

ЛЕКЦИЯ 10

ЦЕНТР КОНЕЧНОЙ p -ГРУППЫ

НОРМАЛИЗАТОРЫ ГРУПП

ТЕОРЕМЫ СИЛОВА

ПРИМЕНЕНИЕ ТЕОРЕМ СИЛОВА

ЦЕНТР КОНЕЧНОЙ p -ГРУППЫ

Теорема 1. *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 2. *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 3 (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 1. 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 1. 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 1 (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 4. 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 2 $Z(G) \neq e$ (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 5 (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 6 (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

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

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 7 (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

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

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)

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

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

$$n(p) = 1 + pq.$$

□

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 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 $(c) \triangleleft G$.

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 $(c) \subseteq H \subset G$. 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,

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

□

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 2.

- 1) Докажите, что если $|G| = 175 = 5^2 \cdot 7$, то группа G абелева.
- 2) Опишите все группы из 12 элементов.