1. Preliminarii

Mulţimi.

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 ($x \in A \Leftrightarrow x \in B$).

Definiţia 1.4. Dacă A şi B sunt mulţimi, spunem că A este *submulţime* a mulţimii B c si notăm $A \subseteq B$ dacă toate elementele lui A sunt şi elemente ale lui B.

Observaţia 1.5. Următoarele afirmaţii sunt adevărate, oricare 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 $\mathrm{C}_E(A) = E \setminus A$.

Mulţimi finite. Spunem că o mulţime A este *finită* daca din $X \subseteq A$ şi $|A| = |X|$ rezultă că $X = A$.

Teorema 1.6. ***(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.*

Mulţimi importante.

- Mulţimea numerelor naturale:

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

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

- Mulţimea numerelor întregi

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

- 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 matricilor pătratice cu n linii, n coloane şi coeficienţi în K: $\mathcal{M}_n(K)$;

Aritmetică în $\mathbb{Z}$.

Teorema 1.7. *(Teorema împăţirii cu rest) Fie $n \in \mathbb{N}^*$ şi $a \in \mathbb{Z}$. Atunci există o unică pereche de numere întregi (q, r) astfel încât*

(i) $a = nq + r$;
(ii) $0 \leq r < n$.

In condiţiile din teoremă,

- q este câtul împărţirii lui a la n şi
- r este împărţirii lui a la n.

Fie a, $b \in \mathbb{Z}$. Spunem că a *divide pe* b şi notăm $a \mid b$ sau $b \vdots a$ dacă există $q \in \mathbb{Z}$, astfel încât $b = a \cdot q$.

Dacă $a \mid b$, mai spunem că a *este divizor pentru* b sau a *este factor al lui* b sau b *este multiplu pentru* a sau b *factorizează prin* a.

Fie $a, b \in \mathbb{Z}^*$ şi $d \in \mathbb{N}^*$. Atunci *cel mai mare divizor comun* al numerelor a şi b este numărul $d \overset{not.}{=} (a, b)$ care îndeplineşte simultan condiţiile:

$$\begin{cases} d \mid a \text{ şi } d \mid b, \\ c \in \mathbb{Z}, c \mid a \text{ şi } c \mid b \Rightarrow c \mid d \end{cases}$$

Teorema 1.8. (*reprezentarea Bézout a c.m.m.d.c.*) *Dacă $a, b \in \mathbb{Z}^*$ şi $d = (a, b)$, atunci există $u, v \in \mathbb{Z}$ astfel încât*

$$d = au + bv.$$

Cel mai mic multiplu comun al numerelor a şi b este numărul $m \overset{not.}{=} [a, b] \in \mathbb{N}^*$ care îndeplineşte simultan condiţiile:

$$\begin{cases} m \in \mathbb{N}^*, \\ a \mid m \text{ şi } b \mid m, \\ c \in \mathbb{Z}^\star, a \mid c \text{ şi } b \mid c \Rightarrow m \leq |c|. \end{cases}$$

Teorema 1.9. *Oricare ar fi $a, b \in \mathbb{N}^*$, are loc egalitatea:*

$$ab = (a, b)[a, b].$$

Notaţia 1.10. Dacă $n \in \mathbb{N}$ şi $\ell \in \mathbb{Z}$, notăm

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

Observaţia 1.11. Fie $n \in \mathbb{N}$, $n \geq 2$, fixat. Dacă $\ell_1, \ell_2 \in \mathbb{Z}$ dau prin împărţire la n resturile r_1 şi r_2, observăm că

$$n\mathbb{Z} + \ell_1 = n\mathbb{Z} + \ell_2 \Leftrightarrow r_1 = r_2.$$

Definiţia 1.12. Fie $n \in \mathbb{N}$, $n \geq 2$, fixat. Pentru orice $\ell \in \mathbb{Z}$ notăm $\widehat{\ell} = n\mathbb{Z} + \ell$ şi numim această mulţime clasa de resturi modulo n a lui ℓ.

Mulţimea

$$\mathbb{Z}_n = \{\widehat{0}, \widehat{1}, \ldots, \widehat{n-1}\}$$

se numeşte *multimea claselor de resturi modulo n.*

Exemplul 1.13. $n = 5$

2. Operaţii binare; Monoizi; Grupuri

Operaţii binare.

Definiţia 2.1. Fie A o mulţime. O funcţie $\varphi : A \times A \to A$ se numeşte *operaţie binară* (*lege de compoziţie*) pe A.

Notaţia 2.2. De obicei, o operaţie binară se notează cu $\cdot$, $+$, $\star$, $\perp$ etc. În loc de $\star(x, y)$ scriem $x \star y$. De exemplu $\cdot(x, y) = x \cdot y$ ($\overset{not}{=} xy$).

Observaţia 2.3. O operaţie binară pe o mulţime finită poate fi reprezentată cu ajutorul unei matrici, numită "tabla lui Cayley".

Definiţia 2.4. 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. $\forall x \in A, x \star e = e \star x = x$.

Definiţia 2.5. 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

Exemplul 2.6. a) Pe $\mathbb{R}^*$: $x \star y = x^y$

b) Operaţiile uzuale

c) Operaţii pe $\mathbb{Z}_n$:

d) Tabla operaţiilor pe $\mathbb{Z}_4$, $\mathbb{Z}_5$.

e) Operaţii cu matrici:

Observaţia 2.7. O operaţie are cel mult un element neutru.

Observaţia 2.8. 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).

Semigrupuri, monoizi, grupuri.

Definiţia 2.9. 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 2.10. Un monoid este un semigrup cu element neutru.

Notaţia 2.11. În general vom nota cu $\cdot$ operaţia unui semigrup sau a unui 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 $a \in A$ (dacă există);

Observaţia 2.12. 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 2.13. Pentru monoizi comutativi se foloseşte de obicei notaţia *additivă* $(A, +)$. Dacă $(A, +)$ este un monoid, atunci

- 0 reprezintă elementul neutru şi este numit *zero*;
- $-a$ este simetricul lui $a \in A$;

Notaţia 2.14. Fie $(A, \cdot)$ un monoid. Vom nota:

- $a^1 = a$, $a^{n+1} = a^n \cdot a, \forall n \in \mathbb{N}^*$ (notaţie valabilă şi pentru semigrupuri);
- $a^0 = 1$.

Dacă se foloseşte notaţia additivă, $(A, +)$, avem $1a = a$, $(n+1)a = na + a$, $\forall n \in \mathbb{N}^*$ (notaţie valabilă şi pentru semigrupuri); $0a = 0$.

Propoziţia 2.15. *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. □

Exemplul 2.16. a) $(\mathbb{N}, +)$
b) $(\mathbb{N}^*, +)$
c) $(\mathbb{Z}, \cdot)$
d) M mulţime, $(M^M, \circ)$.

Grupuri.

Definiţia 2.17. Spunem că monoidul $(G, \cdot)$ este un *grup* dacă toate elementele sale sunt inversable. Dacă, în plus, $\cdot$ este comutativă, atunci spunem că $(G, \cdot)$ este un *grup comutativ* (sau grup *abelian*).

Exemplul 2.18. 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: $(\{1\}, \star)$, $1 \star 1 = 1$.
6) $(\mathbb{Z}_n, +)$
7) $(\mathbb{Z}_n^*, \cdot)$ este grup (abelian) dacă şi numai dacă n este prim.

Propoziţia 2.19. *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. □

Exemplul 2.20. 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 $(\mathcal{M}_n(\mathbb{R}), \cdot)$ este un monoid, iar $(GL_n(\mathbb{R}), \cdot)$ este un grup, numit *grupul general liniar* cu coeficienţi reali.

c) Dacă $n \geq 2$ este un număr natural, atunci $(U(\mathbb{Z}_n, \cdot), \cdot)$ formează un grup abelian.

$U(\mathbb{Z}_n) = \{\widehat{k} \mid (k,n) = 1\}$.
De exemplu, dacă $n = 12$, atunci $U(\mathbb{Z}_n) = \{\widehat{1}, \widehat{5}, \widehat{7}, \widehat{11}\}$.

Teorema 2.21. *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 2.22. *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 2.23. 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.

Ordinul unui element.

Notaţia 2.24. Dacă $(G, \cdot)$ este un grup, $g \in G$ şi $n \in \mathbb{N}$, atunci $g^{-n} = (g^n)^{-1}$.

Propoziţia 2.25. *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) $(g_1 \cdot \ldots \cdot g_k)^{-1} = g_k^{-1} \cdot \ldots \cdot g_1^{-1}$.
(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 2.26. 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 2.27. Notăm cu $\text{ord}(g)$ ordinul lui g.

Exemplul 2.28. 1.

2.

Propoziţia 2.29. *Fie* $(G, \cdot)$ *un grup şi* $x, g, h \in G$ *astfel încât* $\text{ord}(g), \text{ord}(h) \in \mathbb{N}^*$. *Sunt adevărate afirmaţiile:*

(i) *oricare ar fi* $k \in \mathbb{N}$ *avem*

$$\text{ord}(x^k) = \frac{\text{ord}(x)}{(k, \text{ord}(x))};$$

(ii) *dacă* $gh = hg$, *atunci* $\text{ord}(gh) = [\text{ord}(g), \text{ord}(h)]$.

Propoziţia 2.30. *Dacă* G *este un grup şi* $g \in G$, *atunci* $\text{ord}(g)$ *divide* $|G|$.

Morfisme.

Definiţia 2.31. 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'.

Definiţia 2.32. Dacă G şi G' sunt grupuri, spunem că f este un *morfism de grupuri* dacă

$$\forall g, h \in G \text{ avem } f(gh) = f(g)f(h).$$

Definiţia 2.33. În toate cele trei cazuri, dacă f este un morfism şi funcţia f este bijectivă, atunci spunem că f este un *izomorfism*.

Dacă există un izomorfism $f : (G, \cdot) \to (G', \cdot)$, atunci spunem că G şi G' sunt *izomorfe*.

Notaţia 2.34. Notăm cu $G \cong G'$ faptul că G şi G' sunt izomorfe.

Teorema 2.35. *Fie G şi G' două grupuri şi $f : G \to G'$ un morfism de grupuri. Atunci*

(a) *Dacă 1_G este elementul neutru al lui G şi $1_{G'}$ este elementul neutru al lui G', atunci $f(1_G) = 1_{G'}$.*
(b) *Pentru orice $x \in G$ avem $f(x^{-1}) = f(x)^{-1}$.*
(c) *Pentru orice $x \in G$ şi orice $n \in \mathbb{Z}$ avem $f(x^n) = f(x)^n$.*
(d) *Dacă $x \in G$ are ordinul finit, atunci $f(x)$ are ordinul finit şi* $\text{ord}(f(x)) \mid \text{ord}(x)$*;*
(e) *Dacă f este un izomorfism şi $x \in G$, atunci* $\text{ord}(f(x)) = \text{ord}(x)$.

Demonstraţie.

□

Propoziţia 2.36. *a) Compusa a două morfisme este un morfism.*
b) Inversa unui izomorfism este un izomofism.

Exemplul 2.37. 1. $f : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$, $f(\alpha) = \cos(\alpha) + i \sin(\alpha)$

2. Dacă $n \geq 2$, $f : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$, $f(k) = \widehat{k}$

3. Dacă $n \in \mathbb{N}^*$ şi $K \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n, \cdots\}$, atunci funcţia determinant $\det : (GL_n(K), \cdot) \to (K^*, \cdot)$ este un morfism de monoizi. Dacă K^* este grup, atunci det este morfism de grupuri.

Exerciţiul 2.38. Fie $(G, \cdot)$ un grup. Demonstraţi că funcţia $f : G \to G$, $f(x) = x^2$, este un morfism de grupuri dacă şi numai dacă G este comutativ.

Observaţia 2.39. Fie $(G, \cdot)$ şi $(H, \cdot)$ grupoizi astfel încât G şi H sunt mulţimi finite. Dacă există o funcţie bijectivă $f : G \to H$ care transformă tabla operaţiei lui G şi în tabla operaţiei lui H, atunci $G \cong H$.

In aceste condiţii, dacă G este grup (semigrup, monoid), rezultă că G' este de asemenea un grup (semigrup, respectiv monoid) şi el este izomorf cu G.