Лекция 9

Определение 1. Пусть x и y – элементы группы G. *Коммутатором* элементов x и y называется элемент

$$[x, y] = xyx^{-1}y^{-1}.$$

Лемма 1. *$[x, y] = e$ тогда и только тогда, когда элементы x и y перестановочны (то есть $xy = yx$).*

Доказательство.

$$xy = yx \;\Leftrightarrow\; xyx^{-1} = y \;\Leftrightarrow\; xyx^{-1}y^{-1} = e.$$

□

Замечание 1. Обратный элемент к коммутатору является коммутатором. В самом деле:

$$[x, y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y, x].$$

Определение 2. *Коммутант* группы G – это подгруппа, порожденная всеми коммутаторами пар элементов из G. Коммутант группы G обозначается G' или $[G, G]$.

Лемма 2. *Коммутант состоит из произведений коммутаторов.*

Доказательство. По определению, G' состоит из произведений коммутаторов и обратных к ним. Но, так как обратный к коммутатору – коммутатор, G' состоит из произведения коммутаторов. □

Лемма 3. *$G' = \{e\}$ тогда и только тогда, когда G коммутативна.*

Доказательство. Если G коммутативна, то все коммутаторы равны e, и значит, коммутант также равен $\{e\}$.

Если же G не абелева, то найдутся два элемента x и y такие, что $xy \neq yx$. Тогда $[x, y] \neq e \in G'$. □

Лемма 4. *Коммутант G' – нормальная подгруппа в G.*

Доказательство. Заметим, что

$$g[x, y]g^{-1} = gxyx^{-1}y^{-1}g^{-1} = gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} = [gxg^{-1}, gyg^{-1}].$$

Отсюда

$$g[x_1, y_1][x_2, y_2] \ldots [x_n, y_n]g^{-1} = g[x_1, y_1]g^{-1}g[x_2, y_2]g^{-1} \ldots g[x_n, y_n]g^{-1} = \\ = [gx_1g^{-1}, gy_1g^{-1}][gx_2g^{-1}, gy_2g^{-1}] \ldots [gx_ng^{-1}, gy_ng^{-1}].$$

Таким образом, если сопрячь с помощью g элемент коммутанта (то есть произведение коммутаторов), то получится снова элемент коммутанта. Таким образом, коммутант – нормальная подгруппа. □

Лемма 5. *Группа G/G' коммутативна.*

Доказательство. Рассмотрим коммутатор двух произвольных элементов из G/G':

$$[gG', hG'] = gG' \cdot hG' \cdot (gG')^{-1} \cdot (hG')^{-1} = [g, h]G' = G'.$$

То есть коммутатор любых элементов из G/G' равен единице группы G/G'. Значит, G/G' – абелева группа. □

Теорема 1. *а) Пусть H – подгруппа в G и $G' \subseteq H$. Тогда H – нормальная подгруппа и G/H – абелева группа.*

б) Если $G \triangleright H$ и группа G/H – абелева группа то $G' \subset H$.

Доказательство. а) Пусть $g \in G$, $h \in H$. Тогда $ghg^{-1} = [g,h]h \in H$. Значит, $G \triangleright H$.

Рассмотрим коммутатор двух произвольных элементов из G/H:

$$[g_1H, g_2H] = g_1H \cdot g_2H \cdot (g_1H)^{-1} \cdot (g_2H)^{-1} = [g_1, g_2]H = H.$$

Значит, $(G/H)' = \{e\}$, то есть G/H – коммутативная группа.

б) Рассмотрим коммутатор двух произвольных элементов из G/H:

$$[g_1H, g_2H] = g_1H \cdot g_2H \cdot (g_1H)^{-1} \cdot (g_2H)^{-1} = [g_1, g_2]H.$$

Так как G/H – абелева группа, $[g_1H, g_2H] = H$. Получаем $[g_1, g_2]H = H$, следовательно, $[g_1, g_2] \in H$. Поскольку коммутаторы порождают G', выполняется $G' \subset H$. □

Можно рассмотреть кратные коммутанты: $G^{(2)} = (G')'$, $G^{(3)} = \left(G^{(2)}\right)'$, … , $G^{(n)} = \left(G^{(n-1)}\right)'$, …

Определение 3. Группа G называется *разрешимой*, если существует $n \in \mathbb{N}$ такое, что $G^{(n)} = \{e\}$.

Число n называется *ступенью (степенью)* разрешимости G.

Пример 1. *Группа G разрешима ступени 1 тогда и только тогда, когда G абелева.*

Пример 2.

- *Группа S_2 разрешима ступени 1.*
- *Группа S_3 разрешима ступени 2: $S_3' = A_3$, $A_3' = \{\mathrm{id}\}$.*
- *Группа S_4 разрешима ступени 3: $S_4' = A_4$, $A_4' = V_4$, $V_4' = \{\mathrm{id}\}$.*
- *Группа S_n при $n \geq 5$ не разрешима. Действительно, $S_n' = A_n$, $A_n' = A_n$ (будет показано позже).*

Лемма 6. *Подгруппа разрешимой группы разрешима.*

Доказательство. Пусть H – подгруппа G. Тогда $H' \subset G'$, $H'' \subset G''$ и т.д. Значит, $H^{(n)} \subset G^{(n)} = \{e\}$. □

Лемма 7. *Факторгруппа разрешимой группы разрешима.*

Доказательство. Пусть $G \triangleright H$. Имеем

$$[g_1H, g_2H] = g_1Hg_2Hg_1^{-1}Hg_2^{-1}H = [g_1, g_2]H.$$

Отсюда $(G/H)' = \{gH \mid g \in G'\}$. Аналогично $(G/H)^{(n)} = \{gH \mid g \in G^{(n)}\}$. Так как $G^{(n)} = \{e\}$, получем $(G/H)^{(n)} = \{eH\}$. □

Теорема 2 (Критерий разрешимости группы.)**.** *Пусть $G \triangleright H$. Тогда G разрешима тогда и только тогда, когда H разрешима и G/H разрешима.*

Доказательство. В одну сторону (из разрешимости G следует разрешимость H и G/H) утверждение теоремы сводится к предыдущим леммам.

Пусть теперь H и G/H разрешимы. Как было доказано ранее

$$(G/H)^{(i)} = \{gH \mid g \in G^{(i)}\}.$$

Найдется такое натуральное m, что $(G/H)^{(m)} = \{e\}$. Тогда $G^{(m)} \subset H$. Но поскольку H разрешима, найдется натуральное k такое, что $H^{(k)} = \{e\}$. Следовательно

$$G^{(m+k)} \subseteq H^{(k)} = \{e\}.$$

То есть G разрешима. □

Следствие 1. *Пусть задан гомоморфизм $\psi\colon G \to H$. Тогда G разрешима если и только если $\operatorname{Ker}\psi$ и $\operatorname{Im}\psi$ разрешимы.*

Доказательство. Ядро гомоморфизма – нормальная подгруппа, фактор по которой изоморфен образу. □

Предложение 1. *Группа B_n невырожденных верхнетреугольных матриц над полем F разрешима.*

Доказательство. Пусть U_n – группа верхнетреугольных матриц $n \times n$ с единицами на диагонали. Рассмотрим гомоморфизм $\varphi\colon B_n \to (F^\times)^n$,

$$\varphi\colon \begin{pmatrix} a_1 & * & \dots & * \\ 0 & a_2 & \dots & * \\ \vdots & \vdots & \ddots & * \\ 0 & 0 & \dots & a_n. \end{pmatrix} \mapsto (a_1, \dots, a_n)$$

Очевидно, что $\operatorname{Ker}\varphi = U_n$, а $\operatorname{Im}\varphi = (F^\times)^n$. Так как образ – абелева группа, он разрешим. Значит, чтобы доказать разрешимость B достаточно доказать разрешимость U_n.

Рассмотрим гомоморфизм (проверьте это!) $\psi\colon U_n \to F^{n-1}$, заданный по правилу

$$\psi\colon \begin{pmatrix} 1 & b_1 & * & \dots & * \\ 0 & 1 & b_2 & \dots & * \\ \vdots & \vdots & \ddots & \ddots & * \\ 0 & 0 & \dots & 1 & b_{n-1} \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \mapsto (b_1, \dots, b_n)$$

Образ ψ лежит в коммутативной группе. Значит, он разрешим. Ядро ψ – подгруппа

$$U_{n1} = \left\{ \begin{pmatrix} 1 & 0 & * & \dots & * \\ 0 & 1 & 0 & \dots & * \\ \vdots & \vdots & \ddots & \ddots & * \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \right\}.$$

Рассмотрим гомоморфизм $\psi_2\colon U_{n1} \to F^{n-2}$:

$$\psi_2\colon \begin{pmatrix} 1 & 0 & c_1 & * & \dots & * \\ 0 & 1 & 0 & c_2 & \dots & * \\ \vdots & \vdots & \ddots & \ddots & \ddots & * \\ 0 & 0 & \dots & 1 & 0 & c_{n-2} \\ 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 \end{pmatrix} \mapsto (c_1, \dots, c_n).$$

Образ ψ_2 абелев, и значит разрешим, а ядро – подгруппа U_{n2},

$$U_{n2} = \left\{ \begin{pmatrix} 1 & 0 & 0 & * & \dots & * \\ 0 & 1 & 0 & 0 & \dots & * \\ \vdots & \vdots & \ddots & \ddots & \ddots & * \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 \end{pmatrix} \right\}.$$

И т.д. Каждый раз разрешимость U_{ni} сводится к разрешимости $U_{n,i+1}$. Поскольку $U_{n,n-1} = \{e\}$, она разрешима. Это завершает доказательство разрешимости B_n. □

Предложение 2. *Группа порядка pq, где p и q – различные простые числа, разрешима.*

Доказательство. Пусть $|G| = pq$. Можно считать, что $p > q$. Тогда n_p делит q и сравнимо с 1 по модулю p. Значит, $n_p = 1$. Тогда силовская p-подгруппа S нормальна. Так как $|S| = p$ и $|G/S| = q$ эти группы циклические, а значит, разрешимы. По критерию разрешимости G разрешима. □

Дадим несколько применени теорем Силова к доказательству разрешимости групп.

Предложение 3. *Пусть $p > q$ – простые числа. Если p не сравнимо с 1 по модулю q, то существует единственная группа порядка pq (это $\mathbb{Z}_{pq}$).*

Доказательство. По 3 теореме Силова n_p делит q и сравнимо с 1 по модулю p. Значит, $n_p = 1$. С другой стороны n_q делит p и сравнимо с 1 по модулю q. Значит, так как p не сравнимо с 1 по модулю q, $n_q = 1$.

Пусть $N \cong \mathbb{Z}_p$ – это единственная силовская p-подгруппа, а $H \cong \mathbb{Z}_q$ – единственная силовская q-подгруппа. Они нормальны в G. Тогда $N \cap H = \{e\}$ так как они циклические разных простых порядков. С другой стороны так как порядок группы, порожденной H и N делится на p и на q, получаем $G = \langle N, H \rangle$. Таким образом $G \cong N \times H \cong \mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

□

Предложение 4. *Группа порядка p^k разрешима.*

Доказательство. Докажем по индукции по порядку группы. База индукции $|G| = p$, тогда группа циклическая, и следовательно, разрешима. Шаг индукции. У p-группы центр неединичен. Если $Z(G) = G$, то эта группа абелева, и следовательно, разрешима. Если $|Z(G)| < |G|$, то по предположению индукции $Z(G)$ и $G/Z(G)$ разрешимы. Значит, G разрешима. □

Предложение 5. *Группа порядка p^2q, где p и q – различные простые числа, разрешима.*

Доказательство. По 3 теореме Силова n_p сравнимо с 1 по модулю p и делит q. Если $n_p = 1$, то силовская p-группа S нормальна. Так как $|S| = p^2$, она абелева, а так как $|G/S| = q$, эта группа циклическая. Значит, G разрешима.

Пусть $n_p = q$. Значит, $q = pk + 1$ (в частности, $q > p$). Рассмотрим теперь n_q, оно сравнимо с 1 по модулю q и делит p^2. Если $n_q = 1$, то единственная силовская q-подгруппа нормальна и циклическая, а фактор по ней абелев. Следовательно, G разрешима. Если $n_q = p$, то $p > q$, противоречие. Остался случай $n_q = p^2$.

Каждая силовская q-подгруппа состоит из e и $q - 1$ элемента порядка q. Так как силовские q-подгруппы порождаются любым элементом порядка q, они пересекаются только по e. Получаем, что в p^2 силовских q-подгруппах содержится $p^2(q-1) = p^2q-p^2$ элементов порядка q. Значит, элементов порядка не q в G ровно p^2, то есть $n_p = 1$. $\square$