

## 5. Теорема Силова

Мы знаем, что не для любого делителя  $k$  порядка  $n$  конечной группы обязательно найдется подгруппа порядка  $k$ . Скажем, в группе  $A_4$  порядка 12, нет подгрупп порядка 6. Однако, оказывается, если  $k$  — это степень простого числа, то такая подгруппа всегда найдется. Среди таких подгрупп особенно роль играют самые большие — их называют **силовскими**. Теорема (или даже теоремы) о их существовании была доказана Людвигом Силом в 1872 году.

- Т. 1 (Силоз) Пусть  $|G| = p^r \cdot l$ , где  $p$  - простое число и  $p \nmid l$ .
- ① Существование Для  $\forall \alpha \in \{1, \dots, r\}$  в  $G$  существует подгруппа порядка  $p^\alpha$ .
  - ② Вложение Если  $\alpha < r$ , то каждая подгруппа порядка  $p^\alpha$  из  $G$  вложена в некоторую подгруппу порядка  $p^{\alpha+1}$ .
  - ③ Сопряженность Все подгруппы порядка  $p^r$  (они наз-ся **СИЛОВСКИМИ**) группы  $G$  сопряжены в  $G$ .
  - ④ Количество Количество  $n_p$  силовских подгрупп в группе  $G$  делит  $|G|$  и  $n_p \equiv 1 \pmod{p}$ .
- Обозн.  $P \in \text{Syl}_p(G)$  ozn., что  $P$  - силовская  $p$ -подгруппа.

Л-во: ① Пусть  $\mathcal{M} = \{M \subseteq G \mid |M| = p^\alpha\}$ . Имеем  
 $|\mathcal{M}| = C_{p^r-1}^{p^\alpha} = p^{r-\alpha} \cdot \prod_{j=1}^{p^\alpha-1} \frac{p^r-1-j}{j}$ , поэтому  $p^{r-\alpha}$  — это  
 наибольшая степень  $p$ , делящая  $|\mathcal{M}|$ .

Группа  $G$  действует на  $\mathcal{M}$  правыми сдвигами,  
 т.к. если  $M \in \mathcal{M}$ , то  $Mg = \{mg \mid m \in M\} \in \mathcal{M}$ .

Средь орбит это действие есть хотя бы одна,  
 порядок которой делится на  $p^{r-\alpha+1}$ . Пусть  
 $\mathcal{O} = \{M_1, \dots, M_s\}$  — та орбита. Положим  $G_i = \{g \in G \mid$   
 $M_1 g = M_i\}$ ,  $i=1..s$ . Легко проверить, что  $G_1 \leq G$  и  
 $G_i$ ,  $i=1..s$ , — правые смежные классы по подгруппе  $G_1$ .

Мы докажем, что  $G_1$  — простая погр. корт. д.  $p^\alpha$ .

Пусть  $|G_1| = t$ . Тогда  $p^r \cdot t = |G| = |\Omega| |G_1| = st$   
по т. о группе орбит  $(S, \text{действие из т. 9.6.1 из [ВЛМ]})$ .

Так как  $p$  — простая погр., то  $p^r \cdot t = st$  — это  
 $p^{r-\alpha}$ , то  $p^\alpha \mid t$ . В частности,  $t \geq p^\alpha$ . С др. стороны,  
если  $x \in M_1$ , то  $x G_1 \subseteq M_1$ , поэтому  $|G_1| \leq |M_1| \leq p^\alpha$ .

② Пусть  $P \leq G$  :  $|P| = p^\alpha$  и  $\alpha < r$ . Обозначим

$\mathcal{P} = \{ p^g \mid g \in G \}$  — класс погр., сопряженных  
с  $P$  в  $G$ . Группа  $G$  действует на  $\mathcal{P}$  сопряжениями,  
поэтому по т. 9.6.1 из [ВЛМ] имеем  
 $|\mathcal{P}| = |G : N_G(P)|$ , где  $N_G(P) = \{ g \in G \mid p^g = P \}$  —  
нормализатор  $P$  в  $G$ .

Возможны два случая: 1)  $p \nmid |P|$ . Тогда  $p^{d+1} \mid |N_G(P)|$  и, следовательно, в силу первой части т-м в группе  $\overline{N} = N_G(P)/P$  есть подгруппа  $\overline{P}^*$  порядка  $p \Rightarrow \exists e$  прообраз  $\overline{P}^*$  имеет порядок  $p^{d+1}$  и содержит  $P$ .

2)  $p \mid |P|$ . Рассмотрим действие гр.  $P$  на  $P$  сопряжениями. Порядки орбит делят  $|P|$ , т.е. имеют вид  $p^{\alpha_i}$ ,  $\alpha_i \geq 0$ . Имеется по крайней мере одна относительно инвариантная орбита  $\{P\}$ . Т.к.  $p \mid |P|$ , то есть по крайней мере еще одна  $\{Q\}$ ,  $Q \neq P$ . Сл-но,  $QP = PQ \Rightarrow PQ \leq G$ , причем  $|PQ| > |P|$  и  $PQ/Q \simeq P/P \cap Q \Rightarrow PQ$  —  $p$ -подгруппа, порядка

добавим, чем  $P$ , имеем  $Q \trianglelefteq PQ$ . Т.к.  $Q$  и  $P$  лежат в одной орбите  $P$ , то  $\exists g \in G: Q^g = P$ . Тогда  $P = Q^g \trianglelefteq (PQ)^g = P_1$ . Снова, применяя (1), получим в  $P_1/P$  подгруппу  $P^*/P$  порядка  $p$ , её образ  $P^*$  — исконая подгруппа порядка  $p^{d+1}$ .

(3) Пусть теперь  $P \in \text{Syl}_p(G)$ , т.е.  $|P| = p^r$ , а  $P = \{P^g \mid g \in G\}$ . Пусть  $Q \in \text{Syl}_p(G)$ . Надо доказать, что  $Q \in P$ .  $P$ -и  $Q$  — сопряженные  $p$ -подгруппы. Порядки орбит это степени  $|G/N_G(P)|$ , т.е. равны  $p^{d_i}$ ,  $d_i \geq 0$ . Т.к.  $|P| = |G:N_G(P)|$  теперь точно не делится на  $p$ , то имеется орбита  $d_1$   $p$ -н. Тогда  $P'Q = QP' \leq G$  и  $P'Q$  —  $p$ -группа.

Но  $Q \in \text{Syl}_p(G) \Rightarrow |P'Q| = |Q| = |P'| \Rightarrow Q = P'Q = P' \in \mathcal{P}$ ,  
что и требовалось.

(4) В обозн. из (3)  $n_p = |P| = |G : N_G(P)| \text{ делит } |G|$ .

Чтобы доказать, что  $n_p \equiv 1 \pmod{p}$ , достаточно  
показать, что  $|Q|$  — единственный делитель.  
Если  $|Q'|$  — другая такая орбита, то  $QQ'$  —  $p$ -подгруппа,  
отличная от  $Q$ , что невозможно.  $\blacksquare$

Следствие Пусть  $P \in \text{Syl}_p(G)$ . Тогда  $P \trianglelefteq G \Leftrightarrow n_p = 1$ .

Упр 1 Докажите, что другие кориски 196 не хороши.

Теорема 2 Пусть  $p, q$  — простые числа  $p < q$ .

(1)  $|G| = p^2 \Rightarrow G$  абелева, в частности  $G \cong \mathbb{Z}_p^2$  или  $\mathbb{Z}_p \times \mathbb{Z}_p$ .

②  $|G| = pq \Rightarrow G = P \ltimes Q$  - полупрямое произведение циклических  $p$ -подгрупп  $P$  и  $q$ -подгруппы  $Q$  (см. вып 8.1 из AN-22.pdf). Если  $q \not\equiv 1 \pmod{p}$ , то  $G = P \times Q \cong \mathbb{Z}_{pq}$ -группа, если  $q \equiv 1 \pmod{p}$ , то  $\text{mod } a) G \cong \mathbb{Z}_{pq}$ ,  $\text{mod } b) \text{ord}_p = q$ ,  $b^{-1}ab = a^r$ , где  $P = \langle a \rangle$ ,  $Q = \langle b \rangle$  и  $r^p \equiv 1 \pmod{q}$ , но  $r \not\equiv 1 \pmod{q}$ , иными словами, определена хаотическая и  $b$ ) единственность.

Δ-во: ① Т.к.  $G$  -  $p$ -группа, то  $Z(G) \neq 1$  в силу т. 10.3.5. Если  $|Z(G)| = p$ , то  $|G/Z(G)| = p \Rightarrow G/Z(G)$  - циклическая  $\Rightarrow \exists x \in G: G = \bigcup_{k=0}^{p-1} Z'x^k$ , где  $Z = Z(G)$ . Тогда  $\forall g_1 = z_1 x^{k_1}, g_2 = z_2 x^{k_2} \in G$  имеем



$$g_1 \cdot g_2 = z_1 x_1^{k_1} \cdot z_2 x_2^{k_2} = z_1 \cdot z_2 x^{k_1 + k_2} = z_2 x^{k_2} \cdot z_1 x^{k_1} = g_2 g_1$$

$\Rightarrow G$  абелева, удовлетворяющее  $\subset G \supset Z(G) \Rightarrow G = Z(G)$ , т.е.  $G$  абелева. Поэтому  $G \cong \mathbb{Z}_p^2$  или  $\mathbb{Z}_p \times \mathbb{Z}_p$  по теореме о конн.-нормальн. абелевых группах.

(2) По 7. Силова  $\exists P \in \text{Syl}_p(G)$  и  $Q \in \text{Syl}_q(G)$  порядков  $p$  и  $q$  соот-но. Т.к.  $n_q \mid p-1$ ,  $n_q \equiv 1 \pmod{q}$   
 $\Rightarrow n_q = 1$ , т.к.  $p < q$ . Поэтому  $Q \trianglelefteq G$  по след-ствию из 7-го Силова. Т.к.  $(p, q) = 1$ , то  $P \cap Q = 1$ . Кроме того,  $PQ = QP \leq G$ . Но  $|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|} = |P||Q| = |G| \Rightarrow PQ = G$ . Поэтому

$G = P \ltimes Q$  в силу лем. 8.1 конн.нормальн. произведения. Снова  $n_p \mid p-1$  и  $n_p \equiv 1 \pmod{p}$

Поэтому либо  $n_p = 1$  и тогда  $P \trianglelefteq G \Rightarrow G = P \times Q$   
 $\cong \mathbb{Z}_{pq}$ , либо  $n_p = q$ . Тогда  $q \equiv 1 \pmod{p}$ .

В этом случае, получается единственная  
классификация простых порядка  $pq$  (подробности  
см. в п. 11.2 из [KM]).

Упр 2 Найти все возможные простые в  $S_n$   
и указать их число.

Упр 3 Пусть  $p$  - простое число,  $q = p^k$  и  $F$  - поле  
порядка  $q$ . Тогда  $UT_n(F)$  - с nilпотентная  
 $p$ -подгруппа в гр.  $GL_n(F)$ .

Упр 4 (Лемма Фраттини), Если  $H \trianglelefteq G$  и  $P \in \text{Syl}_p(H)$ ,  
то  $G = N_G(P) \cdot H$ .