3. Циклические группы (начало)

Определение. Группа G называется *циклической*, если в ней существует *порождающий элемент*, то есть такой элемент $d \in G$, что $G = \langle d \rangle$.

Если операции в группе G записываются мультипликативно, то $\langle d \rangle = \{d^a \mid a \in \mathbb{Z}\}$, поэтому условие $G = \langle d \rangle$ означает, что циклическая группа G — *группа степеней порождающего элемента*.

Если операции в группе G записываются аддитивно, то $\langle d \rangle = \{ad \mid a \in \mathbb{Z}\}$, поэтому условие $G = \langle d \rangle$ означает, что циклическая группа G — *группа кратных порождающего элемента*.

Так как степени элемента коммутируют между собой (ясно, что $\forall\, a, b \in \mathbb{Z}\ (d^a d^b = d^{a+b} = d^b d^a)$), циклические группы являются абелевыми группами.

• Для любого $n \in \mathbb{N}$ группа $(\mathbb{Z}/n)^+$ циклическая, так как $(\mathbb{Z}/n)^+ = \langle 1 \rangle$ (это очевидно).

• Группа $\mathbb{Z}^+$ циклическая, так как $\mathbb{Z}^+ = \langle 1 \rangle$ (это очевидно).

• Для любого $n \in \mathbb{N}$ группа μ_n циклическая, так как $\mu_n = \langle \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}} \rangle$ (это очевидно).

• Группа $(\mathbb{Z}/5)^\times$ циклическая, так как $(\mathbb{Z}/5)^\times = \langle 2 \rangle$ (проверим это: $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 3$, — вычисляя степени элемента 2 в группе $(\mathbb{Z}/5)^\times$, мы получаем все элементы этой группы).

• Группа $(\mathbb{Z}/7)^\times$ циклическая, так как $(\mathbb{Z}/7)^\times = \langle 3 \rangle$ (проверим это: $3^0 = 1$, $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$ и $3^5 = 5$, — вычисляя степени элемента 3 в группе $(\mathbb{Z}/7)^\times$, мы получаем все элементы этой группы).

• Группа $\mathbb{Q}^+$ абелева, но не циклическая, так как $\forall\, q \in \mathbb{Q}^+\ (\langle q \rangle = q\mathbb{Z} < \mathbb{Q}^+)$.

• Группа D_2 абелева, но не циклическая, так как $\forall\, u \in \mathrm{D}_2\ (\langle u \rangle = \{\mathrm{id}_4, u\} < \mathrm{D}_2)$. (Через D_2 обозначена подгруппа $\{\mathrm{id}_4, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$ группы S_4.)

• Группы S_n и D_n, где $n \in \mathbb{N} \setminus \{1, 2\}$, неабелевы и, значит, нециклические.

В циклической группе может быть несколько порождающих элементов. Например, все порождающие элементы группы $\mathbb{Z}^+$ суть 1 и -1, группы $(\mathbb{Z}/3)^+$ — 1 и 2, группы $(\mathbb{Z}/4)^+$ — 1 и 3, группы $(\mathbb{Z}/5)^+$ — 1, 2, 3 и 4, группы $(\mathbb{Z}/5)^\times$ — 2 и 3 (убедитесь в справедливости этих утверждений). В вопросе 8 курса для любого $n \in \mathbb{N}$ будет дано явное описание всех порождающих элементов группы $(\mathbb{Z}/n)^+$.

Для разных $n \in \mathbb{N}$ группы $(\mathbb{Z}/n)^\times$ могут быть циклическими или нециклическими; если группа $(\mathbb{Z}/n)^\times$ циклическая, то вычисления в этой группе можно проводить эффективно в том смысле, что умножение ее элементов, то есть умножение чисел по модулю n, сводится к сложению степеней порождающего элемента этой группы. В вопросе 9 курса будет дан общий критерий, позволяющий для любого $n \in \mathbb{N}$ определить, является ли группа $(\mathbb{Z}/n)^\times$ циклической. Небольшие значения n, для которых группа $(\mathbb{Z}/n)^\times$ является циклической, перечислены на странице `http://oeis.org/A033948`.

Определение. Число $d \in (\mathbb{Z}/n)^\times$, где $n \in \mathbb{N}$, называется *первообразным корнем по модулю* n, если d — порождающий элемент группы $(\mathbb{Z}/n)^\times$, то есть $(\mathbb{Z}/n)^\times = \langle d \rangle$.

Первообразные корни по модулю n имеют большое значение в криптографии (подробности читайте в статье `http://en.wikipedia.org/wiki/Primitive_root_modulo_n`). Для небольших n значения наименьшего первообразного корня по модулю n имеются на странице `http://oeis.org/A046145`.

Ясно, что для любого $n \in \mathbb{N}$ отображение, действующее из $(\mathbb{Z}/n)^+$ в μ_n по правилу $a \mapsto \mathrm{e}^{\frac{2\pi \mathrm{i} a}{n}}$ для любых $a \in (\mathbb{Z}/n)^+$, — изоморфизм групп и, значит, $\mu_n \cong (\mathbb{Z}/n)^+$. Аналогичный факт имеет место для любой циклической группы и доказан в следующей теореме. Она утверждает, что с точностью до изоморфизма все циклические группы и только они суть группы $(\mathbb{Z}/n)^+$, где $n \in \mathbb{N}$, и группа $\mathbb{Z}^+$.

Теорема об описании циклических групп.

1. Пусть G — группа, и $n \in \mathbb{N}$ и $G \cong (\mathbb{Z}/n)^+$, или $n = \infty$ и $G \cong \mathbb{Z}^+$; тогда группа G циклическая и $|G| = n$.

2. Пусть G — циклическая группа; обозначим через n величину $|G|$; тогда $n \in \mathbb{N}$ и $G \cong (\mathbb{Z}/n)^+$, или $n = \infty$ и $G \cong \mathbb{Z}^+$.

Доказательство. 1. Если $n \in \mathbb{N}$, то обозначим через d прообраз элемента 1 группы $(\mathbb{Z}/n)^+$ относительно изоморфизма между G и $(\mathbb{Z}/n)^+$; очевидно, что $G = \langle d \rangle$. Если $n = \infty$, то обозначим через d прообраз элемента 1 группы $\mathbb{Z}^+$ относительно изоморфизма между G и $\mathbb{Z}^+$; очевидно, что $G = \langle d \rangle$.

2. Пусть $d \in G$ и $G = \langle d \rangle$; в силу леммы о порядке элемента (вопрос 2 курса) $\mathrm{ord}(d) = |\langle d \rangle|$, но $|G| = n$ и, значит, $\mathrm{ord}(d) = n$. Если $n \in \mathbb{N}$, то обозначим через $\exp_d$ отображение, действующее из $(\mathbb{Z}/n)^+$ в G по правилу $a \mapsto d^a$ для любых $a \in (\mathbb{Z}/n)^+$. Если $n = \infty$, то обозначим через $\exp_d$ отображение, действующее из $\mathbb{Z}^+$ в G по правилу $a \mapsto d^a$ для любых $a \in \mathbb{Z}^+$. Из подлеммы, доказанной внутри доказательства леммы о порядке элемента, следует, что $\exp_d$ — мономорфизм, а так как $G = \langle d \rangle$, $\exp_d$ — изоморфизм. □