Лекция 16

Следствие 1. *(Из третьей Теоремы Силова) 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. □

Предложение 1. *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 $G \cong N \times H \cong \mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

□

Лемма 1. *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 2. *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 $n_p = 1$. □

Определение 1. Пусть N, H – группы. Пусть задан гомоморфизм $\psi\colon H \to \mathrm{Aut}(N)$. Рассмотрим множество пар (n, h) с операцией

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot \psi(h_1)(n_2), h_1 \cdot h_2).$$

Получим группу (это мы докажем в следующей лемме), которая называется *полупрямым произведением* групп N и H, (соответствующим гомоморфизму ψ). Обозначать эту группу мы будем $N \leftthreetimes H$.

Лемма 2. *Полупрямое произведение $N \leftthreetimes H$ – группа.*

Доказательство. Проверим ассоциативность операции.

$$((n_1, h_1) \cdot (n_2, h_2)) \cdot (n_3, h_3) = (n_1 \cdot \psi(h_1)(n_2), h_1 \cdot h_2) \cdot (n_3, h_3) = \\ = (n_1 \cdot \psi(h_1)(n_2) \cdot \psi(h_1 h_2)(n_3), h_1 \cdot h_2 \cdot h_3).$$

С другой стороны

$$(n_1, h_1) \cdot ((n_2, h_2) \cdot (n_3, h_3)) = (n_1, h_1) \cdot (n_2 \cdot \psi(h_2)(n_3), h_2 \cdot h_3) = \\ = (n_1 \cdot \psi(h_1)(n_2 \cdot \psi(h_2)(n_3)), h_1 \cdot h_2 \cdot h_3) = (n_1 \cdot \psi(h_1)(n_2) \cdot \psi(h_1 h_2)(n_3), h_1 \cdot h_2 \cdot h_3).$$

Поскольку получили одинаковый результат, умножение ассоциативно.

Единичный елемент (e_N, e_H), действительно

$$(e_N, e_H) \cdot (n, h) = (e_N \psi(e_H)(n), e_H h) = (e_N \mathrm{id}(n), h) = (n, h)$$

и

$$(n, h) \cdot (e_N, e_H) = (n\psi(h)(e_N), h e_H) = (n, h).$$

Обратный к элементу (n, h) – это элемент $(\psi(h^{-1})(n^{-1}), h^{-1})$. В самом деле

$$(n, h)(\psi(h^{-1})(n^{-1}), h^{-1}) = (n\psi(h)(\psi(h^{-1})(n^{-1})), h h^{-1}) = \\ = (n\psi(h h^{-1})(n^{-1}), e_H) = (n\psi(e)(n^{-1}), e_H) = (n\mathrm{id}(n^{-1}), e_H) = (n n^{-1}, e_H) = (e_N, e_H).$$

и

$$(\psi(h^{-1})(n^{-1}), h^{-1})(n, h) = (\psi(h^{-1})(n^{-1})\psi(h^{-1})(n), h^{-1} h) = \\ = (\psi(h^{-1})(n^{-1} n), e_H) = (\psi(h^{-1})(e_N), e_H) = (e_N, e_H).$$

□

Лемма 3. *а) Подмножество $(N, \{e\})$ является подгруппой, изоморфной N.*
б) Подмножество $(\{e\}, H)$ является подгруппой, изоморфной H.
в) Подгруппа $(N, \{e\}) \cong N$ изоморфна N нормальна в G.

Доказательство. а) $(n_1, e) \cdot (n_2, e) = (n_1 \cdot \psi(e)(n_2), e \cdot e) = (n_1 \cdot \mathrm{id}(n_2), e) = (n_1 n_2, e)$. Таким образом $N \to (N, \{e\})$, $n \mapsto (n, e)$ – изоморфизм.

б) $(e, h_1) \cdot (e, h_2) = (e \cdot \psi(h_1)(e), h_1 h_2) = (e, h_1 h_2)$. Таким образом $H \to (\{e\}, H)$, $h \mapsto (e, h)$ – изоморфизм.

в)

$$(\widehat{n}, \widehat{h})(n, e_H)(\widehat{n}, \widehat{h})^{-1} = (*, \widehat{h})(*, e_H)(*, \widehat{h}^{-1}) = (*, \widehat{h} e_H \widehat{h}^{-1}) = (*, e_H).$$

□

Замечание 1. Если ψ переводит все в тождественный автоморфизм, то $N \leftthreetimes H \cong N \times H$.

Предложение 3. *Пусть в некоторой группе G есть две подгруппы N и H, причем $N \cap H = \{e\}$, $G = \langle N, H \rangle$ и N нормальна. Тогда $G \cong N \leftthreetimes H$ – полупрямое произведение, соответствующее гомоморфизму $\psi\colon H \to \mathrm{Aut}(N)$ такому, что $\psi(h)(n) = h n h^{-1}$.*

Доказательство. В самом деле, мы уже знаем, что $G = NH = \{nh \mid n \in N, h \in H\}$. Отождествим nh с парой (n, h). Так как $N \cap H = \{e\}$, если $n_1h_1 = n_2h_2$, то выполнено $n_2^{-1}n_1 = h_2h_1^{-1}$. Этот элемент лежит в N с одной стороны и в H с другой. Так как $N \cap H = \{e\}$, то есть $n_2^{-1}n_1 = h_2h_1^{-1} = e$. Следовательно, $n_1 = n_2$ и $h_1 = h_2$. Значит, соответствие $nh \leftrightarrow (n, h)$ является биекцией.

При этом

$$(n_1h_1) \cdot (n_2h_2) = n_1(h_1n_2h_1^{-1})h_1h_2 = n_1\psi(h_1)(n_2)h_1h_2.$$

Значит, соответствие $nh \leftrightarrow (n, h)$ является гомоморфизмом. Итак, это гомоморфизм и биекция, то есть изоморфизм. □

Пример 1. *Группа D_n изоморфна полупрямому произведению $\mathbb{Z}_n \leftthreetimes \mathbb{Z}_2$, соответствующему гомоморфизму $\psi\colon \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_n)$, такому, что $\psi(0) = \mathrm{id}$, $\psi(1)\colon x \mapsto -x$.*

Действительно, рассмотрим группу поворотов $N \cong \mathbb{Z}_n$ и подгруппу $H = \{\mathrm{id}, s\} \cong \mathbb{Z}_2$, где s – некоторая симметрия. Тогда $N \triangleleft D_n$ и $s \circ R_\alpha \circ s^{-1} = R_{-\alpha}$.

Пример 2. *Группа S_n изоморфна полупрямому произведению $A_n \leftthreetimes \mathbb{Z}_2$ В самом деле при $H = \{\mathrm{id}, (1, 2)\} \cong \mathbb{Z}_2$ имеем $A_n \cap H = \{\mathrm{id}\}$, $A_n \triangleleft S_n$ и $S_n = \langle A_n, H\rangle$.*

Теорема 1. *Пусть $p > q$ – простые числа. Если p не сравнимо с 1 по модулю q, то существует единственная группа порядка pq (это $\mathbb{Z}_{pq}$). Если же p не сравнимо с 1 по модулю q, то существует ровно две группы порядка pq: одна $\mathbb{Z}_{pq}$, а другая – не абелева.*

Доказательство. По 3 теореме Силова n_p делит q и сравнимо с 1 по модулю p. Значит, $n_p = 1$. Пусть N – это единственная силовская p-подгруппа, она нормальна в G. Обозначим через H силовскую q-подгруппу. 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 $G = N \leftthreetimes H$. Это полупрямое произведение соответствует некоторому гомоморфизму

$$\psi\colon \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}.$$

Если p не сравнимо с 1 по модулю q, то $p-1$ не делится на q и образ $\psi(\mathbb{Z}_q)$ равен $\{e\}$. Значит, $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

Пусть p сравнимо с 1 по модулю q. Рассмотрим образ $\psi(\mathbb{Z}_q)$ в $\mathbb{Z}_{p-1}$. Это некая подгруппа в циклической группе. Ее порядок может быть равен либо 1 (и тогда мы получаем $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$) либо q. Если порядок образа равен q, то $\mathrm{Im}\,\psi$ – единственная подгруппа порядка q в $\mathbb{Z}_{p-1}$, то есть $\left\langle \frac{p-1}{q} \right\rangle$. При этом гомоморфизм ψ каким-то образом отображает $H \cong \mathbb{Z}_q$ изоморфно на $\mathrm{Im}\,\psi \cong \mathbb{Z}_q$.

Рассмотрим 2 таких полупрямых произведения, соответствующие гомоморфизмам $\psi_1\colon H \to \left\langle \frac{p-1}{q} \right\rangle$ и $\psi_2\colon H \to \left\langle \frac{p-1}{q} \right\rangle$. Заметим, что так как ψ_2 – изоморфизм, к нему есть орбатный. Рассмотрим отображение

$$\varphi\colon N \leftthreetimes_{\psi_1} H \to N \leftthreetimes_{\psi_2} H,$$

заданное по правилу

$$\varphi(n, h) = (n, \psi_2^{-1} \circ \psi_1(h)).$$

Проверим, что ψ – гомоморфизм. Имеем:

$$\varphi((n, h) \cdot (n', h')) = \varphi(n \cdot \psi_1(h)(n'), hh') = (n \cdot \psi_1(h)(n'), \psi_2^{-1} \circ \psi_1(hh'))$$

С другой стороны

$$\varphi(n,h)\varphi(n',h') = (n, \psi_2^{-1} \circ \psi_1(h))(n', \psi_2^{-1} \circ \psi_1(h')) =$$
$$= (n \cdot \psi_2(\psi_2^{-1} \circ \psi_1(h))(n'), \psi_2^{-1} \circ \psi_1(h) \cdot \psi_2^{-1} \circ \psi_1(h')) = (n \cdot \psi_1(h)(n'), \psi_2^{-1} \circ \psi_1(hh'))$$

Таким образом $\varphi((n,h) \cdot (n',h')) = \varphi(n,h)\varphi(n',h')$, то есть φ – гомоморфизм.

Проверим, что φ – биекция. Первая компонента при φ не меняется, а ко второй применяется композиция изоморфизмов $\psi_2^{-1} \circ \psi_1$. Это доказывает биективность φ.

Итак, гомоморфизм φ является биекцией, а значит, изоморфизмом. Это доказывает, что все полупрямые произведения $\mathbb{Z}_p \leftthreetimes \mathbb{Z}_q$, соответствующие нетривиальным гомоморфизмам $\mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p)$ изоморфны. Таким образом, существуют ровно две неизоморфные группы порядка pq при p сравнимом с 1 по модулю q. Так как абелева группа порядка pq всего одна, группа, соответствующая нетривиальным гомоморфизмам, не абелева. $\square$