Лекция 13

Теорема 1 (Теорема Кэли)**.** *Пусть G – конечная группа порядка n. Тогда G изоморфна некоторой подгруппе в S_n.*

Доказательство. Пусть $|G| = n$. Рассмотрим α – действие G на себе левыми сдвигами. Это действие соответствует гомоморфизму $\varphi_\alpha \colon G \to S(G) \cong S_n$. (Явно этот гомоморфизм задается по правилу: элемент g переходит в биекцию $\overline{g} \mapsto g\overline{g}$ из G в G.) При этом ядро φ_α равно ядру неэффективности α. Но легко видеть, что $\mathrm{St}(e) = \{e\}$, а значит, $\mathrm{Ker}\,\alpha = \{e\}$. Значит, φ_α задает вложение G в S_n. $\square$

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.

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

$\square$

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. $\square$

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 $[x, y] \neq e \in G'$. $\square$

Определение 3. Подгруппа $H \subset G$ называется *характеристической*, если для любого автоморфизма $\varphi \colon G \to G$ выполнено $\varphi(H) = H$.

Характеристическая подгруппа автоматически является нормальной. Для доказательства этого достаточно рассмотреть внутренний автоморфизм $\varphi_g \colon h \mapsto ghg^{-1}$.

Лемма 4. *Характеристическая подгруппа характеристической подгруппы является характеристической.*

Доказательство. Пусть H – характеристическая подгруппа G, а N – характеристическая подгруппа H. Пусть $\varphi \in \mathrm{Aut}(G)$. Тогда $\varphi(H) = H$. Поскольку $\varphi^{-1}(H) = H$, получаем, что $\varphi\,|_H \colon H \to H$ – автоморфизм H. Значит, поскольку N характеристическая, $\varphi(N) = \varphi\,|_H\,(N) = N$. $\square$

Замечание 2. Напомним, что нормальная подгруппа нормальной подгруппы не всегда нормальна.

Предложение 1. *Коммутант и центр – характеристические подгруппы.*

Доказательство. Пусть G – группа. Рассмотрим $z \in Z(G)$, и пусть $\varphi \in \mathrm{Aut}(G)$. Тогда для любого $g \in G$ выполнено
$$\varphi(z)g = \varphi(z\varphi^{-1}(g)) = \varphi(\varphi^{-1}(g)z) = g\varphi(z).$$
То есть $\varphi(z) \in Z(G)$. Пусть теперь $g \in G'$. Тогда
$$g = [x_1, y_1] \dots [x_k, y_k].$$
Получаем
$$\varphi(g) = [\varphi(x_1), \varphi(y_1)] \dots [\varphi(x_k), \varphi(y_k)] \in G'.$$
□

Следствие 1. *Коммутант G' – нормальная подгруппа в G.*

Рассмотрим ряд *кратных коммутантов.* $G \supset G' \supset G'' \supset G^{(3)} \supset G^{(4)} \supset \dots$ Имеется в виду, что $(G^{(i)})' = G^{(i+1)}$. Из предложения следует, что $G^{(i)}$ – характеристическая (и в частности нормальная) подгруппа в G.

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 2. *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 $G' \subset H$. □

Лемма 6. *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, $\sigma = \tau_1 \dots \tau_{2m}$. 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, $H = A_n$.

□

Теорема 3. $S_n' = A_n$.

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 6 а). □

Теорема 4. *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 6 б). □

Теорема 5. *Пусть* F *– поле такое, что* $|F| \geq 4$. *Тогда*
1) $\mathrm{SL}_n(F)' = \mathrm{SL}_n(F)$
2) $\mathrm{GL}_n(F)' = \mathrm{SL}_n(F)$

Доказательство. 1) Для удобства записи сделаем нужную выкладку при $n = 2$. Поскольку $|F| \geq 4$, найдется $a \in F$ такое, что $a \notin \{0, 1, -1\}$. Тогда существует $(a^2-1)^{-1}$, и для любого $\mu \in F$ можно рассмотреть $\lambda = (a^2-1)^{-1}\mu$. Заметим, что

$$\left[\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a\lambda \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} a^{-1} & -a^{-1}\lambda \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & (a^2-1)\lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$$

Аналогично, при любом n выполняется $E + \mu E_{ij} \in \mathrm{SL}_n(F)'$ при всех $i \neq j$.

Группа $\mathrm{SL}_n(F)$ порождается элементами вида $E + \mu E_{ij}$. В самом деле, любую матрицу A из $\mathrm{SL}_n(F)$ можно привести элементарными преобразованиями первого типа к матрице E (докажите это!). При этом происходит умножение на матрицы вида $E+\mu E_{ij}$. Получаем

$$(E+\mu_k E_{i_k j_k})\dots(E+\mu_1 E_{i_1 j_1})A = E.$$

Значит,

$$A = (E-\mu_1 E_{i_1 j_1})\dots(E-\mu_k E_{i_k j_k}).$$

2) $\mathrm{GL}_n(F)' \supset \mathrm{SL}_n(F)' = \mathrm{SL}_n(F)$.

С другой стороны $\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \cong F^\times$ – абелева группа, а значит, $\mathrm{GL}_n(F)' \subset \mathrm{SL}_n(F)$. Получаем $\mathrm{GL}_n(F)' = \mathrm{SL}_n(F)$. □

Лемма 7. *Пусть $\varphi\colon G \to K$ – гомоморфизм групп. Тогда $\varphi(G') \subset K'$. Если гомоморфизм φ сюрeктивен, то $\varphi(G') = K'$.*

Доказательство. Поскольку φ – гомоморфизм,

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

Значит, $\varphi([x,y]) \in K'$, и следовательно, $\varphi(G') \subset K'$.

Если же φ сюръективен, то для любых $a,b \in K$ найдутся $x,y \in G$ такие, что $\varphi(x) = a$, $\varphi(y) = b$. Тогда

$[a,b] = [\varphi(x),\varphi(y)] = \varphi([x,y]) \subset \varphi(G')$. Значит, $\varphi(G') = K'$. □

Следствие 2. *Пусть $G \triangleright H$. Тогда $(G/H)' \cong G'/(H\cap G')$.*

Доказательство. Применим лемму к сюръективному каноническому гомоморфизму $\pi_H\colon G \to G/H$. Получим $(G/H)' = \pi_H(G')$. Рассмотрим ограничение $\pi_H\mid_{G'}$. Имеем $\mathrm{Ker}(\pi_H\mid_{G'}) = H\cap G'$, $\mathrm{Im}(\pi_H\mid_{G'}) = \pi_H(G')$ По теореме о гомоморфизме получаем утверждение следствия. □

Определение 4. 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, $S_n' = A_n$, $A_n' = A_n$.*

Лемма 8. *Подгруппа разрешимой группы разрешима.*

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