4. Grupuri şi subgrupuri ciclice (25 martie 2019)

Definiţia 4.1. Fie G un grup şi $g \in G$. Subgrupul $\langle g \rangle$ s.n. *subgrupul ciclic* generat de G.

Grupul G este *ciclic* dacă exită $g \in G$ a.î. $G = \langle g \rangle$.

Observaţia 4.2. 1. Dacă $(G, \cdot)$ este un grup şi $g \in G$, atunci

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

2. Dacă $(G, +)$ este un grup şi $g \in G$, atunci $\langle g \rangle = \{kg \mid k \in \mathbb{Z}\}$.

Observaţia 4.3. Orice grup ciclic este comutativ.

Exemplul 4.4. 1) $\mathbb{Z}$

2) $\mathbb{Q}$

3) $(\mathbb{Z}_n, +)$

4) Dacă p este prim impar şi $k \in \mathbb{N}^*$ atunci $(U(\mathbb{Z}_n), \cdot)$ este ciclic.

5) $(U(\mathbb{Z}_8), \cdot)$ nu este ciclic.

6) Grupul lui Klein nu este ciclic.

8) Dacă $n \in \mathbb{N}^*$, atunci grupul

$$U_n = \{z \in \mathbb{C} \mid z^n = 1\}$$

este ciclic, generat de $z_1 = \cos \frac{2\pi}{n} + \mathrm{i} \sin \frac{2\pi}{n}$.

Lema 4.5. *Fie $(G, \cdot)$ un grup şi $g \in G$. Atunci:*

(a) *dacă $\operatorname{ord}(g) = n$ şi $k \in \mathbb{Z}$ are proprietatea $g^k = 1$, atunci $n \mid k$;*

(b) *dacă $\operatorname{ord}(g) = n$ şi $k, m \in \mathbb{Z}$, atunci are loc echivalenţa*

$$g^k = g^m \Leftrightarrow n \mid m - k.$$

(c) *dacă $\operatorname{ord}(g) = \infty$ şi $k, m \in \mathbb{Z}$, atunci are loc echivalenţa*

$$g^k = g^m \Leftrightarrow m = k.$$

Propoziţia 4.6. *Dacă G este un grup şi $g \in G$, atunci* $\operatorname{ord}(g) = |\langle g \rangle|$, *unde $|X|$ reprezintă cardinalul mulţimii X. Mai mult,*

(a) *dacă* $\operatorname{ord}(g) = n$, *atunci* $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$*;*
(b) *dacă* $\operatorname{ord}(g) = \infty$, *atunci* $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$*.*

Demonstraţie.

□

Teorema 4.7. *Orice două grupuri ciclice de acelaşi cardinal sunt izomorfe.*

Demonstraţie.

□

Teorema 4.8. ***(Subgrupurile unui grup ciclic)*** *Fie $(G, \cdot)$ un grup ciclic, $G = \langle x \rangle$ şi $H \subseteq G$.*

(a) *$H \leq G$ dacă şi numai dacă există $d \in \mathbb{N}$ astfel încât $H = \langle x^d \rangle$.*
(b) *Dacă G este infinit şi $d, e \in \mathbb{N}$ cu $d \neq e$ atunci $\langle x^d \rangle \neq \langle x^e \rangle$.*
(c) *Dacă $|G| = n$ atunci pentru orice subgrup $H \leq G$ există $d \mid n$ astfel încât $H = \langle x^d \rangle$. Mai mult, din $d, e \mid n$ cu $d \neq e$, rezultă $\langle x^d \rangle \neq \langle x^e \rangle$.*

Demonstraţie.

$\square$

Exemplul 4.9. 1) Subgrupurile lui $\mathbb{Z}$;

2) Subgrupurile lui $\mathbb{Z}_n$;

3) Subgrupurile lui $\mathbb{Z}_{12}$.

Exerciţiul 4.10. Fie $(G, \cdot)$ un grup, $x \in G$ şi $d, e \in \mathbb{N}$. Demonstraţi că:
(1) Dacă $\mathrm{ord}(X) = \infty$, avem

$$\langle x^d \rangle \subseteq \langle x^e \rangle \Leftrightarrow e \mid d.$$

(2) Dacă $\mathrm{ord}(x) = n \in \mathbb{N}^*$ şi $d, e \mid n$, atunci

$$\langle x^d \rangle \subseteq \langle x^e \rangle \Leftrightarrow e \mid d.$$