ЛЕКЦИЯ 14

СМЕЖНЫЕ КЛАССЫ

ТЕОРЕМА ЛАГРАНЖА И ЕЕ СЛЕДСТВИЯ

КОЛЬЦА

СМЕЖНЫЕ КЛАССЫ

Пусть G — группа, H — подгруппа группы G, $x \in G$. *Левым смежным классом группы G по подгруппе H*, порожденным элементом x, называется множество

$$xH = \{xh \mid h \in H\}.$$

Аналогично, *правый смежный класс* определяется как

$$Hx = \{hx \mid h \in H\}.$$

Пример 1. Пусть $G = \mathbb{R}^2$ с операцией сложения, $H = \{(a, 0) \mid a \in \mathbb{R}\}$, $x = (1, 1)$. Тогда

$$x + H = \{(a, b) \in \mathbb{R}^2 \mid b = 1\}.$$

Все смежные классы группы $\mathbb{R}^2$ по H — это все прямые, параллельные прямой H.

Пример 2. Пусть $G = \mathbf{S}_3$,

$$H = \langle (1\,2) \rangle = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\},$$

$$x = (1\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Тогда:

$$xH = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3), \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3) \right\};$$

$$Hx = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3), \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2) \right\}.$$

Замечание 1. 1) Мы видим в этом примере, что $xH \neq Hx$ (т. е. правый и левый смежные классы по подгруппе, порожденные элементом x, могут не совпадать).

2) Если $x = e$ — нейтральный элемент группы G, то $eH = H = He$.

3) $xH = H$ тогда и только тогда, когда $x \in H$; $Hx = H$ тогда и только тогда, когда $x \in H$.

ТЕОРЕМА ЛАГРАНЖА

Теорема 1 ((о разбиении группы на левые смежные классы))**.** *Пусть G — группа и H — подгруппа группы G, тогда*:

1) $x \in xH$ *для всех* $x \in G$;

2) *если* $z \in xH$, *то* $zH = xH$;

3) *если* $xH \cap yH \neq \varnothing$, *то* $xH = yH$ (*т. е. два левых смежных класса либо не пересекаются, либо совпадают*);

4) *равносильны следующие условия*:

a) $xH = yH$;

b) $y^{-1}x \in H$;

c) $x^{-1}y \in H$;

5) $|H| = |xH|$.

Доказательство.

1) $x = xe \in xH$, так как $e \in H$.

2) Если $z \in xH$, то $z = xh_0$, где $h_0 \in H$. Тогда $x = zh_0^{-1}$, где $h_0^{-1} \in H$.

Пусть $h \in H$. Тогда:

$$zh = (xh_0)h = x(h_0h) \in xH, \text{ так как } h_0h \in H;$$
$$xh = (zh_0^{-1})h = z(h_0^{-1}h) \in zH, \text{ так как } h_0^{-1}h \in H.$$

Итак, $zH \subseteq xH$ и $xH \subseteq zH$, т. е. $zH = xH$.

3) Пусть $z \in xH \cap yH$. В силу 2) $xH = zH = yH$.

4) Если $xH = yH$, то $x \in xH = yH$, и поэтому $x = yh$, $h \in H$, т. е. $y^{-1}x = h \in H$. Аналогично, $y \in yH = xH$, $y = xh'$, $h' \in H$, т. е. $x^{-1}y = h' \in H$. Если $y^{-1}x = h \in H$, то $x = yh \in yH$. В силу 2) $xH = yH$. Если $x^{-1}y = h' \in H$, то $y = xh' \in xH$. В силу 2) $yH = xH$.

5) Если $xh = xh'$, то, умножая на x^{-1}, видим, что $h = h'$. $\square$

Теорема 2 ((Лагранж, Joseph Lois Lagrange (1736—1813))). *Если H — подгруппа группы G, $|G| = n < \infty$, $|H| = k$, то k — делитель числа n, а именно, $n = kj$, где j — число левых (правых) смежных классов, называемое индексом подгруппы H в G (обозначение: $j = (G : H)$).*

Доказательство. Рассмотрим разбиение группы G на j различных левых смежных классов xH. Так как $|xH| = |H| = k$, то $n = kj$. □

СЛЕДСТВИЯ ИЗ ТЕОРЕМЫ ЛАГРАНЖА

Следствие 1. *Если $a \in G$, $|G| = n$, то порядок $O(a)$ элемента a является делителем числа n, порядка группы G.*

Доказательство. Рассмотрим циклическую подгруппу $H = \langle a \rangle$. Тогда $|H| = O(a)$. В силу теоремы Лагранжа $n = O(a) \cdot j$. □

Следствие 2. *Если $|G| = n$ и $a \in G$, то $a^n = e$.*

Доказательство. В силу следствия 1 $n = O(a) \cdot j$. Тогда $a^n = \left(a^{O(a)}\right)^j = e^j = e$. □

Следствие 3 ((о цикличности группы простого порядка))**.** *Порядок $|G|$ конечной группы G равен простому числу p тогда и только тогда, когда $G \cong \mathbb{Z}_p$ (т. е. группа G циклическая и изоморфна группе вычетов $\mathbb{Z}_p$ по модулю простого числа p). Итак, если $|G| = p$, то G — циклическая группа и в качестве циклического образующего группы G можно выбирать любой неединичный элемент группы G. В частности, в группе G нет подгрупп, отличных от $\{e\}$ и G.*

Доказательство.

1) Если $G \cong \mathbb{Z}_p$, то $|G| = |\mathbb{Z}_p| = p$.

2) Пусть $|G| = p$ и $e \neq a \in G$. Тогда число $O(a)$ является делителем числа $p = |G|$, поэтому $O(a) = p$ и $|\langle a \rangle| = O(a) = p = |G|$. Следовательно, $\langle a \rangle = G$, т. е. G — циклическая группа порядка p. Итак, $G \cong \mathbb{Z}_p$. □

Упражнение 1 (классификация групп порядка $\boldsymbol{n \leqslant 5}$). Пусть G — группа и $|G| \leqslant 5$. Если $|G| = 1, 2, 3$ или 5, то, по следствию 3 к теореме Лагранжа для $p = 2, 3$ или 5, G — циклическая группа. Если $|G| = 4$ и в G есть элемент a порядка 4, то $G = \langle a \rangle$ — циклическая группа, $G \cong \mathbb{Z}_4$. В противном случае $G = \{e, a, b, c\}$, $a^2 = b^2 = c^2 = e$. Если $ab = e$, то $ab = e = a^2$, и поэтому $b = a$, что противоречит тому, что $a \neq b$; аналогично, $ab \neq a$, $ab \neq b$. Итак, $ab = c$. Так же проверяем, что $ba = c$, $ac = b = ca$, $bc = a = cb$. Таким образом, G — группа Клейна. □

Следствие 4. *Группа* $\mathbf{S}_3$ *является неабелевой группой наименьшего порядка.*

КОЛЬЦА

Определение 1. Пусть K — непустое множество, на котором заданы две бинарные операции $+$ (сложение) и $\cdot$ (умножение), удовлетворяющие следующим свойствам:

(1) $(K, +)$ — абелева группа;

(2) $(K, \cdot)$ — полугруппа;

(3) операции умножения и сложения связаны дистрибутивными законами

$$(a + b)c = ac + bc \text{ и } c(a + b) = ca + cb$$

для всех $a, b, c \in K$.

Тогда $(K, +, \cdot)$ называется *кольцом*.

Структура $(K, +)$ называется аддитивной группой кольца, а $(K, \cdot)$ — его мультипликативной полугруппой.

Если $(K, \cdot)$ — моноид, то говорят, что $(K, +, \cdot)$ — кольцо с единицей.

Единичный элемент кольца принято обозначать обычной единицей 1.

Существование единицы часто вносится в определение кольца, но мы не будет делать этого по умолчанию.

В нашем случае определение введено так, чтобы умножение сразу было ассоциативным. Однако бывает, что рассматривают неассоциативные кольца, в которых ассоциативность по умножению не выполняется.

Подмножество L кольца K называется *подкольцом*, если

$$x, y \in L \Longrightarrow x - y \in L, xy \in L,$$

то есть если L — подгруппа аддитивной группы кольца и подполугруппа мультипликативной полугруппы кольца.

Ясно, что пересечение любого семейства подколец в K является подкольцом, поэтому имеет смысл говорить о подкольце $\langle T \rangle \subset K$, порожденном подмножеством $T \subset K$.

Кольцо K называется *коммутативным*, если

$$xy = yx$$

для всех $x, y \in X$.

Пример 3. Самым простым и первом примером кольца (с единицей) является кольцо целых чисел $\mathbb{Z}$. Оно является коммутативным.

Аналогично, коммутативными кольцами с единицей являются рациональные числа $\mathbb{Q}$ и действительные числа $\mathbb{R}$, причем

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Пример 4. Если R — коммутативное ассоциативное кольцо с единицей (например, целые, рациональные или дейтвительные числа), то $R[x]$ — кольцо многочленов над R от одной переменной, $R[x_1, x_2, \ldots, x_n]$ — кольцо многочленов над R от многих (коммутирующих переменных). Также можно рассмотреть кольцо многочленов от n некоммутирующих переменных $x_1, \ldots, x_n$. Чтобы не путать его с обычным кольцом многочленов, будем обозначать его через $R\langle x_1, x_2, \ldots, x_n\rangle$.

Пример 5. Примером кольца, благодаря которому кольца именно так именуются, является кольцо вычетов по модулю n — $\mathbb{Z}_n$. Данное кольцо состоит из остатков $\{0, 1, 2, \ldots, n-1\}$ от деления на n, операции сложения и умножения проводятся по модулю n.

Очевидно, что данное кольцо коммутативно, единицей служит остаток 1.

Пример 6. Если R — это некоторое ассоциативное кольцо с единицей (для примера можно рассмотреть целые, рациональные или действительные числа), $n \geqslant 1$, то $\mathbf{M}_n(R)$ — кольцо матриц над R. При $n = 1$ оно совпадает с кольцом R, при $n \geqslant 2$ оно обязательно некоммутативно (например, $E_{12}E_{21} \neq E_{21}E_{12}$) и содержит необратимые ненулевые элементы.

Пример 7. Для любого ассоциативного кольца R с единицей можно рассмотреть кольцо *формальных степенных рядов* $R[[x]]$ от одной переменной (также по аналогии вводится кольцо

$$R[[x_1, \ldots, x_n]]$$

формальных степенных рядов от многих переменных). Каждый элемент этого кольца — формальный ряд

$$\sum_{i=0}^{\infty} r_i x^i.$$

Два ряда

$$\sum_{i=0}^{\infty} r_i x^i \text{ и } \sum_{j=0}^{\infty} s_j x^j$$

складываются почленно, а при умножении дают ряд

$$\sum_{n=0}^{\infty} u_n x^n,$$

где

$$u_n = \sum_{k=0}^{n} r_k s_{n-k}.$$

Пример 8. Можно рассмотреть кольцо функций $\mathbb{R}^X$ из некоторого множества X в (например) действительные числа (а можно и в любое другое кольцо). Функции можно поточечно умножать и складывать. Кольцо получится коммутативным. Единицей в нем является константа 1.

Многие свойства колец являются переформулировкой свойств групп и вообще множеств с одной ассоциативной операцией.

Например,

$$a^{m+n} = a^m a^n, \quad (a^m)^n = a^{mn}$$

для всех неотрицательных целых m, n и любого элемента a нашего кольца.

Отметим пару важных свойств колец.

(1) Для всех $a \in R$ выполнено

$$a \cdot 0 = 0 \cdot a = 0.$$

Действительно,

$$a + 0 = a,$$

откуда

$$a(a + 0) = a \cdot a.$$

Раскроем скобки:

$$a \cdot a + a \cdot 0 = a \cdot a.$$

Значит, $a \cdot 0$ — это нейтральный элемент по сложению, то есть ноль.

(2) В кольце, в котором есть больше одного элемента, $0 \neq 1$.

Действительно, пусть $0 = 1$.

Тогда

$$a = a \cdot 1 = a \cdot 0 = 0$$

для всех $a \in R$, то есть кольцо состоит только из нулевого элемента.

(3) Выполнено

$$(-a) \cdot b = a \cdot (-b) = -ab$$

для всех $a, b \in R$.

Действительно,

$$0 = a \cdot 0 = a(b - b) = ab + a(-b) \Longrightarrow a(-b) = -ab.$$