Об алгебраической независимости значений показательной функции

Н. Г. Чудаков

В этой работе дается новый вариант доказательства известной теоремы Линдемана об алгебраической независимости значений показательной функции.

Теорема. *Пусть система алгебраических чисел* $\alpha_1, \ldots, \alpha_l$ *линейно независима по отношению к полю рациональных чисел;* $f(x_1, x_2, \ldots, x_l)$ *любой многочлен с алгебраическими коэфициентами, среди которых не все равны* 0. Тогда

$$f(e^{\alpha_1}, \ldots, e^{\alpha_l}) \neq 0.$$

Историю вопроса см. Гельфонд [1]. Доказательство этой теоремы в моей статье базируется на теории матриц и использует некоторые идеи Т. Сколема [2].

Хотя в этой статье доказательство изложено только для поля комплексных чисел, однако развитый здесь метод допускает широкое обобщение для полей весьма общего класса. Такое обобщение будет сделано в другом месте.

Пусть дано любое коммутативное поле K характеристики 0 и в нем подполе $k \subset \Delta \subset K$, причем Δ пусть является конечным нормальным расширением k (в частности $\Delta = k$). Степ ${}_k\Delta = n$, ϑ примитивный элемент Δ, т. е. $\Delta = k(\vartheta)$; $\vartheta = \vartheta_1, \vartheta_2, \ldots, \vartheta_n$ элементы, сопряженные с ϑ относительно k.

Автоморфизм поля Δ, переводящий ϑ_1 в ϑ_i, будем обозначать символом T_i.

Кольцо многочленов m неизвестных $x_1, x_2 \ldots x_m$ над полем Δ будем обозначать символом $\Delta[x_1, \ldots, x_m]$. Мы будем говорить, что над кольцом $\Delta[x_1, \ldots, x_m]$ выполнен автоморфизм T_i, если коэфициенты каждого многочлена в этом кольце заменены соответственно их образами, даваемыми автоморфизмом T_i.

Элементы $\alpha_1, \ldots, \alpha_m$ поля K назовем алгебраически связанными над полем Δ, если существует в кольце $\Delta[x_1, \ldots, x_m]$ такой многочлен $\varphi(x_1, \ldots, x_m)$, что $\varphi(x_1, \ldots, x_m) \not\equiv 0$ и $\varphi(\alpha_1, \ldots, \alpha_m) = 0$.

Очевидно, что степень φ относительно одного из неизвестных x не равна 0, т. е. $\frac{\partial \varphi}{\partial x_i} \not\equiv 0$. Ясно также, что, не нарушая алгебраической связности системы $\alpha_1, \ldots, \alpha_m$, можно в этой системе элемент α_j, для которого $\frac{\partial \varphi}{\partial x_j} \equiv 0$, заменить любым элементом поля K.

Лемма 1. *Система $\alpha_1, \ldots, \alpha_m$ тогда и только тогда алгебраически связана над Δ, когда для любого целого ν система $\alpha_1^\nu, \ldots, \alpha_m^\nu$ алгебраически связана над k.*

Доказательство. Доказательство требуется только для одной половины этого утверждения, так как достаточность указанного условия очевидна.

Пусть, сначала, $\frac{\partial \varphi}{\partial x_1} \equiv 0$. Тогда в нашей системе элемент α_1 можно будет заменить элементом α_1^ν, т. е. система $\alpha_1^\nu, \alpha_2, \ldots, \alpha_m$ будет алгебраически связанной над Δ. Пусть теперь $\frac{\partial \varphi}{\partial x_1} \not\equiv 0$. В таком случае, присоединяя к полю $\Delta' = \Delta(\alpha_2, \ldots, \alpha_m)$ элемент α_1 мы получим поле $\Delta'' = \Delta'(\alpha_1)$, которое является конечным расширением Δ'.

Но полю Δ'' принадлежит и элемент α_1^ν. Следовательно, существует такой многочлен $\Phi(x) \in \Delta'[x]$, что $\Phi(\alpha_1^\nu) = 0$ и $\Phi(x) \not\equiv 0$.

Каждый коэфициент $\Phi(x)$ есть рациональная функция от элементов $\alpha_2, \ldots, \alpha_m$ с коэфициентами из поля Δ. Умножая $\Phi(x)$ на общего знаменателя всех этих рациональных функций, мы получим многочлен $\varphi_1(x_1, \ldots, x_m) \not\equiv 0$; $\varphi_1 \in \Delta[x_1, \ldots, x_m]$ и $\varphi_1(\alpha_1^\nu, \alpha_2, \ldots, \alpha_m) = 0$. Следовательно, система $\alpha_1^\nu, \alpha_2, \ldots, \alpha_m$ алгебраически связана над Δ.

Беря теперь эту систему $\alpha_1^\nu, \alpha_2, \ldots, \alpha_m$ за исходную и повторяя с ней и с элементом α_2 рассуждения, аналогичные тем, которые мы проводили выше, мы убедимся в том, что и система $\alpha_1^\nu, \alpha_2^\nu, \alpha_3, \ldots, \alpha_m$ алгебраически связана. После m-кратного применения описанных рассуждений мы убедимся и в алгебраической связанности системы $\alpha_1^\nu, \alpha_2^\nu, \ldots, \alpha_m^\nu$. Следовательно, существует многочлен $\varphi_2(x_1, \ldots, x_m)$, принадлежащий $\Delta[x_1, \ldots, x_m]$ и такой, что $\varphi_2(\alpha_1^\nu, \ldots, \alpha_m^\nu) = 0$, причем $\varphi_2 \not\equiv 0$.

Произведем теперь над кольцом $\Delta[x_1, \ldots, x_m]$ все автоморфизмы $T_i (i = 1, \ldots, n)$; многочлен φ_2 перейдет последовательно в сопряженные многочлены $\varphi_{2,i}$ $(i = 1, \ldots, n)$ (мы полагаем $\varphi_2 = \varphi_{2,1}$). Тогда, как известно, многочлен

$$\varphi_3(x_1, \ldots, x_m) = \prod_{i=1}^{n} \varphi_{2,i}(x_1, \ldots, x_m)$$

принадлежит уже кольцу $k[x_1, \ldots, x_m]$. Кроме того, $\varphi_3 \not\equiv 0$ и $\varphi_3(\alpha_1^\nu, \alpha_2^\nu, \ldots, \alpha_m^\nu) = 0$. Следовательно, система $\alpha_1^\nu, \alpha_2^\nu, \ldots, \alpha_m^\nu$ алгебраически связана над k.

Пусть теперь K поле комплексных чисел, а $k = \Gamma$, т. е. поле рациональных чисел; тогда Δ нормальное поле над Γ. Выберем в Δ какой-

либо произвольный базис $\omega_{11}, \omega_{12}, \ldots, \omega_{1n}$, который в дальнейшем фиксируем как базис, соответствующий числу ϑ_1.

Автоморфизмом T_i этот базис преобразуется в новый базис $\omega_{i1}, \omega_{i2}, \ldots, \omega_{in}$. Это преобразование можно записать в матричной форме

$$\overline{\omega}_i = \mathfrak{A}_i \overline{\omega}_1,$$

где вектор $\overline{\omega}_i = (\omega_{i1}, \ldots, \omega_{in})$ $(i = 1, 2, \ldots, n)$, а матрица $\mathfrak{A}_i$, как известно, имеет в качестве своих элементов целые рациональные числа, причем определитель $|\mathfrak{A}_i| = \pm 1$.

Нетрудно видеть, что система матриц $\mathfrak{A}_i$ $(i = 1, \ldots, n)$ образует группу. Прежде всего ясно, что эта система составляет подмножество всех неособых матриц порядка n над кольцом целых рациональных чисел.

Далее пусть $\overline{\alpha}$ и $\overline{\beta}$ два вектора над полем Δ и пусть

$$\overline{\beta} = \mathfrak{A}\overline{\alpha},$$

где $\mathfrak{A}$ целочисленная матрица (т. е. все ее элементы целые рациональные числа). Поэтому, если над полем Δ осуществлен какой-либо из его автоморфизмов, то это последнее равенство преобразуется в новое: $\overline{\beta}' = \mathfrak{A}\overline{\alpha}'$, где $\overline{\alpha}'$ и $\overline{\beta}'$ векторы-образы $\overline{\alpha}$ и $\overline{\beta}$ при данном автоморфизме.

Поэтому $\mathfrak{A}_i \overline{\omega}_j = \overline{\omega}_t$, ибо любой автоморфизм преобразует один базис в другой. Следовательно, $\mathfrak{A}_i \mathfrak{A}_j \overline{\omega}_1 = \mathfrak{A}_t \overline{\omega}_1$, т. е. $\mathfrak{A}_i \mathfrak{A}_j = \mathfrak{A}_t$, ибо компоненты $\overline{\omega}_1$ линейно независимы по отношению к полю Γ. Таким образом, система $\mathfrak{A}_i$ $(i = 1, \ldots, n)$ замкнута по отношению к операции умножения. Следовательно, наша система является группой. Эта группа изоморфна группе Галуа поля Δ.

Лемма 2. *Пусть многочлен* $\varphi(x_1, \ldots, x_m) \not\equiv 0$ и $\varphi \in \Gamma[x_1, \ldots, x_m]$. Этому многочлену можно найти в нашем кольце такой соответствующий многочлен $\Phi(x_1, \ldots, x_m)$, который обладает следующими свойствами:

$$\varphi | \Phi;\ \Phi \not\equiv 0;\ \Phi(e^{\omega_{i1}}, \ldots, e^{\omega_{in}}) = \Phi(e^{\omega_{11}}, \ldots, e^{\omega_{1n}}) \quad (i = 1, \ldots, n).$$

Если все коэфициенты φ целые числа, то и Φ имеет также целые коэфициенты.

Доказательство. Ради сокращения запишем многочлен φ в векторной форме:

$$\varphi(\overline{x}) = \sum_{\overline{a}} A(\overline{a}) \{\overline{x}, \overline{a}\},$$

где $\overline{x} = (x_1, \ldots, x_m)$; $\overline{a} = (a_1, a_2, \ldots, a_m)$; $A(\overline{a})$ — рациональные числа, $\{\overline{x}, \overline{a}\} = x_1^{a_1} x_2^{a_2} \ldots x_m^{a_m}$, вектор $\overline{a}$ пробегает конечное число различных значений, причем компоненты $\overline{a}$ суть неотрицательные целые числа.

Полагаем теперь

$$\Phi(\overline{x}) = \prod_{j=1}^{n} \sum_{\overline{a}} A(\overline{a}) \{\overline{x}, \overline{a}\, \mathfrak{A}_j\} = \sum_{\overline{b}} \overline{B}(b) \{\overline{x}, \overline{b}\}.$$

Нетрудно видеть, что $\Phi(\bar{x})$ искомый многочлен. Прежде всего заметим, что так как все определители $|\mathfrak{A}_j| = \pm 1$, то равенство $\bar{a}'\mathfrak{A}_j = \bar{a}\mathfrak{A}_j$ тогда и только тогда имеет место, когда $\bar{a}' = \bar{a}$. Значит $\Phi(\bar{x})$ равно произведению многочленов, которые не обращаются тождественно в 0, т. е. $\Phi \not\equiv 0$. Далее очевидно, что $\varphi | \Phi$. Наконец, имеем

$$\Phi(e^{\omega_{i1}}, \ldots, e^{\omega_{in}}) = \prod_{i=1}^{n} \sum_{\bar{a}} A(\bar{a}) e^{\bar{a}\mathfrak{A}_j\bar{\omega}_i} =$$

$$= \prod_{i=1}^{n} \sum_{\bar{a}} A(\bar{a}) e^{\bar{a}\mathfrak{A}_j\mathfrak{A}_i\bar{\omega}_1} = \prod_{t=1}^{n} \sum_{\bar{a}} A(\bar{a}) e^{\bar{a}\mathfrak{A}_t\bar{\omega}_1} = \Phi(e^{\omega_{11}}, \ldots, e^{\omega_{1n}}),$$

ибо произведение $\mathfrak{A}_t = \mathfrak{A}_j\mathfrak{A}_i$ пробегает всю группу наших матриц вместе с $\mathfrak{A}_j$.

Переходим теперь к доказательству основной теоремы. Допустим, что она неверна. Тогда система чисел $e^{\alpha_1}, \ldots, e^{\alpha_t}$ будет удовлетворять уравнению $\psi(e^{\alpha_1}, \ldots, e^{\alpha_t})$, где ψ многочлен с алгебраическими коэфициентами, причем $\psi \not\equiv 0$. Пусть Δ' наименьшее нормальное расширение Γ, содержащее все числа $\alpha_1, \ldots, \alpha_t$ и все коэфициенты ψ. Очевидно, что система $e^{\alpha_1}, \ldots, e^{\alpha_t}$ алгебраически связана над Δ'. Пусть, далее ν общий знаменатель чисел $\alpha_1, \ldots, \alpha_t$. Тогда в силу леммы 1 система $e^{\nu\alpha_1}, \ldots, e^{\nu\alpha_t}$ алгебраически связана над Γ, причем все числа $\nu\alpha_i$ целые числа.

Таким образом, мы свели нашу задачу к тому случаю, когда ψ имеет целые рациональные коэфициенты, а все показатели α_i целые числа. Этот случай мы и будем рассматривать в дальнейшем. Все определения, которые были введены в начале статьи, будут теперь относиться к нормальному полю Δ, определенному через показатели α_i, т. е Δ — нормальное расширение $\Gamma(\alpha_1 \ldots \alpha_t)$.

Так как числа $\alpha_1, \ldots, \alpha_t$ линейно независимы по отношению к Γ, то $t \leqslant n$ и в матричном уравнении

$$\bar{\alpha} = \mathfrak{B}\bar{\omega}_1,$$

где $\bar{\alpha} = (\alpha_1, \ldots, \alpha_t)$, матрица $\mathfrak{B}$ имеет ранг равный t и все элементы $\mathfrak{B}$ целые рациональные числа. Поэтому

$$0 = \psi(e^{\alpha_1}, \ldots, e^{\alpha_t}) = \sum_{\bar{k}} A(\bar{k}) e^{\bar{k}\bar{\alpha}} = \sum_{\bar{k}} A(\bar{k}) \cdot e^{\bar{k}\mathfrak{B}\bar{\omega}_1} = \sum_{\bar{l}} A(\bar{l}) e^{\bar{l}\bar{\omega}_1},$$

где положено: $\bar{k} = (k_1, \ldots, k_t)$; $\bar{l} = (l_1, \ldots, l_n)$; $\bar{k}\mathfrak{B} = \bar{l}$. Не трудно видеть, что среди векторов $\bar{l}$ нет равных, ибо в противном случае мы имели бы равенство $\bar{k}'\mathfrak{B} = \bar{k}\mathfrak{B}$ при $\bar{k}' \neq \bar{k}$, что невозможно, так как ранг $\mathfrak{B} = t$, т. е. наивысший из возможных. Пусть теперь натуральное число l_0 так велико, что векторы $\bar{a} = \bar{l} + \bar{l}_0$, где $\bar{l} = (l_0, \ldots, l_0)$, имеют неотрицательные компоненты для любого из наших $\bar{l}$.

Определим теперь многочлен $\varphi(x_1, \ldots, x_n)$ равенством

$$\varphi = \sum_{\bar{a}}' A(\bar{a}) \{\bar{x}, \bar{a}\} = \{\bar{x}, \bar{l}_0\} \sum_{\bar{l}} A(\bar{l}) \{\bar{x}, \bar{l}\}.$$

Очевидно, что $\varphi \not\equiv 0$ и $\varphi(e^{\alpha_1}, \ldots, e^{\alpha_l}) = 0$. К многочлену φ применим лемму 2, которая обнаружит существование другого многочлена $\Phi(x_1, \ldots, x_n)$, обладающего следующими свойствами:

$$\Phi(e^{\omega_{i1}}, e^{\omega_{i2}}, \ldots, e^{\omega_{in}}) = \sum_{\bar{b}} B(\bar{b})\, e^{\varrho_i} = 0 \qquad (i = 1 \ldots n), \tag{1}$$

где положено

$$\Phi(x_1, \ldots, x_n) = \sum_{\bar{b}} B(\bar{b})\, \{\bar{x}, \bar{b}\};$$

$$\varrho_i = \overline{\omega}_i \bar{b} \qquad (i = 1 \ldots n).$$

Все коэфициенты $B(\bar{b})$ целые рациональные числа. Так как $\Phi \not\equiv 0$, то существует $B(\bar{b}_0) \neq 0$.

Пусть, теперь

$$f(x) = \sum_{m=0}^{s} \alpha_m x^m$$

любой многочлен, принадлежащий кольцу $\Delta[x]$. Если над этим кольцом осуществить автоморфизм T_i, то $f(x)$ перейдет в многочлен

$$f_i(x) = \sum_{m=0}^{s} \alpha_{i,m} x^m,$$

где положено $\alpha_m = \alpha_{1,m}$; $f(x) = f_1(x)$.

Полагаем, далее,

$$F_i(x) = \sum_{m=0}^{s} f_i^{(m)}(x);$$

ясно, что все $F_i(x)$ сопряжены друг другу по отношению к полю Γ.

С другой стороны, известно [3], что для любого комплексного x имеет место оценка

$$|F_i(0)\, e^x - F_i(x)| \leqslant e^{|x|} \sum_{m=0}^{s} |\alpha_{i,m}|\, |x|^m.$$

Следовательно, принимая во внимание (1), имеем

$$\left| \sum_{\bar{b}} B(\bar{b})\, F_i(\varrho_i) \right| \leqslant \sum_{\bar{b}} |B(\bar{b})|\, |F_i(0)\, e^{\varrho_i} - F_i(\varrho_i)| \leqslant$$

$$\leqslant \sum_{\bar{b}} |B(\bar{b})|\, e^{|\varrho_i|} \sum_{m=0}^{s} |\alpha_{i,m}|\, |\varrho_i|^m \leqslant h c_1^s,$$

где $h = \max |\alpha_{i,m}|$ $(i = 1, \ldots, n;\ m = 0, 1, \ldots, s)$; $\varrho_0 = \max(|\varrho_i|, 1)$ для всех значений i и $\bar{b}$;

$$c_1 = e^{1+\varrho_0} \varrho_0 \sum_{\bar{b}} |B(\bar{b})|.$$

Так как все числа $\sum_{\bar{b}} B(\bar{b}) F_i(\varrho_i)$ сопряжены друг другу по отношению к полю Γ, то для общей нормы этих чисел имеем оценку:

$$\left| N\left(\sum_{\bar{b}} B(\bar{b}) F_i(\varrho_i)\right)\right| \leqslant h^n c_1^{sn}. \tag{2}$$

Возьмем теперь любой простой идеал $\mathfrak{P}$ поля Δ, который не входит в число

$$B(\bar{b}_0) \prod_{\varrho \neq \varrho_0} (\varrho - \varrho_0), \quad \text{где } \varrho = \varrho_1; \quad \bar{\varrho}_0 = \bar{\omega}_i \bar{b}_0;$$

пусть $\mathfrak{P}/p$, где p рациональное простое.

Полагаем

$$f(x) = \frac{1}{(p-1)!} (x-\varrho_0)^{p-1} \prod_{\varrho \neq \varrho_0} (x-\varrho)^p.$$

Легко видеть, что при таком выборе $f(x)$ мы имеем: $s = Np-1$, где N число различных значений $\bar{b}$.

Элементарная оценка дает нам также

$$h \leqslant (2\varrho_0)^{Np-1}/(p-1)!,$$

что вместе с (2) влечет неравенство:

$$\left| N\left(\sum_{\bar{b}} B(\bar{b}) F_i(\varrho_i)\right)\right| \leqslant c_2^n/(p-1)!,$$

где $c_2 = (2\varrho_0 c_1)^{Nn}$.

Так как p можно взять как угодно большим, то правую часть последнего неравенства можно сделать как угодно малой; поэтому левая часть должна быть равна 0, ибо она не зависит от p. Следовательно

$$\sum_{\bar{b}} B(\bar{b}) F_1(\varrho) = 0. \tag{3}$$

С другой стороны полагаем

$$f(x) = (x-\varrho)^q Q(x),$$

где ϱ любой корень $f(x)$ кратности q. Применяя к $f(x)$ правило дифференцирования произведения, мы без труда получаем

$$f^{(m)}(\varrho) = q! \binom{m-q}{m} Q^{m-q}(\varrho) \qquad \text{для } m \geqslant q.$$

Если $\varrho = \varrho_0$, то $q = p-1$ и

$$f^{(m)}(\varrho_0) = (p-1)! \binom{m-p+1}{m} Q^{m-p+1}(\varrho_0).$$

Для $m = p-1$ имеем

$$f^{(p-1)}(\varrho_0) = (p-1)!\, Q(\varrho_0) = \prod_{\varrho \neq \varrho_0} (\varrho - \varrho_0)^p \not\equiv 0 \pmod{\mathfrak{P}},$$

для $m \geqslant p$

$$f^{(m)}(\varrho_0) = (p-1)! \binom{m-p+1}{m} Q^{(m-p+1)}(\varrho_0) \equiv 0 \pmod{p},$$

ибо $p \Big/ \binom{m-p+1}{m}$. Поэтому: $F_1(\varrho_0) \not\equiv 0 \pmod{\mathfrak{P}}$.

Если же $\varrho \neq \varrho_0$ то, как показывает непосредственный подсчет, мы имеем

$$f^{(m)}(\varrho) = p! \frac{\gamma}{(p-1)!} \equiv 0 \pmod{p}, \text{ где } \gamma \text{ — целое.}$$

Значит в этом случае $F_1(\varrho) \equiv 0 \pmod{\mathfrak{P}}$.

В силу выбора $\mathfrak{P}$ имеем следовательно:

$$\sum_{\bar{b}} B(\bar{b}) F_1(\varrho) \not\equiv 0 \pmod{\mathfrak{P}}, \quad \text{т. е.} \quad \sum_{\bar{b}} B(\bar{b}) F_1(\varrho) \neq 0,$$

что противоречит (3).

ЛИТЕРАТУРА

1. А. О. Гельфонд, Приближение алгебраических чисел алгебраическими же числами, Усп. матем. наук, т. IV, вып. 4 (32), 1949.

2. T. Skolem, A proof of the Algebraic Independence of certain values of the exponential functions, Det Kongelige Norske Videnskabers Selskabs, Bd. XIX, No 2 (1946).

3. E. Landau, Vorlesungen über Zahlentheorie, Bd. III (1927), Satz 741.

Поступила 1.II 1951.

Саратов.
