МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
ШКОЛА ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Теория групп

Автор:

Госткин Евгений Михайлович

Проверили:

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* $H \subset G$:

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 1.5, утверждения 1.1 и следствия 1.1)

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

Утверждение 1.2. Если $\operatorname{ord} g = n$:

1. $g^m = e \Leftrightarrow n|m$;
2. $g^k = g^l \Leftrightarrow k \equiv l \mod n$.

Доказательство. 1. $m = qn + r, \quad 0 \leqslant r < n \Rightarrow$ [1] $g^m = (g^n)^q \cdot g^r = g^r = e \Leftrightarrow r = 0$;

2. $g^k = g^l \Leftrightarrow g^{k-l} = e \Leftrightarrow n|(k-l) \Leftrightarrow k \equiv l \mod n$.

□

Следствие 1.2. Если $\operatorname{ord} g = n$, то $|\langle g \rangle| = n$

Доказательство. $\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$, и все элементы различны. □

Определение 1.8. *Порядок конечной группы* G - количество элементов в ней, т.е. $\operatorname{ord} G = |G|$

Определение 1.9. Группа G называется *циклической*, если $\exists g \in G : G = \langle g \rangle$. Всякий такой элемент - *порождающий*.

Утверждение 1.3. $\operatorname{ord} g = n \Rightarrow \operatorname{ord} g^k = \frac{n}{(n,k)}$

Доказательство. 1. $(n, k) = d, n = n_1 d, k = k_1 d : (n_1, k_1) = 1$;

2. $(g^k)^m = e \Leftrightarrow n|km \Leftrightarrow n_1|k_1 m \Leftrightarrow n_1|m$, откуда $\operatorname{ord} g^k = n_1$.

□

Следствие 1.3. $g^k \in G = \langle g \rangle$ - порождающий $\Leftrightarrow (n, k) = 1$.

Теорема 1.1. Любая бесконечная циклическая группа изоморфна группе $\mathbb{Z}$, любая конечная циклическая группа порядка n изоморфна $\mathbb{Z}_n$

Доказательство. 1. $G = \langle g \rangle, \operatorname{ord} G = \infty \Rightarrow f : \mathbb{Z} \to G, k \mapsto g^k$ - изоморфизм;

2. $G = \langle g \rangle, \operatorname{ord} G = n$. Рассмотрим отображение:

$$f : \mathbb{Z}_n \to G, [k] \mapsto g^k \quad k \in \mathbb{Z} \tag{1}$$

$$[k] = [l] \Leftrightarrow k \equiv l \mod n \Leftrightarrow g^k = g^l \tag{2}$$

Из 2 следует, что f корректно определено и биективно, $f(k + l) = f(k)f(l)$ получается из утверждения 1.1, откуда f - изоморфизм.

□

Теорема 1.2. 1. Любая подгруппа циклической группы - циклическая

2. В циклической группе порядка n порядок любой подгруппы делит n и $\forall q : q|n \exists! H$ - подгруппа порядка q

Доказательство. 1. $G = \langle g \rangle$ - циклическая, H - нетривиальная[2] подгруппа G. Если для $m \in \mathbb{N}\, \exists g^{-m} \in H$, то $g^m \in H$. Пусть m - минимальное натуральное число такое, что $g^m \in H$. Докажем, что $H = \langle g^m \rangle$. Пусть $g \in H, k = qm + r, 0 \leqslant r < m$, тогда $g^r = g^k (g^m)^{-q} \in H$, откуда по определению m получается, что $r = 0$, откуда $g^k = (g^m)^q$.

[1] По определению 1.7

[2] Тривиальная подгруппа, очевидно, циклическая

2. Если $|G| = n$, то предыдущее рассуждение при $k = n(g^k = e \in H)$ показывает, что $n = qm$. При этом
$$H = \{e, g^m, g^{2m}, \dots, g^{(q-1)m}\} \tag{3}$$
и H - единственная подгруппа порядка q в группе G. Обратно, если $q|n, n = qm$, то подмножество H, определенное уравнением (3) - подгруппа порядка q.

□

Следствие 1.4. В циклической группе простого порядка любая неединичная подгруппа совпадает со всей группой.

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

Пример 1.5. $(S_n, \circ)$[5] - группа перестановок элементов вида $\{1, \dots, n\}$, рассматриваемых как функции $\{1, \dots, n\} \to S_n$. $\circ$ - 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 1.4, поэтому можно задать действие S_n на любом конечном множестве.

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

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

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.

Пример 1.8. В группе $\mathbb{Z}$ любая подгруппа имеет вид $n\mathbb{Z}$, где $n > 0$

---

[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', является подгруппой $GL_n(R)$.
[5] Название от 'Symmetric group'.

2 Смежные классы по подгруппе, индекс подгруппы. Теорема Лагранжа.

Определение 2.1. G - группа, $H \subseteq G$ - подгруппа, тогда g_1 и g_2 *сравнимы по модулю* H, если $g_1 \equiv g_2 \mod G \Leftrightarrow g_1^{-1}g_2 \in H \Leftrightarrow \exists h \in H : g_2 = g_1 h$.

Утверждение 2.1. Отношение из определения 2.1 - отношение эквивалентности.

Доказательство. 1. $g \equiv g \mod H : g^{-1}g = e \in H$;

2. $g_1 \equiv g_2 \mod H \Rightarrow g_2 \equiv g_1 \mod H : g_2^{-1}g_1 = (g_1^{-1}g_2)^{-1} \in H$;

3. $g_1 \equiv g_2 \mod H \wedge g_2 \equiv g_3 \mod H \Rightarrow g_1 \equiv g_3 \mod H : g_1^{-1}g_2 \in H, g_2^{-1}g_3 \in H : g_1^{-1}g_3 = g_1^{-1}g_2g_2^{-1}g_3 = (g_1^{-1}g_2)(g_2^{-1}g_3) \in H$.

□

Определение 2.2. Классы эквивалентности $gH = \{gh | h \in H\}$из определения 2.1 называются *левыми смежными классами* по подгруппе H, $Hg = \{hg | h \in H\}$ - *правыми смежными классами.*

Замечание 2.1. $g \mapsto g^{-1}$ - биекция между левыми и правыми смежными классами.

Доказательство.

$$(gH)^{-1} = Hg^{-1}.$$

□

Утверждение 2.2. $H \subseteq G, \forall a, b \in G \; aH \cap bH \neq \emptyset \Rightarrow b \in aH$.

Доказательство. $\forall a, b \in G \; aH \cap bH \neq \emptyset \Leftrightarrow b^{-1}a \in H \Leftrightarrow aH = bH \Leftrightarrow b \in aH$. □

Определение 2.3. Индексом подгруппы H группы G называется число смежных классов G по H, обозначается $|G : H|$.

Теорема 2.1. (Лагранжа) G - конечная группа, $H \subseteq G \Rightarrow |G| = |G : H| \, |H|$.

Доказательство. 1. $\forall X = gH \Rightarrow |X| = |H|$ (очевидно, так как в H все элементы различны, gH, полученный умножением всех $h \in H$ на g, имеет ту же мощность, если бы это было не так, получилось бы, что мощность H меньше, чем была).

2. Смежные классы образуют разбиение G на классы эквивалентности, поэтому $|G|$ есть произведение размерности каждого класса эквивалентности (у всех $|H|$), на их число, т.е. индекс G по H.

□

Следствие 2.1. Порядок любой подгруппы конечной группы делит порядок группы.

Следствие 2.2. Порядок любого элемента подгруппы конечной группы делит порядок группы.

Доказательство. Вытекает из следствия 2.1 и того, что порядок элемента равен порядку порождаемой им циклической подгруппы. □

Следствие 2.3. Всякая конечная группа простого порядка является циклической.

Доказательство. Следствие 2.1$\Rightarrow$ такая группа совпадает с циклической подгруппой, порожденной любым элементом, не равным e. □

3 Гомоморфизмы групп, ядро и образ гомоморфизма. Нормальные подгруппы, факторгруппа. Теоремы о гомоморфизмах.

Определение 3.1. *Гомоморфизмом* групп $(G, \circ)$ и $(H, \cdot)$ называется такое отображение $\phi : G \to H$, что:

$$\forall a, b \in G \; \phi(a \circ b) = \phi(a) \cdot \phi(b)$$

Определение 3.2. *Образом* гомоморфизма ϕ называется множество $\operatorname{Im}\phi = \{h \in H | \exists a \in G : \phi(a) = h\}$.

Определение 3.3. *Ядром* гомоморфизма ϕ называется множество $\operatorname{Ker}\phi = \{g \in G | \phi(g) = e\}$.

Определение 3.4. Подгруппа H группы G называется *нормальной*, если $\forall g \in G \; gH = Hg$.

Утверждение 3.1. $H \subseteq G, |G : H| = 2 \Rightarrow H \triangleleft G$

Доказательство. G разбивается на левые смежные классы $eH = H$ и $G \setminus H$, и аналогично на правые $He = H$ и $G \setminus H$, соответственно:

1. $g \in H \Rightarrow gH = Hg = H$
2. $g \in G \setminus H \Rightarrow gH = G \setminus H = Hg$

□

Утверждение 3.2. $H_1 \triangleleft G \wedge H_2 \triangleleft G \Rightarrow H_1 \cap H_2 \triangleleft G$

Доказательство. 1. $H_1 \cap H_2$, очевидно, подгруппа G;

2. Докажем, что $\forall g \in G g^{-1}(H_1 \cap H_2)g = H_1 \cap H_2$:

   kek

□