

ЛЕКЦИЯ 9

ДЕЙСТВИЯ ГРУППЫ НА МНОЖЕСТВЕ (ПОЛИГОНЫ)

ЦЕНТР КОНЕЧНОЙ p -ГРУППЫ

ПЕРВАЯ И ВТОРАЯ ТЕОРЕМЫ СИЛОВА

ДЕЙСТВИЯ ГРУППЫ НА МНОЖЕСТВЕ (ПОЛИГОНЫ)

Различные группы преобразований дают естественные и многочисленные примеры действия групп на множествах. Это обосновывает рассмотрение *левого полигона M над группой G* (или *левого G -полигона*, обозначение M_G): множества M и отображения $G \times M \rightarrow M$, при котором $(g, m) \rightarrow gm$, $m \in M$, $g \in G$, при этом

- 1) $(gh)m = g(hm)$ для всех $m \in M$, $g, h \in G$;
- 2) $em = m$ для $m \in M$ и нейтрального элемента $e \in G$.

Если $\mathbf{S}(M)$ — группа подстановок на множестве M , т. е. группа всех биекций $\sigma: M \rightarrow M$ с операцией композиции, то задание структуры полигона M_G равносильно заданию гомоморфизма групп

$$\varphi: G \rightarrow \mathbf{S}(M).$$

ОПРЕДЕЛЕНИЕ 1. *Орбитой* элемента m полигона M_G над группой G назовем следующее подмножество в M :

$$\text{Orb}(m) = \{gm \mid g \in G\} (= Gm).$$

ЗАМЕЧАНИЕ 1. $y \in \text{Orb}(m) \iff \text{Orb}(y) = \text{Orb}(m)$.

Действительно, если $y = gm$, то $hy = hgm$ для $h \in G$, т. е. $Gy \subseteq Gm$. Так как $m = g^{-1}y$, то $Gm \subseteq Gy$. Итак, $Gy = Gm$. Если $Gy = Gm$, то $y = ey \in Gy = Gm$.

ЗАМЕЧАНИЕ 2. Отношение $y \sim x \iff y = gx, g \in G$ (т.е. $y \sim x \iff \text{Orb}(y) = \text{Orb}(x)$) является отношением эквивалентности.

Действительно,

1) $x = ex$, т.е. $x \sim x$;

2) если $z \sim y, y \sim x$, т.е. $z = hy, y = gx, h, g \in G$, то $z = hgx$, т.е. $z \sim x$;

3) если $y \sim x$, т.е. $y = gx, g \in G$, то $x = g^{-1}y$, т.е. $x \sim y$.

Теорема 1 (разбиение на непересекающиеся орбиты). Если M_G — полигон над группой G , то M_G является объединением непересекающихся орбит: $M_G = \bigcup_i \text{Orb}(m_i)$, где m_i — представители орбит (т.е. выбранные по одному элементу в каждой орбите).

Следствие 1. Если $|M_G| < \infty$, то

$$|M_G| = |\text{Orb}(m_1)| + \dots + |\text{Orb}(m_k)|,$$

где m_1, \dots, m_k — представители орбит.

Доказательство. вытекает из рассмотрения отношения эквивалентности: $y \sim x \iff \text{Orb}(y) = \text{Orb}(x)$. □

ЗАМЕЧАНИЕ 3. Если $M_G = \text{Orb}(m), m \in G$ (т.е. имеется единственная орбита), то будем говорить, что группа G действует транзитивно.

ОПРЕДЕЛЕНИЕ 2. Если $p \in M_G$, то стабилизатором элемента p назовем следующее подмножество группы G :

$$\text{St}(p) = \{g \in G \mid gp = p\}.$$

Теорема 2. Пусть $p \in M_G$. Тогда():

1) стабилизатор $\text{St}(p)$ элемента $p \in G$ является подгруппой группы G ;

2) соответствие между смежными классами $\text{St}(p)a$, $a \in G$, и элементами $pa \in Gp = \text{Orb}(p)$ является биекцией;

3) если $|G| = n < \infty$, то $|G| = |\text{Orb}(p)| \cdot |\text{St}(p)|$ (и следовательно, $|\text{Orb}(p)|$ и $|\text{St}(p)|$ — делители числа $n = |G|$, при этом $|\text{Orb}(p)| = \frac{|G|}{|\text{St}(p)|}$).

Доказательство.

1) Если $g, h \in \text{St}(p)$ т. е. $gp = p$ и $hp = p$, то $hgp = hp = p$, и поэтому $hg \in \text{St}(p)$. Если $g \in \text{St}(p)$, т. е. $gp = p$, то $g^{-1}p = g^{-1}gp = ep = p$, и поэтому $g^{-1} \in \text{St}(p)$. Ясно, что $ep = p$, т. е. $e \in \text{St}(p)$, т. е. $\text{St}(p) \neq \emptyset$. Таким образом, $\text{St}(p)$ — подгруппа группы G .

2) Если $a, b \in G$, то

$$ap = bp \iff b^{-1}ap = p \iff b^{-1}a \in \text{St}(p) \iff a\text{St}(p) = b\text{St}(p).$$

Таким образом, установлена биекция между различными элементами орбиты $Gp = \text{Orb}(p)$ и множеством различных смежных классов $a\text{St}(p)$ по подгруппе $\text{St}(p)$: $ap \leftrightarrow a\text{St}(p)$.

В силу 2) число различных смежных классов по подгруппе $\text{St}(p)$ совпадает с $|\text{Orb}(p)|$. Применяя теорему Лагранжа, получаем: $|G| = |\text{Orb}(p)| \cdot |\text{St}(p)|$. В частности, $|\text{Orb}(p)| = \frac{|G|}{|\text{St}(p)|}$. \square

Лемма 1. Если $p' = ap \in \text{Orb}(p)$, $p \in M_G$, то:

1) $a \text{St}(p) = \{g \in G \mid gp = p'\}$;

2) $\text{St}(p') = a \text{St}(p) a^{-1}$ (т. е. $\text{St}(p')$ — подгруппа, сопряженная с подгруппой $\text{St}(p)$).

Доказательство.

1) Фактически, это уже было проверено в предыдущей теореме:

$$\begin{aligned} gp = p' &\iff gp = ap &\iff a^{-1}gp = p &\iff \\ &&&\iff a^{-1}g \in \text{St}(p) &\iff g \in a \text{St}(p). \end{aligned}$$

2) Действительно,

$$\begin{aligned} g \in \text{St}(p') &\iff gap = ap &\iff a^{-1}gap = p &\iff \\ &&&\iff a^{-1}ga \in \text{St}(p) &\iff g \in a \text{St}(p) a^{-1}. \quad \square \end{aligned}$$

ПРИМЕРЫ ПОЛИГОНОВ

ПРИМЕР 1. $M_G = \{1, 2, \dots, n\}_{S_n}$, где σi — значение подстановки $\sigma \in S_n$ на элементе i из $\{1, 2, \dots, n\}$. Так как $i(i, j) = j$ для цикла (i, j) , то это действие группы \mathbf{S}_n на $\{1, 2, \dots, n\}$ транзитивно. Ясно, что, например, $\text{St}(n) = \mathbf{S}_{n-1}$. Более общим образом, для любого множества M и группы всех биекций $\mathbf{S}(M)$ имеем полигон $M_{\mathbf{S}(M)}$.

ПРИМЕР 2. Пусть $\sigma \in \mathbf{S}_n$, (σ) — циклическая подгруппа в \mathbf{S}_n , порожденная подстановкой σ . Тогда: $\{1, 2, \dots, n\}_{(\sigma)}$ — полигон над группой (σ) , его различные орбиты — это в точности непересекающиеся циклы подстановки (σ) , перестановочные между собой.

ПРИМЕР 3 (РЕГУЛЯРНОЕ ПРЕДСТАВЛЕНИЕ ЛЕВЫМИ УМНОЖЕНИЯМИ). Пусть $M_G = G_G$ с умножением $(g, x) \rightarrow gx$ для $x \in G, g \in G$. Ясно, что: $(hg)x = h(gx)$ (для $x, g, h \in G$, ассоциативность умножения в группе); $ex = x$ для единицы e группы G .

Если $p, x \in G$, то $\text{St}(p) = \{g \in G \mid gp = p\} = \{e\}$ и $\text{Orb}(x) = Gx = G$ (т. е. это действие транзитивно).

Если $g \in G$, то рассмотрим отображение $\rho_g: G \rightarrow G, \rho_g x = gx$. Так как из $gx = gy$ для $x, y \in G$ следует (умножим на g^{-1} справа в группе G), что $x = y$, то ρ_g — мономорфизм. Так как для любого $z \in G$ имеем $z = gg^{-1}z$, то ρ_g — сюръекция.

Итак, $\rho_g \in \mathbf{S}(G)$.

Так как для $x, g, h \in G$ имеем

$$\rho_{hg}x = (hg)x = h(gx) = \rho_h(\rho_g x),$$

т. е. $\rho_{hg} = \rho_h \rho_g$, то отображение $\rho: G \rightarrow \mathbf{S}^r(G)$, $\rho(g) = \rho_g$, является гомоморфизмом групп.

Если $g, g' \in G$ и $\rho_g = \rho(g) = \rho(g') = \rho_{g'}$, то $g = eg = eg' = g'$.

Таким образом, ρ — инъективный гомоморфизмом.

Итак, мы доказали следующее утверждение.

Теорема 3 (Кэли). *Регулярное представление группы G правыми умножениями*

$$G \xrightarrow{\rho} \mathbf{S}^r(G) = \mathbf{S}(G), \quad g \rightarrow \rho_g, \quad \rho_g x = gx,$$

является инъективным гомоморфизмом.

Следствие 2. *Всякая группа G изоморфна некоторой подгруппе G' группы подстановок $\mathbf{S}(G)$ на множестве G .*

Следствие 3. *Если $n = |G| < \infty$, то группа G изоморфна некоторой подгруппе G' группы подстановок \mathbf{S}_n . С точностью до изоморфизма существует лишь конечное число групп порядка n .*

ЗАМЕЧАНИЕ 4. К сожалению, $|\mathbf{S}_n| = n!$, и подгрупп в \mathbf{S}_n из n элементов достаточно много.

ПРИМЕР 4. Пусть H — подгруппа группы G , рассмотрим полигон

$$M_H = G/H, \quad (hx) \rightarrow hx \text{ для } x \in G, h \in H.$$

Если $p, x \in G$, то

$$\text{St}(p) = \{h \in H \mid hp = p\} = \{e\}$$

и $\text{Orb}(x) = Hx$ — левый смежный класс Hx по подгруппе H , порожденный элементом $x \in G$.

Таким образом, в этом частном случае полигона G/H разбиение на орбиты превращается в хорошо знакомое нам разбиение группы в объединение непересекающихся различных левых смежных классов $G = \dot{\bigcup} Hx$, и как следствие подсчета элементов по орбитам имеем

$$|G| = \sum |\text{Orb}(x)| = \sum |Hx| = [G : H]|H|$$

(т. е. теорему Лагранжа).

ПРИМЕР 5 (ДЕЙСТВИЕ ГРУППЫ G ЛЕВЫМИ УМНОЖЕНИЯМИ НА МНОЖЕСТВЕ ПРАВЫХ СМЕЖНЫХ КЛАССОВ). Пусть H — подгруппа группы G ,

$$M_G = \{xH, x \in G\}, \quad g(xH)g = gxH \quad \text{для } x, g \in G.$$

Это умножение корректно:

если $xH = x'H$, то $x' = xh$, $h \in H$, и поэтому $gx' = gxh$, тогда $gx'H = gxH$.

Если $x, g_1, g_2 \in G$, то $(g_1g_2)(xH) = g_1(g_2(xH))$ и $e(xH) = xH$, т. е. $M_G = \{xH \mid x \in G\}_G$ — правый полигон над группой G .

Так как $\text{Orb}(xH) = M_G$, то это действие группы G транзитивно.

ПРИМЕР 6 (ДЕЙСТВИЕ ГРУППЫ G НА ГРУППЕ G СОПРЯЖЕНИЕМ). Пусть $M_G = G_G$, $(g, m) \rightarrow gmg^{-1} = \alpha_g m$ для $m, g \in G$.

Так как для $m, g, h \in G$ имеем

$$m\alpha_{hg} = (hg)m(hg)^{-1} = h(gmg^{-1})h^{-1} = \alpha_h(\alpha_g m),$$

т. е. $\alpha_{hg} = \alpha_h\alpha_g$,

$$\alpha_e m = em e^{-1} = m,$$

то $M_G = G_G$ с сопряжением — левый G -полигон.

КЛАССЫ СОПРЯЖЕННЫХ ЭЛЕМЕНТОВ

Если $x \in G$, то при сопряжении орбита элемента

$$\text{Orb}(x) = \{g x g^{-1} \mid g \in G\}$$

— это класс сопряженных элементов элемента x .

Ясно, что $\text{Orb}(e) = \{e\}$. Более того, $|\text{Orb}(x)| = 1 \iff x \in \mathbf{Z}(G)$, т. е. одноэлементные орбиты — это в точности элементы центра, поскольку $g x g^{-1} = x$ для всех $g \in G$ равносильно тому, что $x g = g x$ для всех $g \in G$, т. е. тому, что $x \in \mathbf{Z}(G)$.

Ясно, что

$$\text{St}(x) = \{g \mid g x g^{-1} = x\} = \mathbf{C}(x),$$

где $\mathbf{C}(x) = \{y \in G \mid x y = y x\}$ — централизатор элемента $x \in G$.

Таким образом, теорема о разбиении на орбиты в данном случае означает следующее.

Теорема 4 (о разбиении на классы сопряженных элементов). Пусть G — группа, тогда:

1) группа является объединением орбит — непересекающихся различных классов сопряженных элементов (т. е. отношение сопряженности $y \sim x$, если $y = g x g^{-1}$, является отношением эквивалентности);

2) число элементов конечной группы G , сопряженных с элементом $x \in G$, равно индексу централизатора $\mathbf{C}(x)$ элемента $x \in G$ в группе (поскольку $|G| = |\text{Orb}(x)| \cdot |\text{St}(x)| = \{ \text{число сопряженных с } x \text{ элементов} \} \cdot |\mathbf{C}(x)|$), т. е. числу $|G|/|\mathbf{C}(x)|$, и является делителем числа $|G|$. \square

ЦЕНТР КОНЕЧНОЙ p -ГРУППЫ

Теорема 5. *Фактор неабелевой группы по ее центру не может быть циклической группой.*

Доказательство. Предположим, что это не так, т. е. существует некоторая неабелева группа G такая, что $G/\mathbf{Z}(G) = G/Z$ — циклическая группа. Пусть тогда $G/Z = \langle gZ \rangle$. В этом случае любой элемент группы G представляется в виде произведения $g^k z$, где $z \in Z$.

Рассмотрим два произвольных элемента группы G — $g^k z_1$ и $g^l z_2$. Они коммутируют, так как элементы центра коммутируют со всеми элементами группы, а степени элемента g коммутируют между собой.

Таким образом, группа G — абелева, что противоречит предположению. \square

Теорема 6. *Пусть G — конечная p -группа, т. е. $|G| = p^k$, где p — простое число, $k \in \mathbb{N}$. Тогда ее центр нетривиален, т. е. $|\mathbf{Z}(G)| > 1$.*

Доказательство. Рассмотрим разбиение группы G на классы сопряженных элементов. Одноэлементный класс — это в точности элемент центра (один из них $\{e\}$). Содержащий больше одного элемента класс сопряженных элементов содержит p^l элементов, где $l > 1$ (как нетривиальный делитель числа $|G| = p^k$). Отсюда следует, что $|\mathbf{Z}(G)| > 1$ (в противном случае $p^k = 1 + pq$). \square

Теорема 7 (о коммутативности группы из p^2 элементов). Пусть G — конечная группа, $|G| = p^2$, где p — простое число. Тогда G — абелева группа.

Доказательство. В силу предыдущей теоремы $|\mathbf{Z}(G)| > 1$, т. е. $|\mathbf{Z}(G)| = p$ или $|\mathbf{Z}(G)| = p^2$. Но первый случай ($|\mathbf{Z}(G)| = p$) невозможен, поскольку тогда $|G/\mathbf{Z}(G)| = p^2/p = p$, и поэтому $G/\mathbf{Z}(G)$ — циклическая группа, что невозможно. Итак, $|\mathbf{Z}(G)| = p^2$, т. е. $G = \mathbf{Z}(G)$, и поэтому группа G коммутативна. \square

НОРМАЛИЗАТОРЫ ПОДГРУПП

ПРИМЕР 7. Пусть $L_G = L(G)$ — совокупность всех подгрупп H группы G , $(g, H) \rightarrow gHg^{-1}$, $g \rightarrow G$ (действие группы G на подгруппах сопряжением).

ОПРЕДЕЛЕНИЕ 3. Стабилизатор подгруппы H при этом действии группы G сопряжениями

$$\text{St}(H) = \{g \in G \mid gHg^{-1} = H\}$$

называется *нормализатором подгруппы H* в группе G (для него используется обозначение $\mathbf{N}_G(H)$).

Лемма 2 (свойства нормализатора $\mathbf{N}_G(H)$).

- 1) $\mathbf{N}_G(H)$ — подгруппа группы G , содержащая подгруппу H ;
- 2) $H \triangleleft \mathbf{N}_G(H)$;
- 3) если $H \triangleleft K \subseteq G$ (т. е. K — подгруппа группы G , содержащая подгруппу H и H — нормальная подгруппа в K), то $K \subseteq \mathbf{N}_G(H)$, и, таким образом, $\mathbf{N}_G(H)$ — наибольшая подгруппа, содержащая H в качестве нормальной подгруппы (конечно, если $H \triangleleft G$, то $\mathbf{N}_G(H) = G$).

Доказательство.

1) Так как $\mathbf{N}_G(H) = \text{St}(H)$, то ясно, что $\mathbf{N}_G(H)$ (как любой стабилизатор) — подгруппа группы G .

2) Если $g \rightarrow \mathbf{N}_G(H)$, то $gHg^{-1} = H$, т. е. $H \triangleleft \mathbf{N}_G(H)$ (т. е. H — нормальная подгруппа группы $\mathbf{N}_G(H)$).

3) Если $H \triangleleft K \subseteq G$, то для любого элемента $g \in K$ имеем $gHg^{-1} = H$ (поскольку H — нормальная подгруппа группы), т. е. $g \in \text{St}(H) = \mathbf{N}_G(H)$, и поэтому $K \subseteq \mathbf{N}_G(H)$. \square

УПРАЖНЕНИЕ 1. Если B — подгруппа, лежащая в нормализаторе $\mathbf{N}_G(A)$ подгруппы A группы G , то AB — подгруппа группы G и $AB/A \cong B/A \cap B$.

Теорема 8. Пусть G — p -группа, $|G| = p^r$, $r \geq 1$. Тогда группа G содержит нормальную подгруппу порядка p^{r-1} .

Доказательство. Проведем индукцию по r . Ясно, что утверждение верно при $r = 1$. Пусть оно верно для всех $k < r$, где $r > 1$.

В силу теоремы 6 $Z(G) \neq e$ (здесь $Z(G)$ — центр группы G). Так как p делит число $|Z(G)|$, то абелева группа $Z(G)$ содержит элемент g такой, что $p = O(g) = |\langle g \rangle|$. Ясно, что $N = \langle g \rangle \triangleleft G$ и $|G/N| = p^r/p = p^{r-1}$. В силу индуктивного предположения для p^{r-2} фактор-группа $\bar{G} = G/N$ содержит нормальную подгруппу $\bar{H} = H/N$, где H — нормальная подгруппа в G , $N \subset H \triangleleft G$, $|\bar{H}| = p^{r-2}$. Тогда $|H| = |\bar{H}| |N| = p^{r-2} \cdot p = p^{r-1}$. Итак, группа G содержит нормальную подгруппу H порядка p^{r-1} . \square

ПЕРВАЯ ТЕОРЕМА СИЛОВА

Одним из ярких результатов теории конечных групп в направлении частичного обращения теоремы Лагранжа являются следующие три теоремы Силова (1872).

Теорема 9 (первая теорема Силова о существовании силовских подгрупп). Пусть G — конечная группа, $|G| = n = p^k m$, $k \geq 1$, p — простое число, $(p, m) = 1$. Тогда группа G содержит подгруппу H такую, что $|H| = p^k$ (такая подгруппа называется силовской подгруппой группы G).

Доказательство.

1) Если G — абелева группа, $|G| = p^k m$, $(p, m) = 1$, то в качестве H можно взять примарную компоненту G_p группы G (т. е. прямую сумму всех p -примарных циклических групп канонического разложения), и тогда $G_p = p^k$.

2) Если $|G| = p^k$ (т. е. $m = 1$), то $G = H$.

3) Проведем доказательство индуктивно.

СЛУЧАЙ 1. p делит число $|\mathbf{Z}(G)|$ элементов центра $\mathbf{Z}(G)$ группы G .

Из обращения теоремы Лагранжа для абелевых групп найдется подгруппа A в центре $\mathbf{Z}(G)$, $|A| = p$.

Ясно, что $A \triangleleft G$, $|G/A| = n/p = p^{k-1}m < n$.

В силу индуктивного предположения в $\bar{G} = G/A$ найдется подгруппа \bar{B} , $|\bar{B}| = p^{k-1}$. Но $\bar{B} = B/A \subset G/A$, где $A \subseteq B \subseteq G$, поэтому

$$|B| = |A| |B/A| = pp^{k-1} = p^k,$$

т. е. B — силовская подгруппа группы G .

СЛУЧАЙ 2. p не делит порядок $|\mathbf{Z}(G)|$ центра $\mathbf{Z}(G)$ группы G .

Рассмотрим разложение группы на классы сопряженных элементов

$$G = \bigcup_{i=1, \dots, l} C_i.$$

Пусть C_1, \dots, C_r — одноэлементные классы сопряженных элементов (т. е. все элементы центра $\mathbf{Z}(G)$, $r = |\mathbf{Z}(G)|$).

Так как $|G|$ делится на p , а число r не делится на p , найдется орбита

$$C_i = \text{Orb}(x_i), \quad r+1 \leq i \leq l,$$

такая, что $|G|/|C(x_i)| = |C_i|$ не делится на p .

Тогда $|C(x_i)| < n$, но по индуктивному предположению в $C(x_i)$ найдется подгруппа H такая, что $|H| = p^k$, т. е. H — силовская подгруппа группы G ($H \subseteq C(x_i) \subseteq G$). \square

ВТОРАЯ ТЕОРЕМА СИЛОВА

Теорема 10 (вторая теорема Силова о сопряженности силовских подгрупп). Пусть G — конечная группа,

$$|G| = p^k m, \quad k \geq 1, \quad (p, m) = 1.$$

1) Любая p -подгруппа H группы G (т. е. $|H| = p^l$, $l \leq k$) содержится в некоторой силовской p -подгруппе.

2) Любые две силовские подгруппы S_1 и S_2 сопряжены (т. е. $S_2 = gS_1g^{-1}$ для некоторого $g \in G$).

Доказательство. Случай, когда $m = 1$, ясен. Пусть $m > 1$, и пусть S , $|S| = p^k$, — силовская p -подгруппа (существование которой доказано в первой теореме Силова).

Рассмотрим следующее левое действие подгруппой H :

$$M_H = \{xS \mid x \in G\}, \quad (a, xS) \rightarrow axS \text{ для } x \in G, a \in H$$

(т. е. правые смежные классы xS подгруппы S с умножением слева на элементы из подгруппы H); корректность умножения ясна:

$$xS = x'S \implies x' = xs, \quad ax' = (ax)s \implies ax'S = axS.$$

Из теоремы Лагранжа для подгруппы S :

$$|M| = |G|/|S| = p^k m / p^k = m > 1,$$

при этом $(p, m) = 1$.

Так как

$$p^l = |H| = |\text{St}(y)| \cdot |\text{Orb}(y)|$$

для элемента $y \in M_H$, то число элементов в каждой неоднородной орбите действия M_H делится на p .

Следовательно, существует одноэлементная орбита $xS \in M_H$, $x \in G$, т. е. для xS имеем $HxS = xS$.

Но тогда $Hx \subseteq xS$, и поэтому $H \subseteq xSx^{-1}$. Так как

$$|xSx^{-1}| = |S| = p^k,$$

то xSx^{-1} является силовской p -подгруппой, содержащей исходную p -подгруппу H .

Если же H — силовская p -подгруппа, т. е. $|H| = p^k$, то $H = xSx^{-1}$. Тем самым показано, что любые две силовские подгруппы $S_1 = S$ и $S_2 = H$ сопряжены между собой. \square