Записки научных
семинаров ПОМИ
Том 528, 2023 г.

А. Л. Чистов

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

Введение

Данная статья продолжает работу [8] и является её второй частью. В [8] и настоящей статье нумерация теорем (соответственно лемм, выделенных формул и т. д.) одна и та же. В этой статье она продолжается из [8]. Также мы используем обозначения и предположения из введения из [8]. В настоящей статье мы добавили к списку литературы из [8] некоторые другие работы, а также упорядочили его по-новому для удобства.

Основной результат данной статьи – это теорема 3 из §5. Там мы улучшаем теорему 1 [8] и получаем новую версию алгоритма для факторизации унитарных многочленов от одной переменной над кольцом формальных степенных рядов от многих переменных в нулевой характеристике. Именно, сложность алгоритма из теоремы 3 §5 полиномиальна от d^n (конечно, она зависит и от других параметров) в то время, как она полиномиальна от $d^{2^{n^c}}$ для некоторой константы $c > 0$ в теореме 1 [8]. Это главное улучшение. Кроме того, формулировка теоремы 3 является более подробной. Во-первых, во всех оценках теоремы 3 степень трансцендентности l (основного поля k над его примитивным подполем) не предполагается фиксированной константой, как в теореме 1 [8]. Во-вторых, мы приводим явные оценки на знаменатели всех полученных объектов. Мы применяем теорему Бертини для локальных областей целостности, см. [13], для доказательства теоремы 3. И то, что рассматриваемые степени трансцендентности (l и другие) не являются фиксированными, существенно для доказательства теоремы 3.

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

Как следствие теоремы 3 мы получаем новый алгоритм для факторизации многочленов в кольце формальных степенных рядов от многих переменных, следствие 8 §5, ср. следствие 1 и следствие 2 из [8]. Теперь его сложность по существу та же самая, что и сложность алгоритма из теоремы 3.

Для доказательства Теоремы 3 нам требуется прежде всего тщательно проанализировать сложность хорошо известной теоремы 1 §3 Глава IV [1] о факторизации многочленов над полем полным относительно дискретного нормирования. В §3 мы модифицируем доказательство последней теоремы с алгоритмической точки зрения (мы рассматриваем только нашу ситуацию кольца формальных степенных рядов), см. лемму 6 и её следствия.

Заметим, что после этого анализа цитированной теоремы из [1] мы нашли небольшое исправление наших предыдущих результатов, см. замечание 6 §3 и [12].

В §4, применяя лемму 6 §3 и её следствия, мы доказываем теорему 2, которая является аналогом теоремы 1 [8] с дополнительными деталями и в более общей ситуации. В частности в формулировке теоремы 2 базис трансцендентности основного поля над $\mathbb{Q}$ состоит из двух семейств $T_1, \dots, T_l$ и $u_1, \dots, u_{l_1}$. В теореме 2 все оценки степеней и длин записи целых коэффициентов всех объектов на выходе алгоритма и его сложность зависят явно от l и l_1.

Теорема 2 требуется для доказательства основного результата, т.е. теоремы 3 §5. То, что l и l_1 (особенно l_1) не являются фиксированными важно для доказательства основного результата в этом параграфе.

В одной из следующих статей мы надеемся изложить некоторые приложения теоремы 3.

§1. Сложность известного результата о факторизации многочленов над полем полным относительно дискретного нормирования

Сначала нам необходимо изложить теорему 1 §3, глава IV [1] в более алгоритмической форме (сейчас мы рассматриваем только нашу ситуацию формальных степенных рядов). В лемме 6 ниже мы модифицируем доказательство этой теоремы.

Пусть Λ – целостное кольцо с полем частных K. Пусть $f, \overline{g}, \overline{h} \in \Lambda[X, Z]$ являются многочленами со старшими коэффициентами $\mathrm{lc}_Z f =$

$\operatorname{lc}_Z \overline{g} = \operatorname{lc}_Z \overline{h} = 1$ и степенями $\deg_Z \overline{g} = n_1 \geqslant 1$, $\deg_Z \overline{h} = n_2 \geqslant 1$, $\deg_X \overline{g} \leqslant m_1$, $\deg_X \overline{h} \leqslant m_2$.

Пусть $\overline{R} = \operatorname{Res}_Z(\overline{g}, \overline{h})$ является результантом многочленов $\overline{g}, \overline{h}$ относительно Z. Следовательно, $\overline{R} \in \Lambda[X]$. Мы предполагаем, что $\overline{R} \neq 0$. Пусть $\operatorname{ord}_X \overline{R} = \overline{\rho} \geqslant 0$ и $\operatorname{ord}_X(\overline{R} - aX^{\overline{\rho}}) > \overline{\rho}$ для некоторого элемента $0 \neq a \in \Lambda$. Наконец, предположим, что $\operatorname{ord}_X(f - \overline{g}\overline{h}) \geqslant 2\rho_1 + 1$ для целого числа $\rho_1 \geqslant \overline{\rho}$ (поэтому $\deg_Z f = n_1 + n_2$). Положим $\rho = 2\rho_1 - \overline{\rho}$.

Лемма 6. *При сформулированных условиях существует последовательность многочленов $g_{\rho+i}, h_{\rho+i} \in K[X, Z]$, $i \geqslant 1$, удовлетворяющая следующим свойствам. Для всех i степени $\deg_Z g_{\rho+i} < n_1$, $\deg_Z h_{\rho+i} < n_2$,*

$$\deg_X g_{\rho+i} \leqslant \min\{\overline{\rho}, n_1 m_2 + n_2 m_1\}, \quad \deg_X h_{\rho+i} \leqslant \min\{\overline{\rho}, n_1 m_2 + n_2 m_1\}.$$

Для всякого целого числа $j \geqslant 0$ порядок

$$\operatorname{ord}_X \Big(f - \Big(\overline{g} + \sum_{1 \leqslant i \leqslant j} g_{\rho+i} X^{\rho+i} \Big) \Big(\overline{h} + \sum_{1 \leqslant i \leqslant j} h_{\rho+i} X^{\rho+i} \Big) \Big) \geqslant 2\rho_1 + j + 1. \quad (13)$$

Для всякого $i \geqslant 1$

$$a^{2i-1} g_{\rho+i} \in \Lambda[X, Z], \quad a^{2i-1} h_{\rho+i} \in \Lambda[X, Z]. \quad (14)$$

Положим $g = \overline{g} + \sum\limits_{i \geqslant 1} g_{\rho+i} X^{\rho+i} \in K[[X]][Z]$, $h = \overline{g} + \sum\limits_{i \geqslant 1} h_{\rho+i} X^{\rho+i} \in K[[X]][Z]$. Тогда $f = gh$ в кольце $K[[X]][Z]$.

Заметим также, что фактически многочлены $g_{\rho+i}, h_{\rho+i}$, $i \geqslant 1$, однозначно определены в конструкции из доказательства леммы.

Доказательство. Докажем при помощи индукции по $j \geqslant 0$ существование полиномов $g_{\rho+i}, h_{\rho+i}$, удовлетворяющих неравенствам на степени и (13), (14) для $1 \leqslant i \leqslant j$. Для базы индукции $j = 0$ неравенство (13) выполнено согласно условиям леммы и (14) тривиально. Предположим, что $j \geqslant 1$ и индукционное предположение доказано для $j - 1$. Тогда мы можем представить

$$f - \Big(\overline{g} + \sum_{1 \leqslant i \leqslant j-1} g_{\rho+i} X^{\rho+i} \Big) \Big(\overline{h} + \sum_{1 \leqslant i \leqslant j-1} h_{\rho+i} X^{\rho+i} \Big) = \sum_{m \geqslant 0} q_{2\rho_1+j+m} X^{2\rho_1+j+m}, \quad (15)$$

где все $q_{2\rho_1+j+m} \in K[Z]$ и степени $\deg_Z q_{2\rho_1+j+m} < n_1+n_2$. Мы имеем $2\rho \geqslant 2\rho_1$. Поэтому из (15) следует, что

$$f - \overline{g}\overline{h} - \sum_{1\leqslant i\leqslant j-1} (\overline{g}h_{\rho+i} + \overline{h}g_{\rho+i})X^{\rho+i} - \sum_{\substack{1\leqslant i_1,i_2\leqslant j-1,\\ i_1+i_2\leqslant j}} g_{\rho+i_1}h_{\rho+i_2}X^{2\rho+i_1+i_2} = q_{2\rho_1+j}X^{2\rho_1+j} + qX^{2\rho_1+j+1} \quad (16)$$

для некоторого многочлена $q \in K[X,Z]$. Теперь из (14) для $1 \leqslant i \leqslant j-1$ и (16) следует, что $a^{2j-2}q_{2\rho_1+j} \in \Lambda[Z]$ (здесь мы оставляем подробности читателю).

Решая невырожденную линейную систему с квадратной матрицей Сильвестра полиномов $\overline{g}, \overline{h}$ (рассматриваемых как многочлены от Z), мы находим полиномы $u, v \in K[X,Z]$ такие, что $\overline{g}u + \overline{h}v = -\overline{R}q_{2\rho_1+j}$ и степени $\deg_Z u < n_2$, $\deg_Z v < n_1$, $\deg_X u \leqslant n_1m_2 + n_2m_1$, $\deg_X v \leqslant n_1m_2 + n_2m_1$. Более того, из правила Крамера следует, что $a^{2j-2}u$, $a^{2j-2}v \in \Lambda[Z]$.

Представим $u = \sum\limits_{0\leqslant i\leqslant \deg_X u} u_iX^i$, $v = \sum\limits_{0\leqslant i\leqslant \deg_X v} v_iX^i$, где все $u_i, v_i \in K[Z]$. Положим

$$g_{\rho+j} = \sum_{0\leqslant i\leqslant \min\{\overline{\rho},\deg_X v\}} v_iX^i/a, \quad h_{\rho+j} = \sum_{0\leqslant i\leqslant \min\{\overline{\rho},\deg_X u\}} u_iX^i/a.$$

Тогда удовлетворяются требуемые неравенства на степени многочленов $g_{\rho+j}$, $h_{\rho+j}$ и выполняется (14) для $1 \leqslant i \leqslant j$. Далее, можно представить

$$\overline{g}h_{\rho+j}X^{\rho+j} + \overline{h}g_{\rho+j}X^{\rho+j} = -X^{2\rho_1+j}q_{2\rho_1+j} + X^{2\rho_1+j+1}q' \quad (17)$$

для некоторого многочлена $q' \in K[X,Z]$. Теперь из (15) и (17) следует (13). Индуционное предположение доказано. Лемма доказана. □

Замечание 3. В лемме 6 можно заменить многочлены $\overline{g}, \overline{h}$ на $\overline{g}_{\#,2\rho_1}$, $\overline{h}_{\#,2\rho_1}$ и, следовательно, предполагать дополнительно без ограничения общности, что $m_1 \leqslant 2\rho_1$, $m_2 \leqslant 2\rho_1$.

Следствие 3. *При условиях леммы 6 обозначим через $\delta \in \Lambda[X]$ (соответственно δ_1, δ_2, $\overline{\delta}$, $\overline{\delta}_1$, $\overline{\delta}_2$) дискриминант многочлена f (соответственно g, h, $\overline{g}\overline{h}$, $\overline{g}$, $\overline{h}$) относительно Z. Положим* $\operatorname{ord}_X(\delta) = r \geqslant 0$. *Если $\delta \neq 0$, то существует единственное $\delta_0 \in \Lambda$ такое, что* $\operatorname{ord}_X(\delta - \delta_0X^r) > r$.

Обозначим через $R = \mathrm{Res}_Z(g,h) \in K[Z]$ *результант многочленов* g, h *относительно* Z. *Тогда очевидно порядки* $\mathrm{ord}_X R = \overline{\rho}$, $\mathrm{ord}_X(R - aX^{\overline{\rho}}) > \overline{\rho}$.

Если $2\rho_1 \geqslant r$, *то* $r \geqslant 2\overline{\rho}$, $\delta \neq 0$, $\overline{\delta} \neq 0$, $\mathrm{ord}_X(\delta) = \mathrm{ord}_X(\overline{\delta}) = r < +\infty$, $\mathrm{ord}_X(\delta - \overline{\delta}) > r$, $\delta = \pm\delta_1\delta_2 R^2$, $\overline{\delta} = \pm\overline{\delta}_1\overline{\delta_2}\,\overline{R}^2$, $\mathrm{ord}_X(\delta_i) = \mathrm{ord}_X(\overline{\delta}_i)$, $\mathrm{ord}_X(\delta_i - \overline{\delta}_i) > \mathrm{ord}_X(\overline{\delta}_i)$ *для* $i = 1, 2$ *и* a^2 *делит* δ_0 *в кольце* Λ.

Доказательство. Действительно, если $2\rho_1 \geqslant r$, то $\mathrm{ord}_X(f - \overline{g}\overline{h}) \geqslant 2\rho_1 + 1 > r$. Поэтому $\mathrm{ord}_X(\delta) = \mathrm{ord}_X(\overline{\delta}) = r < +\infty$ и $\mathrm{ord}_X(\delta - \overline{\delta}) > r$. Мы имеем $\delta = \pm\delta_1\delta_2 R^2$, $\overline{\delta} = \pm\overline{\delta}_1\overline{\delta_2}\,\overline{R}^2$. Следовательно, $\overline{\delta}_1\overline{\delta}_2 \neq 0$ и $r \geqslant 2\overline{\rho}$.

Положим $\mathrm{ord}_X(\overline{\delta}_1) = \rho' \geqslant 0$, $\mathrm{ord}_X(\overline{\delta}_2) = \rho'' \geqslant 0$. Пусть $a', a'' \in \Lambda$ такие, что $\mathrm{ord}_X(\overline{\delta}_1 - a'X^{\rho'}) > \rho'$ и $\mathrm{ord}_X(\overline{\delta}_2 - a''X^{\rho''}) > \rho''$. Теперь $r = \mathrm{ord}_X(\delta) = \rho' + \rho'' + 2\overline{\rho}$. Поэтому $\rho' \leqslant r - 2\overline{\rho} \leqslant 2\rho_1 - 2\overline{\rho}$, $\rho'' \leqslant r - 2\overline{\rho} \leqslant 2\rho_1 - 2\overline{\rho}$.

С другой стороны, $\mathrm{ord}_X(\overline{g} - g) > 2\rho_1 - \overline{\rho}$, $\mathrm{ord}_X(\overline{h} - h) > 2\rho_1 - \overline{\rho}$. Следовательно, $\mathrm{ord}_X(\delta_1) = \rho'$, $\mathrm{ord}_X(\delta_2) = \rho''$ и $\mathrm{ord}_X(\delta_1 - \overline{\delta_1}) > \rho'$, $\mathrm{ord}_X(\delta_2 - \overline{\delta_2}) > \rho''$. Мы имеем $\delta = \pm\delta_1\delta_2 R^2 \in K[X]$. Наконец, $\delta_0/a^2 = \pm a'a'' \in \Lambda$. Отсюда вытекает последнее утверждение следствия. Следствие доказано. □

Следствие 4. *При условиях леммы 6 и следствия 3 предположим, что* $\rho_1 \geqslant [r/2]$ *(заметим, что если* $\mathrm{ord}_X(f - \overline{g}\overline{h}) \geqslant r$, *то можно взять* $\rho_1 = [r/2]$ *в формулировке леммы 6). Положим* $\rho' = [r/2]$. *Тогда можно заменить в формулировке леммы 6 набор из 8 элементов* $(f, \overline{g}, \overline{h}, \overline{\rho}, \rho_1, a, m_1, m_2)$ *на*

$$(f, \overline{g}_{\#,2\rho'}, \overline{h}_{\#,2\rho'}, \overline{\rho}, \rho', a, \min\{m_1, 2\rho'\}, \min\{m_2, 2\rho'\}).$$

Доказательство. Действительно, $\rho_1 \geqslant \rho' \geqslant \overline{\rho}$. Теперь $\mathrm{ord}_X(f - \overline{g}\overline{h}) \geqslant 2\rho_1 + 1$. Поэтому $\mathrm{ord}_X(\mathrm{Res}_Z(\overline{g}_{\#,2\rho'}, \overline{h}_{\#,2\rho'})) = \overline{\rho}$, $\mathrm{ord}_X(\mathrm{Res}_Z(\overline{g}_{\#,2\rho'}, \overline{h}_{\#,2\rho'}) - aX^{\overline{\rho}}) > \overline{\rho}$, $\mathrm{ord}_X(f - \overline{g}_{\#,2\rho'}\overline{h}_{\#,2\rho'}) \geqslant 2\rho' + 1$. Отсюда следует требуемое утверждение. Следствие доказано. □

Замечание 4. В утверждении следствия 4 можно положить $\rho' = [(r + 1)/2]$ (вместо $\rho' = [r/2]$). В этом случае дополнительно $2\rho' \geqslant r$.

Замечание 5. Согласно замечанию 3 при условиях леммы 6 мы можем предполагать, не умаляя общности, что $\deg_X \overline{g}, \deg_X \overline{h} \leqslant 2\rho_1$. Предположим, что дискриминант $\delta \neq 0$, целое число $\rho_1 \geqslant [r/2]$, см.

утверждения следствий 3 and 4. Тогда, применяя следствие 4 и заменяя при необходимости многочлены $\overline{g}, \overline{h}$ (и целое число ρ_1) на новые, мы получаем полиномы $\overline{g}, \overline{h}$ такие, что

$$\deg_X \overline{g} \leqslant 2[r/2] \quad \text{и} \quad \deg_X \overline{h} \leqslant 2[r/2] \tag{18}$$

(очевидно сейчас $2[r/2] \leqslant 2d^2$). Следовательно, в любом случае при условиях леммы 6, если $\delta \neq 0$, то можно предполагать без ограничения общности, что выполняется (18).

Следствие 5. *Пусть Λ – такое же, как и выше, и $0 \neq c \in \Lambda$. Положим кольцо $\Lambda' = \Lambda[1/c]$. Предположим, что выполняются условия леммы 6 для кольца Λ' вместо Λ. Предположим дополнительно, что многочлены $cf \in \Lambda[X, Z]$, $c\overline{g} \in \Lambda[X, Z]$, $c\overline{h} \in \Lambda[X, Z]$. Тогда $ac^{n_1 n_2} \in \Lambda$ и для всех $i \geqslant 1$ полиномы*

$$c^{n_1}(ac^{n_1 n_2})^{2i-1} g_{\rho+i} \in \Lambda[X, Z], \quad c^{n_2}(ac^{n_1 n_2})^{2i-1} h_{\rho+i} \in \Lambda[X, Z]. \tag{19}$$

Доказательство. Положим $Z_1 = cZ$, $F = c^{n_1+n_2} f(Z_1/c)$, $\overline{G} = c^{n_1}\overline{g}(Z_1/c)$, $\overline{H} = c^{n_2}\overline{h}(Z_1/c)$. Тогда можно применить лемму 6 с $Z_1, F, \overline{G}, \overline{H}$ вместо $Z, f, \overline{g}, \overline{h}$ и получить многочлены $F_{\rho+i}, G_{\rho+i} \in \Lambda[X, Z_1]$, $i \geqslant 1$. Теперь a из формулировки следствия заменяется на $ac^{n_1 n_2} \in \Lambda$. Поэтому согласно лемме 6 мы имеем $(ac^{n_1 n_2})^{2i-1} G_{\rho+i} \in \Lambda[X, Z_1]$, $(ac^{n_1 n_2})^{2i-1} H_{\rho+i} \in \Lambda[X, Z_1]$, $i \geqslant 1$. Очевидно для всех $i \geqslant 1$

$$g_{\rho+i} = G_{\rho+i}(X, Zc)/c^{n_1} \quad h_{\rho+i} = G_{\rho+i}(X, Zc)/c^{n_2}.$$

Отсюда вытекает (19). Следствие доказано. □

Прежде чем формулировать следующие следствия, нам необходимо ввести некоторые новые объекты. Пусть k' – конечное расширение поля k, где k – из введения статьи [8]. Пусть $u_1, \ldots, u_{l_1}$ – трансцендентные элементы над k'. Положим поле $K^{(1)} = k'(u_1, \ldots, u_{l_1})$. Сейчас мы будем предполагать, что степени трансцендентности l и l_1 не являются фиксированными (т.е., мы не рассматриваем l и l_1 как константы). Имеем $l, l_1 \geqslant 0$.

Далее мы предполагаем (без ограничения общности), что многочлен $\varphi \in \mathbb{Z}[T_1, \ldots, T_l, Y]$, см. введение [8], и старший коэффициент $\mathrm{lc}_Y \varphi = 1$. Поле k' задаётся примитивным элементом η' над полем k. Минимальный многочлен $\psi' \in k[Y]$ элемента η' над k задан. Пусть $\lambda \in \mathbb{Z}[T_1, \ldots, T_l]$ – наименьшее общее кратное всех знаменателей из последнего кольца коэффициентов полинома ψ', следовательно, $\lambda\psi' \in$

$\mathbb{Z}[T_1, \ldots, T_l, \eta][Y]$. Если необходимо, мы можем заменить η' на $\lambda(\mathrm{lc}_Y \psi')\eta'$ и предполагать, не умаляя общности, что $\psi' \in \mathbb{Z}[T_1, \ldots, T_l, \eta][Y]$ и старший коэффициент $\mathrm{lc}_Y \psi' = 1$.

Обозначим через $\mathcal{N} : K^{(1)} \to \mathbb{Q}(T_1, \ldots, T_l, u_1, \ldots, u_{l_1})$ отображение нормы расширения полей $K^{(1)} \supset \mathbb{Q}(T_1, \ldots, T_l, u_1, \ldots, u_{l_1})$. Положим $\Lambda_0 = \mathbb{Z}[T_1, \ldots, T_l, u_1, \ldots, u_{l_1}]$ и $\Lambda_1 = \Lambda_0[\eta, \eta']$. Следовательно, Λ_1 является свободным Λ_0-модулем с базисом $\eta^i(\eta')^j$, $0 \leqslant i < \deg_Y \varphi$, $0 \leqslant j < \deg_Y \psi'$. Мы имеем $\mathcal{N}(\Lambda_1) \subset \Lambda_0$. Для любого $0 \neq a \in \Lambda_1$, решая линейную систему над полем $\mathbb{Q}(T_1, \ldots, T_l, u_1, \ldots, u_{l_1})$, можно найти элемент $a' \in \Lambda$ такой, что $1/a = a'/\mathcal{N}(a)$.

Пусть $X_1, \ldots, X_n$ – переменные. Тогда каждый многочлен $q \in K^{(1)}[X_1, \ldots, X_n]$ представляется в виде

$$q = (1/q^{(0)}) \sum_{i_1, \ldots, i_n \geqslant 0} \sum_{0 \leqslant i < \deg_Y \varphi} \sum_{0 \leqslant j < \deg_Y \psi'} q_{i_1, \ldots, i_n, i, j} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n} \eta^i (\eta')^j, \tag{20}$$

где все $q^{(0)}, q_{i_1, \ldots, i_n, i, j} \in \Lambda_0$ и $\mathrm{G\,C\,D}_{i_1, \ldots, i_n, i, j}(q^{(0)}, q_{i_1, \ldots, i_n, i, j}) = 1$ в кольце Λ_0. Степени

$$\deg_{u_1, \ldots, u_{l_1}} q = \max_{i_1, \ldots, i_n, i, j} \{\deg_{u_1, \ldots, u_{l_1}} q^{(0)}, \deg_{u_1, \ldots, u_{l_1}} q_{i_1, \ldots, i_n, i, j}\},$$

$$\deg_{T_1, \ldots, T_l} q = \max_{i_1, \ldots, i_n, i, j} \{\deg_{T_1, \ldots, T_l} q^{(0)}, \deg_{T_1, \ldots, T_l} q_{i_1, \ldots, i_n, i, j}\}$$

и длина записи целых коэффициентов $\mathrm{l}(q) = \max_{i_1, \ldots, i_n, i, j}\{\mathrm{l}(q^{(0)}), \mathrm{l}(q_{i_1, \ldots, i_n, i, j})\}$ определяются естественным образом, ср. введение [8], где рассматривается случай $l_1 = 0$ и $k' = k$.

Напомним, что степень $\deg_{T_1, \ldots, T_l, Y} \varphi \leqslant d_1$ и длина записи целых коэффициентов $\mathrm{l}(\varphi) \leqslant M_1$ для некоторых положительных целых чисел M_1 и d_1, см. введение [8]. Можно определить естественным образом $\deg_{T_1, \ldots, T_l, Y} \psi'$ и длину записи целых коэффициентов $\mathrm{l}(\psi')$. Мы предполагаем, что степень $\deg_{T_1, \ldots, T_l, Y} \psi' \leqslant d_1'$ и длина записи целых коэффициентов $\mathrm{l}(\psi') \leqslant M_1'$ для некоторых положительных целых чисел M_1' и d_1' Сейчас мы считаем также, что $d_1, d_1' \geqslant 2$.

Пусть даны многочлены $f, \overline{g}, \overline{h} \in K^{(1)}[X_1, \ldots, X_n, Z]$ (здесь $n \geqslant 1$). Предположим, что их старшие коэффициенты $\mathrm{lc}_Z f = \mathrm{lc}_Z \overline{g} = \mathrm{lc}_Z \overline{h} = 1$. Предположим, что $cf, c\overline{g}, c\overline{h} \in \Lambda_1[X_1, \ldots, X_n]$ для некоторого элемента $0 \neq c \in \Lambda_0$ (конечно, элемент c известен из представлений (20) для f, $\overline{g}$, $\overline{h}$). Далее, мы предполагаем, что справедливы следующие неравенства

для степеней и длин записи целых коэффициентов:

$$\deg_{X_1,\dots,X_n,Z} f \leqslant d,\ \ \deg_{T_1,\dots,T_l} f < d_2,\ \ \deg_{u_1,\dots,u_{l_1}} f < d_3,\ \ \mathrm{l}(f) \leqslant M_2, \tag{21}$$

$$\deg_{T_1,\dots,T_l} \overline{g} < d_4, \quad \deg_{T_1,\dots,T_l} \overline{h} < d_4, \quad \deg_{T_1,\dots,T_l} c < d_4, \tag{22}$$

$$\deg_{u_1,\dots,u_{l_1}} \overline{g} < d_5, \quad \deg_{u_1,\dots,u_{l_1}} \overline{h} < d_5, \quad \deg_{u_1,\dots,u_{l_1}} c < d_5, \tag{23}$$

$$\mathrm{l}(\overline{g}) \leqslant M_3, \quad \mathrm{l}(\overline{h}) \leqslant M_3, \quad \mathrm{l}(c) \leqslant M_3 \tag{24}$$

для некоторых положительных целых чисел M_2, M_3 и $d, d_2, d_3, d_4, d_5 \geqslant 2$. Предположим, что

$$\deg_{X_1,\dots,X_n} \overline{g} \leqslant \mathcal{P}(d), \quad \deg_{X_1,\dots,X_n} \overline{h} \leqslant \mathcal{P}(d) \tag{25}$$

для некоторого полинома $\mathcal{P}$.

Теперь положим $X = \sum\limits_{1 \leqslant i \leqslant n} X_i$, $X_i = t_i X$, $1 \leqslant i \leqslant n$ (так что $t_1 + \ldots + t_n = 1$). Положим поле $K = K^{(1)}(t_1, \dots, t_{n-1})$. Мы имеем $K^{(1)}[X_1, \dots, X_n] \subset K[X]$ и $K^{(1)}[[X_1, \dots, X_n] \subset K[[X]]$ естественным образом. Отображение $\mathcal{N}$ продолжается до отображения нормы $K \to \mathbb{Q}(T_1, \dots, T_l, u_1, \dots, u_{l_1}, t_1, \dots, t_{n-1})$. Мы будем обозначать последнее отображение снова через $\mathcal{N}$. Положим $\Lambda = \Lambda_1[t_1, \dots, t_{n-1}]$. Заметим, что $\mathcal{N}(\Lambda) \subset \Lambda_0[t_1, \dots, t_{n-1}]$.

Сейчас $f, \overline{g}, \overline{h} \in K[X, Z]$. Мы предполагаем, что выполняются условия леммы 6 и следствия 5 с $K = K^{(1)}(t_1, \dots, t_{n-1})$, $f \in K[X, Z]$ и $\Lambda = \Lambda_1[t_1, \dots, t_{n-1}]$.

Положим $\gamma_0 = c^{\max\{n_1, n_2\}}$ и $\gamma = \mathcal{N}(a^2 c^{2n_1 n_2})$, где целые числа n_1, n_2 и элемент a – из формулировки леммы 6. Мы имеем $\mathcal{N}(ac^{n_1 n_2}) \in \Lambda_0[t_1, \dots, t_{n-1}]$, см. следствие 5. Следовательно, $\gamma \in \Lambda_0[t_1, \dots, t_{n-1}]$.

Напомним, что $\mathcal{P}$ – обозначение для различных полиномов с целыми неотрицательными коэффициентами, см. введение.

Следствие 6. *При предыдущих условиях для всех $i \geqslant 1$ можно представить*

$$g_{\rho+i} = G'_{\rho+i}/(\gamma_0 \gamma^i), \quad h_{\rho+i} = H'_{\rho+i}/(\gamma_0 \gamma^i)$$

для некоторых многочленов $G'_{\rho+i}, H'_{\rho+i} \in \Lambda_0[t_1, \dots, t_{n-1}, X, Z]$ таких, что $\deg_Z G'_{\rho+i} < n_1$, $\deg_Z H'_{\rho+i} < n_2$, $\deg_X G'_{\rho+i} < \overline{\rho}$, $\deg_X H'_{\rho+i} < \overline{\rho}$. Далее, для всех $i \geqslant 1$ степени $\deg_{t_1,\dots,t_{n-1}}(\gamma_0 \gamma^i)$, $\deg_{t_1,\dots,t_{n-1}} G'_{\rho+i}$, $\deg_{t_1,\dots,t_{n-1}} H'_{\rho+i}$ ограничены сверху $i\mathcal{P}(d)$, степени $\deg_{u_1,\dots,u_{l_1}}(\gamma_0 \gamma^i)$,

$\deg_{u_1,\dots,u_{l_1}} G'_{\rho+i}$, $\deg_{u_1,\dots,u_{l_1}} H'_{\rho+i}$ *ограничены сверху* $i\mathcal{P}(d_3,d_5,d)$, *степени* $\deg_{T_1,\dots,T_l}(\gamma_0\gamma^i)$, $\deg_{T_1,\dots,T_l} G'_{\rho+i}$, $\deg_{T_1,\dots,T_l} H'_{\rho+i}$, *ограничены сверху* $i\mathcal{P}(d_1,d'_1,d_2,d_4,d)$, *длины записи целых коэффициентов* $\mathrm{l}(G'_{\rho+i})$, $\mathrm{l}(H'_{\rho+i})$, $\mathrm{l}(\gamma_0\gamma^i)$ *ограничены сверху* $(M_1{+}M'_1{+}M_2{+}M_3{+}l{+}l_1{+}n)\mathcal{P}(i,d_1,d'_1,d_2,d_3,d_4,d_5,d)$.

Для всякого $i\geqslant 1$ *время работы алгоритма для построения* $\gamma_0\gamma^i$, $G'_{\rho+i}$, $H'_{\rho+i}$ *полиномиально от* M_1, M'_1, M_2, M_3, $(dd_1d'_1d_2d_4)^{l+1}$, $(dd_3d_5)^{l_1+1}$, i^{l+l_1+n}, d^n.

Доказательство. Это может быть доказано без затруднений рекурсивно, используя конструкцию из доказательства леммы 6 (мы оставляем подробности читателю; даже могут быть получены более точные оценки). Следствие доказано. □

Представим $\gamma=\sum\limits_{i_1,\dots,i_{n-1}\geqslant 0}\alpha_{i_1,\dots,i_{n-1}}t_1^{i_1}\cdot\ldots\cdot t_{n-1}^{i_{n-1}}$, где все коэффициенты $\alpha_{i_1,\dots,i_{n-1}}\in\Lambda_0$. Положим $\gamma_1=\mathrm{GCD}_{\,i_1,\dots,i_{n-1}\geqslant 0}\{\alpha_{i_1,\dots,i_{n-1}}\}$ в кольце Λ_0. Фактически элемент $\gamma_1\in\Lambda_0=\mathbb{Z}[T_1,\dots,T_l,u_1,\dots,u_{l_1}]$ определён с точностью до множителя ±1. Мы выбираем и фиксируем γ_1.

Следствие 7. *При условиях следствия 6 можно представить*

$$g=Z^{n_1}+\sum_{i\geqslant 0}G''_i/(\gamma_0\gamma^i)X^i,\quad h=Z^{n_2}+\sum_{i\geqslant 0}H''_i/(\gamma_0\gamma^i)X^i,$$

где $G''_i,H''_i\in\Lambda_0[t_1,\dots,t_{n-1},Z]$ *являются многочленами такими, что степени* $\deg_Z G''_i<n_1$, $\deg_Z H''_i<n_2$ *для всех* $i\geqslant 0$. *Более того, если*

$$g,h\in K^{(1)}[[X_1,\dots,X_n]][Z],\tag{26}$$

то для всякого $i\geqslant 0$ *можно представить*

$$G''_i/(\gamma_0\gamma^i)=1/(\gamma_0\gamma_1^i)\sum_{0\leqslant j<n_1}\ \sum_{i_1+\ldots+i_n=i,\,i_1,\dots,i_n\geqslant 0}g_{i_1,\dots,i_n,j}X_1^{i_1}\cdot\ldots\cdot X_n^{i_n}Z^j,\tag{27}$$

$$H''_i/(\gamma_0\gamma^i)=1/(\gamma_0\gamma_1^i)\sum_{0\leqslant j<n_2}\ \sum_{i_1+\ldots+i_n=i,\,i_1,\dots,i_n\geqslant 0}h_{i_1,\dots,i_n,j}X_1^{i_1}\cdot\ldots\cdot X_n^{i_n}Z^j,\tag{28}$$

где все коэффициенты $g_{i_1,\dots,i_n,j},h_{i_1,\dots,i_n,j}\in\Lambda_0$.

Далее, для всех $i\geqslant 0$ *степени* $\deg_{t_1,\dots,t_{n-1}}(\gamma_0\gamma_1^i)$, $\deg_{t_1,\dots,t_{n-1}} G''_i$, $\deg_{t_1,\dots,t_{n-1}} H''_i$ *ограничены сверху* $(i{+}1)\mathcal{P}(d)$,*степени* $\deg_{u_1,\dots,u_{l_1}}(\gamma_0\gamma_1^i)$,

$\deg_{u_1,\dots,u_{l_1}} G_i''$, $\deg_{u_1,\dots,u_{l_1}} H_i''$ *ограничены сверху* $(i+1)\mathcal{P}(d_3,d_5,d)$, *степени* $\deg_{T_1,\dots,T_l}(\gamma_0\gamma_1^i)$, $\deg_{T_1,\dots,T_l} G_i''$, $\deg_{T_1,\dots,T_l} H_i''$, *ограничены сверху* $(i+1)\mathcal{P}(d_1,\, d_1',d_2,d_4,d)$ *и длины записи целых коэффициентов* $\mathrm{l}(\gamma_0\gamma_1^i)$, $\mathrm{l}(G_i'')$, $\mathrm{l}(H_i'')$ *ограничены сверху* $(M_1+M_1'+M_2+M_3+l+l_1+n)\mathcal{P}(i,d_1,d_1',\, d_2,d_3,\, d_4,d_5,d)$.

Аналогично при условии (26) *для всех* j, $i\geqslant 0$ *и* $i_1,\dots,i_n\geqslant 0$ *таких, что* $i_1+\ldots+i_n=i$ *степени* $\deg_{u_1,\dots,u_{l_1}} g_{i_1,\dots,i_n,j}$, $\deg_{u_1,\dots,u_{l_1}} h_{i_1,\dots,i_n,j}$ *ограничены сверху* $(i+1)\mathcal{P}(d_3,d_5,d)$, *степени* $\deg_{T_1,\dots,T_l} g_{i_1,\dots,i_n,j}$, $\deg_{T_1,\dots,T_l} h_{i_1,\dots,i_n,j}$, *ограничены сверху* $(i+1)\mathcal{P}(d_1,d_1',d_2,d_4,d)$ *и длины записи целых коэффициентов* $\mathrm{l}(g_{i_1,\dots,i_n,j})$, $\mathrm{l}(h_{i_1,\dots,i_n,j})$ *ограничены сверху* $(M_1+M_1'+M_2+M_3+l+l_1+n)\mathcal{P}(i,d_1,d_1',d_2,d_3,d_4,d_5,d)$

Для всякого $i\geqslant 0$ *время работы алгоритма для построения* G_i'', H_i'', $\gamma_0(\gamma)^i$, $\gamma_0\gamma_1^i$ *полиномиально от* M_1, M_1', M_2, M_3, $(dd_1d_1'd_2d_4)^{l+1}$, $(dd_3d_5)^{l_1+1}$, i^{l+l_1+1+n}, d^n.

Аналогично при условии (26) *для всякого* $i\geqslant 0$ *время работы алгоритма для построения всех* $g_{i_1,\dots,i_n,j}$, $h_{i_1,\dots,i_n,j}$ *таких, что* $i_1+\ldots+i_n=i$ *полиномиально от* M_1, M_1', M_2, M_3, $(dd_1d_1'd_2d_4)^{l+1}$, $(dd_3d_5)^{l_1+1}$, i^{l+l_1+n}, d^n.

Доказательство. Это следует немедленно из следствия 6. Заметим только, что $K^{(1)}[[X_1,\dots,X_n]][Z]\subset K[[X]][Z]$ и при условии (26), мы имеем очевидное сокращение множителя γ^i/γ_1^i в левых частях (27) и (28). Следствие доказано. □

Замечание 6. Анализируя лемму 6 и её следствия, мы обнаружили небольшое исправление наших предыдущих результатов из [10, 11]. В утверждениях теоремы из [10] и аналогичной теоремы 1 [11] необходимо заменить δ^i на $\delta^{\max\{1,i\}}$. Следовательно, там корректная версия формулы для u имеет вид

$$u=\sum_{i\geqslant 0}\sum_{0\leqslant j<\deg_Z\Phi} u_{i,j}\eta^j X^{i/\nu}/\delta^{\max\{1,i\}},$$

Доказательство остаётся тем же самым, подробности см. в [12].

§2. Сложность построенных алгоритмов в случае, когда степень трансцендентности основного поля не фиксирована

В статье [8] основное поле $k = \mathbb{Q}(T_1, \ldots, T_l)[\eta]$, и для простоты мы рассматривали там степень трансцендентности l поля k над $\mathbb{Q}$ как фиксированную константу. Аналогичная ситуация со степенью трансцендентности основного поля имела место в статье [4]. Теорема 1 из [4] (и её следствие 1) используется для доказательства результатов из [8]. Также, применяя результаты статей [5, 6] в [8], мы снова рассматривали l как фиксированную константу.

В настоящей статье для того, чтобы усилить результаты из [8], нам требуется рассмотреть более общий случай. В предыдущем параграфе мы ввели поле $K^{(1)} = k'(u_1, \ldots, u_{l_1})$. Теперь мы рассматриваем $K_0 = k(u_1, \ldots, u_{l_1})$ в качестве основного поля вместо k. Положим поле $K_0' = \overline{k}(u_1, \ldots, u_{l_1})$. Степень трансцендентности K_0 над $\mathbb{Q}$ равна $l + l_1$, и мы не рассматриваем l и l_1 как фиксированные константы.

Пусть $f \in K_0[X_1, \ldots, X_n, Z]$ – многочлен, введённый перед следствием 6. Мы предполагаем, что для f справедливы верхние оценки на степени и длину записи целых коэффициентов (21) из предыдущего параграфа (теперь с основным полем K_0 вместо $K^{(1)}$) и старший коэффициент $\mathrm{lc}_Z f = 1$. Следовательно, сейчас d, d_2, d_3, M_2 имеют тот же самый смысл, что и в предыдущем параграфе. Пусть δ является дискриминантом многочлена f относительно Z, и $r = \mathrm{ord}(\delta)$ является порядком многочлена δ. Дополнительно теперь мы предполагаем, что полином f неприводим в кольце $\overline{K_0}[X_1, \ldots, X_n]$, где $\overline{K_0}$ – алгебраическое замыкание поля K_0.

В данном параграфе мы собираемся модифицировать алгоритмы из [8]. Именно, мы описываем алгоритмы для разложения на неприводимые многочлена f в кольцах $K_0[[X_1, \ldots, X_n]][Z]$ и $K_0'[[X_1, \ldots, X_n]][Z]$. В теореме 2 ниже мы даём верхние оценки, на степени и длины записи целых коэффициентов всех объектов на на выходе этих алгоритмов, а также на сложность построенных алгоритмов. Эти оценки зависят явно от l и l_1 (если $l_1 = 0$, то мы получаем версию теоремы 1 [8] с подробными оценками, зависящими от l для всех объектов на выходе и для сложности алгоритмов). Это обобщение алгоритмов из [8] будут использовано в следующем параграфе, где применяется теорема

Бертини для локальных колец, чтобы усилить результаты статьи [8]. В доказательстве теоремы 2 мы применяем лемму 6 и её следствия.

Теорема 2. *При сформулированных условиях справедливы следующие утверждения.*

(i) *Можно построить разложение* $f = \prod_{i\in I} f_i$, *где все* f_i *являются неприводимыми элементами из кольца* $K_0[[X_1,\dots,X_n]][Z]$ *и все старшие коэффициенты* $\operatorname{lc}_Z f_i = 1$. *Именно, для всякого* $i \in I$ *строятся многочлены* $\overline{g} = \overline{f}_i = f_i \bmod \mathfrak{m}^{r+1} \in K_0[X_1,\dots,X_n,Z]$ *и* $\overline{h} = (f/f_i) \bmod \mathfrak{m}^{r+1} \in K_0[X_1,\dots,X_n,Z]$. *После этого, применяя лемму 6 и следствие 7 к* $\overline{g},\overline{h}$, *можно построить представление*

$$f_i = \sum_{\substack{i_1,\dots,i_n\geqslant 0,\\ 0\leqslant v<\deg_Y\varphi,\\ 0\leqslant j\leqslant\deg_Z f_i}} f_{i,v,i_1,\dots,i_n,j}/(\gamma_0\gamma_1^{i_1+\dots+i_n})\eta^v X_1^{i_1}\cdot\ldots\cdot X_n^{i_n}Z^j,$$

где все $\gamma_0,\gamma_1,f_{i,v,i_1,\dots,i_n,j} \in \mathbb{Z}[T_1,\dots,T_l,u_1,\dots,u_{l_1}]$ *(элементы* γ_0,γ_1 *– ненулевые и зависят от* i*).*

(ii) *Для всякого* $i \in I$ *строится неприводимый полином* $\varphi_i \in k[Y]$ *степени* $\deg_Y\varphi_i \leqslant d$. *Фактически каждый многочлен* $\varphi_i \in \mathbb{Z}[T_1,\dots,T_l][\eta][Y]$, *и старший коэффициент* $\operatorname{lc}_Y\varphi_i = 1$. *Обозначим через* $\{\theta_w\}_{w\in J_i}$ *семейство всех корней из алгебраического замыкания* $\overline{k}$ *многочлена* φ_i *(эти корни сопряжены над полем* k*). В дальнейшем мы предполагаем, что для всех* $i_1,i_2 \in I$, *если* $i_1 \neq i_2$, *то* $J_{i_1}\cap J_{i_2} = \varnothing$.

(iii) *Для всякого* $i \in I$ *можно построить разложение* $f_i = \prod_{w\in J_i} f_w$, *где все* f_w *являются неприводимыми элементами из кольца* $K_0'[[X_1,\dots,X_n]][Z]$ *и все старшие коэффициенты* $\operatorname{lc}_Z f_w = 1$. *Далее, для всякого* $w \in J_i$ *можно построить многочлены* $\overline{g} = \overline{f}_w = f_w \bmod \mathfrak{m}^{r+1} \in k[\eta_w](u_1,\dots,u_{l_1})[X_1,\dots,X_n,Z]$ *и* $\overline{h} = (f/f_w) \bmod \mathfrak{m}^{r+1} \in k[\eta_w](u_1,\dots,u_{l_1})[X_1,\dots,X_n,Z]$. *Эти многочлены* $\overline{f}_w$ *сопряжены над полем* k *и аналогично* $f_w \in k[\eta_w](u_1,\dots,u_{l_1})[[X_1,\dots,X_n]][Z]$ *сопряжены над полем* k *(здесь группа Галуа* $\operatorname{Gal}(\overline{k}/k)$ *действует на многочленах, рациональных функциях и формальных степенных рядах покоэффициентно). После этого, применяя лемму* 6 *и следствие* 7

к $\overline{g}, \overline{h}$, *строится представление*

$$f_w = \sum_{\substack{i_1,\dots,i_n \geqslant 0,\\ 0 \leqslant v < \deg_Y \varphi,\\ 0 \leqslant u < \deg_Y \varphi_i,\\ 0 \leqslant j \leqslant \deg_Z f_w}} f_{w,v,u,i_1,\dots,i_n,j}/(\lambda_0 \lambda_1^{i_1+\dots+i_n}) \eta^v \eta_w^u X_1^{i_1} \cdot \dots \cdot X_n^{i_n} Z^j,$$

где все $\lambda_0, \lambda_1, f_{w,v,u,i_1,\dots,i_n,j} \in \mathbb{Z}[T_1, \dots, T_l, u_1, \dots, u_{l_1}]$ *(элементы* λ_0, λ_1 *– ненулевые и зависят от* w*).*

(iv) *Степени* $\deg_{T_1,\dots,T_l}$ *относительно* $T_1, \dots, T_l$ *всех элементов* γ_0, γ_1, λ_0, λ_1, $f_i \bmod \mathfrak{m}^{r+1}$, $(f/f_i) \bmod \mathfrak{m}^{r+1}$, φ_i, $f_w \bmod \mathfrak{m}^{r+1}$, $(f/f_w) \bmod \mathfrak{m}^{r+1}$, $w \in J_i$, $i \in I$, *ограничены сверху* $\mathcal{P}(d_1, d_2, d^{2^{n^c}})$ *для абсолютной константы* $c > 0$. *Степени* $\deg_{u_1,\dots,u_{l_1}}$ *относительно* $u_1, \dots, u_{l_1}$ *этих элементов ограничены сверху* $\mathcal{P}(d_3, d^{2^{n^c}})$. *Длины записей целых коэффициентов этих элементов ограничены сверху* $(M_1 + M_2 + l + l_1)\mathcal{P}(d_1, d_2, d_3, d^{2^{n^c}})$.

Положим $\iota = i_1 + \dots + i_n$. *Для всех* $w, v, u, i_1, \dots, i_n, j$ *для всех* $\iota \geqslant 0$ *степени* $\deg_{T_1,\dots,T_l}$ *относительно* $T_1, \dots, T_l$ *всех элементов* $f_{i,v,i_1,\dots,i_n,j}$, $f_{w,v,u,i_1,\dots,i_n,j}$ *таких, что* $i_1 + \dots + i_n = \iota$ *ограничены сверху* $(\iota + 1)\mathcal{P}(d_1, d_2, d^{2^{n^c}})$. *Степени* $\deg_{u_1,\dots,u_{l_1}}$ *относительно* $u_1, \dots, u_{l_1}$ *этих элементов ограничены сверху* $(\iota + 1)\mathcal{P}(d_3, d^{2^{n^c}})$. *Длины записей целых коэффициентов этих элементов ограничены сверху* $(M_1 + M_2 + l + l_1)\mathcal{P}(\iota, d_1, d_2, d_3, d^{2^{n^c}})$.

(v) *Время работы алгоритмов для построения всех элементов* γ_0, γ_1, λ_0, λ_1, $f_i \bmod \mathfrak{m}^{r+1}$, $(f/f_i) \bmod \mathfrak{m}^{r+1}$, φ_i, $f_w \bmod \mathfrak{m}^{r+1}$, $(f/f_w) \bmod \mathfrak{m}^{r+1}$, $w \in J_i$, $i \in I$, *полиномиально от* M_1, M_2, $(d_1 d_2 d^{2^{n^c}})^{l+1}$, $(d_3 d^{2^{n^c}})^{l_1+1}$, $d^{n 2^{n^c}}$.

Для всякого $\iota \geqslant 0$ *время работы алгоритмов для построения всех элементов* $f_{i,v,i_1,\dots,i_n,j}, f_{w,v,u,i_1,\dots,i_n,j}$ *таких, что* $i_1 + \dots + i_n = \iota$ *полиномиально от* $M_1, M_2, (d_1 d_2 d^{2^{n^c}})^{l+1}, (d_3 d^{2^{n^c}})^{l_1+1}$, $d^{n 2^{n^c}}$, ι^{l+l_1+n}.

Доказательство. Мы можем предполагать без ограничения общности, что $n \geqslant 2$, поскольку любой многочлен из $k[X_1, Z]$ может рассматриваться как многочлен из $k[X_1, X_2, Z]$. Сначала нам потребуется переформулировать результаты из [4–6] и [8] для основного поля K_0

вместо k и также дать более подробные оценки на степени и длины записей целых коэффициентов объектов на выходе алгоритмов из этих статей (но в нашей ситуации, когда последние результаты применяются в модифицированной конструкции из [8], которую мы собираемся описать).

Перейдём к подробностям. Положим $z = Z \bmod f \in K_0[X_1, \ldots, X_n, Z]/(f)$. Напомним, что многочлен f неприводим над полем $\overline{K_0}$. Следовательно, мы можем применить алгоритм из теоремы 1 [4] и её следствия 1 [4] к многочлену f и построить неособое в коразмерности один аффинное алгебраическое многообразие V, определённое над полем K_0 и неприводимое над $\overline{K_0}$. Теперь (чтобы избежать путаницы) обозначим через z' элемент z из формулировки утверждения (ii) теоремы 1 [4]. Так что $z' = \sum\limits_{0 \leqslant i < \deg_Z f} z'_i z^i/\delta$, где $z = Z \bmod f$, и $z'_i \in K_0[X_1, \ldots, X_n]$ для всех i. Кольцо определённых над K_0 регулярных функций алгебраического многообразия V равно $K_0[X_1, \ldots, X_n][z, z']$. Алгоритм из теоремы 1 [4] основывается на версии алгоритма Ньютона–Пюизе из [7] и других идеях. Но фактически он сводится к некоторым переборам, вычислению определителей и решению линейных систем с матрицами размера, ограниченного сверху $d^{O(1)}$, над различными полями. Из описания данного алгоритма следует немедленно, что для всех i степени $\deg_{T_1,\ldots,T_l} z'_i$, $\deg_{T_1,\ldots,T_l} \delta$ ограничены сверху $\mathcal{P}(d_1, d_2, d)$, степени $\deg_{u_1,\ldots,u_{l_1}} z'_i$, $\deg_{u_1,\ldots,u_{l_1}} \delta$ ограничены сверху $\mathcal{P}(d_3, d)$ и длины записей целых коэффициентов $\mathrm{l}(z'_i)$, $\mathrm{l}(\delta)$ ограничены сверху $(M_1 + M_2 + l + l_1 + n)\mathcal{P}(d_1, d_2, d_3, d)$. Время работы алгоритма для построения всех z'_i (и, следовательно, z) полиномиально от M_1, M_2, d_1^{l+1}, $(d_2 d)^{l+1}$, $(d_3 d)^{l_1+1}$, d^n.

После этого, применяя к многообразию V алгоритм из [5,6] (напомним, что мы предполагаем, что $n \geqslant 2$ и, следовательно, можно применять алгоритм из этих статей; хотя, если $n = 1$, то можно просто положить $V' = V$), мы строим нормальное алгебраическое многообразие V'. Более точно, строится целое замыкание $K_0[y_1, \ldots, y_N]$ кольца $K_0[X_1, \ldots, X_n, z, z']$ в его поле частных, более подробно об этом см. [8] §1. Кольцо определённых над K_0 регулярных функций алгебраического многообразия V' равно $K_0[y_1, \ldots, y_N]$, и $V' \subset \mathbb{A}^N(\overline{K_0})$ естественным образом. Мы предполагаем без ограничения общности, что $y_i = X_i$ для $1 \leqslant i \leqslant n$ и $y_{n+1} = z$. Далее, каждый элемент y_i, $1 \leqslant i \leqslant N$, представляется в виде $y_i = (1/\delta) \sum\limits_{0 \leqslant i < \deg_Z f} y_{i,j} z^j$, где все $y_{i,j} \in K_0[X_1, \ldots, X_n]$.

Согласно [5, 6] конструкция всех элементов $y_{i,j}$ сводится к некоторым переборам и решению линейных систем с матрицами размера, ограниченного сверху $d^{2^{n^{c'}}}$ для абсолютной константы $c' > 0$. Для краткости положим $D = d^{2^{n^{c'}}}$. Из [5, 6, 16] (и [8]) следует немедленно, что для всех i, j степени $\deg_{T_1,\dots,T_l} y_{i,j}$ ограничены сверху $\mathcal{P}(d_1, d_2, D)$, степени $\deg_{u_1,\dots,u_{l_1}} y_{i,j}$ ограничены сверху $\mathcal{P}(d_3, D)$ и длины записей целых коэффициентов $\mathrm{l}(y_{i,j})$ ограничены сверху $(M_1+M_2+l+l_1)\mathcal{P}(d_1, d_2, d_3, D)$. Время работы алгоритма для построения всех $y_{i,j}$ (и, следовательно, всех y_i, $1 \leqslant i \leqslant N$) полиномиально от M_1, M_2, d_1^{l+1}, $(d_2D)^{l+1}$, $(d_3D)^{l_1+1}$, D^n.

После этого мы следуем описанию алгоритма из [8] с некоторыми изменениями. Морфизмы линейных проекций $\pi_{n+1} : \mathcal{Z}(f) \to \mathbb{A}^n(\overline{K_0})$, $(X_1, \dots, X_{n+1}) \mapsto (X_1, \dots, X_n)$ и $\pi_N : V' \to \mathbb{A}^n(\overline{K_0})$, $(Y_1, \dots, Y_N) \mapsto (X_1, \dots, X_n)$, определены в §2 [8].

Теперь мы применяем лемму 3 [8]. Следовательно, заменяя при необходимости n на $n+1$ и f на $\widetilde{f}$, мы будем предполагать без ограничения общности, что $f(0, \dots, 0, Z) = Z^{\deg_Z f}$. Поэтому число элементов $\pi_{n+1}^{-1}(x^*) = 1$ в обозначениях §1. Положим $z^* = (0, \dots, 0) \in \pi_{n+1}^{-1}(x^*)$. Обозначим через S_{x^*} (соответственно S'_{x^*}) мультипликативно замкнутое множество всех многочленов $s \in K_0[X_1, \dots, X_n]$ (соответственно $s \in K'_0[X_1, \dots, X_n]$) таких, что $s(x^*) \neq 0$. Положим $A = S_{x^*}^{-1}K'_0[X_1, \dots, X_n]$ равным локальному кольцу всех функций, определённых над K'_0 и регулярных в некоторой окрестности точки $x^* \in \mathbb{A}^n(\overline{K_0})$, т.е. локальному кольцу определённых над полем K'_0 функций точки x^* аффинного пространства $\mathbb{A}^n(\overline{K_0})$. Тогда также естественным образом можно отождествить $A = (S'_{x^*})^{-1}K'_0[X_1, \dots, X_n]$. Обозначим через $\mathfrak{m}'$ максимальный идеал кольца A.

Положим $E = A[Z]/(f) = \mathcal{O}_{z^*,\mathcal{Z}(f)}$ равным локальному кольцу определённых над K'_0 функций точки z^* алгебраического многообразия $\mathcal{Z}(f)$ (напомним, что $\mathcal{Z}(f) \subset \mathbb{A}^{n+1}(\overline{K_0})$). Обозначим через E' целое замыкание кольца E в его поле частных K'. Заметим, что K' также является полем частных кольца E, и мы отождествляем

$$K' = K'_0(X_1, \dots, X_n) \otimes_A E' = K'_0(X_1, \dots, X_n) \otimes_A E. \tag{29}$$

Далее можно отождествить

$$E' = K'_0 \otimes_{K_0} S_{x^*}^{-1}K_0[y_1, \dots, y_N] = S_{x^*}^{-1}K'_0[y_1, \dots, y_N] = (S'_{x^*})^{-1}K'_0[y_1, \dots, y_N] \tag{30}$$

в предыдущих обозначениях.

Применяя лемму 2 [8] (теперь с основным полем K_0 вместо k), мы строим линейную форму $Q = \sum\limits_{1\leqslant v\leqslant N} a_v Y_v$ с целыми коэффициентами a_v такую, что число элементов $\#\pi_N^{-1}(x^*) = \#Q(\pi_N^{-1}(x^*))$ и $q = Q(y_1, \dots, y_N)$ является примитивным элементом поля $K_0(X_1, \dots, X_n)[z]$ над полем $K_0(X_1, \dots, X_n)$. Строится минимальный многочлен $F \in K_0[X_1, \dots, X_n, Q]$ примитивного элемента $q \in K_0(X_1, \dots, X_n)[z]$ над полем $K_0(X_1, \dots, X_n)$.

Используя алгоритм из [3], мы строим разложение полинома $F(0, \dots, 0, Q) = \prod_{1\leqslant j\leqslant m} \psi_j^{\varepsilon_j}$, где все $\psi_j \in K_0[Q]$ являются неприводимыми над полем K_0 попарно различными многочленами со старшими коэффициентами $\mathrm{lc}_Q \psi_j = 1$ и $1 \leqslant \varepsilon_i \in \mathbb{Z}$. Положим $\psi = \prod_{1\leqslant j\leqslant m} \psi_j$. Тогда число элементов $\#\pi_N^{-1}(x^*) = \deg_Q \psi$ согласно лемме 2 (ii) [8].

Далее нам требуется разложить на множители каждый полином ψ_j над полем K_0'. Для этого для каждого j построим наименьшее общее кратное a_j всех знаменателей из $\mathbb{Z}[T_1, \dots, T_l, u_1, \dots, u_{l_1}]$ коэффициентов многочлена ψ_j. Теперь $a_j\psi_j \in k[u_1, \dots, u_{l_1}, Q]$, и этот многочлен неприводим в последнем кольце. Используя алгоритм из [3], разложим на неприводимые множители многочлен от многих переменных $a_j\psi_j$ над полем $\overline{k}$. На выходе последнего алгоритма получим конечное расширение полей $k_j' \supset k$. Поле k_j' задано (на выходе) примитивным элементом η_j' над полем k с минимальным многочленом $\psi_j' \in k[Y]$. Следовательно, $k_j' = k[\eta_j']$ и $\psi_j'(\eta_j') = 0$. Обозначим через G_j множество всех вложений поля $k_j \to \overline{k}$ над k. Далее строятся многочлен $\chi_j' \in k_j'[u_1, \dots, u_{l_1}, Q]$ и элемент $0 \neq \lambda_j \in k$ такие, что $a_j\psi_j = \lambda_j \prod_{\sigma\in G_j} (\chi_j')^\sigma$ (σ действует покоэффициентно на многочленах) является разложением многочлена от многих переменных $a_j\psi_j$ над полем $\overline{k}$. Положим $\chi_j = \chi_j'/\mathrm{lc}_Q\chi_j' \in k_j'(u_1, \dots, u_{l_1})[Q]$. Тогда по лемме Гаусса $\psi_j = \prod_{\sigma\in G_j} \chi_j^\sigma$ является требуемым разложением полинома ψ_j в кольце $K_0'[Y]$. Поэтому $\deg_Y \psi_j' = \#G_j \leqslant d$. Заметим, что старший коэффициент $\mathrm{lc}_Q\chi_j = 1$. Положим поле $K_j = k_j'(u_1, \dots, u_{l_1})$. Тогда фактически $\chi_j \in K_j[Q]$.

Более того, мы можем предполагать, не умаляя общности, что $\psi_j' \in \mathbb{Z}[T_1, \dots, T_l, \eta][Y]$ и старший коэффициент $\mathrm{lc}_Y\psi_j' = 1$, ср. замечание о минимальном многочлене ψ' элемента η' в предыдущем параграфе.

Кроме того, каждый полином χ_j можно представить в виде

$$\chi_j = (1/\chi_j^{(0)}) \sum_{u \geqslant 0} \sum_{0 \leqslant v < \deg_Y \varphi} \sum_{0 \leqslant i < \deg_Y \psi_j'} \chi_{j,u,v,i} \eta^v (\eta_j')^i Q^u,$$

где все $\chi_j^{(0)}, \chi_{j,u,v,i} \in \mathbb{Z}[T_1, \ldots, T_l, u_1, \ldots, u_{l_1}]$ и $\mathrm{G\,C\,D}_{u,v,i}\{\chi_i^{(0)}, \chi_{j,u,v,i}\} = 1$ в последнем кольце, ср. (20). Аналогичным образом представляются многочлены (скажем, от Y, или Q, или Z, или $X_1, \ldots, X_n, Q$, или $X_1, \ldots, X_n, Z$) с коэффициентами из K_j (и также из K_0). Следовательно, для таких многочленов естественным образом определены степени $\deg_{T_1,\ldots,T_l}$, $\deg_{u_1,\ldots,u_{l_1}}$ и длины записей целых коэффициентов $\mathrm{l}(\ldots)$, ср. введение из [8].

Обозначим через z_v^*, $1 \leqslant v \leqslant \deg_Q \psi$, все элементы прообраза $\pi_N^{-1}(x^*)$, ср. §1 [8]. Для всякой пары $1 \leqslant j \leqslant m$, $\sigma \in G_j$ обозначим через $\Xi_{j,\sigma}$ подмножество всех целых чисел v таких, что $\chi_j^\sigma(z_v^*) = 0$. Положим $W_{j,\sigma} = \{z_v^* : v \in \Xi_{j,\sigma}\}$.

Обозначим через G группу Галуа $\mathrm{Gal}(\overline{K_0}/K_0')$. Обозначим через $\mathcal{W}$ множество всех определённых над K_0' и неприводимых над K_0' подмногообразий прообраза $\pi_N^{-1}(x^*)$. Следовательно, $W \in \mathcal{W}$ тогда и только тогда, когда W является минимальным непустым подмножеством в $\pi_N^{-1}(x^*)$ таким, что $\sigma(W) = W$ для всякого $\sigma \in G$. Максимальные идеалы кольца E' находятся во взаимно однозначном соответствии с подмногообразиями $W \in \mathcal{W}$. Заметим, что для всех z' и W, если $z' \in W \in \mathcal{W}$, то

$$\{\sigma(z') : \sigma \in G\} = W. \tag{31}$$

Число элементов $\#Q(\pi_N^{-1}(x^*)) = \#\pi_N^{-1}(x^*)$. Поэтому для всякого $z' = (z_1', \ldots, z_N') \in W$ поле $K_0'[z_1', \ldots, z_N'] = K_0'[Q(z_{n+1}', \ldots, z_N')]$. Следовательно, для любого $W' \subset \pi_N^{-1}(x^*)$ мы имеем $\sigma(W') = W'$ для всех $\sigma \in G$ тогда и только тогда, когда $\sigma(Q(W')) = Q(W')$ для всех $\sigma \in G$. Поэтому каждое $W \in \mathcal{W}$ имеет вид $W = W_{j,\sigma}$ для однозначно определённых $1 \leqslant j \leqslant m$, $\sigma \in G_j$ и, следовательно, каждое $W_{j,\sigma} \in \mathcal{W}$ (здесь мы оставляем подробности читателю). Максимальный идеал $\mathfrak{m}_{j,\sigma}$ кольца E', соответствующий $W_{j,\sigma}$ является подмножеством всех $a \in E'$ таких, что $a(z_v^*) = 0$ для всех $v \in \Xi_{j,\sigma}$.

Заметим также, что для произвольного $a \in E'$, если $a(z_v^*) = 0$ для некоторого $v \in \Xi_{j,\sigma}$, то $a \in \mathfrak{m}_{j,\sigma}$. Это следует из (31), поскольку для всякого $\sigma \in G$ мы имеем $a(\sigma(z_v^*)) = \sigma(a(z_v^*)) = 0$ согласно (30).

Положим[1] $S_{j,\sigma}$ равным мультипликативно замкнутому подмножеству всех элементов $s \in K_0'[y_1, \ldots, y_N]$ таких, что $s(z_v^*) \neq 0$ для всех $v \in \Xi_{j,\sigma}$. Следовательно, $S_{j,\sigma} \subset E' \setminus \mathfrak{m}_{j,\sigma}$ и $S_{j,\sigma} \supset S'_{x^*} \supset S_{x^*}$. Положим кольцо $E'_{j,\sigma} = S_{j,\sigma}^{-1} K_0'[y_1, \ldots, y_N]$. Можно также отождествить $E'_{j,\sigma} = S_{j,\sigma}^{-1} E' = (E' \setminus \mathfrak{m}_{j,\sigma})^{-1} E'$. Поэтому $E'_{j,\sigma}$ является локальным кольцом. Имеем естественное вложение колец $\iota : E' \to \prod_{1 \leqslant j \leqslant m,\, \sigma \in G_j} E'_{j,\sigma}$.

Положим $\mathfrak{M}_{j,\sigma} = S_{j,\sigma}^{-1} \mathfrak{m}_{j,\sigma}$ равным максимальному идеалу кольца $E_{j,\sigma}$. Покажем (для полноты; конечно, это известно), что $\mathfrak{m}' E'_{j,\sigma}$-адическая и $\mathfrak{M}_{j,\sigma}$-адическая топологии на кольце $E'_{j,\sigma}$ совпадают. Действительно, очевидно $\mathfrak{m}' E'_{j,\sigma} \subset \mathfrak{M}_{j,\sigma}$ и $\mathfrak{M}_{j,\sigma} \cap E' \subset \mathfrak{m}'$. Пусть $a \in \mathfrak{M}_{j,\sigma}$. Существует $s_1 \in S_{j,\sigma}$ такое, что $s_1 a \in E'$. Далее, существует $s_2 \in S_{j,\sigma}$ такое, что $s_2(\pi^{-1}(x^*) \setminus \Xi_{j,\sigma}) = \{0\}$. Положим $b = s_1 s_2 a \in E'$. Кольцо E' цело над A, и E' является целозамкнутым. Поэтому $b^N + \sum\limits_{0 \leqslant i \leqslant N-1} b^i a_i = 0$ для некоторых $a_i \in A$, $a_0 \neq 0$. Мы имеем также $N \leqslant \deg_Z f \leqslant d$. Очевидно $a_0 \in \mathfrak{m}'$. Положим $i_0 = \min\{i \,:\, a_i \notin \mathfrak{m}'\}$. Следовательно, $1 \leqslant i_0 \leqslant N$. Теперь $b^{i_0}(b^{N-i_0} + \sum\limits_{i_0 \leqslant i \leqslant N-i_0} b^{i-i_0} a_i) \in \mathfrak{m}' E_{j,\sigma}$, и $(b^i + \sum\limits_{i_0 \leqslant i \leqslant N-i_0} b^{i-i_0} a_i) \notin \mathfrak{M}_{j,\sigma}$. Поэтому $b^{i_0} \in \mathfrak{m}' E'_{j,\sigma}$. Следовательно, $a^{i_0} \in \mathfrak{m}' E'_{j,\sigma}$. Отсюда вытекает требуемое утверждение.

Заметим также, что естественным образом пополнение кольца E' относительно $\mathfrak{m}_{j,\sigma}$-адической топологии совпадает с пополнением кольца $E'_{j,\sigma}$ относительно $\mathfrak{M}_{j,\sigma}$-адической топологии.

Кольцо $\widehat{A} = K_0'[[X_1, \ldots, X_n]]$ совпадает с пополнением кольца A относительно $\mathfrak{m}'$-адической топологии. Обозначим через $\widehat{E}, \widehat{E}', \widehat{E}'_{j,\sigma}$, $1 \leqslant j \leqslant m$, $\sigma \in G_j$, пополнения колец $E, E', E'_{j,\sigma}$, $1 \leqslant j \leqslant m$, $\sigma \in G_j$, относительно $\mathfrak{m}'$-адической топологии (более точно, пополнение относительно $\mathfrak{m}' E$-адической, $\mathfrak{m}' E'$-адической и $\mathfrak{m}' E'_{j,\sigma}$-адической топологий соответственно). Кольца E и E' являются конечными A-модулями. Поэтому,

[1] В [8] имеются очевидные неточности в определениях S_v и E'_v, которые легко исправляются, исходя из контекста. Правильная версия этих определений следующая: "Положим S_v равным мультипликативно замкнутому подмножеству всех элементов $s \in \overline{k}[y_1, \ldots, y_N]$ таких, что $s(z_v^*) \neq 0$ и $E'_v = S_v^{-1} \overline{k}[y_1, \ldots, y_N]$" (в переводе на английский язык статьи [8] это исправление внесено).

как хорошо известно, можно отождествить $\widehat{E} = \widehat{A} \otimes_A E$, $\widehat{E}' = \widehat{A} \otimes_A E'$. Но в общем случае[2] $\widehat{E}'_{j,\sigma} \neq \widehat{A} \otimes_A E'_{j,\sigma}$ для всех j, σ.

Обозначим через $K'_0((X_1, \dots, X_n))$ поле частных $\widehat{A}$, ср. замечание 1 во введении из [8]. Положим $\mathcal{K} = K'_0((X_1, \dots, X_n))[Z]/(f)$ равным полному кольцу частных кольца $\widehat{E}$. Согласно (29) можно отождествить

$$\begin{aligned}\mathcal{K} &= K'_0((X_1, \dots, X_n)) \otimes_{K'_0(X_1,\dots,X_n)} K' \\ &= K'_0((X_1, \dots, X_n)) \otimes_A E' = K'_0((X_1, \dots, X_n))[Z]/(f).\end{aligned}$$

Поэтому $\mathcal{K}$ является конечномерной сепарабельной алгеброй над полем $K'_0((X_1, \dots, X_n))$, и q является примитивным элементом алгебры $\mathcal{K}$ над $K'_0((X_1, \dots, X_n))$ по лемме 2 (i).

Согласно теореме 33 из [17] 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 [17] т. II, глава 8, §13 кольцо $\widehat{E}'_{j,\sigma}$ целостное и целозамкнутое, т.е. $E'_{j,\sigma}$ аналитически неприводимо и аналитически нормально.

Далее, хорошо известно, что вложение ι индуцирует канонический изоморфизм полных колец $\widehat{\iota} : \widehat{E}' \to \prod_{1 \leqslant j \leqslant m,\, \sigma \in G_j} \widehat{E}'_{j,\sigma}$. Так что мы отождествляем $\widehat{E}' = \prod_{1 \leqslant j \leqslant m,\, \sigma \in G_j} \widehat{E}'_{j,\sigma}$ с помощью этого изоморфизма $\widehat{\iota}$. Обозначим через $\mathcal{K}_{j,\sigma}$ поле частных кольца $\widehat{E}'_{j,\sigma}$. Следовательно, можно отождествить $\mathcal{K} = \prod_{1 \leqslant j \leqslant m,\, \sigma \in G_j} \mathcal{K}_{j,\sigma}$.

Сейчас, см. лемму 2 утверждение (i), q – примитивный элемент сепарабельной алгебры $\mathcal{K}$ над $\overline{k}((X_1, \dots, X_n))$ с минимальным многочленом F. Рассмотрим разложение

$$F(0, \dots, 0, Q) = \prod_{1 \leqslant j \leqslant m,\, \sigma \in G_j} (\chi_j^\sigma)^{\varepsilon_j}$$

в произведение взаимно простых множителей (минимальных степеней) над полем K'_0. Применяя подъём по лемме Гензеля к этому разложению, мы доказываем существование в точности m попарно различных множителей $F_j \in K'_0[[X_1, \dots, X_n]][Q]$, $1 \leqslant j \leqslant m$, многочлена F

[2]В статье [8] по ошибке мы утверждали, что $\widehat{E}'_v = \widehat{A} \otimes_A E'_v$ для $1 \leqslant v \leqslant \deg_Q \psi$, но фактически это утверждение не использовалось в дальнейшем в [8] (в переводе на английский язык статьи [8] эта ошибка исправлена).

(мы предполагаем, что все старшие коэффициенты $\mathrm{lc}_Q F_j = 1$), удовлетворяющих следующим свойствам: $F_j(0,\dots,0,Q) = \chi_j^{\varepsilon_j}$ для всех $1 \leqslant j \leqslant m$, и $F = \prod_{1\leqslant j\leqslant m,\, \sigma\in G_j} F_j^{\sigma}$.

Положим поле $\mathcal{K}_j = \overline{k}((X_1,\dots,X_n))[Q]/(F_j)$, $1 \leqslant j \leqslant m$. Следовательно, можно отождествить $\mathcal{K}_{j,\sigma} = \mathcal{K}_j^{\sigma} = \overline{k}((X_1,\dots,X_n))[Q]/(F_j^{\sigma})$ для $1 \leqslant j \leqslant m$, $\sigma \in G_j$.

Обозначим через Δ дискриминант многочлена F относительно Q. Решая линейную систему над полем $K_0(X_1,\dots,X_n)$, мы строим представление $z = (1/\Delta) \sum\limits_{0\leqslant i<\deg_Q F} z_i q^i$, где все $z_i \in k[X_1,\dots,X_n]$.

Далее действуем следующим образом[3]. Представим $\psi_j = \chi_j \xi_j$, где многочлен $\xi_j \in K_j[Q]$. Положим $\phi'_j = \prod_{1\leqslant w\leqslant m,\, w\neq j} \psi_w^{\varepsilon_w}$, $\phi_j = \xi_j^{\varepsilon_j}\phi'_j$. Заметим, что полиномы $\chi_j^{\varepsilon_j}$ и ϕ_j взаимно просты в кольце $K_j[Q]$ (соответственно $\psi_j^{\varepsilon_j}$ и ϕ'_j взаимно просты в кольце $K_0[Q]$). Мы имеем $F(0,\dots,0,Q) = \chi_j^{\varepsilon_j}\phi_j$ (соответственно $F(0,\dots,0,Q) = \psi_j^{\varepsilon_j}\phi'_j$). Поэтому можно применить подъём по лемме Гензеля к последнему равенству и получить разложение $F = \Psi_j\Phi_j$ (соответственно $F = \Psi'_j\Phi'_j$) такое, что $\Psi_j, \Phi_j \in K_j[[X_1,\dots,X_n]][Q]$, $\Psi_j(0,\dots,0,Q) = \chi_j^{\varepsilon_j}$, $\Phi_j(0,\dots,0,Q) = \phi_j$ (соответственно $\Psi'_j, \Phi'_j \in K_0[[X_1,\dots,X_n]][Q]$, $\Psi'_j(0,\dots,0,Q) = \psi_j^{\varepsilon_j}$, $\Phi'_j(0,\dots,0,Q) = \phi'_j$) и старшие коэффициенты $\mathrm{lc}_Q\Psi_j = \mathrm{lc}_Q\Phi_j = 1$ (соответственно $\mathrm{lc}_Q\Psi'_j = \mathrm{lc}_Q\Phi'_j$). Заметим, что фактически мы можем построить полиномы $(\Psi_j)_{\#,N}$, $(\Phi_j)_{\#,N}$ (соответственно $(\Psi'_j)_{\#,N}$, $(\Phi'_j)_{\#,N}$) для всякого целого числа $N \geqslant 0$.

Согласно алгоритму из [3] степени $\deg_{T_1,\dots,T_l}$ многочленов Δ, z_i, ψ_j, ψ'_j, χ_j, ξ_j, $\xi_j^{\varepsilon_j}$, $\psi_j^{\varepsilon_j}$, ϕ'_j, ϕ_j ограничены сверху $\mathcal{P}(d_1,d_2,D)$. Степени $\deg_{u_1,\dots,u_{l_1}}$ этих многочленов ограничены сверху $\mathcal{P}(d_3,D)$. Длины записей целых коэффициентов этих многочленов ограничены сверху $(M_1+M_2+l+l_1)\mathcal{P}(d_1,d_2,d_3,\ D)$. Время работы алгоритма для построения этих многочленов полиномиально от M_1, M_2, d_1^{l+1}, $(d_2D)^{l+1}$, $(d_3D)^{l_1+1}$.

Далее для всякого $N \geqslant 0$ можно оценить степени и длины записей целых коэффициентов многочленов $(\Psi_j)_{\#,N}$, $(\Phi_j)_{\#,N}$, $(\Psi'_j)_{\#,N}$,

[3]Здесь ниже в частном случае $l_1 = 0$ мы исправляем некоторые очевидные опечатки (или неточности) из [8], относящиеся к определениям многочленов $\Phi_j, \Psi_j, \Phi'_j, \Psi'_j$ (эти опечатки уже исправлены в переводе на английский язык статьи [8]).

$(\Phi'_j)_{\#,N}$ либо непосредственно, используя известные оценки для стандартной леммы Гензеля, либо, применяя частные случаи следствия 6 и следствия 7 с $\rho = 0$ и полем k'_j вместо поля k'. В любом случае мы получаем, что степени $\deg_{T_1,\dots,T_l}$ многочленов $(\Psi_j)_{\#,N}$, $(\Phi_j)_{\#,N}$, $(\Psi'_j)_{\#,N}$, $(\Phi'_j)_{\#,N}$ ограничены сверху $(N+1)\mathcal{P}(d_1,d_2,D)$. Степени $\deg_{u_1,\dots,u_{l_1}}$ этих многочленов ограничены сверху $(N+1)\mathcal{P}(d_3,D)$. Длины записей целых коэффициентов этих многочленов ограничены сверху $(M_1+M_2+l+l_1)\mathcal{P}(N,d_1,d_2,d_3,D)$. Время работы алгоритма для построения этих многочленов полиномиально от M_1, M_2, d_1^{l+1}, $((N+1)d_2D)^{l+1}$, $((N+1)d_3D)^{l_1+1}$, $((N+1)D)^n$.

Теперь мы имеем следующий аналог леммы 4 [8].

Лемма 7. *Многочлены f_w, $w \in J_i$, $i \in I$, находятся во взаимно однозначном соответствии с многочленами Ψ_j^σ, $\sigma \in G_j$, $1 \leqslant j \leqslant m$. Более точно, положим $\alpha_j = \deg_Q \Psi_j$. Тогда f_w соответствует Ψ_j^σ в том и только в том случае, если*

$$\Delta^{\alpha_j} f_w = \operatorname{Res}_Q\bigl(\Psi_j^\sigma, \Delta Z - \sum_{0\leqslant i<\deg_Q F} z_i Q^i\bigr), \tag{32}$$

где $\operatorname{Res}_Q(\dots)$ обозначает результант относительно Q рассматриваемых полиномов от Z, Q. Более того, пусть (G,H) равно паре многочленов
$(f/f_w, \Phi_j^\sigma)$ (соответственно $(f_i,\Psi'_j),(f/f_i,\Phi'_j)$). Положим $\alpha = \deg_Q H$. Тогда из (32) следует, что

$$\Delta^\alpha G = \operatorname{Res}_Q(H, \Delta Z - \sum_{0\leqslant i<\deg_Q F} z_i Q^i). \tag{33}$$

Поэтому сейчас многочлены $f_w, f/f_w \in k[(\eta'_j)^\sigma](u_1,\dots,u_{l_1})[[X_1,\dots,X_n]]$, $f_i, f/f_i \in K_0[[X_1,\dots,X_n]]$.

Следовательно, см. формулировку теоремы 2, мы полагаем $I = \{1,2,\dots,m\}$, $J_i = G_i$, $\varphi_i = \psi'_i$ для всякого $1 \leqslant i \leqslant m$ и $\theta_w = (\eta'_i)^\sigma$, 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 формулам (32) и (33)) следуют немедленно из свойств результанта двух полиномов. Фактически это хорошо известно. Наконец, последнее утверждение о $I, J_i, \varphi_i, \theta_w$ доказывается непосредственно. Лемма доказана. □

Положим $\gamma = \alpha_j$, $\gamma_2 = \deg_Q \Phi_j$, $\gamma_3 = \deg_Q \Psi'_j$, $\gamma_4 = \deg_Q \Phi'_j$ (конечно, γ_i зависят от j) и $N_u = r + \gamma_u \deg_{X_1,\dots,X_n} \Delta$, $1 \leqslant u \leqslant 4$. Теперь, используя (32), (33), вычислим аппроксимации результантов (эти результанты равны определителям соответствующих матриц Сильвестра) и найдём

$$(\Delta^{\gamma_1} f_w)_{\#,N_1}, \quad (\Delta^{\gamma_2} f/f_w)_{\#,N_2}, \quad (\Delta^{\gamma_3} f_i)_{\#,N_3}, \quad (\Delta^{\gamma_4} f/f_i)_{\#,N_4}.$$

После этого при помощи приближённого деления на Δ^{γ_u}, более подробно см. лемму 5 [8], можно вычислить

$$(f_w)_{\#,r}, \quad (f/f_w)_{\#,r}, \quad (f_i)_{\#,r}, \quad (f/f_i)_{\#,r} \tag{34}$$

для всех $w \in J_i$, $i \in I$.

Поэтому согласно используемым алгоритмам степени $\deg_{T_1,\dots,T_l}$ многочленов (34) ограничены сверху $\mathcal{P}(d_1, d_2, D)$. Степени $\deg_{u_1,\dots,u_{l_1}}$ этих многочленов ограничены сверху $\mathcal{P}(d_3, D)$. Длины записей целых коэффициентов этих многочленов ограничены сверху $(M_1 + M_2 + l + l_1)\mathcal{P}(d_1, d_2, d_3, D)$. Время работы алгоритма для построения этих многочленов полиномиально от M_1, M_2, d_1^{l+1}, $(d_2 D)^{l+1}$, $(d_3 D)^{l_1+1}$, D^n.

Положим $\rho' = \overline{\rho} = [r/2]$ в лемме 6. Напомним, что кольцо $\Lambda = \mathbb{Z}[T_1, \dots, T_l, u_1, \dots, u_{l_1}, t_1, \dots, t_{n-1}][\eta, \eta']$ в формулировке следствия 7. Наконец, мы применяем лемму 6 и её следствие 7 к $(f, \overline{g}, \overline{h}) = (f, (f_i)_{\#,r}, (f/f_i)_{\#,r})$ с $k' = k$, $K^{(1)} = K_0$, $K = K_0(t_1, \dots, t_{n-1})$, $\eta' = 1$ (соответственно $(f, \overline{g}, \overline{h}) = (f, (f_w)_{\#,r}, (f/f_w)_{\#,r})$ с $(\psi', \eta') = (\varphi_i, \theta_w)$, полем $k' = k[\theta_w]$, $K^{(1)} = k[\theta_w](u_1, \dots, u_{l_1})$, $K = K^{(1)}(t_1, \dots, t_{n-1})$) и сразу устанавливаем все утверждения теоремы 2. Теорема доказана. □

Замечание 7. Заметим, что для доказательства теоремы 2 можно обойтись также и без леммы 6 и её следствий. В самом деле, оценки для Ψ_j, H, z_i, см. (32), (33), установлены. Следовательно, можно вычислить непосредственно аппроксимации (34) с произвольным i вместо r с помощью (32), (33) и леммы 5 [8]. Всё же здесь требуется аккуратность (мы оставляем подробности заинтересованному читателю).

§3. Версия теоремы Бертини для локальных областей целостности и её алгоритмические приложения

Цель данного параграфа – усилить теорему 2 при помощи теоремы Бертини для локальных областей целостности. Сначала мы планировали использовать подход из [14]. Однако позже обнаружили, что более простой и конструктивный результат из [13] является достаточным и более подходящим для нашей цели, см лемму 8 ниже.

В этом параграфе поле k и многочлен $\varphi \in k[Y]$ – такие же, как и выше. Следовательно, $k = \mathbb{Q}(T_1, \dots, T_l)[\eta]$, $\varphi \in \mathbb{Z}[T_1, \dots, T_l, Y]$ неприводим, $\varphi(\eta) = 0$, старший коэффициент $\mathrm{lc}_Y \varphi = 1$, степень $\deg_{T_1,\dots,T_l} \varphi \leqslant d_1$ и длина записи целых коэффициентов $\mathrm{l}(\varphi) \leqslant M_1$. Мы собираемся доказать следующий результат.

Теорема 3. *Пусть $f \in k[X_1, \dots, X_n, Z]$ – неприводимый многочлен (в этом кольце) со старшим коэффициентом $\mathrm{lc}_Z f = 1$. Предположим, что справедливы оценки* (21) (*сейчас с $l_1 = 0$, $d_3 = 0$*) *на степени и длину записи целых коэффициентов многочлена f. Пусть дискриминант δ и целое число r – такие же, как и выше. Тогда можно разложить многочлен f на неприводимые множители в кольце $k[[X_1, \dots, X_n]][Z]$ (соответственно $\overline{k}[[X_1, \dots, X_n]][Z]$). Более точно, справедливы следующие утверждения.*

(i) *Строится разложение $f = \prod_{i \in I} f_i$, где все f_i являются неприводимыми элементами из кольца $k[[X_1, \dots, X_n]][Z]$ и старшие коэффициенты $\mathrm{lc}_Z f_i = 1$. Именно, для всякого $i \in I$ строятся полиномы $\overline{g} = \overline{f}_i = f_i \bmod \mathfrak{m}^{r+1} \in k[X_1, \dots, X_n, Z]$ и $\overline{h} = (f/f_i) \bmod \mathfrak{m}^{r+1} \in k[X_1, \dots, X_n, Z]$. После этого, применяя лемму 6 и следствие 7 (с $l_1 = 0$) к $\overline{g}, \overline{h}$, можно построить представление*

$$f_i = \sum_{\substack{i_1,\dots,i_n \geqslant 0,\\ 0 \leqslant v < \deg_Y \varphi,\\ 0 \leqslant j \leqslant \deg_Z f_i}} f_{i,v,i_1,\dots,i_n,j} / (\gamma_0 \gamma_1^{i_1+\dots+i_n}) \eta^v X_1^{i_1} \cdot \ldots \cdot X_n^{i_n} Z^j,$$

где все $\gamma_0, \gamma_1, f_{i,v,i_1,\dots,i_n,j} \in \mathbb{Z}[T_1, \dots, T_l]$ (элементы γ_0, γ_1 – ненулевые и зависят от i).

(ii) *Для всякого $i \in I$ строится неприводимый многочлен $\varphi_i \in k[Y]$ степени $\deg_Y \varphi_i \leqslant d$. Фактически каждый полином $\varphi_i \in \mathbb{Z}[T_1, \dots, T_l][\eta][Y]$, и старший коэффициент $\mathrm{lc}_Y \varphi_i = 1$. Обозначим через $\{\theta_w\}_{w \in J_i}$ семейство всех корней из алгебраического*

замыкания $\overline{k}$ многочлена φ_i (эти корни сопряжены над полем k). В дальнейшем мы предполагаем, что для всех $i_1, i_2 \in I$, если $i_1 \neq i_2$, то $J_{i_1} \cap J_{i_2} = \varnothing$.

(iii) *Для всякого $i \in I$ строится разложение $f_i = \prod_{w \in J_i} f_w$, где все f_w являются неприводимыми элементами из кольца $\overline{k}[[X_1, \dots, X_n]][Z]$ и все старшие коэффициенты $\operatorname{lc}_Z f_w = 1$. Далее, для всякого $w \in J_i$ строятся полиномы $\overline{g} = \overline{f}_w = f_w \bmod \mathfrak{m}^{r+1} \in k[\eta_w][X_1, \dots, X_n, Z]$ и $\overline{h} = (f/f_w) \bmod \mathfrak{m}^{r+1} \in k[\eta_w][X_1, \dots, X_n, Z]$. Эти полиномы $\overline{f}_w$ сопряжены над полем k и аналогично многочлены $f_w \in k[\theta_w] \in k[\eta_w][[X_1, \dots, X_n]][Z]$ сопряжены над полем k (здесь группа Галуа $\operatorname{Gal}(\overline{k}/k)$ действует на формальных степенных рядах покоэффициентно). После этого, применяя лемму 6 и следствие 7 к $\overline{g}, \overline{h}$, можно построить представление*

$$f_w = \sum_{\substack{i_1,\dots,i_n \geqslant 0,\\ 0 \leqslant v < \deg_Y \varphi,\\ 0 \leqslant u < \deg_Y \varphi_i,\\ 0 \leqslant j \leqslant \deg_Z f_w}} f_{w,v,u,i_1,\dots,i_n,j} / (\lambda_0 \lambda_1^{i_1+\dots+i_n}) \eta^v \eta_w^u X_1^{i_1} \cdot \ldots \cdot X_n^{i_n} Z^j,$$

где все $\lambda_0, \lambda_1, f_{w,v,u,i_1,\dots,i_n,j} \in \mathbb{Z}[T_1, \dots, T_l]$ (элементы λ_0, λ_1 – ненулевые и зависят от w).

(iv) *Степени $\deg_{T_1,\dots,T_l}$ относительно $T_1, \dots, T_l$ всех элементов γ_0, γ_1, λ_0, λ_1, $f_i \bmod \mathfrak{m}^{r+1}$, $(f/f_i) \bmod \mathfrak{m}^{r+1}$, φ_i, $f_w \bmod \mathfrak{m}^{r+1}$, $(f/f_w) \bmod \mathfrak{m}^{r+1}$, $w \in J_i$, $i \in I$, ограничены сверху $\mathcal{P}(d_1, d_2, d)$. Длины записей целых коэффициентов этих элементов ограничены сверху $(M_1 + M_2 + l + n)\mathcal{P}(d_1, d_2, d)$.*

Положим $\iota = i_1 + \dots + i_n$. Для всех $w, v, u, i_1, \dots, i_n, j$ для всех $\iota \geqslant 0$ степени $\deg_{T_1,\dots,T_l}$ относительно $T_1, \dots, T_l$ всех элементов $f_{i,v,i_1,\dots,i_n,j}$, $f_{w,v,u,i_1,\dots,i_n,j}$ таких, что $i_1 + \dots + i_n = \iota$, ограничены сверху $(\iota+1)\mathcal{P}(d_1, d_2, d)$. Длины записей целых коэффициентов этих элементов ограничены сверху $(M_1 + M_2 + l + n)\mathcal{P}(\iota, d_1, d_2, d)$.

(v) *Время работы алгоритмов для построения всех элементов γ_0, γ_1, λ_0, λ_1, $f_i \bmod \mathfrak{m}^{r+1}$, $(f/f_i) \bmod \mathfrak{m}^{r+1}$, φ_i, $f_w \bmod \mathfrak{m}^{r+1}$, $(f/f_w) \bmod \mathfrak{m}^{r+1}$, $w \in J_i$, $i \in I$, полиномиально от M_1, M_2, $(d_1 d_2 d)^{l+1}$, d^n.*

Для всякого целого числа $\iota \geqslant 0$ время работы алгоритмов для построения всех элементов $f_{i,v,i_1,\ldots,i_n,j}, f_{w,v,u,i_1,\ldots,i_n,j}$ таких, что $i_1+\ldots+i_n = \iota$, полиномиально от M_1, M_2, $(d_1d_2d)^{l+1}$, d^n, ι^{l+n}.

Для доказательства этой теоремы нам необходим следующий результат.

Лемма 8. *Пусть K – произвольное бесконечное поле, и $n \geqslant 3$ – целое число. Пусть $g \in K[[X_1,\ldots,X_n]][Z]$ многочлен неприводимый в этом кольце со старшим коэффициентом $\mathrm{lc}_Z(g) = 1$. Пусть u_1, u_2 являются трансцендентными элементами над полем K. Положим линейную форму $U_n = X_n - u_1X_1 - u_2X_2 \in K(u_1,u_2)[X_1,\ldots,X_n]$. Мы отождествляем $K(u_1,u_2)[[X_1,\ldots,X_n]]/(U_n) = K(u_1,u_2)[[X_1,\ldots,X_{n-1}]]$ естественным образом.*

Тогда многочлен $g \bmod U_n \in K(u_1,u_2)[[X_1,\ldots,X_{n-1}]][Z]$ является неприводимым в последнем кольце.

Доказательство. Расширим основное поле K до $K(u_1,u_2)$. Заметим, что g является неприводимым в кольце $K(u_2)[[X_1,\ldots,X_n]][Z]$ (здесь мы оставляем подробности читателю). Положим $U_{n,c} = X_n - u_1X_1 - cX_2$, где $c \in K(u_2)$ (так что линейная форма $U_{n,c}$ зависит от c).

Обозначим для краткости $A' = K(u_2)[[X_1,\ldots,X_n]]$. Положим $\mathfrak{m}' = (X_1, \ldots, X_n)$ равным максимальному идеалу кольца A'. Кольцо $A'[Z]/(g)$ – целостное, поскольку кольцо $A'[Z]$ факториально и элемент g неприводим в этом кольце.

Покажем, что $A'[Z]/(g)$ является локальным кольцом. Действительно, как хорошо известно, для всякого максимального идеала $\mathfrak{M}' \subset A'[Z]/(g)$ пересечение $\mathfrak{M}' \cap A'$ является максимальным идеалом кольца A' и, поэтому $\mathfrak{M}' \cap A' = \mathfrak{m}'$. Далее, максимальные идеалы кольца $A'[Z]/(g)$, лежащие над $\mathfrak{m}'$, находятся во взаимно однозначном соответствии с попарно различными неприводимыми множителями полинома $g(0,\ldots,0,Z) \in K(u_2)[Z]$. Если существуют по крайней мере два таких множителя, то мы можем применить подъём по лемме Гензеля к многочлену g и установить, что g не является неприводимым в кольце $A'[Z]$. Это противоречие. Следовательно, существует только один максимальный идеал $\mathfrak{M} \subset A'[Z]/(g)$, и $\mathfrak{M} \cap A' = \mathfrak{m}'$. Поэтому $A'[Z]/(g)$ является локальным кольцом. Более того, идеал $\mathfrak{M}$ совпадает с нильрадикалом идеала $\mathfrak{m}'A'[Z]/(g)$ (здесь мы оставляем подробности читателю). Таким образом, $A'[Z]/(g)$ является целостным полным

локальным кольцом относительно $\mathfrak{M}$-адической или, что то же самое, $\mathfrak{m}'A'[Z]/(g)$-адической топологии.

Далее мы используем теорему Бертини для локальных областей целостности, см. [13] и также neорему (41.7) [15] (в цитированных теоремах основное поле K не расширяется, но для наших целей мы расширяем его до $K(u_2)$). Согласно любой из этих теорем для всех элементов $c \in K(u_2)$, за ислючением конечного их числа, $K(u_1, u_2)[[X_1, \ldots, X_n]][Z]/(g, U_{n,c})$ является является целостным полным локальным кольцом. Следовательно, многочлен $g \bmod U_{n,c} \in K(u_1, u_2)[[X_1, \ldots, X_{n-1}]][Z]$ неприводим в последнем кольце (обозначим его через Λ). В частности, поскольку K бесконечно, существует $c' \in K$ такое, что $g \bmod (X_n - u_1X_1 - (u_2 - c')X_2)$ неприводим в кольце Λ. Положим $u_2' = u_2 - c'$. Теперь $K(u_1, u_2) = K(u_1, u_2')$, и многочлен $g \bmod (X_n - u_1X_1 - u_2'X_2) \in K(u_1, u_2')[[X_1, \ldots, X_{n-1}]][Z]$ неприводим в этом кольце. Очевидно достаточно доказать лемму для пары трансцендентных элементов (u_1, u_2') вместо (u_1, u_2), и это сделано. Лемма доказана. □

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

Пусть $u_1, \ldots, u_{2n-4}$ – трансцендентные элементы над полем k. Положим $l_1 = 2n-4$. Расширим основное поле k до поля $K_0 = k(u_1, \ldots, u_{l_1})$. Положим $U_i = X_i - u_{2i-5}X_1 - u_{2i-4}X_2$, $3 \leqslant i \leqslant n$. Следовательно, можно отождествить $K_0[X_1, X_2] = K_0[X_1, \ldots, X_n]/(U_3, \ldots, U_n)$.

Теперь согласно оригинальной (не для локальных колец) первой теореме Бертини многочлен $f \bmod (U_3, \ldots, U_n) \in K_0[X_1, X_2, Z]$ является неприводимым в кольце $\overline{K_0}[X_1, X_2, Z]$, см. например [9].

Применяя лемму 8 сейчас $(n-2)$ раз, мы устанавливаем, что неприводимые множители из кольца $k[[X_1, \ldots, X_n]][Z]$ (соответственно $\overline{k}[[X_1, \ldots, X_n]][Z]$) многочлена f находятся во взаимно однозначном

соответствии с неприводимыми множителями из кольца $K_0[X_1, X_2]$ (соответственно $K_0'[X_1, X_2]$) многочлена $f \bmod (U_3, \ldots, U_n)$. Пусть $g = g(X_1,\ldots,X_n,Z)$ – неприводимый множитель из кольца $k[[X_1,\ldots,X_n]][Z]$ (соответственно $\overline{k}[[X_1, \ldots, X_n]][Z]$) многочлена f. Тогда это взаимно однозначное соответствие осуществляется по правилу

$$g \mapsto g \bmod (U_2, \ldots, U_n) = \tag{35}$$
$$g(X_1, X_2, u_1X_1 + u_2X_2, u_3X_1 + u_4X_2, \ldots, u_{2n-5}X_1 + u_{2n-4}X_2, Z).$$

Следовательно, каждый неприводимый множитель g' многочлена $f \bmod (U_3, \ldots, U_n)$ из кольца $K_0[X_1, X_2]$ (соответственно $K_0'[X_1, X_2]$) со старшим коэффициентом $\mathrm{lc}_Z g' = 1$ представляется в виде

$$g' = \sum_{i_1, i_2 \geqslant 0} g'_{i_1,i_2} X_1^{i_1} X_2^{i_2}, \tag{36}$$

где все g'_{i_1,i_2} являются полиномами из $k[u_1, \ldots, u_{l_1}]$ (соответственно $\overline{k}[u_1, \ldots, u_{l_1}]$) степеней $\deg_{u_1,\ldots,u_{l_1}} g'_{i_1,i_2} \leqslant i_1 + i_2$.

Более того, пусть $g \mapsto g'$ согласно (35) и $g = \sum\limits_{\iota \geqslant 0} g_\iota$, где все ненулевые g_ι являются однородными полиномами от $X_1, \ldots, X_n$ степени ι. Тогда для всякого $\iota \geqslant 0$

$$g_\iota = \sum_{i_1, i_2 \geqslant 0, i_1 + i_2 = \iota} \left(g'_{i_1,i_1}|_{u_{2i-5} = (X_i - u_{2i-4}X_2)/X_1 \text{ для } 3 \leqslant i \leqslant n}\right) X_1^{i_1} X_2^{i_2}. \tag{37}$$

Поэтому рациональная функция от $u_2, u_4, \ldots, u_{2n-4}$ и $X_1, \ldots, X_n$ в правой части (37) фактически является однородным многочленом от $X_1, \ldots, X_n$ степени ι (если она ненулевая).

Для краткости положим $f_U = f \bmod (U_3, \ldots, U_n)$. Теперь мы можем применить теорему 2 для $n = 2$, $l_1 = 2n - 4$, $d_3 = d$ и разложить на множители многочлен f_U в кольце $K_0[[X_1, X_2]][Z]$ (соответственно $K_0'[[X_1, X_2]][Z]$). В нашем случае мы обозначаем через $f_{U,i}$, $f_{U,w}$, $f_{U,i,v,i_1,i_2,j}$ и $f_{U,w,v,i_1,i_2,j}$ элементы f_i, f_w, $f_{i,v,i_1,\ldots,i_n,j}$ и $f_{w,v,u,i_1,\ldots,i_n,j}$ из теоремы 3. Обозначения $\mathfrak{m}$, I, J_i, φ_i, $\gamma_0, \gamma_1, \lambda_0, \lambda_1$ остаются теми же самыми (имеют тот же самый смысл в рассматриваемом случае). В (36) все g'_{i_1,i_2} являются полиномами от $u_1, \ldots, u_{l_1}$. Следовательно, сейчас согласно (36) можно построить элементы $\gamma_0, \gamma_1, \lambda_0, \lambda_1$ такие, что они фактически принадлежат $\mathbb{Z}[T_1, \ldots, T_l]$ (ср. определение γ_1 с помощью γ в §3; здесь мы оставляем подробности читателю). Поскольку $n = 2$, $l_1 = 2n - 4$, $d_3 = d$, мы имеем некоторые упрощения оценок степеней, длин записи целых коэффициентов и времени работы из теоремы 2.

Кроме того, согласно (36) уже имеются хорошие оценки на степени $\deg_{u_1,\dots,u_{l_1}}$. Таким образом, в нашем случае мы переписываем пункты (iv) и (v) из теоремы 2 следующим образом.

(iv) Степени $\deg_{T_1,\dots,T_l}$ относительно $T_1,\dots,T_l$ всех элементов γ_0, γ_1, λ_0, λ_1, $f_{U,i} \bmod \mathfrak{m}^{r+1}$, $(f_U/f_{U,i}) \bmod \mathfrak{m}^{r+1}$, φ_i, $f_{U,w} \bmod \mathfrak{m}^{r+1}$, $(f_U/f_{U,w}) \bmod \mathfrak{m}^{r+1}$, $w \in J_i$, $i \in I$, ограничены сверху $\mathcal{P}(d_1,d_2,d)$. Длины записей целых коэффициентов этих элементов ограничены сверху $(M_1+M_2+l+n)\mathcal{P}(d_1,d_2,d)$.

Положим $\iota = i_1 + i_2$. Для всех w, v, u, i_1, i_2, j для всех $\iota \geqslant 0$ степени $\deg_{T_1,\dots,T_l}$ относительно $T_1,\dots,T_l$ всех элементов $f_{U,i,v,i_1,i_2,j}$ и $f_{U,w,v,i_1,i_2,j}$ таких, что $i_1+i_2=\iota$ ограничены сверху $(\iota+1)\mathcal{P}(d_1,d_2,d)$. Длины записей целых коэффициентов этих элементов ограничены сверху $(M_1+M_2+l+n)\mathcal{P}(\iota,d_1,d_2,d)$.

(v) Время работы алгоритмов для построения всех элементов γ_0, γ_1, λ_0, λ_1, $f_{U,i} \bmod \mathfrak{m}^{r+1}$, $(f_U/f_{U,i}) \bmod \mathfrak{m}^{r+1}$, φ_i, $f_{U,w} \bmod \mathfrak{m}^{r+1}$, $(f_U/f_{U,w}) \bmod \mathfrak{m}^{r+1}$, $w \in J_i$, $i \in I$, полиномиально от M_1, M_2, $(d_1d_2d)^{l+1}$, d^n.

Для всякого $\iota \geqslant 0$ время работы алгоритмов для построения всех элементов $f_{U,i,v,i_1,i_2,j}$ и $f_{U,w,v,i_1,i_2,j}$ таких, что $i_1+i_2=\iota$ полиномиально от M_1, M_2, $(d_1d_2d)^{l+1}$, d^n, ι^{l+n}.

Наконец, мы осуществляем подстановки (37) для полученных неприводимых множителей $f_{U,i}$ и $f_{U,w}$ (вместо g') и немедленно доказываем утверждения (i)–(v) теоремы 3. Теорема доказана. □

Следствие 8. *Пусть $g \in k[X_1,\dots,X_n]$ – многочлен, удовлетворяющий тем же самым оценкам на степени $\deg_{T_1,\dots,T_l}$, $\deg_{X_1,\dots,X_n}$ и длины записи целых коэффициентов, что и многочлен f из теоремы 3. Тогда можно разложить на неприводимые множители полином g в кольце формальных степенных рядов $k[[X_1,\dots,X_n]]$ (соответственно $\overline{k}[[X_1,\dots,X_n]]$). Оценки на степени всех объектов на выходе и время работы алгоритма факторизации аналогичны оценкам из пунктов* (iv) *и* (v) *теоремы* 3 (*фактически всё сводится немедленно к теореме* 3).

Доказательство. Оно аналогично доказательству следствия 2 и следствия 1 из [8], теперь мы используем теорему 3 вместо теоремы 1 [8]. Следствие доказано. □

Список литературы

1. З. И. Боревич, И. Р. Шафаревич, *"Теория чисел"*, "Наука", Москва 1964
2. Н. Бурбаки, *"Коммутативная алгебра"*, "Мир", 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. Акад. 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. 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.
9. А. Л. Чистов, *Оценка степени системы уравнений, задающей многообразие приводимых многочленов.* — Алгебра и анализ **24**, No. 3 (2012), 1999–222.
10. А. Л. Чистов, *Об оценке коэффициентов неприводимых множителей многочленов над полем формальных степенных рядов в ненулевой характеристике.* — Докл. Акад. Наук **489**, No. 3 (2019), 12–14.
11. А. Л. Чистов, *Эффективная оценка корней из поля дробно-степенных рядов заданного многочлена в ненулевой характеристике.* — Зап. научн. семин. ПОМИ **498** (2020), 64–74.
12. A. L. Chistov, *A correction of my result on the estimation of roots from a field of fractional–power series of a polynomial in nonzero characteristic.* — Preprint of SPbMO, 2023.
13. W.-L. Chow, *On the theorem of Bertini for local domains.* — Proc. National Academy of Sciences **44**, No. 6 (1958), 580–584.
14. H. Flenner, *Die Sätze von Bertini für lokale Ringe.* — Math. Ann., Bd. 229 (1977), 97–111.
15. M. Nagata, *Local rings*, Interscience Publishers, New York London, 1962.
16. A. Seidenberg, *Constructions in algebra.* — Trans. Amer. Math. Soc. **197** (1974), 273–313.
17. О. Зарисский, П. Самюэль, *Коммутативная алгебра*, т. I–II, Изд. иностранной литературы, Москва, 1963.

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

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.

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

Поступило 16 октября 2023 г.