Лекция 15

Теорема 1. *Пусть G – конечная группа. Следующие условия эквивалентны.*

1) Группа G разрешима.

2) G включается в ряд подгрупп

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

где G_i/G_{i+1} абелевы.

3) G включается в ряд подгрупп

$$G = \widetilde{G}_0 \triangleright \widetilde{G}_1 \triangleright \widetilde{G}_2 \triangleright \widetilde{G}_3 \triangleright \ldots \triangleright \widetilde{G}_m = \{e\},$$

где $\widetilde{G}_i/\widetilde{G}_{i+1}$ – циклические простого порядка (то есть $\mathbb{Z}_p$ для некоторого простого p).

Доказательство. $1 \Rightarrow 2$. Если G разрешима, можно взять $G_i = G^{(i)}$. Тогда $G_i/G_{i+1} = G^{(i)}/G^{(i+1)}$ – абелева группа.

$2 \Rightarrow 3$. Ряд $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright G_3 \triangleright \ldots \triangleright G_n = \{e\}$ можно уплотнить до композиционного

$$G = \widetilde{G}_0 \triangleright \widetilde{G}_1 \triangleright \widetilde{G}_2 \triangleright \widetilde{G}_3 \triangleright \ldots \triangleright \widetilde{G}_m = \{e\}.$$

Так как факторгруппы G_i/G_{i+1} абелевы, $G_i' \subseteq G_{i+1}$. Отсюда следует, что $\widetilde{G}_j' \subseteq G_{j+1}$. Тогда факторгруппы $\widetilde{G}_j/G_{j+1}$ абелевы. По предложению из лекции 14, они изоморфны $\mathbb{Z}_p$.

$3 \Rightarrow 1$. Пусть G включается в такой ряд подгрупп. Тогда $G/\widetilde{G}_1$ абелева, а значит, $G' \subseteq \widetilde{G}_1$. Аналогично $G^(2) \subseteq \widetilde{G}_2 \ldots G^(m) \subseteq \widetilde{G}_m = \{e\}$. Значит, G разрешима. $\square$

Определение 1. Группа SO(3) – это всех ортогональных преобразований трехмерного вещественного пространства, сохраняющих ориентацию (то есть определитель матрицы равен 1).

В ортонормированном базисе матрицы преобразований из SO(3) – это ортогональные матрицы ($A^T = A^{-1}$) с определителем 1.

В курсе линейной алгебры доказывалось, что матрица элемента из SO(3) может быть приведена в ортонормированном базисе к виду

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

То есть любой элемент SO(3) – это поворот вокруг некоторой оси.

Лемма 1. *Пусть $h \in \mathrm{SO}(3)$ – поворот на угол θ вокруг оси l. Тогда сопряженный элемент ghg^{-1} – это поворот на угол θ вокруг оси $g(l)$.*

Доказательство. У матрицы поворота на угол θ комплексные собственные значения равны 1, $\cos\theta + i\sin\theta$ и $\cos\theta - i\sin\theta$. Ясно, что у сопряженного оператора комплексные собственные значения такие же. Это доказывает равенство углов. Осталось объяснить, что ось вращения будет $g(l)$.

Пусть v – собственный вектор оператора h с собственным значением 1 (v направлен вдоль оси l). Тогда $(ghg^{-1})(gv) = ghv = gv$, то есть gv – собственный вектор с собственным значением 1 у оператора ghg^{-1}. Вектор gv направлен вдоль оси $g(l)$. $\square$

Лемма 2. *Композиция двух поворотов на угол π с углом между осями l и l' равным α, равна повороту относительно оси m, перпендикулярной l и l', на угол 2α.*

Доказательство. Ось m переворачивается при каждом из данных поворотов, а значит, в итоге с осью m происходит тождественное преобразование. Ось l при первом повороте остается неподвижной, а при втором повернется на угол 2α. □

Теорема 2. *Группа* $\mathrm{SO}(3)$ *проста.*

Доказательство. Пусть $H \neq \{\mathrm{id}\}$ – нормальная подгруппа в $\mathrm{SO}(3)$. Найдется поворот $h \in H$ на угол $\alpha \in (0, 2\pi)$ вокруг оси l. Пусть g – поворот на угол π вокруг оси m, образующей с осью l угол $\beta \in [0, \frac{\pi}{2}]$. Тогда $s = g(hg^{-1}h^{-1}) = (ghg^{-1})h^{-1} \in H$. При этом $hg^{-1}h^{-1}$ – поворот на угол π вокруг оси $h(m)$, которая образует с осью m угол γ. А значит, s – поворот на угол 2γ вокруг оси, перпендикулярной m и $h(m)$.

Угол γ равен 0 при $\beta = 0$ и равен α при $\beta = \frac{\pi}{2}$. По соображениям непрерывности угол γ может принимать все значения от 0 до α, то есть в H найдутся повороты на все углы от нуля до α. Рассматривая степени данных поворотов, получим повороты на все углы. По лемме, если в H лежит поворот на некий угол, то там лежат и все повороты на данный угол. Значит, $H = \mathrm{SO}(3)$. □

Определение 2. Пусть G – конечная группа порядка $|G| = p^k m$, где p – простое число, а m – число не делящееся на p. Подгруппа $S \subset G$ называется *силовской p-подгруппой* в G, если $|S| = p^k$.

Теорема 3 (Первая теорема Силова)**.** *Для каждого простого делителя p порядка группы G существует силовская p-подгруппа $S \subset G$.*

Доказательство. Рассмотрим сначала случай абелевой группы. Если G – абелева группа, то

$$G \cong \mathbb{Z}_{p^{\alpha_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{\alpha_k}} \oplus \mathbb{Z}_{p_1^{\beta_1}} \oplus \ldots \oplus \mathbb{Z}_{p_r^{\alpha_r}}.$$

Тогда

$$S = \mathbb{Z}_{p^{\alpha_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{\alpha_k}} \oplus \{0\} \oplus \ldots \oplus \{0\}.$$

Для общего случая проведем доказательство по индукции по порядку G. База индукции – это случай абелевой группы. Проведем шаг индукции.

Случай 1. $|Z(G)|$ делится на p.

$Z(G)$ – абелева группа. В ней найдется некая подгруппа A такая, что $|A| = p$. Ясно, что A – нормальная подгруппа в G. При этом $|G/A| = \frac{n}{p}$, где $n = |G|$. По предположению индукции в G/A есть силовская p-подгруппа B. Рассмотрим $\pi_A^{-1}(B) \subset G$. Имеем, $|\pi_A^{-1}(B)| = |\mathrm{Ker}\,(\pi_a\,|_{\pi_A^{-1}(B)})| \cdot |\mathrm{Im}\,(\pi_a\,|_{\pi_A^{-1}(B)})| = |A| \cdot |B| = p^k$. Можно взять $S = \pi_A^{-1}(B)$.

Случай 2. $|Z(G)|$ не делится на p.

Расмотрим разложение группы G на классы сопряженных элементов. Классы сопряженности, состоящие из одного элемента – это элементы центра. Так как $|G|$ делится на p, найдется класс сопряженности C такой, что $|C| \neq 1$ не делится на p. Пусть $g \in C$. Рассмотрим $|Z(g)| = \frac{|G|}{|C|} < |G|$. С другой стороны, $|Z(g)|$ делится на p^k. По предположению индукции есть силовская подгруппа $S \subset Z(g) \subset G$, при этом $|S| = p^k$. □

Лемма 3. *Если силовская подгруппа единственна, то она нормальна.*

Доказательство. Рассмотрим gSg^{-1} – это подгруппа G (проверьте это). Но $|gSg^{-1}| = |S|$. В самом деле, очевидно, что $|gSg^{-1}| \leq |S|$, с другой стороны, $S = g^{-1}(gSg^{-1})g$, значит, $S \leq |gSg^{-1}|$. Имеем, gSg^{-1} – силовская подгруппа G, а значит, $gSg^{-1} = S$, то есть S нормальна. □

Теорема 4 (Вторая теорема Силова)**.** *1) Любая p-подгруппа G содержится в некоторой силовской.*

2) Любые две силовские p-подгруппы сопряжены.

Доказательство. Случай $m = 1$ ясен. Пусть $m > 1$.

1) Пусть S – силовская p-подгруппа, $|S| = p^k$. Пусть $H \subset G$ – подгруппа порядка p^l, $l \leq k$. Рассмотрим действие H на множестве левых смежных классов по S:

$$h \cdot gS = (hg)S.$$

Корректность очевидна: если $gS = g'S$, то $g' = gs$ для некоторого $s \in S$. Тогда $hg' = hgs$ и $hgS = hg'S$. Из теоремы Лагранжа количество левых смежных классов по S равно $\frac{|G|}{|S|} = m$. Имеем, $|H| = p^l = |St(gS)| \cdot |Orb(gS)|$, значит, порядок каждой орбиты либо 1, либо степень p. Так как сумма порядков орбит не делится на p, есть орбита из одного элемента. То есть $hgS = gS$. Отсюда $g^{-1}hg \in S$, то есть $h \in gSg^{-1}$. Значит, $H \subset gSg^{-1}$, где $|gSg^{-1}| = p^k$.

2) Если H – силовская подгруппа, то $|H| = p^k$. По доказанному в пункте 1) выполнено $H \subset gSg^{-1}$. Поскольку $|H| = |gSg^{-1}|$, имеем $H = gSg^{-1}$. Значит, любая силовская p-подгруппа H сопряжена фиксированной силовской p-подгруппе S. □

Рассмотрим действие группы G на множестве всех подгрупп в группе G сопряжениями. В самом деле, легко убедиться, что если $H \subset G$ – подгруппа, то gHg^{-1} также подгруппа.

Определение 3. Стабилизатор подгруппы H при данном действии называется *нормализатором* H в G и обозначается $N_G(H)$.

Лемма 4. *1) $N_G(H)$ – подгруппа в G,*

2) $H \subseteq N_G(H)$,

3) H нормальна в $N_G(H)$,

4) Если H нормальна в K, где K – подгруппа G, то $K \subset N_G(H)$.

Доказательство. 1) По определению, $N_G(H)$ – стабилизатор, а значит, подгруппа в G.

2) Если $h \in H$, то $hHh^{-1} = H$. Значит, $h \in N_G(H)$.

3) При $g \in N_G(H)$ имеем $gHg^{-1} = H$, это доказывает нормальность H в $N_G(H)$.

4) Если $H \triangleleft K$, то для любого $k \in K$ выполнено $kHk^{-1} = H$, то есть

$$k \in St(H) = N_G(H).$$

□

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

Теорема 5 (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 M 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 $ss's^{-1} \in S'$. Следовательно, $S \subseteq N_G(S')$. Заметим, что $N_G(S')$ – это подгруппа в G, а значит, $|N_G(S')| = p^u v|$, где $u \leq k$ и $(p, v) = 1$. Так как $S \subseteq N_G(S')$, $u = k$. Значит, S – силовская p-подгруппа в $N_G(S')$. С другой стороны S' – силовская p-подгруппа в $N_G(S')$. Значит, S и S' сопряжены в $N_G(S')$. Но S' нормальна в $N_G(S')$, а значит, сопрягая S' элементами $N_G(S')$ мы не получим дргой подгруппы. ПРотиворечие. Значит, не существует такой $S' \neq S$, что $|Orb(S')| = 1$.

Итак, множество M силовских p-подгрупп состоит из орбит, одна из них имеет порядок 1, а остальные имеют порядки p^l, где $l \neq 0$. Следовательно, $n_p = |M|$ имеет остаток 1 при делении на p.

2) Рассмотрим действие группы G на множестве L 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. □