

Содержание

1 Теория групп.	2
1.1 Таблица Кэли.	3
1.2 Группы.	3
1.3 Перестановки.	4
1.4 Центр группы.	4
1.5 Гомоморфизм группы.	5
1.6 Кватернионы.	5
1.6.1 Группа Кватернионов.	5
1.7 Теоремы об изоморфизме.	5
1.7.1 Первая теорема об изоморфизме.	5
1.7.2 Вторая теорема об изоморфизме.	6
1.7.3 Третья теорема об изоморфизме.	6
1.8 Группы автоморфизмов графа.	6
1.9 Действие группы на множестве.	6

1 Теория групп.

Определение 1.1. Группа — множество с одной операцией $*: G \times G \rightarrow G$ 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: $\text{ord}(x)$. Если такого n не существует, то пишем $\text{ord}(x) = +\infty$.

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

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 $f : X \rightarrow X$ образуют группу относительно композиции. Эту группу обозначают S_X . Если $X = \{1, 2, \dots, n\}$, то S_X обозначают S_n — группа перестановок.

1.1 Таблица Кэли.

Определение 1.12. Пусть G — конечная группа порядка n . Её таблицей Кэли (таблицей умножения) будем называть таблицу $(n+1) \times (n+1)$ (левый столбец и левая строка считаются нулевыми и служат лишь для нумерации). В нулевом столбце и в нулевой строке стоят все элементы группы в одном и том же порядке. На пересечении строки и столбца этой таблицы будем ставить произведение соответствующих элементов в нулевом столбце и в нулевой строке (слева пишется элемент, задающий строку, справа — столбец).

Определение 1.13. Напомним, что перестановкой мы будем называть биекцию $f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$. Умножение перестановок — композиция биекций. Перестановки записываются в две строчки: в первой — числа от 1 до n (как правило, в порядке возрастания, но не обязательно), а во второй строчке под числом k стоит число $f(k)$.

1.2 Группы.

Теорема 1.4. G — группа; $H < G$. Равносильно:

1. $\forall x \ xH = Hx$
2. $\forall x \ xH \subset Hx$
3. $\forall x \ xH \supset Hx$
4. $\forall x \ xHx^{-1} = H$
5. $\forall x \ xHx^{-1} \subset H$
6. $\forall x \ xHx^{-1} \supset H$
7. $\forall x \in G \ \forall h \in H \ x^{-1}hx \in H$

Определение 1.14. Такая H называется нормальной подгруппой. Обозначается $H \triangleleft G$.

Определение 1.15. xhx^{-1} называется сопряженным элементом h .

Утверждение 1.3. $h \sim x^{-1}hx$ — отношение эквивалентности.

Определение 1.16. $H \triangleleft G$. Класс смежности по H можно перемножать.

Определение 1.17. Множество классов смежности образуют группу. Это называется факторгруппой G по H . G/H .

Определение 1.18. Простая группа — группа без нетривиальных нормальных подгрупп.

1.3 Перестановки.

Определение 1.19. Перестановкой конечного множества M называется биекция $\pi : M \rightarrow M$. Множество всех перестановок множества M обозначается символом $S(M)$. Произведением перестановок π и σ называется перестановка $\sigma \cdot \pi$, соответствующая биекции $x \mapsto \sigma(\pi(x))$.

Определение 1.20. Пусть $\pi \in S(M)$. Орбитой элемента $a \in M$ называется множество $orb_\pi(a) = \{a, \pi(a), \pi^2(a), \dots\}$. Порядком элемента a называется мощность его орбиты: $ord(a) = |orb(a)|$.

Определение 1.21. В предыдущей серии показано, что любая перестановка является произведением циклов. Количество циклов в перестановке обозначается $cycl(\pi)$. Если перестановка разбивается на циклы, длины которых $-l_1, \dots, l_m$, то (l_1, \dots, l_m) называется циклическим типом перестановки π . Перестановка, у которой циклический тип $(2, 1, 1, \dots, 1)$, называется транспозицией.

Определение 1.22. Перестановка π называется четной или нечетной в зависимости от четности числа $n + cycl(\pi)$. Знаком перестановки называется число $sign(\pi) = (-1)^{n+cycl(\pi)}$.

Определение 1.23. Хотим \forall перестановки называть ее четной или нечетной: $\mathcal{C}\mathcal{C} = \mathcal{C}$, $\mathcal{H}\mathcal{H} = \mathcal{C}$, $\mathcal{CH} = \mathcal{H}$, $\mathcal{HC} = \mathcal{H}$ и \exists \mathcal{C} и $\mathcal{H}\mathcal{C}$ перестановки.

Определение 1.24. Инверсия: $\alpha = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ a_1 & a_2 & \dots & a_i & \dots & a_j & \dots & n \end{pmatrix}$. Пара (i, j) называется инверсией, если $i < j$ и $a_i > a_j$.

Определение 1.25. Перестановка с четным количеством инверсий — четная, с нечетным — нечетная.

Заметка 1.2. \forall перестановка — произведение транспозиций. Четное количество транспозиций \Leftrightarrow четная перестановка.

Определение 1.26. Четная перестановка $= (n + \text{количество циклов}) \pmod{2}$.

Теорема 1.5. Перестановки сопряжены \Leftrightarrow совпадает их циклический тип.

1.4 Центр группы.

Определение 1.27. G — группа. Центр G : $Z(G) := \{g \in G | gh = hg, \forall g \in G\}$.

Утверждение 1.4. $Z(S_n) = \{e\}$.

Теорема 1.6. $Z(G) \triangleleft G$.

Утверждение 1.5. $Z(GL(\mathbb{R})) = \begin{pmatrix} \alpha & 0 & \dots & 0 \\ 0 & \alpha & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \alpha \end{pmatrix}$

Определение 1.28 (Коммутатор). $x, y \in G$. $[x, y] := xyx^{-1}y^{-1}$.

Утверждение 1.6. $[x, y]^{-1} = [y, x]$.

Заметка 1.3. Произведение коммутаторов не обязательно является коммутатором.

Определение 1.29 (Коммутант). $[G, G] := \langle [x, y] \rangle$.

Теорема 1.7. 1. $[G, G] \triangleleft G$.

2. $G/[G; G]$ — абелева.

3. G/H — абелева $\Rightarrow H \supset [G, G]$.

Утверждение 1.7. $\alpha^{-1}[x, y]\alpha = [\alpha^{-1}x\alpha, \alpha^{-1}y\alpha]$.

Утверждение 1.8. $\alpha^{-1}[x_1, y_1][x_2, y_2] \dots [x_k, y_k]\alpha \in [G, G]$.

Теорема 1.8 (Галуа.). A_n простая, если $n \geq 5$.

1.5 Гомоморфизм группы.

Определение 1.30. $(G, \cdot); (H, *)$ — группы. $f : G \rightarrow H$ — отображение. f называется гомоморфизмом, если $\forall a, b \in G$ $f(a \cdot b) = f(a) * f(b)$.

Определение 1.31. $f : G \rightarrow H$ — гомоморфизм. f называется:

- Эпиморфизмом, если f — суръекция.
- Мономорфизмом, если f — инъекция.
- Изоморфизмом, если f — биекция.

$G \simeq H$, если существует изоморфизм $f : G \rightarrow H$.

1.6 Кватернионы.

$\mathbb{H} := \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}\}$.

\times	i	j	k
i	-1	$k = -ji$	$-j = -ki$
j	$-k = -ij$	-1	$i = -kj$
k	$j = -ik$	$-i = -jk$	-1

1.6.1 Группа Кватернионов.

$\mathbb{H} = \{\pm 1, \pm i, \pm j, \pm k\}$.

Лемма 1.1. a_1, a_2, \dots, a_{2n} — строка из символов j и k . Если перевернуть строку и заменить $j \leftrightarrow k$, то произведение не изменится.

1.7 Теоремы об изоморфизме.

1.7.1 Первая теорема об изоморфизме.

Теорема 1.9. Пусть $f : G \rightarrow H$ — гомоморфизм групп. Тогда $Im(f) \simeq G/Ker(f)$.

1.7.2 Вторая теорема об изоморфизме.

Теорема 1.10. Пусть G — группа, H и K — ее подгруппы, причем K нормальна. Тогда $HK/K \simeq H/(H \cap K)$.

1.7.3 Третья теорема об изоморфизме.

Теорема 1.11. Пусть G — группа, H и K — ее нормальные подгруппы, причем $K \subset N$. Тогда $(G/K)/(N/K) \simeq G/N$.

1.8 Группы автоморфизмов графа.

Определение 1.32. Автоморфизмом графа Γ называется биекция множества его вершин на себя, так что пара вершин смежны тогда и только тогда, когда смежны их образы. Автоморфизмы графа образуют группу относительно композиции. Обозначается $\text{Aut}(\Gamma)$.

Теорема 1.12 (Фрухта). Для любой группы G найдется граф, группа автоморфизмов которого в точности G .

1.9 Действие группы на множестве.

Определение 1.33. G — группа, M — множество. Действием (левое) называем G на M называем $\cdot : G \times M \rightarrow M : (g; x) \mapsto g \cdot x$ или $g(x)$.

Свойство 1.1. 1. $(g \cdot h) \cdot x = g \cdot (h \cdot x)$.

2. $e \cdot x = x$.

Следствие 1.1. $gx = y \Rightarrow g^{-1}y = x$.

Определение 1.34 (2). Действие G на M — это гомоморфизм $F : G \rightarrow S_M$ (группа перестановок M). $g \cdot x := F(g)(x)$. Наоборот: есть $\cdot : G \times M \rightarrow M : F(g)(x) := g(x)$.

Определение 1.35. x неподвижен под действием g , если $g \cdot x = x$. Орбита x : $\text{orb}(x) := \{g \cdot x | g \in G\}$.

Утверждение 1.9. Орбиты либо совпадают, либо не пересекаются.

Определение 1.36. $x \in M$; стабилизатор x — это $\text{st}(x) := \{g \in G | gx = x\}$.

Утверждение 1.10. $\text{st}(x)$ — подгруппа в G .

Определение 1.37. $\text{st}(g) := \{x | gx = x\}$ — стабилизатор g .

Лемма 1.2 (Бермсайда). G — конечная группа; M — конечная \Rightarrow количество орбит $= \frac{1}{|G|} \sum_{g \in G} |\text{st}(g)| = \frac{1}{|G|} \sum_{x \in M} |\text{st}(x)|$, тк $\sum_{g \in G} |\text{st}(g)| = \sum_{x \in M} |\text{st}(x)| = \#\{(g, x) | gx = x\}$.