_a, t'_a : G \to G$, $t_a(x) = ax$, $t'_a(x) = xa$ sunt bijective.*

Observaţia 5.24. Un semigrup finit $(G, \cdot)$ este grup dacă şi numai dacă în tabla operaţiei sale, fiecare linie şi fiecare coloană reprezintă o permutare a mulţimii G.

Subgrupuri.

Definiţia 5.25. Fie $(G, \cdot)$ un grupoid. Spunem că $H \subseteq G$ este o *parte stabilă* a lui G în raport cu $\cdot$ dacă

$$\forall x, y \in H, xy \in H.$$

Definiţia 5.26. Fie G un grup. Spunem că o submulţime $H \subseteq G$ este un *subgrup* al lui G dacă este parte stabilă a lui G în raport cu $\cdot$ şi H împreună cu restricţia operaţiei $\cdot_{|H}$ formează un grup.

Example 5.27. a) $2\mathbb{Z}$ este subgrup în $(\mathbb{Z}, +)$;
b) $\mathbb{N}$ este parte stabilă în $(\mathbb{Z}, +)$, dar **nu** este subgrup.

Notaţia 5.28. Notăm cu $H \leq G$ faptul că H este subgrup al lui G.

Teorema 5.29. *Fie G un grup şi $H \subseteq G$. Următoarele afirmaţii sunt echivalente:*

a) $H \leq G$.
a) i) $1 \in H$;
   ii) $\forall x, y \in H, xy \in H$;
   iii) $\forall x \in H, x^{-1} \in H$.
b) i) $1 \in H$
   ii) $\forall x, y \in H,\ xy^{-1} \in H$

Demonstraţie.

□

Observaţia 5.30. Condiţia $1 \in H$ poate fi înlocuită cu $H \neq \varnothing$.

5.31. Scrieţi enunţul teoremei pentru notaţia aditivă.

Teorema 5.32. *Intersecţia unei familii de subgrupuri este subgrup.*

Demonstraţie.

$\square$

Definiţia 5.33. Fie G un grup şi $X \subseteq G$. Subgrupul

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

s.n. subgrupul generat de X.

Observaţia 5.34. 1. Subgrupul $\langle X \rangle$ este cel mai mic subgrup care conţine mulţimea X.
2. $\langle \varnothing \rangle = \{1\}$.

Propoziţia 5.35. *Fie G un grup şi $\varnothing \neq X \subseteq G$. Atunci*

$$\langle X \rangle = \{x_1 \dots x_n \mid n \in \mathbb{N}^*,\ \forall i \in \{1, \dots, n\}, x_i \in X \cup X^{-1}\},$$

unde $X^{-1} = \{x^{-1} \mid x \in X\}$.

Notaţia 5.36. Dacă $X = \{x_1, \dots, x_n\}$, atunci $\langle X \rangle = \langle x_1, \dots, x_n \rangle$.

Definiţia 5.37. 1. Fie G un grup şi $g \in G$. Subgrupul $\langle g \rangle$ s.n. *subgrupul ciclic* generat de G.
2. Spunem că grupul G este ciclic dacă exită $g \in G$ a.î. $G = \langle g \rangle$.

Example 5.38. $\mathbb{Z}$
$\mathbb{Q}$

Observaţia 5.39. $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$.

Teorema 5.40. *Sugrupurile unui grup ciclic sunt ciclice.*

Ordinul unui element.

Notaţia 5.41. Dacă $(G, \cdot)$ este un grup, $g \in G$ şi $n \in \mathbb{N}$, atunci $g^{-n} = (g^n)^{-1}$.

Propoziţia 5.42. *Dacă G este un grup, atunci*

(a) *Pentru orice $g \in G$ şi orice $m, n \in \mathbb{Z}$ au loc egalităţile*

$$a^m a^n = a^{m+n},\ (a^m)^n = a^{mn};$$

(b) *Dacă $g, h \in G$ sunt elemente care comută (i.e. $gh = hg$), atunci $(gh)^m = g^m h^m$ pentru orice $m \in \mathbb{N}$.*

Definiţia 5.43. Fie G un grup şi $g \in G$. Spunem că

- *ordinul lui g* este ∞ dacă $\forall n \in \mathbb{N}^*,\ g^n \neq 1$;
- *ordinul lui g* este $n \in \mathbb{N}^*$ dacă $g^n = 1$ şi n este cel mai mic număr natural nenul cu această proprietate.

Notaţia 5.44. Notăm cu $\mathrm{ord}(g)$ ordinul lui G.

Example 5.45. 1.
2.

Propoziţia 5.46. *Dacă G este un grup şi $g \in G$, atunci* $\mathrm{ord}(g) = |\langle g \rangle|$, *unde $|X|$ reprezintă cardinalul mulţimii X.*

Demonstraţie.

$\square$

Teorema 5.47. ***(Teorema lui Lagrange)*** *Fie G un grup finit şi $H \leq G$. Atunci $|H|$ divide $|G|$.*

Demonstraţie.

$\square$

Corolarul 5.48. *Dacă G este un grup şi $g \in G$, atunci* $\mathrm{ord}(g)$ *divide* $|G|$.

Morfisme.

Definiţia 5.49. Fie G şi G' grupoizi şi $f : G \to G'$ o funcţie.

- Spunem că f este un *morfism* (*de grupoizi*) dacă $f(gh) = f(g)f(h)$ pentru orice $g, h \in G$.
- Dacă G şi G' sunt monoizi, spunem că f este un morfism de monoizi dacă este un morfism de grupoizi şi $f(1) = 1'$, unde 1 reprezintă unitatea lui G, iar $1'$ este unitatea lui G'.

- Dacă G şi G' sunt grupuri, spunem că f este un *morfism de grupuri* dacă f este un morfism de monoizi şi $\forall g \in G,\ f(g^{-1}) = (f(g))^{-1}$.

În toate cele trei cazuri, dacă în plus f este bijectivă, spunem că f este un *izomorfism*. În această situaţie spunem că G şi G' sunt *izomorfe*.

Notaţia 5.50. Notăm cu $G \cong G'$ faptul că G şi G' sunt izomorfe.

Teorema 5.51. *Fie G şi G' două grupuri şi $f : G \to G'$ o funcţie. Funcţia f este un morfism de grupuri dacă şi numai dacă $\forall x, y \in G,\ f(xy) = f(x)f(y)$ (i.e. f este morfism de grupoizi).*

Demonstraţie.

$\square$

Propoziţia 5.52. *a) Compusa a două morfisme este un morfism.*
b) Inversa unui izomorfism este un izomofism.

Example 5.53. 1.
2.

5.54. Fie $f : G \to G'$ un morfism de monoizi (grupuri). Atunci $f(x^n) = (f(x))^n$ pentru orice $n \in \mathbb{N}$ ($n \in \mathbb{Z}$).

5.55. Fie $f : G \to G'$ un morfism de grupuri.
a) Arătaţi că $\mathrm{Ker}(f) = \{g \in G \mid f(g) = 1'\}$ este un subgrup al lui G (numit *nucleul lui* f).
b) f este funcţie injectivă dacă şi numai dacă $\mathrm{Ker}(f) = \{1\}$.

Exemple de grupuri.

Grupul numerelor întregi: $(\mathbb{Z}, +)$

Teorema 5.56. *O submulţime $H \subseteq \mathbb{Z}$ este subgrup în $\mathbb{Z}$ dacă şi numai dacă $H = n\mathbb{Z}$ pentru $n \in \mathbb{N}$.*

Lema 5.57. *Fie $m, n \in \mathbb{N}$. $m\mathbb{Z} \subseteq n\mathbb{Z} \Leftrightarrow n \mid m$.*

Corolarul 5.58. *a)* $m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z}$;

b) $m\mathbb{Z} + n\mathbb{Z} \overset{def}{=} \{mk + nl \mid k, l \in \mathbb{Z}\} = (m, n)\mathbb{Z}$;

c) $(m, n) = d \Rightarrow \exists k, l \in \mathbb{Z}$ *a.î* $d = km + ln$;

d) $(m, n) = 1 \Leftrightarrow \exists k, l \in \mathbb{Z}$ *a.î* $1 = km + ln$.

Grupuri de clase de resturi. : $(\mathbb{Z}_n, +)$.

Dacă $n \in \mathbb{Z}$, $n \geq 2$, $\mathbb{Z}_n = \{\widehat{0}, \ldots, \widehat{n-1}\}$. Considerăm operaţia

$$\widehat{i} + \widehat{j} = \widehat{i+j}.$$

Atunci $(\mathbb{Z}_n, +)$ este un grup ciclic.

5.59. $\langle \widehat{i} \rangle = \mathbb{Z}_n \Leftrightarrow (i, j) = 1$.

Grupuri de permutări. Dacă X este o mulţime, atunci $X^X = \{f \mid f : X \to X\}$ este un monoid în raport cu compunerea fucţiilor. Rezultă că $(S(X), \circ)$, unde $S(X) = \{f : X \to X \mid f$ este bijectivă$\}$, este un grup, numit grupul permutărilor mulţimii X.

Definiţia 5.60. Spunem că grupul G *se scufundă în* grupul H dacă există un morfism injectiv $G \to H$.

Teorema 5.61. *Orice grup se scufundă într-un grup de permutări.*

Demonstraţie.

$\square$

Dacă $X = \{1, \ldots, n\}$, atunci notăm $S(X) = S_n$ şi grupul permutărilor mulţimii X s.n. *grupul permutărilor de grad* n.

reprezentarea permutărilor de grad n...

Definiţia 5.62. Fie $\sigma \in S_n$. Spunem că o pereche (i, j) cu $1 \leq i < j \leq n$ determină o *inversiune* pentru σ dacă $\sigma(i) > \sigma(j)$. Notăm cu $Inv(\sigma)$ numărul inversiunilor lui σ. Numărul $\epsilon(\sigma) = (-1)^{Inv(\sigma)}$ s.n. *signatura* permutării σ.

Propoziţia 5.63. *a) Dacă $\sigma \in S_n$, atunci $\epsilon(\sigma) = \prod_{1\leq i<j\leq n} \frac{\sigma(j)-\sigma(i)}{j-i}$.*
b) $\epsilon : S_n \to \{1, -1\}$ este un morfism de grupuri.

6. Inele şi corpuri

Definiţia 6.1. Un triplet $(A, +, \cdot)$, format dintr-o mulţime A şi două operaţii pe A s.n. *inel* dacă

a) $(A, +)$ este un grup abelian,
b) $(A, \cdot)$ este un semigrup,
c) operaţia $\cdot$ este distributivă faţă de $+$: $x(y + z) = xy + xz$ şi $(x + y)z = xz + yz$, oricare ar fi $x, y, z \in A$.

Dacă $(A, \cdot)$ este un monoid, atunci spunem că inelul este *cu unitate*.

Notaţia 6.2. Se folosesc notaţiile standard pentru scrierea aditivă, respectiv multiplicativă:

- 0 reprezintă elementul neutru din $(A, +)$ şi este numit *zeroul* inelului.
- dacă $x \in A$, atunci $-x$ este simetricul lui x (faţă de operaţia $+$)
- 1 notează elementul neutru faţă de $\cdot$ (dacă există) şi este numit *unitatea inelului*.

Observaţia 6.3. În cazul general nu putem deduce $0 \neq 1$. Dacă $(A, +)$ este un grup abelian şi $\star$ este operaţia pe A definită de

$$x \star y = 0, \ \forall x, y \in A,$$

atunci $(A, +, \star)$ este un inel cu unitate în care $0 = 1$. Acest inel s.n. *inelul nul*.

6.4. Dacă A este un inel, atunci $x \cdot 0 = 0 \cdot x = 0$, $\forall x \in A$.

Definiţia 6.5. Un inel $(K, +, \cdot)$ pentru care $(K^*, \cdot)$, unde $K^* = K \setminus \{0\}$ este un grup s.n. *corp*. Dacă inelul este comutativ, atunci şi corpul este *corp comutativ*.

6.6. Demonstraţi că orice corp este inel cu unitate.

Definiţia 6.7. Fie A un inel şi $x, y \in A^*$. Dacă $xy = 0$, atunci spunem că x şi y sunt divizori ai lui 0. Un inel comutativ, cu unitate astfel încât $1 \neq 0$ şi fără divizori ai lui 0 s.n. *domeniu de integritate*

6.8. Orice corp comutativ este domeniu de integritate.

Teorema 6.9. *Orice domeniu de integritate finit este un corp.*

Demonstraţie.

□

Exemple de inele şi corpuri.

1. *Inelul numerelor întregi*: $(\mathbb{Z}, +, \cdot)$ este un domeniu de integritate care nu este corp.
2. *Inelul întregilor lui Gauss*

3. *corpul numerelor raţionale* şi *corpul numerelor reale*

4. *corpul cuaternonilor*

5. *Clase de resturi*

6. *Polinoame*

Subinele şi subcorpuri.

Definiţia 6.10. Fie R un inel (corp) şi $S \subseteq R$. Spunem că S este un *subinel* (respectiv *subcorp*) al lui R dacă S este stabilă faţă de operaţii şi împreună cu restricţiile acestora formează un inel (respectiv corp).

Example 6.11.

Teorema 6.12. ***(teorema de caracterizare a subinelelor)*** *Fie R un inel şi $S \subseteq R$. Următoarele afirmaţii sunt echivalente:*

a) *S este un subinel al lui R;*

b) (i) $S \neq \varnothing$ *(*$0 \in S$*),*

(ii) $\forall x, y \in S \ x - y \in S$,

(iii) $\forall x, y \in S \ xy \in S$.

Demonstraţie.

$\square$

Teorema 6.13. ***(teorema de caracterizare a subcorpurilor)*** *Fie K un corp şi $S \subseteq K$. Următoarele afirmaţii sunt echivalente:*

a) *S este un subcorp al lui K;*
b) (i) $|S| > 1$ *($0, 1 \in S$),*
(ii) $\forall x, y \in S$ $x - y \in S$,
(iii) $\forall x \in S$, $\forall y \in S \setminus \{0\}$ $xy^{-1} \in S$.

Demonstraţie. TEMĂ □

Teorema 6.14. *Intersecţia unei familii de subinele (subcorpuri) este un subinel (subcorp).*

Demonstraţie. Temă □

Observaţia 6.15. Ca în cazul grupurilor, se pot defini subinelul generat de o mulţime şi subcorpul generat de o mulţime.