ЛЕКЦИЯ 14

ТЕОРЕМА КЭЛИ

ГОМОМОРФИЗМЫ

СМЕЖНЫЕ КЛАССЫ

ТЕОРЕМА ЛАГРАНЖА

ТЕОРЕМА КЭЛИ

Теорема 1 (Кэли)**.** *Любая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы S_n.*

Доказательство. Пусть G — наша группа, $n = |G|$. Можно считать,что S_n — группа всех биективных преобразований множества G на себя, так как природа элементов, переставляемых элементами из S_n, несущественна.

Для любого элемента $a \in G$ рассмотрим отображение $L_a : G \to G$, определенное формулой

$$L_a(g) = ag.$$

Если $e = g_1, g_2, \ldots, g_n$ — все элементы из G, то $a, ag_2, \ldots, ag_n$ будут теми же элементами, но расположенными в другом порядке. Это понятно, поскольку

$$ag_i = ag_j \Longrightarrow a^{-1}(ag_i) = a^{-1}(ag_j) \Longrightarrow$$
$$\Longrightarrow (a^{-1}a)g_i = (a^{-1}a)g_j \Longrightarrow g_i = g_j.$$

Значит, L_a — биективное отображение (перестановка), обратным к которому будет $L_a^{-1} = L_{a^{-1}}$.

Единичным отображением является, естественно, L_e.

Используя вновь ассоциативность умножения в G, получаем

$$L_{ab}(g) = (ab)g = a(bg) = L_a(L_b g),$$

то есть

$$L_{ab} = L_a L_b.$$

Итак, множество

$$L_e, L_{g_1}, \ldots, L_{g_n}$$

образует подгруппу (скажем, H) в группе $S(G)$ всех биективных отображений множества G на себя, то есть в S_n.

Мы имеем включение $H \subset S_n$ и отображение

$$L : a \mapsto L_a \in H,$$

обладающее всеми свойствами изоморфизма. □

Теорема Кэли, несмотря на свою простоту, имеет важное значение в теории групп. Она выделяет некий универсальный объект (семейство $\{S_n \mid n = 1, 2, \ldots\}$ симметрических групп) — вместилище всех конечных групп, рассматриваемых с точностью до изоморфизма.

Фраза “с точностью до изоморфизма” отражает сущность не только теории групп, стремящейся объединить в один класс все изоморфные группы, но и математики в целом, которая безтаких обобщений была бы лишена смысла.

Положив $G = G'$ в определении изоморфизма, мы получим изоморфное отображение $\varphi : G \to G$ группы G на себя. Оно называется *автоморфизмом* группы G.

Например, единичное отображение $e_G = 1 : g \mapsto g$ всегда является автоморфизмом. Чаще всего группа G обладает и нетривиальными автоморфизмами.

Пример 1. Например, группа $\mathbb{Z}_2$, состоящая только из 0 и 1, не имеет нетривиальных автоморфизмов, так как 0 обязательно должен отображаться сам в себя как нейтральный элемент группы, поэтому для единицы нет больше никаких возможностей — только отобразиться в саму себя.

Если же мы рассмотрим группу $\mathbb{Z}_3$, то в ней уже возникает нетривиальный автоморфизм

$$a \mapsto -a,$$

при котором 0 останется на месте, а 1 и -1 поменяются местами.

Лемма 1. *При изоморфизме (автоморфизме) $\varphi : G \to G'$ любой элемент $x \in G$ порядка n (или бесконечного порядка) переходит в элемент того же порядка.*

Доказательство. Действительно, если $x^n = e$, то $\varphi(x)^n = \varphi(e) = e'$, то есть порядок элемента $\varphi(x)$ является делителем числа n.

С другой стороны, изоморфизм (или автоморфизм) — это обратимое отображение, можно применить те же рассуждению к изоморфизму φ^{-1}, поэтому окажется, что и число n делит порядок элемента $\varphi(x)$. Значит, эти два числа совпадают. □

Пример 2. Рассмотрим симметрическую группу S_3. Заметим, что транспозиции должны переходить в транспозиции, так как они являются элементами порядка два. При этом, понятно, они должны переставляться. Кроме того, если мы знаем образы транспозиций, то полностью знаем автоморфизм, так как транспозициями порождается вся группа S_3.

Значит, можно считать, что группа автоморфизмов $\operatorname{Aut} S_3$ содержится в S_3.

В реальности можно насчитать шесть разных автоморфизмов, которые задаются отображениями

$$\varphi_\sigma : \tau \mapsto \sigma\tau\sigma^{-1}, \text{ где } \sigma, \tau \in S_3.$$

Значит, $\operatorname{Aut} S_3 \cong S_3$.

Заметим, что композиция автоморфизмов — автоморфизм, обратный к автоморфизму — автоморфизм, то есть все автоморфизмы данной группы образуют группу $\operatorname{Aut}(G)$.

ГОМОМОРФИЗМЫ

Определение 1. Отображение $f : G \to G'$ группы $(G, *)$ в группу $(G', \circ)$ называется *гомоморфизмом*, если

$$\forall a, b \in G \quad f(a * b) = f(a) \circ f(b).$$

Ядром гомоморфизма f называется множество

$$\ker f = \{g \in G \mid f(g) = e'\}.$$

Заметим, что ядро гомоморфизма всегда является подгруппой группы G, так как если два элемента отображаются в единицу, то их произведение отображаетсяв единицу; сама единица отображается в единицу; если элемент отображается в единицу, то и обратный к нему элемент тоже отображается в единицу.

Гомоморфизм группы в саму себя называется *эндоморфизмом.*

Заметим, что в определении гомоморфизма от f не требуется не только инъективности, но и сюръективности. Это не слишком существенно, так как всегда можно заменить группу G' на образ гомоморфизма $f(G) = \Im f \subset G'$. Этот образ — тоже группа (подгруппа в G'), что совсем очевидно.

Пример 3. Группу целых чисел $\mathbb{Z}$ можно гомоморфно отобразить на группу $\mathbb{Z}_n$, надо при этом каждое целое число взять по модулю n. Понятно, что ядро такого гомоморфизма — это все числа, которые делятся на n, данная подгруппа в $\mathbb{Z}$ записывается как $n\mathbb{Z}$.

Пример 4. Построим гомоморфизм общей линейной группы $\mathrm{GL}_n(\mathbb{R})$ на мультипликативную группу поля действительных чисел $\mathbb{R}^*$, сопоставив каждой матрице $A \in \mathrm{GL}_n(\mathbb{R})$ ее определитель $\det A$.

Благодаря тому, что

$$\det AB = \det A \det B,$$

это отображение — гомоморфизм.

Очевидно, что его ядром должны являться матрицы с определителем 1, то есть ровно группа $SL_n(\mathbb{R})$.

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 5. 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 6. 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 2 (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 3 (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 (теорема Эйлера и малая теорема Ферма). *Если $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$, то*

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

где $\varphi(m) = |U(\mathbb{Z}_m)|$ — функция Эйлера. В частности, при $m = p$ получаем малую теорему Ферма: если a не делится на простое число p, то

$$a^{p-1} \equiv 1 \pmod{p}$$

(другими словами, $a^p \equiv a \pmod{p}$).

Доказательство.

1) Пусть $G = \mathbf{U}(\mathbb{Z}_m)$ — группа обратимых элементов кольца вычетов $\mathbb{Z}_m$, $|G| = |\mathbf{U}(\mathbb{Z}_m)| = \varphi(m)$ — функция Эйлера (т. е. $\varphi(m)$ — число тех $x \in \mathbb{N}$, что $0 < x < m$, $(x, m) = 1$). Так как

$$(a, m) = 1 \iff a + \mathbb{Z}m \in \mathbf{U}(\mathbb{Z}_m),$$

то

$$(a + \mathbb{Z}_m)^{\varphi(m)} = a^{\varphi(m)} + \mathbb{Z}m = 1 + \mathbb{Z}m,$$

и поэтому

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

2) Если $m = p$, то $\varphi(p) = p - 1$. □

Замечание 2. На применении малой теоремы Ферма основаны вероятностные алгоритмы нахождения больших простых чисел p: для достаточно большого числа случайных значений $a < p$ проверяется, что $a^{p-1} \equiv 1 \pmod{p}$.

Следствие 4 (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 4 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 5. *Группа $\mathbf{S}_3$ является неабелевой группой наименьшего порядка.*