Записки научных
семинаров ПОМИ
Том 543, 2025 г.

А. Л. Чистов

СЛОЖНОСТЬ ПОСТРОЕНИЯ КОРНЕЙ МНОГОЧЛЕНА В ПОЛЕ КРАТНЫХ ФОРМАЛЬНЫХ ДРОБНО-СТЕПЕННЫХ РЯДОВ В НУЛЕВОЙ ХАРАКТЕРИСТИКЕ

Введение

Пусть k – основное поле характеристики нуль с алгебраическим замыканием $\overline{k}$. Мы предполагаем, что k конечно порождено над его примитивным подполем $\mathbb{Q}$. Пусть $f \in k[X_1, \dots, X_n,\ Z]$ – многочлен степени $\deg_{Z,X_1,\dots,X_n} \leqslant d$ для некоторого целого числа $d \geqslant 2$.

Рассмотрим $f \in k(X_1, \dots, X_n)[Z]$ как многочлен от одной переменной с Z с коэффициентами из поля $k(X_1, \dots, X_n)$. Тогда корни $Z = z_u$, $1 \leqslant u \leqslant \deg_Z f$ (мы учитываем кратности корней), многочлена f принадлежат полю кратных формальных дробно–степенных рядов от $X_1, \dots, X_n$, т.е. к объединению по всем целым числам $\nu_1, \dots, \nu_n \geqslant 1$ полей кратных формальных дробно–степенных рядов с фиксированными $\nu_1, \dots, \nu_n$:

$$\bigcup_{\nu_1,\dots,\nu_n \geqslant 1} \overline{k}((X_1^{1/\nu_1}))((X_2^{1/\nu_2}))\dots((X_n^{1/\nu_n})). \tag{1}$$

Поле (1) алгебраически замкнуто. Цель данной статьи – привлечь внимание к оценке и построению корней z_u в поле (1) (конечно, требуется оценить размеры коэффициентов из поля $\overline{k}$ корней z_u в поле (1)). Эта проблема решена для $n = 1$ в [4]. По нашим сведниям для случая $n > 1$ до сих пор оценок получено не было.

ПРИМЕР. Пусть $f = Z^2 - 2X_1X_2 - X_2^2 - X_3^2$. Тогда один из корней полинома f

$$z_u = \sqrt{2}X_1^{1/2}X_2^{1/2}(1 + X_2/(2X_1) + X_3^2/(2X_1X_2))^{1/2} \in$$
$$\mathbb{Q}[\sqrt{2}][[X_1^{1/2}, X_2^{1/2}/X_1^{1/2}, X_3/(X_1^{1/2}X_2^{1/2})]].$$

Так что в общем случае требуется построить аналогичное представление для z_u (и оценить все его параметры), т.е. построить поле k_u,

Ключевые слова: формальные дробно-степенные ряды, формальные степенные ряды, факторизация многочленов, многие переменные, сложность алгоритмов.

которое является конечным расширением поля k, и представить z_u как формальный степенной ряд с коэффициентами из k_u от частных дробно-степенных мономов от $X_1, \ldots, X_n$.

Если целые числа $\nu_1, \ldots, \nu_n \geqslant 1$ являются минимально возможными такими, что

$$z_u \in \overline{k}((X_1^{1/\nu_1}))((X_2^{1/\nu_2})), \ldots, ((X_n^{1/\nu_n})), \tag{2}$$

то существует не меньше $\nu = \mathrm{LCM}\{\nu_1, \ldots, \nu_n\}$ (здесь LCM обозначает наименьшее общее кратное) попарно различных корней z_u многочлена f. Поэтому все $\nu_i \leqslant \nu \leqslant \deg_Z f \leqslant d$ (конечно ν_i и ν зависят от u). Обозначим через $\widehat{f}$ многочлен $f(X_1^{\nu_1}, \ldots, X_n^{\nu_n}, Z)$. Тогда $\widehat{z}_u = z_u(X_1^{\nu_1}, \ldots, X_n^{\nu_n})$ является корнем полинома $\widehat{f}$, элемент $\widehat{z}_u \in \overline{k}((X_1))((X_2)) \ldots ((X_n))$ и

$$z_u = \widehat{z}_u(X_1^{1/\nu_1}, \ldots, X_1^{1/\nu_n}). \tag{3}$$

В дальнейшем мы будем использовать обозначение $\nu_i = \nu_{u,i}$, если важна зависимость от u. Заметим, что степень многочлена $\widehat{f}$ ограничена сверху d^2.

Далее для всех $1 \leqslant j \leqslant n$ положим

$$X'_j = X_j^{1/\nu_j}/(X_1^{\mu_{j,1}/\nu_1} \cdot \ldots \cdot X_{j-1}^{\mu_{j,j-1}/\nu_{j-1}}) \tag{4}$$

для некоторых целых чисел $\mu_{j,i} \geqslant 0$ (так что $X'_1 = X_1$). Мы докажем, что можно выбрать целые числа $\mu_{j,i}$ так, что

$$z_u \in \overline{k}[[X'_1, \ldots, X'_n]], \tag{5}$$

т.е. z_u является формальным степенным рядом от $X'_1, \ldots, X'_n$ с коэффициентами из $\overline{k}$. Фактически существование целых чисел $\mu_{j,i}$ следует из конструкции, описанной в цитированной статье [4], применённой рекурсивно.

Решая линейную систему $Z'_j = -Z_1\mu_{j,1} - \ldots - Z_{j-1}\mu_{j,j-1} + Z_j$, $1 \leqslant j \leqslant n$, относительно $Z_1, \ldots, Z_n$ по правилу Крамера, мы получаем её решение $Z_j = Z'_1\varkappa_{j,1} + \ldots + Z'_{j,j-1}\varkappa_{j,j-1} + Z'_j$, $1 \leqslant j \leqslant n$, где все $\varkappa_{j,i} \geqslant 0$ являются целыми числами. Следовательно, в мультипликативной форме мы имеем

$$X_j^{1/\nu_j} = (X'_1)^{\varkappa_{j,1}} \cdot \ldots \cdot (X'_{j-1})^{\varkappa_{j,j-1}} X'_j, \quad 1 \leqslant j \leqslant n. \tag{6}$$

Так что каждое X_j^{1/ν_j}, $1 \leqslant j \leqslant n$, является мономом от $X'_1, \ldots, X'_j$ степени 1 относительно X'_j и с коэффициентом 1.

Используя (6), мы получаем многочлен $\widetilde{f}$ такой, что

$$\widetilde{f}(X_1', \ldots, X_n', Z) = \widehat{f}.$$

Теперь формальный степенной ряд z_u (см. (5)) является корнем многочлена $\widetilde{f}$. Отметим здесь, что множества коэффициентов из k полиномов f и $\widetilde{f}$ совпадают (но, конечно, множества их мономов различны в общем случае).

Предположим, что мы имеем некоторые верхние границы для целых чисел $\mu_{j,i}$. Тогда можно оценить все $\varkappa_{j,i}$, используя правило Крамера, и при помощи (6) оценить степень многочлена $\widetilde{f}$. После этого оценки сверху для коэффициентов формальных степенных рядов (5) могут быть получены, применяя результаты [5, 6] к многочлену $\widetilde{f}$. Заметим здесь, что в [6] результаты из [5] усиливаются: если быть кратким, то сложность алгоритмов из [5] полиномиальна от $d^{2^{n^c}}$ для некоторой константы $c > 0$, а в [6] она полиномиальна от d^n (конечно, сложность зависит также от других параметров). Результат из [8] важен для доказательства основной теоремы 3 в [6].

Теперь остаётся оценить требуемые целые числа $\mu_{j,i}$. Это может быть сделано, применяя результаты из [4] рекурсивно. Непосредственное использование [4] даёт дважды экспоненциальную от n оценку сверху для $\mu_{j,i}$. Но мы улучшаем оценки из [4] и получаем верхние границы для $\mu_{j,i}$ субэкпоненциальные от числа коэффициентов многочлена f, более точно, эти верхние оценки полиномиальны от d^n.

В дальнейшем, для того чтобы рекурсивные доказательства стали возможными, нам требуются две верхние границы на степени: $\deg_Z f \leqslant d$ и $\deg_{X_1,\ldots,X_n} f \leqslant D$, см. ниже. Если $D = d$, то мы получаем результат, описанный в начале введения.

Перейдём к точным формулировкам. Поле k конечно порождено над полем рациональных чисел $\mathbb{Q}$. Мы предполагаем, что

$$k = \mathbb{Q}(T_1, \ldots, T_l)[\theta],$$

элементы $T_1, \ldots, T_l$ являются алгебраически независимыми над $\mathbb{Q}$, элемент θ – алгебраический над полем $\mathbb{Q}(T_1, \ldots, T_l)$, и дан минимальный многочлен $\varphi \in \mathbb{Q}(T_1, \ldots, T_l)[Z]$ элемента θ над полем $\mathbb{Q}(T_1, \ldots, T_l)$.

Мы представляем многочлен $\varphi = 1/\varphi^{(0)} \sum_{0 \leqslant i \leqslant \deg_Z \varphi} \varphi_i Z^i$, где все $\varphi_i^{(0)}, \varphi_i \in \mathbb{Z}[T_1, \ldots, T_l]$ и $\mathrm{G\,C\,D}_i\{\varphi_i^{(0)}, \varphi_i\} = 1$ в $\mathbb{Z}[T_1, \ldots, T_l]$. Многочлен

$f \in k[X_1, \ldots, X_n, Z]$ представляется в виде

$$f = \frac{1}{a^{(0)}} \sum_{0 \leqslant i < \deg_Z \varphi,\, i_1, \ldots, i_n \geqslant 0} a_{i, i_1, \ldots, i_n} \theta^i X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}, \tag{7}$$

где все $a_{i,i_1,\ldots,i_n}, a^{(0)} \in \mathbb{Z}[T_1, \ldots, T_l]$, и в этом кольце наибольший общий делитель $\mathrm{G\,C\,D}_{\,i,i_1,\ldots,i_n}\{a_{i,i_1,\ldots,i_n}, a^{(0)}\} = 1$. Положим

$$\deg_{T_1,\ldots,T_l} f = \max\{\deg_{T_1,\ldots,T_l} a_{i,i_1,\ldots,i_n}, \deg_{T_1,\ldots,T_l} a^{(0)}\}. \tag{8}$$

Длина записи $\mathrm{l}(h)$ целого числа $h \in \mathbb{Z}$ равна его длине в битовой двоичной записи. Обозначим через $\mathrm{l}(f)$ максимум длин записи коэффициентов из $\mathbb{Z}$ при мономах от $T_1, \ldots, T_l$ полиномов $a_{i,i_1,\ldots,i_n}, a^{(0)}$. Аналогичным образом определяются степень $\deg_{T_1,\ldots,T_l,Z} \varphi$ и длина записи коэффициентов $\mathrm{l}(\varphi)$. Мы будем предполагать, что

$$\begin{aligned} &\deg_{T_1,\ldots,T_l,Z} \varphi < d_1, \quad \deg_{T_1,\ldots,T_l} f < d_2, \quad \deg_{X_1,\ldots,X_n} f \leqslant D, \\ &\deg_Z f \leqslant d, \quad \mathrm{l}(\varphi) \leqslant M_1, \quad \mathrm{l}(f) \leqslant M_2. \end{aligned} \tag{9}$$

для некоторых положительных целых чисел $d \geqslant 2$, D, d_1, d_2, M_1, M_2.

В дальнейшем мы будем предполагать без ограничения общности (заменяя при необходимости элемент θ на новый), что старший коэффициент $\mathrm{lc}_Z \varphi = 1$ и $\varphi \in \mathbb{Z}[t_1, \ldots, t_l, Z]$. Далее, предполагаем, что $a^{(0)} = 1$. Пусть $a = \mathrm{lc}_Z f$ является старшим коэффициентом полинома f относительно Z. Положим $g = a^{-1+\deg_Z f} f(X_1, \ldots, X_n, Z/a)$. Тогда $g \in \mathbb{Z}[T_1, \ldots, T_l, \theta,\ X_1, \ldots, X_n, Z]$, и старший коэффициент $\mathrm{lc}_Z g = 1$. Каждый корень z_u многочлена f представляется в виде

$$z_u = z'_u / a \tag{10}$$

где z'_u является корнем многочлена g. Можно построить z'_u и оценить все его параметры (длины записи целых коэффициентов, степени и т.д.) при помощи теоремы 1, см. чуть ниже, и теоремы 3 [6]. После этого можно построить z_u и получить аналогичные оценки для z_u, используя (10) (мы оставляем здесь подробности читателю). Так что в дальнейшем, заменяя f на g, мы будем предполагать дополнительно, не умаляя общности, что старший коэффициент $\mathrm{lc}_Z f = 1$ и $f \in \mathbb{Z}[T_1, \ldots, T_l, \theta, X_1, \ldots,\ X_n, Z]$.

Напомним некоторые определения, см. [5]. Обозначим через $\mathfrak{m}$ максимальный идеал кольца $\widehat{A} = \overline{k}[[X_1, \ldots, X_n]]$ формальных степенных рядов. Так что идеал $\mathfrak{m}$ порождён элементами $X_1, \ldots, X_n$. Пусть $z \in \widehat{A}$ и $N \geqslant 0$ – целое число. Тогда существует единственный полином

$z' \in \overline{k}[X_1, \ldots, X_n]$ степени $\deg_{X_1,\ldots,X_n} z' \leqslant N$ такой, что $z - z' \in \mathfrak{m}^{N+1}$. По определению положим $z_{\#,N} = z'$. Мы будем отождествлять множество элементов факторкольца $\widehat{A}/\mathfrak{m}^{N+1}$ с линейным пространством полиномов степени самое большее N из $\overline{k}[X_1, \ldots, X_n]$. Следовательно, теперь $z_{\#,N} = z \bmod \mathfrak{m}^{N+1}$ для любого $z \in \widehat{A}$.

Пусть Z – переменная, и многочлен $g = \sum_{0 \leqslant j \leqslant \deg_Z g} g_j Z^j \in \widehat{A}[Z]$, где все коэффициенты $g_j \in \widehat{A}$. Тогда для всякого $N \geqslant 0$ положим

$$g_{\#,N} = g \bmod \mathfrak{m}^{N+1} = \sum_{0 \leqslant j \leqslant \deg_Z g} (g_j)_{\#,N} Z^j \in \overline{k}[X_1, \ldots, X_n, Z].$$

Определение 1 *Мы будем говорить, что алгоритм строит элемент $z \in \widehat{A}$ (соответственно многочлен $g \in \widehat{A}[Z]$) в том и только в том случае, если для всякого заданного целого числа $N \geqslant 0$ этот алгоритм может построить многочлен $z_{\#,N}$ (соответственно $g_{\#,N}$).*

Конечно, здесь все коэффициенты полинома $z_{\#,N}$ (соответственно $g_{\#,N}$) являются элементами из некоторого конечного расширения основного поля k, и это расширение строится данным алгоритмом явно. Аналогичным образом эти определения применяются к кольцам формальных степенных рядов от других переменных, не обязательно $X_1, \ldots, X_n$ (и над другими полями).

В дальнейшем в этой статье в верхних оценках степеней, длин записи целых коэффициентов и т.д. мы используем обозначение $\mathcal{P}$ для полинома (может быть от многих переменных) с неотрицательными целыми коэффициентами. Если не оговорено противное, то мы не предполагаем, что этот полином является одним и тем же в разных местах в тексте (даже близких друг к другу). Коэффициенты каждого такого полинома $\mathcal{P}$ являются абсолютными константами.

Теперь мы можем сформулировать наш основной результат.

Теорема 1 *Пусть многочлен f – такой же, как и выше, старший коэффициент $\mathrm{lc}_Z f = 1$. Пусть $\nu_1, \ldots, \nu_n \geqslant 1$ являются целыми числами такими, что выполняется соотношение (2). Пусть полиномы $\widehat{f}, \widetilde{f}$, корень z_u многочлена f, целые числа $\mu_{j,i}$ – такие же, как и выше. Следовательно, имеют место равенства (3), (4) и соотношение (5). Тогда справедливы следующие утверждения.*

(i) *Для всякого корня z_u многочлена f существуют целые числа $\mu_{j,i} \geqslant$, $1 \leqslant j \leqslant n$, $1 \leqslant i \leqslant j-1$, такие, что $\sum_{1 \leqslant i \leqslant j-1} \mu_{j,i} \leqslant$*

$D^2(c_1 d)^{(n+1-j)c}$ для абсолютных констант $c_1, c > 0$ (такие константы несложно вычислить[1]*) для всех j, i. Отсюда следует, что для всех j, i целые числа $\varkappa_{j,i} \leqslant D^{2n}\mathcal{P}(d^{n^2})$, см. (6), и степень $\deg_{X_1,\dots,X_n,Z} \widetilde{f} \leqslant D^{2n}\mathcal{P}(d^{n^2})$.*

(ii) *Для всякого корня z_u многочлена f можно построить целые числа $\nu_1, \dots, \nu_n$ и после этого все $\mu_{j,i}$ и многочлен $\widetilde{f}$. Далее, применяя теорему 3 [6] к многочлену $\widetilde{f}$, можно построить представления*

$$z_u \in k_u[[X_1', \dots, X_n']], \tag{11}$$

где k_u является конечным расширением поля k. Поле k_u задано примитивным элементом над k со своим минимальным многочленом над k. Это минимальный многочлен также строится, см. подробности в [6].

Поэтому согласно (11), (3) и (4) для всякого $1 \leqslant u \leqslant \deg_Z f$ мы получаем представление корня z_u как элемента кольца

$$k_u\big[\big[X_1^{1/\nu_1}, X_2^{1/\nu_2}/X_1^{\mu_{2,1}/\nu_1}, \dots, X_n^{1/\nu_n}/\big(X_1^{\mu_{j,1}/\nu_1}\cdot\ldots\cdot X_{j-1}^{\mu_{n,n-1}/\nu_{n-1}}\big)\big]\big] \tag{12}$$

формальных степенных рядов от частных дробно-степенных мономов от $X_1, \dots, X_n$.

(iii) *Время работы алгоритма для построения для всех $1 \leqslant u \leqslant \deg_Z f$ всех целых чисел $\nu_1, \dots, \nu_n$, $\mu_{j,i}$ и полей k_u (каждое из этих полей задаётся примитивным элементом над k) полиномиально от M_1, M_2, $(d_1 d_2 D^n d^{n^2})^{l+1}$, D^{n^2}, d^{n^3} (подробности см. в теореме 3 [6]).*

(iv) *Для всякого целого числа $\iota \geqslant 0$ время работы алгоритма для построения для всех $1 \leqslant u \leqslant \deg_Z f$ всех элементов $(z_u)_{\#,\iota}$ (эти элементы определяются при помощи (11)) полиномиально от M_1, M_2, $(d_1 d_2 D^n d^{n^2})^{l+1}$, D^{n^2}, d^{n^3}, ι^{l+n} (подробности см. в теореме 3 [6]).*

Доказательство теоремы 1 основывается на теореме 2 раздела 1, которая доказывается в разделе 2 и разделе 3. Теорема 2 является более сильной версией результата из [4]. Отметим, что в разделе 2 устанавливается существование некоторых объектов, связанных с алгоритмом

[1]Конечно, поскольку $d \geqslant 2$, здесь положить $c_1 = 1$, увеличивая c, но приведённая верхняя граница для $\sum_{1\leqslant i\leqslant j-1} \mu_{j,i}$ получается естественным образом в доказательстве.

Ньютона–Пюизе. Фактически фактов из раздела 2 достаточно для доказательства теоремы 1.

При доказательстве теоремы 1, чтобы оценить целые числа $\mu_{j,i}$, требуется рассматривать алгоритм Ньютона-Пюизе для более общих основных полей рекурсивно. Именно в нашей рекурсии имеются разложения Ньютона-Пюизе от переменной X_i для корней полинома из $k(X_1,\dots,X_{i-1})[X_i,Z]$, $1\leqslant i\leqslant n$ и использются хорошие оценки на степени относительно $X_1,\dots,X_i$ построенных объектов. Основное поле здесь равно $k(X_1,\dots,X_{i-1})$. При этом имеются два семейства трансцендентных элементов над примитивным подполем $\mathbb{Q}$: $T_1,\dots,T_l$ и $X_1,\dots,X_{i-1}$.

Такая ситуация уже рассматривалась в теореме 2 из раздела 2 [3] об алгоритме Ньютона-Пюизе. Но там достаточно только небольшой модификации оригинальной версии результата из [4] (поскольку в [3] нет рекурсии, подобной той, что имеется в настоящей статье). Конечно, теорема 2 раздела 2 [3] может быть доказана аналогично теореме 2 настоящей статьи. Заметим также, что, если степень трансцендентности l не фиксирована (такова ситуация в [6] и настоящей статье), то следует принимать во внимание замечание 1, см. чуть ниже, при доказательстве теоремы 2 раздела 2 [3].

Отметим ещё, что из оригинальной версии основной теоремы [4] получаются лишь оценки, подобные (29), (30) раздел 3 (хотя они и не приводятся в [4] явно). Если их применять рекурсивно в доказательстве теоремы 1, то это может дать лишь дважды экспоненциальные оценки на степени относительно $X_1,\dots,X_n$ построенных объектов.

Кроме того, недавно мы обнаружили небольшую неточность в формулировке леммы 2.1 из [4]. Одно из утверждений этой леммы состоит в том, что $\mu(i,j)=\mu_1(i,j)/\nu(i)$ для некоторых целых чисел $\mu_1(i,j)$ и $\nu(i)$, где $\nu(i)$ зависит только от i. Но в общем случае это верно только, если $\xi_i\neq 0$ (в обозначениях из этой леммы).

Эта неточность не является существенной для основного результата [4] и его доказательства. Требуются только небольшие изменения в определениях чисел $\mu_1(i,j)$, $\nu(i)$ и μ в §2 [4]. Мы приведём подробности в разделе 1.

Замечание 1. В настоящей статье нам требуется раскладывать на неприводимые множители многочлен f в кольце $k[X_1,\dots,X_n,Z]$ (и

также также другие многочлены в аналогичных кольцах). Сейчас степень трансцендентности l основного поля k не является фиксированной константой. Сложность алгоритма из [2] для факторизации f полиномиальна от d^{n+l}, но теперь нам необходима оценка полиномиальная от d^n. Подобная оценка для сложности может быть получена, применяя результат из [7] для случая гиперповерхности, или непосредственно из модифицированной версии алгоритма для факторизации многочленов из [7].

Замечание 2. В [6] степень трансцендентности l также не является фиксированной. Более того, в [6] имеется ещё семейство трансцендентных элементов $u_1, \dots, u_{l_1}$. Так что в [6] существует три семейства трансцендентных элементов над примитивным подполем: $T_1, \dots, T_l$, $u_1, \dots, u_{l_1}$ и $X_1, \dots, X_n$. Мы применяем там алгоритм для факторизации из [2] (и ссылаемся на [2]), но фактически мы используем неявно алгоритм разложения на множители многочленов из [7]. Даже более продвинутая (но аналогичная) версия этого последнего алгоритма требуется в [6]. Именно, в [7] в алгоритме для факторизации описана некоторая двухшаговая редукция, однако для доказательства теоремы 2 [6] требуется редукция из трёх шагов (всё же для доказательства основной теоремы 3 [6] достаточно двухшаговой редукции, поскольку в этом случае $l_1 = O(n)$ и рассматриваемая степень относительно $u_1, \dots, u_{l_1}$ ограничена сверху d). Но обобщение с двух шагов до трёх шагов в [7] не представляет затруднений.

§1. Сложность алгоритма Ньютона–Пюизе (для некоторых новых основных полей)

Прежде всего мы хотели бы исправить неточность из [4]. В формулировке леммы 2.1 [4] следует удалить утверждение “и $\mu(i,j) = \mu_1(i,j)/\nu(i)$, где $\mu_1(i,j) \in \mathbb{Z}$, $1 \leqslant \nu(i) < d$, $\nu(i) \in \mathbb{Z}$) и $\nu(i)$ зависит только от корня y_i” (это утверждение не верно в общем случае, оно верно только, если $\xi_i \neq 0$ в обозначениях из этой леммы). Доказательство исправленной версии леммы остаётся тем же самым.

Далее, после доказательства леммы 2.1, требуется дать новые определения чисел $\mu_1(i,j)$, $\nu(i)$, μ и элемента $Q_{i,j}$ следующим образом: “Положим $\mu'(i,j) = \mu(i,j)$, если $\xi_i \neq 0$ и

$$\mu'(i,j) = \min\{\mathrm{ord}_X f'(y_i), \mathrm{ord}_X f^{(\gamma)}(y_i)\},$$

если $\xi_i = 0$ (мы имеем $\mu'(i,j) \geqslant \mu(i,j)$ в любом случае). Теперь можно представить $\mu'(i,j) = \mu_1(i,j)/\nu(i)$, где $\mu_1(i,j) \in \mathbb{Z}$, $1 \leqslant \nu(i) < d$, $\nu(i) \in \mathbb{Z}$, $\mathrm{G\,C\,D}\,(\mu_1(i,j), \nu(i)) = 1$ и $\nu(i)$ зависит только от корня y_i. Положим $\mu = \mu(i) = \max\{\mu'(i,j) \,:\, j \neq i\}$." Наконец, в §2 [4] следует заменить "$Q_{i,j} = x^{\mu-\mu(i,j)} f^{(\gamma)}(Y) + \rho_{i,j} x^{\mu}$" на "$Q_{i,j} = x^{\mu-\mu'(i,j)} f^{(\gamma)}(Y) + \rho_{i,j} x^{\mu}$". После этого все построения и доказательства из §2 [4] остаются без изменений.

Результат статьи [4] является весьма важным. Всё же эта работа не была переведена на русский язык до сих пор. Не слишком хороший английский и рукописные формулы представляют дополнительные трудности для чтения [4]. Теперь для удобства читателя мы описываем подробно конструкцию из [4] для более общего основного поля. В этой статье мы доказываем лемму 1 и лемму 2, которые аналогичны лемме 2.1 и лемме 2.2 [4] (приведённым там без доказательств). Однако мы опускаем аналоги лемм из [4], относящихся к оценкам степеней и длин записи целых коэффициентов всех полученных многочленов, поскольку доказательства этих лемм не представляют затруднений. Мы приводим все требуемые оценки на степени и длины записей целых коэффициентов, но оставляем установить их заинтересованному читателю.

Пусть k – основное поле из введения. Напомним, что это поле задано своим примитивным элементом θ с минимальным многочленом $\varphi \in \mathbb{Q}(T_1, \ldots, T_l)[Z]$ над $\mathbb{Q}$. Положим $K = k(X_1, \ldots, X_{n-1})$ равным полю рациональных функций от $X_1, \ldots, X_{n-1}$ над K. Пусть $\overline{K}$ является алгебраическим замыканием поля K.

Положим $X = X_n$. Положим $\Omega = \bigcup_{1 \leqslant \nu \in \mathbb{Z}} \overline{K}((X^{1/\nu}))$ равным полю дробно–степенных рядов от X над $\overline{K}$. Каждый элемент $\omega \in \Omega$ может быть представлен в виде $\omega = \sum_{i \in \mathbb{Q}} \omega_i X^i$, где $\omega_i \in \overline{K}$ и существуют $i_0 \in \mathbb{Q}$ и $0 < \nu \in \mathbb{Z}$ такие, что $\omega_i \neq 0$ только, если $\nu i \in \mathbb{Z}$ и $i \geqslant i_0$. Порядок $\mathrm{ord}_X \omega = \inf\{i \,:\, \omega_i \neq 0\}$. Пусть $\psi = \sum_{0 \leqslant j \leqslant \deg_Z \psi} \psi_j Z^j \in \Omega[Z]$, $\psi_i = \sum_{j \in \mathbb{Q}} \psi_{i,j} X^i$, где $\psi_{i,j} \in \overline{K}$ для всех i, j. Положим $P(\psi) = \{(i,j) \,:\, \psi_{i,j} \neq 0\}$. Если $\alpha, \beta \in \mathbb{Q}$, $(\alpha, \beta) \neq (0,0)$, то положим $\mathrm{ord}_{\alpha,\beta}(\psi) = \inf\{\alpha i + \beta j \,:\, (i,j) \in P(\psi)\}$, $P(\psi, \alpha, \beta) = \{(i,j) \in P(\psi) \,:\, \alpha i + \beta j = \mathrm{ord}_{\alpha,\beta}(\psi)\}$, $\psi^*(\alpha, \beta) = \sum_{(i,j) \in P(\psi,\alpha,\beta)} \psi_{i,j} Z^j \in \overline{k}[Z]$. Порядок многочлена $\mathrm{ord}_X(\psi) = \mathrm{ord}_{1,0}(\psi) = \min\{j \,:\, \mathrm{ord}_X \psi_{i,j}\}$[2].

[2]Имеется опечатка: "max" вместо "min" в соответствующем месте в начале §1 [4].

Точка (i,j) является вершиной[3] в $P(\psi)$ в том и только в том случае, если существуют рациональные числа α,β такие, что $P(\psi,\alpha,\beta)=\{(i,j)\}$. Пара вершин $\{(i_1,j_1),(i_2,j_2)\}=e$ является ребром в $P(\psi)$ в том и только в том случае, если существуют рациональные числа (α,β) такие, что $e\subset P(\psi,\alpha,\beta)$. В этом случае мы будем обозначать $e=e(\psi,\alpha,\beta)$.

Далее, ломаная Ньютона многочлена ψ, обозначим её через $E(\psi)$, есть множество всех рёбер e в $P(\psi)$ с $\alpha>0$ в предыдущем определении.[4] Если $e\in E(\psi)$, то существует единственная пара $(\alpha(e),\beta(e))\in\mathbb{Z}^2$ такая, что $\mathrm{GCD}\,(\alpha(e),\beta(e))=1$, $\alpha(e)>0$ и $e\subset P(\psi,\alpha(e),\beta(e))$. Коэффициент наклона ребра e равен по определению $\beta(e)/\alpha(e)$. Отрезок $s(e)$ ребра $e=\{(i_1,j_1),(i_2,j_2)\}$ определяется по формуле $s(e)=\{(ti_1+(1-t)i_2,tj_1+(1-t)j_2)\,:\,0\leqslant t\leqslant 1\}\subset\mathbb{R}^2$.

Заметим, что в важном случае, когда $\mathrm{ord}_X(\psi)\geqslant 0$ и старший коэффициент $\mathrm{lc}_Z\psi=1$, мы имеем $\beta(e)\geqslant 0$ для всякого ребра e ломаной Ньютона многочлена ψ.

Для всякого элемента $z\in\overline{K}[X^{1/\nu},Z]$, $1\leqslant\nu\in\mathbb{Z}$, мы имеем $z(X^\nu)\in\overline{K}[X,Z]$, и мы определяем степень $\deg_X z=\deg_X(z(X^\nu))/\nu$ естественным образом.

Для $\psi\in\Omega[Z]$ пусть $\psi^{(m)}=d^m/dX^m(\Psi)$ обозначает m-ую производную многочлена ψ.

Пусть $f\in k[X_1,\dots,X_n,Z]$ – многочлен из введения со старшим коэффициентом $\mathrm{lc}_Z f=1$. В частности, справедливы верхние оценки (9) на степени и длин записи целых коэффициентов многочлена f. Положим $M=M_1+M_2+ld_2+nD$.

Произвольный корень z_u многочлена f может рассматриваться как элемент поля $\overline{K}((X_n^{1/\nu_{u,n}}))$ (фактически $z_u\in\overline{K}[[X_n^{1/\nu_{u,n}}]]$, поскольку старший коэффициент $\mathrm{lc}_Z f=1$), где целое число $1\leqslant\nu_{u,n}\leqslant\deg_Z f\leqslant d$ зависит от u, см. введение. Алгоритм Ньютона-Пюизе для всякого u вычисляет кратность корня z_u, строит конечное расширение $K_u\supset K$ и представление корня

$$z_u=\sum_{w\geqslant 0}z_{u,w}X_n^{w/\nu_{u,n}},$$

[3]В [4] мы имеем “многоугольника Ньютона многочлена ψ” вместо “of $P(\psi)$” в этих определениях. Но это не очень хорошо, так как многоугольник Ньютона не может быть определён естественным образом, если множество $P(\psi)$ бесконечно.

[4]В определении ломаной Ньютона в [4] мы требуем дополнительно “$\beta\geqslant 0$”. Но это условие является слишком ограничительным в некоторых случаях.

(см. Определение 1), где все коэффициенты $z_{u,w} \in K_u$ и поле K_u порождается над K всеми элементами $z_{u,w}$. Поле K_u задаётся на выходе алгоритма Ньютона-Пюизе своим примитивным элементом η_u с минимальным многочленом φ_u над K. Так что $\varphi_u \in K[Z]$. Фактически построенный многочлен $\varphi_u \in \mathbb{Z}[T_1, \ldots, T_l, \theta, Z]$, и старший коэффициент $\mathrm{lc}_Z \varphi_u = 1$.

Далее, строится многочлен $\Delta_u \in \mathbb{Z}[T_1, \ldots, T_l, X_1, \ldots, X_{n-1}]$ такой, что $z_{u,w} = \overline{z}_{u,w}/\Delta_u^{\max\{1, w+w_0\}}$, где элемент

$$\overline{z}_{u,w} \in \mathbb{Z}[T_1, \ldots, T_l, \theta, X_1, \ldots, X_{n-1}, \eta_u]$$

и $w_0 = w_{u,0} \geqslant 0$ – целое число, зависящее от u. Точное определение этого числа w_0 будет дано в разделе 2. Для всех $1 \leqslant u \leqslant \deg_Z f$, $w \geqslant 0$ мы представляем

$$\overline{z}_{u,w} = \sum_{\substack{0 \leqslant v_1 < \deg_Z \varphi, \\ 0 \leqslant v_2 < \deg_Z \varphi_u}} \overline{z}_{u,w,v_1,v_2} \theta^{v_1} \eta_u^{v_2}, \tag{13}$$

где все коэффициенты $\overline{z}_{u,w,v_1,v_2} \in \mathbb{Z}[T_1, \ldots, T_l, X_1, \ldots, X_{n-1}]$ строятся алгоритмом. Таким образом, на выходе алгоритма имеем представления

$$z_u = \overline{z}_{u,0}/\Delta_u^{\max\{1, w_0\}} + \sum_{w \geqslant 1} \overline{z}_{u,w}/\Delta_u^{w+w_0} X^{w/\nu_{u,n}}. \tag{14}$$

Положим $\nu = \nu_{u,n}$. Пусть $\sigma \in \mathrm{Gal}(\overline{K}/K)$ – автоморфизм поля $\overline{K}$ над K. Теперь дополнительно для всякого индекса u_1, если $Z = z_{u_1}$ – другой корень многочлена f такой, что $\nu_{u_1,n} = \nu$ и $\sigma(z_{u,w}) = z_{u_1,w}$ для всех $i \geqslant 0$ для некоторого автоморфизма σ, то $\varphi_{u_1} = \varphi_u$ и $\eta_{u_1} = \sigma(\eta_u)$ для построенных элементов η_{u_1} и φ_{u_1}, т.е. фактически строятся классы сопряжённых над K корней или, что то же самое, каждый корень $z_u \in K((X^{1/\nu}))$ задаётся на выходе алгоритма с точностью до сопряжения над K. В этом случае $\Delta_u = \Delta_{u_1}$, $w_0 = w_{0,u} = w_{0,u_1}$, $\overline{z}_{u,w,v_1,v_2} = \overline{z}_{u_1,w,v_1,v_2}$ для всех w, v_1, v_2.

Теперь мы можем сформулировать теорему о сложности алгоритма Ньютона–Пюизе над K. Заметим, что оценки из этой версии являются более подробными, чем в основной теореме [4] [5]

[5] В [4] имеются небольшие отличия в определениях верхних границ на степени, в частности, там есть две верхние границы d_0, d_1 вместо одной аналогичной границы d_1 в этой статье, но это не существенно сейчас.

Теорема 2. *В предыдущих условиях вычисляются кратности и строятся представления* (14), (13) *корней многочлена* f. *Для степеней и длин записи целых коэффициентов всех построенных элементов* w_0 (*напомним, что* $w_0 = w_{0,u}$ *зависит от* u), φ_u, Δ_u, $\overline{z}_{u,w,v_1,v_2}$ *справедливы следующие оценки.*

$$
\begin{aligned}
&w_0 \leqslant D\mathcal{P}(d),\\
&\deg_Z \varphi_u \leqslant d,\ \ \deg_{T_1,\dots,T_l} \varphi_u \leqslant d_2\mathcal{P}(d,d_1),\ \ \deg_{X_1,\dots,X_{n-1}} \varphi_u \leqslant D\mathcal{P}(d),\\
&\mathrm{l}(\varphi_u) \leqslant M\mathcal{P}(d,d_1),\\
&\deg_Z \Delta_u \leqslant d,\ \ \deg_{T_1,\dots,T_l} \Delta_u \leqslant d_2\mathcal{P}(d,d_1),\ \ \deg_{X_1,\dots,X_{n-1}} \Delta_u \leqslant D\mathcal{P}(d),\\
&\mathrm{l}(\Delta_u) \leqslant M\mathcal{P}(d,d_1),\\
&\deg_{T_1,\dots,T_l} \overline{z}_{u,w,v_1,v_2} \leqslant (w+w_0+1)d_2\mathcal{P}(d,d_1),\\
&\deg_{X_1,\dots,X_{n-1}} \overline{z}_{u,w,v_1,v_2} \leqslant (w+w_0+1)D\mathcal{P}(d),\\
&\mathrm{l}(\overline{z}_{u,w,v_1,v_2}) \leqslant M((w+w_0+1)\log_2(w+w_0+1))\mathcal{P}(d,d_1).
\end{aligned}
$$

Время работы алгоритма для построения всех целых чисел w_0, *многочленов* φ_u *и элементов* Δ_u *полиномиально от* M_1, M_2, $(dDd_1d_2)^{l+1}$, $(dD)^n$.

Для всякого целого числа $\iota \geqslant 0$ *время работы алгоритма для построения всех элементов* $\overline{z}_{u,w,v_1,v_2}$ *с* $w \leqslant \iota$ *полиномиально от* M_1, M_2, $(dDd_1d_2)^{l+1}$, $(dD)^n$, ι^{n+l}.

§2. Доказательство теоремы 2: существование требуемых объектов

Обозначим через $\delta_0 \in \mathbb{Z}[T_1,\dots,T_l]$ дискриминант относительно Z многочлена φ. Следовательно, $\delta_0 \neq 0$. Обозначим через Λ целое замыкание кольца $\mathbb{Z}[T_1,\dots,T_l,\theta]$ в его поле частных. Так что каждый элемент $\lambda \in \Lambda$ представляется в виде $\lambda = \lambda_1/\delta_0$, где $\lambda_1 \in \mathbb{Z}[T_1,\dots,T_l,\theta]$. Мы можем построить бесквадратную часть f_{sqf} многочлена f. Мы будем предполагать, что $\mathrm{lc}_Z f_{\mathrm{sqf}} = 1$. Тогда $f_{\mathrm{sqf}} \in \Lambda[X_1,\dots,X_n,Z]$, поскольку коэффициенты f_{sqf} целы над $\mathbb{Z}[T_1,\dots,T_l,\theta]$. Более того, в то же самое время можно получить разложение на множители

$$
f_{\mathrm{sqf}} = \prod_{\gamma\geqslant 1} f_{\mathrm{sqf},\gamma}, \tag{15}
$$

где $f_{\mathrm{sqf},\gamma} \in \Lambda[X_1,\dots,X_n,Z]$, $\mathrm{lc}_Z f_{\mathrm{sqf},\gamma} = 1$, каждый корень полинома $f_{\mathrm{sqf},\gamma}$ является корнем кратности γ многочлена f для всякого $\gamma \geqslant 1$.

Мы имеем $\mathrm{l}(f_{\mathrm{sqf}}) \leqslant M\mathcal{P}(d, d_1)$ и $\deg_{T_1,\dots,T_l} \leqslant d_2\mathcal{P}(d, d_1)$ (конечно, здесь можно привести и лучшие оценки). Аналогичные оценки справедливы для всех полиномов $f_{\mathrm{sqf},\gamma}$.

Если построены корни полинома f_{sqf}, то можно вычислить кратности корней многочлена f, рассматривая факторизацию (15) (здесь мы оставляем подробности читателю).

Заменяя f на f_{sqf}, мы будем предполагать в дальнейшем без ограничения общности, что многочлен f сепарабелен (но теперь не обязательно $f \in \mathbb{Z}[T_1, \dots, T_l, \theta, X_1, \dots, X_n, Z]$).

Для краткости будем обозначать $f = f(X, Z)$, т.е. рассматривать f как элемент кольца $K[X, Z]$. Положим $r = \mathrm{ord}_X(\mathrm{Res}_Z(f, f'))$ равным порядку дискриминанта полинома f относительно Z. Напомним, что для всякого корня $z_u \in \Omega$ многочлена f целое число $\nu_{u,n} \geqslant 1$ является минимально возможным таким, что $z_u \in \Omega((X^{1/\nu_{u,n}}))$, см. введение. Следующая лемма является аналогом леммы 2.1 [4].

Лемма 1. *Пусть $z_i, z_j \in \Omega$, $1 \leqslant i \neq j \leqslant \deg_Z f$, – два различных корня многочлена f. Тогда существует целое число $\gamma = \gamma(i, j)$, $1 \leqslant \gamma < \deg_Z f$, элементы $\xi_i, \xi_j \in \overline{K}$ и рациональное число $\mu(i, j)$ такие, что*

$$\mathrm{ord}_X(f^{(\gamma)}(z_u) - \xi_u X^{\mu(i,j)}) > \mu(i, j), \quad u = i, j \tag{16}$$

и $\xi_i \neq \xi_j$. Более того, $\mu(i, j) \leqslant \mathrm{ord}_X f'(X, z_i) \leqslant r/2$ и, если $\xi_i \neq 0$, то $\nu_{i,n}\mu(i, j)$ целое число.

Доказательство. Разложения Ньютона–Пюизе корней z_u, $1 \leqslant u \leqslant \deg_Z f$, имеют вид

$$z_u = \sum_{v \geqslant 0} r_{u,v} X^{\varepsilon_{u,v}} \tag{17}$$

где все коэффициенты $0 \neq r_{u,v} \in \overline{K}$ и $\{\varepsilon_{u,v}\}_{v \geqslant 0}$ строго возрастающая последовательность (бесконечная, конечная или даже пустая, если $z_u = 0$) рациональных чисел такая, что $\nu_{u,n}\varepsilon_{u,v} \in \mathbb{Z}$ являются целыми числами для всех v. Положим

$$v^{(0)} = v^{(0)}(i, j) = \sup\{v \,:\, (r_{i,w} = r_{j,w})\&(\varepsilon_{i,w} = \varepsilon_{j,w})\ \forall(0 \leqslant w \leqslant v)\},$$
$$z^{(0)} = z^{(0)}(i, j) = \sum_{0 \leqslant v \leqslant v^{(0)}} r_{i,v} X^{\varepsilon_{i,v}}.$$

Так что $v^{(0)} \geqslant 0$ – целое число или $v^{(0)} = -\infty$ (если $\mathrm{ord}_X(z_i - z_j) = 0$) и $z^{(0)} \in \overline{K}[X^{1/\nu'}]$, где ν' делит $\mathrm{GCD}\,(\nu_{i,n}, \nu_{j,n})$. Положим многочлен

$g = f(X, Z+z^{(0)})$. Можно представить $g = \sum_{u,v\geqslant 0} g_{u,v} X^{u/\nu'} Z^v$, где все $g_{u,v} \in \overline{K}$ и только конечное число из них не равны нулю.

Рассмотрим ломаную Ньютона $E(g)$ многочлена g. Если $z_u \neq z^{(0)}$, то существует ребро $e(g, 1, \varepsilon_{u,v_0+1}) \in E(g)$. Для по крайней мере одного $u = i, j$ мы имеем $z_u \neq z^{(0)}$, поскольку $z_i \neq z_j$. Если $z_u = z^{(0)}$, то положим $\varepsilon_{u,v^{(0)}+1} = +\infty$. Положим $\varepsilon = \min\{\varepsilon_{i,v^{(0)}+1}, \varepsilon_{j,v_0+1}\}$.

Пусть $u = i$ или $u = j$. Если $\varepsilon_{u,v^{(0)}+1} = \varepsilon$, то полагаем $a_u = r_{u,v^{(0)}+1}$. Если $\varepsilon_{u,v^{(0)}+1} > \varepsilon$, то полагаем $a_u = 0$. Мы имеем $a_i \neq a_j$ в любой случае, $E(g)$ содержит ребро $e(g, 1, \varepsilon)$. Кроме того, a_i и a_j являются корнями полинома $g^*(1, \varepsilon)$. Поэтому $2 \leqslant \deg_Z g^*(1, \varepsilon) \leqslant \deg_Z f$. Теперь согласно данным выше определениям

$$g^*(1, \varepsilon)(Z + a_u) = g(X, Z + a_u X^{\varepsilon})^*(1, \varepsilon) = f(X, Z + z_u)^*(1, \varepsilon), \quad u = i, j \tag{18}$$

(здесь мы оставляем подробности читателю).

Положим $\gamma = -1+\deg_Z g^*(1, \varepsilon)$. Следовательно, $1 \leqslant \gamma \leqslant -1+\deg_Z f$. Обозначим через $\widetilde{\xi}_u$ коэффициент при Z^γ в многочлене $f(X, Z+z_u)^*(1, \varepsilon)$. Тогда из (18) следует, что $\widetilde{\xi}_i \neq \widetilde{\xi}_j$, поскольку $a_i \neq a_j$.

С другой стороны, $f(X, Z + z_u) = \sum_{m\geqslant 0} f^{(m)}(X, z_u) Z^m/m!$. Напомним, что $s(e(g, 1, \varepsilon))$ является отрезком ребра e. Точка $(\mu(i, j), \gamma) \in s(e(g, 1, \varepsilon))$ для однозначно определённого рационального числа $\mu(i, j)$. Поэтому согласно данным определениям

$$\operatorname{ord}_X(f^{(\gamma)}(X, z_u) - \gamma!\widetilde{\xi}_u X^{\mu(i,j)}) > \mu(i, j), \quad u = i, j.$$

Положим $\xi_u = \gamma!\widetilde{\xi}_u$, $u = i, j$. Теперь выполняется (16) и $\xi_i \neq \xi_j$.

Если $\xi_i \neq 0$, то по (18) точка $(\mu(i, j), \gamma) \in P(f(X, Z + z_i))$ и, следовательно, $\nu_{i,n}\mu(i, j) \in \mathbb{Z}$. Если $\varepsilon_{i,v^{(0)}+1} = \varepsilon$, то $\nu_{i,n}\varepsilon \in \mathbb{Z}$ и снова $\nu_{i,n}\mu(i, j) \in \mathbb{Z}$.

Наконец, для всякой точки $(y_1, y_2) \in s(e)$ для любого ребра e ломаной Ньютона многочлена $f(X, Z + z_u)$, $u = i, j$, справедливо неравенство $y_1 \leqslant \operatorname{ord}_X f'(X, z_u)$ (это неравенство строгое, если $y_2 > 1$). Кроме того, очевидно $\operatorname{ord}_X f'(X, z_u) \leqslant r/2$. Поэтому $\mu(i, j) \leqslant \operatorname{ord}_X f'(X, z_i) \leqslant r/2$. Лемма доказана. □

Замечание 3. Лемма 1 доказана для пары (i, j). Так что можно использовать более точное обозначение $\xi_{i,i,j} = \xi_i$, и $\xi_{j,i,j} = \xi_j$, т.е. ξ_i и ξ_j зависят от (i, j). Теперь из конструкции из доказательства леммы для пар (j, i) и (i, j) мы получаем $\gamma(i, j) = \gamma(j, i)$, $\xi_{i,j,i} = \xi_{i,i,j} = \xi_i$,

$\xi_{j,j,i} = \xi_{j,i,j} = \xi_j$ и, если $\xi_i \neq 0$ и $\xi_j \neq 0$, то $\mu(i,j) = \mu(j,i)$. Но, если $\xi_i = 0$ или $\xi_j = 0$, то $\mu(i,j) \neq \mu(j,i)$.

Пусть z_i – корень многочлена f. Применим лемму 1. Положим $\mu'(i,j) = \mu(i,j)$, если $\xi_i \neq 0$ и

$$\mu'(i,j) = \min\{\mathrm{ord}_X f'(X, z_i), \mathrm{ord}_X f^{(\gamma)}(X, z_i)\},$$

если $\xi_i = 0$. Так что $\mu(i,j) \leqslant \mu'(i,j) \leqslant r/2$ в любом случае. Теперь можно представить $\mu'(i,j) = \mu_1(i,j)/\nu(i)$, где $\mu_1(i,j) \in \mathbb{Z}$, $1 \leqslant \nu(i) \leqslant \deg_Z f$, $\nu(i) \in \mathbb{Z}$. Более точно, можно взять $\nu(i) = \nu_{i,n}$ в обозначениях из введения.

Определим множество индексов $A(i) = \{j \in \mathbb{Z} : 1 \leqslant j \neq i \leqslant \deg_Z f\}$. Положим

$$\mu = \mu(i) = \max\{\mu'(i,j) : j \in A(i)\}. \tag{19}$$

Следовательно, $\mu'(i,j) \leqslant \mu \leqslant r/2$ для всех пар (i,j) таких, что $i \neq j$. Для всякого $j \in A(i)$ существует целое число $\rho_{i,j}$ такое, что $\xi_i + \rho_{i,j} \neq 0$ и, если $\xi_i \neq 0$, то также $\xi_j + \rho_{i,j} \neq 0$. Фактически здесь можно выбрать $0 \leqslant \rho_{i,j} \leqslant 2$ (но позднее мы будем рассматривать другие значения $\rho_{i,j}$). Зафиксируем такие целые числа $\rho_{i,j}$. Положим $Q_{i,j} = X^{\mu-\mu'(i,j)} f^{(\gamma)}(X,Z) + \rho_{i,j} X^{\mu}$. Пусть $\varkappa_{i,j}$ и $\varkappa_i$ – целые числа. Определим многочлен

$$q = \delta_0 \sum_{j \in A(i)} \varkappa_{i,j} Q_{i,j} + \varkappa_i X^{\mu+1} Z \in K[X^{1/\nu(i)}, Z],$$

(так что q зависит от i).

Положим $\Omega[z] = \Omega[Z]/(f)$, где $z = Z \bmod f$. Тогда по китайской теореме об остатках мы имеем естественный изоморфизм Ω–алгебр $\Omega[z] \simeq \prod_{1 \leqslant i \leqslant \deg_Z f} \Omega[z_i]$, $z \mapsto \{z_i\}_{1 \leqslant i \leqslant \deg_Z f}$. Следующая лемма аналогична лемме 2.2 [4].

Лемма 2. *Существуют целые числа $0 \leqslant \varkappa_{i,j} \leqslant 2d-1$, $0 \leqslant \varkappa_i \leqslant d(d-1)/2$ такие, что для полинома q справедливы следующие утверждения.*

(i) *Существует элемент $0 \neq b_i \in \overline{K}$ такой, что $\mathrm{ord}_X(q(z_i) - b_i X^{\mu}) > \mu$.*

(ii) *Для всякого $j \in A(i)$ мы имеем $0 \leqslant \mathrm{ord}_X(q(z_j)) \leqslant \mu$ и, если $\mathrm{ord}_X(q(z_j)) = \mu$, то существует элемент $0 \neq b_j \in \overline{K}$ такой, что $\mathrm{ord}_X(q(z_j) - b_j X^{\mu}) > \mu$ и $b_j \neq b_i$.*

(iii) *Включение* $\Omega[z] \supset \Omega[q(z)]$ *является равенством, т.е.* $q(z)$ – *примитивный элемент сепарабельной алгебры* $\Omega[z]$.

(iv) $q \in \mathbb{Z}[T_1, \dots, T_l, \theta, X_1, \dots, X_{n-1}, X^{1/\nu(i)}, Z]$.

Доказательство. Утверждение (iv) следует из определения q, поскольку $f \in \Lambda[X_1, \dots, X_{n-1}, X, Z]$ и $\delta_0\Lambda \in \mathbb{Z}[T_1, \dots, T_l, \theta]$, см. выше.

Докажем утверждения (i) и (ii). Если $\xi_i \neq 0$, то $\mu'(i,j) = \mu(i,j)$, и согласно определениям $\rho_{i,j}$ и $Q_{i,j}$ мы имеем

$$\mathrm{ord}_Z Q_{i,j}(z_i) = \mathrm{ord}_Z Q_{i,j}(z_j) = \mu. \tag{20}$$

Если $\xi_i = 0$, то $\mu'(i,j) > \mu(i,j)$ и согласно определениям $\rho_{i,j}$ и $Q_{i,j}$ мы имеем $\mathrm{ord}_Z Q_{i,j}(z_i) = \mu$ и $\mathrm{ord}_Z Q_{i,j}(z_j) < \mu$. Поэтому в любом случае

$$\mathrm{ord}_Z Q_{i,j}(z_i) = \mu, \quad \mathrm{ord}_Z Q_{i,j}(z_j) \leqslant \mu, \tag{21}$$

В дальнейшем, чтобы избежать двусмысленности в доказательстве, мы будем использовать обозначения $\xi_{i,i,j}$, $\xi_{j,i,j}$, см. замечание 3, вместо ξ_i, ξ_j из леммы 1. Для всякого целого числа $1 \leqslant u \leqslant \deg_Z f$ положим $\omega(u) = \min\{\mathrm{ord}_Z Q_{i,j}(z_u) : j \in A(i)\}$. Следовательно, $\omega(u) \leqslant \mu$ для всякого u, и $\omega(i) = \mu$ согласно (21). Пусть $\mathrm{ord}(Q_{i,j}(z_u) - q_{u,i,j}X^{\omega(u)}) > \omega(u)$, где $q_{u,i,j} \in \overline{K}$ для всех u, i, j.

Покажем, что утверждения (i) и (ii) выполняются, если для всех $1 \leqslant u \leqslant \deg_Z f$

$$\sum_{j \in A(i)} \varkappa_{i,j} q_{u,i,j} \neq 0 \tag{22}$$

и для всякого $u \in A(i)$ такого, что $\omega(u) = \mu$,

$$\sum_{j \in A(i)} \varkappa_{i,j} (q_{i,i,j} - q_{u,i,j}) \neq 0. \tag{23}$$

Действительно, (22) справедливо в том и только в том случае, если $(\omega(u), 0) \in P(q(z_u))$. Если $u = i$, то отсюда следует (i) и, если $u \in A(i)$, то $0 \leqslant \mathrm{ord}_X(q(z_u)) \leqslant \mu$, т.е. справедлива первая часть утверждения (ii).

Если $u \in A(i)$, $\omega(u) = \mu$ и выполняется (23), то существует элемент $0 \neq b_u \in \overline{K}$ такой, что $\mathrm{ord}_X(q(z_u) - b_u X^\mu) > \mu$ и $b_u \neq b_i$, т.е. выполняется вторая часть утверждения (ii). Таким образом, утверждения (i) и (ii) выполняются, если справедливы (22) и (23) для всех $1 \leqslant u \leqslant \deg_Z f$.

Левые части неравенств (22) и (23) являются линейными формами от $\varkappa_{i,j}$ с коэффициентами из $\overline{K}$. Для всякого u существует $j \in A(i)$ такое, что $q_{u,i,j} \neq 0$, поскольку не все $Q_{i,j}(z_u)$, $j \in A(i)$, равны нулю. Именно по (21) мы имеем $Q_{i,u}(z_u) \neq 0$, если $u \in A(i)$, и $Q_{i,j}(z_i) \neq 0$ для всякого $j \in A(i)$, если $u = i$. Поэтому линейные формы в (22) – ненулевые.

Если $u \in A(i)$ и $\omega(u) = \mu$, то $\mu'(i,u) = \mu(i,u)$, $\xi_{i,i,u} \neq 0$, (20) истинно для $j = u$ и $q_{i,i,u} = \xi_{i,i,u} + \rho_{i,u}$, $q_{u,i,u} = \xi_{u,i,u} + \rho_{i,u}$. Поэтому $q_{i,i,u} - q_{u,i,u} = \xi_{i,i,u} - \xi_{u,i,u} \neq 0$ согласно лемме 1. Следовательно, линейные формы в (23) – ненулевые.

Произведение линейных форм (22) и (23) является полиномом степени самое большее $2d-1$. Следовательно, существуют значения $\varkappa_{i,j} \in \mathbb{Z}$, $0 \leqslant \varkappa_{i,j} \leqslant 2d-1$, для которых этот полином не обращается в нуль, и поэтому для этих значений выполняются утверждения (i) и (ii).

Теперь для того, чтобы удовлетворить дополнительно условию (iii), достаточно найти целое число $0 \leqslant \varkappa_i \leqslant d(d-1)/2$ такое, что элементы $q(z)^u$, $0 \leqslant u < \deg_Y f$, являются линейно независимыми над полем Ω. Пусть $q(z)^u = \sum_{0 \leqslant u < \deg_Z f} \lambda_{u,v} z^v$, где все $\lambda_{u,v} \in \overline{K}[\varkappa_i]$ (здесь мы рассматриваем $\varkappa_i$ как переменную). Тогда степень определителя $\deg_{\varkappa_i} \det(\lambda_{u,v}) = \deg_Z f(\deg_Z f - 1)/2$. Следовательно, требуемое целое число $\varkappa_i$ существует. Лемма доказана. $\square$

Для краткости обозначим $\nu = \nu_{i,n}$ и

$$\Lambda_0 = \mathbb{Z}[T_1, \ldots, T_l, \theta, X_1, \ldots, X_{n-1}], \quad \Lambda_1 = \Lambda[X_1, \ldots, X_{n-1}].$$

Следовательно, $\Lambda_0 \subset \Lambda_1 \subset K$, кольцо Λ_1 целозамкнуто, Λ_1 цело над Λ_0 и $\delta_0 \Lambda_1 \subset \Lambda_0$.

Пусть Q – новая переменная. Положим $R = \delta_0 \mathrm{Res}_Z(Q - q, f) \in \Omega[Q]$ равным результанту многочленов $Q - q$ и f относительно Z, умноженному на δ_0. Следовательно, $R \in \Lambda_0[X^{1/\nu}, Q] \subset \Omega[Q]$, и старший коэффициент $\mathrm{lc}_Q R = \delta_0$. Многочлены $q(z_u) - q$ и f имеют общий корень $Z = z_u$ для всякого $1 \leqslant u \leqslant \deg_Z f$, и $\deg_Q R = \deg_Z f = \dim_\Omega \Omega[z]$. Поэтому R является минимальным полиномом элемента $q(z) \in \Omega[z]$ над полем Ω.

Степени $\deg_{T_1,\ldots,T_l} R \leqslant d_2 \mathcal{P}(d, d_1)$, $\deg_{X_1,\ldots,X_{n-1}} R \leqslant D\mathcal{P}(d)$, $\deg_X R \leqslant D\mathcal{P}(d)$, $\deg_Q R = \deg_Z f \leqslant d$, и длина записи целых коэффициентов $\mathrm{l}(R) \leqslant M\mathcal{P}(d, d_1)$.

Согласно лемме 2 существует ребро $e \in E(R)$ с коэффициентом наклона $\beta(e)/\alpha(e) = \mu$, все корни многочлена $R^*(1, \mu)$ – ненулевые и

$b_i = q(z_i)^*$ является корнем многочлена $R^*(1,\mu)$ кратности один[6], и $\mathrm{ord}_X q(z_i) = \mu$. В данной ситуации коэффициенты разложения Ньютона–Пюизе элемента $q(z_i)$ получаются при помощи конструкции аналогичной лемме Гензеля.

Многочлен $R^*(1,\mu) \in \Lambda_0[Q] \subset K[Q]$. Положим $B_1 = \mathrm{lc}_Q R^*(1,\mu) \in \Lambda_0$ и $B = \delta_0 B_1 \in \Lambda_0$. Положим $b = Bb_i \in \overline{K}$ (так что B_1, B и b зависят от i). Тогда $B_1 b_i$ цело над Λ_0. Обозначим через $\widetilde{\Phi} \in K[Q]$ минимальный многочлен элемента $B_1 b_i$ над полем K такой, что старший коэффициент $\mathrm{lc}_Q \widetilde{\Phi} = 1$. Тогда $\widetilde{\Phi} \in \Lambda_1[Q]$. Поэтому $\delta_0 \widetilde{\Phi} \in \Lambda_0[Q]$ также является минимальным многочленом элемента $B_1 b_i$. Положим $\widetilde{d} = \deg_Q \widetilde{\Phi}$ и $\Phi = \delta_0^{\widetilde{d}} \widetilde{\Phi}(Q/\delta_0)$. Теперь $\Phi \in \Lambda_0[Q]$ – минимальный многочлен элемента b, и старший коэффициент $\mathrm{lc}_Q \Phi = 1$.

Согласно оценкам для неприводимых множителей многочленов от многих переменных и данным выше определениям мы имеем $\deg_{T_1,\dots,T_l} \widetilde{\Phi} \leqslant d_2 \mathcal{P}(d, d_1)$, $\deg_{X_1,\dots,X_{n-1}} \widetilde{\Phi} \leqslant D\mathcal{P}(d)$, $\deg_Q \widetilde{\Phi} \leqslant d$, $\mathrm{l}(\widetilde{\Phi}) \leqslant M\mathcal{P}(d, d_1)$. Оценки для длин записи целых коэффициентов неприводимых множителей многочленов от многих переменных см. в лемме II §4 глава III [1] для случая многочленов с целыми коэффициентами и в [2] в общем случае. Для многочлена Φ справедливы те же самые оценки, что и для $\widetilde{\Phi}$.

Многочлен $B^{\deg_Q R} R(Q + b_i X^\mu) \in \Lambda_0[b][X^{1/\nu}, Q]$. Обозначим через $\widetilde{a}$ коэффициент при Q многочлена $B^{\deg_Q R} R(Q + b_i X^\mu)^*(1,\mu)$. Следовательно, $\widetilde{a} \in \Lambda_0[b]$. Через $N = N_{K[b]/\mathbb{Q}(T_1,\dots,T_l,X_1,\dots,X_{n-1})}$ обозначим отображение нормы расширения полей $K[b] \supset \mathbb{Q}(T_1,\dots,T_l,\, X_1,\dots,X_{n-1})$. Положим $a = N(\widetilde{a})$ равным норме элемента $\widetilde{a}$. Тогда $a \in \mathbb{Z}[T_1,\dots,T_l,X_1,\dots,X_{n-1}]$. Далее, $a/\widetilde{a} \in \Lambda_0[b]$, поскольку многочлены $\varphi \in \mathbb{Z}[T_1,\dots,\, T_l, Z]$, $\Phi \in \mathbb{Z}[T_1,\dots,T_l,\theta,\, X_1,\dots,X_{n-1},Q]$ и $\mathrm{lc}_X \varphi = 1$, $\mathrm{lc}_Q \Phi = 1$ (здесь мы оставляем подробности читателю; для вычисления $N(a)$ можно использовать транзитивность норм расширений полей $K[b](X_1,\dots,\, X_{n-1}) \supset K(X_1,\dots,X_{n-1}) \supset \mathbb{Q}(T_1,\dots,T_l,X_1,\, \dots,X_{n-1})$ и представить нормы элементов как значения некоторых результантов полиномов; фактически эта конструкция хорошо известна).

[6]В §2 [4] мы утверждали, что “многочлен $R^*(1,\mu)(Q)$ не имеет кратных корней”. Однако это не верно в общем случае. Фактически мы имели там в виду, что “все корни многочлена $R^*(1,\mu)$ – ненулевые, и b_i – корень полинома $R^*(1,\mu)$ кратности 1”. Только то, что b_i – корень полинома $R^*(1,\mu)$ кратности 1, используется в [4].

Мы имеем $\deg_{T_1,\dots,T_l} a \leqslant d_2\mathcal{P}(d,d_1)$, $\deg_{X_1,\dots,X_{n-1}} a \leqslant D\mathcal{P}(d)$, $\mathrm{l}(a) \leqslant M\mathcal{P}(d,\, d_1)$. Аналогичные оценки справедливы для элементов $\widetilde{a}$ и $a/\widetilde{a}$.

Положим $\widetilde{R} = (a/\widetilde{a})B^{\deg_Q R}R(Q + b_iX^\mu) \in \Omega[Q]$. Теперь $\widetilde{R} \in \Lambda_0[b][X^{1/\nu}, Q]$. Более того, Q делит $\widetilde{R}^*(1,\mu)$, и коэффициент при Q многочлена $\widetilde{R}^*(1,\mu)$ равен a.

Степени $\deg_{T_1,\dots,T_l} \widetilde{R} \leqslant d_2\mathcal{P}(d,d_1)$, $\deg_{X_1,\dots,X_{n-1}} \widetilde{R} \leqslant D\mathcal{P}(d)$, $\deg_X \widetilde{R} \leqslant D\mathcal{P}(d)$, $\deg_Q \widetilde{R} = \deg_Z f \leqslant d$, и длины записей целых коэффициентов $\mathrm{l}(\widetilde{R}) \leqslant M\mathcal{P}(d,d_1)$.

Теперь согласно алгоритму Ньютона-Пюизе можно представить

$$q(z_i) = \sum_{0\leqslant j\in\mathbb{Z}} h_jX^{(j+\mu\nu)/\nu},$$

где $h_j \in K[b]$, $h_0 = b_i$. Далее,

$$\widetilde{R}/(Q + b_iX^\mu - q(z_i)) = \sum_{0\leqslant j\in\mathbb{Z}} g_j(X^{-\mu}Q)X^{(j+\omega)/\nu},$$

$$\widetilde{R} = \sum_{0\leqslant j\in\mathbb{Z}} r_j(X^{-\mu}Q)X^{(j+\omega+\mu\nu)/\nu},$$

где $g_j, r_j \in K[b][Z]$, $\omega \in \mathbb{Z}$, $\omega/\nu + \mu = \mathrm{ord}_{1,\mu}(\widetilde{R})$, степени $\deg_Z g_j < \deg_Q \widetilde{R}$, $\deg_Z r_j \leqslant \deg_Q \widetilde{R}$ для всех $0 \leqslant j \in \mathbb{Z}$. Кроме того, $r_0(Q) = \widetilde{R}^*(1,\mu)(Q)$, $g_0(Q) = \widetilde{R}^*(1,\mu)(Q)/Q$. Положим $g = \widetilde{R}/(Q+b_iX^\mu-q(z_i))$. Так что $g_0(0) = a$, и коэффициент при Q многочлена r_0 равен a.

ЛЕММА 3 *Для всякого* $j \geqslant 1$

$$a^{2j-1}g_j, a^{2j-1}h_j \in \Lambda_0[b]\,[Z],$$

Положим $\overline{g}_j = a^{2j-1}g_j$, $\overline{h}_j = a^{2j-1}h_j$. *Тогда степени* $\deg_{T_1,\dots,T_l} \overline{g}_j$, $\deg_{T_1,\dots,T_l} \overline{h}_j \leqslant (2j-1)d_2\mathcal{P}(d,d_1)$, $\deg_{X_1,\dots,X_{n-1}} \overline{g}_j$, $\deg_{X_1,\dots,X_{n-1}} \overline{h}_j \leqslant (2j-1)D\mathcal{P}(d)$, *и длины записи целых коэффициентов* $\mathrm{l}(\overline{g}_j)$, $\mathrm{l}(\overline{h}_j) \leqslant (2j-1)\log_2(j+1)M\mathcal{P}(d,d_1)$.

Доказательство. Положим $\overline{r}_j = a^{2j-2}r_j$, $\overline{g}_{j,0} = \overline{g}_j(0)$, $\overline{r}_{j,0} = \overline{r}_j(0)$ для всякого $j \geqslant 1$. Тогда из равенства $(Q-\sum_{j\geqslant 1} h_jX^{j/\nu+\mu})g = \widetilde{R}$ вытекает, что

$$Z\overline{g}_j - \overline{h}_jg_0 = a\overline{r}_j + a\sum_{0<w<j} \overline{g}_w\overline{h}_{j-w}$$

$j \geqslant 1$. Следовательно,

$$\overline{h}_j = -\overline{r}_{j,0} - \sum_{0<w<j} \overline{g}_{w,0}\overline{h}_{j-w,0},$$

$$\overline{g}_j = -\Big(\overline{r}_{j,0} - \sum_{0<w<j} \overline{g}_{w,0}\overline{h}_{j-w,0}\Big)g_0 + a\Big(\overline{r}_j + \sum_{0<w<j} \overline{g}_w\overline{h}_{j-w}\Big)\Big/Z.$$

Из этих формул с помощью индукции по j мы доказываем требуемые утверждения. Лемма доказана. $\square$

Пусть $N_{K/\mathbb{Q}(T_1,\ldots,T_l)}$ – отображение нормы расширения полей $K \supset \mathbb{Q}(T_1, \ldots, T_l)$, мы будем использовать то же самое обозначение для отображения нормы расширения

$$K(X_1,\ldots,X_{n-1},X^{1/\nu}) \supset \mathbb{Q}(T_1,\ldots,T_l,X_1,\ldots,X_{n-1},X^{1/\nu}).$$

Положим $B^{(0)} = N_{K/\mathbb{Q}(T_1,\ldots,T_l)}(B) \in \mathbb{Z}[T_1,\ldots,T_l,X_1,\ldots,X_{n-1}]$ и $B^{(1)} = B^{(0)}/B$. Следовательно, $B^{(1)} \in \mathbb{Z}[T_1,\ldots,T_l,\theta,X_1,\ldots,X_{n-1}]$. Теперь $b/B = (bB^{(1)})/B^{(0)}$, т.е. можно сделать знаменатель коэффициента при X^μ в разложении $q(z_i)$ равным элементу из кольца

$$\mathbb{Z}[T_1,\ldots,T_l,X_1,\ldots,X_{n-1}].$$

Степени $\deg_{T_1,\ldots,T_l} B^{(v)} \leqslant d_2\mathcal{P}(d,d_1)$, $\deg_{X_1,\ldots,X_{n-1}} B^{(v)} \leqslant D\mathcal{P}(d)$, и длины записей целых коэффициентов $l(B^{(v)}) \leqslant M\mathcal{P}(d,d_1)$ для $v = 1,2$.

Таким образом, в итоге можно представить

$$q(z_i) = (bB^{(1)}/B^{(0)})X^\mu + \sum_{1\leqslant j\in\mathbb{Z}} (\overline{h}_j/a^{2j-1})X^{(j/\nu)+\mu}, \tag{24}$$

где все элементы $\overline{h}_j \in \mathbb{Z}[T_1,\ldots,T_l,\theta,X_1,\ldots,X_{n-1},b]$.

Напомним, что $q(z)$ является примитивным элементом алгебры $\Omega[z]$ над Ω и $\nu = \nu_{i,n} = \nu(i)$. Поэтому, решая линейную систему над полем $K(X^{1/\nu})$ по правилу Крамера, можно представить

$$z = (1/\delta) \sum_{0\leqslant v<\deg_Z f} a_j q(z)^w,$$

где все элементы $\delta, a_v \in \mathbb{Z}[T_1,\ldots,T_l,\theta,X_1,\ldots,X_{n-1},X^{1/\nu}]$. Следовательно,

$$z_i = (1/\delta) \sum_{0\leqslant v<\deg_Z f} a_v q(z_i)^v. \tag{25}$$

Более того, заменяя δ на норму $\delta^{(0)} = N_{K/\mathbb{Q}(T_1,\dots,T_l)}\delta$ и a_j на $a_j\delta^{(0)}/\delta$, мы можем без ограничения общности предполагать дополнительно, что $\delta \in \mathbb{Z}[T_1,\dots,T_l,X_1,\dots,X_{n-1},X^{1/\nu}]$.

Теперь степени $\deg_{T_1,\dots,T_l}\delta \leqslant d_2\mathcal{P}(d,d_1)$, $\deg_{X_1,\dots,X_{n-1}}\delta \leqslant D\mathcal{P}(d)$, $\deg_X \delta \leqslant D\mathcal{P}(d)$, длины записей целых коэффициентов $\mathrm{l}(\delta) \leqslant M\mathcal{P}(d,d_1)$. Такие же оценки справедливы для всех коэффициентов a_v.

В результате, используя (24) и (25), можно представить

$$z_i = z_{i,0} + \sum_{w\geqslant 1} z_{i,w}X^{w/\nu}, \tag{26}$$

где все коэффициенты $z_{i,0}, z_{i,w} \in K[b]$.

Положим $\lambda = \mathrm{ord}_X\delta$, $w_0 = \nu\lambda$ и

$$\Delta = \Delta_i = a^2\delta^*(1,0)^2(B^{(0)})^{d-1} \in \mathbb{Z}[T_1,\dots,T_l,X_1,\dots,X_{n-1}].$$

Следовательно, $w_0 \leqslant D\mathcal{P}(d)$.

Заметим, что

$$\begin{aligned}
&X^\lambda/\delta \in (1/\delta^*(1,0))\Lambda_0[[X^{1/\nu}/\delta^*(1,0)]] \subset (1/\delta^*(1,0))\Lambda_0 + \Lambda_0[[X^{1/\nu}/\Delta]],\\
&q(z_i)^j \in (1/(B^{(0)})^{d-1})\Lambda_0[b][[X^{1/\nu}/a^2]] \subset\\
&(1/(B^{(0)})^{d-1})\Lambda_0[b] + \Lambda_0[b][[X^{1/\nu}/\Delta]], \quad 0 \leqslant j < \deg_Z f,\\
&(X^\lambda/\delta^*(1,0))(1/(B^{(0)})^{d-1})\Lambda_0 \subset (1/\Delta)\Lambda_0.
\end{aligned}$$

Поэтому $z_i \in (1/(X^\lambda\Delta))\Lambda_0[b] + (1/X^\lambda)\Lambda_0[b][[X^{1/\nu}/\Delta]]$. Мы имеем $\mathrm{ord}_X z_i \geqslant 0$. Отсюда вытекает, что $z_i - z_{i,0} \in (1/\Delta^{w_0})(\Lambda_0[b][[X^{1/\nu}/\Delta]] \setminus \Lambda_0[b])$ и $z_{i,0} \in (1/\Delta^{\max\{1,w_0\}})\Lambda_0[b]$.

Следовательно, существуют элементы $\overline{z}_{i,w} \in \Lambda_0[b]$, $w \geqslant 0$, такие, что $z_{i,w} = \overline{z}_{i,w}/\Delta^{\max\{1,w+w_0\}}$ для всех $w \geqslant 0$ (здесь мы оставляем подробности читателю). Далее, имеют место представления (13) раздел 1 с $u = i$, $\varphi_u = \Phi$, где все $\overline{z}_{i,w,v_1,v_2} \in \mathbb{Z}[T_1,\dots,T_l,X_1,\dots,X_{n-1}]$.

Мы имеем

$$\begin{aligned}
&\deg_{T_1,\dots,T_l}\Delta \leqslant d_2\mathcal{P}(d,d_1), \quad \deg_{X_1,\dots,X_{n-1}}\Delta \leqslant D\mathcal{P}(d),\\
&\mathrm{l}(\Delta) \leqslant M\mathcal{P}(d,d_1).
\end{aligned} \tag{27}$$

Далее, для всех $1 \leqslant i \leqslant \deg_Z f$ и $w \geqslant 0$, $0 \leqslant v_1 < \deg_Z\varphi$, $0 \leqslant v_2 < \deg_Z\Phi$ степени и длины записей целых коэффициентов

$$\begin{aligned}
&\deg_{T_1,\dots,T_l}\overline{z}_{i,w,v_1,v_2} \leqslant (w+w_0+1)d_2\mathcal{P}(d,d_1),\\
&\deg_{X_1,\dots,X_{n-1}}\overline{z}_{i,w,v_1,v_2} \leqslant (w+w_0+1)D\mathcal{P}(d),\\
&\mathrm{l}(\overline{z}_{i,w,v_1,v_2}) \leqslant ((w+w_0+1)\log_2(w+w_0+1))M\mathcal{P}(d,d_1).
\end{aligned} \tag{28}$$

§3. Доказательство теоремы 2: алгоритм

В этом разделе мы предполагаем аналогично тому, как это было в разделе 2, что многочлен f сепарабелен. До сих пор описываемая конструкция была экзистенциональной. Теперь мы собираемся показать, как получить многочлен Φ и разложения (24), (25), (26) при помощи алгоритма. Сначала можно построить для всех $1 \leqslant u \leqslant \deg_Z f$ начальные члены разложения (17), применяя алгоритм Ньютона-Пюизе в его классической форме. Алгоритм рекурсивен по $v \geqslant 0$. С помощью ломаных Ньютона и алгоритма для факторизации многочленов из [2] и [7] мы строим последовательно для всякого u для $v = 0, 1, 2, \ldots, v_u$ (мы уточним v_u позже) следующие объекты. Конечное расширение полей $K_{u,v} = K[\eta_{u,v}] \supset K$, где $\eta_{u,v}$ – примитивный элемент поля $K_{u,v}$ над K. Он задан своим минимальным полиномом $\varphi_{u,v} \in K[Z]$ над K. Этот полином $\varphi_{u,v}$ строится. Следовательно, $K_{u,v} = K[Z]/(\varphi_{u,v})$, $\eta_{u,v} = Z \bmod \varphi_{u,v}$. Коэффициенты $r_{u,0}, \ldots, r_{u,v} \in K[Z]/(\varphi_{u,v})$ и представления элементов $r_{u,0}, \ldots, r_{u,v}$ в базисе $\{\eta_{u,v}^w\}_{0 \leqslant w < \deg_Z \varphi_{u,v}}$ строятся алгоритмом. Более того, $K_{u,v} = K[r_{u,0}, \ldots, r_{u,v}]$ и $\eta_{u,v} = c_{u,0} r_{u,0} + \ldots + c_{u,v} r_{u,v}$ для некоторых целых чисел $c_{u,0}, \ldots, c_{u,v}$ с длинами записи $O(d^2)$. Эти целые числа строятся. Рациональные числа $\varepsilon_{u,0}, \ldots, \varepsilon_{u,v}$ строятся. Если наборы из v элементов $(r_{u,0}, \ldots, r_{u,v})$ и $(r_{u_1,0}, \ldots, r_{u_1,v})$ сопряжены над K и $\varepsilon_{u,0} = \varepsilon_{u_1,0}, \ldots, \varepsilon_{u,v} = \varepsilon_{u_1,v}$, то дополнительно $c_{u,0} = c_{u_1,0}, \ldots, c_{u,v} = c_{u_1,v}$. Поэтому в этом случае $\varphi_{u,v} = \varphi_{u_1,v}$, т.е. элементы $\eta_{u,v}$ и $\eta_{u_1,v}$ сопряжены над K. Более подробно см., например, в §1 [4] (там рассмотрен случай $n = 1$, но сам алгоритм по существу – тот же самый для произвольного основного поля нулевой характеристики). Более формально, в §1 [4] описано дерево корней, возникающее в алгоритме Ньютона–Пюизе. Однако слишком формальное изложение не помогает лучшему пониманию сути, и в данной статье мы хотели бы избежать этого.

Более точно, предположим, что $\operatorname{ord}_X(z_u - \sum_{0 \leqslant w < v} r_{u,w} X^{\varepsilon_{u,w}}) \leqslant r/2$ для некоторого u. Это условие может быть проверено, если рассмотреть ломаную Ньютона полинома $f(X, Z + \sum_{0 \leqslant w < v} r_{u,w} X^{\varepsilon_{u,w}})$ (последний полином известен из предыдущих шагов рекурсии). Тогда мы переходим к следующему v-ому шагу рекурсии для данного u. На этом шаге мы строим элементы $\varphi_{u,v} \in \mathbb{Z}[T_1, \ldots, T_l, \eta, X_1, \ldots, X_{n-1}, Z]$, $\operatorname{lc}_Z \varphi_{u,v} = 1$, $\varepsilon_{u,v}$ и $r_{u,v}$. Далее, элементы $r_{u,w}$, $0 \leqslant w \leqslant v$, представляются в виде $\overline{r}_{u,w}/\Delta_{u,v}^{\alpha_{v,w}}$, где $\Delta_{u,v} \in \mathbb{Z}[T_1, \ldots, T_l, X_1, \ldots, X_{n-1}]$, все $\overline{r}_{u,w} \in \mathbb{Z}[T_1, \ldots, T_l, \eta, X_1, \ldots, X_{n-1}, \eta_{u,v}]$ и $\alpha_{v,w} \in \mathbb{Z}$, $1 \leqslant \alpha_{v,w} \leqslant \varepsilon_{u,w} d$.

Для всех $1 \leqslant u \leqslant \deg_Z f$, $0 \leqslant w \leqslant v$ мы имеем оценки (27), (28) (только существование этих неравенств известно сейчас) для элементов $r_{u,v}$ в базисе $\{\theta^{v_1}\eta_{u,v}^{v_2}\}$, $0 \leqslant v_1 < \deg_Z \varphi$, $0 \leqslant v_2 < \deg_Z \varphi_{u,v}$, над полем $\mathbb{Q}(T_1, \ldots, T_l, X_1, \ldots, X_{n-1}, X^{1/\nu_{u,n}})$. Теперь используя (27), (28) и линейную алгебру, т.е. решая линейные системы, мы получаем следующие оценки.

$$\begin{aligned}
&\deg_{T_1,\ldots,T_l} \varphi_{u,v} \leqslant (D+\varepsilon_{u,v})d_2\mathcal{P}(d,d_1),\\
&\deg_{X_1,\ldots,X_{n-1}} \varphi_{u,v} \leqslant (D+\varepsilon_{u,v})D\mathcal{P}(d),\\
&\mathrm{l}(\varphi_{u,v}) \leqslant ((D+\varepsilon_{u,v})\log_2(D+\varepsilon_{u,v}))M\mathcal{P}(d,d_1),\\
&\deg_{T_1,\ldots,T_l} \Delta_{u,v} \leqslant (D+\varepsilon_{u,v})d_2\mathcal{P}(d,d_1),\\
&\deg_{X_1,\ldots,X_{n-1}} \Delta_{u,v} \leqslant (D+\varepsilon_{u,v})D\mathcal{P}(d),\\
&\mathrm{l}(\Delta_{u,v}) \leqslant ((D+\varepsilon_{u,v})\log_2(D+\varepsilon_{u,v}))M\mathcal{P}(d,d_1),
\end{aligned} \tag{29}$$

и

$$\begin{aligned}
&\deg_{T_1,\ldots,T_l} \overline{r}_{u,w} \leqslant (D+\varepsilon_{u,v})d_2\mathcal{P}(d,d_1),\\
&\deg_{X_1,\ldots,X_{n-1}} \overline{r}_{u,w} \leqslant (D+\varepsilon_{u,v})D\mathcal{P}(d,d_1),\\
&\mathrm{l}(\overline{r}_{u,w}) \leqslant ((D+\varepsilon_{u,v})\log_2(D+\varepsilon_{u,v}))M\mathcal{P}(d,d_1).
\end{aligned} \tag{30}$$

(здесь мы оставляем подробности читателю).

Таким образом, v_u – последний шаг рекурсии для рассматриваемого u в том и только в том случае, если $\mathrm{ord}_X\big(z_u - \sum_{0\leqslant w\leqslant v_u} r_{u,w}X^{\varepsilon_{u,w}}\big) > r/2$. Время работы алгоритма для построения всех φ_{u,v_u}, Δ_{u,v_u} и всех $\varepsilon_{u,v}$, $\overline{r}_{u,w}$, $0 \leqslant w \leqslant v_u$, $1 \leqslant u \leqslant \deg_Z f$, полиномиально от M_1, M_2, $(Ddd_1d_2)^{l+1}$, $(dD)^n$.

Заметим, что $\nu_{u,n} = \nu(u)$ равно наименьшему целому числу $\nu \geqslant 1$ такому, что $\nu\varepsilon_{u,w} \in \mathbb{Z}$ для всех $0 \leqslant w \leqslant v_u$. Так что $\nu_{u,n}$ может быть вычислено для всякого u.

Конечно, можно продолжить рекурсию для $v > v_u$ с $K_{u,v} = K_{u,v_u}$, $\varphi_{u,v} = \varphi_{u,v_u}$ (т.е. можно взять все $c_{u,w} = 0$ для $w > v_u$), $\Delta_{u,v} = \Delta_{u,v_u}$. Оценки (30) справедливы также для $v > v_u$. Теперь время работы алгоритма для построения всех $\overline{r}_{u,w}$, $0 \leqslant w \leqslant v$, $1 \leqslant u \leqslant \deg_Z f$, полиномиально от M_1, M_2, $(Ddd_1d_2)^{l+1}$, $(dD)^n$, v^{l+n}.

Пусть $\iota \geqslant 0$ – произвольное целое число. Покажем, как построить для всех $1 \leqslant i \leqslant \deg_Z f$ элементы $q, \Phi, b, B^{(0)}, B^{(0)}, \Delta, w_0, \overline{z}_{i,w,v_1,v_2}$, для всех $0 \leqslant w \leqslant \iota$, см. выше раздел 3 (эти элементы зависят от i). Положим $z_i^{(1)} = \sum_{0\leqslant\gamma\leqslant v_i} r_{i,\gamma}X^{\varepsilon_{i,\gamma}} \in K_{i,v_i}[X^{1/\nu_{i,n}}]$. Для всех $1 \leqslant m \leqslant -1 + \deg_Z f$ мы вычисляем $\mathrm{ord}_X(f^{(m)}(X, z_i^{(1)}))$ и строим $f^{(m)}(X, z_i^{(1)})^*(1,0) \in K_{i,v_i}$. Это позволяет нам найти ломаную Ньютона $E(f(X, Z + z_i^{(1)}))$

многочлена $f(X, Z + z_i^{(1)})$ и для всякого ребра $e \in E(f(X, Z + z_i^{(1)}))$ построить многочлен $f(X, Z + z_i^{(1)})^*(1, \beta(e)/\alpha(e))$. Обозначим через $E'(f(X, Z+z_i^{(1)}))$ подмножество всех рёбер $e \in E(f(X, Z+z_i^{(1)}))$ таких, что $\deg_Z f(X, Z + z_i^{(1)})^*(1, \beta(e)/\alpha(e)) \geqslant 2$.

Если $\operatorname{ord}_X(f^{(m)}(X, z_i^{(1)})) \leqslant r/2$, то

$$\operatorname{ord}_X(f^{(m)}(X, z_i)) = \operatorname{ord}_X(f^{(m)}(X, z_i^{(1)}))$$

и

$$f^{(m)}(X, z_i^{(1)})^*(1, 0) = f^{(m)}(X, z_i^{(1)})^*(1, 0) \in K_{i,v_i},$$

поскольку $\operatorname{ord}_X(z_i - z_i^{(1)}) > r/2$, см. выше. Следовательно, для ломаной Ньютона $E(f(X, Z + z_i))$ полинома $f(X, Z + z_i)$ мы имеем

$$E(f(X, Z + z_i) = E'(f(X, Z + z_i^{(1)}).$$

Более того, если $e \in E(f(X, Z + z_i))$, то

$$f(X, Z + z_i)^*(1, \beta(e)/\alpha(e)) = f(X, Z + z_i^{(1)})^*(1, \beta(e)/\alpha(e)) \in K_{i,v_i}[Z]$$

Таким образом, строятся эти многочлены $f(X, Z + z_i)^*(1, \beta(e)/\alpha(e))$, $e \in E(f(X, Z + z_i))$. Для краткости обозначим

$$f_e^* = f(X, Z + z_i)^*(1, \beta(e)/\alpha(e)).$$

Для всякого ребра $e \in E(f(X, Z + z_i))$ положим

$$\gamma = \gamma(e) = -1 + \deg_Z f(X, Z + z_i)^*(1,$$

$\beta(e)/\alpha(e))$ и $\widetilde{\xi}_e$ равным коэффициенту при Z^γ полинома f_e^*. Положим $\xi_e = \gamma!\,\xi_e$. Обозначим через $\mu(e)$ рациональное число такое, что точка $(\mu(e), \gamma) \in s(e)$. Теперь $\xi_e \neq 0$ в том и только в том случае, если $\operatorname{ord}_X(f^{(\gamma)}(X, z_i)) = \mu(e)$.

Положим $\mu'(e) = \mu(e)$, если $\xi_e \neq 0$ и $\mu'(e) = \min\{\operatorname{ord}_X(f^{(\gamma)}(X, z_i)), \operatorname{ord}_X(f'(X, z_i))\}$, если $\xi_e = 0$.

Предположим, что $\xi_e \neq 0$. Тогда мы вычисляем бесквадратную часть $g_e \in K_{i,v_i}[Z]$ многочлена f_e^*. Заметим, что Z делит g_e, и $\deg g_e \geqslant 2$. Положим $y = Z \bmod g_e \in K_{i,v_i}[Z]/(g_e)$. Пусть a_e равен коэффициенту при $Z^{\gamma-1}$ многочлена f_e^*. Мы находим целое число $0 \leqslant \rho_e \leqslant \deg_Z g_e$ такое, что

$$(\gamma + 1)y\operatorname{lc}_Z f_e^* + a_e + \rho_e/\gamma! \tag{31}$$

не является делителем нуля в алгебре $K_{i,v_i}[Z]/(g_e)$.

Предположим, что $\xi_e = 0$ и $\operatorname{ord}_X(f^{(\gamma)}(X, z_i)) \leqslant \operatorname{ord}_X(f'(X, z_i))$. Тогда полагаем $\rho_e = 0 \in \mathbb{Z}$.

Предположим, что $\xi_e = 0$ и $\mathrm{ord}_X(f^{(\gamma)}(X, z_i)) > \mathrm{ord}_X(f'(X, z_i))$. Тогда полагаем $\rho_e = 1 \in \mathbb{Z}$.

Положим $\mu' = \max\{\mu'(e) : e \in E(f(X, Z + z_i))\}$ и

$$Q_e = X^{\mu'-\mu'(e)} f^{(\gamma)}(X, Z)) + \rho_e X^{\mu} \in K[X^{1/\nu(i)}, Z].$$

Мы строим все элементы Q_e.

Для всякого $e \in E(f(X, Z + z_i))$ обозначим через J_e множество всех j таких, что $1 \leqslant j \leqslant \deg_Z f$ и $\mathrm{ord}_X(z_j - z_i) = \beta(e)/\alpha(e)$.

Далее мы используем обозначения ξ_i, ξ_j, $\rho_{i,j}$, $\mu(i, j)$, $\mu'(i, j)$ из раздела 2. Теперь $\xi_i = \xi_e$ и для всякого $j \in J_e$ элемент $\widetilde{\xi}_j$ является коэффициентом при X^{γ} многочлена $f(X, Z+z_j)^*(1, \beta(e)/\alpha(e))$. Для всякого $j \in J_e$ положим $\rho_{i,j} = \rho_e$. Тогда мы имеем $\mu(i, j) = \mu(e)$, $\mu'(i, j) = \mu'(e)$, $\mu = \mu(i) = \mu'$ (см. (19)) и $Q_{i,j} = Q_e$. Кроме того, для всякого $j \in J_e$ мы имеем $\xi_i + \rho_{i,j} \neq 0$ и, если $\xi_i \neq 0$, то $\xi_j + \rho_{i,j} \neq 0$. Последнее утверждение справедливо, поскольку элемент (31) не является делитем нуля в алгебре $K_{i,v_i}[Z]/(g_e)$.

Пусть $\varkappa_e$ и $\varkappa_i$ – целые числа. Положим

$$q = \delta_0 \sum_{e \in E'(f(X, Z+z^{(1)}))} \varkappa_e Q_e + \varkappa_i X^{\mu+1} Z \in K[X^{1/\nu(i)}, Z]. \tag{32}$$

Следующая лемма аналогична лемме 2.

Лемма 4. *Существуют целые числа* $0 \leqslant \varkappa_e \leqslant 2d - 1$, $0 \leqslant \varkappa_i \leqslant d(d-1)/2$ *такие, что справедливы утверждения (i)–(iv) леммы 2 для* q*, определённого согласно (32).*

Доказательство. Оно аналогично доказательству леммы 2. Лемма доказана. □

Теперь мы можем построить элемент q. Пусть

$$z = Z \bmod f \in K(X^{1/\nu(i)})[Z]/(f).$$

Пусть $E(f(X, Z+z_i)) = \{e_1, \ldots, e_m\}$ и число элементов $\#E(f(X, Z+z_i)) = m$. Положим $q_v = \delta_0 \sum_{1 \leqslant w \leqslant v} \varkappa_w Q_w$, $0 \leqslant v \leqslant m$ (так что $q_0 = 0$). При помощи рекурсии по v мы строим последовательно элементы q_v, $v = 1, 2, \ldots, m$ следующим образом. Положим $q_{v,m} = q_{v-1} + m\delta_0 Q_{e_v} \in K[X^{1/\nu(i)}, Z]$, $0 \leqslant m \leqslant 2d-1$. Для всякого $0 \leqslant m \leqslant 2d-1$ мы строим минимальный многочлен $\Psi_{v,m} \in K(X^{1/\nu(i)})[Z]$ элемента $q_{v,m}(X^{1/\nu(i)}, z) \in K(X^{1/\nu(i)})[Z]/(f)$ над полем $K(X^{1/\nu(i)})$ такой, что старший коэффициент $\mathrm{lc}_Z \Psi_{v,m} = 1$. Тогда фактически $\Psi_{v,m} \in K[X^{1/\nu(i)}, Z]$. После

этого мы вычисляем многочлен $\Psi^*_{v,m}(1,\mu) \in K[Z]$ и его бесквадратную часть $g_{v,m} \in K[Z]$. Мы выбираем m_0 таким, что $\deg_Z g_{v,m_0} = \max\{\deg_Z g_{v,m} : 0 \leqslant m \leqslant 2d-1\}$. Положим $\varkappa_{e_v} = m_0$ и $q_v = q_{v,m_0}$. Так что на каждом шаге рекурсии число значений $q_v(z_j)$, $1 \leqslant j \leqslant \deg_Z f$, таких, что $\operatorname{ord}_X q(z_j) = \mu$ является максимально возможным.

Наконец, мы вычисляем минимальные многочлены $\Phi_{2d-1,m}$ всех элементов $q_{2d-1}(X^{1/\nu(i)}, z) + mX^\mu z$, $0 \leqslant m \leqslant d(d-1)/2$ над полем $K(X^{1/\nu(i)})$. Мы выбираем m_1 так, что $\deg_Z \Phi_{2d-1,m_1} = \deg_Z f$. Положим $\varkappa_i = m_1$ и $q = q_{2d-1} + mX^\mu Z$. Теперь для построенных элементов $\varkappa_e$, $\varkappa_i$ и q выполняются утверждения (i)–(iv) из леммы 4.

Оставшаяся часть конструкции из раздела 2 вполне алгоритмична. Действуя таким образом, можно построить $\Phi, b, B^{(0)}, B^{(0)}$, Δ, w_0, $\overline{z}_{i,w,v_1,v_2}$, для всех $0 \leqslant w \leqslant \iota$. Напомним, что все эти элементы зависят от i. Мы будем использовать обозначения $b = b(i)$, $\Phi = \Phi_i$, $\Delta = \Delta_i$, если важна зависит от i.

Теперь мы можем дать определения всех элементов из формулировки теоремы 2. Положим $\Delta_u = \Delta$, этот элемент для $i = u$ уже определён в разделе 2. Далее, полагаем $\eta_u = b(u)$, $\varphi_u = \Phi_u$ для всякого $1 \leqslant u \leqslant \deg_Z f$.

Верхние границы на степени и длины записи целых коэффициентов всех построенных элементов удовлетворяют требуемым оценкам из теоремы 2. Эти оценки установлены в разделе 2. Наконец, время работы описанного алгоритма удовлетворяет оценкам из формулировки теоремы 2. Таким образом, эта теорема доказана. □

§4. Доказательство теоремы 1

В следующей лемме мы предполагаем, что многочлен f удовлетворяет условиям из формулировки теоремы 2. Следовательно, имеют место верхние оценки (9), но многочлен f не обязательно сепарабелен. При этих условиях мы применяем теорему 2 к многочлену f и рассматриваем представления (14) и (13) для корней многочлена f (напомним, что в действительности технически эти представления строятся для корней бесквадратной части f_{sqf} многочлена f). Отметим также, что в дальнейшем для доказательства теоремы 1 нам требуется только существование этих представлений (14) и (13).

Таким образом мы получаем элементы w_0, φ_u, Δ_u и $\overline{z}_{u,w,v_1,v_2}$. В дальнейшем $1 \leqslant u \leqslant \deg_Z f$ является произвольным индексом, конструкция осуществляется для всех u.

Лемма 5. *Существуют целые числа* $\nu_1, \ldots, \nu_n \geqslant 1$ *и* $\mu_{j,i} \geqslant 0$, $1 \leqslant i \leqslant j-1$, $1 \leqslant j \leqslant n$, *зависящие от* u, *такие, что* $\nu_1, \ldots, \nu_n$ *являются минимально возможными, наименьшее общее кратное*

$$\mathrm{LCM}\{\nu_1, \ldots, \nu_n\} \leqslant \deg_Z f \leqslant d,$$

для всех j, i

$$\sum_{1 \leqslant i \leqslant j-1} \mu_{j,i} \leqslant D^2 (c_1 d)^{(n-j+1)c} \tag{33}$$

для абсолютных констант $c, c_1 > 0$ *(можно легко вычислить такие константы) и*

$$z_u \in \overline{k}[[X_1^{1/\nu_1}, X_2^{1/\nu_2}/X_1^{\mu_{2,j}/\nu_1}, \ldots, X_n^{1/\nu_n}/(X_1^{\mu_{n,1}/\nu_1} \cdot \ldots \cdot X_{n-1}^{\mu_{n,n-1}/\nu_{n-1}})]].$$

Доказательство. Заметим, что если $\nu_1, \ldots, \nu_n$ минимально возможные, то существует по крайней мере $\mathrm{LCM}\{\nu_1, \ldots, \nu_n\}$ попарно различных корней многочлена f и, следовательно, $\mathrm{LCM}\{\nu_1, \ldots, \nu_n\} \leqslant \deg_Z f \leqslant d$.

Далее, мы будем использовать индукцию по n. Утверждение леммы для базы индукции $n = 1$ следует немедленно из теоремы 2 для $n = 1$, т.е. $X = X_1$, $K = k$ или непосредственно (в этом случае требуется установить только существование ν_1, а это почти тривиально). Предположим, что $n \geqslant 2$ и, что требуемое утверждение доказано для $n-1$, т.е. для всех многочленов от $X_1, \ldots, X_{n-1}, Z$. Докажем его для n.

Рассмотрим лексикографический порядок на мультииндексах из $\mathbb{Z}^{n-1}$. Именно, $(i_1, \ldots, i_{n-1}) > (j_1, \ldots, j_{n-1})$ тогда и только тогда, когда существует $1 \leqslant m \leqslant n-1$ такое, что $i_{m+1} = j_{m+1}, \ldots, i_{n-1} = j_{n-1}$, но $i_m > j_m$.

Пусть

$$\Delta_u = \sum_{i_1, \ldots, i_{n-1} \geqslant 0} \Delta_{u, i_1, \ldots, i_{n-1}} X_1^{i_1} \cdot \ldots \cdot X_{n-1}^{i_{n-1}},$$

где все коэффициенты $\Delta_{u, i_1, \ldots, i_{n-1}} \in \mathbb{Z}[T_1, \ldots, T_l]$. Положим

$$(j_1, \ldots, j_{n-1}) = \min\{(i_1, \ldots, i_n) \,:\, \Delta_{u, i_1, \ldots, i_{n-1}} \neq 0\},$$

где минимум берётся относительно рассматриваемого лексикографического порядка. Положим

$$\Delta'_u = \Delta_u / (\Delta_{u, j_1, \ldots, j_n} X_1^{j_1} \cdot \ldots \cdot X_{n-1}^{j_{n-1}}).$$

Мы имеем $(i_1 - j_1, \dots, i_{n-1} - j_{n-1}) \geqslant (0, \dots, 0)$ для всякого мультииндекса $(i_1, \dots, i_{n-1})$ такого, что $\Delta_{u,i_1,\dots,i_{n-1}} \neq 0$. Поэтому

$$(\Delta'_u)^{-1} \in k[[X_1, X_2/X_1^{j_1}, X_3/(X_1^{j_1}X_2^{j_2}), \dots, X_{n-1}/(X_1^{j_1} \cdot \ldots \cdot X_{n-2}^{j_{n-2}})]]. \quad (34)$$

Далее, $\sum_{1 \leqslant i \leqslant n-1} j_i \leqslant \deg_{X_1,\dots,X_{n-1}} \Delta_u \leqslant DP_1(d)$ для абсолютного (ни от чего не зависящего) полинома P_1 с целыми коэффициентами.

Обозначим через Λ_2 кольцо из (34). Положим $\nu_n = \nu_{u,n}$, см. (14). Напомним, что $w_0 = w_{u,0}$ введено перед формулировкой теоремы 2 и определено в разделе 2. Положим $w_1 = \max\{1, w_0\}$. Тогда очевидно $X_n^{1/\nu_n}/(X_1^{j_1} \cdot \ldots \cdot X_{n-1}^{j_{n-1}}) \in \Lambda_2[[X_n^{1/\nu_n}/(X_1^{j_1 w_1} \cdot \ldots \cdot X_{n-1}^{j_{n-1} w_1})]]$. Следовательно, согласно (14), см. раздел 1,

$$z_u \in \Lambda_2[[X_n^{1/\nu_n}/(X_1^{j_1 w_1} \cdot \ldots \cdot X_{n-1}^{j_{n-1} w_1})]]\,[\eta_u, z_{u,0}].$$

Теперь мы применяем индукционное предположение к многочлену φ_u, см. раздел 2, и его корню η_u. Напомним, что $\varphi_u = \Phi$ в обозначениях из раздела 2, степени $\deg_Z \varphi_u \leqslant d$ и $\deg_{X_1,\dots,X_{n-1}} \varphi_u \leqslant D\mathcal{P}(d)$ см. формулировку теоремы 2. Мы получаем целые числа $\nu'_1, \dots, \nu'_{n-1}$ и $\mu'_{j,i} \geqslant 0$, такие, что наименьшее общее кратное $\mathrm{LCM}\{\nu'_1, \dots, \nu'_n, \nu_n\} \leqslant \deg_Z f \leqslant d$ и по индукционному предположению

$$\sum_{1 \leqslant i \leqslant j-1} \mu'_{j,i} \leqslant D^2 P_2(d)(c_1 d)^{(n-j)c}$$

для абсолютного полинома P_2 с целыми коэффициентами для всех j, i. Положим $\nu_i = \nu'_i$, $1 \leqslant i \leqslant n-1$.

Далее мы применяем индукционное предположение к многочлену

$$f(X_1, \dots, X_{n-1}, 0, Z) \in k[X_1, \dots, X_{n-1}, Z]$$

и его корню $z_{u,0}$. Мы получаем целые числа $\nu''_1, \dots, \nu''_{n-1}$ и $\mu''_{j,i} \geqslant 0$, такие, что наименьшее общее кратное $\mathrm{LCM}\{\nu''_1, \dots, \nu''_{n-1}, \nu_n\} \leqslant \deg_Z f \leqslant d$ и по индукционному предположению $\sum_{1 \leqslant i \leqslant j-1} \mu''_{j,i} \leqslant D^2 (c_1 d)^{(n-j)c}$ для всех j, i. Элемент $z_{u,0} \in K[\eta_u]$, см. раздел 2. Следовательно, ν''_i делит ν_i. Поэтому мы можем предполагать без ограничения общности, что $\nu''_i = \nu_i$ и $\sum_{1 \leqslant i \leqslant j-1} \mu''_{j,i} \leqslant D^2 d (c_1 d)^{(n-j)c}$ для всех j, i.

Положим $\mu_{n,i} = j_i w_1 \nu_i$ для всех $1 \leqslant i \leqslant n-1$. Тогда $\sum_{1 \leqslant i \leqslant n-1} \mu_{n,i} \leqslant D^2 P_3(d)$ для абсолютного полинома P_3 с целыми коэффициентами

Положим $\mu_{j,i} = \max\{j_i\nu_i, \mu'_{j,i}, \mu''_{j,i}\}$ для всех $1 \leqslant j \leqslant n-1$, $1 \leqslant i \leqslant j-1$. Тогда для всех $1 \leqslant j \leqslant n$ мы имеем

$$\sum_{1\leqslant i\leqslant j-1} \mu_{j,i} \leqslant \max\{D^2P_3(d), DdP_1(d), D^2P_2(d), D^2d\}(c_1d)^{(n-j)c}$$
$$\leqslant D^2(c_1d)^{(n-j+1)c}$$

при подходящем выборе констант $c, c_1 > 0$. Положим

$$X'_j = X_j^{1/\nu_j}/(X_1^{\mu_{j,1}/\nu_1} \cdot \ldots \cdot X_{j-1}^{\mu_{j,j-1}/\nu_{j-1}}), \quad 1 \leqslant j \leqslant n.$$

Тогда

$$\Lambda_2[[X_n^{1/\nu_n}/(X_1^{j_1} \cdot \ldots \cdot X_{n-1}^{j_{n-1}})]][\eta_u, z_{u,0}] \subset \overline{k}[[X'_1, \ldots, X'_n]]$$

Следовательно для определённых выше ν_i, $\mu_{j,i}$ справедливы утверждения леммы. Лемма доказана. □

Замечание 4. Заметим, что D^2 вместо D появляется в доказательстве (и, следовательно, в формулировке) леммы только, поскольку нет оценки для $\sum_i \mu_{n,i}$ подобной $\sum_i \mu_{n,i} \leqslant D\mathcal{P}(d)$. Именно, мы знаем только, что обе величины $\sum_i j_i$ и w_1 ограничены сверху $D\mathcal{P}(d)$. Сначала мы надеялись доказать неравенство (33) из леммы 5 с D вместо D^2, но не смогли. И всё же нам его удалось доказать для D^2.

Теперь мы собираемся описать алгоритм для теоремы 1. Сначала, перебирая элементы конечного множества $\{(\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}^n : \forall i\,(1 \leqslant \gamma_i \leqslant d)\}$, мы строим множество S всех наборов из n целых чисел $(\nu_1, \ldots, \nu_n)$ таких, что наименьшее общее кратное $\mathrm{LCM}\{\nu_1, \ldots, \nu_n\} \leqslant d$.

Мы перебираем элементы из S. Пусть $(\nu_1, \ldots, \nu_n) \in S$. Теперь положим $\mu_{j,i} = [c_1d^{1+(n-j+1)c}]$, $1 \leqslant j \leqslant n$, где c_1 и c – константы из леммы 5 и $[\ldots]$ обозначает целую часть числа. Тогда существуют целые числа $\varkappa_{j,i} \geqslant 0$, $1 \leqslant i \leqslant j-1$, $1 \leqslant j \leqslant n$, такие, что $X_j^{1/\nu_j} = (X'_1)^{\varkappa_{j,1}} \cdot \ldots \cdot (X'_{j-1})^{\varkappa_{j,j-1}} X'_j$ для $1 \leqslant j \leqslant n$, ср. введение. Заметим, что все целые числа $\varkappa_{j,i}$ ограничены сверху $D^{2n}\mathcal{P}(d^{n^2})$. Это следует немедленно из оценок $\varkappa_{j,i}$ как решений линейной системы, полученных по правилу Крамера.

Положим $\widehat{f} = f(X_1^{\nu_1}, \ldots, X_n^{\nu_n}, Z)$ и

$$\widetilde{f} = \widehat{f}(X'_1, (X'_1)^{\varkappa_{2,1}}X'_2, \ldots, (X'_1)^{\varkappa_{n,1}} \cdot \ldots \cdot (X'_{n-1})^{\varkappa_{n,n-1}}X'_n, Z)$$

Применяя теорему 3 [6], мы строим корни многочлена $\widetilde{f}$ в кольце $\overline{k}[[X'_1, \ldots, X'_n]]$. После этого мы переходим к следующему элементу из S в описываемом переборе.

Действуя таким образом, мы построим множество $R_{\nu_1,\ldots,\nu_n}$ всех корней многочлена f в кольце (12), см. введение, для всякого $(\nu_1, \ldots, \nu_n) \in S$. Однако при этом некоторые корни могут появиться несколько раз в $R_{\nu_1,\ldots,\nu_n}$ для различных $(\nu_1, \ldots, \nu_n) \in S$. Именно, если $(\nu'_1, \ldots, \nu'_n) \in S$ – другой элемент такой, что ν'_i делит ν_i для всякого $1 \leqslant i \leqslant n$, то $R_{\nu'_1,\ldots,\nu'_n} \subset R_{\nu_1,\ldots,\nu_n}$. Но можно сравнить любой корень $z_u \in R_{\nu_1,\ldots,\nu_n}$ с любым другим корнем $z_{u'} \in R_{\nu'_1,\ldots,\nu'_n}$ и выяснить верно ли, что z_u и $z_{u'}$ сопряжены над k покоэффициентно. Действительно, для этой цели достаточно выяснить верно ли, что поля коэффициентов k_u и $k_{u'}$ изоморфны над k. Это может быть проделано с помощью алгоритма для факторизации многочленов из [2], [7]. Если k_u не изоморфно $k_{u'}$, то корни не сопряжены над k. Если k_u изоморфно $k_{u'}$, то можно построить начальные аппроксимации $(z_u)_{\#,\iota}$ и $(z_{u'})_{\#,\iota}$ в кольце $k_u[X'_1, \ldots, X'_n]$ (это кольцо определено для набора из n чисел $(\nu_1, \ldots, \nu_n)$) для достаточно большого ι, ограниченного сверху $\mathcal{P}(D^n d^{n^2})$. После этого можно выяснить верно ли, что $(z_u)_{\#,\iota}$ и $(z_{u'})_{\#,\iota}$ сопряжены над k. Корни z_u и $z_{u'}$ сопряжены над k в том и только в том случае, если $(z_u)_{\#,\iota}$ и $(z_{u'})_{\#,\iota}$ сопряжены над k, см. [6]. Таким образом, можно заменить каждое множество $R_{\nu_1,\ldots,\nu_n}$ на $R_{\nu_1,\ldots,\nu_n} \setminus \bigcup_{(\nu'_1,\ldots,\nu'_n)} R_{\nu'_1,\ldots,\nu'_n}$, где объединение берётся по всем $(\nu'_1, \ldots, \nu'_n) \in S$ таким, что ν'_i делит ν_i для всех i и $(\nu'_1, \ldots, \nu'_n) \neq (\nu_1, \ldots, \nu_n)$. Следовательно, теперь каждый корень z_u принадлежат только к одному множеству $R_{\nu_1,\ldots,\nu_n}$ и $\nu_1, \ldots, \nu_n$ являются минимально возможными.

Утверждения (i) и (ii) теоремы 1 доказаны. Оценки для времени работы алгоритма следуют немедленно из теоремы 3 [6]. Теорема 1 доказана. □

Замечание 5. Вероятно можно построить минимально возможные целые числа $\mu_{j,i} \geqslant 0$, но мы не рассматриваем эту проблему в данной статье.

Список литературы

1. А. О. Гельфонд, *Трансцендентные и алгебраические числа*, ГИТТЛ, Москва (1952).
2. А. Л. Чистов *Алгоритм полиномиальной сложности для разложения многочленов на неприводимые множители и нахождение компонент многообразия*

в субэкспоненциальное время. — Зап. научн. семин. ЛОМИ, **137** (1984), 124–188; English transl., J. Sov. Math. **34**, No. 4, (1986), 1838–1882.

3. A. L. Chistov, *Effective Construction of a Nonsingular in Codimension One Algebraic Variety over a Zero-Characteristic Ground Field.* — Зап. научн. семин. ПОМИ, **387** (2011), 167–188; English transl., J. Math. Sci., **179** (2011), 729–740.
4. A. L. Chistov, *Polynomial complexity of the Newton–Puiseux algorithm.* — In: International Symposium on Mathematical Foundations of Computer Science 1986. Lecture Notes in Computer Science Vol. 233 Springer (1986), pp. 247–255.
5. А. Л. Чистов *Алгоритм для факторизации многочленов в кольце формальных степенных рядов от многих переменных в нулевой характеристике.* — Зап. научн. семин. ПОМИ, **517** (2022), 268–290; English transl., to appear in J. Math. Sci.
6. А. Л. Чистов, *Алгоритм для факторизации многочленов в кольце формальных степенных рядов от многих переменных в нулевой характеристике. II.* — Зап. научн. семин. ПОМИ, **529** (2023), 261–290; English transl., to appear in J. Math. Sci.
7. A. L. Chistov, *An improvement of the complexity bound for solving systems of polynomial equations.* — Зап. научн. семин. ПОМИ, **390** (2011), 299–306.
8. W.-L. Chow, *On the theorem of Bertini for local domains.* — Proceedings of the National Academy of Sciences, **44**, #6 (1958), 580–584.

Chistov A. L. Complexity of constructing the roots of a polynomial in the field of multiple formal fractional power series in zero characteristic.

By a change of variables we reduce the problem of constructing the roots of a polynomial in the field of multiple formal fractional power series in zero characteristic to constructing the roots of another polynomial in the ring of multivariables formal power series. The efficient estimates for this change of variables are obtained. To achieve this aim we suggest a new refined version of the result on the complexity of the Newton–Puiseux algorithm. After that one can apply the algorithm for factoring polynomials over the ring multivariables formal power series constructed by the author earlier with efficient estimates for the working time.

Санкт-Петербургское отделение
Математического института им. В. А. Стеклова
Российской академии наук,
наб. р. Фонтанки 27
191023 Санкт-Петербург, Россия
E-mail: alch@pdmi.ras.ru

Поступило ?????2024