Последние три лекции по теории чисел

Лектор А.И. Галочкин

ОБОЗНАЧЕНИЯ: $\mathbf{A}$ – поле алгебраических чисел, $\mathbf{Z_A}$– кольцо целых алгебраических чисел. Длиной многочлена P называется сумма модулей его коэффициентов $L(P)$.

27. Обобщение теоремы Лиувилля на многочлены от нескольких алгебраических чисел

Теорема. *Пусть $\alpha_1, \dots, \alpha_s$ – алгебраические числа степеней соответственно $m_1, \dots, m_s$. Тогда существует такая положительная постоянная $C = C(\alpha_1, \dots, \alpha_s)$, что для любого многочлена $P(x_1, \dots, x_s) \in \mathbb{Z}[x_1, \dots, x_s]$ либо $P(\alpha_1, \dots, \alpha_s) = 0$, либо выполняется неравенство*

$$|P(\alpha_1, \dots, \alpha_s)| \geq L^{1-(m_1 \cdots m_s)} C^{-d}, \tag{1}$$

где d и L – соответственно степень и длина многочлена $P(x_1, \dots, x_s)$.

Доказательство разобьем на отдельные пункты.

1) Существует такое натуральное число a, что все числа $a\alpha_1, \dots, a\alpha_s$ – целые алгебраические.

Утверждение было доказано ранее. a равно произведению старших коэффициентов канонических многочленов чисел $\alpha_1, \dots, \alpha_s$.

2) Число $\beta = a^d P(\alpha_1, \dots, \alpha_s) \in \mathbb{Z}_{\mathbb{A}}$.

Действительно, если $k_1, \dots, k_s$ – неотрицательные целые числа и $k_1 + \cdots k_s \leq d$, то

$$a^d \alpha_1^{k_1} \cdots \alpha_s^{k_s} = (a\alpha_1)^{k_1} \cdots (a\alpha_s)^{k_s} a^{d-k_1-\cdots k_s} \in \mathbb{Z}_{\mathbb{A}},$$

откуда легко следует утверждение.

3) Пусть $\alpha_{i1}, \dots, \alpha_{im_i}$. – числа, сопряженные алгебраическому числу α_i, $i = \overline{1, s}$. Тогда все числа

$$|a^d P(\alpha_{1r_1}, \dots, \alpha_{sr_s})| \leq C_1^d L,$$

где $1 \leq r_i \leq m_i$, а положительная постоянная C_1 не зависит от многочлена P.

Утверждение легко доказывается с

$$C_1 = a \max_{i,j}(1, |\alpha_{ij}|).$$

$$4) A(x) = \prod_{r_1=1}^{m_1} \cdots \prod_{r_s=1}^{m_s} (x - a^d P(\alpha_{1r_1}, \ldots, \alpha_{sr_s})) \in \mathbb{Q}[x]$$

Утверждение легко следует из того, что

$$A(x) = A(x \,|\, \overline{\alpha}_1, \ldots, \overline{\alpha}_s)$$

– симметрический многочлен относительно s систем переменных $\overline{\alpha}_i = (\alpha_{i1}, \ldots, \alpha_{im_i})$ и из ранее доказанной леммы о симметрических многочленах от нескольких систем сопряженных алгебраических чисел.

Доказательство. Пусть

$$B(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0 = (x - \beta_1) \cdots (x - \beta_n)$$

– минимальный многочлен числа $\beta = \beta_1$. Поскольку $\beta \in \mathbb{Z}_{\mathbb{A}}$ (см. пункт 2)), то $B(x) \in \mathbb{Z}[x]$ и $|b_0| \geq 1$, если только $P(\alpha_1, \ldots, \alpha_s) \neq 0$.

Многочлены $A(x)$ и $B(x)$ имеют рациональные коэффициенты и общий корень β, а т.к. $B(x)$ – минимальный многочлен числа β, то $B(x) \,|\, A(x)$ и все корни $B(x)$ суть корни $A(x)$. А тогда по утверждению 3)

$$1 \leq |b_0| = |\beta| \cdot |\beta_2 \cdots \beta_s| \leq a^d |P(\alpha_1, \ldots, \alpha_s)| (C_1^d L)^{n-1},$$

А так как $n \leq m_1 \cdots m_s$, то из этого неравенства следует утверждение теоремы с $C = aC_1^{(m_1 \cdots m_s)-1}$.

28. Лемма Зигеля об оценках решений систем уравнений с целыми коэффициентами

Лемма. *Пусть* $a_{ij} \in \mathbb{Z}$, $|a_{ij}| < A$ *и*

$$L_i(\overline{x}) = \sum_{j=1}^{q} a_{ij} x_j, \qquad i = \overline{1, p}; \quad p < q.$$

Тогда система уравнений

$$L_i(\overline{x}) = 0, \qquad i = \overline{1, p}$$

имеет решение $(x_1^{(0)}, \ldots, x_q^{(0)})$, $x_j^{(0)} \in \mathbb{Z}$, *такое, что*

$$0 < \max_j |x_j^{(0)}| \leq 1 + (qA)^{\frac{p}{q-p}}.$$

Доказательство. Пусть X – натуральное число, которое будет выбрано в дальнейшем, и каждая из величин x_j пусть независимо друг от друга принимает значения $0, \pm 1, \ldots, \pm X$. Всего получим $(2X+1)^q$ наборов $\overline{x} = (x_1, \ldots, x_q)$. Каждому из этих наборов соответствует набор $\overline{L}(\overline{x}) = (L_1(\overline{x}), \ldots, L_p(\overline{x}))$, причем $|L_i(\overline{x})| \leq qAX$ и, следовательно, всего может быть не более $(2qAX + 1)^p$ различных наборов $\overline{L}(\overline{x})$. Если

$$(2X + 1)^q > (2qAX + 1)^p, \tag{2}$$

то по принципу Дирихле можно найти два набора $\overline{x}$: $\overline{x}^{(1)}$ и $\overline{x}^{(2)}$, которым соответствует один и тот же набор значений $\overline{L}(\overline{x})$, то есть

$$\overline{L}(\overline{x}^{(2)}) - \overline{L}(\overline{x}^{(1)}) = \overline{L}(\overline{x}^{(2)} - \overline{x}^{(1)}) = \overline{0},$$

а, значит, $\overline{x}^{(0)} = \overline{x}^{(2)} - \overline{x}^{(1)}$ – решение системы, причем $|\overline{x}^{(0)}| \le 2X$.

Неравенство (2) выполняется, если

$$(2X+1)^q > ((qA)(2X+1))^p,$$

то есть при

$$2X > (qA)^{\frac{p}{q-p}} - 1,$$

а значит можно найти такое решение $\overline{x}^{(0)}$, что

$$2X \le (qA)^{\frac{p}{q-p}} + 1,$$

откуда следует утверждение леммы.

29. Формулировка теоремы Линдемана. Ее следствия. Построение вспомогательной функции, оценки ее порядка нуля.

Теорема Линдемана. *Если α – алгебраическое число, отличное от нуля, то число e^α трансцендентно.*

Следствия. 1) *Число e трансцендентно.*

2) *Число π трансцендентно.*

Легко следует из равенства $e^{\pi i} = -1$.

3) *Если α – алгебраическое число, отличное от 0 и 1, то число $\ln\alpha$ трансцендентно.*

Легко следует из равенства $e^{\ln\alpha} = \alpha$.

4) *Если $\alpha \ne 0$ –алгебраическое число, то числа $\sin\alpha$, $\cos\alpha$, $\operatorname{tg}\alpha$ трансцендентны.*

Эти утверждения легко следуют из равенств

$$\sin\alpha = \frac{e^{i\alpha} - e^{-i\alpha}}{2i}, \qquad \cos\alpha = \frac{e^{i\alpha} + e^{-i\alpha}}{2}.$$

В дальнейшем пусть n – натуральное число, которое будет выбрано достаточно большим, $\gamma_1, \gamma_2 \ldots,$ – не зависящие от n положительные постоянные.

Лемма 1 *Существует такая функция*

$$f(z) = \sum_{k=0}^{n-1}\sum_{l=0}^{n-1} a_{kl} z^k e^{lz} \tag{3}$$

с коэффициентами $a_{kl} \in \mathbb{Z}$, что

$$0 < \max_{k,l} |a_{kl}| < n^{\gamma_1 n}, \tag{4}$$

$$f^{(t)}(0) = 0, \quad t = \overline{0, [n^{3/2}] - 1}, \tag{5}$$

где $[\cdot]$ – целая часть числа.

Доказательство. Из формулы Лейбница следует, что

$$f^{(t)}(z) = \sum_{k,l=0}^{n-1} a_{kl} \sum_{s=0}^{\min(t,k)} C_t^s k(k-1)\cdots(k-s+1) z^{k-s} l^{t-s} e^{lz}. \tag{6}$$

Поэтому

$$f^{(t)}(0) = \sum_{k,l=0,\, k\le t}^{n-1} C_t^k (k!) l^{t-k} a_{kl},$$

и для завершения доказательства нам осталось оценить решение системы из $p = [n^{3/2}]$ уравнений (5) относительно $q = n^2$ неизвестных a_{kl}. Их коэффициенты

$$|C_t^k (k!) l^{t-k}| < 2^{n^{3/2}} n^n n^{n^{3/2}} < n^{(3n^{3/2})} = A$$

По лемме Зигеля существует ненулевое решение этой системы в целых числах a_{kl}, удовлетворяющих неравенству

$$|a_{kl}| < 1 + (qA)^{\dfrac{p}{q-p}} < n^{\gamma_1 n}.$$

Обозначим через $\operatorname{ord}_{z=a} f(z)$ порядок нуля функции $f(z)$ в точке $z = a$.

Лемма 2 $[n^{3/2}] \le \operatorname{ord}_{z=0} f(z) \le n^2$.

Доказательство. Оценка снизу следует из (5). Докажем правое неравенство. Все функции $z^k e^{lz}, \quad k, l = \overline{0, n-1}$, являются решениями дифференциального уравнения

$$D^n (D-1)^n \cdots (D-n+1)^n y = 0, \quad D = \frac{d}{dz},$$

с постоянными коэффициентами порядка n^2, следовательно, функция $f(z)$ тоже является решением этого уравнения и, если $f^{(t)}(0) = 0, \quad t = \overline{0, n^2-1}$, то по теореме о единственности решения дифференциального уравнения $f(z) \equiv 0$, что невозможно, поскольку $f(x) \to \infty$ при $x \to +\infty, \quad x \in \mathbf{R}$.

30. Оценка вспомогательной функции и завершение доказательства теоремы Линдемана.

Пусть X – не зависящее от n натуральное число, которое будет выбрано в дальнейшем,

$$T = \min_{x=\overline{0,X}} \operatorname{ord}_{z=x\alpha} f(z) \tag{7}$$

Лемма 3 *Справедливы неревенства*

$$|f^{(T)}(x\alpha)| < n^{-\gamma_2 n^{3/2} - 1/3(X-6)T}, \qquad x = \overline{0, X}.$$

Доказательство. Из (7) и леммы 2 следует, что функция

$$g(z) = f(z)z^{-[n^{3/2}]}(z-\alpha)^{-T}\cdots(z-X\alpha)^{-T}$$

имеет лишь устранимые особые точки, поэтому для нее справедлив принцип максимума модуля. Возьмем $r = X|\alpha| + 1 < \sqrt{n}$. Тогда

$$\max_{|z|\le r}|g(z)| \le \max_{|u|=2\sqrt{n}}|g(u)|.$$

Поэтому при достаточно большом n

$$\begin{aligned} M_r &= \max_{|z|\le r}|f(z)| \le \\ &\le \max_{|u|=\sqrt{n}}|f(u)|\cdot \ max_{|z|\le r,\,|u|=\sqrt{n}}\left|\left(\frac{z}{u}\right)^{[n^{3/2}]}\left(\frac{z-\alpha}{u-\alpha}\right)^{T}\cdots\left(\frac{z-X\alpha}{u-X\alpha}\right)^{T}\right| \le \\ &\le n^2 n^{\gamma_1 n}(\sqrt{n})^n e^{n^{3/2}}\cdot n^{-0{,}4n^{3/2}-0{,}4XT} < n^{-1/3n^{3/2}-1/3XT}. \end{aligned} \tag{8}$$

Далее,

$$f^{(T)}(x\alpha) = \frac{T!}{2\pi i}\oint_{|z-x\alpha|=1}\frac{f(z)\,dz}{(z-x\alpha)^{T+1}},$$

поэтому по лемме 2

$$f^{(T)}(x\alpha) \le (T!)M_r \le T^T M_r \le n^{2T}M_r$$

и из (8) следует утверждение леммы.

Доказательство теоремы Линдемана. Из (7) следует, что существует такой индекс x_0, что $f^{(T)}(x_0\alpha) \ne 0$, причем эта производная является многочленом $P(\alpha, e^\alpha)$ с целыми коэффициентами.

Допустим, что при некотором ненулевом α оба числа α и e^α алгебраические степеней соответственно m_1 и m_2. Тогда к многочлену $P(\alpha, e^\alpha)$ можно применить обобщенную теорему Лиувилля. С помощью равенства (6) оценим его длину и степень:

$$L(P) \le n^2 n^{\gamma_1 n}(n!)x_0^n\sum_{s=0}^{T}C_T^s(n-1)^{T-s} \le n^{\gamma_3 n+T}, \qquad \deg P \le n + Xn.$$

Из обобщенной теоремы Лиувилля получаем, что

$$|f^{(T)}(x_0\alpha)| = |P(\alpha, e^\alpha)| \ge (L(P))^{1-m_1m_2}C^{-\deg P} > n^{-\gamma_4 n - m_1m_2T}.$$

С другой стороны, по лемме 3 при $X = 3m_1m_2 + 6$ выполняется неравенство

$$|f^{(T)}(x_0\alpha)| < n^{-\gamma_2 n^{3/2}-m_1m_2T}.$$

Последние две оценки при достаточно большом n противоречивы. Теорема Линдемана доказана.

31. Седьмая проблема Гильберта. Формулировка теоремы Гельфонда – Шнейдера. Ее следствия. Построение вспомогательной функции для доказательства теоремы Гельфонда-Шнейдера, оценки ее порядка нуля.

В 1900 году Д.Гильберт в своем докладе на Втором международном конгрессе математиков назвал 23 проблемы "исследование которых может стимулировать дальнейшее развитие науки". Под номером семь фигурировала проблема трансцендентности алгебраических степеней алгебраических чисел.

Частичное решение этой проблемы было найдено А.О.Гельфондом в 1929 году и Р.О.Кузьминым в 1930 году. Полностью ее решили независимо в 1934 году А.О.Гельфонд и Т.Шнейдер.

Теорема Гельфонда – Шнейдера. *Пусть a – алгебраическое число, отличное от 0 и 1, а β – алгебраическое число, не являющееся рациональным. Тогда число $a^\beta = e^{\beta \ln a}$ трансцендентно.*

Примечание. Под $\ln a$ понимается значение, взятое на любой ветви комплексного логарифма.

Следствия. 1) *Число e^π трансцендентно.*

Утверждение легко следует из равенства $(e^\pi)^i = -1$.

2) *Если a и b – алгебраические числа, отличные от 0 и 1, то число $\log_a b = (\ln a)/(\ln b)$ либо рационально, либо трансцендентно.*

Утверждение следует из основного логарифмического тождества.

Лемма 4 *Пусть $\beta \in \mathbb{Z}_\mathbb{A}$ и*

$$\beta^m = b_{m-1}\beta^{m-1} + \cdots + b_1\beta + b_0, \qquad b_j \in \mathbb{Z}, \quad |b_j| \le B. \tag{9}$$

Тогда для любой натуральной степени числа β справедливы утверждения:

$$\beta^t = b_{t,m-1}\beta^{m-1} + \cdots + b_{t,1}\beta + b_{t,0}, \qquad b_{t,j} \in \mathbb{Z}, \quad |b_{t,j}| \le (B+1)^t.$$

Кроме того, если k и l – неотрицательные целые числа, не превосходящие n, то

$$(k+l\beta)^t = B_{t,k,l,m-1}\beta^{m-1} + \cdots + B_{t,k,l,1}\beta + B_{t,k,l,0}; \quad B_{t,k,l,j} \in \mathbb{Z}, \quad |B_{t,k,l,j}| \le (B+2)^t n^t.$$

Доказательство первого утверждения проводится по индукции. При $t \le m$ утверждение следует из (9). Пусть оно верно при t. Тогда в силу (9)

$$\beta^{t+1} = b_{t,m-1}(b_{m-1}\beta^{m-1} + \cdots + b_0) + b_{t,m-2}\beta^{m-1} + \cdots + b_{t,0}\beta,$$

и из предположения индукции легко следует справедливость утверждения при $t+1$.

Докажем второе утверждение

$$(k+l\beta)^t = \sum_{s=0}^{t} C_t^s k^{t-s} l^s \sum_{j=0}^{m-1} b_{sj}\beta^j,$$

откуда следует, что коэффициенты при β^j не превосходят

$$\sum_{s=0}^{t} C_t^s k^{t-s} l^s (B+1)^s = (k + l(B+1))^t \le (B+2)^t n^t.$$

Лемма доказана.

Лемма 5 *Пусть β – целое алгебраическое число степени m. Тогда существует такая функция*

$$f(z) = \sum_{k=0}^{n-1} \sum_{l=0}^{n-1} a_{kl} e^{(k+l\beta)z}$$

с коэффициентами $a_{kl} \in \mathbb{Z}$, что

$$0 < \max_{k,l} |a_{kl}| < n^{\gamma_5 n},$$
$$f^{(t)}(0) = 0, \quad t = \overline{0, [n^{3/2}] - 1}.$$

Доказательство. Мы имеем:

$$f^{(t)}(z) = \sum_{k,l=0}^{n-1} a_{kl} (k + l\beta)^t e^{(k+l\beta)z}, \tag{10}$$

поэтому по лемме 4

$$f^{(t)}(0) = \sum_{k,l=0}^{n-1} a_{kl} (k + l\beta)^t = \sum_{k,l=0}^{n-1} \sum_{s=0}^{m-1} B_{t,k,l,s} \beta^s a_{kl}$$

Приравняем к нулю коэффициенты при степенях β^s. Получим систему

$$\sum_{k,l=0}^{n-1} \sum_{s=0}^{m-1} B_{t,k,l,s} a_{kl} = 0, \qquad t = \overline{0, [n^{3/2}] - 1}, \quad s = \overline{0, m-1},$$

состоящую из $p = m[n^{3/2}]$ уравнений относительно $q = n^2$ неизвестных a_{kl}. По лемме 4

$$|B_{t,k,l,s}| < (B+2)^t n^t < n^{2n^{3/2}} = A \qquad (t < n^{3/2})$$

и для завершения доказательства осталось применить лемму Зигеля.

Пусть X – не зависящее от n натуральное число, которое будет выбрано в дальнейшем,

$$T = \min_{x=\overline{0,X}} \operatorname{ord}_{z=x \ln a} f(z) \tag{11}$$

Лемма 6 $[n^{3/2}] \le \operatorname{ord}_{z=0} f(z) \le n^2$.

Доказательство. Оценка снизу следует из леммы 5. Докажем правое неравенство. Допустим противное. Тогда

$$f^{(t)}(0) = \sum_{k,l=0}^{n-1} a_{kl}(k+l\beta)^t = 0, \quad t = \overline{0,\, n^2-1}.$$

Получили систему из n^2 линейных уравнений с n^2 неизвестными a_{kl}. Определитель системы есть определитель Вандермонда. Он отличен от нуля, так как, ввиду иррациональности числа β, все числа $k+l\beta$ различны между собой. Следовательно, система может иметь лишь нулевое решение, что противоречит лемме 5.

32. Оценки вспомогательной функции и завершение доказательства теоремы Гельфонда-Шнейдера.

Лемма 7 *Справедливы неревенства*

$$|f^{(T)}(x\ln a)| < n^{-\gamma_6 n^{3/2} - 1/3(X-6)T}, \qquad x = \overline{0, X}.$$

Доказательство этой леммы весьма сходно с доказательством леммы 3. На этот раз надо применить принцип максимума модуля к функции

$$g(z) = f(z)z^{-[n^{3/2}]}(z-\ln a)^{-T}\cdots(z-X\ln a)^{-T}$$

и положить $r = X|\ln a| + 1 < \sqrt{n}$.

Доказательство теоремы Гельфонда – Шнейдера. Без ограничения общности можно считать, что число β – целое алгебраическое – в противном случае умножим его на такое натуральное число b, чтобы $b\beta \in \mathbf{Z_A}$, докажем, что число $a^{b\beta}$ трансцендентно, и уже отсюда легко установим трансцендентность числа a^β.

Из (11) следует, что существует такой индекс x_0, что $f^{(T)}(x_0\ln a) \neq 0$, причем эта производная является многочленом $P(\beta, a, a^\beta)$ с целыми коэффициентами.

Допустим, что при выполненных условиях теоремы все три числа β, a и a^β алгебраические степеней соответственно m, m_1 и m_2. Тогда к многочлену $P(\beta, a, a^\beta)$ можно применить обобщенную теорему Лиувилля. С помощью равенства (10) оценим его длину и степень:

$$L(P) \le n^2 n^{\gamma_5 n}(2n)^T, \quad \deg P \le T + 2nX.$$

Из обобщенной теоремы Лиувилля получаем, что

$$|f^{(T)}(x_0\ln a)| = |P(\beta, a, a^\beta)| > (L(P))^{1-mm_1m_2} C^{-\deg P} > n^{-\gamma_7 n - mm_1m_2T}.$$

С другой стороны, по лемме 7 при $X = 3mm_1m_2 + 6$ выполняется неравенство

$$|f^{(T)}(x_0\ln a)| < n^{-\gamma_6 n^{3/2} - mm_1m_2T}.$$

Последние две оценки при достаточно большом n противоречивы. Теорема доказана.