Теория групп, ФПМИ МФТИ

Госткин Евгений Михайлович

Оглавление

1 Понятие группы. Примеры. Циклические группы и их подгруппы.

Определение 1.1. *Группа* - множество G с операцией $\cdot$ (умножения), обладающей следующими свойствами:

1. $\forall a, b, c \in G : (ab)c = a(bc)$ (ассоциативность);
2. $\exists e \in G \; \forall a \in G \; ae = ea = a$ (существование единицы);
3. $\forall a \in G \; \exists a^{-1} \in G : aa^{-1} = a^{-1}a = e$ (существование обратного элемента).

Определение 1.2. *Абелева группа* (коммутативная) - $\forall a, b \in G \; ab = ba$.

Определение 1.3. *Подгруппа* группы G - $H \subset G$:

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

Определение 1.4. *Группа преобразований* множества X - совокупность G его биективных преобразований, удовлетворяющая следующим условиям:

1. $\phi, \psi \in G \Rightarrow \phi \circ \psi \in G$;
2. $\phi \in G \Rightarrow \phi^{-1} \in G$;
3. $id \in G$ (тождественное).

Определение 1.5. Для любой группы G можно определить *степень* элемента $g \in G$ с целым показателем:

$$g^k = \begin{cases} \underbrace{gg\ldots g}_{k}, & k > 0 \\ e, & k = 0 \\ \underbrace{g^{-1}g^{-1}\ldots g^{-1}}_{k}, & k < 0. \end{cases}$$

Утверждение 1.1. $\forall g \in G \; \forall k, l \in \mathbb{Z} \; g^k g^l = g^{k+l}$

Доказательство. Рассмотрим различные случаи для k, l

1. $k, l > 0$ - очевидно
2. $k > 0, l < 0, k + l > 0$:

$$g^k g^l = \underbrace{gg\ldots g}_{k}\underbrace{g^{-1}g^{-1}\ldots g^{-1}}_{l} = \underbrace{gg\ldots g}_{k+l} = g^{k+l}.$$

Остальные случаи рассматриваются аналогично. □

Следствие 1.1. $(g^k)^{-1} = g^{-k}$.

Определение 1.6. $\langle g \rangle$ - *циклическая подгруппа, порожденная элементом* g - подгруппа степеней элемента $g \in G$ (является подгруппой из определения **??**, утверждения **??** и следствия **??**)

Определение 1.7. Минимальное $m \in \mathbb{N} : g^m = e$ - *порядок* элемента g, обозначается $\operatorname{ord} g$

Пример 1.1. $(\mathbb{Z}, +)$ - абелева группа по сложению

- $0 \in \mathbb{Z}$ - нейтральный элемент, т.к. $\forall a \in \mathbb{Z} a + 0 = 0 + a = a$
- $\forall a \in \mathbb{Z}\ \exists a^{-1} = -a : a + (-a) = (-a) + a = 0$

Пример 1.2. $(\mathbb{Q}^\times, \cdot)$ - абелева группа по умножению, где $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$

- $1 \in \mathbb{Q}^\times$ - нейтральный элемент, т.к. $\forall a \in \mathbb{Q}^\times\ a \cdot 1 = 1 \cdot a = a$
- $\forall a \in \mathbb{Q}^\times\ \exists a^{-1} = \frac{1}{a} : a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$

Пример 1.3. $GL_n(\mathbb{R})$[1] - группа невырожденных[2] матриц по умножению[3].

Пример 1.4. $SL_n[\mathbb{R}] \subset GL_n[\mathbb{R}] :=$ [4]$\forall A \in SL_n[\mathbb{R}]\ \det A = 1$

Пример 1.5. $(S_n, \circ)$[5] - группа перестановок элементов вида $\{1, \ldots, n\}$, рассматриваемых как функции $\{1, \ldots, n\} \to S_n$. $\circ$ - операция композиции функций. Является группой, т.к. есть тождественная перестановка и у каждой перестановки есть обратная. Также следует заметить, что S_n подходит под определение **??**, поэтому можно задать действие S_n на любом конечном множестве.

Пример 1.6. D_{2n} - группа Диэдра - группа симметрий правильного n-угольника $A_1, \ldots, A_n$, включающая поворот и отражение. Состоит из $2n$ элементов:

$$\{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\},$$

где r - поворот n-угольника на $\frac{2\pi}{n}$, а s - отражение относительно OA_1, где O - центр фигуры. Таким образом, rs - повернуть и отразить (читаем слева направо, как композиция функций). В частности, $r^n = s^2 = 1$ и $r^k s = sr^{-k}$.

Пример 1.7. $\{1\}$ - тривиальная группа.

[1] Название произошло от 'General linear group'.
[2] Для тех, кто не помнит: матрицы с ненулевым определителем.
[3] Из курса алгема: $\forall A : \det A \neq 0 \Rightarrow \exists A^{-1} : AA^{-1} = A^{-1}A = E$, где E - единичная, и $\det AB = \det A \cdot \det B$.
[4] Название от 'Special linear group'.
[5] Название от 'Symmetric group'.