
Лекция №3 (15.09.20)

1.3 Циклические группы

1.3.1 Свойства циклических групп

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

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

1. *Если $\operatorname{ord} a \geq \infty$, то $a^i = a^j \Leftrightarrow i = j$ (G - бесконечная).*
2. *Если $\operatorname{ord} a = n < \infty$, то $< a >= \{a, a^2, ..., a^{n-1}, a^n = e\}$, $a^i = a^j \Leftrightarrow n|(i-j)$.*

Следствие 1. $\operatorname{ord} a = | < a > |$.

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

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

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

Следствие 4. *Пусть $\operatorname{ord} a = n$*
Тогда $< a^i >=< a^j > \Leftrightarrow НОД(n,i) = НОД(n,j)$ и $\operatorname{ord} a^i = \operatorname{ord} a^j \Leftrightarrow НОД(n,i) = НОД(n,j)$.

Следствие 5. *Пусть $\operatorname{ord} a = n$. Тогда $< a >=< a^j > \Leftrightarrow НОД(n,j) = 1$ и $\operatorname{ord} a = \operatorname{ord} a^j \Leftrightarrow НОД(n,j) = 1$.*

Следствие 6. *Целое k в $\mathbb{Z}_n$ – образующий элемент в $\mathbb{Z}_n^* \Leftrightarrow НОД(n,k) = 1$. Другими словами, $(U(n) =< k > \Leftrightarrow (n,k) = 1)$.*

1.3.2 Классификация подгрупп циклических групп

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

Следствие 7. *Для $\forall k|n$ множество $< \frac{n}{k} >$ - ! 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 $\phi(d)$.*