Algebra

2.1. Grupuri

Definiție 2.1.1.

Un grup este o pereche $(G, \cdot)$ care constă dintr-o mulțime G împreună cu o operație $\cdot : G \times G \to G$, a.î. $\cdot$ este asociativă, are un element neutru și fiecare element din G este inversabil în raport cu $\cdot$. În cazul în care $\cdot$ este și comutativă atunci G se numește abelian sau comutativ.

Exemplu 2.1.2.

Următoarele perechi sunt grupuri (abeliene):

(a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$

- asociativitate: $x+(y+z) = (x+y)+z$
- element neutru: 0, deoarece $x+0 = x$
- invers: $\forall\, x \in \mathbb{Z}$, inversul este $-x$, deoarece $x - x = 0$

(b) $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$

(c) $(M_{m\times n}(\mathbb{Z}), +)$, $(M_{m\times n}(\mathbb{Q}), +)$, $(M_{m\times n}(\mathbb{R}), +)$, $(M_{m\times n}(\mathbb{C}), +)$

Următoarele perechi sunt monoizi (nu necesită să aibă un invers) dar nu grupuri:

(a) $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$

- asociativitate: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- element neutru: 1, deoarece $x \cdot 1 = x$

(b) $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$

(c) $(M_{m \times m}(\mathbb{Z}), \cdot)$, $(M_{m \times m}(\mathbb{Q}), \cdot)$, $(M_{m \times m}(\mathbb{R}), \cdot)$, $(M_{m \times m}(\mathbb{C}), \cdot)$

Observație 2.1.4.

Cel mai adesea operația unui grup oarecare este notată multiplicativ, adică $(G, \cdot)$. În acest caz elementul neutru este notat 1 și pentru $x \in G$ notăm cu x^{-1} elementul invers. Pentru un grup abelian însă operația este adesea notată aditiv, adică $(G, +)$. În acest caz, elementul neutru se notează 0, iar pentru $x \in G$ notăm $-x$ elementul opus.

Subgrupuri

Definiție 2.1.7.

Fie $(G, *)$ un grup. Un subgrup al lui G este o submulțime $H \subseteq G$, a.î. operația pe G induce o operație bine definită pe H ($x, y \in H \Rightarrow x * y$ (calculat cu operația din G) $\in H$; se spune de asemenea că H este o parte stabilă a lui G), și H împreună cu operația indusă formează un grup. Se scrie $H \leq G$.

Exemplu 2.1.8.

(1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ (cu adunarea)

(2) $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$ (cu înmulțirea)

(3) $\mathbb{R}^*_+ \leq \mathbb{R}^*$, unde $\mathbb{R}^*_+ = (0, \infty)$

(4) Orice grup G are așa numitele subgrupuri triviale i.e. $\{1\}$ și G.

Propoziție 2.1.9.

(Teorema de caracterizare a grupurilor). Fie $(G, \cdot)$ un grup și fie $H \subseteq G$ o submulțime. Următoarele afirmații sunt echivalente:

(i) $H \leq G$

(ii) (a) $1 \in H$

(b) $x, y \in H \Rightarrow xy \in H$

(c) $x \in H \Rightarrow x^{-1} \in H$

(iii) (a) $1 \in H$

(b) $x, y \in H \Rightarrow xy^{-1} \in H$

<u>Propoziție</u> 2.1.10.

Fie $(G, \cdot)$ un grup. Dacă $H_i \leq G$, unde $i \in I$, atunci $\bigcap_{i \in I} H_i \leq G$

<u>Observație</u> 2.1.11.

Reuniunea a două sau mai multe subgrupuri nu este cu necesitate subgrup. De exemplu avem două subgrupuri $H_1 = \mathbb{R}^+$ și $H_2 = \{-1, 1\}$, $H_1 \cup H_2$ conține toate elementele lor dar dacă $x \in \mathbb{R}^+$, $y = -1$ se poate ca $x \cdot y \notin H_1 \cup H_2$.

Definiție 2.1.12.

Fie $(G, \cdot)$ un grup și $X \subseteq G$ o submulțime a lui G.
Subgrupul generat de X este definit prin:

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

Dacă $X = \{x_1, x_2, \dots, x_n\}$ este o mulțime finită atunci scriem $\langle x_1, x_2, \dots, x_n \rangle$ în loc de $\{$

dacă avem o **submulțime** $X \subseteq G$, **subgrupul generat de** X este definit ca:

$\langle X \rangle = \bigcap \{ H \leq G \mid X \subseteq H \}$,

unde H sunt toate subgrupurile din G care conțin X.

- Este garantat că $\langle X \rangle$ este un subgrup (pentru că intersecția subgrupurilor este tot un subgrup).
- Spre deosebire de reuniunea subgrupurilor, $\langle X \rangle$ este construit astfel încât să fie **cel mai mic subgrup** al lui G care conține toate elementele din X.

De exemplu dacă $G = (\mathbb{Z}, +)$ și $X = \{3\}$ obținem:

$$\langle 3 \rangle = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\} = 3\mathbb{Z}$$

Lemă 2.1.13.

Fie $(G, \cdot)$ un grup și $X \subseteq G$ o submulțime a lui G.
Atunci:

(a) $\langle X \rangle \leq G$.

(b) $X \subseteq \langle X \rangle$ și $X = \langle X \rangle$ ddacă $X \leq G$.

(c) $\langle X \rangle$ este cel mai mic subgrup a lui G care conține submulțimea X

(d) dacă $X \subseteq Y \subseteq G$, atunci $\langle X \rangle \leq \langle Y \rangle \leq G$

<u>Propoziție</u> 2.1.14.

Fie $(G, \cdot)$ un grup și $X \subseteq G$ o submulțime a lui G. Atunci: $\langle X \rangle = \{ x_1, x_2, \ldots, x_n \mid n \in \mathbb{N},\ x_1, x_2, \ldots, x_n \in X \cup X^{-1} \}$, unde $X^{-1} = \{ x^{-1} \mid x \in X \}$. Asta înseamnă că grupul generat $\langle X \rangle$ este format din toate elementele care se pot exprima ca produse finite de elemente din X și din X^{-1}

<u>Observație</u> 2.1.15.

Fie $(G, \cdot)$ un grup și $x \in G$. Pentru orice $n \in \mathbb{Z}$ se definește:

$$x^n = \begin{cases} xx\ldots x \ (n \text{ ori}),\ n > 0 \\ 1,\ n = 0 \\ x^{-1} x^{-1} \ldots x^{-1} \ (n \text{ ori}),\ n < 0 \end{cases}$$

Dacă operația este aditivă, adică $(G, +)$ atunci scriem

$$nx = \begin{cases} x + x + \dots + x \ (n \text{ ori}), & n > 0 \\ 0, & n = 0 \\ (-x) + (-x) + \dots + (-x) \ (n \text{ ori}), & n < 0 \end{cases}$$

Corolar 2.1.16.

Fie $(G, \cdot)$ un grup

(a) Pentru $x \in G$ avem $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$

(b) Pentru $x, y \in G$ avem $\langle x, y \rangle = \{x^n y^m \mid n, m \in \mathbb{Z}\}$

Homomorfisme de grupuri

Definiție 2.1.17.

Fie $(G, *)$ și $(H, *)$ două grupuri. Se numește homomorfism (de grupuri) între G și H o funcție $f: G \to H$ cu proprietatea $f(x * y) = f(x) * f(y)$ pentru orice $x, y \in G$. Se numește izomorfism (de grupuri) un homomorfism care este bijectiv. În acest caz grupurile se zic izomorfe și notăm $G \cong H$.

Exemplu 2.1.18.

Pentru orice două grupuri G și H funcțiile 1_G și

$e: G \to H$, $e(x) = 1$ sunt un izomorfism, respectiv un homomorfism de grupuri.

<u>Lemă</u> 2.1.19.

Dacă $f: G \to H$ este un homomorfism de grupuri atunci:

(a) $f(1) = 1$

(b) $f(x^{-1}) = f(x)^{-1}$

<u>Lemă</u> 1.2.20.

Compunerea a două homomorfisme este de asemenea un homomorfism. Funcția inversă a unui izomorfism de grupuri este de asemenea un izomorfism.

<u>Definiție</u> 2 1.21.

Fie $f: G \to H$ un homomorfism. Numim nucleul respectiv imaginea lui f mulțimile:

$$\text{Ker} f = \{x \in G \mid f(x) = 1_H\}$$

Fie $f : \mathbb{Z} \to \mathbb{Z}_6$, definit prin:

$f(n) = n \bmod 6$

unde $\mathbb{Z}$ este grupul numerelor întregi sub adunare, iar $\mathbb{Z}_6$ este grupul numerelor modulo 6 sub adunare.

1. f **este un homomorfism**:

$f(a+b) = (a+b) \bmod 6 = f(a) + f(b)$

2. Nucleul funcției f:

$\ker(f) = \{n \in \mathbb{Z} \mid f(n) = 0\} = \{n \in \mathbb{Z} \mid n \bmod 6 = 0\}$

Rezultă că:

$\ker(f) = 6\mathbb{Z} = \{0, \pm 6, \pm 12, \pm 18, \ldots\}$

Propoziție 2.1.22.

Dacă $f: G \to H$ este un homomorfism, atunci:

a) $\operatorname{Ker} f \leq G$

b) $\operatorname{Im} f \leq H$

(c) f este injectiv dacă $\operatorname{Ker} f = \{e_H\}$

(d) f este surjectiv dacă $\operatorname{Im} f = H$

Grupuri ciclice și ordinul unui element

Definiție 2.1.23.

Un grup ciclic este un grup în care toate elementele sale pot fi obținute prin ridicarea la putere a unui singur element.

Definiție 2.1.24.

Fie $(G, \cdot)$ un grup și $x \in G$. Se spune că x este de ordin finit dacă există $n \in \mathbb{N}^*$ a.î. $x^n = e$ sau $x \cdot n = e, (G,+)$. În acest caz se numește ordinul lui x cel mai mic număr natural $n \in \mathbb{N}^*$ cu această proprietate; scriem $n = \operatorname{ord}(x)$. Elementul x este de ordin infinit dacă el nu este de ordin finit, caz în care scriem $\text{ord}(x) = \infty$.

Exemplu 2.1.25.

(1) În orice grup $(G, \cdot)$ există un singur element de ordin 1, anume elementul neutru $\text{ord}(1) = 1$

(2) În $(\mathbb{Z}, +)$ avem $\text{ord}(x) = \infty \quad \forall\, x \neq 0$

(3) În $(\mathbb{R}^*, \cdot)$ avem $\text{ord}(-1) = 2$ și $\text{ord}(x) = \infty, \forall\, x \in \mathbb{R}^* / \{1, -1\}$

(4) În $(\mathbb{C}^*, \cdot)$ avem $\text{ord}(i) = \text{ord}(-i) = 4$

Propoziție 2.1.26.

Fie $(G, \cdot)$ un grup, $x \in G$, $n \in \mathbb{N}^*$. Avem:

$$\text{ord}(x) = n \text{ ddacă } \begin{cases} x^n = 1 \\ \text{dacă } m \in \mathbb{Z} \text{ are proprietatea } x^m = 1,\ n \mid m \end{cases}$$

Propoziției 2.1.27.

Fie $(G, +)$ un grup. Pentru orice $x \in G$ avem $\text{ord}(x) = \text{card}\langle x \rangle$

$\langle 1 \rangle = \{0, 1, 2, 3, 4, 5\}$ (întreg grupul, 1 este generator).

$\langle 2 \rangle = \{0, 2, 4\}$. 2

$\langle 3 \rangle = \{0, 3\}$.

$(\mathbb{Z}_6, +)$,
element neutru $= 0$

$\text{ord}(x) = x \cdot n = 0$

Acțiuni ale grupurilor pe mulțimi

Definiție 2.1.28.

Fie A o mulțime și $(G,*)$ un grup. Se numește acțiune (la stânga) a lui G pe A o funcție $\alpha : G \times A \to A$ cu proprietățile:

(1) $\alpha(g, \alpha(h,x)) = \alpha(g*h, x)$ $\forall\ g,h \in G$ și $\forall\ x \in A$

(2) $\alpha(e, x) = x$ pentru orice $x \in A$

Observație 2.1.29.