3. Subgrupuri (18 martie 2019)

3.1. **Definiţie, caracterizare şi exemple.**

Definiţia 3.1. Fie G un grup. O submulţime $H \subseteq G$ este un *subgrup* al lui G dacă

(i) pentru orice $x, y \in H$ avem $xy \in H$ (spunem că H este *parte stabilă* a lui G în raport cu $\cdot$) şi
(ii) H împreună cu restricţia operaţiei $\cdot_{|H}$ formează un grup.

Notaţia 3.2. Notăm cu $H \leq G$ faptul că H este subgrup al lui G.

Exemplul 3.3. a) Dacă $(G, \cdot)$ este un grup, atunci $\{1\}$ şi G sunt subgrupuri în G (numite *subgrupuri triviale*).
b) $\mathbb{N}$ este parte stabilă în $(\mathbb{Z}, +)$, dar **nu** este subgrup.
c) Relativ la operaţia $+$ avem: $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.
d) Relativ la operaţia $\cdot$ avem: $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$.
e) In $D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ avem:

- $\{1, r, r^2, r^3\}$, $\{1, s\}$, $\{1, s, r^2, sr^2\}$ sunt subgrupuri în D_4;
- $\{1, sr, sr^2, sr^3\}$ nu este subgrup in D_4 (nu este parte stabilă).

Teorema 3.4. *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 3.5. Condiţia $1 \in H$ poate fi înlocuită cu $H \neq \varnothing$.

Exerţiul 3.6. Scrieţi enunţul teoremei pentru notaţia aditivă.

Exemplul 3.7. Dacă $n \in \mathbb{N}$, atunci $n\mathbb{Z}$ este subgrup în $(\mathbb{Z}, +)$;

Observaţia 3.8. Relaţia de a fi subgrup este tranzitivă:

$$H \leq K \text{ şi } K \leq G \Rightarrow H \leq G.$$

3.2. **Subgrupuri şi morfisme.**

Propoziţia 3.9. *Fie $f : G \to K$ un morfism de grupuri.*
(1) *Dacă $H \leq G$, atunci $f(H) \leq K$.*
(2) *Dacă $L \leq K$, atunci $f^{-1}(L) \leq G$*

Demonstraţie.

$\square$

Corolarul 3.10. *Dacă $f : G \to K$ este un morfism de grupuri, atunci:*
(a) *$f(G) \leq K$;*
(b) *$\mathrm{Ker}(f) = \{g \in G \mid f(g) = 1_K\} \leq G$.*

Definiţia 3.11. Dacă $f : G \to K$ este un morfism de grupuri, atunci
(a) $f(G)$ se numeşte *imaginea* lui f;
(b) $\mathrm{Ker}(f)$ se numeşte *nucleul* lui f.

Este evident că morfismul f este surjectiv ddacă $f(G) = K$. Morfismele injective pot fi caracterizate cu ajutorul nucleului astfel:

Propoziţia 3.12. *Dacă $f : G \to K$ este un morfism de grupuri, atunci următoarele afirmaţii sunt echivalente:*

(a) *funcţia f este injectivă;*
(b) $\mathrm{Ker}(f) = \{1_G\}$.

Demonstraţie.

$\square$

3.3. **Subgrup generat.**

Teorema 3.13. *Intersecţia unei familii de subgrupuri este subgrup.*

Demonstraţie.

$\square$

Corolarul 3.14. *Dacă G este un grup şi $H_1, H_2 \leq G$, atunci $H_1 \cap H_2 \leq G$.*

Observaţia 3.15. In general reuniunea a două sau mai multe subgrupuri nu este subgrup. De exemplu, $2\mathbb{Z}, 3\mathbb{Z} \leq (\mathbb{Z}, +)$, dar $2\mathbb{Z} \cup 3\mathbb{Z}$ nu este subgrup în $\mathbb{Z}$ (nu este parte stabilă).

Definiţia 3.16. Fie G un grup şi $X \subseteq G$. Subgrupul

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

se numeşte *subgrupul generat* de X.

Observaţia 3.17. 1. Subgrupul $\langle X\rangle$ este cel mai mic subgrup care conţine mulţimea X, adică

$$\langle X\rangle = K \Leftrightarrow \begin{cases} \text{i) } K \leq G; \\ \text{ii) } X \subseteq K; \\ \text{iii) } S \leq G \text{ şi } X \leq S \Rightarrow K \leq S. \end{cases}$$

2. $\langle\varnothing\rangle = \{1\}$.

Propoziţia 3.18. *Fie G un grup şi $\varnothing \neq X \subseteq G$. Atunci*

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

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

Demonstraţie.

$\square$

Notaţia 3.19. Dacă $X = \{x_1,\ldots,x_n\}$, atunci $\langle X\rangle = \langle x_1,\ldots,x_n\rangle$.

Observaţia 3.20. 1) Produsele $x_1 \cdot \ldots \cdot x_n$ pot fi înlocuite cu produse de forma $y_1^{k_1} \cdot \ldots \cdot y_m^{k_m}$ cu $k_1,\ldots,k_m \in \mathbb{Z}$.

2) Dacă grupul G este abelian, atunci în expresia $y_1^{k_1} \cdot \ldots \cdot y_m^{k_m}$ putem presupune că elementele $y_1,\ldots,y_m$ sunt diferite două câte două.

Exemplul 3.21. 1) In grupul simetric S_n considerăm

$$X = \{\tau \in S_n \mid \tau \text{ este o transpoziţie}\}$$

şi

$$Y = \{\rho \in S_n \mid \rho \text{ este un ciclu de lungime } 3\}.$$

Atunci

a) $\langle X \rangle = S_n$;
b) $\langle Y \rangle = A_n$, unde $A_n = \{\sigma \in S_n \mid \sigma \text{ este pară}\}$.

a)

b) Incluziunea $\langle Y \rangle \subseteq A_n$ este evidentă.

Orice permutare pară este produsul unui număr par de transpoziţii. Orice produs de două transpoziţii diferite este produs de cicluri de lungime 3:

- dacă $i \neq j \neq k \neq i$, atunci $(i,j)(j,k) = (i,k,j)^2$;
- dacă i,j,k,ℓ sunt două câte două diferite, atunci $(i,j)(k,\ell) = (i,k,j)(i,k,\ell)$.

Definiţia 3.22. Grupul A_n se numeşte *grupul altern* de grad n.

2) In $(\mathbb{Q},+)$ luăm $X = \{\frac{1}{p} \mid p \text{ este prim}\}$. Atunci

$$\langle X \rangle = \{\frac{a}{b} \mid b \text{ este liber de pătrate}\}.$$