Лекция 8

Определение 1. Пусть G – конечная группа порядка $|G| = p^k m$, где p – простое число, а m – число не делящееся на p. Подгруппа $S \subset G$ называется *силовской p-подгруппой* в G, если $|S| = p^k$.

Теорема 1 (Первая теорема Силова)**.** *Для каждого простого числа p существует силовская p-подгруппа $S \subset G$.*

Доказательство. Докажем данное утверждение индукцией по $|G|$. Базой индукции будет случай, когда $|G|$ не делится на p. Тогда $S = \{e\}$.

Проведем шаг индукции.

Случай 1. $|Z(G)|$ делится на p.

$Z(G)$ – абелева группа. В ней найдется некая подгруппа A такая, что $|A| = p$. Ясно, что A – нормальная подгруппа в G. При этом $|G/A| = \frac{n}{p}$, где $n = |G|$. По предположению индукции в G/A есть силовская p-подгруппа B. Рассмотрим $\pi_A^{-1}(B) \subset G$. Имеем, $|\pi_A^{-1}(B)| = |\mathrm{Ker}\,(\pi_a \mid_{\pi_A^{-1}(B)})| \cdot |\mathrm{Im}\,(\pi_a \mid_{\pi_A^{-1}(B)})| = |A| \cdot |B| = p^k$. Можно взять $S = \pi_A^{-1}(B)$.

Случай 2. $|Z(G)|$ не делится на p.

Расмотрим разложение группы G на классы сопряженных элементов. Классы сопряженности, состоящие из одного элемента – это элементы центра. Так как $|G|$ делится на p (иначе мы в условиях базы индукции), найдется класс сопряженности C такой, что $|C| \neq 1$ не делится на p. Пусть $g \in C$. Рассмотрим $|Z(g)| = \frac{|G|}{|C|} < |G|$. С другой стороны, $|Z(g)|$ делится на p^k. По предположению индукции есть силовская подгруппа $S \subset Z(g) \subset G$, при этом $|S| = p^k$. □

Лемма 1. *Если силовская подгруппа единственна, то она нормальна.*

Доказательство. Рассмотрим gSg^{-1} – это подгруппа G (проверьте это). Но $|gSg^{-1}| = |S|$. В самом деле, очевидно, что $|gSg^{-1}| \leq |S|$, с другой стороны, $S = g^{-1}(gSg^{-1})g$, значит, $S \leq |gSg^{-1}|$. Имеем, gSg^{-1} – силовская подгруппа G, а значит, $gSg^{-1} = S$, то есть S нормальна. □

Теорема 2 (Вторая теорема Силова)**.** *1) Любая p-подгруппа G содержится в некоторой силовской.*

2) Любые две силовские p-подгруппы сопряжены.

Доказательство. Случай $m = 1$ ясен. Пусть $m > 1$.

1) Пусть S – силовская p-подгруппа, $|S| = p^k$. Пусть $H \subset G$ – подгруппа порядка p^l, $l \leq k$. Рассмотрим действие H на множестве левых смежных классов по S:

$$h \cdot gS = (hg)S.$$

Корректность очевидна: если $gS = g'S$, то $g' = gs$ для некоторого $s \in S$. Тогда $hg' = hgs$ и $hgS = hg'S$. Из теоремы Лагранжа количество левых смежных классов по S равно $\frac{|G|}{|S|} = m$. Имеем, $|H| = p^l = |St(gS)| \cdot |Orb(gS)|$, значит, порядок каждой орбиты либо 1, либо степень p. Так как сумма порядков орбит не делится на p, есть орбита из одного элемента. То есть $hgS = gS$. Отсюда $g^{-1}hg \in S$, то есть $h \in gSg^{-1}$. Значит, $H \subset gSg^{-1}$, где $|gSg^{-1}| = p^k$.

2) Если H – силовская подгруппа, то $|H| = p^k$. По доказанному в пункте 1) выполнено $H \subset gSg^{-1}$. Поскольку $|H| = |gSg^{-1}|$, имеем $H = gSg^{-1}$. Значит, любая силовская p-подгруппа H сопряжена фиксированной силовской p-подгруппе S. □

Рассмотрим действие группы G на множестве всех подгрупп в группе G сопряжениями. В самом деле, легко убедиться, что если $H \subset G$ – подгруппа, то gHg^{-1} также подгруппа.

Определение 2. Стабилизатор подгруппы H при данном действии называется *нормализатором* H в G и обозначается $N_G(H)$.

Лемма 2. *1) $N_G(H)$ – подгруппа в G,*
2) $H \subseteq N_G(H)$,
3) H нормальна в $N_G(H)$,
4) Если H нормальна в K, где K – подгруппа G, то $K \subset N_G(H)$.

Доказательство. 1) По определению, $N_G(H)$ – стабилизатор, а значит, подгруппа в G.
2) Если $h \in H$, то $hHh^{-1} = H$. Значит, $h \in N_G(H)$.
3) При $g \in N_G(H)$ имеем $gHg^{-1} = H$, это доказывает нормальность H в $N_G(H)$.
4) Если $H \triangleleft K$, то для любого $k \in K$ выполнено $kHk^{-1} = H$, то есть

$$k \in St(H) = N_G(H).$$

□

Пусть $|G| = p^k m$. Обозначим через n_p число силовских p-подгрупп в группе G.

Теорема 3 (Третья теорема Силова)**.**
1) n_p сравнимо с 1 по модулю p,
2) n_p делит m.

Доказательство. 1) Пусть S – одна из силовских p-подгрупп. Рассмотрим действие S на множестве M силовских p-подгрупп сопряжениями. То есть $s \cdot S' = sS's^{-1}$. Пусть $Orb(S')$ – некая орбита. Тогда $|Orb(S')| \cdot |St(S')| = |S| = p^k$. Значит, $|Orb(S')| = p^l$. Среди орбит есть $Orb(S)$, которая состоит только из одной подгруппы S, таким образом, $|Orb(S)| = 1$.

Пусть $S' \neq S$, допустим, что $|Orb(S')| = 1$. Тогда для любых $s \in S, s' \in S'$ имеем $ss's^{-1} \in S'$. Следовательно, $S \subseteq N_G(S')$. Заметим, что $N_G(S')$ – это подгруппа в G, а значит, $|N_G(S')| = p^u v|$, где $u \leq k$ и $(p, v) = 1$. Так как $S \subseteq N_G(S')$, $u = k$. Значит, S – силовская p-подгруппа в $N_G(S')$. С другой стороны S' – силовская p-подгруппа в $N_G(S')$. Значит, S и S' сопряжены в $N_G(S')$. Но S' нормальна в $N_G(S')$, а значит, сопрягая S' элементами $N_G(S')$ мы не получим дргой подгруппы. ПРотиворечие. Значит, не существует такой $S' \neq S$, что $|Orb(S')| = 1$.

Итак, множество M силовских p-подгрупп состоит из орбит, одна из них имеет порядок 1, а остальные имеют порядки p^l, где $l \neq 0$. Следовательно, $n_p = |M|$ имеет остаток 1 при делении на p.

2) Рассмотрим действие группы G на множестве L всех подгрупп в G. То есть $g \cdot H = gHg^{-1}$. По второй теореме Силова все силовские p-подгруппы образуют одну орбиту $\mathcal{O}$. Пусть S – одна из силовских p-подгрупп. Тогда

$$|G| = |\mathcal{O}| \cdot |St(S)| = n_p \cdot |St(S)|.$$

Отсюда $|G| = p^k m$ делится на n_p. Так как НОД$(n_p, p) = 1$, получаем m делится на n_p. □

Пример 1. *Группа порядка 15 обязательно изоморфна* $\mathbb{Z}_{15}$. *Докажем это. Применим третью теорему Силова к* $p = 3$ *и* $p = 5$ *в нашей группе. Получим*

$$\begin{cases} n_3 \equiv 1 (\mathrm{mod}\, 3); \\ n_3 \mid 5. \end{cases}$$

Отсюда $n_3 = 1$. *А также*

$$\begin{cases} n_5 \equiv 1 (\mathrm{mod}\, 5); \\ n_5 \mid 3. \end{cases}$$

Отсюда $n_5 = 1$. *Это значит, что в нашей группе есть 2 подгруппы* $H_3 \cong \mathbb{Z}_3$ *и* $H_5 \cong \mathbb{Z}_5$, *причцм они обе нормальны (так как являются единственными силовскими подгруппами). Пересечение* H_3 *и* H_5 *– это только* $\{e\}$, *так как любой неединичный элемент в* H_3 *имеет порядок 3, а любой неединичный элемент в* H_5 *имеет порядок 5. Докажем, что* $\langle H_3, H_5 \rangle = G$. *В самом деле, пусть* $\langle H_3, H_5 \rangle = L \subseteq G$. *Тогда по теореме Лагранжа* $|L|$ *делится на 3 и на 5. То есть* $|L|$ *делится на 15. Следовательно,* $L = G$. *Получаем, что для подгрупп* H_3 *и* H_5 *выполнены условия внутреннего прямого произведения, что означает*

$$G \cong H_3 \times H_5 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{15}.$$