Глава 2

Алгебраическая независимость значений Е-функций.

Лекция 2

Экспоненциальная функция e^z есть решение дифференциального уравнения $y' = y$. Основной результат второй главы обобщает теорему Линдемана - Вейерштрасса на целые функции, удовлетворяющие произвольным линейным дифференциальным уравнениям с коэффициентами из $\mathbb{C}(z)$. Дополнительно, рассматриваемые функции должны обладать некоторыми арифметическими свойствами, что делают их похожими в определенном смысле на e^z. Этот класс функций, они носят название Е-функции, был введен в 1929г. К.Зигелем, которому удалось исследовать значения Е-функций, удовлетворяющих линейным дифференциальным уравнениям второго порядка, или совокупностям таких уравнений. В полной общности соответствующий результат был доказан в 1955г. А.Б.Шидловским.

2.1 Е-функции и их основные свойства.

Следующее определение было предложено в 1929г. К.Зигелем.

Определение 1. *Аналитическая функция*

$$f(z) = \sum_{n=0}^{\infty} c_n \frac{z^n}{n!} \tag{2.1}$$

называется Е-функцией, если

1. *все коэффициенты c_n содержатся в некотором поле алгебраических чисел $\mathbf{K}$, имеющем конечную степень;*

2. *при любом $\varepsilon > 0$ и $n \to \infty$ справедлива оценка*

$$\overline{|c_n|} = O(n^{\varepsilon n}),$$

где, как и в Главе 1, символ $\overline{|a|}$ обозначает максимум модулей чисел, сопряженных с a;

3. *при любом* $\varepsilon > 0$ *существует последовательность натуральных чисел* $q_1, q_2, \ldots$, $q_n = O(n^{\varepsilon n})$, *такая, что при всех* n *имеет место включение*

$$q_n c_j \in \mathbb{Z}_{\mathbf{K}}, \quad 0 \le j \le n.$$

Экспоненциальная функция e^z, конечно, является E-функцией. Любой многочлен с алгебраическими коэффициентами также принадлежит к классу E-функций. Чуть позже мы приведем и другие примеры. Сейчас же отметим некоторые свойства класса E-функций, полезные, в частности, и для конструкции новых примеров. Из определения сразу же следует, что каждая E-функция является целой функцией.

Лемма 1. 1. *Совокупность E-функций образует кольцо относительно обычных операций сложения и умножения. Оно в дальнейшем будет обозначаться буквой* $\mathbb{E}$.

2. *Кольцо* $\mathbb{E}$ *замкнуто относительно операций дифференцирования и интегрирования в пределах от* 0 *до* z.

3. *Если функция (2.1) принадлежит к кольцу E-функций и последовательность* $\gamma_n \in \mathbf{K}, n \ge 0$, *удовлетворяет условиям 2 и 3 определения E-функции, то функция*

$$g(z) = \sum_{n=0}^{\infty} c_n \gamma_n \frac{z^n}{n!}$$

также является E-функцией. В частности, при любом алгебраическом α *имеем* $f(\alpha z) \in \mathbb{E}$.

В частности, из этой леммы следует, что функции

$$\sin z = \frac{e^{iz} - e^{-iz}}{2i}, \quad \cos z = \frac{e^{iz} + e^{-iz}}{2}$$

принадлежат к кольцу E-функций.

Доказательство. Пусть

$$u(z) = \sum_{n=0}^{\infty} a_n \frac{z^n}{n!}, \qquad v(z) = \sum_{n=0}^{\infty} b_n \frac{z^n}{n!}$$

- две E-функции. Не уменьшая общности можно считать, что конечное расширение $\mathbf{K} \supset \mathbb{Q}$ содержит как все коэффициенты a_n, так и все коэффициенты b_n. Пусть ε - произвольное положительное число. Тогда согласно определению E-функции существует постоянная $\kappa_1 = \kappa_1(\varepsilon) > 0$ такая, что

$$\overline{|a_n|} \le \kappa_1 n^{\varepsilon n}, \quad \overline{|b_n|} \le \kappa_1 n^{\varepsilon n}. \tag{2.2}$$

Кроме того существуют последовательность целых чисел q_n и постоянная $\kappa_2 = \kappa_2(\varepsilon) > 0$ с условием

$$q_n a_k \in \mathbb{Z}_{\mathbf{K}},\ q_n b_k \in \mathbb{Z}_{\mathbf{K}}, \quad n \ge 0,\ 0 \le k \le n,$$
$$0 \le q_n \le \kappa_2 n^{\varepsilon n}$$

Пользуясь теперь оценками для суммы сопряженных чисел, находим

$$\overline{|a_n \pm b_n|} \le 2\kappa_1 n^{\varepsilon n}, \quad q_n(a_k \pm b_k) \in \mathbb{Z}_{\mathbf{K}}, \quad 0 \le k \le n.$$

Это доказывает, что функции $u(z) \pm v(z)$ также принадлежат к классу Е-функций.

Имеем представление $u(z) \cdot v(z) = \sum_{n=0}^{\infty} c_n \frac{z^n}{n!}$, где $c_n = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}$. Поэтому

$$\overline{|c_n|} \le \kappa_3 n^{2\varepsilon n}, \quad q_n^2 c_n \in \mathbb{Z}_{\mathbf{K}}, \quad q_n^2 \le \kappa_2^2 n^{2\varepsilon n}.$$

В силу произвольности ε последние неравенства означают, что функция $u(z)v(z)$ является Е-функцией. Этим завершается доказательство пункта 1 леммы 2.1.

Для доказательства пункта 2 заметим, что для Е-функции $f(z)$, определенной рядом (2.1), справедливы равенства

$$f'(z) = \sum_{n=0}^{\infty} c_{n+1} \frac{z^n}{n!}, \quad \int_0^z f(t)dt = \sum_{n=1}^{\infty} c_{n-1} \frac{z^n}{n!}.$$

Теперь нужное утверждение получается с помощью тривиальных оценок.

Доказательство пункта 3 также проводится с помощью несложных оценок и оставляется в качестве упражнения. □

2.2 Гипергеометрические Е-функции.

Для построения новых примеров Е-функций над понадобится следующее вспомогательное утверждение. В его формулировке используется обозначение $(\alpha)_k = \alpha(\alpha+1)\cdots(\alpha+k-1)$, $k \ge 1$, и $(\alpha)_0 = 1$.

Лемма 2. *Пусть $\alpha, \beta \in \mathbb{Q}, \beta \ne 0, -1, -2, \ldots$. Обозначим*

$$\xi_k = \frac{(\alpha)_k}{(\beta)_k}, k \ge 1$$

и $d_n \in \mathbb{Z}, d_n > 0$ - общий знаменатель чисел $\xi_1, \cdots, \xi_n$. Тогда существуют положительные числа γ_1, γ_2, зависящие только от α и β такие, что

$$|\xi_n| \ \le \ e^{\gamma_1 n}, \quad d_n \le e^{\gamma_2 n} \ \textit{для} \ \ n \ge 1.$$

Доказательство. Пусть $k \ge n_0$ где n_0 - наименьшее целое, удовлетворяющее неравенству $n_0 \ge |\alpha| + 2|\beta|$. Тогда для всех $k \ge n_0$ справедливы неравенства

$$\left|\frac{\xi_{k+1}}{\xi_k}\right| \ = \ \left|\frac{\alpha+k}{\beta+k}\right| \ \le \ 2.$$

Это означает, что для всех $n \ge n_0$ справедливы неравенства

$$\mid \xi_n \ \mid \le \mid \xi_{n_0} \mid 2^{n-n_0},$$

доказывающие верхнюю оценку для $\mid \xi_n \mid$.

Пусть $\alpha = \frac{a}{b}, \beta = \frac{c}{d}$, где $b > 0, d > 0$ и $(a, b) = (c, d) = 1$. Тогда

$$\xi_k = \frac{d^k a(a+b)\cdots(a+(k-1)b)}{b^k c(c+d)\cdots(c+(k-1)d)} \;=\; \frac{d^k M_k}{b^k N_k},$$

где $N_k = c(c+d)\cdots(c+(k-1)d)$.

Для каждого целого N будем обозначать символом $\nu_p(N)$ кратность, с которой простое число p входит в разложение N на простые сомножители. Это обозначение естественным способом распространяется на рациональные числа N.

Пусть $N = u_1 \cdots u_k, u_k \in \mathbb{Z}$, и s_r обозначает количество сомножителей $u_j, 1 \leq j \leq k$, делящихся на $p^r, r \geq 1$. Тогда

$$\nu_p(N) = (s_1 - s_2) + 2(s_2 - s_3) + 3(s_3 - s_4) + \cdots = s_1 + s_2 + \cdots .$$

Если $p \nmid d$, то любое множество из p^r целых чисел $v, v+d, \ldots, v+(p^r-1)d$ содержит единственное число, делящееся на p^r. Поэтому для N_k справедливы неравенства

$$\left[\frac{k}{p^r}\right] \leq s_r \leq 1 + \left[\frac{k}{p^r}\right]$$

и $s_r = 0$, если $p^r > |c| + kd$.

Отсюда имеем

$$\nu_p(N_k) \leq \sum_{i \geq 1} \left[\frac{k}{p^i}\right] + \left[\frac{\log(\mid c \mid + kd)}{\log p}\right], \quad k \geq 1. \tag{2.3}$$

Это неравенство, конечно, выполняется и для простых чисел p, делящих d.

Те же соображения показывают, что при $p \nmid b$ справедливо неравенство

$$\nu_p(M_k) \geq \sum_{i \geq 1} \left[\frac{k}{p^i}\right], \quad k \geq 1. \tag{2.4}$$

Рассмотрим отдельно два случая. Если $p \mid b$, то

$$\nu_p(\xi_k) \geq -\nu_p(b^k) - \nu_p(N_k) \geq$$
$$-k\nu_p(b) - \sum_{i \geq 1} \frac{k}{p^i} - \left[\frac{\log(\mid c \mid + kd)}{\log p}\right] \geq -2k\nu_p(b) - \left[\frac{\log(\mid c \mid + kd)}{\log p}\right]. \tag{2.5}$$

Если же $p \nmid b$, то согласно (2.3) и (2.4) имеем

$$\nu_p(\xi_k) \geq \nu_p(M_k) - \nu_p(N_k) \geq -\left[\frac{\log(\mid c \mid + kd)}{\log p}\right]. \tag{2.6}$$

Обозначим

$$q_n = b^{2n} \prod_{p \leq |c| + nd} p^{\left[\frac{\log(|c| + nd)}{\log p}\right]}.$$

Тогда q_n - натуральное число, и из (2.5), (2.6) следует, что $q_n \xi_n \in \mathbb{Z}$. Так как при этом $q_n \mid q_{n+1}$, заключаем, что $q_n \xi_k \in \mathbb{Z}$ для $0 \leq k \leq n$. Теорема Чебышева об оценке количества простых чисел утверждает, что

$$\pi(x) = \sum_{p \leq x} 1 = O(\frac{x}{\log x}).$$

Поэтому
$$q_n \le b^{2n} \prod_{p\le |c|+nd} (\mid c \mid +nd) \ \le \ e^{\gamma_2 n},$$
и это завершает доказательство Леммы 2.2. $\square$

Лекция 3

Следующая лемма была доказана в конце прошлой лекции. В её формулировке используется обозначение $(\alpha)_k = \alpha(\alpha+1)\cdots(\alpha+k-1)$, $k\ge 1$, и $(\alpha)_0 = 1$.

Лемма 3. *Пусть $\alpha, \beta \in \mathbb{Q}, \beta \ne 0, -1, -2, \ldots$. Обозначим*
$$\xi_k = \frac{(\alpha)_k}{(\beta)_k}, k \ge 1$$
и $d_n \in \mathbb{Z}, d_n > 0$ - общий знаменатель чисел $\xi_1, \cdots, \xi_n$. Тогда существуют положительные числа γ_1, γ_2, зависящие только от α и β такие, что
$$|\xi_n| \ \le \ e^{\gamma_1 n}, \quad d_n \le e^{\gamma_2 n} \ \textit{для} \ \ n \ge 1.$$

Рассмотрим теперь обобщенную гипергеометрическую функцию
$$f(z) =_p F_q \left(\begin{array}{c} a_1, \cdots, a_p \\ b_1, \cdots, b_q \end{array} \middle| \ z \right) = \sum_{n=0}^{\infty} \frac{(a_1)_n \cdots (a_p)_n}{(b_1)_n \cdots (b_q)_n} \frac{z^n}{n!},$$
где $a_1, \ldots, a_p, b_1, \ldots, b_q \in \mathbb{C}, b_j \ne 0, -1, -2, \ldots$ и $0 \le p \le q$. Эта функция удовлетворяет дифференциальному уравнению
$$(\theta \prod_{i=1}^{q} (\theta + b_i - 1) - z \prod_{i=1}^{p} (\theta + a_i))y = 0,$$
где $\theta = z\frac{d}{dz}$. Действительно, если обозначить коэффициенты ряда, оgределяющего $f(z)$, буквами c_n, т.е. так, что $f(z) = \sum_{n=0}^{\infty} c_n \frac{z^n}{n!}$, то
$$\theta \prod_{i=1}^{q} (\theta + b_i - 1) f(z) = \sum_{n=1}^{\infty} c_n (n+b_1-1)\cdots(n+b_q-1)\frac{z^n}{(n-1)!},$$
$$z \prod_{i=1}^{p} (\theta + a_i) f(z) = \sum_{n=0}^{\infty} c_n (n+a_1)\cdots(n+a_q)\frac{z^{n+1}}{n!}.$$

Следующее утверждение принадлежит К.Зигелю.

Лемма 4. *Если $a_1, \ldots, a_p, \ b_1, \ldots, b_q \in \mathbb{Q}, \ b_j \ne 0, -1, \ldots,$ и $m = q - p + 1 \ge 0$, то функция*
$$f(z) =_p F_q \left(\begin{array}{c} a_1, \cdots, a_p \\ b_1, \cdots, b_q \end{array} \middle| \ z^m \right)$$
является E-функцией.

Доказательство. Воспользуемся, как и ранее, обозначениями

$$f(z)=\sum_{n=0}^{\infty}\frac{(a_1)_n\cdots(a_p)_n}{(b_1)_n\cdots(b_q)_n}\frac{z^{mn}}{n!}=\sum_{n=0}^{\infty}c_n\frac{z^n}{n!},$$

где

$$c_n=\begin{cases}0,\text{если } m\nmid n,\\ d_k,\text{если } n=mk,\end{cases}\tag{2.7}$$

причем

$$d_k=\frac{(a_1)_k\cdots(a_p)_k(k!)^{q-p}}{(b_1)_k\cdots(b_q)_k}\cdot\frac{(mk)!}{(k!)^m}.$$

Все отношения

$$\frac{(a_j)_k}{(b_j)_k},\quad \frac{k!}{(b_j)_k}$$

имеют такой же вид, как числа ξ_k из леммы 2, а множитель $\frac{(mk)!}{(k!)^m}$ есть целое число, ограниченное сверху величиной m^{mk}. По этой лемме и пункту 3 леммы 1 можно утверждать, что функция $g(z)=\sum\limits_{n=0}^{\infty}d_n\frac{z^n}{n!}$ является E-функцией. Более того, из леммы 2 следует, что с некоторой положительной константой γ_1 выполняются неравенства $|d_n|\le e^{\gamma_1 n},\ n\ge 1$, а общий знаменатель q_n для чисел $d_0,\dots,d_n$ также оценивается сверху величиной $e^{\gamma_2 n},\ n\ge 1,\gamma_2>0$. Из (2.7) следует теперь, что $|c_n|\le e^{\gamma_1 n},\ n\ge 1$ и $q_nc_j\in\mathbb{Z}_{\mathbf{K}},\ n\ge 1, 0\le j\le n$. Это завершает доказательство леммы. □

E-функции, определенные в лемме 3, принято называть гипергеометрическими E-функциями. Из доказательства леммы 3 следует, что для таких функций оценки $O(n^{\varepsilon n})$ в п.п. 2,3 определения E-функции могут быть заменены на $O(c^n)$ при достаточно большой постоянной c, зависящей от a_j,b_j.

2.3 Теорема Шидловского и некоторые её следствия.

Основной результат о значениях E-функций дает следующая теорема.

Теорема 1 (А.Б. Шидловский, 1955г.)**.** *Пусть E-функции $f_1(z),\dots,f_m(z)$ составляют решение системы линейных дифференциальных уравнений*

$$y_k'=q_{k0}+\sum_{j=1}^{m}q_{kj}y_j,\quad q_{kj}\in\mathbb{C}(z),\tag{2.8}$$

и алгебраически независимы над полем рациональнх функций $\mathbb{C}(z)$. Тогда для любого алгебраического числа α, отличного от нуля и особых точек системы (2.17), значения

$$f_1(\alpha),\dots,f_m(\alpha)$$

алгебраически независимы над $\mathbb{Q}$.

Например, функции $f_j(z) = e^{\beta_j z}, 1 \le j \le r$ при алгебраических β_j принадлежат к классу E-функций и удовлетворяют системе дифференциальных уравнение $y_j' = \beta_j y_j$. Если показатели β_j линейно независимы над $\mathbb{Q}$, то функции $f_j(z)$ алгебраически независимы над $\mathbb{C}(z)$. Из теоремы 2.1 следует, что значения этих функций в точке $z = 1$, т.е. числа $e^{\beta_1}, \ldots, e^{\beta_r}$ алгебраически независимы над $\mathbb{Q}$. Это доказывает теорему 1.4. Таким образом, теорема 2.1 обобщает теорему Линдемана - Вейерштрасса.

В 1929г. К.Зигель исследовал алгебраическую независимость значений функции

$$K_\lambda(z) = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!(\lambda+1)\cdots(\lambda+n)} \left(\frac{z}{2}\right)^{2n}$$

и ее производной $K_\lambda'(z)$, $\lambda \in \mathbb{Q}$, в алгебраических точках. Эта функция связана с функцией Бесселя $J_\lambda(z)$ соотношением

$$J_\lambda(z) = \frac{1}{\Gamma(\lambda+1)} \left(\frac{z}{2}\right)^{\lambda} K_\lambda(z)$$

и удовлетворяет дифференциальному уравнению

$$y'' + \frac{2\lambda+1}{z} y' + y = 0. \tag{2.9}$$

Справедливо тождество

$$K_\lambda(z) = {}_1F_2\left(\begin{array}{c} 1 \\ 1, \lambda+1 \end{array} \middle| \left(\frac{iz}{2}\right)^2 \right),$$

из которого в силу лемм 2.3 и 2.1 следует, что при рациональных $\lambda \ne -1, -2, \ldots$, функция $K_\lambda(z)$ является E-функцией.

Следующая теорема, доказанная в 1929г., принадлежит К.Зигелю.

Теорема 2. *Если λ - рациональное число, отличное от отрицательных целых, и кроме того удовлетворяющее условию $\lambda - \frac{1}{2} \notin \mathbb{Z}$, а α - отличное от нуля алгебраическое число, то числа*

$$K_\lambda(\alpha), \qquad K_\lambda'(\alpha)$$

алгебраически независимы над $\mathbb{Q}$.

Зигель доказал Теорему 2.2 непосредственно. Соответствующим образом развитый, его метод позволил А.Б.Шидловскому доказать и общую теорему 2.1, содержащую, в частности, утверждение Теоремы 2.2. Мы сейчас покажем, каким образом Теорема 2.2 может быть выведена из Теоремы 2.1. Обозначим для этого $f_1(z) = K_\lambda(z),\ f_2(z) = K_\lambda'(z)$. Так как функция $K_\lambda(z)$ есть решение уравнения (2.9), то определенные выше функции $f_j(z)$ составляют решение системы дифференциальных уравнений вида (2.17) порядка 2 с единственной особенностью в точке $z = 0$. Ниже в параграфе 2.6 (см. Теорему 2.4) мы докажем, что функции $f_j(z)$ алгебраически независимы над $\mathbb{C}(z)$. Воспользовавшись этим фактом, немедленно выводим утверждение Теоремы 2.2 из Теоремы 2.1.

Следствием Теоремы 2.2 является, например, трансцендентность непрерывной дроби

$$\xi = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \ddots}}.$$

Можно доказать, что $\xi = i\dfrac{K_0'(2i)}{K_0(2i)}$.

Следующая лемма показывает, что условие алгебраической независимости функций $f_j(z)$ в Теореме 2.1 необходимо для ее утверждения.

Лемма 5. *Пусть E-функции $f_1(z), \dots, f_m(z) \in \mathbb{A}[[z]]$ алгебраически зависимы над полем $\mathbb{C}(z)$. Тогда для любого $\alpha \in \mathbb{A}$ числа $f_1(\alpha), \dots, f_m(\alpha)$ алгебраически зависимы над $\mathbb{Q}$.*

Доказательство. Пусть $P = \sum a_{\overline{k}} z^{k_0} x_1^{k_1} \cdots x_m^{k_m} \in \mathbb{C}[z, x_1, \cdots, x_m]$ и выполняется равенство $P(z, f_1(z), \cdots, f_m(z)) = 0$. Так как $f_j \in \mathbb{A}[[z]]$, заключаем, что числа $a_{\overline{k}}$ удовлетворяют бесконечной системе линейных однородных алгебраических уравнений с коэффициентами в $\mathbb{A}$. Эта система имеет нетривиальное решение $b_{\overline{k}} \in \mathbb{A}$. Следовательно, существует нетривиальный многочлен $Q(z, x_1, \dots, x_m) = \sum b_{\overline{k}} z^{k_0} x_1^{k_1} \dots x_1^{k_m} \in \mathbb{A}[z, x_1, \dots, x_m]$ такой, что $Q(z, f_1(z)), \dots, f_m(z)) = 0$. Не уменьшая общности можно считать, что Q не имеет нетривиальных делителей из кольца $\mathbb{A}[z]$. Поэтому

$$R(x_1, \dots, x_m) = Q(\alpha, x_1, \dots, x_m) \neq 0, \text{но } R(f_1(\alpha), \dots, f_m(\alpha)) = 0.$$

Таким образом, числа $f_1(\alpha), \dots, f_m(\alpha)$ алгебраически зависимы над полем $\mathbb{A}$ и, следовательно, над $\mathbb{Q}$. $\square$

Можно проверить, что при $\lambda - \frac{1}{2} \in \mathbb{Z}$ функции $K_\lambda(z),\ K_\lambda'(z)$ алгебраически зависимы над $\mathbb{C}(z)$. Например, $K_{\frac{1}{2}}(z) = \cos z, K_{\frac{1}{2}}'(z) = -\sin z$. Так что условие $\lambda \neq \frac{1}{2} + k,\ k \in \mathbb{Z}$ необходимо для справедливости теоремы 2.2.

Проблема доказательства алгебраической независимости функций над $\mathbb{C}(z)$ есть чисто функциональная проблема. Её необходимо решать всякий раз применяя Теорему 2.1. Чаще всего она требует достаточно сложных рассуждений, но эта функциональная часть, как показывает лемма 2.4, абсолютно необходима для доказательства числовых результатов.

Мы приведем здесь без доказательства еще одно приложение теоремы 2.1, полученное в 1990г. В.Х.Салиховым. Основные трудности были связаны именно с исследованием алгебраической независимости соответствующих функций над $\mathbb{C}(z)$.

Теорема 3. *Пусть $p \geq 3$ - нечетное число и*

$$\varphi(z) = \sum_{n=0}^{\infty} \frac{1}{(\lambda_1 + 1)_n \cdots (\lambda_p + 1)_n} (\frac{z}{p})^{np},\ \lambda_i \in \mathbb{Q},\ \lambda_i \neq -1, -2, \dots.$$

Пусть также $\xi_1, \dots, \xi_m \in \mathbb{A}, \dfrac{\xi_i}{\xi_j} \notin \mathbb{Q}(\zeta)$, где $\zeta^p = 1$. При этих условиях числа

$$\varphi^{(i)}(\xi_j), \quad 0 \leq i \leq p-1, 1 \leq j \leq m$$

будут алгебраически зависимы над $\mathbb{Q}$, если и только если $p\lambda_j \in \mathbb{Z}, j = 1, \dots, p$, и, возможно после перестановки индексов, $p\lambda_j \equiv j(\mod p)$.

2.3.1 Линейная схема исключения переменных по Зигелю.

Зигель первым нашел, что можно доказывать линейную независимость каких-либо чисел $\omega_1, \dots, \omega_m$ не только с помощью совместных рациональных приближений к ним, как это делал Эрмит, но используя более общий подход, основанный на конструкции полного набора (число форм равно числу переменных) линейно независимых линейных форм с целыми или с целыми алгебраическими коэффициентами, достаточно малых в точке $\overline{\omega} = (\omega_1, \ldots, \omega_m)$. Общая схема его рассуждений излагается ниже.

Пусть формы

$$L_i = L_i(\overline{x}) = \sum_{j=0}^{m} a_{ij} x_j, \qquad i = 1, \ldots, m, \tag{2.10}$$

линейно независимы, $\max_{1 \le j \le m} |a_{ij}| \le H_i$. Тогда с $\Delta = \det \|a_{ij}\|$ и некоторыми числами Δ_{ik} (алгебраическими дополнениями к соответствующим элементам матрицы $\|a_{ik}\|$) справедливы тождества

$$\Delta x_i = \sum_{k=1}^{m} \Delta_{ik} L_k(\overline{x}). \tag{2.11}$$

Из них же, как легко проверить, для любой точки $\overline{\omega} = (\omega_1, \ldots, \omega_m) \in \mathbb{C}^m$ следует неравенство

$$\sum_{i=1}^{m} \frac{|L_i(\overline{\omega})|}{H_i} \ge c_0 \frac{|\Delta|}{H_1 \cdots H_m}, \tag{2.12}$$

где $c_0 = (m!)^{-1} \max_{1 \le j \le m} |\omega_j|$. Буквами c с нижними индексами и в дальнейшем будут обозначаться константы, зависящие только от m и чисел $\omega_1, \ldots, \omega_m$.

Мы будем работать с линейными формами, имеющими целые алгебраические коэффициенты. Пусть $\mathbf{K} \supset \mathbb{Q}$ алгебраическое расширение конечной степени $\nu = [\mathbf{K} : \mathbb{Q}], \mathbb{Z}_{\mathbf{K}}$ - кольцо целых чисел поля $\mathbf{K}$. Для каждого элемента $\alpha \in \mathbf{K}$, как и ранее, будем обозначать $\overline{|\alpha|}$ - максимум из модулей чисел, сопряженных с α. Тогда для любого $\alpha \in \mathbb{Z}_{\mathbf{K}}, \alpha \ne 0$, выполняется

$$|\alpha| \ge \overline{|\alpha|}^{1-\nu}.$$

Последнее неравенство, заменяющее собой фундаментальное свойство целых чисел - их дискретность, доказывается следующим образом:

$$1 \le |N(\alpha)| = |\alpha^{(1)} \cdots \alpha^{(\nu)}| \le |\alpha| \; \overline{|\alpha|}^{\nu-1}.$$

Для каждого многочлена $P(\overline{x}) \in \mathbb{Z}[x_1, \ldots, x_m]$ будем обозначать $\overline{|P|}$ - максимум модулей всех чисел, сопряженных с коэффициентами многочлена $P(\overline{x})$.

В основу доказательства линейной независимости чисел Зигель положил следующие соображения.

Предложение 1. *Пусть* $\mathbf{K} \supset \mathbb{Q}$ *- конечное расширение,* $\overline{\omega} = (\omega_1, \ldots, \omega_m)$ *- ненулевой набор комплексных чисел, среди которых имеется не более, чем* r *линейно независимых над* $\mathbf{K}$. *Существует положительная постоянная* c_1, *зависящая только от чисел* $m, \omega_1, \ldots, \omega_m$ *и степени* ν *расширения* $\mathbf{K} \supset \mathbb{Q}$ *такая, что для любой совокупности линейно независимых над* $\mathbf{K}$ *линейных форм (2.3.1) с условием* $a_{ij} \in \mathbb{Z}_{\mathbf{K}}$ *и любого действительного числа* H *с условием*

$$\overline{|L_i|} \le H, \quad i = 1, \ldots, m,$$

выполняются неравенства

$$\max_{1 \le i \le m} |L_i(\overline{\omega})| \ge c_1 H^{1 - r\nu}.$$

Лекция 4

Пусть формы

$$L_i = L_i(\overline{x}) = \sum_{j=0}^{m} a_{ij}x_j, \qquad i = 1, \ldots, m,$$

линейно независимы, $\max\limits_{1\le j\le m} |a_{ij}| \le H_i$. Тогда с $\Delta = \det \|a_{ij}\|$ и некоторыми числами Δ_{ik} (алгебраическими дополнениями к соответствующим элементам матрицы $\|a_{ik}\|$) справедливы тождества

$$\Delta x_i = \sum_{k=1}^{m} \Delta_{ik} L_k(\overline{x}).$$

Из них же, как легко проверить, для любой точки $\overline{\omega} = (\omega_1, \ldots, \omega_m) \in \mathbb{C}^m$ следует неравенство

$$\sum_{i=1}^{m} \frac{|L_i(\overline{\omega})|}{H_i} \ge c_0 \frac{|\Delta|}{H_1 \cdots H_m},$$

где $c_0 = (m!)^{-1} \max\limits_{1\le j\le m} |\omega_j|$. Буквами c с нижними индексами и в дальнейшем будут обозначаться константы, зависящие только от m и чисел $\omega_1, \ldots, \omega_m$.

Предложение 2. *Пусть $\mathbf{K} \supset \mathbb{Q}$ - конечное расширение, $\overline{\omega} = (\omega_1, \ldots, \omega_m)$ - ненулевой набор комплексных чисел, среди которых имеется не более, чем r линейно независимых над $\mathbf{K}$. Существует положительная постоянная c_1, зависящая только от чисел $m, \omega_1, \ldots, \omega_m$ и степени ν расширения $\mathbf{K} \supset \mathbb{Q}$ такая, что для любой совокупности линейно независимых над $\mathbf{K}$ линейных форм (2.3.1) с условием $a_{ij} \in \mathbb{Z}_{\mathbf{K}}$ и любого действительного числа H с условием*

$$\overline{|L_i|} \le H, \quad i = 1, \ldots, m,$$

выполняются неравенства

$$\max_{1\le i\le m} |L_i(\overline{\omega})| \ge c_1 H^{1-r\nu}.$$

Доказательство. Согласно условию Предложения 1 любые $r+1$ из чисел $\omega_1, \ldots, \omega_m$ линейно зависимы над полем $\mathbf{K}$. Поэтому существуют линейные формы

$$l_i(\overline{x}) = b_{i1}x_1 + \cdots + b_{im}x_m, \quad 1 \le i \le m - r, \qquad (2.13)$$
$$b_{ij} \in \mathbb{Z}_{\mathbf{K}}, \quad \max_{ij} \overline{|b_{ij}|} = h, \quad h \ge 1,$$

линейно независимые над $\mathbf{K}$ и такие, что $l_i(\overline{\omega}) = 0, i = 1, \ldots, m - r$. Применяя к формам (2.13) и подмножеству $L_{m-r+1}, \ldots, L_m$ форм (2.3.1), линейно независимых с $l_1, \ldots, l_{m-r}$ неравенство (2.3.1), получим

$$\sum_{i=m-r+1}^{m} |L_i(\overline{\omega})| \ge \frac{c_0}{h^{m-r}} H^{1-r} |\Delta|. \qquad (2.14)$$

Так как Δ - целое алгебраическое число, $\overline{|\Delta|} \le c_2 H^r$ и $\Delta \ne 0$, то $|\Delta| \ge c_3 H^{r(1-\nu)}$ и из (2.14) следует неравенство, утверждаемое Предложением 1.1. □

Допустим, что существует возрастающая последовательность натуральных чисел S, для каждого из которых удается построить систему линейно независимых линейных форм (2.3.1), $a_{ij} \in \mathbb{Z}_{\mathbf{K}}$, естественно зависящую от переменного номера S, так, чтобы выполнялись условия

$$\max_{i,j} \overline{|a_{ij}|} \le S, \quad |L_i(\overline{\omega})| = o(S^{1-d}), \quad 1 \le i \le m, \tag{2.15}$$

где $d > 0$.

Обозначим буквой r количество линейно независимых над $\mathbf{K}$ чисел среди $\omega_1, \ldots, \omega_m$. Согласно Предложению 1.1 это число удовлетворяет неравенству $1 - d \ge 1 - r\nu$ или

$$r \ge \frac{d}{\nu}.$$

В частности, при $\nu = 1$ и $d > m - 1$ отсюда следует линейная независимость чисел $\omega_1, \ldots, \omega_m$ над $\mathbb{Q}$.

Фактическое конструирование систем линейных форм $L_j(\overline{x})$ удается достаточно редко. Иногда удается доказать лишь существование соответствующих последовательностей линейных форм. Именно так в оригинальной работе Зигеля, [**?**], где и был предложен этот подход, проводилось исследование значений E-функций (см. далее гл.2).

2.4 Сведение доказательства Теоремы 1 к линейному случаю.

Основу доказательства Теоремы 1 составляет следующее утверждение.

Предложение 3 (Предложение 1.). *Пусть совокупность E-функций $f_1(z), \cdots, f_m(z)$ составляет решение системы дифференциальных уравнений*

$$y'_k = \sum_{j=1}^{m} q_{kj} y_j, \quad q_{kj} \in \mathbb{C}(z), \tag{2.16}$$

и линейно независима над $\mathbb{C}(z)$, α - любое алгебраическое число, отличное от нуля и особых точек системы (2.19), $\mathbf{K}$ - поле алгебраических чисел, содержащее α и коэффициенты разложений в ряд Тейлора (2.1) всех функций $f_i(z)$, $\nu = [\mathbf{K} : \mathbb{Q}] < \infty$. Тогда для любого $\varepsilon, 0 < \epsilon < 1$ и всех достаточно больших натуральных чисел n существуют линейно независимые формы

$$L_i = \sum_{j=1}^{m} a_{ij} x_j, \quad a_{ij} \in \mathbb{Z}_{\mathbf{K}},\ 1 \le i, j \le m,$$

такие, что

$$\overline{|\ a_{ij}\ |} \le n^{(1+\varepsilon)n}, \quad |\ L_i(f_1(\alpha), \ldots, f_m(\alpha))\ | \le n^{-(m-1-\varepsilon)n}.$$

Из Предложения 1 непосредственно получается аналог Теоремы 5.

Следствие 1 (Следствие 1.). *В условиях Предложения 1 среди чисел*

$$f_1(\alpha), \ldots, f_m(\alpha)$$

имеется не менее чем $\dfrac{m}{\nu}$ линейно независимых над $\mathbf{K}$.

Вывод Следствия 1. Для доказательства Следствия 1 воспользуемся Предложением 1. Выберем для этого для этого произвольное число ε и определим числа S и d равенствами

$$S = n^{(1+\varepsilon)n}, \qquad d + \varepsilon = \frac{m}{1+\varepsilon}.$$

Тогда

$$n^{-(m-1-\varepsilon)n} = S^{-\frac{m-1-\varepsilon}{1+\varepsilon}} = S^{1-d-\varepsilon} = o(S^{1-d}).$$

Применим это предложение к линейным формам, построенным в Предложении 1. Обозначим также r - максимальное количество линейно независимых над $\mathbf{K}$ среди чисел $f_i(\alpha)$. Тогда справедливы неравенства

$$r \geq \frac{d}{\nu} = \frac{1}{\nu}\left(\frac{m}{1+\varepsilon} - \varepsilon\right).$$

Устремляя в последнем неравенстве ε к нулю справа и пользуясь тем, что числа m, ν, r не зависят от ε, находим $r \geq \frac{m}{\nu}$. $\square$

Зигель предположил, что для E-функций должен быть справедлив не только аналог Теоремы 5 главы 1, но и утверждение подобное Теореме 3. Следствие 1 означает его справедливость при $\nu = 1$ т.е. в случае $\mathbf{K} = \mathbb{Q}$. Кроме того, аналог Теоремы 3 может быть доказан и в случае, когда $\mathbf{K}$ - мнимое квадратичное поле. Общий случай сравнительно недавно был доказан Ф. Бейкерсом, 2006.

Конец четвёртой лекции.

Лекция 5.

Теорема 4 (Теорема 1. А.Б. Шидловский, 1955г.)**.** *Пусть E-функции $f_1(z), \ldots, f_m(z)$ составляют решение системы линейных дифференциальных уравнений*

$$y_k' = q_{k0} + \sum_{j=1}^{m} q_{kj} y_j, \quad q_{kj} \in \mathbb{C}(z), \tag{2.17}$$

и алгебраически независимы над полем рациональнх функций $\mathbb{C}(z)$. Тогда для любого алгебраического числа α, отличного от нуля и особых точек системы (2.17), значения

$$f_1(\alpha), \ldots, f_m(\alpha)$$

алгебраически независимы над $\mathbb{Q}$.

Основу доказательства Теоремы 1 составляет следующее утверждение.

Предложение 4 (Предложение 1.)**.** *Пусть совокупность E-функций $f_1(z), \cdots, f_m(z)$ составляет решение системы дифференциальных уравнений*

$$y_k' = \sum_{j=1}^{m} q_{kj} y_j, \quad q_{kj} \in \mathbb{C}(z), \tag{2.18}$$

и линейно независима над $\mathbb{C}(z)$, α - любое алгебраическое число, отличное от нуля и особых точек системы (2.19), $\mathbf{K}$ - поле алгебраических чисел, содержащее α и коэффициенты разложений в ряд Тейлора (2.1) всех функций $f_i(z)$, $\nu = [\mathbf{K} : \mathbb{Q}] < \infty$. Тогда для любого $\varepsilon, 0 < \epsilon < 1$ и всех достаточно больших натуральных чисел n существуют линейно независимые формы

$$L_i = \sum_{j=1}^{m} a_{ij} x_j, \quad a_{ij} \in \mathbb{Z}_{\mathbf{K}}, \ 1 \leq i, j \leq m,$$

такие, что

$$\overline{| \, a_{ij} \, |} \leq n^{(1+\varepsilon)n}, \quad | \, L_i(f_1(\alpha), \ldots, f_m(\alpha)) \, | \leq n^{-(m-1-\varepsilon)n}.$$

Из Предложения 1 непосредственно получается аналог Теоремы 5.

Следствие 2 (Следствие 1.)**.** *Пусть совокупность E-функций $f_1(z), \cdots, f_m(z)$ составляет решение системы дифференциальных уравнений*

$$y_k' = \sum_{j=1}^{m} q_{kj} y_j, \quad q_{kj} \in \mathbb{C}(z), \tag{2.19}$$

и линейно независима над $\mathbb{C}(z)$, α - любое алгебраическое число, отличное от нуля и особых точек системы (2.19), $\mathbf{K}$ - поле алгебраических чисел, содержащее α и коэффициенты разложений в ряд Тейлора (2.1) всех функций $f_i(z)$, $\nu = [\mathbf{K} : \mathbb{Q}] < \infty$. Тогда среди чисел

$$f_1(\alpha), \ldots, f_m(\alpha)$$

имеется не менее чем $\dfrac{m}{\nu}$ линейно независимых над $\mathbf{K}$.

Доказательство Теоремы 1. Предположим, что выполнены условия Теоремы 1. Выберем достаточно большое натуральное число N и рассмотрим следующие функции

$$F_{\overline{k}}(z) = f_1^{k_1}(z)\cdots f_m^{k_m}(z), \quad k_i \geq 0,\ k_1+\ldots+k_m \leq N. \tag{2.20}$$

Линейное пространство над $\mathbf{K}$, порожденное числами $F_{\overline{k}}(\alpha)$ обозначим буквой $\mathfrak{L}$.

Количество функций $F_{\overline{k}}(z)$ равно $\begin{pmatrix} N+m \\ m \end{pmatrix}$. Заметим, что в силу (2.17) функции (2.20) составляют решение системы линейных однородных дифференциальных уравнений, особые точки которой совпадают с особыми точками системы (2.17). Из алгебраической независимости функций $f_i(z)$ над $\mathbb{C}(z)$ следует линейная независимость $F_{\overline{k}}(z)$. Поскольку E-функции образуют кольцо (Лемма 2.1), то все произведения (2.20) принадлежат к классу E-функций. Применяя к ним Следствие 2.1, заключаем, что

$$\dim\mathfrak{L} \geq \frac{1}{\nu}\begin{pmatrix} N+m \\ m \end{pmatrix} = \frac{1}{\nu m!}N^m + O(N^{m-1}) \tag{2.21}$$

Если числа $f_1(\alpha),\ldots,f_m(\alpha_m)$ алгебраически зависимы над $\mathbf{K}$, то существует ненулевой многочлен $P\in\mathbf{K}[x_1,\ldots,x_m]$ с $d=\deg P$ такой, что $P(f_1(\alpha),\ldots,f_m(\alpha))=0$. Многочлены

$$Q_{\overline{\ell}} = x_1^{\ell_1}\ldots x_m^{\ell_m}P(x_1,\ldots,x_m), \quad \ell_i\geq 0,\ \ell_1+\ldots+\ell_m\leq N-d, \tag{2.22}$$

рассматриваемые как линейные формы от произведений степеней

$$x_1^{k_1}\cdots x_m^{k_m}, \quad k_i\geq 0, \quad k_1+\ldots+k_m\leq N,$$

линейно независимы, и обращаются в нуль при подстановке $x_i=f_i(\alpha)$. Так как количество многочленов $Q_{\overline{\ell}}$ равно $\binom{N-d+m}{m}$, то

$$\dim\mathfrak{L} \leq \begin{pmatrix} N+m \\ m \end{pmatrix} - \begin{pmatrix} N-d+m \\ m \end{pmatrix} = O(N^{m-1}),$$

но это противоречит неравенству (2.21). Получившееся противоречие завершает вывод Теоремы 2.1 из Следствия 2.1. □

2.5 Линейные неравенства и уравнения.

Технические утверждения этого параграфа необходимы для построения линейных форм, о которых идет речь в Предложении 2.1. Они неоднократно будут использоваться и в дальнейшем.

Доказательство следующей леммы основано на "принципе ящиков"Дирихле.

Лемма 6. *Пусть задана совокупность линейных форм*

$$M_i(\overline{x}) = \sum_{j=1}^{n} a_{ij}x_j, \quad 1\leq i\leq m,$$

с действительными коэффициентами a_{ij}, причем $n>m$. Если A и B действительные числа, удовлетворяющие неравенствам

$$A \geq \max_{ij} \mid a_{ij} \mid, \quad B\geq 1, \quad A\geq 1,$$

то существует ненулевой вектор $\overline{x}_0 = (x_{01}, \ldots, x_{0n}) \in \mathbb{Z}^n$, *удовлетворяющий неравенствам*

$$| M_i(\overline{x}_0) |< \frac{1}{B}, \quad 1 \le i \le m,$$
$$| x_{0,j} |\le (nAB)^{\frac{m}{n-m}} \quad 1 \le j \le n.$$

Доказательство. Положим

$$X = \left[(nAB)^{\frac{m}{n-m}}\right]$$

и

$$C = \{\overline{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n \mid \quad 0 \le x_j \le X\}.$$

Рассмотрим отображение

$$\varphi : \mathbb{R}^n \longrightarrow \mathbb{R}^m,$$

переводящее вектор $\overline{x} = (x_1, \ldots, x_n)$ в вектор $(M_1(\overline{x}), \ldots, M_m(\overline{x}))$.

Если обозначить

$$U_i = \sum_{j: a_{ij} \ge 0} a_{ij}, \quad V_i = -\sum_{j: a_{ij} < 0} a_{ij},$$

то легко видеть, что

$$U_i + V_i \le nA, \tag{2.23}$$

а для каждого вектора $\overline{x} \in C$ выполняются неравенства

$$-XV_i \le M_i(\overline{x}) \le XU_i, \quad 1 \le i \le m. \tag{2.24}$$

Рассмотрим параллелепипед $C' \subset \mathbb{R}^m$, определенный неравенствами

$$C' = \{\overline{y} = (y_1, \ldots, y_m) \mid -XV_i \le y_i \le XU_i, 1 \le i \le m\}.$$

Неравенства (2.24) означают, что $\varphi(C) \subset C'$.

Разделим каждую сторону параллелепипеда C' на $T = 1 + [nABX]$ равных отрезков. Тогда C' разделится на T^m равных параллелепипедов ("ящиков"). Параметры X и T выбраны так, что справедливы неравенства

$$T \le 1 + nABX \le nAB(1 + X) < (1 + X)^{\frac{n}{m}}$$

или

$$(1 + X)^n > T^m.$$

Это неравенство означает, что количество точек в множестве C ("предметов") больше, чем количество "ящиков и, следовательно, найдутся две различные точки $\overline{x}' = (x'_1, \ldots, x'_n)$, $\overline{x}'' = (x''_1, \ldots, x''_n) \in C$, образы которых принадлежат одному и тому же малому параллелепипеду.

В силу определения C' и неравенства (2.23) длины всех ребер малых параллелепипедов не превосходят

$$\frac{nAX}{T} < \frac{nAX}{nABX} = \frac{1}{B},$$

принадлежность точек $\varphi(\overline{x}')$ и $\varphi(\overline{x}'')$ одному малому параллелепипеду влечет выполнимость неравенств

$$|M_i(\overline{x}') - M_i(\overline{x}'')| < \frac{1}{B}, \quad 1 \le i \le m. \tag{2.25}$$

Обозначив теперь $\overline{x}_0 = \overline{x}' - \overline{x}''$, получим

$$|x_{0j}| = |x'_j - x''_j| \leq X \leq (nAB)^{\frac{m}{n-m}}$$

и, в силу линейности форм M_i и (2.25),

$$|M_i(\overline{x}_0)| = |M_i(\overline{x}') - M_i(\overline{x}'')| < \frac{1}{B}.$$

Существование вектора $\overline{x}_0$ с требуемыми свойствами доказано. $\square$

Следствие 3. *Пусть задана совокупность линейных форм*

$$M_i(\overline{x}) = \sum_{j=1}^{n} a_{ij}x_j, \quad 1 \leq i \leq m,$$

с целыми коэффициентами a_{ij}, причем $n > m$. Если $A \geq 1$ действительное число, удовлетворяющее неравенствам

$$\max_{ij} \mid a_{ij} \mid \leq A,$$

то система уравнений

$$M_i(\overline{x}) = 0, \quad 1 \leq i \leq m,$$

имеет ненулевое решение $\overline{x}_0 = (x_{01}, \ldots, x_{0n}) \in \mathbb{Z}^n$, удовлетворяющее неравенствам

$$\mid x_{0,j} \mid \leq (nA)^{\frac{m}{n-m}} \quad 1 \leq j \leq n.$$

Доказательство. Применим к линейным формам $M_i(\overline{x})$ Лемму 2.5 с $B = 1$. Пусть $\overline{x}_0$ - целый вектор, существование которого следует из Леммы 2.5. Так как коэффициенты линейных форм есть целые числа, то $M_i(\overline{x}_0) \in \mathbb{Z}$ и неравенства $|M_i(\overline{x}_0)| < 1$, выполняющиеся согласно Лемме 2.5 означают, что вектор $\overline{x}_0$ есть решение системы уравнений, заданной в следствии. $\square$

Теперь мы обобщим Следствие 2.5 на системы линейных уравнений с алгебраическими коэффициентами.

Лемма 7. *Пусть $\mathbf{K}$ - поле алгебраических чисел, $\nu = [\mathbf{K} : \mathbb{Q}] < \infty$. Пусть также задана совокупность линейных форм*

$$M_i(\overline{x}) = \sum_{j=1}^{n} \alpha_{ij}x_j, \quad 1 \leq i \leq m,$$

с коэффициентами $\alpha_{ij} \in \mathbb{Z}_{\mathbf{K}}$, причем $n > m$. Если $A \geq 1$ действительное число, удовлетворяющее неравенствам

$$\max_{ij} \overline{\mid \alpha_{ij} \mid} \leq A,$$

то система уравнений

$$M_i(\overline{x}) = 0, \quad 1 \leq i \leq m,$$

имеет ненулевое решение $\overline{x}_0 = (x_{01}, \ldots, x_{0n}) \in \mathbb{Z}^n_{\mathbf{K}}$, удовлетворяющее неравенствам

$$\overline{\mid x_{0,j} \mid} \leq c_1(c_1 nA)^{\frac{m}{n-m}} \quad 1 \leq j \leq n,$$

где c_1 - некоторая положительная постоянная, зависящая только от поля $\mathbf{K}$.

Доказательство. Пусть $\{\xi_1, \dots, \xi_\nu\}$ - фиксированный фундаментальный базис кольца $\mathbb{Z}_{\mathbf{K}}$ и $\{\xi'_1, \dots, \xi'_\nu\}$ - дуальный базис поля $\mathbf{K}$. Мы воспользуемся функцией след Tr на поле $\mathbf{K}$. Эта $\mathbb{Q}$ линейная функция на поле $\mathbf{K}$ со значениями в $\mathbb{Q}$ обладает следующими свойствами

- справедливы равенства
$$\mathrm{Tr}(\xi_i\xi'_j) = \begin{cases} 1, & \text{если } i = j, \\ 0, & \text{если } i \neq j, \end{cases}$$

- для каждого элемента $\alpha \in \mathbb{Z}_{\mathbf{K}}$ имеем $\mathrm{Tr}(\xi'_s\alpha) \in \mathbb{Z},\ s = 1, \dots, \nu,$

- если $\alpha \in \mathbf{K}$ и
$$\mathrm{Tr}(\xi_s\alpha) = 0, \quad s = 1, \dots, \nu,$$
то $\alpha = 0$.

Рассмотрим теперь систему уравнений

$$\sum_{j=1}^{n}\sum_{k=1}^{\nu} \mathrm{Tr}(\xi'_s\alpha_{ij}\xi_k)x_{jk} = 0, \tag{2.26}$$
$$i = 1, \dots, m, \quad s = 1, \dots, \nu.$$

Коэффициенты этой системы есть целые числа, удовлетворяющие, как легко видеть, неравенствам
$$|\mathrm{Tr}(\xi'_s\alpha_{ij}\xi_k)| \leq c_2A,$$
где $c_2 = \nu \max\limits_s \overline{|\xi'_s|} \max\limits_k \overline{|\xi_k|}$ - константа, зависящая от поля $\mathbf{K}$. Система уравнений (2.26) удовлетворяет условиям Следствия 2.2. Согласно этому следствию существует нетривиальный набор целых чисел u_{ij}, удовлетворяющий системе уравнений (2.26) и такой, что

$$|u_{ij}| \leq (n\nu c_2 A)^{\frac{m}{n-m}}.$$

Определим теперь вектор $\overline{x}_0 = (x_{01}, \dots, x_{0\nu})$ равенствами

$$x_{0j} = \sum_{k=1}^{\nu} u_{jk}\xi_k \in \mathbb{Z}_{\mathbf{K}}.$$

Тогда
$$\overline{|x_{0j}|} \leq c_3(n\nu c_2 A)^{\frac{m}{n-m}},$$
и для каждого $s = 1, \dots, \nu$ справедливы равенства

$$\mathrm{Tr}(\xi'_s M_i(\overline{x}_0)) = \sum_{j=1}^{n}\sum_{k=1}^{\nu} \mathrm{Tr}(\xi'_s\alpha_{ij}\xi_k)u_{jk} = 0,$$

означающие, что $M_i(\overline{x}_0) = 0,\ i = 1, \dots, m$. Это завершает доказательство леммы. □

Конец пятой лекции