Лекция 10

Лемма 1. *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 1 (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 нееединичен. 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. $\square$

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 $n_p = 1$. $\square$

Лемма 2. *а) A_n порождается тройными циклами.*

б) При $n \geq 5$ группа A_n порождается парами несмежных транспозиций $(i, j)(k, s)$.

Доказательство. а) Пусть $\sigma \in A_n$. Любая перестановка разлагается в произведение транспозиций. Поскольку σ – четная перестановка, $\sigma = \tau_1 \ldots \tau_{2m}$. Рассмотрим $\tau_{2l-1}\tau_{2l}$. Возможны 3 варианта:

1) $\tau_{2l-1} = \tau_{2l}$. Тогда из произведения можно их удалить.

2) $\tau_{2l-1} = (i, j)$, $\tau_{2l} = (j, k)$. Тогда $\tau_{2l-1}\tau_{2l} = (i, j, k)$.

3) $\tau_{2l-1} = (i, j)$, $\tau_{2l} = (k, s)$. Тогда $\tau_{2l-1}\tau_{2l} = (i, j)(j, k)(j, k)(k, s) = (i, j, k)(j, k, s)$.

б) Пусть H – подгруппа A_n, $n \geq 5$ порожденная всеми парами несмежных транспозиций.

$$(i, j)(k, s) \cdot (k, s)(j, r) = (i, j)(j, r) = (i, j, r).$$

Значит, H содержит все тройные циклы. Но, как уже доказано, тройные циклы порождают A_n. Следовательно, $H = A_n$.

$\square$

Теорема 2. $S'_n = A_n$.

Доказательство. Как известно, $A_n \triangleleft S_n$ и $S_n/A_n \cong \mathbb{Z}_2$ – абелева группа. Следовательно, $S'_n \subset A_n$.

Обратное включение будет следовать из явных выкладок.

$$[(i, j), (j, k)] = (i, j)(j, k)(i, j)(j, k) = (i, k, j).$$

Значит, любой тройной цикл (i, k, j) лежит в S'_n. Далее утверждение теоремы следует из леммы 2 а). $\square$

Теорема 3. *1) $A'_3 = \{id\}$,*

2) $A'_4 = V_4$,

3) $A'_n = A_n$ при $n \geq 5$.

Доказательство. 1) Группа A_3 изоморфна $\mathbb{Z}_3$ и является абелевой.

2) $|A_4| = 12$, $|V_4| = 4$, следовательно, $|A_4/V_4| = 3$, то есть $A_4/V_4 \cong \mathbb{Z}_3$ – абелева группа. Значит, $A_4' \subset V_4$. С другой стороны

$$[(i,j,k),(j,k,s)] = (i,j,k)(j,k,s)(i,k,j)(j,s,k) = (i,s)(j,k).$$

Следовательно, $V_4 \subset A_4'$. Итак, $A_4' = V_4$.

3) Как следует из предыдущего пункта при $n \geq 4$ выполнено $(i,s)(j,k) \in A_n'$ $\forall i,j,k,s$. Далее утверждение теоремы вытекает из леммы 2 б). $\square$

Лемма 3. *Пусть H – нормальная подгруппа группы G. Допустим, что в группе G/H есть нормальная подгруппа $\{e\} \subsetneq K \subsetneq G/H$. Тогда $L = \pi_H^{-1}(K)$ – нормальная подгруппа в группе G, причем $H \subsetneq L \subsetneq G$.*

Доказательство. Проверим то, что прообраз группы при гомоморфизме является группой. Пусть $l_1, l_2 \in L$. Тогда $\pi_H(l_2 l_2) = \pi_H(l_1)\pi_H(l_2) \in K$. Следовательно, $l_1 l_2 \in L$. Также $\pi_H(l_1^{-1}) = \pi_H(l_1)^{-1} \in K$, значит, $l_1^{-1} \in L$. Кроме того $e \in L$. Значит, L – подгруппа.

Пусть $g \in G$, $l \in L$. Тогда $\pi_H(glg)^{-1} = \pi_H(g)\pi_H(l)\pi_H(g)^{-1} \in K$. Значит, $glg^{-1} \in L$. То есть L нормальна в G.

Так как π_H – сюръекция и $K \neq \{e\}$, получаем $L = \pi_H^{-1}(K) \supsetneq \pi_H^{-1}(e) = H$. Аналогично так как $K \neq G/H$, получаем $L = \pi_H^{-1}(K) \subsetneq \pi_H^{-1}(G/H) = G$. $\square$

Определение 1. Группа G называется *простой*, если у нее нет нормальных подгрупп, отличных от $\{e\}$ и самой G.

Определение 2. Назовем *субнормальным* рядом группы G ряд подгрупп

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright G_3 \triangleright \ldots \triangleright G_n = \{e\},$$

каждая следующая из которых нормальна в предыдущей. Этот ряд называется *композиционным рядом группы G*, если все факторгруппы G_i/G_{i+1} простые.

Например, для разрешимой группы ряд из кратных коммутантов – это субнормальный ряд.

Предложение 6. *Для конечной группы любой субнормальный ряд может быть уплотнен до композиционного. (То есть можно добавить промежуточные группы так, чтобы ряд стал композиционным.)*

Доказательство. Если факторгруппа G_i/G_{i+1} не простая, то по лемме 3 можно уплотнить субнормальный ряд, то есть добавить в него еще одну подгруппу. Так как группа G конечна, уплотнение не может происходить бесконечно. $\square$

Предложение 7. *Абелева группа проста тогда и только тогда, когда она изоморфна $\mathbb{Z}_p$ для простого p.*

Доказательство. В абелевой группе все подгруппы являются нормальными. Поэтому абелева группа проста тогда и только тогда, когда в ней нет других подгрупп, кроме $\{e\}$ и G. Для каждого $g \in G$ можно рассмотреть циклическую подгруппу $\langle g \rangle \subset G$. Если $g \neq e$, то $\langle g \rangle \neq \{e\}$. Значит, $\langle g \rangle = G$, то есть G – циклическая. Если $G \cong \mathbb{Z}$, то в ней есть нетривиальные подгруппы $k\mathbb{Z}$. Если же $G \cong \mathbb{Z}_{ab}$, где $a \neq 1$ и $b \neq 1$, то в G есть нетривиальная подгруппа $\langle a \rangle \cong \mathbb{Z}_b$. $\square$

Теорема 4 (Жордан-Гельдер)**.** *Факторы G_i/G_{i+1} композиционного ряда определены однозначно с точностью до перестановки.*

Теорема Жордана-Гельдера связывает с любой группой некоторый набор простых групп (факторов композиционного ряда). Это дает мотивацию изучать простые группы. Например, очень популярной темой является классификация конечных простых групп. Конечные простые группы содержат несколько серий (одна из котрорых – это группы $A_n, n \in \mathbb{N}$). Также есть (довольно большие) единичные примеры групп, они называются *спорадическими группами*. Различные математики не сходятся во мнении, можно ли считать классификацию конечных простых групп завершенной. Дело в том, что она содержится в большом количестве работ и все эти работы не может прочитать за свою жизнь один человек.

Стоит упомянуть, что изучение простых факторов композиционного ряда не дает полной классификации групп, так как могут быть различные группы с одинаковым набором факторов.