Теория групп. Лекция 5

Штепин Вадим Владимирович

3 октября 2019 г.

1 Классические действия групп на множествах

Следствия утв. $Shift(\omega, \omega') = St(\omega')s = sSt(\omega)$, $s \in Shift(\omega, \omega')$ — произвольный элемент.

Следствие.
Если ω, ω' — элементы одной орбиты, то $St(\omega)$ и $St(\omega')$ сопряжены.

Доказательство
$\exists s: \ s(\omega) = \omega'$ и $st(\omega') = sSt(\omega)s^{-1}$ ч.т.д.

Следствие.
Пусть $G(\omega)$ — орбита элемента ω.
$|G(\omega)| = |G : St(\omega)| = \frac{|G|}{|St(\omega)|}$. Последнее равенство верно при условии, что G — конечно.

Доказательство
Фиксируем $\omega \in \Omega$.
Тогда, $aSt(\omega) \to a(\omega) \in G(\omega)$ — биекция, так как $aSt(\omega) = bSt(\omega) \Leftrightarrow a^{-1}b \in St(\omega) \Leftrightarrow a^{-1}b(\omega) = \omega \Leftrightarrow a(\omega) = b(\omega)$.
Значит, число левых смежных классов равно $|G(\omega)|$.

Два левых смежных класса по стабилизатору ω совпадают тогда, и только тогда, когда соответствующие им элементы Ω равны $(a(\omega) = b(\omega))$.

Упражнение. Проверить, что мощность орбиты не зависит от выбора представителя.

2 Формула орбит

Пусть $|\Omega| < \inf$
Пусть $\Omega = \Omega_1 \cup \Omega_2 \cup ... \cup \Omega_s$ — разбиение на попарно различные классы (орбиты).
В каждой орбите выберем по представителю $a_i \in \Omega_i$.
$|\Omega| = \sum\limits_{i=1}^{s} |\Omega_i| = \sum\limits_{i=1}^{s} |G : St(a_i)|$
Классические действия

1. Действие G на себя левыми сдвигами. $\Omega = G$, $I_a(x) = ax$ — левый сдвиг.

   I_a — действие, так как $I_{ab} = I_a(I_b(x)) = abx$.

   $KerI = \{a \in G \mid ax = x\} = \{e\} \Rightarrow I$ — точное (эффективное).

   I — свободное, так как $\forall a \neq e \ a\omega = \omega$ — не выполнено $\forall \omega \in G$.

   Пусть не так, значит $a\omega = \omega$. Умножим на $\omega^{-1} \Rightarrow a = e$. Противоречие.

$ImI \sim G/KerI = G \Rightarrow G \leq S(G)$.

Если $|G| = n$, $S(G) \sim S_n$.

Вывод. Конечная группа $G \sim G' \leq S_n$ — теорема Кэли.

2. Действие G на себя сопряжением.

   $I_a : G \to S(G)$, $I_a(x) = axa^{-1} = x^{a^{-1}}$. Это действие, так как $I_{ab}(x) = abx(ab)^{-1} = abxb^{-1}a^{-1} = I_a(I_b(x))$.

   $G(x) = \{I_a(x) \mid a \in G\} = \{axa^{-1} \mid a \in G\} = x^G$ — класс сопряженных элементов, порожденный G.

   $St(x) = \{a \in G \mid axa^{-1} = x\} = \{a \in G \mid ax = xa\} = C_G(x)$ — централизатор элемента $x \in G$.

Опр. **Централизатор элемента** x — стационарная подгруппа x при действии сопряжением.

$|G(x)| = |G : St(x)| \Rightarrow |x^G| = |G : C_G(x)|$ — мощность класса сопряженных элементов равна индексу централизатора любого элемента этого класса.

$KerI = \{a \in G \mid axa^{-1} = x \ \forall x \in G\} = \{a \in G \mid ax = xa \ \forall x \in G\}$.

$Z(G) = \{a \in G \mid ax = xa \ \forall x \in G\}$. Тогда $Z(G) \triangleleft G$

Утв. $C_G(x)$ — наибольшая подгруппа H в G, что $x \in Z(H)$

I — точное $\Leftrightarrow G$ имеет тривиальный центр.

I никогда не бывает свободна, так как $\forall a \in G \ I_a(e) = e$

Утв. Если G — конечно, то $\frac{G}{ord(x)} \vdots |x^G|$

Доказательство

$|x^G| = |G : C_G(x)|$. $\langle x \rangle \leq G$ — конечно.

$|\langle x \rangle| = ord(x)$, очевидно $\langle x \rangle \leq C_G(x) \Rightarrow |C_G(x)| \vdots ord(x) \Rightarrow |C_G(x)| = ord(x)n, \ n \in N$ — по теореме Лагранжа.

$|x^G| = \frac{|G|}{ord(x)n}$

3 Автоморфизм

Опр. Всякий изоморфизм $\phi : G \to G$ называется **автоморфизм** группы G.

Очевидно, что множество автоморфизмов группы — группа относительно композиции.

$Aut(G)$ — группа автоморфизмов.

$I_a(x) = axa^{-1}$ — автоморфизм.

$I_a(xy) = I_a(x)I_a(y)$, так как $I_a(xy) = (xy)^{a^{-1}} = y^{a^{-1}}x^{a^{-1}} = I_a(x)I_a(y)$

Опр. Множество всех автоморфизмов вида $I_a(x) = axa^{-1}$ — внутренние автоморфизмы.

Было проверено, что множество внутренних автоморфизмов образует группу относительно композиции.

$Inn(G)$ — группа внутренних автоморфизмов.

Утв. $Inn(G) \sim G/Z(G)$

Доказательство

$Z(G) = KerI, \ ImI = \{I_a \mid I_a(x) = axa^{-1}\} = Inn(G)$.

$I : G \to S(G),\ I : G \to Inn(G),\ a \to I_a$. По основной теореме о гомоморфизме $Inn(G) \sim G/Z(G)$

Замечание Группы $Aut(G)$ и $Im(G)$ могут быть различны.
Пример.
Пусть G — абелева. Тогда $I_a(x) = axa^{-1} = x$. Однако автоморфизм, сопоставляющий числу его обратное, не является внутренним.

Замечание
В случае неабелевой группы $J_a(x) = x^a$ — не действие.

4 Формула классов

Утв. $|G| = |Z(G)| + \sum\limits_{i=1}^{r} |G : C_G(a_i)|$, где a_i — представитель тех классов сопряженных элементов, содержащих > 1 элемент.

Доказательство
$x \in Z(G) \Rightarrow |x^G| = 1,\ x^G = \{axa^{-1} \mid a \in G\} = x$.
Пусть $x \notin Z(G)$. Покажем, что $|x^G| > 1$.
$\exists a \in G : ax \neq xa \Leftrightarrow axa^{-1} \neq x$ и $axa^{-1} \in x^G$.
Пусть в G имеется r классов сопряженных, содержащих > 1 элемент.
$|G| = |Z(G)| + \sum\limits_{i=1}^{r} |G : C_G(a_i)|$.

Опр. Конечная группа G — это p**-группа**, если $\exists k \in N,\ |G| = p^k,\ p$-простое.

Теорема
Всякая p-группа имеет нетривиальный центр $Z(G) \neq \{e\}$

Доказательство.
Пусть $|G| = p^n$.

1. $G = Z(G) \Rightarrow Z(G)$ — нетривиален.
2. $G \neq Z(G) \Rightarrow r \geq 1$ в формуле классов. Значит, $C_G(a_i) \leq G \Rightarrow |C_G(a_i)| = p^{l_i},\ 0 \leq l_i < n$ — порядок централизатора (теорема Лагранжа). Или, что эквивалентно, орбита элемента a_i нетривиальна.

   $|Z(G)| = |G| - \sum\limits_{i=1}^{r} \frac{p^n}{p^{l_i}} = |G| - \sum\limits_{i=1}^{r} p^{n-l_i}$ — делится на p. Значит, $|Z(G)|$ делится на p.

   $|Z(G)| \neq 0$, так как $e \in Z(G)$.

Теорема
Если G — неабелева конечная группа, то $G/Z(G)$ не циклическая.

Доказательство
Пусть $Z = Z(G)$ и $G/Z = \langle aZ \rangle$, aZ — порождающий элемент. Пусть $x, y \in G$ — произвольные. $x \in a^l Z,\ y \in a^k Z \Rightarrow \exists z_1 \in Z,\ z_2 \in Z$ и $xy = a^l z_1 a^k z_2 = yx$ — противоречие.

Теорема
Если $|G| = p^2$, то G — абелева

Доказательство
Если $G = Z(G) \Rightarrow G$ — абелева.
Пусть $Z(G) \neq G \Rightarrow Z(G) \triangleleft G$, значит либо

1. $|Z(G)| = p$ Тогда $|G/Z(G)| = p$ — циклическая $\Rightarrow G$ абелева (так как в противном случае $G/Z(G)$ не циклична)

2. $|Z(G)| = p^2$. Тогда $G = Z(G)$