

ЛЕКЦИЯ 9

ПРОСТОТА ГРУППЫ A_n

ТЕОРЕМЫ СИЛОВА

ПРИМЕНЕНИЕ ТЕОРЕМ СИЛОВА

ПРОСТОТА ГРУППЫ A_n

Мы доказываем теорему о том, что при $n \geq 5$ группа A_n является простой. Напомним ключевые леммы предыдущей лекции.

ЛЕММА 1. При $n \geq 5$ любые два 3-цикла в группе A_n сопряжены.

ЛЕММА 2. Подстановки вида $(12)(34)$ и $(ab)(cd)$ сопряжены в A_n при $n \geq 5$.

ТЕОРЕМА 1. A_n , $n \geq 5$, — простая (некоммутативная) группа.

Доказательство. Пусть $\{e\} \neq H \triangleleft A_n$.

Если $\sigma = (abc) \in H$, то теорема доказана, так как циклы длины три сопряжены в A_n , $n \geq 5$, и порождают A_n .

Пусть H содержит некоторую подстановку σ , в разложении которой на непересекающиеся циклы есть цикл длины $ge4$, т.е. $\sigma = (abcd \dots)\sigma_2 \dots \sigma_k$.

Тогда

$$\begin{aligned}\sigma' &= (abc)\sigma(cba) = (abc)(abcd \dots)(cba)\sigma_2 \dots \sigma_k = \\ &= (bcad \dots)\sigma_2 \dots \sigma_k \in H,\end{aligned}$$

откуда

$$\sigma'\sigma^{-1} = (bcad \dots)(abcd \dots)^{-1} = (bda) \in H,$$

т.е. $H = A_n$.

Таким образом, мы можем считать, что в подгруппе H все подстановки при разложении в произведение непересекающихся циклов имеют только циклы длин два и три.

Если подстановка $\sigma \in H$ состоит не только из циклов длины три, то в ее разложении есть по крайней мере две транспозиции (так как она четна):

$$\sigma = (ab)(cd)\sigma_3 \dots \sigma_k.$$

В этом случае

$$\begin{aligned} \sigma' &= (abc)\sigma(cba) = (abc)(ab)(cd)(cba)\sigma_3 \dots \sigma_k = \\ &= (ad)(cb)\sigma_3 \dots \sigma_k \in H, \end{aligned}$$

откуда в H содержится подстановка $\sigma'\sigma^{-1}$, равная $(ac)(bd)$.

Таким образом, подгруппа H содержит все пары непересекающихся транспозиций, которые порождают \mathbf{A}_n .

Остался только случай, когда σ есть произведение непересекающихся циклов длины три, где циклов в разложении больше одного:

$$\sigma = (abc)(def)\sigma_3 \dots \sigma_k \in H.$$

Тогда

$$\begin{aligned} \sigma' &= (bcd)\sigma(dcb) = (bcd)(abc)(def)(dcb)\sigma_3 \dots \sigma_k = \\ &= (acd)(bef)\sigma_3 \dots \sigma_k \in H, \end{aligned}$$

после чего

$$\sigma'\sigma^{-1} = (acd)(bef)(cba)(fed) = (adbce) \in H,$$

откуда по предыдущему $H = \mathbf{A}_n$. □

ПЕРВАЯ ТЕОРЕМА СИЛОВА

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

ТЕОРЕМА 2 (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 $C_i = \text{Orb}(x_i)$, $r + 1 \leq i \leq l$, 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 3 (ВТОРАЯ ТЕОРЕМА СИЛОВА О СОПРЯЖЕННОСТИ СИЛОВСКИХ ПОДГРУПП). Пусть G — конечная группа, $|G| = p^k m$, $k \geq 1$, $(p, m) = 1$.

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 : $M_H = \{xS \mid x \in G\}$, $(a, xS) \rightarrow axS$ 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: $xS = x'S \implies x' = xs$, $ax' = (ax)s \implies ax'S = axS$.

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

ТРЕТЬЯ ТЕОРЕМА СИЛОВА

ТЕОРЕМА 4 (ТРЕТЬЯ ТЕОРЕМА СИЛОВА О ЧИСЛЕ СИЛОВСКИХ ПОДГРУПП). Пусть G — конечная группа, $n = |G| = p^k m$, $k \geq 1$, $(p, m) = 1$. Через $n(p)$ обозначим число силовских p -подгрупп. Тогда:

- 1) $n(p)$ — делитель числа $n = |G|$;
- 2) $n(p) \equiv 1 \pmod{p}$ (т. е. остаток при делении числа $n(p)$ на простое число p равен 1).

Доказательство.

1) Рассмотрим левое действие группой G

$$M_G = L(G) = \{H \mid H \subseteq G\},$$

$$(H, g) \rightarrow gHg^{-1}, \quad g \in G$$

(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 $\text{Orb}(S)$ в M_G , где S — одна из силовских подгрупп группы G , $n(p) = |\text{Orb}(S)|$. Так как $|G| = |\text{St}(S)| \cdot |\text{Orb}(S)|$, то ясно, что $n(p) = |\text{Orb}(S)|$ — делитель числа $n = |G|$.

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

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

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

а) Ясно, что $aS_1 a^{-1} = S_1$ 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 $|\text{Orb}(S_i)| = 1$ для $i \neq 1$, т. е. $aS_i a^{-1} = S_i$ для всех $a \in S_1$. Следовательно, $S_1 S_i = S_i S_1$, и поэтому подмножество $H = S_i S_1 = S_1 S_i$ 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 $S_1 = hS_i h^{-1}$ для $h = ab \in H = S_1 S_i$, $a \in S_1$, $b \in S_i$.

Но тогда

$$S_1 = hS_i h^{-1} = (ba)S_i (ba)^{-1} = b(aS_i a^{-1})b^{-1} = bS_i b^{-1} = S_i$$

(здесь мы использовали равенство $aS_i a^{-1} = S_i$, 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 $\Sigma_{S_1} = \{S_1, \dots, S_{n(p)}\}$ разбиение на орбиты, имеем единственную одноэлементную орбиту $\text{Orb}(S_1) = \{S_1\}$, при этом при $i > 1$ для других орбит (содержащих более одного элемента)

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

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

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

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 , $l \leq k$, 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 : $|\mathbf{Z}(G)| > 1$. В силу следствия из структурной теоремы для конечной абелевой группы $\mathbf{Z}(G)$ имеет место обращение теоремы Лагранжа. В частности, для делителя p числа $p^l = |\mathbf{Z}(G)|$ найдется циклическая подгруппа (c) из p элементов в группе $\mathbf{Z}(G)$. Ясно, что $(c) \triangleleft G$. 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 $(c) \subseteq H \subseteq G$. Так как

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

то подгруппа H является искомой. □

СЛЕДСТВИЕ 3. Если $M \triangleleft G$ 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,

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

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 $A \triangleleft G$, $B \triangleleft G$ 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} . \square

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

2) Описать все группы из 12 элементов.

ПРИМЕНЕНИЕ ТЕОРЕМ СИЛОВА ДЛЯ ДОКАЗАТЕЛЬСТВА НЕПРОСТОТЫ КОНЕЧНОЙ ГРУППЫ

ЛЕММА 3. *Не существует неабелевых простых групп G порядка $|G| = p^l m$, где p — простое число, p не делит m , p^l не делит $(m - 1)!$.*

Доказательство. Допустим противное, пусть G — такая группа. Тогда G содержит силовскую p -подгруппу S , $|S| = p^l$, $(G : S) = m$. Так как конечные неабелевы p -группы не являются простыми (центр является нетривиальной нормальной подгруппой), то можно считать, что $m > 1$. Ясно (действие на множестве смежных классов G по S), что существует гомоморфизм $\varphi: G \rightarrow \mathbf{S}_m$ такой, что $\ker \varphi \subseteq S$. Так как G — простая группа, то $\ker \varphi = \{e\}$, т. е. φ — инъекция. Поэтому $G \cong \varphi(G) \subseteq \mathbf{S}_m$. По теореме Лагранжа $p^l m \mid m!$, следовательно, $p^l \mid (m - 1)!$, что противоречит нашему предположению. \square

ЛЕММА 4. *Если p — простое число, G — конечная p -группа и $|G| > p$, то группа G не является простой.*

Доказательство. Центр $\mathbf{Z}(G)$ нетривиален, при этом $\mathbf{Z}(G) \triangleleft G$.

Если $\mathbf{Z}(G) \neq G$, то группа G не является простой.

Если $\mathbf{Z}(G) = G$, то G — абелева группа. Если она простая, то $|G| = p$, что противоречит нашему предположению. \square

ТЕОРЕМА 5. Среди конечных групп G , порядок которых меньше чем 60, $|G| < 60$, нет неабелевых простых групп.

Доказательство. В силу двух предшествующих лемм из чисел $2, 3, \dots, 59$ надо рассмотреть лишь случаи $n = |G| = 30, 40, 56$.

а) Пусть есть простая группа G , $n = |G| = 30 = 2 \cdot 3 \cdot 5$. Пусть S — силовская 5-подгруппа простой группы G , $|S| = 5$. Число r_5 сопряженных силовских 5-подгрупп (как делитель 30 и $r_5 \equiv 1 \pmod{5}$) равно 1 или 6. Но если $r_5 = 1$, то $S \triangleleft G$, что противоречит простоте группы G . Итак, $r_5 = 6$, при этом пересечение любых двух различных силовских 5-подгрупп из пяти элементов каждая равно $\{e\}$. Итак, их объединение содержит 24 неединичных элемента.

Аналогично число r_3 силовских 3-подгрупп равно 10 ($r_3 \neq 1$, r_3 — делитель 30, $r_3 \equiv 1 \pmod{3}$), в их объединении 20 неединичных элементов.

Так как $24 + 20 = 44 > 30$, то получаем противоречие. Итак, группа G с $|G| = 30$ не может быть простой.

б) Пусть есть простая группа G , $n = |G| = 40 = 2^3 \cdot 5$. Пусть S — силовская 5-подгруппа группы G . Так как $r_5 = 1$ ($r \mid 40$, $r \equiv 1 \pmod{5}$), то $P \triangleleft G$, и поэтому группа G не может быть простой.

в) Пусть есть простая группа G , $n = |G| = 56 = 2^3 \cdot 7$. Пусть S — силовская 7-подгруппа группы G . Так как $r_7 = 8$ ($r_7 \mid 56$, $r_7 \equiv 1 \pmod{7}$) и пересечение любых двух различных подгрупп из семи элементов равно $\{e\}$, то их объединение содержит 48 неединичных элементов.

Силовская 2-подгруппа содержит восемь элементов, поэтому $48 + 8 = 56 = |G|$, но $r_8 > 1$ (если $r_8 = 1$, то эта силовская подгруппа из восьми

элементов нормальна, что противоречит простоте нашей группы G), однако для неединичных элементов второй силовской 2-подгруппы в нашем балансе подсчета элементов уже нет места. Получили противоречие. \square