GROUP THEORY

ФЁДОР АЛЕКСЕЕВ

Содержание

Часть 1. **Лекция 1. Группа, подгруппа. Изоморфизм групп.**

1. Группа

Определение. *Группа* — это множество G с определённой на нём бинарной операцией (т. е. $\forall a, b \in G$ определён результат операции $a \cdot b \in G$)

1. **Ассоциативность:** $\forall a, b, c \in G \to (a \cdot b) \cdot c = a \cdot (b \cdot c)$;
2. **Наличие нейтрального элемента:** $\exists e \in G : \forall a \in G \to a \cdot e = e \cdot a$;
3. **Наличие обратного элемента:** $\forall g \in G \to \exists g^{-1} \in G : g \cdot g^{-1} = g^{-1} \cdot g = e$.

Группа *абелева*(*коммутативная*), если $\forall a, b \in G \to a \cdot b = b \cdot a$.

Замечание. Произведение $g_1 \cdot g_2 \cdot \dots \cdot g_n$ также не зависит от порядка.

Утверждение 1. $\forall g \in G \to \exists! g^{-1}$.

Доказательство. Пусть a — левый обратный к g (т. е. $ag = e$), b — правый обратный к g (т. е. $gb = e$). Докажем, что $a = b$:

$$b = eb = (ag)b = a(gb) = ae = a$$

□

Упражнение 1. Условие 3 из определения можно заменить на $\forall g \in G \to \exists g^{-1}$ — правый обратный.

Пример 1. $(\mathbb{Z}, +)$

Пример 2. $(\mathbb{R}, +)$, и даже $(F, +)$.

Пример 3. $(\mathbb{R}\backslash\{0\}, 0)$, и даже $F^* = (F\backslash\{0\}, \cdot)$.

Замечание. Более общо, если R — кольцо, то $(R, +)$ и $(R^*, \cdot)$ — абелевы группы (R^* — множество обратимых элементов R). Хорошо бы доказать, впрочем, что если $a, b \in R^*$, то $ab \in R^*$:

$$ab(ab)^{-1} = abb^{-1}a^{-1} = aa^{-1} = e$$

Пример 4. $M_{n\times n}(F)$ — кольцо. $(M_{n\times n})^* = GL(F)$ — мультипликативная группа невырожденных матриц $n \times n$.

Пример 5. $(\mathbb{Z}_n, +)$ и $(\mathbb{Z}_n^*, \cdot)$, где $\mathbb{Z}_n^*$ — все взаимно простые с n.

Доказательство. Если $(a, n) \neq 1$, то $ka \not\equiv 1 \pmod n$. Если $(a, n) = 1$, то $\exists u, v : au + nv = a \Rightarrow au \equiv 1 \pmod n$ □

Значит $|\mathbb{Z}_n^*| = \varphi(n)$.

Определение. *Порядок группы* G — это количество её элементов $|G|$.

Пример 6. Пусть S_n — все перестановки множества $[n] = \{1, \dots, n\}$, т. е. биекции $[n] \to [n]$. Тогда $(S_n, \circ)$ — группа.

Если Ω — произвольное множество, то аналогичное множество будем обозначать $S(\Omega)$. Это тоже группа.

2. Подгруппы. Изоморфизмы

Определение. Пусть G — группа, $\varnothing \neq H \subset G$. H — *подгруппа* G, если $\forall a, b \in H \to ab \in H, a^{-1} \in H$. Обозначается как $H \leqslant G$.

Определение. $\{e\} \leqslant G$, $G \leqslant G$ — несобственные подгруппы.

Пример 7. $D_n(F^*) \leqslant GL_n(F)$, где $D_n(F)$ — множество диагональных матриц над F.

Пример 8. $GL_n(F) \geqslant SL_N(F) = \{A \in GL_n(F) | \det A = 1\}$.

Упражнение 2. $GL_n(F) \geqslant T_n(F)$ (T — верхнетреугольные. Здесь с не нулями на диагонали.).

Пример 9. $GL_n(R) \geqslant O_n$ — группа ортогональных матриц ($A^{-1} = A^T$).

Пример 10. $O_n \geqslant \mathcal{D}_n = \{f \in O_n : f(P_n) = P_n\}$ (P_n — это многоугольник) — группа диэдра.

Упражнение 3. $|\mathcal{D}_n| = 2n$ (по n поворотов и симметрий).

Определение. Пусть G и H — две группы. $\varphi : G \to H$ — *изоморфизм*, если φ — биекция, и $\forall a, b \to$
(1) $\varphi(ab) = \varphi(a)\varphi(b)$
(2) $\varphi(a^{-1}) = (\varphi(a))^{-1}$.

Определение. Две группы *изоморфны*, если $\exists\varphi$ — изоморфизм.

Пример 11. $\mathcal{D}_3 \cong S_3$

Пример 12. $\mathbb{C}^* \geqslant \mathbb{C}_n = \{z \in \mathbb{C} : z^n = 1\}$. $\mathbb{Z}_n \cong \mathbb{C}_n \cong$ группе вращений правильного n-угольника.

Упражнение 4. Свойство 2 определения изоморфизма не нужно.

Определение. G — группа, $M \subset G$ — подмножество. *Подгруппой*, порождённой множеством M называется пересечение всех подгрупп в G содержащих M:

$$(M) = \bigcap_{H \leqslant G, M \leqslant H} H$$

Утверждение 2. Пересечение любого семейства подгрупп — подгруппа. (в т. ч., (M) — подгруппа)

Доказательство. Пусть $K = \bigcap_{H_i \leqslant G, i \in I} H_i$. Если $a, b \in K$, то $a, b \in H_i \Rightarrow \begin{cases} ab \in H_i \Rightarrow & ab \in K \\ a^{-1} \in H_i \Rightarrow & a^{-1} \in K \end{cases}$, кроме того, $e \in k$. □

Утверждение 3. $(M) = \{a_1, \ldots, a_k : \forall i \leqslant k \to a_i \in M \vee a^{-1} \in M\}$.

Доказательство. Обозначим правую часть за N.

- $N \subset (M)$: если $a_i, \ldots, a_k \in N$, то $a_i \in (M) \Rightarrow a_1, \ldots, a_k \in (M)$.
- $(M) \subset N$: это так, ибо N — подгруппа, содержащая M.

□