

---

## Лекция №2

---

### 1.3 Циклические группы

#### 1.3.1 Свойства циклических групп

Напомним, что циклическая группа имеет вид  $G = \langle a \rangle = \{a^n | n \in \mathbb{Z}\}$ , где  $a$  – ее образующий элемент.

**Теорема 1.** Пусть  $G$  – группа,  $a \in G$  – элемент этой группы. Тогда

1. Если  $\text{ord } a \geq \infty$ , то  $a^i = a^j \Leftrightarrow i = j$  ( $G$  – бесконечная).
2. Если  $\text{ord } a = n < \infty$ , то  $\langle a \rangle = \{a, a^2, \dots, a^{n-1}, a^n = e\}$ ,  $a^i = a^j \Leftrightarrow n | (i - j)$ .

**Следствие 1.**  $\text{ord } a = |\langle a \rangle|$ .

**Следствие 2.** Пусть  $G$  – группа,  $a \in G$  и  $\text{ord } a = n$ . Если  $a^k = e$ , то  $n | k$ . При этом  $k$  называется показателем элемента  $a$ .

**Теорема 2.** Пусть  $\text{ord } a = n$  и  $k$  – положительное целое. Тогда  $\langle a^k \rangle = \langle a^{(n,k)} \rangle$  и  $\text{ord } a^k = \frac{n}{\text{НОД}(n,k)}$ .

**Следствие 3.** В конечной циклической группе порядок элементов делит порядок группы.

**Следствие 4.** Пусть  $\text{ord } a = n$ . Тогда  $\langle a^i \rangle = \langle a^j \rangle \Leftrightarrow \text{НОД}(n, i) = \text{НОД}(n, j)$  и  $\text{ord } a^i = \text{ord } a^j \Leftrightarrow \text{НОД}(n, i) = \text{НОД}(n, j)$ .

**Следствие 5.** Пусть  $\text{ord } a = n$ . Тогда  $\langle a \rangle = \langle a^j \rangle \Leftrightarrow \text{НОД}(n, j) = 1$  и  $\text{ord } a = \text{ord } a^j \Leftrightarrow \text{НОД}(n, j) = 1$ .

**Следствие 6.** Целое  $k$  в  $\mathbb{Z}_n$  – образующий элемент в  $\mathbb{Z}_n \Leftrightarrow \text{НОД}(n, k) = 1$ .

#### 1.3.2 Классификация подгрупп циклических групп

**Теорема 3.**  $\forall$  подгруппа циклической группы является циклической. Кроме того, если  $|\langle a \rangle| = n$ , то порядок подгруппы  $\langle a \rangle$  делит  $n$ . Для каждого положительного  $k | n$  группа  $\langle a \rangle$  имеет в точности одну подгруппу  $\langle a^{\frac{n}{k}} \rangle$  порядка  $k$ .

**Следствие 7.** Для  $\forall k | n$  множество  $\langle \frac{n}{k} \rangle$  – ! подгруппа в  $\mathbb{Z}_n$  порядка  $k$ .

**Определение 1.**  $\phi(n)$  – функция Эйлера – количество чисел, взаимнопростых с  $n$ .

**Теорема 4.** Пусть  $d | n$ . Тогда число элементов порядка  $d$  в циклической группе порядка  $n$  равно  $\phi(d)$ .