

# Теория групп. Лекция 9

Штепин Вадим Владимирович

31 октября 2019 г.

## 1 Критерий разрешимости группы

**Теорема (критерий разрешимости в терминах нормальной подгруппы)**

Пусть  $K \triangleleft G$ . Тогда  $G$  — разрешима  $\Leftrightarrow K$  и  $G/K$  разрешимы.

**Доказательство**

1. Необходимость. Пусть  $G^{(n)} = \{e\}$ .  $K \triangleleft G \Rightarrow K' \triangleleft G' \Rightarrow K^{(n)} \triangleleft G^{(n)} = \{e\} \Rightarrow K$  разрешима.

Обозначим  $\bar{G} = G/K$ . Пусть  $p : G \rightarrow \bar{G}$  — канонический гомоморфизм.  $p|_{G'} : G' \rightarrow \bar{G}'$ , т.е.  $p(G') \subset \bar{G}'$ , так как гомоморфизм сохраняет коммутаторы.

Всякий коммутатор элементов из  $\bar{G}$  — образ коммутатора элементов из  $G$ . В силу сюръективности получаем  $p(G^{(n)}) = \bar{G}^{(n)}$ , но  $G^{(n)} = \{e\} \Rightarrow \bar{G}^{(n)} = \{e\}$  и  $\bar{G}$  разрешима.

2. Достаточность.

Пусть  $K$  и  $\bar{G}$  разрешимы. Пусть  $K^{(n)} = \{e\}$  и  $\bar{G}^{(l)} = \{e\}$ .  $p : G \rightarrow \bar{G}$  — канонический гомоморфизм.  $p(G^{(l)}) = \bar{G}^{(l)} = \{e\} \Rightarrow G^{(l)} \subset \text{Ker}(p) = K \Rightarrow G^{(l+n)} \subset K^{(n)} = \{e\} \Rightarrow G$  — разрешима.

**Следствие**

Пусть  $|G : H| = 2$ . Тогда  $G$  разрешима  $\Leftrightarrow H$  — разрешима.

**Доказательство**

$H \triangleleft G$  как группа индекса 2.  $G/H \simeq C_2$  — разрешима (абелева)

**Пример**

$H = \langle R \rangle \leq D_n$ ,  $H \simeq C_n$  — разрешима и  $|D_n : H| = 2$ . Значит,  $D_n$  разрешима.

**Следствие**

Пусть  $G$  — конечна,  $K_1, K_2 \triangleleft G$  и разрешимы. Тогда  $K_1 K_2$  нормальная и разрешимая.

**Доказательство**

$K_1 K_2 \triangleleft G$  — было доказано.  $K_1 K_2 / K_2 \simeq K_1 / (K_1 \cap K_2)$  по первой теореме об изоморфизме.  $K_1 / (K_1 \cap K_2)$  разрешима, так как  $K_1$  разрешима. По критерию,  $K_1 K_2$  так же разрешима.

**Теорема**

Пусть  $G$  — конечная группа. Тогда в  $G$  найдется наибольшая нормальная разрешимая подгруппа  $S$ . Более того,  $G/S$  не содержит нетривиальных разрешимых подгрупп.

**Доказательство**

Пусть  $K_1, \dots, K_s$  — все нормальные разрешимые подгруппы  $G$ . Положим  $S = \langle K_1 \cup K_2 \dots \cup K_s \rangle$ . По следствию,  $S$  нормальная и разрешимая, причем  $S$  — максимальная такая подгруппа.

Пусть в  $G/S$  есть нетривиальные ( $\neq \{e\}$ ) разрешимые нормальные подгруппы:  $L/S \triangleleft G/S \Rightarrow L \triangleleft G$  по второй теореме об изоморфизме. Так как  $S, L/S$  нормальные и разрешимые группы, то и  $L$  нормальная и разрешимая по критерию в терминах нормальной подгруппы. Значит,  $S \triangleleft L \triangleleft G$ , причем, в силу нетривиальности,  $L \neq S$  — противоречие с максимальностью  $S$ .

Опр. Построенная наибольшая нормальная разрешимая подгруппа — **разрешимый радикал**  $S(G)$

### Теорема (критерий разрешимости)

Следующие условия эквивалентны:

1.  $G$  — разрешима
2. В  $G$   $\exists$  цепочка подгрупп  $G = G_0 \geq G_1 \geq \dots \geq G_n = \{e\}$  со свойствами  $G_k \triangleleft G$  и  $G_k/G_{k+1}$  абелева.
3. В  $G$   $\exists$  цепочка подгрупп  $G = G_0 \geq G_1 \geq \dots \geq G_n = \{e\}$  со свойствами  $G_{k+1} \triangleleft G_k$  и  $G_k/G_{k+1}$  абелева.

### Доказательство

1.  $1 \Rightarrow 2$  Положим  $G_k = G^{(k)}$  — производный ряд. Если  $K \triangleleft G$ , то  $K' \triangleleft G$  по свойству производной. Значит  $G_k \triangleleft G$ .

По свойствам коммутанта  $G/G'$  абелева, значит  $G_k/G_{k+1}$  абелева.

2.  $2 \Rightarrow 3$  Очевидно,  $G_{k+1} \triangleleft G_k$
3.  $3 \Rightarrow 1$  Покажем, что  $\forall k \ G^{(k)} \leq G_k$  индукцией по  $k$ .

База:  $G_0 = G \subset G$

Переход: Пусть  $G^{(k)} \subset G_k$ . Тогда  $G^{(k+1)} = [G^{(k)}, G^{(k)}] \subset [G_k, G_k]$ .  $G_k/G_{k+1}$  абелева  $\Leftrightarrow \forall x, y \in G_k [xG_{k+1}, yG_{k+1}] = \{G_{k+1}\}$ .  $[x, y]G_{k+1} = [xG_{k+1}, yG_{k+1}] = G_{k+1} \Leftrightarrow [x, y] \in G_{k+1} \Rightarrow [G_k, G_k] \subset G_{k+1}$

### Напоминание

Конечная группа  $G$  — это  $p$ -группа, если  $|G| = p^n$ ,  $p$  — простое.

### Теорема

Всякая  $p$ -группа  $G$  разрешима

### Доказательство

Было доказано, что всякая  $p$ -группа имеет нетривиальный центр  $Z = Z(G) \neq \{e\}$

1. Если  $Z = G$ , то  $G$  абелева и разрешима.
2. Докажем индукцией по  $n$ :

База: Пусть  $|G| = p \Rightarrow G$  — циклична по теореме Лагранжа и разрешима.

Переход: Пусть  $\forall G : |G| < p^n$  доказано. Пусть  $\{e\} < Z < G \Leftrightarrow |G/Z| < p^n \Leftrightarrow G/Z$  разрешима ( $|G/Z| = p^m$ ,  $m < n$ ).  $Z$  разрешима, так как абелева.  $Z \triangleleft G$ , так как  $\forall x \in G \ xZ = Zx$ . Значит,  $G$  разрешима.

**Следствие**

Если  $G$  —  $p$ -группа, то  $G' \neq G$

**Доказательство**

Если  $G' = G$ , то  $\forall n \ G^{(n)} = G$  — противоречие с разрешимостью.

**Теорема (о подгруппах в конечной  $p$ -группе)**

Пусть  $G$  —  $p$ -группа и  $|G| = p^n$ .

Тогда  $\forall k, 1 \leq k \leq n$  в  $G$  есть подгруппа  $H$  мощности  $p^k$ .

**Доказательство**

Индукция по  $k$ .

База:  $k = 0, H = \{e\}$

Переход: Пусть  $\exists$  подгруппа  $H_k, |H_k| = p^k, k \leq n$ . Покажем, что в  $G$  есть подгруппа порядка  $k+1$  ( $k+1 \leq n$ ). Пусть  $Z = Z(G)$ .

$\exists a \in Z, a \neq e \Rightarrow \langle a \rangle \subset Z \Rightarrow \text{ord}(a) = p^l \Rightarrow$  в  $\langle a \rangle$  есть элемент порядка  $p$ . Пусть  $\text{ord}(z) = p, L = \langle z \rangle \triangleleft G$  (так как  $z \in Z$ ). Рассмотрим  $G/L: |G/L| \geq p^k$ . По предположению индукции, в  $G/L$  есть подгруппа порядка  $p^k$ . Пусть  $H/L$  — подгруппа порядка  $p^k$ . Тогда  $|H| = p^{k+1}$

## 2 Простые группы

**Опр.** Группа  $G$  — **простая**, если она не имеет нетривиальных нормальных подгрупп.

**Теорема (об описании простых абелевых групп)**

Среди абелевых групп простые только  $C_p$  при простом  $p$ .

**Доказательство**

1.  $C_p$  простая по теореме Лагранжа
2. Если группа  $G$  абелева и  $|G| = n$  — составное число, то  $G$  не простая. Возьмем  $a \neq e$  и рассмотрим  $|\langle a \rangle| = k : p$  — простое. Тогда  $(a^{\frac{k}{p}})^p = e \Rightarrow \text{ord}(a^{\frac{k}{p}}) = p \Rightarrow \langle a^{\frac{k}{p}} \rangle \neq G$  и  $\langle a^{\frac{k}{p}} \rangle \triangleleft G$ , так как  $G$  абелева.  
Если  $|G| = \infty$ , и  $\exists a : \text{ord}(a) = k$ , то  $\langle a \rangle \neq G$ .  
Если  $\forall a \text{ ord}(a) = \infty$ , то  $\exists H \simeq Z, H = \langle a \rangle$ . Тогда  $\langle a^2 \rangle \leq H$  и  $\langle a^2 \rangle \neq G$ .

**Лемма**

Пусть  $|G : H| = 2, G$  — конечная группа. Тогда

1. Если  $C_G(h) \neq C_H(h)$ , то  $h^G = h^H$
2. Если  $C_G(h) = C_H(h)$ , то  $h^G = \frac{h^H}{2}$ , где  $h^G = \{g^{-1}hg \mid g \in G\}$

**Доказательство**

1. Пусть  $a \in C_G(h) \setminus C_H(h) \Rightarrow ah = ha \Leftrightarrow a \in G/H \Rightarrow G = H \cup aH$   
 $h^G = h^{(H \cup aH)} = h^H \cup h^{aH} = h^H \cup (h^a)^H = h^H \cup h^H = h^H$
2. Пусть  $C_G(h) = C_H(h)$ . Тогда  $|h^G| = \frac{|G|}{|C_G(h)|} = \frac{2|H|}{|C_H(h)|} = 2|h^H|$

**Замечание**

Если  $G = H \cup aH, a \notin H$  во втором случае, то  $h^G = h^H \cup (h^a)^H$  и  $(h^a)^H \neq h^H$ , но  $|(h^a)^H| = |h^H|$