

Лекция 10. Подгруппы, смежные классы, индекс подгруппы в группе. Теорема Лагранжа о порядке конечной группы. Нормальные подгруппы, фактор-группа. Орбита и стабилизатор элемента, теорема о порядке стабилизатора элемента. Лемма Бернсайда.

Лектор - доцент Селезнева Светлана Николаевна

Лекции по "Избранным вопросам дискретной математики".
3-й курс, группа 318,
факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте <http://mathcyb.cs.msu.su>

Смежные классы

Пусть $G = (S; *)$ – группа, а $H = (T; *)$, $T \subseteq S$, – ее подгруппа. Определим на множестве S бинарное отношение R_H : если $a, b \in S$, то

$$aR_H b \Leftrightarrow \exists h \in H : a * h = b.$$

Заметим, что отношение R_H можно задавать так: если $a, b \in S$, то

$$aR_H b \Leftrightarrow a' * b \in H,$$

где элемент a' симметричен элементу a в группе G .

Отношение эквивалентности по подгруппе

Теорема 1. *Отношение R_H является отношением эквивалентности на множестве S .*

Доказательство. Свойства отношения эквивалентности.

1) Рефлексивность. Для каждого $a \in S$ выберем $e \in H$ – нейтральный элемент. Тогда $a * e = a$, поэтому $aR_H a$.

2) Симметричность. Пусть для элементов $a, b \in S$ верно $aR_H b$, т.е. найдется такой элемент $h \in H$, что $a * h = b$. Тогда

$$a * h = b, a * h * h' = b * h', a = b * h'.$$

Т.к. H – группа, $h' \in H$. Откуда $bR_H a$.

3) Транзитивность. Пусть для элементов $a, b, c \in S$ верно $aR_H b$ и $bR_H c$, т.е. найдутся такие элементы $h_1 \in H$ и $h_2 \in H$, что $a * h_1 = b$ и $b * h_2 = c$. Тогда

$$a * (h_1 * h_2) = (a * h_1) * h_2 = b * h_2 = c.$$

Т.к. H – группа, $h_1 * h_2 = h \in H$. Откуда $aR_H c$.

Смежные классы

Класс эквивалентности множества S по отношению эквивалентности R_H называется **левым смежным классом** группы G по подгруппе H .

Обозначение: левый смежный класс, порожденный элементом $a \in S$:

$$aH = \{b \in S \mid \exists h \in H : a * h = b\}.$$

В аддитивной символике обозначение:

$$a + H = \{b \in S \mid \exists h \in H : a + h = b\}.$$

Напомним, что классы эквивалентности или не пересекаются, или совпадают. Поэтому отношение R_H **разбивает** множество S на левые смежные классы. Такое разбиение называется **левосторонним разложением** группы G по подгруппе H .

Аналогично вводится **правостороннее разложение** группы G по подгруппе H .

Смежные классы

Пусть $H = \{h_1 = e, h_2, \dots, h_m\}$ – конечная подгруппа группы $G = (S; *)$.

Тогда для каждого элемента $a \in S$ левый смежный класс

$$aH = \{a * h_1, a * h_2, \dots, a * h_m\}$$

также содержит конечное число элементов.

Пример. Найдём левостороннее разложение симметрической группы перестановок S_3 по подгруппе H вращений правильного треугольника в плоскости.

Напомним, подгруппа

$$H = \{e = (1)(2)(3), (123), (132)\}.$$

Тогда

$$eH = H = \{e = (1)(2)(3), (123), (132)\};$$

$$(1)(23)H = \{(1)(23), (12)(3), (13)(2)\}.$$

Смежные классы

Теорема 2. В каждом левом (правом) смежном классе группы по конечной подгруппе число элементов совпадает с порядком этой подгруппы.

Доказательство. Пусть $H = \{h_1 = e, h_2, \dots, h_m\}$ – конечная подгруппа группы $G = (S; *)$.

Тогда для элемента $a \in S$ левый смежный класс aH состоит из элементов вида

$$a * h_1, a * h_2, \dots, a * h_m.$$

Поэтому $|aH| \leq |H|$.

Предположим, что $|aH| < |H|$. Т.е. найдутся такие элементы $h_i, h_j \in H$, $h_i \neq h_j$, что

$$a * h_i = a * h_j.$$

Тогда по правилу сокращения $h_i = h_j$ – противоречие.
Следовательно, $|aH| = |H|$.

Теорема Лагранжа

Следствие 2.1. (теорема Лагранжа) *Порядок каждой подгруппы конечной группы делит порядок группы.*

Доказательство. Пусть $G = (S; *)$ – конечная группа, а H – ее подгруппа. Рассмотрим левостороннее разложение группы G по подгруппе H . Тогда по теореме 2 все левые смежные классы равномощны, и их мощность равна порядку подгруппы H . Каждый элемент множества S лежит ровно в одном левом смежном классе, поэтому

$$|G| = |H| \cdot \{\text{число левых смежных классов}\}.$$

Откуда $|H| \mid |G|$.



Порядок элемента конечной группы

Следствие 2.2. *Порядок каждого элемента конечной группы делит порядок группы.*

Доказательство. Пусть $G = (S; *)$ – конечная группа, и $a \in S$ – какой-то ее элемент. Достаточно рассмотреть циклическую ее подгруппу $H = \langle a \rangle$ с образующим элементом $a \in S$. Тогда порядок элемента a равен порядку группы H , и по следствию 2.1 делит порядок группы G .

□

Индекс подгруппы в группе

Число смежных классов конечной группы G по подгруппе называется **индексом подгруппы H в группе G** и обозначается как $(G : H)$.

Следствие 2.3. *Порядок конечной группы равен произведению порядка какой-то ее подгруппы на индекс этой подгруппы в группе, т.е.*

$$|G| = |H| \cdot (G : H),$$

где G – конечная группа, а H – ее подгруппа.

Пример: все неизоморфные группы из 5 элементов

Пример. Найдем все возможные группы из 5 элементов (с точностью до изоморфизма).

Решение. Пусть $|S| = 5$, и $G = (S; *)$ – группа.

Если $a \in S$, то (по следствию 2.2) порядок элемента a делит порядок группы, т.е. делит 5.

Т.е. каждый элемент этой группы имеет порядок или 1, или 5.

Но порядок 1 может иметь только нейтральный элемент e .

Значит, все другие элементы имеют порядок 5. Т.е. эта группа циклическая, и

$$S = \{a, a^2, a^3, a^4, a^5 = e\}.$$

Следовательно, с точностью до изоморфизма существует только **одна** группа из 5 элементов, и она является циклической.

Несложно заметить, что это группа вращений правильного пятиугольника в плоскости.

Нормальные подгруппы

Пусть $G = (S; *)$ – группа, а $H = (T; *)$, $T \subseteq S$, – ее подгруппа.

Подгруппа H называется **нормальной подгруппой** (или **нормальным делителем**) группы G , если для каждого элемента $a \in S$ его левые и правые смежные классы совпадают, т.е. если

$$\forall a \in S \ aH = Ha.$$

Заметим, что каждая подгруппа абелевой группы нормальна.

Если подгруппа H нормальна в группе G , то левостороннее и правостороннее разложения группы G по подгруппе H совпадают.

Критерий нормальности подгруппы

Теорема 3. Подгруппа $H = (T; *)$ является нормальной подгруппой группы $G = (S, *)$ тогда и только тогда, когда для каждого элемента $a \in S$ для любого элемента $h \in H$ верно, что

$$a' * h * a \in H,$$

где элемент a' симметричен элементу a в группе G .

Критерий нормальности подгруппы

Доказательство.

\Rightarrow . Если для каждого элемента $a \in S$ верно $aH = Ha$, то для любого элемента $h \in H$ найдется такой элемент $h_1 \in H$, что

$$a * h_1 = h * a.$$

Откуда

$$a' * (a * h_1) = a' * (h * a), \quad h_1 = a' * h * a.$$

Т.е. $a' * h * a \in H$.

Критерий нормальности подгруппы

Доказательство.

\Leftarrow . Если для каждого элемента $a \in S$ для любого элемента $h \in H$ верно $a' * h * a \in H$, то

$$a' * h * a = h_1 \in H.$$

Откуда

$$a * (a' * h * a) = a * h_1, \quad h * a = a * h_1.$$

Т.е. $Ha \subseteq aH$.

Включение $aH \subseteq Ha$ доказывается аналогично, рассматривая произведение $(a')' * h * a'$, $a' \in S$.

Поэтому, $aH = Ha$.

□

Нормальные подгруппы в S_n

Пример. Докажем, что группа H вращений правильного треугольника в плоскости является нормальной подгруппой группы S_3 .

Напомним, что группа

$$S_3 = \{e = (1)(2)(3), (1)(23), (12)(3), (13)(2), (123), (132)\},$$

и подгруппа H

$$H = \{(1)(2)(3), (123), (132)\}.$$

Тогда

$$eH = H = \{(1)(2)(3), (123), (132)\} = He,$$

и

$$(1)(23)H = \{(1)(23), (12)(3), (13)(2)\} = H(1)(23).$$

Т.е. подгруппа H – нормальная подгруппа группы S_3 .

Фактор-группа

Пусть $G = (S; *)$ – группа, и $N = (T; *)$ – ее **нормальная** подгруппа.

Рассмотрим разложение группы G по нормальной подгруппе N .

Введем операцию умножения смежных классов: если элементы $a, b \in S$, то

$$(aN)(bN) = (ab)N.$$

Фактор-группа

Теорема 4. Если N – нормальная подгруппа группы $G = (S; *)$, то введенная выше операция умножения смежных классов корректна.

Доказательство. Если элементы $a, b \in S$, то

$$(aN)(bN) = \{a*h_1 \mid h_1 \in N\}\{b*h_2 \mid h_2 \in N\} = \{a*h_1*b*h_2 \mid h_1, h_2 \in N\}$$

Т.к. N – нормальная подгруппа группы G , то $b * N = N * b$.

Откуда, найдется такой элемент $h_3 \in N$, что

$$h_1 * b = b * h_3.$$

Тогда

$$(aN)(bN) = \{a*b*h_3*h_2 \mid h_1, h_2 \in N\} = \{a*b*h \mid h \in N\} = (ab)N.$$



Фактор-группа

Теорема 5. Если N – нормальная подгруппа группы $G = (S; *)$, то множество смежных классов группы G по подгруппе N с операцией их умножения образует группу.

Доказательство. Свойства группы.

- 1) Ассоциативность операции умножения – следует из ассоциативности операции $*$ в группе G .
- 2) Существование нейтрального элемента – $eN = N$, где $e \in S$ – нейтральный элемент группы G .
- 3) Для каждого элемента aN , где $a \in S$, существование симметричного элемента – $a'N$, где элемент $a' \in S$ симметричен элементу a в группе G .

□

Группа смежных классов группы G по нормальной ее подгруппе N с операцией их умножения называется **фактор-группой** группы G по подгруппе N и обозначается G/N .

Фактор-группа

Теорема 5. *Порядок фактор-группы G/N конечной группы G по нормальной ее подгруппе N равен индексу подгруппы N в группе G , т.е.*

$$|G/N| = (G : N) = \frac{|G|}{|N|}.$$

Фактор-группа

Пример. Найдем фактор-группу S_3/H группы S_3 по нормальной подгруппе H вращений правильного треугольника в плоскости.

Тогда фактор-группа

$$S_3/H = (\{eH, (1)(23)H\}, \cdot),$$

где

$$eH = H = \{(1)(2)(3), (123), (132)\},$$

и

$$(1)(23)H = \{(1)(23), (12)(3), (13)(2)\}.$$

В фактор-группе S_3/H верно

$$\begin{aligned} eH \cdot X &= X \cdot eH = X, \text{ при } X = eH, (1)(23)H; \\ (1)(23)H \cdot (1)(23)H &= eH. \end{aligned}$$

Т.е. фактор-группа S_3/H изоморфна группе S_2 .

Эквивалентность по группе перестановок

Пусть G – подгруппа симметрической группы перестановок S_n .
Напомним, что $N = \{1, 2, \dots, n\}$.

Определим бинарное отношение R_G на множестве N : если $a, b \in N$, то

$$aR_G b \Leftrightarrow \exists \pi \in G : \pi(a) = b.$$

Эквивалентность по группе перестановок

Теорема 6. *Отношение R_G является отношением эквивалентности на множестве N .*

Доказательство. Свойства отношения эквивалентности.

1) Рефлексивность. Для каждого элемента $a \in N$ выберем $\pi_1 = e \in G$ – тождественную перестановку. Тогда $\pi_1(a) = a$, поэтому $aR_G a$.

2) Симметричность. Пусть для элементов $a, b \in N$ верно $aR_G b$, т.е. найдется такая перестановка $\pi \in G$, что $\pi(a) = b$. Тогда

$$\pi(a) = b, \pi^{-1}(\pi(a)) = \pi^{-1}(b), a = \pi^{-1}(b).$$

Т.к. G – группа, $\pi^{-1} \in G$, откуда $bR_G a$.

3) Транзитивность. Пусть для элементов $a, b, c \in N$ верно $aR_G b$ и $bR_G c$, т.е. найдутся такие перестановки $\pi_1 \in G$ и $\pi_2 \in G$, что $\pi_1(a) = b$ и $\pi_2(b) = c$. Тогда

$$(\pi_1 \circ \pi_2)(a) = \pi_2(\pi_1(a)) = \pi_2(b) = c.$$

Т.к. G – группа, $\pi_1 \circ \pi_2 = \pi \in G$, откуда $aR_G c$.

Эквивалентность по группе перестановок

Пусть G – подгруппа симметрической группы перестановок S_n .

Отношение эквивалентности R_G обозначается как \sim_G .

Если для элементов $a, b \in N$ верно $a \sim_G b$, то говорят, что элементы a и b эквивалентны по группе G (или относительно группы G).

Орбита элемента

Пусть $G = \{\pi_1 = e, \pi_2, \dots, \pi_m\}$ – подгруппа симметрической группы перестановок S_n .

Для элемента $a \in N$ его **орбитой** (в группе G) называется порожденный им класс эквивалентности по отношению \sim_G .

Обозначение:

$$O_a = \{b \in N \mid \exists \pi \in G : \pi(a) = b\},$$

или

$$O_a = \{\pi_1(a) = a, \pi_2(a), \dots, \pi_m(a)\}.$$

Пример: вращения правильного треугольника в плоскости

Пример. Пусть $N = \{1, 2, 3\}$, и $H = \{\pi_1 = e = (1)(2)(3), \pi_2 = (123), \pi_3 = (132)\}$ – группа вращений правильного треугольника в плоскости. Группа G является подгруппой симметрической группы перестановок S_3 .

Найдем орбиту элемента $1 \in N$ в группе H :

$$O_1 = \{\pi_1(1), \pi_2(1), \pi_3(1)\} = \{1, 2, 3\}.$$

Другими словами, перестановками группы H элемент 1 может быть переведен в любой другой элемент множества N .

Т.е. вращениями правильного треугольника в плоскости вершина 1 может перейти в любую другую его вершину.

Стабилизатор элемента

Пусть $G = \{\pi_1 = e, \pi_2, \dots, \pi_m\}$ – подгруппа симметрической группы перестановок S_n .

Для элемента $a \in N$ его **стабилизатором** (в группе G) называется подмножество перестановок группы G , оставляющих его на месте.

Обозначение:

$$G_a = \{\pi \in G \mid \pi(a) = a\}.$$

Пример: симметрическая группа перестановок S_3

Пример. Пусть $N = \{1, 2, 3\}$. Рассмотрим симметрическую группу перестановок

$$S_3 = \{\pi_1 = e = (1)(2)(3), \pi_2 = (123), \pi_3 = (132), \\ \pi_4 = (1)(23), \pi_5 = (13)(2), \pi_6 = (12)(3)\}.$$

Найдем стабилизатор элемента $1 \in N$ в группе S_3 :

$$G_1 = \{\pi_1 = (1)(2)(3), \pi_4(1) = (1)(23)\}.$$

Несложно увидеть, что G_1 – подгруппа группы S_3 .

Оказывается, что стабилизатор элемента в группе перестановок всегда является подгруппой этой группы перестановок.

Стабилизатор элемента

Теорема 7. *Для каждого элемента $a \in N$ его стабилизатор G_a является подгруппой группы G .*

Доказательство проведем по критерию подгруппы (теореме 7 лекции 9).

Пусть $\pi, \rho \in G_a$. Рассмотрим перестановку $\pi \circ \rho^{-1}$. Тогда

$$(\pi \circ \rho^{-1})(a) = \rho^{-1}(\pi(a)) = \rho^{-1}(a) = a.$$

Т.е. $\pi \circ \rho^{-1} \in G_a$. □

Индекс стабилизатора в группе перестановок

Теорема 8. Для каждого элемента $a \in N$ индекс его стабилизатора G_a в группе перестановок G равен мощности его орбиты O_a , т.е. $(G : G_a) = |O_a|$.

Доказательство. Рассмотрим левостороннее разложение группы G по подгруппе G_a , определяющей отношение эквивалентности \sim_{G_a} . Пусть перестановки $\rho, \tau \in G$.

1) Если они из одного смежного класса, т.е. $\rho \sim_{G_a} \tau$, то найдется такая перестановка $\pi \in G_a$, что $\pi \circ \rho = \tau$. Тогда

$$\tau(a) = (\pi \circ \rho)(a) = \rho(\pi(a)) = \rho(a).$$

2) Пусть они из разных смежных классов. Предположим, что $\rho(a) = \tau(a)$. Тогда перестановка $\tau \circ \rho^{-1} \in G_a$, и по второму определению отношения эквивалентности по подгруппе $\rho \sim_{G_a} \tau$, и они лежат в одном смежном классе – противоречие. Т.е. $\rho(a) \neq \tau(a)$.

Индекс стабилизатора в группе перестановок

Доказательство. Следовательно,

$$\rho(a) = \tau(a) \Leftrightarrow \rho \sim_{G_a} \tau \Leftrightarrow \rho, \tau \text{ из одного смежного класса.}$$

Т.е. $(G : G_a) = |O_a|$.

□

Пример: индекс подгруппы G_1 в группе S_3

Пример. Мы нашли стабилизатор элемента $1 \in N$ в группе S_3 :

$$G_1 = \{\pi_1 = (1)(2)(3), \pi_4(1) = (1)(23)\}.$$

Найдем разложение симметрической группы перестановок S_3 на смежные классы по подгруппе G_1 :

Класс	π	$\pi(1)$
$(1)(2)(3)G_1$	$(1)(2)(3), (1)(23)$	1
$(123)G_1$	$(123), (12)(3)$	2
$(132)G_1$	$(132), (13)(2)$	3

Несложно увидеть, что $(S_3 : G_1) = O_1$.

Лемма Бернсайда

Теорема 9. (лемма Бернсайда) Число $N(G)$ орбит элементов по группе перестановок G равно

$$N(G) = \frac{1}{|G|} \sum_{\pi \in G} \lambda_1(\pi),$$

где $\lambda_1(\pi)$ – число неподвижных элементов перестановки π .

Лемма Бернсайда

Доказательство. Пусть $G = \{\pi_1 = e, \pi_2, \dots, \pi_m\}$.

Построим таблицу $T = (t_{ij})$, в которой

$$t_{ij} = 1, \quad \text{если } \pi_j(i) = i;$$

$$t_{ij} = 0, \quad \text{иначе.}$$

$T :$	$N \setminus G$	$\pi_1 = e$	π_2	\dots	π_m	
	1	1		\dots		$ G_1 $
	2	1		\dots		$ G_2 $
	\dots			\dots		\dots
	n	1		\dots		$ G_n $
		$\lambda_1(\pi_1)$	$\lambda_1(\pi_2)$	\dots	$\lambda_1(\pi_m)$	

В таблице T число единиц в каждой строке равно порядку стабилизатора элемента - номера этой строки, число единиц в каждом столбце равно числу неподвижных элементов перестановки с номером этого столбца.

Лемма Бернсайда

Доказательство.

Число единиц в таблице T можно подсчитать

по строкам как $\sum_{i=1}^n |G_i|$

и по столбцам как $\sum_{j=1}^m \lambda_1(\pi_j)$.

Тогда

$$\sum_{i=1}^n |G_i| = \sum_{j=1}^m \lambda_1(\pi_j).$$

Лемма Бернсайда

Доказательство.

По теореме 5 $|G_i| = \frac{|G|}{|O_i|}$. Поэтому

$$\sum_{i=1}^n |G_i| = |G| \sum_{i=1}^n \frac{1}{|O_i|}.$$

Если для элементов $i, k \in N$ верно $i \sim_G k$, то $O_i = O_k$, и $|O_i| = |O_k|$. Пусть

$$O_{a_1}, \dots, O_{a_{N(G)}}$$

все **различные** орбиты по группе G .

Тогда

$$\sum_{i=1}^n \frac{1}{|O_i|} = \sum_{l=1}^{N(G)} \frac{1}{|O_{a_l}|} \sum_{i \sim_G a_l} 1 = \sum_{l=1}^{N(G)} \frac{1}{|O_{a_l}|} \cdot |O_{a_l}| = N(G).$$

Лемма Бернсайда

Доказательство.

Откуда

$$|G| \cdot N(G) = \sum_{j=1}^m \lambda_1(\pi_j).$$

□

Лемма Бернсайда

Пример. Найдем число орбит элементов множества $N = \{1, 2, 3\}$ по группе H вращений правильного треугольника в плоскости. Сколько их?

Напомним, что

$$H = \{\pi_1 = e = (1)(2)(3), \pi_2 = (123), \pi_3 = (132)\}.$$

Тогда

$$\lambda_1(\pi_1) = 3, \lambda_1(\pi_2) = \lambda_1(\pi_3) = 0.$$

Значит,

$$N(H) = \frac{1}{|H|} \sum_{j=1}^3 \lambda_1(\pi_j) = \frac{1}{3}(3 + 0 + 0) = 1.$$

Все элементы множества N из одной орбиты, т.е. перестановками группы H каждый элемент множества N можно перевести в любой другой элемент этого множества.

Задачи для самостоятельного решения

1. Найти все неизоморфные группы из 4-х элементов.
2. Найти все неизоморфные группы из p элементов, где p – простое число.
3. Найти группу перестановок вершин правильного шестиугольника при его вращениях в плоскости. Найти все подгруппы этой группы. Найти орбиту вершины 1 в группе и в каждой из подгрупп. По лемме Бернсайда подсчитать число орбит вершин по каждой из подгрупп.
4. По лемме Бернсайда подсчитать число орбит вершин правильного восьмиугольника при его вращениях в плоскости на угол, кратный $\frac{\pi}{2}$.
5. Пусть H – подгруппа группы G , и порядок H равен $\frac{|G|}{2}$. Доказать, что H – нормальная подгруппа группы G .

Литература к лекции 10

1. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. Гл. 1, с. 12-23.

Конец лекции 10