Лекция 6. Подгруппы. Смежные классы, индекс подгруппы в группе. Теорема Лагранжа о порядке подгруппы конечной группы. Нормальные подгруппы. Фактор-группы. Цикловой индекс группы перестановок.

Лектор — Селезнева Светлана Николаевна
selezn@cs.msu.su

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.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_Ha.
2) Симметричность. Пусть для элементов $a, b \in S$ верно aR_Hb, 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, $h' \in H$. Отсюда bR_Ha.
3) Транзитивность. Пусть для элементов $a, b, c \in S$ верно aR_Hb и bR_Hc, 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, $h_1 * h_2 = h \in H$. Отсюда aR_Hc.

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 $H = \{h_1 = e, h_2, \ldots, h_m\}$ — конечная подгруппа группы $G = (S; *)$.
Тогда для каждого элемента $a \in S$ левый смежный класс

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

также содержит конечное число элементов.

Пример. Найдем 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 $H = \{h_1 = e, h_2, \ldots, h_m\}$ — конечная подгруппа группы $G = (S; *)$.

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

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

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, $|aH| = |H|$. $\square$

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

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

Отсюда $|H| \mid |G|$. $\square$

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 $H =< a >$ с образующим элементом $a \in S$. Тогда порядок элемента a равен порядку группы H, и по следствию 2.1 делит порядок группы G.

$\square$

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 нейтральные 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 коммутативной 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

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

Отсюда

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

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

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

Отсюда

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

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

$\square$

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 ввведенная 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 $b * N = N * b$. Отсюда, найдется такой элемент $h_3 \in N$, что

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

Тогда

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

$\square$

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.

$\square$

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 ее нормальной 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

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

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

Цикловой индекс

Пусть $G = (S; \circ)$ — подгруппа симметрической группы перестановок S_n.

Цикловым индексом группы перестановок G называется многочлен n переменных

$$Z_G(t_1, \ldots, t_n) = \frac{1}{|G|} \sum_{\pi \in G} t_1^{\lambda_1(\pi)} \cdot \ldots \cdot t_n^{\lambda_n(\pi)},$$

где $\lambda(\pi) = (\lambda_1(\pi), \ldots, \lambda_n(\pi))$ — тип перестановки π.

Цикловой индекс

1. Найдем цикловой индекс группы H вращений правильного треугольника в плоскости.

Для каждой перестановки ищем ее тип:

$\pi_1 = e = (1)(2)(3), \;\; \lambda(\pi_1) = (3, 0, 0);$

$\pi_2 = (123), \;\; \lambda(\pi_2) = (0, 0, 1);$

$\pi_3 = (132), \;\; \lambda(\pi_3) = (0, 0, 1).$

Замечая, что $|H| = 3$, получаем цикловой индекс

$$Z_H(t_1, t_2, t_3) = \frac{1}{3}(t_1^3 + 2t_3).$$

Цикловой индекс

2. Найдем цикловой индекс симметрической группы перестановок S_3.

Аналогично находим типы всех ее перестановок:

$\pi_1 = e = (1)(2)(3), \;\; \lambda(\pi_1) = (3,0,0);$

$\pi_2 = (1)(23),\; \pi_3 = (13)(2),\; \pi_4 = (12)(3),$

$\lambda(\pi_2) = \lambda(\pi_3) = \lambda(\pi_4) = (1,1,0);$

$\pi_5 = (123),\; \pi_6 = (132), \;\; \lambda(\pi_5) = \lambda(\pi_6) = (0,0,1).$

Порядок группы $|S_3| = 3! = 6.$

Поэтому ее цикловой индекс

$$Z_{S_3}(t_1, t_2, t_3) = \frac{1}{6}(t_1^3 + 3t_1t_2 + 2t_3).$$

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. Какие из них являются нормальными подгруппами?

4. Пусть H — подгруппа группы G, и порядок H равен $\frac{|G|}{2}$. Доказать, что H — нормальная подгруппа группы G.

Литература к лекции

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

Конец лекции