Записки научных
семинаров ПОМИ
Том 517, 2022 г.

А. Л. Чистов

АЛГОРИТМ ДЛЯ ФАКТОРИЗАЦИИ МНОГОЧЛЕНОВ В КОЛЬЦЕ ФОРМАЛЬНЫХ СТЕПЕННЫХ РЯДОВ ОТ МНОГИХ ПЕРЕМЕННЫХ В НУЛЕВОЙ ХАРАКТЕРИСТИКЕ

Введение

Пусть k – основное поле характеристики нуль с алгебраическим замыканием $\overline{k}$. В дальнейшем в алгоритмах мы будем предполагать, что k конечно порождено над его примитивным подполем, подробности см. ниже. Пусть $k[[X_1, \dots, X_n]]$ (соответственно $\overline{k}[[X_1, \dots, X_n]]$) является кольцом формальных степенных рядов от переменных $X_1, \dots, X_n$ с коэффициентами из поля k (соответственно $\overline{k}$). По определению алгоритм строит многочлен с коэффициентами в кольце формальных степенных рядов в том и только в том случае, если он может построить произвольные аппроксимации всех коэффициентов этого многочлена, см. ниже определение 1 более подробно.

Хорошо известно, что кольца формальных степенных рядов над полем, а также кольца многочленов над такими кольцами формальных степенных рядов являются факториальными, см. [2, 10].

Пусть $f \in k[X_1, \dots, X_n, Z]$ – многочлен со старшим коэффициентом относительно Z равным 1 (см. замечание 1 ниже более подробно о случае произвольного старшего коэффициента). Цель настоящей статьи – предложить алгоритмы для факторизации многочлена f в кольцах $k[[X_1, \dots, X_n]][Z]$ и $\overline{k}[[X_1, \dots, X_n]][Z]$. По нашим сведениям до сих пор никто не описал подобных алгоритмов в случае $n \geqslant 2$ (может быть, рассматривались только частные случаи). Как непосредственное следствие предложенных алгоритмов мы получаем алгоритмы факторизации полиномов из $k[X_1, \dots, X_n]$ в кольцах формальных степенных рядов $k[[X_1, \dots, X_n]]$ и $\overline{k}[[X_1, \dots, X_n]]$. Снова, насколько нам известно, такие алгоритмы до сих пор не были получены для $n \geqslant 3$ (случай $n = 1$ тривиален, а случай $n = 2$ может быть рассмотрен при помощи метода ломаных Ньютона, ср. [7]).

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

Для любого $j \geqslant 1$ предлагаемые алгоритмы могут строить j-ую аппроксимацию всех объектов на их выходе, см. ниже более подробно. Мы устанавливаем явные оценки сложности для времени работы описываемых алгоритмов. Эти оценки сложности полиномиальны от j и длины записи входных данных, если число n переменных фиксировано, скажем $n = 2, 3, 4, \ldots$.

Лёгкого решения рассматриваемой проблемы факторизации полинома $f \in k[X_1, \ldots, X_n, Z]$ с помощью только многоугольников или многогранников Ньютона для $n \geqslant 2$ не имеется. Конечно, корни многочлена f принадлежат полю кратных формальных дробно-степенных рядов от $X_1, \ldots, X_n$, т.е. объединению по всем целым $\nu_1, \ldots, \nu_n \geqslant 1$ полей

$$\overline{k}((X_1^{1/\nu_1}))((X_2^{1/\nu_2})) \ldots ((X_n^{1/\nu_2})).$$

Однако, например, сложно выяснить верно ли, что корень z многочлена f из поля $k((X_1))((X_2)) \ldots ((X_n))$ на самом деле принадлежит $k[[X_1, \ldots, X_n]]$.

Наш метод основывается на результатах о нормализации алгебраических многообразий и пополнениях их локальных колец. Прежде всего, это эффективная нормализация алгебраических многообразий в характеристике нуль с явной оценкой сложности. Она описана автором ранее, см. [4–6]. Во-вторых, мы используем теоремы, относящиеся к аналитической неприводимости и аналитической нормальности нормальных алгебраических многообразий, см. [10, т. II, Гл. 8 §13 теоремы 31–33].

В данной статье мы не рассматриваем случай ненулевой характеристики главным образом, поскольку в этом случае не было получено результатов аналогичных [4]. Но, конечно, можно использовать другие алгоритмы для нормализации алгебраических многообразий в ненулевой характеристике (в литературе нет явных оценок сложности этих алгоритмов) и получить аналог теоремы 1 в ненулевой характеристике, но без оценки сложности алгоритмов.

Пусть $n \geqslant 1$ – целое число. Положим $\widehat{A} = \overline{k}[[X_1, \ldots, X_n]]$ равным кольцу формальных степенных рядов от $X_1, \ldots, X_n$ с коэффициентами из поля $\overline{k}$ (локальное кольцо A будет введено позже, см. раздел 2). Если $0 \neq a \in \widehat{A}$, то формальный степенной ряд a может быть однозначно представлен в виде $a = \sum\limits_{i_0 \leqslant i \in \mathbb{Z}} a_i$, где каждый ненулевой $a_i \in \overline{k}[X_1, \ldots, X_n]$ является однородным многочленом степени i и

$a_{i_0} \neq 0$ для некоторого целого числа $i_0 \geqslant 0$. По определению $\operatorname{ord}(a) = i_0$ и $\operatorname{ord}(0) = +\infty$.

Обозначим через $\mathfrak{m}$ максимальный идеал локального кольца $\widehat{A}$. Так что идеал $\mathfrak{m}$ порождён элементами $X_1, \ldots, X_n$. Пусть $z \in \widehat{A}$ и $N \geqslant 0$ является целым числом. Тогда существует единственный многочлен $z' \in \overline{k}[X_1, \ldots, X_n]$ 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 многочленов степени самое большее N из кольца $\overline{k}[X_1, \ldots, X_n]$. Следовательно, теперь $z_{\#,N} = z \bmod \mathfrak{m}^{N+1}$ для любого $z \in \widehat{A}$.

Пусть Z – переменная, и полином $g = \sum_{0 \leqslant j \leqslant \deg_Z g} g_j Z^j \in \widehat{A}[Z]$, 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 полином $g \in \widehat{A}[Z]$) в том и только в том случае, если для любого целого числа $N \geqslant 0$ этот алгоритм может построить многочлен $z_{\#,N}$ (соответственно $g_{\#,N}$).*

Конечно, здесь коэффициенты полинома $z_{\#,N}$ (соответственно $g_{\#,N}$) являются элементами из некоторых конечных расширений основного поля k, и эти расширения строятся данным алгоритмом явно.

Пусть $f \in k[X_1, \ldots, X_n, Z]$ – многочлен со степенями $\deg_{Z,X_1,\ldots,X_n} f \leqslant d$, $\deg_Z f \geqslant 1$, и старший коэффициент $\operatorname{lc}_Z f = 1$. В настоящей статье наша цель – построить факторизацию полинома f в кольцах $\widehat{A}[Z]$ и $k[[X_1, \ldots, X_n]][Z]$. Прежде всего, применяя алгоритм из [3], мы построим разложение $f = \mu \prod\limits_{\nu \in N} f_\nu^{e_\nu}$ многочлена f в произведение неприводимых множителей, где все $f_\nu \in k[X_1, \ldots, X_n, Z]$ являются неприводимыми, $0 < e_\nu \in \mathbb{Z}$, $0 \neq \mu \in k$. После этого достаточно разложить на множители каждый полином f_ν в кольцах $\widehat{A}[Z]$ и $k[[X_1, \ldots, X_n]][Z]$. Так что в дальнейшем мы будем предполагать без ограничения общности (если только не оговорено противное), что многочлен f неприводим в кольце $k[X_1, \ldots, X_n, Z]$.

Обозначим через $\operatorname{lc}_Z f$ старший коэффициент многочлена f относительно Z. В дальнейшем считаем, что $\operatorname{lc}_Z f = 1$ (случай, когда $\operatorname{lc}_Z f \notin k$ не рассматривается в этой статье). При этих условиях пусть

$f = \prod_{w\in J} f_w$ является разложением полинома f на неприводимые множители в кольце $\widehat{A}[Z]$, и старшие коэффициенты $\mathrm{lc}_Z f_w = 1$ для всех $w \in J$. Тогда мы строим начальные приближения $f_w \bmod \mathfrak{m}^{N+1}$ (для некоторого $N \geqslant 0$) всех $f_w \in \widehat{A}[Z]$ такие, что для всякого целого числа $j > N+1$ можно найти $f_w \bmod \mathfrak{m}^j$, применяя версию леммы Гензеля, подробности см. ниже в формулировке теоремы 1. Число N ограничено сверху полиномом от d. Время работы алгоритма для построения всех $f_w \bmod \mathfrak{m}^j$, $w \in J$, полиномиально от $d^{2^{n^c}}$, j^n и длины записи входных данных для некоторой абсолютной константы $c > 0$. Аналогичным образом можно получить разложение многочлена f на неприводимые множители в кольце $k[[X_1, \ldots, X_n]][Z]$.

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

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

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

Мы представляем многочлен $\varphi = 1/\varphi^{(2)} \sum\limits_{0\leqslant i\leqslant \deg_Z \varphi} \varphi_i^{(1)} Z^i$, где все $\varphi_i^{(1)}$, $\varphi^{(2)} \in \mathbb{Z}[T_1, \ldots, T_l]$ и $\mathrm{GCD}_i\{\varphi_i^{(1)}, \varphi^{(2)}\} = 1$ в $\mathbb{Z}[T_1, \ldots, T_l]$. Многочлен $f \in k[X_1, \ldots, X_n, Z]$ записывается в виде

$$f = \frac{1}{b} \sum_{0\leqslant i<\deg_Z \varphi, i_1, \ldots, i_n} a_{i,i_1,\ldots,i_n} \eta^i X_1^{i_1} \cdot \ldots \cdot X_n^{i_n},$$

где все $a_{i,i_1,\ldots,i_n}, b \in \mathbb{Z}[T_1, \ldots, T_l]$, и в этом кольце наибольший общий делитель $\mathrm{GCD}_{i,i_1,\ldots,i_n}\{a_{i,i_1,\ldots,i_n}, b\} = 1$. Положим

$$\deg_{T_1,\ldots,T_l} f = \max\{\deg_{T_1,\ldots,T_l} a_{i,i_1,\ldots,i_n}, \deg_{T_1,\ldots,T_l} b\}. \tag{1}$$

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

$$\deg_{T_1,\ldots,T_l,Z} \varphi < d_1, \quad \deg_{T_1,\ldots,T_l} f < d_2, \quad \deg_{X_1,\ldots,X_n,Z} f \leqslant d,$$
$$\mathrm{l}(\varphi) \leqslant M_1, \quad \mathrm{l}(f) \leqslant M_2$$

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

Мы хотели бы избежать зависимости от l оценок в формулировках теоремы и лемм ниже. Полагаю, что здесь (и почти во всех других моих статьях) эффективные конструкции и алгоритмы сами по себе являются более важными, чем оценки их сложности. Так что в дальнейшем для простоты мы будем предполагать, что l является фиксированной константой. Всё же заинтересованный читатель может получить оценки, зависящие от l, ср. [3].

Прежде чем формулировать основной результат, нам требуется ввести вариант леммы Гензеля. Сейчас (и в формулировке леммы 1 ниже) мы предполагаем только, что многочлен f сепарабелен и старший коэффициент $\mathrm{lc}_Z f = 1$. Обозначим через $\delta \in k[X_1, \dots, X_n]$ дискриминант полинома f относительно Z. Следовательно, $\delta \neq 0$. Положим $r = \mathrm{ord}(\delta)$. Положим $X = X_1 + X_2 + \ldots + X_n$ и $t_i = X_i/X$. Так что $\sum\limits_{1 \leqslant i \leqslant n} t_i = 1$. Положим поля $L = k(t_1, \dots, t_{n-1})$ и $L' = \overline{k}(t_1, \dots, t_{n-1})$. Поэтому $L \subset L'$. Мы будем отождествлять $\overline{k}[X_1, \dots, X_n, Z] \subset L'[X, Z]$ и $\overline{k}[[X_1, \dots, X_n]][Z] \subset L'[[X]][Z]$. Каждый ненулевой элемент $b \in L'[[X]][Z]$ может быть представлен в виде $b = \sum\limits_{i_0 \leqslant i \in \mathbb{Z}} b_i X^i$, где все $b_i \in L'[Z]$ и $b_{i_0} \neq 0$. По определению положим $\mathrm{ord}_X(b) = i_0$ и $\mathrm{ord}_X(0) = +\infty$. Для всякого целого числа $j \geqslant 0$ определим $b \bmod X^{j+1} = \sum\limits_{i_0 \leqslant i \leqslant j} b_i X^i$ и $0 \bmod X^{j+1} = 0$. Очевидно $f \in L[X, Z]$, дискриминант $0 \neq \delta \in L[X]$ и $\mathrm{ord}_X(\delta) = r$.

Теперь пусть $f = gh$, где $g, h \in \widehat{A}[Z]$, степени $\deg_Z g \geqslant 1$, $\deg_Z h \geqslant 1$ и старшие коэффициенты $\mathrm{lc}_Z g = \mathrm{lc}_Z h = 1$. Положим $R = \mathrm{Res}_Z(g, h)$ равным результанту многочленов g и h относительно Z. Следовательно, $0 \neq R \in \widehat{A} \subset L'[[X]]$ и R^2 делит δ в кольце $\widehat{A}$. Положим $r_1 = \mathrm{ord}_X(R)$.

Обозначим $\varkappa = r - 2r_1 \geqslant 0$. Положим $\overline{g} = g \bmod \mathfrak{m}^{r+1} \in \overline{k}[X_1, \dots, X_n][Z]$, $\overline{h} = h \bmod \mathfrak{m}^{r+1} \in \overline{k}[X_1, \dots, X_n][Z]$. Тогда $\overline{g}, \overline{h} \in k_1(t_1, \dots, t_{n-1})[X, Z]$, где $k_1 \supset k$ является конечным расширением. Положим поле $L_1 = k_1(t_1, \dots, t_{n-1}) \subset L'$. Заметим, что $r + 1 = 2r_1 + \varkappa + 1$. Теперь из доказательства теоремы 1 [1, §3 Глава IV] следует, что существуют многочлены $\widetilde{g}, \widetilde{h} \in L_1[[X]][Z]$ такие, что $\mathrm{ord}_X(\widetilde{g} - \overline{g}) \geqslant r_1 + \varkappa + 1$, $\mathrm{ord}_X(\widetilde{h} - \overline{h}) \geqslant r_1 + \varkappa + 1$, старшие коэффициенты $\mathrm{lc}_Z \widetilde{g} = \mathrm{lc}_Z \widetilde{h} = 1$ и $f = \widetilde{g}\widetilde{h}$.

Далее, покажем, что $\widetilde{g} = g$, $\widetilde{h} = h$. Допустим, что $\widetilde{g} \neq g$. Положим $q_1 = \mathrm{G\,C\,D}\,(\widetilde{g}, g)$, $q_2 = \mathrm{G\,C\,D}\,(\widetilde{h}, h)$, где $q_1, q_2 \in L'[[X]][Z]$, и дополнительно $\mathrm{lc}_Z\, q_1 = \mathrm{lc}_Z\, q_2 = 1$. Положим $G = g/q_1 \neq 1$, $\widetilde{G} = \widetilde{g}/q_1 \neq 1$, $H = h/q_2$, $\widetilde{H} = \widetilde{h}/q_2$. Тогда $f/(q_1q_2) = GH = \widetilde{G}\widetilde{H}$ и, следовательно, $G = \widetilde{H}$, $H = \widetilde{G}$. Поэтому $f = G\widetilde{G}q_1q_2$. Мы имеем $\mathrm{ord}_X \mathrm{Res}_Z(G, \widetilde{G}) \geqslant r_1 + \varkappa + 1$, поскольку $\mathrm{ord}_X(G - \widetilde{G}) \geqslant r_1 + \varkappa + 1$ и $\deg_Z G = \deg_Z \widetilde{G}$. Очевидно $2(r_1 + \varkappa + 1) = 2(r - r_1 + 1) > r + 1$. Поэтому $\mathrm{ord}_X(\delta) > r + 1$. Данное противоречие доказывает требуемое утверждение.

Лемма 1. *Предположим, что даны многочлены f, $\overline{g}$ и $\overline{h}$, см. выше. Тогда для всякого $j \geqslant 1$ полиномы $\widetilde{g} \bmod X^j, \widetilde{h} \bmod X^j$ можно построить с помощью метода из доказательства теоремы* 1 [1, §3 Глава IV] *за время полиномиальное от j^n, d^n, d_1, d_2, M_1, M_2 и длин записи многочленов $\overline{g}$, $\overline{h}$. Согласно доказанной единственности мы имеем $g = \widetilde{g}$ и $h = \widetilde{h}$. Отсюда следует, что $\widetilde{g}, \widetilde{h} \in k_1[t_1, \ldots, t_{n-1}][[X]][Z]$. Далее, можно представить*

$$\widetilde{g} = \sum_{j \geqslant 0} \widetilde{g}_j X^j, \quad \widetilde{h} = \sum_{j \geqslant 0} \widetilde{h}_j X^j,$$

где все $\widetilde{g}_j, \widetilde{h}_j \in k_1[t_1, \ldots, t_{n-1}]$, степени $\deg_{t_1,\ldots,t_{n-1}} \widetilde{g}_j, \deg_{t_1,\ldots,t_{n-1}} \widetilde{h}_j \leqslant j$. Поэтому все ненулевые $\widetilde{g}_j X^j$, $\widetilde{h}_j X^j$ являются однородными многочленами из кольца $k_1[X_1, \ldots, X_n]$ степени j, и $g, h \in k_1[[X_1, \ldots, X_n]][Z]$.

Таким образом, согласно цитированной теореме из [1], *если даны многочлены $g \bmod \mathfrak{m}^{r+1}$ и $h \bmod \mathfrak{m}^{r+1}$, то для всякого целого числа $j > r+1$ можно построить многочлены $g \bmod \mathfrak{m}^j, h \bmod \mathfrak{m}^j$. Поэтому можно построить полиномы g и h.*

Доказательство. Это получается непосредственно. Подробности оставляем читателю. □

Теорема 1. *Пусть $f \in k[X_1, \ldots, X_n, Z]$ – неприводимый многочлен (в этом кольце) со старшим коэффициентом $\mathrm{lc}_Z f = 1$. Пусть дискриминант δ и целое число r – такие же, как и выше. Тогда можно разложить полином f на неприводимые множители в кольце $k[[X_1, \ldots, X_n]][Z]$ (соответственно $\overline{k}[[X_1, \ldots, X_n]][Z]$). Более точно, справедливы следующие утверждения.*

(i) *Можно построить разложение $f = \prod_{i \in I} f_i$, где все f_i являются неприводимыми элементами кольца $k[[X_1, \ldots, X_n]][Z]$ и*

все старшие коэффициенты $\operatorname{lc}_Z f_i = 1$. *Именно, для всякого* $i \in I$ *строится полином* $\overline{f}_i = f_i \bmod \mathfrak{m}^{r+1}$ *и после этого для того, чтобы получить* f_i, *можно применить лемму 1* (*к* $\overline{g} = \overline{f}_i$ *и* $\overline{h} = \bigl(\prod\limits_{i_1 \in I,\, i_1 \neq i} \overline{f}_{i_1}\bigr) \bmod \mathfrak{m}^{r+1}$).

(ii) *Для всякого* $i \in I$ *строится неприводимый многочлен* $\varphi_i \in k[Y]$ *степени* $\deg_Y \varphi_i \leqslant d$. *Обозначим через* $\{\eta_w\}_{w \in J_i}$ *семейство всех корней из алгебраического замыкания* $\overline{k}$ *многочлена* φ_i (*эти корни сопряжены над полем* k).

(iii) *Для всякого* $i \in I$ *можно построить разложение* $f_i = \prod\limits_{w \in J_i} f_w$, *где все полиномы* f_w *являются неприводимыми элементами кольца* $\overline{k}[[X_1, \ldots, X_n]][Z]$ *и все старшие коэффициенты* $\operatorname{lc}_Z f_w = 1$. *Именно, для всякого* $w \in J_i$ *строится полином* $\overline{f}_w = f_w \bmod \mathfrak{m}^{r+1} \in k[\eta_w][X_1, \ldots, X_n, Z]$, *и после этого для того, чтобы получить* f_w, *можно применить лемму 1* (*к* $\overline{g} = \overline{f}_w$ *и* $\overline{h} = \bigl(\prod_{w_1 \in J_i,\, w_1 \neq w} \overline{f}_{w_1}\bigr) \bmod \mathfrak{m}^{r+1}$). *Эти многочлены* $\overline{f}_w$ *сопряжены над полем* k *и аналогично многочлены* $f_w \in k[\eta_w][[X_1, \ldots, X_n]][Z]$ *сопряжены над полем* k (*группа Галуа* $\operatorname{Gal}(\overline{k}/k)$ *действует на рассматриваемых формальных степенных рядах и многочленах покоэффицентно*). *В дальнейшем мы предполагаем, что для всех* $i_1, i_2 \in I$, *если* $i_1 \neq i_2$, *то* $J_{i_1} \cap J_{i_2} = \varnothing$.

(iv) *Время работы для построения всех многочленов* $\overline{f}_i$, φ_w, $\overline{f}_w$, $w \in J_i$, $i \in I$, *полиномиально от* $d^{2^{n^c}}$, d_1, d_2, M_1, M_2 *для абсолютной константы* $c > 0$. *Для всякого* $j \geqslant 1$ *время работы алгоритма для построения всех многочленов* $f_i \bmod \mathfrak{m}^j$, $f_w \bmod \mathfrak{m}^j$ *полиномиально от* j^n, $d^{2^{n^c}}$, d_1, d_2, M_1, M_2.

Заметим, что для любого фиксированного n, скажем для $n = 2, 3, 4, \ldots$, время работы алгоритма из теоремы 1, см. (iv), полиномиально от j, d, d_1, d_2, M_1, M_2, т.е. это время работы полиномиально от j и длины записи входных данных.

Следствие 1. *При условиях теоремы 1 положим* $I'' = \{i \in I : f_i(0, \ldots, 0, 0) \neq 0\}$ *и* $I' = I \setminus I''$. *Обозначим* $a = \prod\limits_{i \in I''} f_i$ (*так что* a *является обратимым элементом кольца* $\widehat{A}[[Z]]$). *Тогда для всякого* $i \in I'$ *многочлен* f_i *является неприводимым элементом кольца*

$k[[X_1,\dots,X_n,Z]]$. Для всякого $i\in I'$, $w\in J_i$ многочлен f_w неприводим в кольце $\overline{k}[[X_1,\dots,X_n,Z]]$. Следовательно, $f=a\prod\limits_{i\in I'} f_i$ (соответственно $f=a\prod\limits_{i\in I',\,w\in J_i} f_w$) – разложение на неприводимые многочлена f в кольце $k[[X_1,\dots,X_n,Z]]$ (соответственно $\overline{k}[[X_1,\dots,X_n,Z]]$).

Доказательство. Это вытекает немедленно из предложения 7 [2, §3 Глава VII]. □

Следствие 2. *Используя следствие* 1, *можно получить алгоритм для факторизации любого многочлена $g\in k[X_1,\dots,X_n]$ (здесь мы предполагаем, что $n\geqslant 2$) в кольцах $k[[X_1,\dots,X_n]]$ и $\overline{k}[[X_1,\dots,X_n]]$.*

Доказательство. Осуществляя линейное преобразование переменных, мы можем предполагать без ограничения общности, что старший коэффициент $\mathrm{lc}_{X_n} g=1$. После этого достаточно заменить в условиях предыдущего следствия $n+1$ на n, переменные $X_1,\dots,X_n,Z$ на $X_1,\dots,X_n$ и многочлен f на g. □

Замечание 1. Заметим, что кольца формальных степенных рядов над полем являются целозамкнутыми. Обозначим через $k((X_1,\dots,X_n))$ (соответственно $\overline{k}((X_1,\dots,X_n))$) поле частных кольца $k[[X_1,\dots,X_n]]$ (соответственно $\overline{k}[[X_1,\dots,X_n]]$). Тогда в случае произвольного старшего коэффициента $\mathrm{lc}_Z f\in k[X_0,\dots,X_n]$, используя стандартную замену переменных $Y=(\mathrm{lc}_Z f)Z$ и применяя теорему 1, можно разложить f на неприводимые множители над полем $k((X_1,\dots,X_n))$ (соответственно $\overline{k}((X_1,\dots,X_n))$). Однако, если $\mathrm{lc}_Z f\notin k$, то это не даёт алгоритма для факторизации полинома f в кольце $k[[X_1,\dots,X_n]]$ (соответственно $\overline{k}[[X_1,\dots,X_n]]$).

Замечание 2. Кажется весьма вероятным, что можно улучшить алгоритм из теоремы 1 таким образом, что время работы модификациого алгоритма будет полиномиально от j^n, d^{n^c}, d_1, d_2, M_1, M_2 (т.е. сейчас $d^{2^{n^c}}$ заменяется на d^{n^c} в утверждении (iv) теоремы 1). Для этого следует получить явную версию первой теоремы Бертини для локальных колец. Возможно, достаточно будет вывести некоторые следствия из [8].

§1. Эффективный алгоритм нормализации алгебраических многообразий и его следствия

В статье [4] мы предлагаем алгоритм для построения неособого в коразмерности один алгебраического многообразия в характеристике нуль. Более точно, пусть $f \in k[X_1, \dots, X_n]$ – многочлен степени d неприводимый над алгебраическим замыканием $\overline{k}$ со старшим коэффициентом $\mathrm{lc}_{X_n} f = 1$. Тогда в [4] мы строим неособое в коразмерности один аффинное алгебраическое многообразие V и конечный бирациональный изоморфизм $V \to \mathcal{Z}(f)$, где $\mathcal{Z}(f)$ гиперповерхность всех общих нулей многочлена f в аффинном пространстве. Время работы алгоритма для построения V полиномиально от длины записи входных данных. Отметим также, что аффинное алгебраическое многообразие $V \subset \mathbb{A}^{n+1}(\overline{k})$ и степень многообразия V, равна $d^{O(1)}$, см. теорему 1 [4][1] (везде в настоящей статье константы в $O(\dots)$ являются абсолютными).

В [5] (и в краткой версии [6] этой статьи) мы предлагаем алгоритм для эффективной нормализации неособого в коразмерности один алгебраического многообразия в произвольной характеристике основного поля. Именно, пусть V – неособое в коразмерности один проективное алгебраическое многообразие (соответственно аффинное алгебраическое многообразие) степени D и размерности n. Мы предполагаем, что V определено над полем k и неприводимо над $\overline{k}$. Можно также считать, не умаляя общности, (особенно в настоящей статье, поскольку ниже мы применяем результат из [4]), что $V \subset \mathbb{P}^{n+2}(\overline{k})$. Тогда мы доказываем, что конструкция нормализации алгебраического многообразия V может быть сведена за время полиномиальное от $D^{n^{O(1)}}$ к решению линейного уравнения $aX + bY + cZ = 0$ над некоторым кольцом полиномов (число переменных этого кольца ограничено сверху $n^{O(1)}$). Поэтому согласно [9] для предложенного алгоритма мы получаем оценку сложности полиномиальную от $D^{2^{n^{O(1)}}}$ и длины записи входных данных, подробности см. в [5]. Если V является проективным алгебраическим многообразием (соответственно аффинным алгебраическим многообразием), то его нормализация снова – проективное алгебраическое многообразие (соответственно аффинное алгебраическое многообразие). Мы хотели бы отметить, что мы даём только абрис требуемой конструкции в [5]. Вероятно читателю потребуется много

[1] Имеется очевидная опечатка в формулировке утверждения (iv) цитированной теоремы: там следует заменить z_1, z_2 на z, как это видно из контекста.

усилий, чтобы восстановить все детали в доказательствах. Но полная версия [5] – слишком объёмная. Всё же мы надеемся опубликовать её в будущем.

В [5] случай проективного алгебраического многообразия V рассматривается более подробно (чем случай аффинного алгебраического многообразия). Там описывается каноническая конструкция над полем k_u, являющимся некоторым чисто трансцендентным расширением основного поля k. Однако также аналогичная, но менее каноническая конструкция возможна над полем k. Именно, обозначим через B однородное кольцо над полем k проективного алгебраического многообразия V и через B' целое замыкание B в его поле частных. Так что B' является градуированным кольцом. Строится система $\{y_v\}_{1\leqslant v\leqslant N}$ однородных образующих k-алгебры B', см. [5] более подробно. Обозначим это семейство образующих через $\mathcal{Y}$.

Заметим также, что, используя каноническую конструкцию из [5], можно построить сначала систему $\mathcal{Y}' = \{y'_v\}_{1\leqslant v\leqslant N'}$ образующих k_u-алгебры $k_u \otimes_k B'$ (эта алгебра равна целому замыканию кольца $k_u[X_1, \ldots, X_n, Z]/(f)$). Расширение полей $k_u \supset k$ является чисто трансцендентным. Следовательно, после этого с помощью $\mathcal{Y}'$ можно немедленно получить семейство $\mathcal{Y}$.

Положим m_v равным однородной степени элемента y_v и $m > 0$ равным наименьшему общему кратному всех m_v, $1 \leqslant v \leqslant N$. Для всякого целого числа $\mu \geqslant 0$ обозначим через B'_μ однородную компоненту кольца B' однороднй степени μ. Положим $\widetilde{B}_\mu = B'_{\mu m}$ для всякого целого числа $\mu \geqslant 0$. Тогда $\widetilde{B} = \oplus_{\mu\geqslant 0}\widetilde{B}_{\mu m}$ является градуированным кольцом, соответствующим проективному алгебраическому многообразию $\widetilde{V}$. Теперь очевидно $\widetilde{V}$ изоморфно нормализации проективного алгебраического многообразия V.

Случай аффинного алгебраического многообразия аналогичен и даже является более простым, см. замечания в конце введения из [5]. В этом случае B является кольцом регулярных функций, определённых над k, алгебраического многообразия V. Снова B' – целое замыкание B в его поле частных. Следовательно, B' является кольцом регулярных функций, определённых над k, нормализации V' алгебраического многообразия V. Система $\{y_v\}_{1\leqslant v\leqslant N}$ образующих k-алгебры B' строится алгоритмом.

В настоящей статье случай аффинного алгебраического многообразия будет центральным. Объединяя результаты [4] (с $n+1$ вместо n

и $X_1, \ldots, X_n$, Z вместо $X_1, \ldots, X_n$) и [5] в характеристике нуль, мы получаем алгоритм для построения системы образующих $\{y_v\}_{1 \leqslant v \leqslant N}$ над полем k целого замыкания B' кольца $k[X_1, \ldots, X_n, Z]/(f)$ в его поле частных. Таким образом, конструкция B' или, более точно, системы образующих $\{y_v\}_{1 \leqslant v \leqslant N}$ сводится к решению линейного уравнения $aX + bY + cZ = 0$ над кольцом многочленов, см. выше. Сложность алгоритма для построения этой системы образующих полиномиальна от $d^{2^{n^{O(1)}}}$ и длины записи входных данных. Мы хотели бы подчеркнуть, что до сих пор алгоритмы нормализации алгебраических многообразий, описанные другими авторами, не имели в общем случае явных оценок для сложности и степеней элементов, которые строятся этими алгоритмами.

Теперь мы переходим к вспомогательным результатам, требуемым для доказательства теоремы 1. В дальнейшем в этом разделе мы будем предполагать, что f – многочлен из введения, и дополнительно, что f неприводим в кольце $\overline{k}[X_1, \ldots, X_n, Z]$. Положим $z = Z \bmod f \in k(X_1, \ldots, X_n)[Z]/(f)$. Заметим, что каждый элемент a из поля частных кольца $k[X_1, \ldots, X_n, Z]/(f)$ может быть единственным образом представлен в виде $a = \sum\limits_{0 \leqslant i < \deg_Z f} b_i z^i$, где все $b_i \in k(X_1, \ldots, X_n)$. Напомним, что δ является дискриминантом полинома f относительно Z. Если a цел на кольцом $k[X_1, \ldots, X_n]$, то, как хорошо известно, для всякого i можно представить $b_i = a_i/\delta$, где $a_i \in k[X_1, \ldots, X_n]$. Таким образом, мы строим систему образующих $\{y_v\}_{1 \leqslant v \leqslant N}$ кольца B', см. выше, и представляем каждый y_v в виде

$$y_v = (1/\delta) \sum_{0 \leqslant i < \deg_Z f} y_{v,i} z^i \tag{2}$$

где все $y_{v,i} \in k[X_1, \ldots, X_n]$. Согласно [4, 5] целое число N ограничено сверху $d^{2^{n^{O(1)}}}$, степени $\deg_{X_1,\ldots,X_n} y_{v,i}$ ограничены сверху $d^{2^{n^{O(1)}}}$. Степени $\deg_{t_1,\ldots,t_l} y_{v,i}$ ограничены сверху полиномом от d_1, d_2 и $d^{2^{n^{O(1)}}}$. Длины записи коэффициентов $\mathrm{l}(y_{v,i})$ ограничены сверху полиномом от M_1, M_2, d_1, d_2 и $d^{2^{n^{O(1)}}}$ (напомним, что l является фиксированной константой).

Можно добавить элементы $X_1, \ldots, X_n, z$ к семейству $\{y_v\}_{1 \leqslant v \leqslant N}$. Поэтому мы будем предполагать дополнительно в дальнейшем, не умаляя

общности, что $N \geqslant n+1$, элементы $y_i = X_i$ для $1 \leqslant i \leqslant n$ и $y_{n+1} = z$. Пусть $Y_1, \ldots, Y_N$ – новые переменные. Пусть $n \leqslant v \leqslant N$ – целое число.

Обозначим через $\mathfrak{a}_v$ ядро гомоморфизма $k[Y_1, \ldots, Y_v] \to k[y_1, \ldots, y_v]$, $Y_j \mapsto y_j$ для всех j. Обозначим через $\mathbb{A}^v(\overline{k})$ аффинное пространство с координатными функциями $Y_1, \ldots, Y_v$ и через $W_v \subset \mathbb{A}^v(\overline{k})$ определённое над k аффинное алгебраическое многообразие с идеалом $\mathfrak{a}_v$. Следовательно, можно отождествить $W_n = \mathbb{A}^n(\overline{k})$, $W_{n+1} = \mathcal{Z}(f) \subset \mathbb{A}^{n+1}(\overline{k})$ и $W_N = V'$. Мы имеем естественные регулярные конечные доминантные проекции $\pi'_v : W_v \to W_{v-1}$, $n+1 \leqslant v \leqslant N$, индуцированные вложениями колец регулярных функций. Эти проекции являются бирациональными изоморфизмами для $n+2 \leqslant v \leqslant N$. Положим $\pi_v = \pi'_v \circ \pi'_{v-1} \circ \ldots \circ \pi'_{n+1}$ для $n+1 \leqslant v \leqslant N$. Следовательно, $\pi_v : W_v \to \mathbb{A}^n(\overline{k})$ являются доминантными морфизмами. Положим $x^* = (0, \ldots, 0) \in \mathbb{A}^n(\overline{k})$.

Пусть $Q = \sum\limits_{n+1 \leqslant v \leqslant N} a_v Y_v \in k[Y_{n+1}, \ldots, Y_N]$ – ненулевая линейная форма с целыми коэффициентами a_v. Предположим, что все эти коэффициенты a_v заданы. Обозначим через $F \in k(X_1, \ldots, X_n)[Q]$ минимальный многочлен элемента $Q(y_{n+1}, \ldots, y_N)$ над полем $k(X_1, \ldots, X_n)$ такой, что старший коэффициент $\mathrm{lc}_Y F = 1$. Тогда фактически $F \in k[X_1, \ldots, X_n, Q]$. Теперь, используя (2), мы можем построить представления

$$Q(y_{n+1}, \ldots, y_N)^j = (1/\delta) \sum_{0 \leqslant i < \deg_Z f} a_{j,i} z^i, \quad 0 \leqslant j \leqslant \deg_Z f, \qquad (3)$$

где все коэффициенты $a_{j,i} \in k[X_1, \ldots, X_n]$. После этого, решая линейные системы над полем $k(X_1, \ldots, X_n)$, можно найти полином F. Положим ψ равным бесквадратной части многочлена $F(0, \ldots, 0, Q)$, т.е. ψ является сепарабельным полиномом максимальной возможной степени таким, что ψ делит $F(0, \ldots, 0, Q)$. Мы предполагаем дополнительно, что $\mathrm{lc}_Q \psi = 1$. Применяя алгоритм из [3], можно построить ψ, и после этого разложить на неприводимые $\psi = \prod\limits_{1 \leqslant j \leqslant m} \psi_j$, где все $\psi_j \in k[Q]$ являются неприводимыми многочленами со старшими коэффициентами $\mathrm{lc}_Q \psi_j = 1$. Положим поле $k_j = k[Z]/(\psi_j(Z))$ и $q_j = Z \bmod \psi_j(Z) \in k_j$ для всякого $1 \leqslant j \leqslant m$. Заметим, что $k_j \supset k$ является конечным расширением полей. Мы отождествляем поле k_j с подполем поля $\overline{k}$. Обозначим через G_j множество всех вложений поля $k_j \to \overline{k}$ над k. Следовательно, $\#G_j = \deg_Q \psi$.

Если важна зависимость от Q, то мы будем писать $a_{Q,v}$, F_Q, ψ_Q, $m_Q, \psi_{Q,j}$, $q_{Q,j}$, $G_{Q,j}$ вместо $a_v, F, \psi, m, \psi_j, q_j, G_j$.

Положим $K = k(X_1, \dots, X_n)[Z]/(f)$ (соответственно $K' = \overline{k}(X_1, \dots, X_n)[Z]/(f)$) равным полю частных кольца $k[X_1, \dots, X_n, Z]/(f)$ (соответственно $\overline{k}[X_1, \dots, X_n, Z]/(f)$).

Лемма 2. *Можно построить линейную форму Q, минимальный многочлен F, полином ψ и все полиномы ψ_j, $1 \leqslant j \leqslant m$, удовлетворяющие следующим свойствам.*

(i) *Положим $q = Q(y_{n+1}, \dots, y_N)$. Тогда q является примитивным элементом расширения полей $K \supset k(X_1, \dots, X_n)$. Поэтому степень $\deg_Q F = \deg_Z f$. Кроме того, абсолютные величины целых коэффициентов $|a_v| \leqslant 2(\deg_Z f)^2$ для всех $n+1 \leqslant v \leqslant N$.*

(ii) *Число элементов $\#\pi_N^{-1}(x^*) = \#Q(\pi_N^{-1}(x^*)) = \deg_Q \psi$.*

(iii) *Для всякого $1 \leqslant j \leqslant m$ существует точка $y^{(j)} = (y_1^{(j)}, \dots, y_N^{(j)}) \in \pi_N^{-1}(x^*)$ такая, что для всякого $n+1 \leqslant v \leqslant N$ её координата $y_v^{(j)}$ представляется в виде*

$$y_v^{(j)} = \sum_{1 \leqslant \nu < \deg_Q \psi_j} y_{v,\nu}^{(j)} q_j^{\nu}, \tag{4}$$

где все коэффициенты $y_{v,\nu}^{(j)} \in k$ строятся алгоритмом.

(iv) *Можно представить $\pi_N^{-1}(x^*) = \bigcup\limits_{1 \leqslant j \leqslant m} S_j$, где*

$$S_j = \left\{ (y^{(j)})^{\sigma} \,:\, \sigma \in G_j \right\}$$

и $(y^{(j)})^{\sigma} = ((y_1^{(j)})^{\sigma}, \dots, (y_N^{(j)})^{\sigma})$. Следовательно, число элементов $\#S_j = \deg_Q \psi_j$ для всякого $1 \leqslant j \leqslant m$ и $S_{j_1} \cap S_{j_2} = \varnothing$, если $j_1 \neq j_2$.

Время работы алгоритма для построения всех объектов Q, F, ψ, ψ_j, $y_{v,\nu}^{(j)}$ полиномиально от d^n и длины записи входных данных, т.е. от d^n и длин записи многочленов f, φ и всех коэффициентов $y_{v,i}$, $n+1 \leqslant v \leqslant N$, $0 \leqslant i < \deg_Z f$, см. (2). Следовательно, это время работы полиномиально от $d^{2^{n^c}}$, d_1, d_2, M_1, M_2 согласно алгоритмам из [4,5].

Доказательство. Для всех целых чисел w таких, что $n+1 \leqslant w \leqslant N$, мы построим рекурсивно линейные формы $Q_w = \sum\limits_{n+1 \leqslant v \leqslant w} a_{w,v} Y_v$ с целыми коэффициентами $a_{w,v}$ такие, что справедливы свойства (i)–(iv)

из утверждения леммы для $w, Q_w, F_{Q_w}, \psi_{Q_w}, m_{Q_w}, \psi_{Q_w,j}$, $q_{Q_w,j}, G_{Q_w,j}$ вместо N, Q, F, ψ, m, ψ_j, q_j, G_j. Мы будем обозначать через $(\mathrm{i})_w$–$(\mathrm{iv})_w$ эти новые свойства (i)–(iv), соответствующие Q_w. Теперь элементы $y^{(j)}$, $y_v^{(j)}$, $y_{v,\nu}^{(j)}$, q_j из (iii) будут обозначаться через $y_{Q_w}^{(j)}$, $y_{Q_w,v}^{(j)}$, $y_{Q_w,v,\nu}^{(j)}$, $q_{Q_w,j}$ в $(\mathrm{iii})_w$. Обозначим через $(4)_w$ формулу (4) из $(\mathrm{iii})_w$.

В качестве базы рекурсии возьмём $Q_{n+1} = Y_{n+1}$. Предположим, что $n+1 < w \leqslant N$ и линейная форма Q_{w-1} построена. Покажем, как найти Q_w. Пусть t – трансцендентный элемент над полем k. Расширим основное поле k до $k(t)$. Положим $Q' = Q_{w-1} + tY_w$. Далее мы строим многочлены $F_{Q'}, \psi_{Q'}$ и все полиномы $\psi_{Q',j}$, $1 \leqslant j \leqslant m_{Q'}$. Расширение колец $k[t, Y_1, \ldots, Y_w] \supset k[t, X_1, \ldots, X_n]$ является целым, и кольцо многочленов $k[t, X_1, \ldots, X_n]$ целозамкнуто. Поэтому фактически $F_{Q'} \in k[t, X_1, \ldots, X_n, Q']$ и $\psi_{Q'}, \psi_{Q',j} \in k[t, Q']$ для всех $1 \leqslant j \leqslant m_{Q'}$. Обозначим через G множество всех вложений полей $K \to \overline{K}$ над полем $k(X_1, \ldots, X_n)$. Заметим, что все элементы $Q_{w-1}(y_{n+1}^\sigma, \ldots, y_{w-1}^\sigma)$, $\sigma \in G$, попарно различны согласно (i). Следовательно, мы имеем $F_{Q'} = \prod_{\sigma \in G} (Q' - Q_{w-1}(y_{n+1}^\sigma, \ldots, y_{w-1}^\sigma) - t y_w^\sigma)$. Поэтому степени $\deg_t F_{Q'} \leqslant \#G = \deg_Z f$ и $\deg_t \psi_{Q'} \leqslant \deg_Z f$.

Обозначим через $\Delta_{Q'}$ (соответственно $\delta_{Q'}$) дискриминант многочлена $F_{Q'}$ (соответственно $\psi_{Q'}$) относительно Q'. Следовательно, $\Delta_{Q'}\delta_{Q'} \neq 0$, и $\deg_t(\Delta_{Q'}\delta_{Q'}) < 4(\deg_Z f)^2$. Мы находим целое число $t' \neq 0$ такое, что $|t'| \leqslant 2(\deg_Z f)^2$ и $(\Delta_{Q'}\delta_{Q'})|_{t=t'} \neq 0$. Положим $Q_w = Q_{w-1} + t'Y_w$.

Теперь выполняется свойство $(\mathrm{i})_w$, поскольку $\Delta_{Q'}|_{t=t'} \neq 0$. Далее, покажем, что $\pi_w^{-1}(x^*) = \#Q'(\pi_w^{-1}(x^*)) = \deg_{Q'} \psi_{Q'}$. Действительно, каждая точка из $Q'(\pi_w^{-1}(x^*))$ имеет вид $Q_{w-1}(y_{n+1}^*, \ldots, y_{w-1}^*) + ty_w^*$, где $(y_1^*, \ldots, y_w^*) \in \pi_w^{-1}(x^*)$, и все $y_j^* \in \overline{k}$. Из свойств целых расширений колец выводим, что $\pi_{w-1}^{-1}(x^*) = \{(y_1^*, \ldots, y_{w-1}^*) : (y_1^*, \ldots, y_w^*) \in \pi_w^{-1}(x^*)\}$. Согласно $(\mathrm{ii})_{w-1}$ отображение $\pi_w^{-1}(x^*) \to \overline{k}^2$, $(y_1^*, \ldots, y_w^*) \mapsto (Q_{w-1}(y_{n+1}^*, \ldots, y_{w-1}^*), y_w^*)$ является инъективным. Отсюда следует требуемое утверждение.

Мы имеем $\#Q_w(\pi_w^{-1}(x^*)) = \deg \psi_{Q_w} = \deg \psi_{Q'}$, поскольку $\delta_{Q'}|_{t=t'} \neq 0$. Следовательно, выполняется свойство $(\mathrm{ii})_w$.

Для всякого $1 \leqslant j \leqslant m_{Q'}$ корни многочлена $\psi_{Q',j}$ сопряжены над полем $k(t)$. Поэтому многочлен $\psi_{Q',j}|_{t=0} = \psi_{Q_{w-1},j^*}^{e_{j^*}}$ для однозначно определённых целых чисел $e^* \geqslant 1$ и $1 \leqslant j^* \leqslant m_{Q_{w-1}}$ таких, что если $(y_1^*, \ldots, y_w^*) \in \pi_w^{-1}(x^*)$ и $Q_{w-1}(y_{n+1}^*, \ldots, y_{w-1}^*) + ty_w^*$ – корень полинома

$\psi_{Q',j}$, то $Q_{w-1}(y^*_{n+1},\dots,y^*_{w-1})$ является корнем полинома ψ_{Q_{w-1},j^*}. Вычисляя бесквадратную часть многочлена $\psi_{Q',j}|_{t=0}$, можно найти j^*, e^* и построить полином ψ_{Q_{w-1},j^*}.

Две точки $(y^*_1,\dots,y^*_w),(y'_1,\dots,y'_w)\in\pi_w^{-1}(x^*)$ сопряжены над полем k в том и только в том случае, если $Q'(y^*_{n+1},\dots,y^*_w)$ и $Q'(y'_{n+1},\dots,y'_w)$ сопряжены над полем $k(t)$ (соответственно в том и только в том случае, если $Q_w(y^*_{n+1},\dots,y^*_w)$ и $Q_w(y'_{n+1},\dots,y'_w)$ сопряжены над полем k). Отсюда следует, что $m_{Q'}=m_{Q_w}$ и можно положить по определению $\psi_{Q_w,j}=\psi_{Q',j}|_{t=t'}$ для всех $1\leqslant m\leqslant m_{Q'}$. И тогда существует точка $y^{(j)}=(y^{(j)}_1,\dots,y^{(j)}_w)\in\pi_w^{-1}(x^*)$, удовлетворяющая следующему свойству. Элемент $Q_w(y^{(j)}_{n+1},\dots,y^{(j)}_w)$ является корнем полинома $\psi_{Q_w,j}$, и $y^{(j)}_v=y^{(j^*)}_v$ для всех $1\leqslant v\leqslant w-1$.

Теперь мы можем доказать свойство $(\mathrm{iii})_w$ и построить представление $(4)_w$. Именно, используя алгоритм из [3], разложим на неприводимые многочлен $\psi_{Q',j}$ над полем $k(t)[Z]/(\psi_{Q_w,j}(Z))$. Мы имеем $\psi_{Q',j}|_{t=t'}=\psi_{Q_w,j}$. Следовательно, в этом разложении на неприводимые полинома $\psi_{Q',j}$ существует единственный линейный множитель вида

$$Q'-\sum_{0\leqslant\nu<\deg\psi_{Q_w,j}}(b'_\nu+tb_\nu)q^\nu_{Q_w,j},\tag{5}$$

удовлетворяющий следующим свойствам. Все коэффициенты $b'_\nu,b_\nu\in k$, далее, $b'_\nu+t'b_\nu=0$ для $\nu\neq1$ и $b'_1+t'b_1=1$. Поэтому

$$q_{Q_{w-1,j^*}}=\sum_{0\leqslant\nu<\deg\psi_{Q_w,j}}b'_\nu q^\nu_{Q_w,j}\tag{6}$$

и $y^{(j)}_w=\sum\limits_{0\leqslant\nu<\deg\psi_{Q_w,j}}b_\nu q^\nu_{Q_w,j}$. Последнее соотношение даёт формулу $(4)_w$ для $v=w$. Для того, чтобы получить $(4)_w$ для $n+1\leqslant v\leqslant w-1$, мы подставляем правую часть (6) вместо $q_{Q_{w-1,j^*}}$ в формулу $(4)_{w-1}$. Наконец, мы редуцируем степени $q_{Q_w,j}$, используя деление многочленов с остатком.

Свойство $(\mathrm{iv})_w$ следует немедленно из $(\mathrm{ii})_w$ и $(\mathrm{iii})_w$. Таким образом, рекурсивный шаг описан полностью.

В заключение положим $Q=Q_N$. Так все что соответствующие F,ψ,ψ_j, $y^{(j)}_{v,\nu}$ уже построены. Утверждения о времени работы рассматриваемого алгоритма следуют немедленно из оценок на время работы использованных алгоритмов. Лемма доказана. □

§2. Доказательство теоремы 1

Применяя алгоритм из [3], разложим многочлен f на неприводимые множители в кольце $\overline{k}[X_1, \ldots, X_n, Z]$. Каждый абсолютно неприводимый множитель f' полинома f имеет коэффициенты в конечном расширении k' основного поля k. Это расширение $k' \supset k$ строится алгоритмом из [3]. Следовательно, достаточно доказать теорему 1 для каждого абсолютно неприводимого множителя f' с основным полем k' вместо k (здесь мы оставляем подробности читателю). Так что применяя алгоритм из [3] и заменяя k на k' и f на f' (последовательно для всех f' и k'), мы будем предполагать в дальнейшем без ограничения общности, что многочлен f является неприводимым над алгебраическим замыканием $\overline{k}$.

Далее, мы хотели бы использовать только теоремы 32 и 33 из [10, т. II, Глава 8 §13] вместе с результатами из раздела 1 в нашем доказательстве. Поэтому нам требуется некоторое сведение, после которого условия цитированных теорем 32 и 33 были бы выполнены.

Пусть $g = \sum\limits_{0 \leqslant w \leqslant \deg_Z g} g_w Z^w \in \overline{k}[[X_1, \ldots, X_n]][Z]$ – произвольный многочлен со всеми коэффициентами $g_w \in \overline{k}[[X_1, \ldots, X_n]]$. Тогда по определению положим

$$\widetilde{g} = \sum_{0 \leqslant w \leqslant \deg_Z g} g_w Z^w X_{n+1}^{\deg_Z(g)-w} \in \overline{k}[[X_1, \ldots, X_{n+1}]][Z],$$

где X_{n+1} – новая переменная. Заметим здесь, что $g = \widetilde{g}|_{X_{n+1}=1}$.

Лемма 3. *Пусть $f \in k[X_1, \ldots, X_n, Z]$ – многочлен из введения. Пусть $f = \prod\limits_{i \in I} f_i$ (соответственно $f_i = \prod\limits_{w \in J_i} f_w$, $i \in I$) является разложением на неприводимые множители полинома f (соответственно f_i) в кольце $k[[X_1, \ldots, X_n]][Z]$ (соответственно $\overline{k}[[X_1, \ldots, X_n]][Z]$), см. утверждения* (i) *и* (iii) *теоремы* 1. *Тогда $\widetilde{f} = \prod\limits_{i \in I} \widetilde{f}_i$ (соответственно $\widetilde{f}_i = \prod\limits_{w \in J_i} \widetilde{f}_w$, $i \in I$) является разложением на неприводимые множители многочлена $\widetilde{f}$ в кольце $k[[X_1, \ldots, X_{n+1}]][Z]$ (соответственно многочлена $\widetilde{f}_i$ в кольце $\overline{k}[[X_1, \ldots, X_{n+1}]][Z]$).*

Другими словами, отображение $f_i \mapsto \widetilde{f}_i$, $i \in I$ (соответственно $f_w \mapsto \widetilde{f}_w$, $w \in J_i$ для всякого $i \in I$) определяет взаимно однозначное соответствие между элементами рассматриваемых семейств неприводимых множителей.

Доказательство. Действительно, пусть $b \in \widehat{A}[Z]$, степень $\deg_Z b \geqslant 1$ и старший коэффициент $\mathrm{lc}_Z b = 1$. Предположим, что $\widetilde{b} = GH$, где $G, H \in \overline{k}[[X_1, \ldots, X_{n+1}]][Z]$, $\mathrm{lc}_Z G = \mathrm{lc}_Z H = 1$ и $\deg_Z G, \deg_Z H \geqslant 1$. Тогда можно представить $G = \sum\limits_{j' \leqslant j \in \mathbb{Z}} G_j$, $H = \sum\limits_{j'' \leqslant j \in \mathbb{Z}} H_j$, где все $G_j, H_j \in \widehat{A}[X_{n+1}, Z]$ являются однородными многочленами относительно X_{n+1}, Z с коэффициентами из $\widehat{A}$, степени $\deg_{X_{n+1},Z} G_j = j$, $\deg_{X_{n+1},Z} H_j = j$ (при условии, что эти полиномы не равны нулю) и $G_{j'} \neq 0$, $H_{j''} \neq 0$. Очевидно $j' \leqslant \deg_Z G$ и $j'' \leqslant \deg_Z H$. Многочлен $\widetilde{b}$ однороден относительно X_{n+1}, Z. Следовательно, $\widetilde{b} = G_{j'} H_{j''}$. Отсюда следует, что $j' = \deg_Z G$, $j'' = \deg_Z H$ и существуют многочлены $g, h \in \widehat{A}[Z]$ такие, что $G_{j'} = \widetilde{g}$, $H_{j''} = \widetilde{h}$. Поэтому $\widetilde{b} = \widetilde{g}\widetilde{h}$.

Следовательно, элемент b неприводим в кольце $\widehat{A}[Z]$ в том и только в том случае, если $\widetilde{b}$ неприводим в кольце $\overline{k}[[X_1, \ldots, X_{n+1}]][Z]$. Отсюда вытекают все утверждения леммы. □

Теперь мы можем применить лемму 3. Следовательно, заменяя n на $n+1$ и f на $\widetilde{f}$, мы будем предполагать, не умаляя общности, что $f(0, \ldots, 0, Z) = Z^{\deg_Z f}$. Поэтому число элементов $\pi_{n+1}^{-1}(x^*) = 1$ в обозначениях раздела 1. Положим $z^* = (0, \ldots, 0) \in \pi_{n+1}^{-1}(x^*)$. Обозначим через S_{x^*} мультипликативно замкнутое подмножество всех полиномов $s \in k[X_1, \ldots, X_n]$ таких, что $s(x^*) \neq 0$. Положим $A = S_{x^*}^{-1}\overline{k}[X_1, \ldots, X_n]$ равным локальному кольцу всех функций определённых над $\overline{k}$ и регулярных в окрестности точки $x^* \in \mathbb{A}^n(\overline{k})$, т.е. это локальное кольцо точки x^* на аффинном пространстве $\mathbb{A}^n(\overline{k})$. Обозначим через $\mathfrak{m}'$ максимальный идеал кольца A.

Далее, положим $E = A[Z]/(f) = \mathcal{O}_{z^*, \mathcal{Z}(f)}$ равным локальному кольцу точки z^* на алгебраическом многообразии $\mathcal{Z}(f)$ (напомним, что $\mathcal{Z}(f) \subset \mathbb{A}^{n+1}(\overline{k})$). Обозначим через E' целое замыкание кольца E в его поле частных K'. Следовательно, можно отождествить $E' = \overline{k} \otimes_k S_{x^*}^{-1} k[y_1, \ldots, y_N]$ в обозначениях раздела 1.

Мы строим систему образующих $y_1, \dots, y_N$, см. раздел 1. После этого мы применяем лемму 2 и строим все объекты из формулировки этой леммы. Напомним, что $y_v = X_v$ для $1 \leqslant v \leqslant n$, $z = y_{n+1}$, $q = Q(y_{n+1}, \dots, y_N)$, см. лемму 2, и поле $K' = \overline{k}(X_1, \dots, X_n)[Z]/(f)$.

Обозначим через z_v^*, $1 \leqslant v \leqslant \deg_Q \psi$, все элементы прообраза $\pi_N^{-1}(x^*)$, см. раздел 1. Положим S_v равным мультипликативно замкнутому подмножеству всех элементов $s \in k[y_1, \dots, y_N]$ таких, что $s(z_v^*) \neq 0$. Следовательно, $S_v \supset S_{x^*}$. Обозначим через $E'_v = \overline{k} \otimes_k S_v^{-1} k[y_1, \dots, y_N]$ локальное кольцо точки z_v^* на нормализации алгебраического многообразия $\mathcal{Z}(f)$. Следовательно, E'_v является локализацией кольца E'. Мы имеем естественное вложение колец $\iota : E' \to \prod\limits_{1 \leqslant v \leqslant \deg_Q \psi} E'_v$.

Кольцо $\widehat{A} = \overline{k}[[X_1, \dots, X_n]]$ совпадает с пополнением кольца A относительно $\mathfrak{m}'$-адической топологии. Обозначим через $\widehat{E}, \widehat{E}', \widehat{E}'_v$, $1 \leqslant v \leqslant \deg_Q \psi$, пополнения колец E, E', E'_v, $1 \leqslant v \leqslant \deg_Q \psi$, относительно $\mathfrak{m}'$-адической топологии. Следовательно, как хорошо известно, можно отождествить $\widehat{E} = \widehat{A} \otimes_A E$, $\widehat{E}' = \widehat{A} \otimes_A E'$ и $\widehat{E}'_v = \widehat{A} \otimes_A E'_v$ для всех i. Напомним, что $\overline{k}((X_1, \dots, X_n))$ является полем частных кольца $\widehat{A}$, см. замечание 1 во введении. Положим $\mathcal{K} = \overline{k}((X_1, \dots, X_n))[Z]/(f)$ равным полному кольцу частных кольца $\widehat{E}$. Можно отождествить $\mathcal{K} = \overline{k}((X_1, \dots, X_n)) \otimes_{\overline{k}(X_1, \dots, X_n)} K'$. Поэтому $\mathcal{K}$ является конечномерной сепарабельной алгеброй над $\overline{k}((X_1, \dots, X_n))$, и q является примитивным элементом алгебры $\mathcal{K}$ над $\overline{k}((X_1, \dots, X_n))$ по лемме 2 (i).

Согласно Теореме 33 из [10, т. II, Глава 8 §13] кольцо $\widehat{E}'$ является полулокальным, и оно изоморфно целому замыканию кольца $\widehat{E}$ в его полном кольце частных $\mathcal{K}$. По Теореме 32 из [10, т. II, Глава 8 §13] кольцо $\widehat{E}'_v$ является целостным и целозамкнутым, т.е. E'_v аналитически неприводимо и аналитически нормально.

Далее хорошо известно, что вложение ι индуцирует канонический изоморфизм полных колец $\widehat{\iota} : \widehat{E}' \to \prod\limits_{1 \leqslant v \leqslant \deg_Q \psi} \widehat{E}'_v$. Поэтому мы будем отождествлять $\widehat{E}' = \prod\limits_{1 \leqslant v \leqslant \deg_Q \psi} \widehat{E}'_v$ с помощью этого изоморфизма $\widehat{\iota}$. Обозначим через $\mathcal{K}_v$ поле частных кольца $\widehat{E}'_v$. Следовательно, мы можем отождествить $\mathcal{K} = \prod\limits_{1 \leqslant v \leqslant \deg_Q \psi} \mathcal{K}_v$.

Теперь, см. лемму 2 утверждение (i), q является примитивным элементом сепарабельной алгебры $\mathcal{K}$ над $\overline{k}((X_1,\dots,X_n))$ с минимальным многочленом F. Согласно лемме 2 (ii) число попарно различных корней многочлена $F(0,\dots,0,Q)$ равно в точности $\#\pi_N^{-1}(x^*) = \deg_Q \psi$. Рассмотрим разложение многочлена $F(0,\dots,0,Q)$ в произведение взаимно простых множителей (минимально возможных степеней) над полем $\overline{k}$. Применяя подъём по лемме Гензеля к этому разложению, мы доказываем существование $\deg_Q \psi$ попарно различных множителей $F_v \in \overline{k}[[X_1,\dots,X_n]][Q]$, $1 \leqslant v \leqslant \deg_Q \psi$, полинома F (мы предполагаем, что все старшие коэффициенты $\mathrm{lc}_Q F_v = 1$). Следовательно, можно отождествить $\mathcal{K}_v = \overline{k}((X_1,\dots,X_n))[Q]/(F_v)$ для $1 \leqslant v \leqslant \deg_Q \psi$.

Более точно, алгоритмически мы действуем следующим образом. Сначала, используя алгоритм из [3], мы находим разложение на неприводимые $F(0,\dots,0,Q) = \prod\limits_{1\leqslant j\leqslant m} \psi_j^{\varepsilon_j}$, где $\varepsilon_j \geqslant 1$ – некоторые целые числа. Мы представляем $\psi_j = (Q-q_j)\xi_j$, где многочлен $\xi_j \in k_j[Q]$. Положим $\varphi_j = \xi_j^{\varepsilon_j} \prod\limits_{1\leqslant w\leqslant m,\, w\neq j} \psi_w^{\varepsilon_w}$. Заметим, что многочлены $(Q-q_j)^{\varepsilon_j}$ и φ_j являются взаимно простыми в кольце $k_j[Q]$. Имеем $F(0,\dots,0,Q) = (Q-q_j)^{\varepsilon_j}\varphi_j$ в этом кольце. Следовательно, можно применить подъём по лемме Гензеля к последнему равенству и получить разложение $F = \Psi_j\Phi_j$ такое, что $\Psi_j, \Phi_j \in k_j[[X_1,\dots,X_n]][Q]$, $\Psi_j(0,\dots,0,Q) = (Q-q_j)^{\varepsilon_j}$, $\Phi_j(0,\dots,0,Q) = \varphi_j$ и старшие коэффициенты $\mathrm{lc}_Q\Psi_j = \mathrm{lc}_Q\Phi_j = 1$. Заметим, что фактически мы можем построить полиномы $(\Psi_j)_{\#,N}$, $(\Phi_j)_{\#,N}$ для всякого $N \geqslant 0$.

Можно представить $\Psi_j = \sum\limits_{v,i_1,\dots,i_n\geqslant 0} a_{j,v,i_1,\dots,i_n} X_1^{i_1}\cdot\ldots\cdot X_n^{i_n} Q^v$, где все коэффициенты $a_{j,v,i_1,\dots,i_n} \in k_j$. Тогда для всякого $\sigma \in G_j$ положим $\Psi_j^\sigma = \sum\limits_{v,i_1,\dots,i_n\geqslant 0} a^\sigma_{j,v,i_1,\dots,i_n} \cdot X_1^{i_1}\cdot\ldots\cdot X_n^{i_n} Q^v$. Теперь по лемме 2 множества полиномов

$$\{\Psi_j^\sigma \,:\, \sigma\in G_j,\ 1\leqslant j\leqslant m\} = \{F_v \,:\, 1\leqslant v\leqslant \deg_Q\psi\}$$

совпадают. Таким образом, можно построить разложение многочлена F на неприводимые множители над полем $\overline{k}((X_1,\dots,X_n))$ и, следовательно, получить изоморфизм $\mathcal{K} = \prod\limits_{1\leqslant v\leqslant \deg_Q\psi} \mathcal{K}_v$.

Вернёмся к многочлену f. Заметим, что $\overline{k}((X_1,\dots,X_n))[Z]/(f) = \mathcal{K}$ и можно отождествить

$$\overline{k}((X_1,\dots,X_n))[Z]/(f) = \prod_{i\in I}\prod_{w\in J_i}\overline{k}((X_1,\dots,X_n))[Z]/(f_w),$$

см. формулировку теоремы 1 (полиномы f_w, $w\in J_i$, $i\in I$, очевидно существуют, но они ещё не построены нами). Многочлен f_w неприводим над полем $\overline{k}((X_1,\dots,X_n))$, поскольку f_w неприводим в кольце $\overline{k}[[X_1,\dots,X_n]][Z]$ и кольцо формальных степенных рядов $\overline{k}[[X_1,\dots,X_n]]$ является целозамкнутым. Поэтому существует взаимно однозначное соответствие между элементами семейств многочленов f_w, $w\in\bigcup\limits_{i\in I} J_i$, и Ψ_j^σ, $\sigma\in G_j$, $1\leqslant j\leqslant m$. Именно f_w соответствует Ψ_j^σ тогда и только тогда, когда при описанных отождествлениях

$$\overline{k}((X_1,\dots,X_n))[Z]/(f_w) = \mathcal{K}_v \quad\text{и}\quad \overline{k}((X_1,\dots,X_n))[Z]/(\Psi_j^\sigma) = \mathcal{K}_v$$

для одного и того же индекса $1\leqslant v\leqslant \deg_Q\psi$.

Построим это соответствие явно. Обозначим через Δ дискриминант полинома F относительно Q. Используя соотношения (3) раздел 1 для $0\leqslant j<\deg_Z f$ и решая линейную систему над полем $k(X_1,\dots,X_n)$, мы строим представление $z=(1/\Delta)\sum\limits_{0\leqslant j<\deg_Q F} z_{j,i}q^i$, где все коэффициенты $z_{j,i}\in k[X_1,\dots,X_n]$. Для краткости положим $\alpha_j=\deg_Q\Psi_j$, $\beta_j=\deg_Q\Phi_j$, $1\leqslant j\leqslant m$.

Лемма 4. *Пусть $w\in J_i$, $i\in I$, см. формулировку теоремы 1. Тогда многочлен f_w соответствует Ψ_j^σ, см. выше, в том и только в том случае, если*

$$\Delta^{\alpha_j} f_w = \operatorname{Res}_Q\Big(\Psi_j^\sigma,\ \Delta Z - \sum_{0\leqslant j<\deg_Q F} z_{j,i}Q^i\Big), \tag{7}$$

где $\operatorname{Res}_Q(\dots)$ обозначает результант рассматриваемых многочленов из $\overline{k}[[X_1,\dots,X_n]][Z,Q]$ относительно Q. Далее, в этом случае

$$\Delta^{\beta_j}\prod_{w_1\in J_i,\,w_1\neq w} f_{w_1} = \operatorname{Res}_Q\Big(\Phi_j^\sigma,\ \Delta Z - \sum_{0\leqslant j<\deg_Q F} z_{j,i}Q^i\Big), \tag{8}$$

$$\Delta^{\alpha_j+\beta_j} f_i = \operatorname{Res}_Q\Big(\Phi_j\cdot\Psi_j,\ \Delta Z - \sum_{0\leqslant j<\deg_Q F} z_{j,i}Q^i\Big). \tag{9}$$

Поэтому многочлены

$$\Delta^{\alpha_j} f_w,\ \Delta^{\beta_j} \cdot \prod_{w_1 \in J_i,\, w_1 \neq w} f_{w_1} \in k[q_j^\sigma][[X_1, \ldots, X_n]][Z], \tag{10}$$

$$\Delta^{\alpha_j+\beta_j} f_i \in k[[X_1, \ldots, X_n]][Z] \tag{11}$$

и, см. формулировку теоремы 1, *можно взять* $I = \{1, 2, \ldots, m\}$, $J_i = G_i$, $\varphi_i = \psi_i$ *для всякого* $1 \leqslant i \leqslant m$ *и* $\eta_w = q_i^\sigma$, *где* $w = \sigma \in J_i$ *для всех* $1 \leqslant i \leqslant m$ *и* $w \in J_i$.

Доказательство. Первые два утверждения леммы (относящиеся к (7), (8) и (9)) следуют немедленно из свойств результанта двух полиномов. Фактически это хорошо известно.

Теперь (10) следует из (7) и (8). Аналогично (11) следует из (10), поскольку $\Phi_j \cdot \Psi_j \in k[[X_1, \ldots, X_n]][Q]$. Наконец, последнее утверждение о $I, J_i, \varphi_i, \eta_w$ получается непосредственно. Лемма доказана. □

В дальнейшем мы предполагаем, что справедливы формулы, определяющие $I, J_i, \varphi_i, \eta_w$ из последнего утверждения леммы 4.

Лемма 5. *Пусть* $a, b, c \in \widehat{A}$, $a = bc$ *и* $a \neq 0$. *Пусть* $\operatorname{ord}(a) = \mu$, $\operatorname{ord}(b) = \nu$, $a = \sum\limits_{i \geqslant 0} a_{\mu+i}$, $b = \sum\limits_{i \geqslant 0} b_{\nu+i}$, *где каждое ненулевое* $a_{\mu+i}$ (*соответственно* $b_{\nu+i}$) *является однородным многочленом из* $\overline{k}[X_1, \ldots, X_n]$ *степени* $\mu + i$ (*соответственно* $\nu + i$). *Тогда* $\operatorname{ord}(c) = \mu - \nu$, *и можно представить* $c = \sum\limits_{i \geqslant 0} c_{\mu-\nu+i}$, *где каждое ненулевое* $c_{\mu-\nu+i}$ *является однородным многочленом из* $\overline{k}[X_1, \ldots, X_n]$ *степени* $\mu - \nu + i$. *Далее, для всякого целого числа* $i \geqslant 0$

$$c_{\mu-\nu+i} = \Big(a_{\mu+i} - \sum_{1 \leqslant j \leqslant i} b_{\nu+j} c_{\mu-\nu+i-j} \Big) \Big/ b_\nu \tag{12}$$

Поэтому, если для целого числа $N \geqslant 0$ *даны многочлены* $a_{\#,\mu+N}$ *и* $b_{\#,\nu+N}$, *то, используя* (12), *можно построить последовательно все полиномы* $c_{\mu-\nu+i}$ *для* $0 \leqslant i \leqslant N$. *Следовательно, при этих условиях можно построить многочлен* $c_{\#,\mu-\nu+N}$.

Доказательство. Все утверждения леммы получаются непосредственно, и их доказательства мы оставляем читателю. Лемма доказана. □

Заметим, что достаточно построить многочлены f_w for $w = \sigma = \mathrm{id}$ и $1 \leqslant j \leqslant \deg_Q \psi$, где id – тождественное вложение, но для нас удобно рассматривать произвольное σ ниже.

Напомним, что число r определено во введении. Положим целые числа $\gamma_1{=}\alpha_j$, $\gamma_2{=}\beta_j$, $\gamma_3{=}\alpha_j{+}\beta_j$. Обозначим $N_i = r + \gamma_i \deg_{X_1,\dots,X_n} \Delta$, $i = 1, 2, 3$. Вычислим многочлены $(\Psi_j^\sigma)_{\#,N_1}$, $(\Phi_j^\sigma)_{\#,N_2}$ и $(\Phi_j \cdot \Psi_j)_{\#,N_3}$, см. выше. Заменяя в (7) (соответственно (8), (9)) многочлен Ψ_j^σ (соответственно Φ_j^σ, $\Phi_j \cdot \Psi_j$) на $(\Psi_j^\sigma)_{\#,N_1}$ (соответственно $(\Phi_j^\sigma)_{\#,N_2}$, $(\Phi_j \cdot \Psi_j)_{\#,N_3}$), вычислим полином $(\Delta^{\alpha_j} f_w)_{\#,N_1}$ (соответственно

$$(\Delta^{\beta_j} \prod_{w_1 \in J_i,\, w_1 \neq w} f_{w_1})_{\#,N_2},$$

$(\Delta^{\alpha_j+\beta_j} f_i)_{\#,N_3}$). Заметим, что $\operatorname{ord}\Delta \leqslant \deg_{X_1,\dots,X_n} \Delta$. Пусть $H \in \overline{k}(X_1, \dots, X_n)[Z]$ является одним из многочленов

$$(\Delta^{\alpha_j} f_w)_{\#,N_1}, \quad \Big(\Delta^{\beta_j} \prod_{w_1 \in J_i,\, w_1 \neq w} f_{w_1}\Big)_{\#,N_2}, \quad (\Delta^{\alpha_j+\beta_j} f_i)_{\#,N_3},$$

и a – коэффициент многочлена H (фактически мы перебираем все коэффициенты полинома H как значения a). Положим $b = \mathrm{lc}_Z H$ равным старшему коэффициенту многочлена H. Мы применяем лемму 5 с a и b для всех возможных a. В результате мы вычислим многочлены

$$(f_w)_{\#,r}, \qquad \Big(\prod_{w_1 \in J_i,\, w_1 \neq w} f_{w_1}\Big)_{\#,r}, \qquad (f_i)_{\#,r}$$

для всех $i \in I$, $w \in J_i$ (здесь мы оставляем подробности читателю). После этого мы вычисляем все многочлены

$$\Big(\prod_{i_1 \in I,\, i_1 \neq i} f_{i_1}\Big)_{\#,r} = \Big(\prod_{i_1 \in I,\, i_1 \neq i} (f_{i_1})_{\#,r}\Big)_{\#,r}, \quad i \in I.$$

Таким образом, утверждения (i)–(iii) теоремы 1 доказаны. Утверждение (iv) теоремы 1 следует немедленно из оценок на время работы применяемых в доказательстве теоремы алгоритмов. Теорема 1 доказана. □

Список литературы

1. З. И. Боревич, И. Р. Шафаревич, *Теория чисел*, М., Наука, 1964.
2. Н. Бурбаки, *Коммутативная алгебра*, М., Москва, 1971.

3. 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.
4. 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.
5. A. L. Chistov, *An overview of effective normalization of a nonsingular in codimension one projective algebraic variety.* — Зап. научн. семин. ПОМИ **373** (2009), 295–317.
6. А. Л. Чистов, *Эффективная нормализация неособого в коразмерности один алгебраического ногообразия.* — Докл. Академии наук **427**, No. 5 (2009), 605–608.
7. 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.
8. H. Flenner, *Die Sätze von Bertini für lokale Ringe.* — Math. Ann. **229** (1977), 97–111.
9. A. Seidenberg, *Constructions in algebra*, Transactions of the American Mathematical Society **197** (1974) pp. 273–313.
10. О. Зарисский, П. Самюэль, *Коммутативная алгебра*, т. I-II, Издательство иностранной литературы, Москва, 1963.

Chistov A. L. An algorithm for factoring polynomials in the ring of multivariable formal power series in zero–characteristic.

We suggest algorithms for factoring polynomials in the rings of multivariables formal power series over the ground field of zero–characteristic and over an algebraic closure of this ground field. Also we construct algorithms for factoring monic polynomials in one variable over these formal power series rings. We give explicit estimates for the complexity of suggested algorithms. These results are important for local investigation of algebraic varieties from the algorithmic point of view.

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

Поступило 12 сентября 2022 г.