ЛЕКЦИЯ 10

ТРЕТЬЯ ТЕОРЕМА СИЛОВА

ПРИМЕНЕНИЕ ТЕОРЕМ СИЛОВА

ГРУППЫ ПОДСТАНОВОК

ПРОСТОТА ГРУППЫ $\mathbf{A}_5$

ТРЕТЬЯ ТЕОРЕМА СИЛОВА

Теорема 1 (третья теорема Силова о числе силовских подгрупп)**.** *Пусть G — конечная группа, $n = |G| = p^k m$, $k \geqslant 1$, $(p, m) = 1$. Через $n(p)$ обозначим число силовских p-подгрупп. Тогда*:

1) *$n(p)$ — делитель числа $n = |G|$;*

2) *$n(p) = 1 + pq$ (т. е. остаток при делении числа $n(p)$ на простое число p равен* 1).

Доказательство.

1) Рассмотрим левое действие группой G

$$M_G = L(G) = \{H \mid H \subseteq G\},$$
$$(H, g) \to gHg^{-1}, \quad g \in G$$

(т. е. группа G действует на множестве всех подгрупп H группы G сопряжением).

В силу второй теоремы Силова *все* силовские p-подгруппы образуют одну из орбит $\operatorname{Orb}(S)$ в M_G, где S — одна из силовских подгрупп группы G, $n(p) = |\operatorname{Orb}(S)|$. Так как

$$|G| = |\operatorname{St}(S)| \cdot |\operatorname{Orb}(S)|,$$

то ясно, что $n(p) = |\operatorname{Orb}(S)|$ — делитель числа $n = |G|$.

2) Рассмотрим теперь множество *всех* силовских p-подгрупп $\Sigma_{S_1} = \{S_1, \ldots, S_{n(p)}\}_{S_1}$ как левый S_1-полигон (здесь $S = S_1$) с сопряжением:

$$(a, S_i) \to aS_ia^{-1}, \quad S_i \in \Sigma, \ \ a \in S_1$$

(ясно, что $|aS_ia^{-1}| = |S_i| = p^k$, т. е. $aS_ia^{-1} \in \Sigma$).

а) Ясно, что $aS_1a^{-1} = S_1$ для $a \in S_1$, т. е. S_1 — неподвижная точка в Σ при действии группы S_1 (т. е. одноэлементная орбита в Σ_{S_1}). Покажем, что S_1 — единственная неподвижная точка.

Действительно, допустим противное, т. е. что $|\operatorname{Orb}(S_i)| = 1$ для $i \neq 1$, т. е. $aS_ia^{-1} = S_i$ для всех $a \in S_1$. Следовательно, $S_1S_i = S_iS_1$, и поэтому подмножество $H = S_iS_1 = S_1S_i$ является подгруппой.

По теореме Лагранжа для подгруппы H имеем:

$$|G| = |H| \cdot [G : H],$$

таким образом, S_1 и S_i также являются силовскими p-подгруппами и в группе H; применяя к ним в группе H вторую теорему Силова, получаем, что

$$S_1 = hS_ih^{-1}$$

для

$$h = ab \in H = S_1S_i, \quad a \in S_1, \ b \in S_i.$$

Но тогда

$$S_1 = hS_ih^{-1} = (ba)S_i(ba)^{-1} = b(aS_ia^{-1})b^{-1} = bS_ib^{-1} = S_i$$

(здесь мы использовали равенство $aS_ia^{-1} = S_i$, поскольку S_i — орбита, состоящая из одного элемента), но это противоречит тому, что $i > 1$, т. е. $S_i \neq S_1$.

б) *Завершение доказательства третьей теоремы Силова.*

Итак, рассматривая для полигона $\Sigma_{S_1} = \{S_1, \ldots, S_{n(p)}\}$ разбиение на орбиты, имеем единственную одноэлементную орбиту $\mathrm{Orb}\,(S_1) = \{S_1\}$, при этом при $i > 1$ для других орбит (содержащих более одного элемента)

$$p^k = |S_1| = |\,\mathrm{St}\,(S_i)|\,|\,\mathrm{Orb}\,(S_i)|,$$

т. е. число элементов в этих орбитах делится на p (как делитель числа p^k). Таким образом,

$$n(p) = 1 + pq. \qquad \square$$

СЛЕДСТВИЯ ИЗ ТЕОРЕМ СИЛОВА

Следствие 1. *В конечной группе силовская p-группа единственна (т. е. $n(p) = 1$) тогда и только тогда, когда эта силовская подгруппа является нормальной подгруппой.*

Следствие 2 (обращение теоремы Лагранжа для конечных p-групп)**.** *Пусть G — конечная p-группа, $|G| = p^k$.*

Тогда для любого делителя p^l, $l \leqslant k$, числа p^k существует подгруппа H группы G такая, что $|H| = p^l$.

Доказательство (*индукцией по k*). Случай $k = 0$ ясен.

Пусть $|G| = p^k > 1$.

В силу теоремы о центре $\mathbf{Z}(G)$ p-группы G имеем $|\mathbf{Z}(G)| > 1$.

В силу следствия из структурной теоремы для конечной абелевой группы $\mathbf{Z}(G)$ имеет место обращение теоремы Лагранжа.

В частности, для делителя p числа $p^l = |H|$ найдется циклическая подгруппа (c) из p элементов в группе $\mathbf{Z}(G)$.

Ясно, что $(c) \lhd G$.

Тогда для фактор-группы $\bar{G} = G/(c)$ имеем: $|\bar{G}| = |G|/p = p^{k-1}$. В силу индуктивного предположения (так как $p^{k-1} < p^k$) в $\bar{G}$ найдется подгруппа $\bar{H}$ такая, что $|\bar{H}| = p^{l-1}$, при этом $\bar{H} = H/(c)$, где H — подгруппа группы G такая, что $(c) \subseteq H \subset G$. Так как

$$|H| = |\bar{H}|\,|(c)| = p^{l-1} \cdot p = p^l,$$

то подгруппа H является искомой. □

Следствие 3. *Если $M \lhd G$ и P — силовская p-подгруппа группы M, $\mathbf{N}_G(P)$ — нормализатор подгруппы P в G, то*

$$M \cdot \mathbf{N}_G(P) = G.$$

Доказательство. Пусть $g \in G$. Тогда

$$gPg^{-1} \subseteq gMg^{-1} = M,$$

поэтому P и gPg^{-1} — две силовские p-подгруппы группы M. По второй теореме Силова подгруппы P и gPg^{-1} сопряжены с помощью элемента $h \in M$,

$$hPh^{-1} = gPg^{-1},$$

поэтому

$$g^{-1}hP(g^{-1}h)^{-1} = P.$$

Таким образом,

$$g^{-1}h \in \mathbf{N}_G(P),$$

и поэтому

$$g = hh^{-1}g = h(g^{-1}h) \in M \cdot \mathbf{N}_G(P).$$

Итак,

$$M \cdot \mathbf{N}_G(P) = G. \qquad \square$$

ГРУППЫ ИЗ 15 ЭЛЕМЕНТОВ

Пусть G — конечная группа, $|G| = 15 = 3 \cdot 5$. Рассматривая все делители 1, 3, 5, 15 числа 15, видим, что $n(3) = 1$ и $n(5) = 1$. Поэтому существуют единственные (и поэтому нормальные) силовские 3-подгруппа A и 5-подгруппа B.

Из $A \lhd G$, $B \lhd G$ следует, что AB — подгруппа. Так как $|A| = 3$, $|B| = 5$, то $A \cong \mathbb{Z}_3$, $B \cong \mathbb{Z}_5$, $|A \cap B| = 1$, т. е. $A \cap B = \{e\}$.

Поэтому $AB = A \times B$ и $|AB| = 3 \times 5 = 15$, т. е. $AB = G$.

Итак, $G = A \times B \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{15}$, т. е. существует лишь единственная (с точностью до изоморфизма) конечная группа из 15 элементов — циклическая группа $\mathbb{Z}_{15}$. □

Упражнение 1.

1) Докажите, что если $|G| = 175 = 5^2 \cdot 7$, то группа G абелева.

2) Опишите все группы из 12 элементов.

ГРУППЫ ПОДСТАНОВОК

Напомним, что мы рассматриваем группу подстановок $\mathbf{S}_n$ с записью умножения слева от аргумента: $(\sigma\tau)(i) = \sigma\big(\tau(i)\big)$.

Заметим, что:

$$(i_1\, i_2\, \ldots\, i_k) = (i_1\, i_k)(i_1\, i_{k-1}) \ldots (i_1\, i_2)$$

(в частности, $(1\,2\,\ldots\,k) = (1\,k)(1\,k{-}1)\ldots(1\,2)$); $(i\,j) = (1\,i)(1\,j)(1\,i)$ для $1 \neq i$, $1 \neq j$.

Нам будут полезны разные системы образующих группы $\mathbf{S}_n$:

$$\mathbf{S}_n = \langle (i\,j),\ i \neq j \rangle = \langle (1\,2), (1\,3), \ldots, (1\,n) \rangle.$$

Лемма 1.

$$\tau(1, 2, \ldots, k)\tau^{-1} = \big(\tau(1), \ldots, \tau(k)\big)$$

$(\tau^{-1}(1, 2, \ldots, k)\tau = (\tau^{-1}(1), \ldots, \tau^{-1}(k))$.

Доказательство. Если $\sigma(i) = j$, $\tau(i) = s$, $\tau(j) = t$, то

$$(\tau\sigma\tau^{-1})(s) = (\tau\sigma\tau^{-1})\big(\tau(i)\big) = (\tau\sigma)(i) = \tau(j) = t. \qquad \square$$

Теорема 2. *Две подстановки $\sigma, \gamma \in \mathbf{S}_n$ сопряжены тогда и только тогда, когда они имеют одинаковое цикловое разложение.*

Доказательство.

1) Если $\gamma = \tau\sigma\tau^{-1}$ и $\sigma = \sigma_1 \dots \sigma_r$ — разложение подстановки σ в произведение циклов с непересекающимися орбитами, то

$$\gamma = (\tau\sigma_1\tau^{-1})(\tau\sigma_2\tau^{-1}) \dots (\tau\sigma_r\tau^{-1}),$$

$\{\tau\sigma_i\tau^{-1}\}$ — циклы, орбиты которых являются образами орбит циклов σ_i, и поэтому эти орбиты дают разбиение множества $\{1, 2, \dots, n\}$. Таким образом, подстановки γ и σ имеют одинаковые цикловые разложения.

2) Если γ и σ имеют одинаковое цикловое разложение, то соответствие между элементами соответствующих орбит приводит нас к биекции τ, т. е. $\sigma \in \mathbf{S}_n$, для которой $\gamma = \tau\sigma\tau^{-1}$. $\square$

Лемма 2. *Для циклов длины* 2 τ_1, τ_2 (*т. е. для транспозиций*) *группы* $\mathbf{S}_n$ *при* $n \geqslant 3$ *произведение* $\tau_1\tau_2$ — *либо* 3*-цикл, либо произведение двух* 3*-циклов.*

Доказательство.

Случай 1. Если $\tau_1 = \tau_2$, то

$$\tau_1\tau_2 = \tau_1^2 = e = (i\,j\,k)(k\,j\,i).$$

Случай 2. $\tau_1 \neq \tau_2$.

2а) орбиты пересекаются (по одному элементу i):

$$(i\,k)(i\,l) = (i\,l\,k),$$

здесь $k \neq l$.

2б) Орбиты транспозиций τ_1 и τ_2 не пересекаются:

$$(i\,j)(k\,l) = (i\,l\,j)(i\,l\,k). \qquad \square$$

Теорема 3. $\mathbf{A}_n = \langle\{(i\,j\,k)\}\rangle = \langle(1\,2\,3), (1\,2\,4), \ldots, (1\,2\,n)\rangle$ *при* $n \geqslant 3$.

Доказательство.

1) Если $\sigma \in \mathbf{A}_n$, $n \geq 3$, то $\sigma = \tau_1 \ldots \tau_{2m}$, где τ_i — транспозиция (цикл длины 2). Так как $\tau_{2i-1}\tau_{2i}$ — или 3-цикл, или произведение двух 3-циклов, то

$$\mathbf{A}_n = \langle\{(i, j, k)\}\rangle.$$

2)

$$\begin{aligned}(i\,j\,k) &= (1\,2\,i)(2\,j\,k)(1\,2\,i)^{-1};\\ (2\,j\,k) &= (1\,2\,j)(1\,2\,k)(1\,2\,j)^{-1};\\ (1\,j\,k) &= (1\,2\,k)^{-1}(1\,2\,j)(1\,2\,k).\end{aligned}$$

□

Упражнение 2. $\mathbf{A}_5 = \langle(2\,5\,4), (1\,2\,3\,4\,5)\rangle$.

Теорема 4.

1) $[\mathbf{S}_2, \mathbf{S}_2] = \{e\}$; $[\mathbf{S}_n, \mathbf{S}_n] = \mathbf{A}_n$ *при* $n \geqslant 3$.

2) $[\mathbf{A}_3, \mathbf{A}_3] = \{e\}$; $[\mathbf{A}_4, \mathbf{A}_4] = \mathbf{V}_4$; $[\mathbf{A}_n, \mathbf{A}_n] = \mathbf{A}_n$ *при* $n \geqslant 5$.

Доказательство.

1) Так как $[a, b] = a^{-1}b^{-1}ab$ для $a, b \in \mathbf{S}_n$ всегда является четной подстановкой, то $[\mathbf{S}_n, \mathbf{S}_n] \subseteq \mathbf{A}_n$.

Так как $\mathbf{A}_n = \langle\{(i\,j\,k)\}\rangle$ и

$$(i\,j\,k) = (i\,j)(i\,k)(i\,j)(i\,k) = [(i\,j), (i\,k)],$$

то $\mathbf{A}_n \subseteq [\mathbf{S}_n, \mathbf{S}_n]$.

2а) Так как

$$[(i\,j\,k), (i\,j\,l)] = (k\,j\,i)(l\,j\,i)(i\,j\,k)(i\,j\,l) = (i\,j)(k\,l),$$
$$[(i\,j\,k), (i\,l\,j)] = (k\,j\,i)(j\,l\,i)(i\,j\,k)(i\,l\,j) = (i\,k)(j\,l),$$

то $\mathbf{V}_4 \subseteq [\mathbf{A}_4, \mathbf{A}_4]$.

Так как $|\mathbf{A}_4/\mathbf{V}_4| = 12/4 = 3$, то $\mathbf{A}_4/\mathbf{V}_4$ — абелева группа, поэтому $[\mathbf{A}_4, \mathbf{A}_4] \subseteq \mathbf{V}_4$. Итак, $[\mathbf{A}_4, \mathbf{A}_4] = \mathbf{V}_4$.

2б) При $n \geqslant 5$ для $\{i, j, k\}$ найдутся $l, m \notin \{i, j, k\}$, $l \neq m$. Поэтому

$$(i\,j\,k) = (i\,j\,m)(i\,k\,l)(m\,j\,i)(l\,k\,i) = [(m\,j\,i), (l\,k\,i)],$$

таким образом, $\mathbf{A}_n \subseteq [\mathbf{A}_n, \mathbf{A}_n]$, и следовательно, $\mathbf{A}_n = [\mathbf{A}_n, \mathbf{A}_n]$ при $n \geqslant 5$. □

Упражнение 3. Каждый элемент группы $\mathbf{A}_5$ является коммутатором.

ПРОСТЫЕ ГРУППЫ

Группа G называется *простой*, если у нее нет нормальных подгрупп $N \lhd G$, отличных от $\{e\}$ и G.

Замечание 1. Простые абелевы группы — это в точности циклические группы простого порядка. Действительно, в абелевой группе любая подгруппа нормальна. Поэтому простая абелева группа является циклической. В группе $\mathbb{Z}$ много подгрупп, в частности $2\mathbb{Z}$, т. е. она не является простой. Если $G = (a)$, $O(a) = n = kl$, то $(a^k) \subset (a)$, и группа G не является простой. Итак, $G(a)$ — простая группа тогда и только тогда, когда $|G| = \emptyset(a) = p$.

Замечание 2. Если $|G| = p^k$, $k > 1$, — конечная p-группа из p^k, $k > 1$, элементов, то G не является простой. Действительно, $e \neq \mathbf{Z}(G) \lhd G$.

Теорема о классификации конечных простых групп, видимо, завершена, ее полное связное доказательство создается.

Мы докажем теорему о том, что при $n \geqslant 5$ группа $\mathbf{A}_n$ является простой (в частности, $\mathbf{A}_5$ — простая группа).

Лемма 3. *При $n \geqslant 5$ любые два 3-цикла в группе $\mathbf{A}_n$ сопряжены.*

Доказательство. Пусть $\sigma_1 = (1\,2\,3)$, $\sigma_2 = (a\,b\,c) \in \mathbf{A}_n$, $n \geqslant 5$. Найдется $\tau \in \mathbf{S}_n$, для которой $\sigma_2 = \tau(1\,2\,3)\tau^{-1}$.

а) Если $\tau \in \mathbf{A}_n$, то все доказано.

б) Если $\tau \in \mathbf{S}_n \setminus \mathbf{A}_n$, то $\rho = \tau(4\,5) \in \mathbf{A}_n$, $(4\,5) \in \mathbf{C}_{\mathbf{A}_5}\big((1\,2\,3)\big)$. Тогда

$$\rho(1\,2\,3)\rho^{-1} = \tau(4\,5)(1\,2\,3)(4\,5)^{-1}\tau^{-1} = \tau(1\,2\,3)\tau^{-1} = \sigma_2. \qquad \square$$

Лемма 4. *Подстановки вида $(1\,2)(3\,4)$ и $(a\,b)(c\,d)$ сопряжены в $\mathbf{A}_n$ при $n \geqslant 5$.*

Доказательство. Пусть $m = 5$ (отличный от 1, 2, 3, 4). Тогда $(3\,4\,m)(1\,2)(3\,4)(3\,4\,m)^{-1} = (1\,2)(4\,m)$. $\square$

Теорема 5. $\mathbf{A}_5$ — *простая* (*некоммутативная*) *группа.*

Доказательство. Пусть $\{e\} \neq H \lhd \mathbf{A}_5$.

Случай 1. Пусть $(a\,b\,c) \in H$. Тогда и все сопряженные с ним циклы длины 3 лежат в H, а циклы длины три порождают все $\mathbf{A}_5$, поэтому $H = \mathbf{A}_5$.

Случай. 2. $\alpha = (a\,b\,c\,d\,e) \in H$. Тогда

$$(a\,b)(c\,d)(a\,b\,c\,d\,e)(a\,b)(c\,d) = (b\,a\,d\,c\,e) \in H,$$
$$(b\,a\,d\,c\,e)(a\,b\,c\,d\,e) = (b\,e\,d) \in H,$$

и поэтому (случай 1) $H = \mathbf{A}_5$.

Случай 3. $(a\,b)(c\,d) \in H$. Тогда

$$(a\,b\,c\,e\,d) = (d\,e)(a\,c)(c\,d)(a\,b) \in H,$$

и (случай 2) поэтому $H = \mathbf{A}_5$. □