Содержание

1 Теория групп. **2**

1 Теория групп.

Определение 1.1. *Группа — множество с одной операцией* $*$: $G \times G \to G$ *со следующими свойствами:*

1. $a * (b * c) = (a * b) * c$
2. $\exists e$: $a * e = e * a = a$
3. $\forall a\ \exists a^{-1}$: $a * a^{-1} = a^{-1} * a = e$

Пример 1.1.

- $(\mathbb{Z}; +)$
- $(\mathbb{Q}; +)$
- $(\mathbb{R}; +)$
- $(\mathbb{C}; +)$
- $(V; +)$
- $(\mathbb{R}_+; \cdot)$
- $(\mathbb{R} \setminus \{0\}; \cdot)$
- $(\mathbb{Z}_n; +)$

Определение 1.2. *Пусть* G *— группа,* $H \subset G$. *Говорим, что* H *является подгруппой (пишем* $H < G$*), если* H *является группой относительно операции в* G. *Чтобы проверить, что* H *является подгруппой, необходимо убедиться, что произведение двух элементов из* H *принадлежит* H*, и элементы, обратные к* H*, тоже лежат в* H.

Теорема 1.1 (Кэли)**.** *Любая группа* G *является подгруппой в группе подстановок, а именно* S_G.

Определение 1.3. *Абелева группа — группа с коммутативностью.*

Определение 1.4. *Говорят, что группа* G *порождается элементами* $\{x_i\}$*, если любой элемент из* G *можно представить как произведение нескольких* x_i *и обратных к ним. Группа называется циклической, если она порождена одним элементом.*

Теорема 1.2. *Конечная циклическая группа изоморфна* $(\mathbb{Z}_n, +)$.

Определение 1.5. *Пусть* G *— группа,* $H < G$. *Введем два отношения эквивалентности на* G: $x \sim_1 y$ *если* $xy^{-1} \in H$, $x \sim_2 y$ *если* $x^{-1}y \in H$.

Утверждение 1.1. $\sim_1$ *и* $\sim_2$ *совпадают в абелевой группе.*

Заметка 1.1. *Классы эквивалентности по отношению* $\sim_1$ *называются левыми смежными классами; класс элемента* x *обозначается* xH. *Классы эквивалентности по* $\sim_2$ *— правые смежные классы, обозначаются* Hx.

Определение 1.6. *Пусть теперь группа* G *конечна,* $H < G$. *Количество классов эквивалентности* $\sim_1$ *называется индексом* G *по* H *и обозначается* $[G : H]$.

Теорема 1.3 (Лагранжа)**.** $|G| = |H| \cdot [G : H]$.

Определение 1.7. *Пусть* $x \in G$. *Порядком элемента* x *называется наименьшее натуральное число* n*, такое что* $x^n = e$*, где* e *— нейтральный элемент. Обозначение:* $ord(x)$. *Если такого* n *не существует, то пишем* $ord(x) = +\infty$.

Определение 1.8. *Пусть* $X, Y \subset G$ *— подмножества группы. Их произведением будем называть множество* $\{xy | x \in X, y \in Y\}$.

Определение 1.9. *Полная линейна группа* $GL(n, F)$ *— это множество всех квадратных матриц размера* $n \times n$ *с элементами из поля* F*, которые являются обратимыми* ($\det \neq 0$)*, вместе с операцией матричного умножения.*

Определение 1.10. *Специальная линейная группа* $SL(n, F)$ *— это подгруппа полной линейной группы, состоящая из всех матриц с определителем, равным* 1. *То есть это множество всех матриц* A *размера* $n \times n$ *над полем* F*, таких что* $\det(A) = 1$.

Определение 1.11. *Специальная ортогональная группа* $SO(n, F)$ *— группа из ортогональных матриц. Матрица* A *называется ортогональной, если* $A^T \times A = A \times A^T = E$.

Утверждение 1.2. *Пусть* X *— произвольное множество. Тогда множество всех биекций* $f : X \to X$ *образуют группу относительно композиции. Эту группу обозначают* S_X. *Если* $X = \{1, 2, \ldots, n\}$*, то* S_X *обозначают* S_n *— группа подстановок.*