1 Лекция 1.04

Определение 1. *Множество с бинарной операцией $\circ$ — множество M с заданным отображением $M \times M \to M$, такое что $(a, b) \to a \circ b$.*

Определение 2. *$(M, \circ)$ называется полугруппой, если операция ассоциативна, то есть $(a \circ b) \circ c = a \circ (b \circ c)$.*

Полугруппа обозначается как $(S, \circ)$.

Определение 3. *Полугруппа $(S, \circ)$ называется моноидом, если в ней существует нейтральный элемент e ($e \in S$), то есть такой, что $\forall s \in S : e \circ s = s \circ e = s$.*

Пример. $(\mathbb{N}, +)$ — не моноид, $(\mathbb{Z}_{\geq 0}, +)$ — моноид.

Лемма 1. *Нейтральный элемент единствен.*

Доказательство. Пусть их хотя бы 2. Обозначим их за e_1 и e_2 соответственно. Тогда:

$$e_1 \circ e_2 = e_1 = e_2$$

□

Определение 4. *Моноид $(S, \circ)$ называется группой, если все его элементы обратимы, то есть $\forall a \in S \; \exists b \in S : a \circ b = b \circ a = e$. Тогда говорят, что b обратен a. Обозначается как $b = a^{-1}$.*

Лемма 2. *Обратный элемент, если он существует, единственен.*

Определение 5. *Группа $(G, \circ)$ называется коммутативной (или абелевой), если $\forall a, b \in G : a \circ b = b \circ a$.*

Обозначения

- Произвольные группы (мультипликативные) обозначаем как $(G, \circ)$.
- Коммутативные группы обозначаем как $(A, +)$.

Определение 6. *Порядок группы G — число элементов в ней. Обозначается как $|G|$.*

Примеры групп

1. Числовые аддитивные: $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Z}_n, +)$.
2. Числовые мультипликативные: $(\mathbb{Q} \setminus \{0\}, \times), (\mathbb{R} \setminus \{0\}, \times), (\mathbb{C} \setminus \{0\}, \times), (\mathbb{Z}_p \setminus \{0\}, \times), (\mathbb{Z}_n^*, \times)$.
3. Группы матриц (по умножению):
   (a) $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}$
   (b) $SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A = 1\}$
4. Группы подстановок S_n. Также есть группа четных перестановок $A_n = \{\sigma \in S_n \mid \sigma \text{ четна}\}$. Нетрудно видеть, что $|A_n| = \frac{n!}{2}$. A_n также называют знакопеременной.

Упражнение. S_n – коммутативна $\Leftrightarrow n \leq 2$.

Упражнение. A_n – коммутативна $\Leftrightarrow n \leq 3$.

Определение 7. *Подмножество $H \subseteq G$, где G — группа, называется подгруппой, если $H \neq \emptyset$ и $\forall a, b \in H : ab^{-1} \in H$.*

Нетрудно видеть, что это определение эквивалентно:

1. $e \in H$
2. $\forall a, b \in H : ab \in H$
3. $\forall a \in H : a^{-1} \in H$

В любой группе есть 2 несобственные подгруппы: $H_1 = \{e\}, H_2 = G$.

Пример. $G = (\mathbb{Z}, +), H = 2\mathbb{Z}$.

Утверждение 1. *Всякая подгруппа в $(\mathbb{Z}, +)$ имеет вид $k\mathbb{Z}$, где $k \in \mathbb{Z}_+$.*

Доказательство. Ясно, что $k\mathbb{Z}$ — подгруппа. Пусть H — подгруппа. Если $H = \{0\}$, то $k = 0$. Иначе пусть k – наименьшее натуральное число в H. Тогда $k\mathbb{Z} \subseteq H$. Теперь в обратную сторону, возьмем $a \in H$. Представим $a = kq + r$, где $q \in \mathbb{Z}, 0 \leq r \leq k - 1$. Тогда $r = a - kq \in H$, но так как k – минимальное натуральное, $r = 0$. □

Определение 8. *Пусть G — группа и $g \in G$. Тогда циклическая подгруппа в G, порожденная элементом g, это подгруппа $H = \langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$. Элемент g называется порождающим (или образующим).*

Пример. $2\mathbb{Z} \subseteq \mathbb{Z}$, причем $2\mathbb{Z} = \langle 2 \rangle = \langle -2 \rangle$.

Определение 9. *Пусть G — группа и $g \in G$. Тогда порядком элемента g называется наименьшее натуральное s, такое что $g^s = e$. Если такого s не существует, то порядок равен ∞. Обозначается как* $\mathrm{ord}(g)$.

Утверждение 2. *Пусть G — группа и $g \in G$. Тогда* $\mathrm{ord}(g) = |\langle g \rangle|$.

Доказательство. Заметим, что $g^k = g^s$ тогда и только тогда, когда $g^{k-s} = e$. Поэтому если $\mathrm{ord}(g) = \infty$, то все g^m ($m \in \mathbb{Z}$) попарно различны. Следовательно $\mathrm{ord}(g) = |\langle g \rangle| = \infty$.

Теперь рассмотрим случай, когда $\mathrm{ord}(g) = m$. Тогда элементы $g^0, g^1, \ldots, g^{m-1}$ попарно различны. С другой стороны, $g^n = g^{mq+r} = (g^m)^q \cdot g^r = 1^q \cdot g^r = g^r$. Поэтому $|\langle g \rangle| = |\{g^0, g^1, \ldots, g^{m-1}\}| = m = \mathrm{ord}(g)$, что и требовалось. □

Определение 10. *Группа G называется циклической, если существует такой $g \in G$, что $G = \langle g \rangle$.*