Curs VIII
ELEMENTE DE TEORIA GRUPURILOR

§ 7. GRUPURI CICLICE

Am observat anterior că grupurile aditive **Z** şi $\mathbf{Z}_n$, $n \geq 1$, sunt ciclice. Următoarea teoremă arată că acestea sunt singurele tipuri de grupuri ciclice.

Teorema 7.1. (Teorema de structură a grupurilor ciclice) Orice grup ciclic G este izomorf fie cu grupul **Z** al numerelor întregi, fie cu un anumit grup $\mathbf{Z}_n$, $n \geq 1$, de clase de resturi modulo n.

Demonstraţie. Dacă G = <a>, considerăm funcţia φ: $\mathbf{Z} \to G$, $\varphi(n) = a^n$, definită mai înainte. Avem

$$\varphi(m + n) = a^{m+n} = a^m a^n = \varphi(m)\varphi(n)$$

şi deci φ este morfism de grupuri. Mai mult, φ este evident morfism surjectiv, deci Im φ = G. Considerând nucleul lui φ, Ker φ, distingem două cazuri:

1) Ker $\varphi = \{0\}$;

2) Ker $\varphi \neq \{0\}$.

În primul caz, conform teoremei fundamentale de izomorfism, avem

$$\mathbf{Z}/\{0\} \cong \text{Im } \varphi, \text{ adică } \mathbf{Z} \cong G;$$

În cazul al doilea, Ker φ este de forma $n\mathbf{Z}$ cu $n \geq 1$ un număr întreg şi deci

$$\mathbf{Z}/n\mathbf{Z} \cong \text{Im } \varphi, \text{ adică } \mathbf{Z}_n \cong G.$$

Observaţie. Din teorema de mai înainte rezultă că dacă G este un grup ciclic şi *a* un generator al său, atunci:

1) Dacă *a* este de ordin infinit, atunci G este izomorf cu grupul aditiv **Z** al numerelor întregi.

2) Dacă *a* este de ordin n (finit), atunci G este izomorf cu grupul aditiv $\mathbf{Z}_n$ al claselor de resturi modulo n.

Propoziţia 7.2. Orice subgrup şi orice grup factor al unui grup ciclic este ciclic.

Demonstraţie. Dacă G = <a> este un grup ciclic, iar H un subgrup al său, atunci grupul factor G/H este ciclic generat de [a], clasa lui a modulo H, adică G/H = <[a]>.

Să arătăm acum că orice subgrup al unui grup ciclic este ciclic. Într-adevăr, dacă G este izomorf cu **Z**, am arătat că subgrupurile lui **Z** sunt de forma $n\mathbf{Z}$, adică sunt ciclice; deci şi subgrupurile lui G sunt ciclice.

Fie G un grup ciclic finit al cărui generator *a* este de ordin n şi fie H un subgrup al său. Dacă H = {e}, atunci, evident, H este ciclic generat de elementul e. Dacă $H \neq \{e\}$, atunci există $x \in H$, $x \neq e$. Dar cum $x \in G$, avem că $x = a^k$ cu $k \neq 0$. De asemenea, $x^{-1} \in H$, adică $a^{-k} \in H$, deci există $r \geq 1$ astfel încât $a^r \in H$. Mulţimea de numere naturale $M = \{n \mid a^n \in H, n > 0\}$ este nevidă şi cum **N** este bine ordonată, M are un cel mai mic

element m. Vom arăta că $H = \langle a^m \rangle$, adică H este ciclic generat de a^m. Fie $x \in \langle a^m \rangle$; atunci $x = (a^m)^k$, $k \in \mathbf{Z}$ şi cum H este subgrup, iar $a^m \in H$ rezultă că $x \in H$. Reciproc, dacă $y \in H$, atunci $y \in G$, adică $y = a^t$ cu $t \in \mathbf{Z}$. Din teorema împărţirii cu rest pentru numere întregi, $t = mq + r$ cu $q, r \in \mathbf{Z}$ iar $0 \leq r < m$ şi deci $y = a^t = a^{mq+r} = a^{mq} a^r = (a^m)^q a^r$, de unde $a^r = (a^m)^{-q} y$. Deci $a^r \in H$ şi cum m este cel mai mic element al lui M, rezultă $r = 0$ şi deci $t = mq$. Aşadar $y = a^{mq} = (a^m)^q = \langle a^m \rangle$.

Observaţie. Dacă $G = \langle a \rangle$ este un grup ciclic de ordin n, din teorema precedentă rezultă că izomorfismul dintre G şi grupul aditiv $\mathbf{Z}_n$ este dat de funcţia $\varphi : \mathbf{Z}_n \to G$, definită prin $\varphi([k]) = a^k$. Aşadar, având în vedere caracterizarea generatorilor grupului aditiv $\mathbf{Z}_n$ dată în secţiunea 2, avem că elementul a^k este generator al lui G dacă şi numai dacă k este prim cu n.

Fie acum $n \geq 1$ un număr natural şi U_n grupul multiplicativ al rădăcinilor de ordinul n ale unităţii, adică

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

Avem că $U_n = \{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}\}$, unde

$$\varepsilon_k = \cos(2k\pi/n) + i \sin(2k\pi/n), \quad 0 \leq k \leq n - 1.$$

Din formula lui Moivre avem că $\varepsilon_k = \varepsilon_1^k$ şi deci U_n este grup ciclic de ordinul n, un generator al său fiind ε_1.

Definiţia 7.3. Un generator al grupului U_n se numeşte *rădăcină primitivă de ordinul n a unităţii*.

Conform celor de mai înainte rezultă că ε_k este rădăcină primitivă de ordinul n a unităţii dacă şi numai dacă k este relativ prim cu n.

Exerciţiu. Arătaţi că grupurile $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$ şi $(\mathbf{C}, +)$ nu sunt ciclice.

§ 8. GRUPUL DIEDRAL D_4. GRUPUL CUATERNIONILOR.

Exerciţiu. Daţi un exemplu de grup G care are două subgrupuri H, K cu proprietatea că $H \lhd K$ şi $K \lhd G$, dar H nu este normal în G.