

1 Подгруппы, смежные классы, порядок и индекс подгруппы

Определение 1.1 (Подгруппа). Подгруппа - подмножество H группы G , само являющееся группой относительно операции, определяющей G
Подгруппа - подалгебра в группе

Следствие 1.2. Подгруппа является группой

Определение 1.3 (Тривиальная подгруппа). Тривиальная подгруппа - подгруппа, состоящая только из одного нейтрального элемента группы или равна самой группе

Пример 1.4 (Пример подгрупп).

Пример 1.5. $(\mathbb{Z}_p; +, 0, -)$, p - простое число
В этой группе нет нетривиальных подгрупп

ДОКАЗАТЕЛЬСТВО. $A \subseteq \mathbb{Z}_p$, $x \in A$, $x, 2x, 3x, \dots, px$ - все разные
предположим, что $ix = jx (i < j)$, тогда $jx - ix = 0 \Rightarrow (j - i)x = 0$
 $(j - i)x \bmod p = 0$
 $(j - i) \bmod p = 0$
 $j - i = 0$ ПОЧЕМУ
 $j = i$
 $A = \mathbb{Z}_p$

□

Теорема 1.6. Любая бесконечная группа имеет нетривиальную подгруппу

ДОКАЗАТЕЛЬСТВО. Пусть $a \in G$, $a \neq e$, тогда
 $A = \{a^0 = e, a^1, a^2, \dots, a^{-1}, a^{-2}, \dots\}$

1. $A \neq G$ A - нетривиальная подгруппа
2. $A = G$ $A' = \{a^0, a^2, a^4, \dots, a^{-2}, a^{-4}, \dots\}$

□

Пример 1.7 (Пример подгрупп). Возьмём группу из ?? и выпишем подгруппы:

1. $\{e\}$ - тривиальная подгруппа

2. $\{e, r_1, r_2, s_1, s_2, s_3\}$ - тривиальная подгруппа

3. $\{e, r_1, r_2\}$

4. $\{e, s_1\}, \{e, s_2\}, \{e, s_3\}$

Пример 1.8. Группа операций над треугольником - подгруппа

Пример 1.9. Является ли группой моноид $(\mathcal{A}; \cap, e)$, где \mathcal{A} - множество фигур на плоскости, e - вся плоскость.

ДОКАЗАТЕЛЬСТВО. $A \cap A^{-1} = e$, этого не может быть, $(\mathcal{A}; \cap, e)$ - не группа \square

Является ли группой алгебра $(\mathcal{A}; \div)$, где \mathcal{A} - множество фигур на плоскости.

ДОКАЗАТЕЛЬСТВО. Сперва докажем ассоциативность \div : $A \div (B \div C) = (A \div B) \div C$

$$A \div B = (\overline{A} \cap B) \cup (\overline{B} \cap A)$$

$$A \div (B \div C) = (\overline{A} \cap (B \div C)) \cup (A \cap (\overline{B \div C})) =$$

$$(\overline{A} \cap ((\overline{B} \cap C) \cup (\overline{C} \cap B))) \cup (A \cap (\overline{(\overline{B} \cap C) \cup (\overline{C} \cap B)})) =$$

$$(\overline{A} \cap ((\overline{B} \cap C) \cup (\overline{C} \cap B))) \cup (A \cap ((\overline{\overline{B} \cap C}) \cap \overline{\overline{C} \cap B})) =$$

$$(\overline{A} \cap ((\overline{B} \cap C) \cup (\overline{C} \cap B))) \cup (A \cap ((B \cup \overline{C}) \cap (C \cup \overline{B}))) =$$

$$(\overline{A} \cap \overline{B} \cap C) \cup (\overline{A} \cap B \cap \overline{C}) \cup (A \cap ((B \cup \overline{C}) \cap (C \cup \overline{B}))) =$$

$$(\overline{A} \cap \overline{B} \cap C) \cup (\overline{A} \cap B \cap \overline{C}) \cup (A \cap B \cap \overline{B}) \cup (A \cap B \cap C) \cup (A \cap \overline{B} \cap \overline{C}) \cup (A \cap \overline{C} \cap C) =$$

$$(\overline{A} \cap \overline{B} \cap C) \cup (\overline{A} \cap B \cap \overline{C}) \cup (A \cap B \cap C) \cup (A \cap \overline{B} \cap \overline{C})$$

$$(A \div B) \div C = C \div (A \div B) = \dots =$$

$$(\overline{C} \cap \overline{B} \cap A) \cup (\overline{C} \cap B \cap \overline{A}) \cup (C \cap B \cap A) \cup (C \cap \overline{B} \cap \overline{A})$$

$$A \div (B \div C) = (A \div B) \div C$$

теперь доказать существование обратного

Пусть $e = \emptyset$, Тогда $A \div \emptyset = A$

$$A \div A^{-1} = \emptyset \Rightarrow (\overline{A} \cap A^{-1}) \cup (\overline{A^{-1}} \cap A) = \emptyset \Rightarrow A^{-1} = A$$

$(\mathcal{A}; \div)$ - группа \square

Таблица умножения *

	e
e	e

Пример 1.10. Конечные группы

1. $\mathcal{G}_1 = (\{e\}; *)$

2. $\mathcal{G}_2 = (\{e, a\}; *)$

Таблица умножения *

	e	a
e	e	a
a	a	e

3. $\mathcal{G}_3 = (\{e, a, b\}; *)$

Таблица умножения *

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

4. $\mathcal{A} = (\{e, a, b, c\}, *)$

Пример 1.11. Построить группу симметрии правильного n -угольника (Диэдрическая группа)

$\mathcal{D}_n = (r_0, \dots, r_{n-1}, s_1, \dots, s_n; \circ, e, {}^{-1})$, где r_0, \dots, r_{n-1} - повороты, s_1, \dots, s_n - отражения, эти элементы множества являются автоморфизмами, композиция задана следующей таблицей умножения:

Таблица умножения $*$

	e	a	b	c
e	e	a	b	c
a	a	e	b	c
b	b	c	e	a
c	c	b	a	e

Таблица умножения \circ

	r_i	s_i
r_j	$r_{(i+j) \bmod n}$	$s_{(i+j) \bmod n}$
s_j	$s_{(j-i) \bmod n}$	$r_{(i-j) \bmod n}$

нейтральным элементом является r_0 , обратным к любому отражению s_i само отражение s_i , обратным к повороту r_i поворот r_{n-i}

Определение 1.12 (Рекурсивная перестановка). Рекурсивная перестановка - однозначная общерекурсивная функция, область значений которой - множество ω

Теорема 1.13. Рекурсивные перестановки с операцией композиции образуют группу

ДОКАЗАТЕЛЬСТВО. Надо доказать ассоциативность \circ , существование нейтрального и обратных

1. $a \in \omega$, $a = g(b)$, $b = f(c)$, $a = g(f(c)) = (f \circ g)(c)$, \circ ассоциативна
2. $e = \text{Id}_1^1$, $(f \circ e)(a) = e(f(a)) = f(a)$
3. $f^{-1} =$

□

Теорема 1.14. Любая группа вкладывается в группу перестановок

ДОКАЗАТЕЛЬСТВО. Пусть $\mathcal{G} = (G, *)$, S - множество перестановок G , надо доказать

$$h(x * y) = h(x) \circ h(y)$$

Пусть $h(x) = f_x$, такой что $f_x(y) = y * x$ (А существует ли f_x для каждого x ?). h однозначна, так как $f_x(e) = f_y(e) \Rightarrow ex = ey \Rightarrow x = y$,

$$\begin{aligned} h(x * y)(a) &= f_{x*y}(a) = a * (x * y) = (a * x) * y = f_x(a) * y = f_y(f_x(a)) = \\ &= (f_x \circ f_y)(a) = (h(x) \circ h(y))(a) \end{aligned}$$

□

Теорема 1.15. *Любой конечный моноид, в котором нет неединичных идемпотентов является группой*

ДОКАЗАТЕЛЬСТВО. Пусть M - конечный моноид, $a \in M$, $a * a^{-1} = e$

Индукция по количеству элементов

Базис: $n = 1$, $a = e$, $M = \{e\}$

Шаг индукции: пусть для моноидов с $k < n$ верно. Тогда для $k = n$

Пусть $a \in M$, A - циклический моноид, порождённый a

1. $A \neq M$, $|A| < n$, по индукционному предположению
2. $A = M$, так как M не содержит неединичных идемпотентов, то A - это моноид типа $(0, n)$

$$a^x a^y = \begin{cases} a^{x+y} & , \text{если } x + y < n, y < n - 1 \\ a^{j+(x+y-i)} & , \text{если } x + y \geq n \end{cases}$$

следовательно $a^x a^y = a^{(x+y) \bmod n}$ и $a^{-1} = a^{n-1}$

□

Пример 1.16. *Построить группу симметричную чему-то там*

Теорема 1.17. *Любая чётная перестановка является произведением циклов длины 3*

ДОКАЗАТЕЛЬСТВО. Любую чётную перестановку можно разложить в произведение циклов длины 2. Таких циклов будет чётное число, соответственно будет n произведений циклов вида $(ab)(cd)$

1. $b = c$, тогда $(ab)(cd) = (abd)$
2. $b \neq c$, тогда $(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)$

□

Теорема 1.18. Если \mathcal{G} - группа, $\mathcal{H} \subseteq \mathcal{G}$, $\mathcal{H} \neq \emptyset$, $a, b \in \mathcal{H} \rightarrow ab^{-1} \in \mathcal{H}$, тогда \mathcal{H} является подгруппой

ДОКАЗАТЕЛЬСТВО. Пусть $a, b \in H$

1. $H \neq \emptyset$, $a \in H \Rightarrow aa^{-1} \in H \Rightarrow e \in H$ есть нейтральный элемент
2. $a \in H \Rightarrow ea^{-1} \in H \Rightarrow a^{-1} \in H$, есть обратные
3. $a, b \in H$, $b^{-1} \in H \Rightarrow a(b^{-1})^{-1} \in H \Rightarrow ab \in H$, замкнуто по операции группы \mathcal{G}
 \mathcal{H} - подгруппа

□

Определение 1.19 (Центр группы). Центр группы - $\mathcal{Z} = \{a \in G, ab = ba \text{ для всех } b \in G\}$

Пример 1.20. $\mathcal{M} = (M_2^*(\mathbb{R}); \cdot)$, невырожденные матрицы

$$\mathcal{Z} = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R} \right\}$$

Теорема 1.21. Центр группы - подгруппа

ДОКАЗАТЕЛЬСТВО. $a, b \in \mathcal{Z}$, $ab^{-1} \in \mathcal{Z}$

Надо доказать: $x \in \mathcal{G}$, $(ab^{-1})x = x(ab^{-1})$

$$(ab^{-1})x = ab^{-1}xe = ab^{-1}xbb^{-1} = ab^{-1}bxb^{-1} = axb^{-1} = x(ab)^{-1}$$

следует что $x \in \mathcal{Z}$ (что это вообще доказывает)

□

Определение 1.22 (Циклическая группа). Циклическая группа - группа, порождённая одним элементом. $\langle a \rangle$ - циклическая группа порождённая a .

$(\omega, +, 0)$ изоморфно бесконечной циклической группе
 моноид типа (i, j) изоморфен конечной циклической группе

Теорема 1.23. $\mathcal{G} = \langle a \rangle$, тогда $\mathcal{G} \cong (\mathbb{Z}, +)$ или $\mathcal{G} \cong (\mathbb{Z}_n, +)$ для некоторого n

ДОКАЗАТЕЛЬСТВО. Пусть \mathcal{M} - подмоноид, порождённый a . M - циклический

$$1. \mathcal{M} \cong (\omega, +, 0)$$

$$x \in \mathcal{M} \quad x^{-1} x x^{-1} = e$$

$$x \in \mathcal{M} \quad x \neq e \quad x^{-1} \neq \mathcal{M}$$

$$0 = h(x) + h(x^{-1}) = h(xx^{-1}) = h(e) = 0$$

Доказать что изоморфизм

2. \mathcal{M} - конечный (i, j) моноид, если $i > 0$, то в \mathcal{M} есть неединичный идемпотент, следовательно он необратимый, следовательно в группе должно быть $i = 0$

$$a^x a^y = \begin{cases} a^{x+y} & , \text{если } x + y < j \\ a^{(x+y) \pmod j} & , \text{если } x + y \geq j \end{cases}$$

\mathcal{M} - группа

$$a^x = a^{j-x} = a^j \pmod j = e$$

\mathcal{M} - группа порождённая a , $\mathcal{M} = \mathcal{G}$

$$h : a^x \rightarrow x$$

□

Теорема 1.24. В циклической группе существуют нетривиальные группы тогда и только тогда когда она бесконечна или n в $(\mathbb{Z}_n, +)$ составное

ДОКАЗАТЕЛЬСТВО. 1. \Rightarrow пусть имеется $(\mathbb{Z}_n, +)$, n - простое, $a \neq 0$, $a < n$, a и n взаимно простые, следовательно $xa + yn = 1$. пусть $b \in \mathbb{Z}$, тогда

$$b = b \cdot 1 = b(ax + yn) = (bx)a + (by)n$$

$$\underbrace{(a + a + \dots + a)}_{bx} \pmod n = (b - (by)n) \pmod n = b \pmod n = b$$

Таким (КАКИМ) образом любые подгруппы, содержащие не только 0 содержат \mathbb{Z}_n

2. \Leftarrow

(а) бесконечная циклическая группа имеет нетривиальную подгруппу

(b) пусть $n = xy$, тогда $(\mathbb{Z}_{xy}, +) \supseteq \{0, x, 2x, \dots, (y-1)x\}$

□

Определение 1.25 (Порядок группы). Порядок группы - количество элементов группы. $\text{ord} \mathcal{G}$

Определение 1.26 (Порядок элемента). Порядок элемента - порядок порождённой им циклической подгруппы $\text{orda} = \text{ord} \langle a \rangle$

Пример 1.27. *Пример на порядок через группу треугольника*

$$\mathcal{D}_3 = \{e, r_1, r_2, s_1, s_2, s_3\}$$

$$\text{ord } \mathcal{D}_3 = 6$$

$\langle r_0 \rangle = \{r_0\}$	$\text{ord } r_0 = 1$
$\langle r_1 \rangle = \{r_0, r_1, r_2\}$	$\text{ord } r_1 = 3$
$\langle r_2 \rangle = \{r_0, r_1, r_2\}$	$\text{ord } r_2 = 3$
$\langle s_1 \rangle = \{r_0, s_1\}$	$\text{ord } s_1 = 2$
$\langle s_2 \rangle = \{r_0, s_2\}$	$\text{ord } s_2 = 2$
$\langle s_3 \rangle = \{r_0, s_3\}$	$\text{ord } s_3 = 2$

Следствие 1.28. $\text{ord } e = 1$, $\langle e \rangle = \{e\}$

Определение 1.29 (Смежный класс). Пусть \mathcal{G} - группа, $\mathcal{H} \subseteq \mathcal{G}$, $a \in \mathcal{G}$
 Левый смежный класс a по \mathcal{H} - $a\mathcal{H} = \{ab : b \in \mathcal{H}\}$
 Правый смежный класс a по \mathcal{H} - $\mathcal{H}a = \{ba : b \in \mathcal{H}\}$

Пример 1.30. *Пример смежных классов:*

$$\langle s_1 \rangle \subseteq \mathcal{D}_3, r_1 \in \mathcal{D}_3$$

$$r_1 \langle s_1 \rangle = r_1 \{r_0, s_1\} = \{r_1, s_2\}$$

$$\langle s_1 \rangle r_1 = \{r_0, s_1\} r_1 = \{r_1, s_3\}$$

$$r_1 \langle s_1 \rangle \neq \langle s_1 \rangle r_1$$

Определение 1.31 (Нормальная подгруппа). Нормальная подгруппа - подгруппа, у которой любой левый смежный класс совпадает с правым

Пример 1.32. *Пример нормальных групп*

$$\langle r_1 \rangle = \{r_0, r_1, r_2\} \subseteq \mathcal{D}_3$$

$$r_i \langle r_1 \rangle = r_i \{r_0, r_1, r_2\} = \{r_{0+i}, r_{1+i}, r_{2+i}\} = \langle r_1 \rangle$$

$$\langle r_1 \rangle r_i = \{r_0, r_1, r_2\} r_i = \{r_{0+i}, r_{1+i}, r_{2+i}\} = \langle r_1 \rangle$$

$$r_i \langle r_1 \rangle = \langle r_1 \rangle r_i$$

$$s_i \langle r_1 \rangle = \{s_i r_0, s_i r_1, s_i r_2\} = \{s_i, s_{i-1}, s_{i+1}\}$$

$$\langle r_1 \rangle s_i = \{r_0 s_i, r_1 s_i, r_2 s_i\} = \{s_i, s_{i+1}, s_{i-1}\}$$

$$s_i \langle r_1 \rangle = \langle r_1 \rangle s_i$$

$\langle r_1 \rangle$ - нормальная подгруппа

Теорема 1.33. *Если \mathcal{G} - группа, $\mathcal{H} \subseteq \mathcal{G}$, \equiv - отношение принадлежности к одному левому смежному классу, то \equiv - отношение эквивалентности*

Доказательство. 1. Рефлексивность $a \in a\mathcal{H} \Rightarrow a \equiv a$

2. Симметричность $a \equiv b \Rightarrow a \in x\mathcal{H}, b \in x\mathcal{H} \Rightarrow b \equiv a$

3. Транзитивность $a \equiv b, b \equiv c \Rightarrow$

$$\begin{array}{lll} a, b \in x\mathcal{H} & a = xh_a & b = xh_b \\ b, c \in y\mathcal{H} & b = yh'_b & c = yh_c \end{array}$$

$$xh_b = yh'_b \Rightarrow x = yh'_b h_b^{-1} \Rightarrow a = y \underbrace{h'_b h_b^{-1} h_a}_{\mathcal{H}}$$

$$\left. \begin{array}{l} c \in y\mathcal{H} \\ a \in y\mathcal{H} \end{array} \right\} a \equiv c$$

□

Следствие 1.34. *Каждый левый смежный класс является классом эквивалентности*

Следствие 1.35. *Левые смежные классы или совпадают или не пересекаются*

Следствие 1.36. *Количество элементов в левом смежном классе совпадает с $\text{ord } \mathcal{H}$*

ДОКАЗАТЕЛЬСТВО. Пусть $f : \mathcal{H} \rightarrow a\mathcal{H}$, $f(x) = ax$, тогда

$$f(x) = f(y) \Rightarrow ax = ay \Rightarrow a^{-1}ax = a^{-1}ay \Rightarrow x = y$$

f - взаимнооднозначная функция, соответственно $\text{ord } a\mathcal{H} = \text{ord } \mathcal{H}$ □

Определение 1.37 (Индекс подгруппы). Индекс подгруппы - количество левых смежных классов $\text{ind } H$

Теорема 1.38. Если H - подгруппа G , то $\text{ord } G = \text{ord } H \cdot \text{ind } H$

ДОКАЗАТЕЛЬСТВО. Разобьём группу G на левые смежные классы. Их количество - $\text{ind } H$, каждый содержит $\text{ord } H$ элементов. Общее количество этих элементов - $\text{ind } H \cdot \text{ord } H$ □

Следствие 1.39. $\text{ind } H = \frac{\text{ord } G}{\text{ord } H}$

Следствие 1.40. $\text{ord } H \mid \text{ord } G$

Следствие 1.41. $\text{ord } a \mid \text{ord } \mathcal{G}$

ДОКАЗАТЕЛЬСТВО. $\mathcal{H} = \langle a \rangle$, $\text{ord } a = \text{ord } \mathcal{H}$ □

Теорема 1.42. $a^{\text{ord } a} = e$

ДОКАЗАТЕЛЬСТВО. $\langle a \rangle = \underbrace{\{a^0, a^1, \dots, a^{\text{ord } a - 1}\}}_{\text{ord } a}$, $a^{\text{ord } a} = a^0 = e$ □

Теорема 1.43. $a^n = e \Leftrightarrow \text{ord } a \mid n$

ДОКАЗАТЕЛЬСТВО. Пусть $x = \text{ord } a + r = n$, ($0 \leq r < \text{ord } a$), тогда

$$e = a^n = a^{x + r} = a^x \cdot a^r = (a^{\text{ord } a})^x \cdot a^r = e^x \cdot a^r = a^r$$

$$a^r = e \Rightarrow r = 0 \Rightarrow n = x \cdot \text{ord } a \Rightarrow \text{ord } a \mid n$$

□

Теорема 1.44. $a^{\text{ord } G} = e$

ДОКАЗАТЕЛЬСТВО. $\text{ord } a \mid \text{ord } \mathcal{G} \Rightarrow \text{ord } \mathcal{G} = x \cdot \text{ord } a \Rightarrow a^{\text{ord } \mathcal{G}} = (a^{\text{ord } a})^x = e$ □

Пример 1.45. A_5 - группа чётных перестановок из 5 элементов. В A_5 нет нормальных подгрупп

Доказательство. ДОКАЖИ ДОМА))))))))))))))

□

Теорема 1.46. Любая подгруппа индекса 2 является нормальной

Доказательство. 1. (a) $e\mathcal{H} = \mathcal{H}$

$$\begin{aligned} \text{(b) } a\mathcal{H} &\neq \mathcal{H} \\ a\mathcal{H} &= \mathcal{G}/\mathcal{H} \end{aligned}$$

2. (a) $\mathcal{H}e = \mathcal{H}$

$$\begin{aligned} \text{(b) } \mathcal{H}a &\neq \mathcal{H} \\ \mathcal{H}a &= \mathcal{G}/\mathcal{H} \end{aligned}$$

Что и зачем

□