Лекция 14.

Гайфуллин Сергей Александрович

МГУ

10 ноября, 2020

Пусть $|G| = p^k m$. Обозначим через n_p число силовских p-подгрупп в группе G.

Третья теорема Силова.
1) n_p сравнимо с 1 по модулю p,
2) n_p делит m.

Доказательство. 1) Пусть S – одна из силовских p-подгрупп. Рассмотрим действие S на множестве N силовских p-подгрупп сопряжениями. То есть $s \cdot S' = sS's^{-1}$. Пусть $Orb(S')$ – некая орбита. Тогда $|Orb(S')| \cdot |St(S')| = |S| = p^k$. Значит, $|Orb(S')| = p^l$. Среди орбит есть $Orb(S)$, которая состоит только из одной подгруппы S, таким образом, $|Orb(S)| = 1$. Пусть $S' \neq S$, допустим, что $|Orb(S')| = 1$. Тогда для любых $s \in S, s' \in S'$ имеем $ss's^{-1} \in S'$. Рассмотрим $H = SS' = \{ss' \mid s \in S, s' \in S'\}$. Докажем, что H – подгруппа. Действительно,

$$(s_1 s_1') \cdot (s_2 s_2') = s_1(s_2 s_2^{-1}) s_1' s_2 s_2' = s_1 s_2 (s_2^{-1} s_1' s_2) s_2' \in H,$$

$$(ss')^{-1} = s'^{-1} s^{-1} = (s^{-1}s) s'^{-1} s^{-1} = s^{-1}(ss'^{-1}s^{-1}) \in H.$$

Продолжение доказательства.

Получаем, что H – подгруппа в G. Получаем, что $|G| = p^k m$ делится на $|H|$, а $|H|$ делится на $|S| = p^k$. Значит, $|H| = p^k r$, где НОД$(r, p) = 1$. Поскольку, S и S' – силовские подгруппы в H, они сопряжены. То есть существует $h \in H$ такой, что $hS'h^{-1} = S$. Но $h = ss'$. Значит, $ss'S'(ss')^{-1} = S$. Но если $ss'S'(ss')^{-1} = s(s'S's'^{-1})s^{-1} \subset sS's^{-1}$. Но так как $|Orb(S')| = 1$, то $sS's^{-1} = S'$. Противоречие. Итак, множество N силовских p-подгрупп состоит из орбит, одна из них имеет порядок 1, а остальные имеют порядки p^l, где $l \neq 0$. Следовательно, $n_p = |N|$ имеет остаток 1 при делении на p.

Продолжение доказательства.

2) Рассмотрим действие группы G на множестве M всех подгрупп в G. То есть $g \cdot H = gHg^{-1}$. По второй теореме Силова все силовские p-подгруппы образуют одну орбиту $\mathcal{O}$. Пусть S – одна из силовских p-подгрупп. Тогда

$$|G| = |\mathcal{O}| \cdot |St(S)| = n_p \cdot |St(S)|.$$

Отсюда $|G| = p^k m$ делится на n_p. Так как НОД$(n_p, p) = 1$, получаем m делится на n_p.

Следствие. 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.

Утверждение. 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.

Следствие. 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

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, которая называется полупрямым произведением групп N и H, (соответствующим гомоморфизму ψ).

Обозначать эту группу мы будем $N \leftthreetimes H$.

Лемма. $N \leftthreetimes H$ – 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

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

Единичный елемент (e_N, e_H), Обратный к элементу (n, h) – это элемент $(\psi(h^{-1})(n^{-1}), h^{-1})$

Замечание.

Подгруппа $(N, \{e\}) \cong N$ изоморфна N нормальна в G.

Замечание.

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

Предложение. 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 $G \cong N \leftthreetimes H$, соответствующему $\psi(h)(n) = hnh^{-1}$.

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 $n_1 h_1 = n_2 h_2$, то $n_2^{-1} n_1 = h_2 h_1^{-1} = e$, то есть $n_1 = n_2$ и $h_1 = h_2$. При этом $(n_1 h_1) \cdot (n_2 h_2) = n_1 (h_1 n_2 h_1^{-1}) h_1 h_2 = n_1 \psi(h_1)(n_2) h_1 h_2$.

Пример.

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

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

Пример.

$S_n \cong A_n \leftthreetimes \mathbb{Z}_2$

В самом деле при $H = \{\mathrm{id}, (1,2)\} \cong \mathbb{Z}_2$ имеем $A_n \cap H = \{\mathrm{id}\}$, $A_n \lhd S_n$ и $S_n = \langle A_n, H \rangle$.

Теорема. 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 сравнимо с 1 по модулю q, то существует ровно две группы порядка pq: одна $\mathbb{Z}_{pq}$, а другая – не абелева.

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, $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

Продолжение доказательства.

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 $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$) либо q. Если порядок образа равен q, то $\operatorname{Im}\psi$ – 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 $\operatorname{Im}\psi \cong \mathbb{Z}_q$.

Рассмотрим 2 таких полупрямых произведения, соответствующие гомоморфизмам $\psi_1 \colon H_1 \to \left\langle \frac{p-1}{q} \right\rangle$ и $\psi_2 \colon H_2 \to \left\langle \frac{p-1}{q} \right\rangle$. Рассмотрим изоморфизм $\varphi \colon N \leftthreetimes H_1 \to N \leftthreetimes H_2$, $\varphi(n, h_1) = (n, \psi_2^{-1} \circ \psi_1(h_1))$.

Гомоморфизм φ является изоморфизмом.