Начала теории групп

Опр: 1. Группа - это множество G, на котором задана бинарная операция $\cdot\colon G \times G \to G$, обычно называемая умножением, которая должна удовлетворять свойствам, называемыми аксиомами группы:

1) **Ассоциативность**:
$$\forall a, b, c \in G,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

2) **Существование нейтрального элемента**:
$$\exists\, e \in G\colon \forall g \in G,\ g \cdot e = e \cdot g = g$$
где e - нейтральный элемент или ещё его называют единицей в группе G;

3) **Существование обратного элемента**:
$$\forall a \in G,\ \exists\, b \in G\colon a \cdot b = b \cdot a = e$$
где b - обратный элемент к элементу a.

Обозначение: $b = a^{-1}$;

Опр: 2. Подмножество $H \subseteq G$ называется подгруппой, если $e \in H$ и $\forall a, b \in H,\ ab^{-1} \in H$.

Утв. 1.
$$\forall a, b \in H,\ ab^{-1} \in H \Leftrightarrow \begin{cases} \forall a, b \in H, & ab \in H \\ \forall a \in H, & a^{-1} \in H \end{cases}$$

□

$(\Rightarrow)$ $\forall a, b \in H ab^{-1} \in H \Rightarrow \forall b \in H,\ eb^{-1} = b^{-1} \in H,\ \forall a, b^{-1} \in H,\ a(b^{-1})^{-1} = ab \in H$.

$(\Leftrightarrow)$ $\forall a, b \in H,\ ab \in H,\ a^{-1} \in H \Rightarrow b^{-1} \in H, \Rightarrow ab^{-1} \in H$. ■

Rm: 1. Подгруппа это подмножество, которое само является группой относительно той же операции.

Опр: 3. Подгруппы $H = \{e\} \subseteq G$, $H = G \subseteq G$ называются несобственными. Группы отличные от несобственных называются собственными.

Rm: 2. В любой группе G всегда есть несобственные подгруппы.

Пример подгруппы: $G = (\mathbb{Z}, +)$, тогда $H = \{-1, 1\}$ - не подгруппа, поскольку не содержит 0. При этом это является группой относительно умножения.

Как проверить, что $H \subseteq G$ является подгруппой? Необходимо проверить свойства группы, при этом ассоциативность проверять не нужно, потому что H это подмножество G, в котором для любых элементов выполнено свойство ассоциативности.

Пример подгрупп: Пусть $G = (\mathbb{Z}, +)$, тогда $H = n\mathbb{Z}$, где n - фиксировано, $n \in \mathbb{Z}_{\geq 0}$.

1) $n = 0 \Rightarrow n\mathbb{Z} = 0 = \{e\}$;

2) $n = 1 \Rightarrow n\mathbb{Z} = \mathbb{Z}$;

3) $n = 2 \Rightarrow n\mathbb{Z} = 2\mathbb{Z}$ - чётные;

Таким образом, мы можем прийти к следующему предложению.

Утв. 2. Любая подгруппа в $(\mathbb{Z}, +)$ имеет вид $n\mathbb{Z}$, $n \in \mathbb{Z}_{\geq 0}$.

Rm: 3. $n \in \mathbb{Z}_{\geq 0}$, поскольку подгруппа, например, $-3\mathbb{Z}$ совпадает с подгруппой $3\mathbb{Z}$.

$\square$

($\Leftarrow$) Ясно, что $n\mathbb{Z}$ - подгруппа.

($\Rightarrow$) Пусть $H \subseteq G$ - некоторая подгруппа. Если $H = \{0\}$, то $n = 0$. Если $H \neq \{0\}$, то:

$$\exists\, a \in H, a \neq 0 \Rightarrow \pm a \in H \Rightarrow \exists\, a \in H, a > 0$$

Пусть $n \in \mathbb{N}$ - наименьшее, лежащее в $H \Rightarrow n\mathbb{Z} \subseteq H$. Разделим $a \in H$ с остатком на n:

$$a = nq + r,\ 0 \leq r < n,\ r = a - nq \in H \Rightarrow r = 0$$

так как n - минимальный положительный $\Rightarrow H = n\mathbb{Z}$, поскольку каждый элемент подгруппы H представим в виде nq для некоторого $q \in \mathbb{Z}$. $\blacksquare$

Опр: 4. Пусть $(G, \circ)$ и $(H, *)$ - группы, тогда гомоморфизм $\varphi\colon G \to H$ это отображение вида:

$$\forall a, b \in G,\ \varphi(a \circ b) = \varphi(a) * \varphi(b)$$

Утв. 3. Для гомоморфизма будет верно:

1) $e_G \in G$, $e_H \in H \Rightarrow \varphi(e_G) = e_H$;
2) $\varphi(a^{-1}) = \varphi(a)^{-1}$;

$\square$

1) $\forall a \in G$, $\varphi(a) = \varphi(a \circ e_G) = \varphi(a) * \varphi(e_G) \Rightarrow \varphi(a)^{-1} * \varphi(a) = \varphi(a)^{-1} * \varphi(a) * \varphi(e_G) \Rightarrow e_H = \varphi(e_G)$;
2) $\forall a \in G$, $\varphi(a \circ a^{-1}) = \varphi(e_G) \Rightarrow \varphi(a)^{-1} * e_H = \varphi(a)^{-1} = \varphi(a)^{-1} * \varphi(a) * \varphi(a^{-1}) = e_H * \varphi(a^{-1}) = \varphi(a^{-1})$;

$\blacksquare$

Порядок элемента группы

Опр: 5. Возведение элемента $g \in G$ в степень $n \in \mathbb{Z}$: $g^n = \begin{cases} \underbrace{g \cdot \ldots \cdot g}_{n}, & n > 0 \\ \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{|n|}, & n < 0 \\ e, & n = 0 \end{cases}$.

Утв. 4. **Свойства возведения в степень**:

1) $g^n \cdot g^m = g^{n+m}$;
2) $(g^n)^m = g^{nm}$;

$\square$

1) Рассмотрим возможные случаи:

(1) $n, m > 0 \Rightarrow g^n g^m = \underbrace{g\cdot \ldots \cdot g}_{n} \cdot \underbrace{g\cdot \ldots \cdot g}_{m} = \underbrace{g\cdot \ldots \cdot g}_{n+m} = g^{n+m}$;

(2) $n, m < 0 \Rightarrow g^n g^m = \underbrace{g^{-1}\cdot \ldots \cdot g^{-1}}_{|n|} \cdot \underbrace{g^{-1}\cdot \ldots \cdot g^{-1}}_{|m|} = \underbrace{g^{-1}\cdot \ldots \cdot g^{-1}}_{|n|+|m|} = \underbrace{g^{-1}\cdot \ldots \cdot g^{-1}}_{|n+m|} = g^{nm}$;

(3) $n > |m| > 0, m < 0 \Rightarrow g^n g^m = \underbrace{g\cdot \ldots \cdot g}_{n} \cdot \underbrace{g^{-1}\cdot \ldots \cdot g^{-1}}_{|m|} = \underbrace{g\cdot \ldots \cdot g}_{n-|m|} \cdot \underbrace{e\cdot \ldots \cdot e}_{|m|} = \underbrace{g\cdot \ldots \cdot g}_{n+m} = g^{n+m}$;

(4) $|m| > n > 0, m < 0 \Rightarrow g^n g^m = \underbrace{g\cdot \ldots \cdot g}_{n} \cdot \underbrace{g^{-1}\cdot \ldots \cdot g^{-1}}_{|m|} = \underbrace{e\cdot \ldots \cdot e}_{n} \cdot \underbrace{g^{-1}\cdot \ldots \cdot g^{-1}}_{|m|-n} = \underbrace{g^{-1}\cdot \ldots \cdot g^{-1}}_{|m+n|} = g^{n+m}$;

(5) $n, m = 0 \Rightarrow g^n g^m = ee = e = g^{n+m}$;

2) Отметим,что $(g^n)^-1 = g^{-n}$, поскольку:

$$g^n\cdot g^{-n} = g^{-n}\cdot g^n = g^{n-n} = g^0 = e$$

Рассмотрим возможные случаи:

(1) $m > 0 \Rightarrow (g^n)^m = \underbrace{g^n\cdot \ldots \cdot g^n}_{m} = g^{n+n+\ldots+n} = g^{nm}$;

(2) $m < 0 \Rightarrow (g^n)^m = \underbrace{(g^n)^{-1}\cdot \ldots \cdot (g^n)^{-1}}_{|m|} = \underbrace{g^{-n}\cdot \ldots \cdot g^{-n}}_{|m|} = g^{-n-n-\ldots-n} = g^{-|m|n} = g^{mn}$;

(3) $m = 0 \Rightarrow (g^n)^0 = e = g^{n\cdot 0} = g^{nm}$;

■

Если мы возьмем элемент $g \in G$ и начнём возводить в степени, то возможны две ситуации:

1) Все g^n различны при разных $n \in \mathbb{Z}$;

2) Существуют повторения: $g^k = g^l$ при некоторых $k > l$, $k, l \in \mathbb{Z}$. В этом случае, если домножить левую и правую части на g^{-l}, то получим:

$$m = k - l \in \mathbb{N},\ g^m = g^{k-l} = e$$

Опр: 6. Порядок элемента $g \in G$ это наименьшое $m \in \mathbb{N}$ для которого $g^m = e$ или ∞, если такого m не существует.

Обозначение: $o(g)$ или $\mathrm{ord}(g)$.

Примеры порядков элементов:

1) **Цикл длины** l: $\sigma = (i_1, i_2, \ldots, i_l) \in S_n$. Элементы орбиты: $i_1 \to i_2 \to \ldots \to i_l \to i_1$, все остальные элементы: $i \to i$. Каков порядок такой подстановки? Под действием σ каждый элемент сдвигается в следующий по циклу $\Rightarrow$ можем применить подстановку несколько раз, тогда:

$$\sigma^m = \varepsilon \Leftrightarrow m \vdots l \Rightarrow \mathrm{ord}(\sigma) = l$$

2) **Произвольная подстановка** $\sigma \in S_n$: По теореме о разложении на независимые циклы, будет верно:

$$\sigma = \sigma_1\cdot \ldots \cdot\sigma_s \Rightarrow \sigma^m = \sigma_1^m\cdot \ldots \cdot\sigma_s^m,\ \sigma^m = \varepsilon \Leftrightarrow \sigma_1^m = \ldots = \sigma_s^m = \varepsilon \Leftrightarrow m \vdots l_1, l_2, \ldots l_s$$

где $l_1, \ldots, l_s$ - их длины $\Rightarrow$ у нас несколько непересекающихся орбит разных длин и чтобы найти порядок σ мы должны найти наименьшее $m \in \mathbb{N}$, которое делится на длины всех этих орбит:

$$\operatorname{ord}(\sigma) = [l_1, \ldots, l_s] = \text{НОК}(l_1, \ldots, l_s)$$

3) $G = (\mathbb{Z}, +)$, тогда: $\forall a \in \mathbb{Z}$, $a \neq 0 \Rightarrow \operatorname{ord}(a) = \infty$, $\operatorname{ord}(0) = 1$;

Утв. 5. (**Свойства порядка**) Пусть $g \in G$ - элемент группы, $\operatorname{ord}(g) = m \in \mathbb{N}$ или ∞, тогда:

1) $g^n = e \Leftrightarrow n \,\vdots\, m$ или $n = 0$;
2) $g^k = g^l \Leftrightarrow k \equiv l \pmod{m}$ или $k = l$;

□

1) При $\operatorname{ord}(g) = \infty$ это очевидно, поскольку $g^0 = e$, а остальные g^n, $n \neq 0$ это другие элементы группы. При $\operatorname{ord}(g) = m \in \mathbb{N}$, поделим n с остатком: $n = mq + r$, $0 \leq r < m$, тогда:

$$g^n = g^{mq+r} = (g^m)^q \cdot g^r = e^q \cdot g^r = e \cdot g^r = g^r$$

$$g^n = e \Leftrightarrow g^r = e \Leftrightarrow r = 0 \Leftrightarrow n \,\vdots\, m$$

где второе верно, поскольку m - наименьшее натуральное для которого $g^m = e$, а $0 \leq r < m$;

2) Воспользуемся результатами предыдущего пункта:

$$g^k = g^l \Leftrightarrow g^{k-l} = e \Leftrightarrow k - l \,\vdots\, m \vee k - l = 0 \Leftrightarrow k \equiv l \pmod{m} \vee k = l$$

таким образом, что для конечного, что для бесконечного порядка мы доказали равносильность;

■

Изоморфизм групп

Вспомним немного про изоморфизм. Пусть $(G, \circ)$, $(H, *)$ - группы. $\varphi\colon G \to H$ - гомоморфизм:

$$\forall a, b \in G,\ \varphi(a \circ b) = \varphi(a) * \varphi(b)$$

Опр: 7. Изоморфизм это биективный гомоморфизм.

Утв. 6. Для изоморфизма $\varphi\colon G \to H$ верно:

$$\exists\, \varphi^{-1}\colon H \to G,\ \forall c, d \in H,\ \varphi^{-1}(cd) = \varphi^{-1}(c)\varphi^{-1}(d)$$

□ Поскольку φ - биекция, то $\exists\, \varphi^{-1}\colon H \to G$. Тогда:

$$\forall c, d \in H,\ \varphi(\varphi^{-1}(c * d)) = c * d = \varphi(\varphi^{-1}(c)) \circ \varphi(\varphi^{-1}(d)) = \varphi(\varphi^{-1}(c) \circ \varphi^{-1}(d)) \Rightarrow$$
$$\Rightarrow \varphi^{-1}(c * d) = \varphi^{-1}(c) \circ \varphi^{-1}(d)$$

так как φ - биекция. ■

Rm: 4. Таким образом, изоморфизм это обратимый гомоморфизм, и обратный к нему также будет гомоморфизмом.

Опр: 8. Группы G и H изоморфны, если существует изоморфизм: $\varphi\colon G \to H$.

Обозначение: $G \simeq H$.

Пример изоморфизма: $G = (\mathbb{R}, +)$, $H = (\mathbb{R}^\times, \cdot)$, $\varphi\colon G \to H$, $\forall a \in \mathbb{R}$, $\varphi(a) = e^a$, тогда:

$$\forall a, b \in \mathbb{R},\ \varphi(a+b) = e^{a+b} = e^a e^b = \varphi(a)\varphi(b)$$

Следовательно, φ - гомоморфизм. $\forall c \in \mathbb{R}^\times$, $\varphi^{-1}(c) = \ln(c) \Rightarrow \varphi$ - изоморфизм и $G \simeq H$.

С точки зрения теории групп это одна и та же группа, и все утверждения, доказанные для одной из них, также будут верны и для другой.

Опр: 9. Эндоморфизм это гомоморфизм в себя: $\varphi\colon G \to G$.

Опр: 10. Автоморфизм это изоморфизм в себя: $\varphi\colon G \xrightarrow{\sim} G$.

Очевидно, что каждая группа одинакова сама с собой, но важно понять, сколькими способами можно отождествить группу с собой. Есть группы у которых почти нет автоморфизмов (когда отождествить группу с собой можно единственным способом), а есть группы для которых это можно сделать несколькими способами (аналог замены координат в группе).

Ядро и образ

Опр: 11. Если $\varphi\colon G \to H$ это гомоморфизм, то:

1) Ядром φ называется множество:
$$\ker\varphi = \{a \in G \mid \varphi(a) = e_H\}$$

2) Образом φ называется множество:
$$\operatorname{Im}\varphi = \{b \in H \mid \exists\, a \in G\colon \varphi(a) = b\}$$

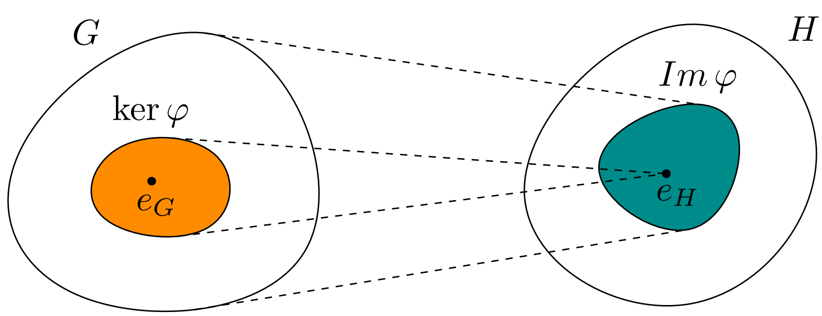

Рис. 1: Образ и ядро оператора φ.

Упр. 1. Пусть $\varphi\colon G \to H$ - гомоморфизм, тогда:

1) φ - изоморфизм $\Leftrightarrow \operatorname{Im}\varphi = H$, $\ker\varphi = \{e_G\}$;

2) $\ker\varphi \subseteq G$, $\operatorname{Im}\varphi \subseteq H$ - подгруппы;

$\square$

1) $(\Rightarrow)$ φ - изоморфизм, тогда φ - биекция:
$$\forall b \in H,\ \exists\, a \in G\colon \varphi(a) = b \Rightarrow H \subseteq \operatorname{Im}\varphi \Rightarrow \operatorname{Im}\varphi = H$$
$$\forall a \in G,\ \varphi(a \circ e_G) = \varphi(e_G \circ a) = \varphi(a) = \varphi(a) * \varphi(e_G) = \varphi(e_G) * \varphi(a) \Rightarrow$$
$$\Rightarrow \varphi(e_G) = e_H \Rightarrow \ker\varphi = \{e_G\}$$

($\Leftarrow$) $\operatorname{Im}\varphi = H \Rightarrow \varphi$ - сюръекция. Поскольку $\ker\varphi = \{e_G\} \Rightarrow \varphi(e_G) = e_H$, тогда:

$$\forall a, b \in G, \varphi(a) = \varphi(b) \Rightarrow \varphi(a \circ a^{-1}) = \varphi(b \circ a^{-1}) \Rightarrow e_H = \varphi(e_G) = \varphi(b \circ a^{-1}) \Rightarrow$$

$$\Rightarrow b \circ a^{-1} \in \ker\varphi \Rightarrow b \circ a^{-1} = e_G \Rightarrow b \circ a^{-1} \circ a = e_G \circ a \Rightarrow b = a$$

Следовательно, φ - биекция;

2) Проверим, что $\ker\varphi \subseteq G$ это подгруппа G:

$$\forall a, b \in \ker\varphi,\ \varphi(a \circ b) = \varphi(a) * \varphi(b) = e_H \cdot e_H = e_H \Rightarrow a \circ b \in \ker\varphi$$

$$\forall a \in \ker\varphi,\ \varphi(a) = e_H \Rightarrow \varphi(a)\varphi(a^{-1}) = e_H\varphi(a^{-1}) \Rightarrow \varphi(e_G) = e_H = \varphi(a^{-1}) \Rightarrow a^{-1} \in \ker\varphi$$

Проверим, что $\operatorname{Im}\varphi \subseteq H$ это подгруппа H:

$$\forall a, b \in \operatorname{Im}\varphi,\ \exists\, c, d \in G \colon \varphi(c) = a,\ \varphi(d) = b \Rightarrow \varphi(c \circ d) = a * b$$

$$a * b \in H,\ c \circ d \in G,\ \varphi(c \circ d) = a * b \Rightarrow a * b \in \operatorname{Im}\varphi$$

$$\forall a \in \operatorname{Im}\varphi,\ \exists\, c \in G \colon \varphi(c) = a,\ a \in H,\ c \in G \Rightarrow \exists\, a^{-1} \in H,\ \exists\, c^{-1} \in G \Rightarrow$$

$$a * a^{-1} = a^{-1} * a = \varphi(c) * a^{-1} = a^{-1} * \varphi(c) = e_H \Rightarrow$$

$$\Rightarrow \varphi(c^{-1}) * \varphi(c) * a^{-1} = \varphi(c^{-1}) * e_H \Rightarrow \varphi(e_G) * a^{-1} = a^{-1} = \varphi(c^{-1}) \Rightarrow a^{-1} \in \operatorname{Im}\varphi$$

■

Примеры групп

1) **Числовые аддитивные группы**: $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{C}, +)$ это всё примеры бесконечных групп, $(\mathbb{Z}_n, +)$ - пример конечной аддитивной группы. Все эти группы коммутативны;

2) **Числовые мультипликативные группы**: $(\mathbb{Z}^\times, \cdot) = \{-1, 1\}$, $(F^\times, \cdot)$, где $F^\times = F \setminus \{0\}$ и F - любое поле, $(\mathbb{Z}_n^\times, \cdot)$, где $\mathbb{Z}_n^\times = \{\overline{k} \mid (k, n) = 1\}$. Все эти группы коммутативны;

3) **Группа подстановок**: S_n - симметрическая группа, $A_n \subseteq S_n$ - группа четных подстановок или знакопеременная группа (alternating group);

4) **Группа Клейна**:

$$V_4 = \{id, (12)(34), (13)(24), (14)(23)\} \subseteq S_4$$

Для подстановок длины 4 все пары независимых циклов оказываются подгруппой. Каждый элемент обратен сам к себе, а произведение двух подстановок равняется третьей. Это уникальное свойство S_4. Например, в S_5 пары независимых циклов уже не образуют подгруппу;

5) **Группа матриц** (по умножению):

(1) $GL_n(F) = \{A \in \operatorname{Mat}_{n,n} \mid \det(A) \neq 0\}$ полная линейная группа над полем F;

(2) $SL_n(F) = \{A \in \operatorname{Mat}_{n,n} \mid \det(A) = 1\} \subseteq GL_n(F)$ специальная линейная группа над полем F;

(3) $D_n(F) = \left\{ A \in \operatorname{Mat}_{n,n} \,\middle|\, A = \begin{pmatrix} * & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & * \end{pmatrix} \right\}$ диагональные матрицы.

Заметим, что на диагонали должны стоять ненулевые элементы для обратимости;

(4) $B_n(F) = \left\{ A \in \mathrm{Mat}_{n,n} \middle| A = \begin{pmatrix} * & * & * \\ 0 & \ddots & * \\ 0 & 0 & * \end{pmatrix} \right\}$ верхнетреугольные матрицы.

Заметим,что на диагонали должны стоять ненулевые элементы для обратимости, над диагональю - произвольные элементы;

(5) $U_n(F) = \left\{ A \in \mathrm{Mat}_{n,n} \middle| A = \begin{pmatrix} 1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & 1 \end{pmatrix} \right\}$ унитреугольные матрицы;

6) **Группа кватернионов**: $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, $i^2 = j^2 = k^2 = -1$, определим умножение по цепочке:

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

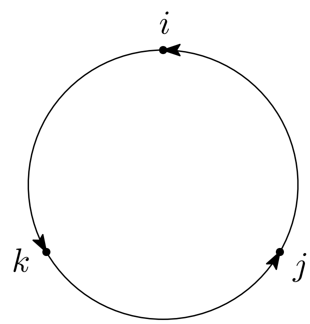

Рис. 2: Умножение в группе кватернионов.

Если идти против часовой стрелки, то перемножение соседних элементов даст следующий элемент со знаком $+$, если перемножать по часовой стрелке, то со знаком минус;

Циклические группы

Пусть $g \in G$, рассмотрим множество, состоящее из всех степеней g: $H = \{g^n \mid n \in \mathbb{Z}\}$. Это множество замкнуто относительно умножения и взятия обратного элемента, то есть это подгруппа G.

Опр: 12. Множеством всех степеней элемента $g \in G$ называется множество: $H = \{g^n \mid n \in \mathbb{Z}\} \subseteq G$.

Обозначение: $H = \langle g \rangle$. Если $\mathrm{ord}(g) = m$, то $H = \langle g \rangle_m$. Если $\mathrm{ord}(g) = \infty$, то $H = \langle g \rangle_\infty$.

Rm: 5. Множество $H = \langle g \rangle$, $g \in G$ также ещё называется циклической подгруппой G и это самая маленькая подгруппа, содержащая элемент g в том смысле, что она лежит в любой другой подгруппе, содержащей g. Действительно, если в подгруппе $K \subseteq G$ есть g, то там же есть и e, подгруппа замкнута относительно операции на ней $\Rightarrow g{\cdot}g \in K \Rightarrow$ и все степени g.

Пример циклической подгруппы: $G = (\mathbb{Z}, +)$, $g = 2 \Rightarrow \langle g \rangle = 2\mathbb{Z}$.

Опр: 13. Группа G называется циклической группой, если $G = \langle g \rangle$ для некоторого $g \in G$.

Опр: 14. Элемент $g \in G = \langle g \rangle$ называется порождающим элементом циклической группы G.

Rm: 6. Порождающий элемент, вообще говоря, определен неоднозначно в циклической группе.

Примеры циклических групп:

1) $(\mathbb{Z}, +)$ - бесконечная циклическая группа, $\mathbb{Z} = \langle 1 \rangle_\infty = \langle -1 \rangle_\infty$, в данном случае 1 или -1 будут порождающими элементами;

2) $(\mathbb{Z}_m, +)$ - конечная циклическая группа, $\mathbb{Z}_m = \langle 1 \mod m \rangle_m$;

Упр. 2. Найти все порождающие элементы в группе $(\mathbb{Z}_m, +)$.

Обозначение: порядок произвольного множества M:

(1) $|M| =$ число элементов в M, если M конечно;

(2) $|M| = \infty$, если M - бесконечно;

Rm: 7. В случае конечных множеств, мощность и порядок множеств это одно и то же, в случае бесконечного множества мощность отлична от порядка, поскольку существуют бесконечные множества разной мощности, но с точки зрения порядка нам это не интересно.

Утв. 7. (**Свойство порядка циклических подгрупп**)

$$\operatorname{ord}(g) = |\langle g \rangle|$$

☐ Циклическая подгруппа состоит из всех степеней элемента g, её порядок это количество различных элементов, то есть количество различных степеней. По свойству порядка 2):

$$g^k \neq g^l \Leftrightarrow k \not\equiv l \pmod m \vee k \neq l$$

Если $\operatorname{ord}(g) < \infty$, то количество различных степеней равно количеству остатков при делении на m или, что тоже самое, количеству классов вычетов и равно m:

$$m = \operatorname{ord}(g) \Rightarrow e, g, g^2, \ldots, g^{m-1} \text{ - попарно различны}$$

В самом деле, если $g^k = g^l$, $k > l$, то $g^{k-l} = e$, если $k - l < m$, то получаем противоречие с определением порядка. С другой стороны, если $k \in \mathbb{Z}$, то:

$$k = mq + r,\ 0 \leq r < m \Rightarrow$$

$$\Rightarrow g^k = g^{mq+r} = (g^m)^q g^r = g^r,\ 0 \leq r \leq m-1 \Rightarrow |\langle g \rangle| = \operatorname{ord}(g) = m < \infty$$

Если $\operatorname{ord}(g) = \infty$, то все степени различны при разных показателях $\Rightarrow$ циклическая группа будет бесконечной $\Rightarrow |\langle g \rangle| = \operatorname{ord}(g) = \infty$. ■

Теорема 1. Все циклические подгруппы одного порядка изоморфны друг другу.

☐ Пусть $G = \langle g \rangle$. Рассмотрим два случая:

1) $\operatorname{ord}(g) = \infty \Rightarrow \varphi\colon (\mathbb{Z}, +) \to G$, $\varphi(n) = g^n$. Очевидно, что φ - взаимнооднозначно:

   (1) Инъективность: следует из свойства порядка 2): $g^k = g^l \Leftrightarrow k = l$;

   (2) Сюръективность: следует из того, что $\forall a \in G$, $\exists\, n \in \mathbb{Z}\colon g^n = a$;

   Проверим свойство согласованности изоморфизма с операциями в обеих группах:

$$\forall k, l \in \mathbb{Z},\ \varphi(k + l) = g^{k+l} = g^k \cdot g^l = \varphi(k) \cdot \varphi(l)$$

   Следовательно, φ - изоморфизм $\Rightarrow G \simeq \mathbb{Z}$;

2) $\mathrm{ord}(g) = m \in \mathbb{N} \Rightarrow \varphi\colon (\mathbb{Z}_n, +) \to G$, $\varphi(\overline{n}) = g^n$, где $\overline{n} = (n \bmod m)$. Проверим корректность определения, поскольку один и тот же класс вычетов может иметь разных представителей:

$$\overline{n} = \overline{k} \Rightarrow n \equiv k \pmod m \Rightarrow g^n = g^k$$

Следовательно, отображение определено корректно. Проверим биективность:

(1) Инъективность: следует из свойства порядка 2): $g^k = g^l \Leftrightarrow k \equiv l \pmod m \Leftrightarrow \overline{n} = \overline{l}$;

(2) Сюръективность: следует из того, что $\forall a \in G$, $\exists\, \overline{n} \in \mathbb{Z}_n\colon g^n = a$, либо это можно сразу понять из инъективности функции на конечных множествах;

Проверим свойство согласованности изоморфизма с операциями в обеих группах:

$$\forall \overline{k}, \overline{l} \in \mathbb{Z}_n,\ \varphi(\overline{k} + \overline{l}) = \varphi(\overline{k + l}) = g^{k+l} = g^k \cdot g^l = \varphi(\overline{k}) \cdot \varphi(\overline{l})$$

Следовательно, φ - изоморфизм $\Rightarrow G \simeq \mathbb{Z}_n$;

■

Rm: 8. В частности теорема говорит, что любая бесконечная циклическая подгруппа изоморфна $(\mathbb{Z}, +)$, а любая циклическая группа порядка m изоморфна $\mathbb{Z}_m$.

Пример: Рассмотрим $\mathbb{U}_m = \{\varepsilon_0 = 1, \varepsilon_1, \ldots, \varepsilon_{m-1}\}$, где $\varepsilon_k = \cos \frac{2\pi k}{m} + i \sin \frac{2\pi k}{m}$, тогда:

$$\varepsilon_k = (\varepsilon_1)^k \Rightarrow \mathbb{U}_m = \langle \varepsilon_1 \rangle_m \Rightarrow \mathbb{U}_m \simeq \mathbb{Z}_m,\ \varepsilon_k \leftrightarrow k \bmod m = \overline{k}$$

Теорема 2. Пусть G это циклическая группа, тогда:

1) Любая подгруппа $H \subset G$ также будет циклической;
2) Если $|G| = \infty$, то тогда либо $|H| = \infty$, либо $H = \{e\}$;
3) Если $|G| = m \in \mathbb{N}$, то тогда $|G| \vdots |H|$, где H - подгруппа;
4) Если $|G| = m \in \mathbb{N}$, то тогда $\forall d \in \mathbb{N}\colon m \vdots d$, $\exists!$ подгруппа $H \subset G\colon |H| = d$;

□ Пусть $G = \langle g \rangle$, тогда:

1) Либо $H = \{e\} \Rightarrow$ доказано, либо $\exists\, n \in \mathbb{Z}$, $n \neq 0\colon g^n \in H \Rightarrow \exists\, n > 0\colon g^n \in H$, при $n < 0$ можно взять обратный элемент: $(g^n)^{-1} = g^{-n} \in H$. Возьмем наименьшее $n \in \mathbb{N}\colon g^n \in H$, тогда:

$$\forall k \in \mathbb{Z},\ k = nq + r,\ 0 \le r < n \Rightarrow g^k = (g^n)^q \cdot g^r \Rightarrow$$

$$\Rightarrow g^r = (g^n)^{-q} \cdot g^k,\ (g^n)^{-q} \in H \Rightarrow g^k \in H \Leftrightarrow g^r \in H \Leftrightarrow r = 0 \Leftrightarrow k \vdots n$$

где предпоследнее верно в силу того, что $n \in \mathbb{N}$ - наименьшее для которого $g^n \in H$, а $r < n$. Следовательно, $H = \langle g^n \rangle$. В частности, подгруппа H является циклической;

2) $|G| = \infty \Rightarrow$ либо $H = \{e\}$, если $g = e$, либо $H = \{\ldots, g^{-2n}, g^{-n}, e, g^n, g^{2n}, \ldots\}$, но поскольку группа бесконечна, то все степени в H - разные $\Rightarrow |H| = \infty$;

3) $|G| = m = |\langle g \rangle| = \mathrm{ord}(g) \Rightarrow g^m = e \in H \Rightarrow m \vdots n$, $m = n \cdot d$, где $n \in \mathbb{N}$ наименьший чтобы $g^n \in H$, по аналогии с пунктом 1), тогда: $H = \langle g^n \rangle$ и он будет состоять из следующих элементов:

$$(g^n)^0 = e, (g^n)^1 = g^n, (g^n)^2 = g^{2n}, \ldots, (g^n)^{d-1} = g^{n(d-1)}, (g^n)^d = g^{nd} = g^m = e \Rightarrow$$

$$\Rightarrow H = \langle g^n \rangle = \{e, g^n, g^{2n}, \ldots, g^{n(d-1)}\} \Rightarrow |H| = d \Rightarrow |G| \vdots |H|$$

4) Пусть $d \mid m$, $d > 0$ - произвольный делитель m больше 0, предъявим подгруппу H в группе G порядка d. Положим $n = \frac{m}{d}$ и рассмотрим $H = \langle g^n \rangle$, тогда:

$$H = \{e, g^n, g^{2n}, \dots, g^{n(d-1)}\} \Rightarrow |H| = d$$

Из пункта 3) видно, что $H = \langle g^n \rangle$ это единственная подгруппа порядка d, иначе другая подгруппа должна быть порождена другим элементом g^k и тогда k - другой делитель числа m, но тогда $m = k{\cdot}p$, где $p \neq d$. То есть порождающий элемент g^n подгруппы H однозначно определяется по d;

■

Смежность классов и теорема Лагранжа

Пусть G - группа, $H \subseteq G$ - подгруппа.

Опр: 15. Смежность слева элементов $g_1, g_2 \in G$ по подгруппе H: $g_1 \underset{H}{\sim} g_2$, если $\exists\, h \in H\colon g_1{\cdot}h = g_2$.

Если H фиксированно, то знак H под эквивалентность писать не будем.

Утв. 8. Смежность слева это отношение эквивалентности.

□

1) Рефлексивность:
$$\forall g \in G,\ g{\cdot}e = g,\ e \in H \Rightarrow g \sim g$$

2) Симметричность:
$$g_1 \sim g_2 \Rightarrow \exists\, h \in H\colon g_1{\cdot}h = g_2 \Rightarrow h^{-1} \in H,\ g_2{\cdot}h^{-1} = g_1{\cdot}h{\cdot}h^{-1} = g_1{\cdot}e = g_1 \Rightarrow g_2 \sim g_1$$

3) Транзитивность:
$$g_1 \sim g_2,\ g_2 \sim g_3 \Rightarrow \exists\, h, h' \in H\colon g_1{\cdot}h = g_2,\ g_2{\cdot}h' = g_3 \Rightarrow g_1{\cdot}\underbrace{h{\cdot}h'}_{\in H} = g_2{\cdot}h' = g_3 \Rightarrow g_1 \sim g_3$$

■

Соответственно, отношение эквивалентности на множестве разбивает его на попарно непересекающиеся классы эквивалентности.

Опр: 16. Левым смежным классом элемента $g \in G$ по подгруппе H называется подмножество в G:

$$g{\cdot}H = \{g{\cdot}h \mid h \in H\}$$

Rm: 9. Вся группа G разбивается на попарно непересекающиеся левые смежные классы.

Лемма 1.

1) $\forall g, g' \in G$, либо $g{\cdot}H = g'{\cdot}H$, либо их смежные классы не пересекаются: $g{\cdot}H \cap g'{\cdot}H = \varnothing$;
2) $\forall g \in G$, $|g{\cdot}H| = |H|$;

□

1) Если $g{\cdot}H \cap g'{\cdot}H \neq \varnothing$, то:

$$\exists\, h, h' \in H\colon g{\cdot}h = g'{\cdot}h' \Rightarrow g = g'{\cdot}h'{\cdot}h^{-1} \Rightarrow g{\cdot}H = g'{\cdot}\underbrace{h'{\cdot}h^{-1}}_{\in H}{\cdot}H = g'{\cdot}H$$

где $h'{\cdot}h^{-1}{\cdot}H$ это просто перестановка элементов $H \Rightarrow h'{\cdot}h^{-1}{\cdot}H = H \Rightarrow g{\cdot}H = g'{\cdot}H$;

2) Поскольку $g{\cdot}H = \{g{\cdot}h \mid h \in H\} \Rightarrow |g{\cdot}H| \leq |H|$. Если $g{\cdot}h = g{\cdot}h'$, то умножим на g^{-1} слева, тогда: $h = h' \Rightarrow |g{\cdot}H| = |H|$, поскольку $<$ это на случай, если совпадут $g{\cdot}h$ для разных h;

■

Обозначение: Множество всех левых классов G по группе H принято обозначать как G/H:

$$G/H = \{g{\cdot}H \mid g \in G\}$$

Опр: 17. Индексом подгруппы $H \subseteq G$ называется число левых смежных классов в G по подгруппе H.

Обозначение: $|G/H| = (G\colon H) = [G\colon H]$.

Rm: 10. Аналогично можно определить отношение смежности справа по подгруппе H

Опр: 18. Смежность справа элементов $g_1, g_2 \in G$ по подгруппе H: $g_1 \sim g_2$, если $\exists\, h \in H\colon h{\cdot}g_1 = g_2$.

Опр: 19. Правым смежным классом элемента $g \in G$ по подгруппе H называется подмножество в G:

$$H{\cdot}g = \{h{\cdot}g \mid h \in H\}$$

Упр. 3. Количество правых смежных классов по подгруппе H равно количеству левых смежных классов по подгруппе H.

Пример: $G = (\mathbb{Z}, +)$ это циклическая группа, значит всякая подгруппа тоже циклическая, следовательно она порождена каким-то одним элементом $m \Rightarrow H = m{\cdot}\mathbb{Z}$, $m \in \mathbb{Z}_{\geq 0}$, тогда:

$$k \sim l \Leftrightarrow \exists\, n \in \mathbb{Z}\colon k + n{\cdot}m = l \Leftrightarrow k \equiv l \pmod{m}$$

Получается, что отношение смежности (кроме случая с 0, когда числа просто совпадают) это отношение сравнимости по модулю m. Следовательно, смежные классы это классы вычетов по модулю m и множество смежных классов это просто множество классов вычетов:

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m \Rightarrow (\mathbb{Z}\colon m\mathbb{Z}) = m$$

Теорема 3. (**Лагранжа**) Пусть G - конечная группа, а $H \subseteq G$ - подгруппа, тогда: $|G| = |H|{\cdot}(G\colon H)$.

□

1) $\forall g \in G$ существует взаимнооднозначное соответствие: $H \to g{\cdot}H$, $h \mapsto g{\cdot}h$ - биекция:

   (1) Инъективность: $g{\cdot}h_1 = g{\cdot}h_2 \Rightarrow g^{-1}{\cdot}g{\cdot}h_1 = h_1 = h_2$;

   (2) Сюръективность: Очевидна по определению смежного класса: $\forall v \in g{\cdot}H$, $\exists\, h \in H\colon g{\cdot}h = v$;

   Таким образом, получили биекцию и в частности $|H| = |g{\cdot}H|$;

2) Поскольку $|G| < \infty$, то рассмотрим множество:

$$G/H = \{g_1{\cdot}H, g_2{\cdot}H, \ldots, g_s{\cdot}H\},\ s = (G\colon H) \Rightarrow G = g_1{\cdot}H \sqcup g_2{\cdot}H \sqcup \ldots \sqcup g_s{\cdot}H$$

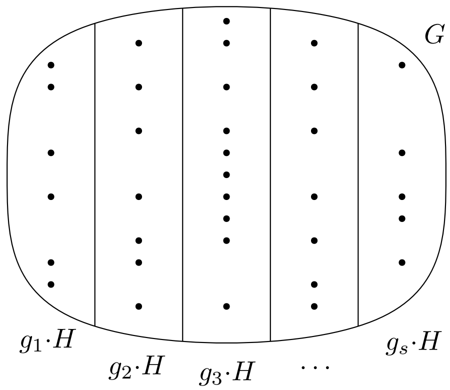

Рис. 3: Разбиение группы G на смежные классы.

Таким образом, поскольку классы не пересекаются, мы получим:

$$|G| = |g_1{\cdot}H| + |g_2{\cdot}H| + \ldots + |g_s{\cdot}H| = \underbrace{|H| + |H| + \ldots + |H|}_{s} = |H|{\cdot}s = |H|{\cdot}(G\colon H)$$

■

Rm: 11. Также можно было воспользоваться леммой, которую мы рассмотрели ранее.

Следствие 1. Пусть G - конечная группа, а $H \subseteq G$ - подгруппа, тогда: $|G| \,\vdots\, |H|$.

□ Очевидно: $|G| = |H|{\cdot}(G\colon H) \Rightarrow \frac{|G|}{|H|} = (G\colon H) \in \mathbb{N} \Rightarrow |G| \,\vdots\, |H|$. ■

Следствие 2. $\forall g \in G$, $|G| \,\vdots\, \operatorname{ord}(g)$.

□ Возьмем $H = \langle g \rangle$, тогда $\operatorname{ord}(g) = |H| \Rightarrow$ применим предыдущее следствие и получим требуемое. ■

Следствие 3. $|G| = n \Rightarrow \forall g \in G,\ g^n = e$.

□ Пусть $\operatorname{ord}(g) = m$, тогда по следствию 2 верно: $m \mid n$, $n = m{\cdot}d \Rightarrow g^n = (g^m)^d = e^d = e$. ■

Пусть $m \in \mathbb{N}$, рассмотрим функцию Эйлера:

$$\varphi(m) = \{k \in 1, \ldots, m-1 \mid (m, k) = 1\}$$

Известна следующая теорема из теории чисел.

Теорема 4. (**Эйлера**) $\forall k \in \mathbb{Z},\ (m, k) = 1 \Rightarrow k^{\varphi(m)} \equiv 1 \pmod{m}$.

□ Рассмотрим $\mathbb{Z}_m^\times = \{\overline{k} \mid (k, m) = 1\}$, тогда $|\mathbb{Z}_m^\times| = \varphi(m)$ по определению. По следствию 3:

$$\forall \overline{k} \in \mathbb{Z}_m^\times,\ \overline{k}^{\varphi(m)} = \overline{1} \Rightarrow k^{\varphi(m)} \equiv 1 \pmod{m}$$

■

Также с помощью теоремы Лагранжа можно вывести малую теорему Ферма.

Следствие 4. (**Малая теорема Ферма**) Пусть p - простое число и $\overline{a} \in \mathbb{Z}_p$, тогда $\overline{a}^p = \overline{a}$.

$\square$ Рассмотрим группу $G = (\mathbb{Z}_p \setminus \{0\}, \times)$, $|G| = p - 1$, тогда по следствию 3:

$$\forall \overline{a} \in \mathbb{Z}_p^{\times},\ \overline{a}^{p-1} = \overline{1} \Rightarrow \overline{a}^p = \overline{a} \cdot \overline{a}^{p-1} = \overline{a} \cdot \overline{1} = \overline{a}$$

Но это будет выполнено и для $0 \Rightarrow$ равенство выше верно $\forall \overline{a} \in \mathbb{Z}_p$. ■

Следствие 5. Пусть p - простое число, $|G| = p \Rightarrow G$ это циклическая группа, порождается любым неединичным элементом. Более точно: $G \simeq \mathbb{Z}_p$, в частности, G коммутативна.

$\square$ По следствию 2:

$$\forall g \in G \setminus \{e\},\ |G| = p \,\vdots\, |\langle g \rangle| \Rightarrow |\langle g \rangle| \in \{1, p\}$$

Но $|\langle g \rangle| \geq 2$, так как $e \neq g$, $e \in \langle g \rangle$, $g \in \langle g \rangle \Rightarrow |\langle g \rangle| = p \Rightarrow \langle g \rangle = G$. Коммутативность следует из коммутативности цикличных групп (циклические группы всегда коммутативны). ■

Из теоремы Лагранжа также можно доказать для конечных групп равенство числа левых смежных классов и правых смежных классов, поскольку:

$$|gH| = |H| = |Hg| \Rightarrow \frac{|G|}{|gH|} = \frac{|G|}{|H|} = \frac{|G|}{|Hg|}$$

Также отметим, что при этом разбиение на левые смежные классы и правые смежные классы могут не совпадать, но если G - абелева, то $gH = Hg$, $\forall g \in G$.

Пример несовпадения левых и правых смежных классов: Рассмотрим $G = S_3$, $|G| = 6$ - это самая маленькая неабелева группа.

Рассмотрим подгруппу: $H = A_3$ это группа всех четных подстановок (все циклы длины 3 без транспозиций) в ней совпадут левые и правые смежные классы, поскольку $(G \colon H) = 2$, так как $|G| = 6$, а четных подстановок в ней 3. Поскольку A_3 - всегда смежный класс единицы (и левый, и правый), то:

1) Левый смежный класс: Половина чётные, половина нечётные;
2) Правый смежный класс: Тоже самое - всего два класса: половина чётные, половина нечётные;

Рассмотрим подгруппу: $H = \langle (12) \rangle = \left\{ e, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$, тогда её смежные классы будут устроены так:

1) Левые: $H = \{e, (12)\}$, $g = (13)$, $(13)(12) = (123)$; $g = (23)$, $(23)(12) = (132)$;
2) Правые: $H = \{e, (12)\}$, $g = (13)$, $(12)(13) = (132)$; $g = (23)$, $(12)(23) = (123)$;

Упр. 4. Обратное утверждение к теореме Лагранжа не верно: пусть G - конечная группа и d - делитель числа $|G|$. Тогда в группе G есть подгруппа H у которой порядок равен d, то есть $|H| = d$. Привести контрпример.