Лекция 11

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.

$2 \Rightarrow 3$. По лемме **??** 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 **??**, 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. □

Теорема 2. *Группа A_n проста при $n \geq 5$.*

Сперва докажем следующие две леммы.

Лемма 1. *При $n \geq 5$ все циклы длины 3 сопряжены в A_n.*

Доказательство. Докажем, что любой тройной цикл (a, b, c) сопряжен циклу $(1, 2, 3)$. В S_n эти циклы сопряжены перестановкой

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots \\ a & b & c & u & v & \ldots \end{pmatrix},$$

то есть $\sigma(1, 2, 3)\sigma^{-1} = (a, b, c)$. Если σ – четная перестановка, то $(1, 2, 3)$ и (a, b, c) сопряжены в A_n. Если же σ – нечетная перестановка, то рассмотрим

$$\widehat{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots \\ a & b & c & v & u & \ldots \end{pmatrix} \in A_n.$$

Тогда $\widehat{\sigma}(1, 2, 3)\widehat{\sigma}^{-1} = (a, b, c)$ □

Лемма 2. *В A_n все пары несмежных транспозиций сопряжены.*

Доказательство. Пусть $\sigma = (a, b)(c, d)$ – пара несмежных транспозиций. Докажем, что σ сопряжена $(1, 2)(3, 4)$. Возьмем

$$\xi = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots \\ a & b & c & d & \ldots \end{pmatrix} \in S_n.$$

Тогда $\xi(1,2)(3,4)\xi^{-1} = \sigma$. Если $\xi \in A_n$, то $(1,2)(3,4)$ и σ сопряжены в A_n. Если же ξ – нечетная перестановка, то рассмотрим

$$\widehat{\xi} = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots \\ b & a & c & d & \dots \end{pmatrix} \in A_n.$$

Имеем $\widehat{\xi}(1,2)(3,4)\widehat{\xi}^{-1} = \sigma$, то есть $(1,2)(3,4)$ и σ сопряжены в A_n. □

Доказательство теоремы 2. Пусть H – нормальная подгруппа в A_n.

Случай 1. В H есть тройной цикл (abc). Поскольку H нормальна в A_n, а все тройные циклы в A_n сопряжены (по лемме 1), то все тройные циклы лежат в H. Поскольку A_n порождается тройными циклами (см. лемму **??**), $H = A_n$.

Случай 2. В H есть перестановка δ, в разложении которой есть цикл длины не менее 5.

$$\delta = (x_1, x_2, x_3, x_4, x_5, \dots, x_m)(\dots)\dots(\dots)$$

Сопряжем δ с помощью перестановки $\xi = (x_1x_3)(x_2x_4)$. Получаем

$$\xi\delta\xi^{-1} = (x_1x_3)(x_2x_4)(x_1, x_2, x_3, x_4, x_5, \dots, x_m)(\dots)\dots(\dots)(x_1x_3)(x_2x_4) = \\ = (x_3x_4x_1x_2x_5\dots, x_m)(\dots)\dots(\dots) \in H.$$

Тогда

$$[(x_3, x_4, x_1, x_2, x_5, \dots, x_m)(\dots)\dots(\dots)]^{-1} \circ [(x_1, x_2, x_3, x_4, x_5, \dots, x_m)(\dots)\dots(\dots)] = \\ = (x_2x_mx_4) \in H$$

Попадаем в случай 1.

Случай 3. В H есть перестановка σ, в разложении которой есть хотя бы два цикла длины 3.

$$\sigma = (a, b, c)(d, e, f)\dots.$$

Тогда

$$(a, b, c, d, e)\sigma(a, b, c, d, e)^{-1} = (b, c, d)(e, a, f)\dots = \delta.$$

Имеем $\delta^{-1}\sigma = (a, d, f, c, e)$. Попадаем в случай 2.

Случай 4. В H есть перестановка σ, в разложении которой есть хотя бы три цикла длины 2. Сопряжем $\sigma = (a, b)(c, d)(e, f)\dots$ с помощью (a, b, c, d, e), получим

$$\delta = (bc)(de)(af)\dots.$$

Перемножив $\delta^{-1}\sigma$, получаем $(a, c, e)(b, f, d)$ и попадем в случай 3.

Случай 5. В H есть перестановка, разлагающаяся в 2 цикла длины 2. По лемме 2 там есть все пары несмежных транспозиций. А они порождают A_n.

Случай 6. В H есть перестановка σ, в разложении которой есть циклы длины 2 и 3 при этом есть хотя бы 1 цикл длины 3. Если мы не в условиях случая 3, то в σ есть лишь 1 цикл длины 3. Возведем σ в квадрат, попадем в случай 1.

Случай 7. В H есть перестановка σ, в разложении которой есть циклы длины 2, 3 и 4 при этом есть хотя бы 1 цикл длины 4. Возведем σ в квадрат, попадем в один из случев 6, 4 или 5.

□

Определение 1. Множество R с двумя бинарными операциями $+$ и $\cdot$ называется *кольцом*, если выполнено
1) $(a+b)+c=a+(b+c)$,
2) существует 0 такой, что $a+0=0+a=a$,
3) для каждого a существует $(-a)$ такой, что $a+(-a)=(-a)+a=0$,
4) $a+b=b+a$,
5) $a(b+c)=ab+ac$,
6) $(a+b)c=ac+bc$.

Кольцо ассоциативно, если
7) $(ab)c=a(bc)$.
Кольцо с единицей, если
8) существует 1 такой, что $1a=a1=a$.
Кольцо коммутативно, если
9) $ab=ba$.
Коммутативное ассоциативное кольцо с единицей называется *полем*, если выполнено
10) для каждого $a\neq 0$ найдется a^{-1} такой, что $aa^{-1}=a^{-1}a=1$.

Пример 1. *1)* $\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}_p$ *– это поля.*
2) $\mathbb{Z},\mathbb{Z}_n,\mathbb{R}[x]$ *– коммутативные кольца.*
3) $\mathrm{Mat}_n(F),\mathbb{C}[G]$ *– вообще говоря не коммутативные, но ассоциативные кольца.*
4) $(\mathbb{R}^3,+,[,])$ *– не ассоциативное кольцо.*

Замечание 1. Далее в нашем курсе мы будем рассматривать только ассоциативные кольца. Таким образом все кольца, о которых будет идти речь, предполагаются ассоциативными.

Определение 2. Пусть фиксировано поле F. Множество A называется *алгеброй* (над F), если на нем определены три операции: сложение, умножение и умножение на скаляр (элемент поля F) такие, что
1) A с операциями сложения и умножения – это кольцо,
2) A с операциями сложения и умножения на скаляр – это векторное пространство над F,
3) $(\lambda a)b=a(\lambda b)=\lambda(ab)$.

Пример 2. *Матрицы* $n\times n$ *образуют ассоциативную алгебру с единицей.*

Определение 3. Если $a,b\in R$ и выполнено $a\neq 0$, $b\neq 0$, $ab=0$, то элемент a называется *левым делителем нуля*, а элемент b – *правым делителем нуля.*

Объединение множества левых и правых делителей нуля называется множеством делителей нуля.

Лемма 3. *Обратимые элементы не являются делителями нуля.*

Доказательство. Пусть $a\neq 0$, $b\neq 0$, $ab=0$. В пусть при этом элемент a обратим. Тогда $b=a^{-1}ab=a^{-1}0=0$. Противоречие. □

Определение 4. Элемент $x\neq 0$ называется *нильпотентным*, если существует натуральное n такое, что $x^n=0$.

Замечание 2. Так как $x^n=x\cdot x^{n-1}=x^{n-1}\cdot x$, нильпотент является (двусторонним) делителем нуля.

Пример 3. *1) В кольце* $\mathbb{Z}_6$ *выполнено* $2 \cdot 3 = 0$*, то есть 2 и 3 – делители нуля (но не нильпотенты).*

2) В кольце $\mathbb{Z}_4$ *выполнено* $2^2 = 0$*, то есть 2 – нильпотент.*

3) В кольце $\mathrm{Mat}_2(\mathbb{R})$ *выполнено* $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$*, то есть это делители нуля (не нильпотенты).*

4) В кольце $\mathrm{Mat}_2(\mathbb{R})$ *выполнено* $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$*, то есть это нильпотент.*

Определение 5. *Алгебра* над полем F – это множество A с тремя операциями. Две из них бинарные: сложение и умножение. А последняя – умножение на число (элемент поля F). При этом выполнены следующие свойства.

1) $(a + b) + c = a + (b + c)$;
2) существует $0 \in A$ такой, что $a + 0 = 0 + a = a$;
3) $\forall a \in A$ существует $-a \in A$: $a + (-a) = (-a) + a = 0$;
4) $a + b = b + a$;
5) $a(b + c) = ac + ac$;
6) $(a + b)c = ac + bc$;
7) $\lambda(a + b) = \lambda a + \lambda b$;
8) $(\lambda + \mu)a = \lambda a + \mu a$;
9) $(\lambda\mu)a = \lambda(\mu)a$;
10) $1a = a$;
11) $\lambda(ab) = (\lambda a)b = a(\lambda b)$.

Пример 4. *1)* $\mathrm{Mat}_{n\times n}(F)$ *– алгебра над* F*;*

2) $F[x_1, \ldots, x_n]$ *– алгебра над* F*;*

3) Если $F \subset K$ *– вложение полей, то* K *– алгебра над* F*. (Например,* $\mathbb{C}$ *– алгебра над* $\mathbb{R}$*);*

4) $\mathbb{H}$ *– алгебра кватернионов над* $\mathbb{R}$*.*

$\mathbb{H} = \langle 1, i, j, k\rangle_{\mathbb{R}}$*, где умножение базисных элементов происходит как в* Q_8*.* $\mathbb{H}$ *– ассоциативная не коммутативная 4-мерная алгебра с единицей над* $\mathbb{R}$*.*

Пусть $q = a + bi + cj + dk$*. Определим сопряженный кватернион* $\overline{q} = a - bi - cj - dk$*. Тогда* $q\overline{q} = a^2 - (bi + cj + dk)^2 = a^2 + b^2 + c^2 + d^2 = |q|^2$*.*