Записки научных
семинаров ПОМИ
Том 448, 2016 г.

А. Л. Чистов

ЭФФЕКТИВНОЕ РАЗЛОЖЕНИЕ МНОГОЧЛЕНОВ С ПАРАМЕТРИЧЕСКИМИ КОЭФФИЦИЕНТАМИ НА АБСОЛЮТНО НЕПРИВОДИМЫЕ МНОЖИТЕЛИ

Введение

Пусть k – произвольное поле, содержащее по крайней мере $2d^2+1$ попарно различных элементов (d уточняется ниже, см. (1)). Пусть p – характеристическая экспонента поля k, т.е. $p=1$, если $\mathrm{char}(k)=0$, и $p=\mathrm{char}(k)$, если $\mathrm{char}(k)>0$. Пусть $a_1,\dots,a_\nu$ – семейство независимых переменных (или параметров) над k. Обозначим через $\mathbb{A}^\nu(\overline{k})$ аффинное пространство параметров с координатными функциями $a_1,\dots,a_\nu$ (в более общей ситуации можно рассматривать алгебраическое многообразие параметров $\mathcal{V}\subset\mathbb{A}^\nu(\overline{k})$, но этот случай легко сводится к частному случаю $\mathcal{V}=\mathbb{A}^\nu(\overline{k})$).

Пусть $f\in k[a_1,\dots,a_\nu,X_1,\dots,X_n]$ – многочлен и

$$\deg_{X_1,\dots,X_n} f\leqslant d,\quad \deg_{a_1,\dots,a_\nu} f\leqslant d' \tag{1}$$

для некоторых целых чисел $d\geqslant 2$ и $d'\geqslant 2$. В настоящей статье мы рассматриваем проблему, состоящую в том, чтобы представить пространство параметров

$$\mathbb{A}^\nu(\overline{k})=\bigcup_{\alpha\in A}\mathcal{W}_\alpha \tag{2}$$

как объединение конечного числа ($\#A<+\infty$) квазипроективных алгебраических многообразий $\mathcal{W}_\alpha$, удовлетворяющих следующим свойствам. Для всякого $\alpha\in A$ для всех $a^*=(a_1^*,\dots,a_\nu^*)\in\mathcal{W}_\alpha$ существует разложение

$$f(a_1^*,\dots,a_\nu^*,X_1,\dots,X_n)=\lambda_{a^*}\prod_{\gamma\in\Gamma_\alpha}F_{\gamma,a^*}^{e_\gamma}(X_1^{p^{i_\gamma}},\dots,X_n^{p^{i_\gamma}}), \tag{3}$$

Ключевые слова: параметрические коэффициенты, стратификации, абсолютно неприводимые множители, факторизация многочленов.

где $f_{\gamma,a^*} \in \overline{k}[X_1,\dots,X_n]$ – неприводимые многочлены над полем $\overline{k}$, $\lambda_{a^*} \in k$, $0 \leqslant e_\gamma \in \mathbb{Z}$, $1 \leqslant i_\gamma \in \mathbb{Z}$, $\#\Gamma_\alpha < +\infty$. Разложение (3) задано равномерно, т.е. некоторыми алгебраическими формулами (см. подробности ниже), определёнными везде на $\mathcal{W}_\alpha$ и зависящими от $a_1^*,\dots,a_\nu^*$ как от параметров. Отметим здесь, что все целые числа e_γ, i_γ и множества индексов Γ_α не зависят от $a^* \in \mathcal{W}_\alpha$.

Теперь мы собираемся придать точный смысл этой равномерности. Именно, разложение (2) удовлетворяет следующим свойствам.

(i) Для всякого $\alpha \in A$ многообразие $\mathcal{W}_\alpha$ непусто. Для всех пар $\alpha_1,\alpha_2 \in A$ если $\alpha_1 \neq \alpha_2$, то $\mathcal{W}_{\alpha_1} \cap \mathcal{W}_{\alpha_2} = \varnothing$, т.е. эти многообразия $\mathcal{W}_\alpha$ являются попарно непересекающимися; так что мы будем называть их стратами, а объединение (2) стратификацией.

(ii) Можно представить $\mathcal{W}_\alpha$ в виде

$$\mathcal{W}_\alpha = \mathcal{W}_\alpha^{(1)} \setminus \bigcup_{2\leqslant\beta\leqslant\mu_\alpha} \mathcal{W}_\alpha^{(\beta)},$$

где $\mathcal{W}_\alpha^{(\beta)} = \mathcal{Z}(\psi_{\alpha,1}^{(\beta)},\dots,\psi_{\alpha,m_{\alpha,\beta}}^{(\beta)})$, $1 \leqslant \beta \leqslant \mu_\alpha$, есть множество всех общих нулей многочленов $\psi_{\alpha,1}^{(\beta)},\dots,\psi_{\alpha,m_{\alpha,\beta}}^{(\beta)} \in k[a_1,\dots,a_\nu]$ в аффинном пространстве $\mathbb{A}^\nu(\overline{k})$, а $m_{\alpha,\beta} \geqslant 1$ – целое число.

Для всякого $\alpha \in A$ обозначим через $\overline{\mathcal{W}}_\alpha$ замыкание относительно топологии Зарисского алгебраического многообразия $\mathcal{W}_\alpha$ в $\mathbb{A}^\nu(\overline{k})$. Обозначим через $\mathcal{I}_\alpha$ идеал аффинного алгебраического многообразия $\overline{\mathcal{W}}_\alpha$.

(iii) Существуют множество индексов J_α, многочлены $\lambda_{\alpha,0},\lambda_{\alpha,1} \in k[a_1,\dots,a_\nu]$, многочлены $f_j \in k[a_1,\dots,a_\nu,X_1,\dots,X_n]$, целые числа e_j, взаимно простые с p, целые числа $i_j \geqslant 0$ для всех $j \in J_\alpha$, такие, что $\lambda_{\alpha,0},\lambda_{\alpha,1}$ не обращаются в нуль ни в какой точке алгебраического многообразия $\mathcal{W}_\alpha$ и

$$f = \frac{\lambda_{\alpha,1}}{\lambda_{\alpha,0}} \prod_{j\in J_\alpha} f_j^{e_j}(a_1,\dots,a_\nu,X_1^{p^{i_j}},\dots,X_n^{p^{i_j}}) \tag{4}$$

на алгебраическом многообразии $\overline{\mathcal{W}}_\alpha$ (это означает, что многочлен $\lambda_{\alpha,0}f - \lambda_{\alpha,1}\prod_{j\in J_\alpha} f_j^{e_j}(a_1,\dots,a_\nu,X_1^{p^{i_j}},\dots,X_n^{p^{i_j}})$ лежит в $\mathcal{I}_\alpha$ и $J_{\alpha_1} \cap J_{\alpha_2} = \varnothing$ при $\alpha_1 \neq \alpha_2$. Кроме того, если $p = 1$, то $i_j = 0$ для всякого $j \in J_\alpha$.

(iv) Для всякого $i = -1, 0$ существует не более одного $\alpha \in A$, такого, что $\deg f_j = i$ для некоторого $j \in J_\alpha$. В этом случае имеем $\#J_\alpha = 1$, $e_j = 1$, $\lambda_{\alpha,0} = \lambda_{\alpha,1} = 1$ и если $i = -1$, то $f_j = 0$, если $i = 0$, то $0 \neq f_j = f(a_1, \dots, a_\nu, 0, \dots, 0) \in k[a_1, \dots, a_\nu]$.

(v) Для всякого $\alpha \in A$ для всякого $j \in J_\alpha$ для всякого $a^* \in \mathcal{W}_\alpha$

$$\deg_{X_1,\dots,X_n} f_j(a_1^*, \dots, a_\nu^*, X_1, \dots, X_n) = \deg_{X_1,\dots,X_n} f_j.$$

Если $\deg_{X_1,\dots,X_n} f_j \geqslant 0$, то многочлен $f_j(a_1^*, \dots, a_\nu^*, X_1, \dots, X_n)$ сепарабелен (не имеет кратных множителей в $\overline{k}[X_1, \dots, X_n]$). Для всех попарно различных индексов $j_1, j_2 \in J_\alpha$ многочлены $f_{j_1}(a_1^*, \dots, a_\nu^*, X_1, \dots, X_n)$ и $f_{j_2}(a_1^*, \dots, a_\nu^*, X_1, \dots, X_n)$ взаимно просты в кольце $\overline{k}[X_1, \dots, X_n]$.

Обозначим через A' подмножество в A, такое, что $\deg f_j \geqslant 1$ для всех $j \in J_\alpha$. Для всех $\alpha \in A'$, $j \in J_\alpha$ существует многочлен $H_j \in k[a_1, \dots, a_\nu][Z]$, удовлетворяющий следующим свойствам.

(vi) Пусть $\alpha \in A'$, $j \in J_\alpha$. Обозначим через $\Delta_j \in k[a_1, \dots, a_\nu]$ дискриминант многочлена H_j относительно Z. Тогда Δ_j не обращается в нуль ни в какой точке алгебраического многообразия $\mathcal{W}_\alpha$.

В условиях пункта (vi) для всякого $a^* \in \mathcal{W}_\alpha$ обозначим через Ξ_{j,a^*} множество всех корней многочлена $H_{\alpha,j}(a_1^*, \dots, a_\nu^*, Z) \in \overline{k}[Z]$. Тогда согласно (vi) для всякого $a^* \in \mathcal{W}_\alpha$ число корней $\#\Xi_{j,a^*}$ равно $\deg_Z H_j$ и старший коэффициент $\mathrm{lc}_Z H_j$ не обращается в нуль ни в какой точке a^*.

(vii) Пусть $\alpha \in A'$, $j \in J_\alpha$. Тогда существует такой многочлен $F_j \in k[a_1, \dots, a_\nu, Z, X_1, \dots, X_n]$, что для всякого $a^* \in \mathcal{W}_\alpha$ для всякого корня $\xi \in \Xi_{j,a^*}$ многочлен $F_j(a_1^*, \dots, a_\nu^*, \xi, X_1, \dots, X_n)$ неприводим в кольце $\overline{k}[X_1, \dots, X_n]$ (т.е. абсолютно неприводим), $0 \leqslant \deg_Z F_j < \deg_Z H_j$ и

$$\deg_{X_1,\dots,X_n} F_j(a_1^*, \dots, a_\nu^*, \xi, X_1, \dots, X_n) = \deg_{X_1,\dots,X_n} F_j.$$

(viii) Пусть $\alpha \in A'$, $j \in J_\alpha$. Тогда

$$f_j(a_1^*, \dots, a_\nu^*, X_1, \dots, X_n) = \prod_{\xi \in \Xi_{j,a^*}} F_j(a_1^*, \dots, a_\nu^*, \xi, X_1, \dots, X_n) \qquad (5)$$

и, таким образом, (5) есть разложение сепарабельного многочлена $f_j(a_1^*, \dots, a_\nu^*, X_1, \dots, X_n)$ в произведение попарно различных абсолютно неприводимых множителей. Следовательно, степень $\deg_Z H_j = \#\Xi_{j,a^*}$ ограничена сверху числом d.

Теперь мы можем сформулировать наш основной результат.

Теорема 1. *Пусть многочлен* $f \in k[a_1, \dots, a_\nu, X_1, \dots, X_n]$ *– такой же, как и выше. Тогда существует стратификация* $\{\mathcal{W}_\alpha\}_{\alpha \in A}$ *пространства параметров* $\mathbb{A}^\nu(\overline{k})$*, удовлетворяющая свойствам* (i)–(viii) *и такая, что*

(a) *число элементов* $\#A$ *и целые числа* μ_α *ограничены сверху величиной* $(d')^\nu\ d^{O(\nu)}$ *с абсолютной константой в* $O(\nu)$*,*

(b) *степени относительно переменных* $a_1, \dots, a_\nu$ *всех многочленов* $\psi^{(\beta)}_{\alpha,1}, \dots, \psi^{(\beta)}_{\alpha,m_{\alpha,\beta}}$*,* $\lambda_{\alpha,0}, \lambda_{\alpha,1}$*,* H_j*,* F_j*,* f_j *ограничены сверху величиной* $d' d^{O(1)}$ *с абсолютной константой в* $O(1)$*.*

Доказательство этой теоремы основывается на работах [1, 2]. Можно рассмотреть также случай покрытия пространства параметров вместо его стратификации (т.е. в этом случае свойство (i) не обязательно выполняется). Если заменить “(i)–(viii)” в формулировке теоремы 1 на “(ii)–(viii)”, то можно утверждать дополнительно, что $\mu_\alpha = 2$ для всякого $\alpha \in A$.

Замечание 1. Пусть $d \geqslant -1$ – целое число. Согласно [1] мы отождествляем множество многочленов из $\overline{k}[X_1, \dots, X_n]$ степени не больше d с $\overline{k}^{N(n,d)}$, где $N(n,d) = \binom{n+d}{n}$. Обозначим через $P_{n,d} \subset \overline{k}^{N(n,d)}$ подмножество многочленов из $\overline{k}[X_1, \dots, X_n]$ степени d. В [1] мы ввели функцию $\mathrm{RDP}_{X_1,\dots,X_n} : \bigcup\limits_{d \geqslant 0} \overline{k}^{N(n,d)} \to \bigcup\limits_{d \geqslant 0} P_{n,d}$, соответствующую некоторому лесу вычислений, см. [1]. Именно, если $g \in \overline{k}^{N(n,d)}$, то $\mathrm{RDP}_{X_1,\dots,X_n}(g) \in P_{n,d'}$, где $d' = \deg_{X_1,\dots,X_n} g$ – степень многочлена g, и $g = \mathrm{RDP}_{X_1,\dots,X_n}(g)$ в $\overline{k}[X_1, \dots, X_n]$. На протяжении этой статьи иногда мы применяем функцию $\mathrm{RDP}_{X_1,\dots,X_n}$ (или аналогичную функцию с другими переменными вместо $X_1, \dots, X_n$), не упоминая об этом. Это не приведёт к двусмысленности. Функция $\mathrm{RDP}_{X_1,\dots,X_n}$ используется, когда необходимо знать точные степени рассматриваемых многочленов.

§1. Нётерова нормализация многочлена

Пусть k – поле. Пусть $0 \neq f \in k[X_1, \dots, X_n]$ – многочлен степени $\deg_{X_1,\dots,X_n} f = d$ для некоторого целого числа $d \geqslant 0$. Тогда можно

представить f в виде

$$f = \sum_{\substack{i_1,\dots,i_n \geqslant 0 \\ i_1+\dots+i_n \leqslant d}} f_{i_1,\dots,i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n},$$

где все коэффициенты $f_{i_1,\dots,i_n}$ лежат в k.

Положим $K_0 = k_0 = \mathbb{Z}$, если $\mathrm{char}(k) = 0$. Если $\mathrm{char}(k) = p > 0$, то пусть $k_0 = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ является примитивным полем. Далее, положим K_0 равным некоторому кольцу, такому, что $k_0 \subset K_0 \subset k$ и K_0 содержит по крайней мере $2d^2+1$ элементов. Кольцо K_0 существует, поскольку $\#k \geqslant 2d^2+1$, см. введение. В дальнейшем нам потребуется выбирать конечные множества с достаточно большим числом элементов из поля k. Мы будем выбирать эти множества из кольца K_0.

Пусть $\mathcal{J}_d \subset K_0$ – подмножество, содержащее в точности $d+1$ элементов. Мы выбираем и фиксируем это подмножество $\mathcal{J}_d$. В случае $\mathrm{char}(k) = 0$ положим $\mathcal{J}_d = \{0, 1, \dots, d\} \subset \mathbb{Z}$. Дополнительно мы будем предполагать без ограничения общности, что множество $\mathcal{J}_d$ является вполне упорядоченным.

Пусть $j_2, \dots, j_n \in \mathcal{J}_d$. Положим

$$f^{(j_2,\dots,j_n)} = f(X_1, X_2 + j_2X_1, \dots, X_n + j_nX_1) \in k[X_1, \dots, X_n].$$

Упорядочим множество мультииндексов $(j_2, \dots, j_n) \in \mathcal{J}_d^{n-1}$ лексикографически: $(j_2, \dots, j_n) < (j_2', \dots, j_n')$ в том и только в том случае, если существует целое число α, где $2 \leqslant \alpha \leqslant n$, такое, что $j_v = j_v'$ при $2 \leqslant v < \alpha$, но $j_\alpha < j_\alpha'$. Обозначим через $\mathcal{J}_{n,d}$ множество всех мультииндексов $(j_2, \dots, j_n) \in \mathcal{J}_d^{n-1}$, таких, что $j_\alpha \in \mathcal{J}_d$ при $2 \leqslant \alpha \leqslant n$. Тогда множество $\mathcal{J}_{n,d}$ линейно упорядочено и $\#\mathcal{J}_{n,d} = (d+1)^{n-1}$.

Пусть $f = \varphi_0 + \varphi_1 + \dots + \varphi_d$, где $\varphi_i \in k[X_1, \dots, X_n]$ – однородный многочлен степени i.

Положим $\mathrm{NN}_{X_1}(f; X_1, \dots, X_n) = f^{(\iota_2,\dots,\iota_n)}$, где $(\iota_2, \dots, \iota_n)$ – наименьший мультииндекс из $\mathcal{J}_{n,d}$, такой, что

$$0 \neq \varphi_d(1, \iota_2, \dots, \iota_n) \in k$$

(здесь NN – сокращение для нётеровой нормализации). Положим

$$\mathrm{inn}_{X_1}(f; X_1, \dots, X_n) = (\iota_2, \dots, \iota_n).$$

Тогда $f \mapsto \mathrm{inn}_{X_1}(f; X_1, \dots, X_n)$ есть функция $P_{n,d} \to \mathcal{J}_{n-1,d}$.

Другими словами,

$$\mathrm{NN}_{X_1}(f; X_1, \dots, X_n) = f^{(\iota_2,\dots,\iota_n)} \text{ и } \mathrm{inn}_{X_1}(f; X_1, \dots, X_n) = (\iota_2, \dots, \iota_n)$$

тогда и только тогда, когда $\varphi_d(1, \iota_2, \dots, \iota_n) \neq 0$ и $\varphi_d(1, j_2, \dots, j_n) = 0$ для всех $(j_2, \dots, j_n) \in J_{n,d}$, таких, что $(j_2, \dots, j_n) < (\iota_2, \dots, \iota_n)$.

Если $k = \overline{k}$ (т.е. поле k алгебраически замкнуто), то функция

$$\bigcup_{d \geqslant 0} P_{n,d} \to \bigcup_{d \geqslant 0} P_{n,d}, \quad f \mapsto \mathrm{NN}_{X_1}(f; X_1, \dots, X_n),$$

является алгоритмом, соответствующим лесу вычислений. Обозначим этот лес через $\{T_d\}_{d \geqslant 0}$. Каждое дерево T_d имеет $(d+1)^{n-1}$ листьев и уровень $l(T_d) = 1$.

Заметим, что определена композиция $\mathrm{LC}_{X_1} \circ \mathrm{NN}_{X_1}$, см. пример 3 из раздела 3 работы [1], и $\mathrm{LC}_{X_1}(\mathrm{NN}_{X_1}(f)) = f(1, \iota_2, \dots, \iota_n)$.

§2. Разложение на свободные от квадратов множители

Сначала напомним результат работы [3] в требуемой для нас форме. Если не оговорено противное, в этом разделе Λ является целостной алгеброй над основным полем k с полем частных L (конечно, читатель увидит, что некоторые утверждения справедливы в случае, когда Λ – произвольное целостное кольцо). Пусть $f, g \in \Lambda[X]$ – два многочлена от одной переменной X. Пусть $\deg_X f = n \geqslant 0$, $\deg_X g = m \geqslant 0$. Пусть r – целое число, $0 \leqslant r \leqslant \min\{n, m\} - 1$. Пусть $A, B \in L[X]$ – многочлены, такие, что $0 \leqslant \deg_X A \leqslant m-r-1$, $0 \leqslant \deg_X B \leqslant n-r-1$. Положим $h = Af + Bg$.

Пусть

$$f = \sum_{0 \leqslant i \leqslant n} f_i X^i, \quad g = \sum_{0 \leqslant i \leqslant m} g_i X^i, \quad h = \sum_{0 \leqslant i \leqslant m+n-r-1} h_i X^i,$$
$$A = \sum_{0 \leqslant i \leqslant m-r-1} A_i X^i, \quad B = \sum_{0 \leqslant i \leqslant n-r-1} B_i X^i,$$

где $f_i, g_i \in \Lambda$, $h_i, A_i, B_i \in L$. Предположим, что f, g, h заданы. Тогда равенство $Af + Bg = h$ эквивалентно линейной системе

$$\sum_{\max\{\nu-n,0\} \leqslant i \leqslant \nu} A_i f_{\nu-i} + \sum_{\max\{\nu-m,0\} \leqslant j \leqslant \nu} B_j g_{\nu-j} = h_\nu,$$
$$0 \leqslant \nu \leqslant n+m-r-1, \tag{6}$$

относительно неизвестных A_i, $0 \leqslant i \leqslant m-r-1$, и B_j, $0 \leqslant j \leqslant n-r-1$, которую мы обозначим $\mathcal{S}_r$. Обозначим через S_r матрицу коэффициентов этой системы. Она имеет $m+n-r$ строк и $m+n-2r$ столбцов.

Заметим, что S_r является подматрицей матрицы Сильвестра $\mathrm{Syl}(f,g)$ многочленов f и g.

Для всякого i, $0 \leqslant i \leqslant r$, обозначим через $\mathcal{S}_{r,i}$ подсистему системы $\mathcal{S}_r$, состоящую из уравнений из (6) с $\nu = i$ и $r+1 \leqslant \nu \leqslant n+m-r-1$ (так что число уравнений системы $\mathcal{S}_{r,i}$ равно $m+n-2r$). Обозначим через $S_{r,i}$ матрицу коэффициентов системы $\mathcal{S}_{r,i}$. Тогда $S_{r,i}$ имеет $m+n-2r$ строк и $m+n-2r$ столбцов. Положим $\delta_{r,i} = \det(S_{r,i})$, $0 \leqslant i \leqslant r$.

Если $h = \gcd(f,g) \in L[X]$ – наибольший общий делитель многочленов f, g в кольце многочленов $L[X]$ (он однозначно определён с точностью до множителя из $L \setminus \{0\}$) и $\deg_X h = r$, $0 \leqslant r \leqslant \min\{m,n\} - 1$ (так что $h_i = 0$ при $r+1 \leqslant i \leqslant n+m-r-1$), то существуют единственные многочлены $A, B \in L[X]$, такие, что $\deg_X A \leqslant m-r-1$, $\deg_X B \leqslant n-r-1$ и $h = Af + Bg$.

Далее, рассмотрим случай $r = \min\{n,m\}$ (в котором система $\mathcal{S}_r$ не определена). Если $n = r$, то положим по определению $\delta_{r,i} = f_i$ при $0 \leqslant i \leqslant r$, а если $n \neq r$, то положим $\delta_{r,i} = g_i$ при $0 \leqslant i \leqslant r$.

Лемма 1. *В описанных условиях справедливы следующие утверждения.*

(i) *Пусть $h = \gcd(f,g) \in L[X]$ – наибольший общий делитель многочленов f, g в кольце $L[X]$ и $\deg_X h = r \leqslant \min\{m,n\}$. Тогда если $r \leqslant \min\{m,n\} - 1$, то система $\mathcal{S}_r$ эквивалентна системе $\mathcal{S}_{r,r}$ и система $\mathcal{S}_{r,r}$ имеет единственное решение.*

Следовательно, при $0 \leqslant r \leqslant \min\{m,n\}$ имеем $\delta_{r,r} \neq 0$, и при $0 \leqslant i \leqslant r$ имеем $h_i/h_r = \delta_{r,i}/\delta_{r,r}$.

(ii) *Предположим, что $0 \leqslant r \leqslant \min\{m,n\} - 1$, $h_i = 0$ при $r+1 \leqslant i \leqslant n+m-r-1$, $h_r \neq 0$ и система $\mathcal{S}_{r,r}$ не имеет решения. Тогда $\delta_{r,r} = 0$ и $\deg_X \gcd(f,g) > r$.*

Доказательство. Эти утверждения следуют из данных определений непосредственно, и мы оставляем их доказательство читателю, ср. также [3]. □

Следствие 1. *Для заданных многочленов $f, g \in \Lambda[X]$, таких, как выше, $\deg_X \gcd(f,g) = r \leqslant \min\{m,n\}$ в том и только в том случае, если $\delta_{j,j} = 0$ при $0 \leqslant j \leqslant r-1$ и $\delta_{r,r} \neq 0$. Более того, в этом случае*

$$\gcd(f,g) = \sum_{0 \leqslant i \leqslant r} \delta_{r,i} X^i \in \Lambda[X]. \tag{7}$$

Доказательство. Это немедленно вытекает из леммы 1. □

Очевидно, существуют единственные такие многочлены $\Delta_{r,i} \in k_0\ [Y_0, \dots, Y_n, Z_0, \dots, Z_m]$ (здесь Y_i, Z_j – новые переменные), что $\delta_{r,i} = \Delta_{r,i}(f_0, \dots, f_n, g_0, \dots, g_m)$ для всех i, $0 \leqslant i \leqslant r$, и всех многочленов f, g и колец Λ, таких, как выше. При $0 \leqslant r \leqslant \min\{m, n\}$, $0 \leqslant i \leqslant r$ мы имеем следующие оценки на степени относительно всех переменных $Y_0, \dots, Y_n$ и $Z_0, \dots, Z_m$:

$$\deg_{Y_0,\dots,Y_n} \Delta_{r,i} \leqslant m - r, \quad \deg_{Z_0,\dots,Z_m} \Delta_{r,i} \leqslant n - r. \tag{8}$$

Напомним, что $f, g \in \Lambda[X]$, $\deg_X f = n \geqslant 0$, $\deg_X g = m \geqslant 0$. Мы используем следующее определение.

(**) Пусть r – произвольное целое число, $0 \leqslant r \leqslant \min\{m, n\}$. Если $\Delta_{j,j}(f_0, \dots, f_n, g_0, \dots, g_m) = 0$ при $0 \leqslant j < r$ и

$$\Delta_{r,r}(f_0, \dots, f_n, g_0, \dots, g_m) \neq 0,$$

то

$$\mathrm{G\,C\,D}_{\Lambda,X}(f, g) = \sum_{0 \leqslant i \leqslant r} \Delta_{r,i}(f_0, \dots, f_n, g_0, \dots, g_m) X^i.$$

В частном случае, когда $k = \overline{k}$ есть алгебраически замкнутое поле, функция $\mathrm{G\,C\,D}_{\overline{k},X} : \bigcup_{n,m \geqslant 0}(P_n \times P_m) \to \bigcup_{r \geqslant 0} P_r$ является алгоритмом, соответствующим лесу вычислений. Обозначим этот лес через $\{T_{n,m}\}_{n,m \geqslant 0}$. Каждое дерево $T_{n,m}$ имеет $1 + \min\{m, n\}$ листьев и уровень 1.

Лемма 2. *Пусть n, m – целые числа, $n \geqslant m \geqslant 0$. Существуют многочлены*

$$Q_i \in k_0[Y_0, \dots, Y_n, Z_0, \dots, Z_m], \quad 0 \leqslant i \leqslant n - m,$$
$$R_i \in k_0[Y_0, \dots, Y_n, Z_0, \dots, Z_m], \quad 0 \leqslant i \leqslant m - 1,$$

удовлетворяющие следующим свойствам. Пусть Λ – произвольная коммутативная алгебра над k_0 с единицей. Пусть $f, g \in \Lambda[X]$ – два многочлена, такие, что $\deg_X f = n$, $\deg_X g = m$ и $f = \sum\limits_{0 \leqslant i \leqslant n} f_i X^i$, $g = \sum\limits_{0 \leqslant j \leqslant m} g_j X^j$, где $f_i, g_j \in \Lambda$. Тогда

$$g_m^{n-m+1} f = g \sum_{0 \leqslant i \leqslant m-n} Q_i(f_0, \dots, f_n, g_0, \dots, g_m) X^i$$
$$+ \sum_{0 \leqslant i \leqslant m-1} R_i(f_0, \dots, f_n, g_0, \dots, g_m) X^i$$

в кольце $\Lambda[X]$. *Кроме того,*

$$\deg_{Y_0,\dots,Y_n} Q_i \leqslant 1, \quad \deg_{Z_0,\dots,Z_m} Q_i \leqslant n-m, \quad 0 \leqslant i \leqslant n-m, \tag{9}$$

$$\deg_{Y_0,\dots,Y_n} R_i \leqslant 1, \quad \deg_{Z_0,\dots,Z_m} R_i \leqslant n-m+1, \quad 0 \leqslant i \leqslant m-1. \tag{10}$$

Далее, пусть L *– полное кольцо частных кольца* Λ. *Предположим дополнительно, что старший коэффициент* $g_m = \mathrm{lc}_X g$ *не является делителем нуля в* Λ *и* g *делит* f *в кольце* $L[X]$. *Тогда для всех* i

$$R_i(f_0,\dots,f_n,g_0,\dots,g_m) = 0.$$

Доказательство. Утверждение получается непосредственно. □

Для любых многочленов f, g, удовлетворяющих условиям леммы 2, положим по определению

$$Q_{\Lambda,X}(f,g) = \sum_{0\leqslant i\leqslant m-n} Q_i(f_0,\dots,f_n,g_0,\dots,g_m)X^i,$$

$$R_{\Lambda,X}(f,g) = \sum_{0\leqslant i\leqslant m-1} R_i(f_0,\dots,f_n,g_0,\dots,g_m)X^i.$$

Рассмотрим случай многих переменных. Пусть $n \geqslant 2$. Пусть $f,g \in k[X_1,\dots,X_n]$, $\deg_{X_1,\dots,X_n} f = d_1 \geqslant 0$, $\deg_{X_1,\dots,X_n} g = d_2 \geqslant 0$. Положим

$$f_1 = \mathrm{NN}_{X_1}(f;X_1,\dots,X_n), \quad \mathrm{inn}_{X_1}(f;X_1,\dots,X_n) = (i_2,\dots,i_n),$$

$g_1 = g(X_1, X_2 + i_2X_1,\dots,X_1 + i_nX_n)$. Положим $\Lambda = k[X_2,\dots,X_n]$ и $h = \mathrm{G\,C\,D}_{\Lambda,X_1}(f_1,g_1)$, $a = \mathrm{LC}_{X_1}(h)$,

$$a_1 = \mathrm{NN}_{X_2}(a;X_2,\dots,X_n), \quad (\iota_3,\dots,\iota_n) = \mathrm{inn}_{X_2}(a;X_2,\dots,X_n),$$

$h_1 = h(X_1,X_2,X_3+\iota_3X_2,\dots,X_n+\iota_nX_2)$, $\Lambda_1 = k[X_1,X_3,\dots,X_n]$, $q_1 = Q_{\Lambda_1,X_2}(h_1,a_1)$ и $q_2 = q_1(X_1,X_2,X_3-\iota_3X_2,\dots,X_n-\iota_nX_2)$, $q = q_2(X_1,X_2-i_2X_1,\dots,X_1-i_nX_n)$. Тогда, очевидно, q является наибольшим общим делителем многочленов f,g в кольце $k[X_1,\dots,X_n]$. Если $k=\overline{k}$, то определена функция

$$\mathrm{G\,C\,D}_{X_1,\dots,X_n} : \bigcup_{d_1,d_2\geqslant 0}(P_{n,d_1}\times P_{n,d_2}) \to \bigcup_{d\geqslant 0} P_{n,d}, \quad (f,g)\mapsto q.$$

Эта функция $\mathrm{G\,C\,D}_{X_1,\dots,X_n}$ соответствует лесу вычислений $\{T_{d_1,d_2}\}_{d_1,d_2\geqslant 0}$, см. определения в [1].

Теперь мы переходим к факторизации на бесквадратные многочлены. Пусть $f \in k[X_1, \dots, X_n]$ – многочлен с $\deg_{X_1,\dots,X_n} f \geqslant 1$. Обозначим через k_{pf} совершенное замыкание поля k. Тогда можно представить f в виде

$$f = \lambda_0 F_1 F_2^2 \dots F_d^d, \tag{11}$$

где $0 \neq \lambda_0 \in k$, все многочлены $F_i \in k_{\mathrm{pf}}[X_1, \dots, X_n]$ являются сепарабельными (или, что то же самое, бесквадратными), при $1 \leqslant i_1 \neq i_2 \leqslant d$ наибольший общий делитель $\gcd(F_{i_1}, F_{i_2})$ равен 1 и $\deg_{X_1,\dots,X_n} F_i \geqslant 0$. Мы увидим, что $F_i^i \in k[X_1, \dots, X_n]$, $1 \leqslant i \leqslant d$.

Сначала предположим, что $\mathrm{char}(k) = 0$. Тогда $k = k_{\mathrm{pf}}$. Положим

$$f_1 = \mathrm{NN}_{X_1}(f; X_1, \dots, X_n), (\iota_2, \dots, \iota_n) = \mathrm{inn}_{X_1}(f; X_1, \dots, X_n).$$

Пусть $\Lambda = k[X_2, \dots, X_n]$. Пусть $f_1' = \frac{df_1}{dX}$ – производная многочлена f_1. Тогда положим

$$q_1 = Q_{\Lambda, X_1}(f_1, \mathrm{G\,C\,D}_{X_1,\dots,X_n}(f_1, f_1')) \in k[X_1, \dots, X_n]$$

и $G = q_1(X_1, X_2 - \iota_2 X_1, \dots, X_n - \iota_n X_1)$. Очевидно, $G = \lambda_1 F_1 F_2, \dots, F_d$, где $0 \neq \lambda_1 \in k$, так что G является бесквадратной частью многочлена f в кольце $k[X_1, \dots, X_n]$.

Предположим, что $\mathrm{char}(k) = p > 0$. Пусть i – неотрицательное целое число. Положим $B_i = \{jp^i : 1 \leqslant jp^i \leqslant d \ \&\ j \in \mathbb{Z}\}$ (следовательно, $B_i = \varnothing$, если $p^i > d$) и $\Phi_i = \prod\limits_{j \in B_i} F_j^j$. Положим

$$\Psi_i = \Phi_i(X_1^{p^{-i}}, \dots, X_n^{p^{-i}}) / \Phi_{i+1}(X_1^{p^{-i}}, \dots, X_n^{p^{-i}}).$$

Теперь

$$f = \lambda_0 \prod_{0 \leqslant i \leqslant \log_p d} \Psi_i(X_1^{p^i}, \dots, X_n^{p^i})$$

и

$$\Psi_i = \prod_{j \in B_i \setminus B_{i+1}} F_j(X_1^{p^{-i}}, \dots, X_n^{p^{-i}})^j.$$

Заметим, что если $j \in B_i \setminus B_{i+1}$, то j/p^i является целым числом и p не делит j/p^i.

Пусть i фиксировано. Можно представить многочлен f в виде $f = \sum\limits_{0 \leqslant r_1, \dots, r_n < p^i} X_1^{r_1} \cdot \ldots \cdot X_n^{r_n} f_{i, r_1, \dots, r_n}$, где $f_{i, r_1, \dots, r_n} \in k[X_1^{p^i}, \dots, X_n^{p^i}]$. Мы имеем $\gcd\{f_{i, r_1, \dots, r_n} : 0 \leqslant r_1, \dots, r_n < p^i\} = \Phi_i$ в кольце $k[X_1, \dots, X_n]$ (мы оставляем подробности читателю).

Тогда можно вычислить Φ_i, например, следующим образом. Пусть $Y_1, \dots, Y_n$ – новые переменные. Положим

$$q_i = \sum_{0 \leqslant r_1, \dots, r_n < p^i} Y_1^{r_1} \dots Y_n^{r_n} f_{i, r_1, \dots, r_n} \in k[Y_1 \dots, Y_n, X_1, \dots, X_n].$$

Тогда $\Phi_i = \mathrm{G\,C\,D}_{Y_1 \dots, Y_n, X_1, \dots, X_n}(q_i, \mathrm{LC}_Y(q_i))$ с точностью до ненулевого множителя из k, и мы будем предполагать без ограничения общности, что этот множитель равен 1.

Положим $\Lambda = k[X_2, \dots, X_n]$,

$$\varphi_1 = \mathrm{NN}_{X_1}(\Phi_{i+1}; X_1, \dots, X_n), \quad (\iota_1, \dots, \iota_n) = \mathrm{inn}_{X_1}(\Phi_{i+1}; X_1, \dots, X_n),$$

$\varphi_2 = \Phi_i(X_1, X_2 + \iota_2 X_1, \dots, X_n + \iota_n X_1)$, $\psi_1 = Q_{\Lambda, X_1}(\varphi_2, \varphi_1)$, $\psi_2 = \psi_1(X_1, X_2 - \iota_2 X_1, \dots, X_n - \iota_n X_1)$, $\psi_3 = \psi_2(X_1^{p^{-i}}, \dots, X_n^{p^{-i}})$. Теперь многочлен ψ_3 совпадает с Ψ_i с точностью до ненулевого множителя из k.

Далее, аналогично случаю нулевой характеристики положим

$$\psi = \mathrm{NN}_{X_1}(\psi_3; X_1, \dots, X_n), \quad (\iota'_2, \dots, \iota'_n) = \mathrm{inn}_{X_1}(\psi_3; X_1, \dots, X_n),$$
$$q_1 = Q_{\Lambda, X_1}\Big(\psi, \mathrm{G\,C\,D}_{Y_1, \dots, Y_n, X_1, \dots, X_n}\Big(\psi, \sum_{1 \leqslant i \leqslant n} Y_i \frac{\partial \psi}{\partial X_i}\Big)\Big) \in k[X_1, \dots, X_n]$$

и $G_i = q_1(X_1, X_2 - \iota'_2 X_1, \dots, X_n - \iota'_n X_1)$. Очевидно, G_i является бесквадратной частью многочлена Ψ_i в кольце $k[X_1, \dots, X_n]$. Мы имеем

$$G_i(X_1^{p^i}, \dots, X_n^{p^i}) = \mu_i \prod_{j \in B_i \setminus B_{i+1}} F_j^{p^i},$$
$$\prod_{0 \leqslant i \leqslant \log_p d} G_i(X_1^{p^i}, \dots, X_n^{p^i})^{p^{-i}} = \mu F_1, \dots, F_d,$$

где $0 \neq \mu_i \in k$, $0 \neq \mu \in k_{\mathrm{pf}}$. Так что фактически семейство сепарабельных многочленов G_i, $0 \leqslant i \leqslant \log_p d$, определяет бесквадратную часть многочлена f.

Вернёмся к случаю произвольной характеристики основного поля. Пусть j – произвольное целое число, $1 \leqslant j \leqslant d$.

Если $\mathrm{char}(k) = 0$, то положим $G_0 = G$, $B_0 = \{1, 2, \dots, d\}$, $B_1 = \varnothing$, $i = 0$, $p = 1$. Если $\mathrm{char}(k) = p > 0$, то пусть p^i делит j и p^{i+1} не делит j для некоторого целого числа i, $0 \leqslant i \leqslant \log_p d$.

Теперь мы собираемся найти многочлен $F_j^{p^i}(X_1^{p^{-i}},\dots,X_n^{p^{-i}})$ с точностью до ненулевого множителя из k. Положим

$$G_{i,\alpha} = \mathrm{G\,C\,D}_{X_1,\dots,X_n}(G_i(X_1^{p^i},\dots,X_n^{p^i}),F^\alpha),\quad 1\leqslant\alpha\in\mathbb{Z}.$$

Тогда $G_{i,\alpha}$ совпадает с

$$\prod_{j\in B_i\setminus B_{i+1}\,\&\,j<\alpha p^i} F_j^j \times \prod_{j\in B_i\setminus B_{i+1}\,\&\,j\geqslant\alpha p^i} F_j^{\alpha p^i}$$

с точностью до ненулевого множителя из k. Частное $G_{i,\alpha}/G_{i,\alpha-1}$ совпадает с

$$\prod_{j\in B_i\setminus B_{i+1}\,\&\,j\geqslant\alpha p^i} F_j^{p^i}$$

с точностью до ненулевого множителя из k.

Пусть $B_i\setminus B_{i+1}=\{\alpha_1p^i,\dots,\alpha_rp^i\}$, где $\alpha_1,\dots,\alpha_r$ – целые числа, $1\leqslant\alpha_1<\alpha_2<\dots<\alpha_r\leqslant d/p^i$. Тогда для всякого s, $1\leqslant s<r$, частное

$$Q_s=(G_{i,\alpha_s}/G_{i,\alpha_s-1})/(G_{i,\alpha_{s+1}}/G_{i,\alpha_{s+1}-1})$$

совпадает с $F^{p^i}_{\alpha_sp^i}$ с точностью до ненулевого множителя из k. Частное $G_{i,\alpha_r}/G_{i,\alpha_r-1}$ совпадает с $F^{p^i}_{\alpha_rp^i}$ с точностью до ненулевого множителя из k.

Применяя нётерову нормализацию и лемму 2 (ср. с вычислением G_i), мы находим для всякого s, $1\leqslant s\leqslant r-1$, многочлен $\widetilde{F}_{\alpha_sp^i}$, совпадающий с Q_s с точностью до ненулевого множителя из k. Следовательно, $\widetilde{F}_{\alpha_sp^i}$ совпадает с $F^{p^i}_{\alpha_sp^i}$ с точностью до ненулевого множителя из k. Аналогично мы вычисляем многочлен $\widetilde{F}_{\alpha_rp^i}$, совпадающий с $F^{p^i}_{\alpha_rp^i}$ с точностью до ненулевого множителя из k.

Таким образом, для всякого $j\in B_i\setminus B_{i+1}$ многочлен $\widetilde{F}_j(X_1^{p^{-i}},\dots,X_n^{p^{-i}})\in k[X_1,\dots,X_n]$ совпадает с $F_j^{p^i}(X_1^{p^{-i}},\dots,X_n^{p^{-i}})$ с точностью до ненулевого множителя из k. В частности, мы доказали, что можно выбрать каждый многочлен F_j так, чтобы F_j^j имел коэффициенты из k.

Пусть $1\leqslant j\leqslant d$. Если $\mathrm{char}(k)=0$, то положим

$$\mathrm{SQF}_{j,X_1,\dots,X_n}(f)=\widetilde{F}_j.$$

Если $\mathrm{char}(k)=p>0$, то положим

$$\mathrm{SQF}_{j,X_1,\dots,X_n}(f)=\widetilde{F}_j(X_1^{p^{-i}},\dots,X_n^{p^{-i}})$$

в том и только в том случае, если $j \in B_i \setminus B_{i+1}$, $0 \leqslant i \leqslant \log_p d$. Пусть $k = \overline{k}$. Тогда мы определяем функцию

$$\begin{aligned} &\mathrm{SQF}_{X_1,\dots,X_n} : \bigcup_{d\geqslant 1} P_{n,d} \to \bigcup_{d\geqslant 1}\Big(\bigcup_{m\geqslant 1} P_{n,m}\Big)^d, \\ &f \mapsto \{\mathrm{SQF}_{j,X_1,\dots,X_n}(f)\}_{1\leqslant j\leqslant d}. \end{aligned}$$

Согласно описанной конструкции, функция $\mathrm{SQF}_{X_1,\dots,X_n}$ является алгоритмом, соответствующим лесу вычислений. Обозначим этот лес через $\{T'_d\}_{d\geqslant 1}$ (число n сейчас фиксировано).

§3. Факторизация на абсолютно неприводимые множители

Пусть $F \in k[X_1,\dots,X_n]$ – многочлен, $\deg_{X_1,\dots,X_n} F = d \geqslant 2$. В этом разделе мы будем предполагать, что F сепарабелен, т.е. $\deg F_i = 0$ при $2 \leqslant i \leqslant d$ в (11), см. раздел 2. Обозначим через $P_{\mathrm{spr},n,d}$ множество всех сепарабельных многочленов из $\overline{k}[X_1,\dots,X_n]$ степени d.

Пусть $u_2,\dots,u_n,w_2,\dots,w_n$ – алгебраически независимые над полем k элементы. Для краткости обозначим через $k[u,w]$ кольцо $k[u_2,\dots,u_n,w_2,\dots,w_n]$ и через $k_{u,w}$ поле частных кольца $k[u,w]$. Если $a \in k[u,w]$, то положим $\deg_{u,w} a = \deg_{u_2,\dots,u_n,w_2,\dots,w_n} a$.

Положим $F_{u,w} = F(X_1, u_2X_1 + w_2,\dots,u_nX_1 + w_n)$. По теореме Безу многочлен $F_{u,w} \in k_{u,w}[X_1]$ имеет d попарно различных корней в алгебраическом замыкании $\overline{k_{u,w}}$ поля $k_{u,w}$. Поэтому дискриминант многочлена $F_{u,w}$ относительно X_1 не равен нулю:

$$\Delta = \mathrm{Res}_{X_1}\left(F_{u,w}, \frac{\partial F_{u,w}}{\partial X_1}\right) \neq 0.$$

Заметим, что $\Delta \in k[u,w]$ и $\deg_{u,w}\Delta \leqslant (2d-1)d$. Выберем и зафиксируем множество $\mathcal{J}_{2d^2} \subset K_0$ (напомним, что обозначения $\mathcal{J}_d$ и $\mathcal{J}_{n,d}$ введены в разделе 1). Как в разделе 1, мы будем предполагать, что множество $\mathcal{J}_{2d^2}$ является вполне упорядоченным и $\mathcal{J}_{2n-1,2d^2}$ упорядочено лексикографически.

Положим

$$\begin{aligned} &\mathrm{NND}_{X_1}(F; X_1,\dots,X_n) = F(X_1, X_2+\alpha_2X_1+\beta_2,\dots,X_n+\alpha_nX_1+\beta_n), \\ &\mathrm{innd}_{X_1}(F; X_1,\dots,X_n) = (\alpha_2,\dots,\alpha_n,\beta_2,\dots,\beta_n), \end{aligned} \tag{12}$$

где $(\alpha_2,\dots,\alpha_n,\beta_2,\dots,\beta_n)\in\mathcal{J}_{2n-1,2d^2}$ – наименьший мультииндекс, такой, что $\Delta(\alpha_2,\dots,\alpha_n,\beta_2,\dots,\beta_n)\neq 0$ и $\Phi_d(1,\alpha_2,\dots,\alpha_n)\neq 0$, где Φ_d – форма степени d, такая, что $\deg_{X_1,\dots,X_n}(F-\Phi_d)<d$.

Пусть $f=\mathrm{NND}_{X_1}(F;X_1,\dots,X_n)$. Тогда, очевидно, имеем

$$\deg_{X_1} f(X_1,0,\quad\dots,0)=d$$

и многочлен $f(X_1,0,\dots,0)\in k[X_1]$ является сепарабельным, т.е. имеет d попарно различных корней в $\overline{k}$. Положим $c=\mathrm{LC}_{X_1}f=\mathrm{lc}_{X_1}f(X_1,0)$, так что c – старший коэффициент многочлена f относительно X_1.

Если $k=\overline{k}$, то функция

$$\bigcup_{d\geqslant 2}P_{\mathrm{spr},n,d}\to\bigcup_{d\geqslant 0}P_{\mathrm{spr},n,d},\quad F\mapsto\mathrm{NND}_{X_1}(F;X_1,\dots,X_n),$$

является алгоритмом, соответствующим лесу вычислений. Обозначим этот лес через $\{T''_d\}_{d\geqslant 0}$.

Теперь мы собираемся применить результаты работы [2]. Пусть $v_3,\dots,v_n$ – алгебраически независимые над полем k элементы. Для краткости обозначим через $k[v]$ кольцо $k[v_3,\dots,v_n]$ и через k_v поле частных кольца $k[v]$ (в дальнейшем мы будем использовать аналогичные обозначения). Если $a\in k[v]$, то $\deg_v a=\deg_{v_3,\dots,v_n}a$.

Положим $X=X_1$, $T=X_2$, $f_v=f(X,T,v_3T,\dots,v_nT)\in k[v][X,T]$. Положим $\rho=\deg_T f_v$.

Положим $f_0=f(X,0,\dots,0)$. Представим многочлен f_0 в виде $f_0=f_0(Z)+(X-Z)g_0$, где $g_0\in k[Z,X]$. Заметим, что $g_0(Z,Z)=f_0'(Z)=\frac{d\,f_0}{dZ}$. Определим $\delta=f_0'(Z)$.

Пусть $f_v=\sum\limits_{i\geqslant 0}f_{v,i}T^i$, где $f_{v,i}\in k[v][X]$ (следовательно, если $i>\rho$, то $f_{v,i}=0$). Положим $\overline{f}_{v,i}=\delta^{2i-2}f_{v,i}$ при $i\geqslant 1$. Положим $\overline{z}_0=Z$.

Для всех $i\geqslant 1$ определим рекурсивно многочлены $\overline{g}_{i,j}\in k_v[Z]$, где $0\leqslant j\leqslant m-2$, и $\overline{z}_i\in k_v[Z]$. Положим $\overline{g}_i=\sum\limits_{0\leqslant j\leqslant m-2}\overline{g}_{i,j}X^j\in k_v[Z,X]$.

Пусть $\overline{g}_j$ и $\overline{z}_j$ определены для всех j из интервала $0\leqslant j<i$ для некоторого $i\geqslant 1$. Тогда

$$(X-Z)\overline{g}_i-g_0\overline{z}_i=\delta\Big(\overline{f}_{v,i}+\sum_{1\leqslant w\leqslant i-1}\overline{g}_w\overline{z}_{i-w}\Big).\tag{13}$$

Теперь, чтобы найти многочлены $\overline{g}_{i,j}\in k(Z)$, $0\leqslant j\leqslant m-2$, и $-\overline{z}_i\in k(Z)$, следует решить линейную систему с коэффициентами из

$k(Z)$ по правилу Крамера. Она соответствует формуле (13). Матрица коэффициентов этой линейной системы является матрицей Сильвестра многочленов $X-Z$ и g_0. Её определитель равен $\pm\delta$. Все свободные члены этой системы делятся на δ. Поэтому фактически $\overline{g}_{i,j} \in k[v][Z]$ и $\overline{z}_i \in k[v][Z]$ для всех i, j. Рекурсивный шаг для определения $\overline{g}_i$ и $\overline{z}_i$ описан.

Рассмотрим сепарабельную k-алгебру $k' = k[Z]/(f_0(Z))$. Положим $z = Z \bmod f_0(Z) \in k'$. Аналогично определяется сепарабельная k_v-алгебра $k'_v = k_v[Z]/(f_0(Z))$. Имеем $k'_u \supset k'$.

Тогда $f_0 = (X-z)g_0(z,X)$, где $g_0(z,X) \in k'_v[X]$. Заметим, что $\delta(z) = g_0(z,z)$ является обратимым элементом в k', поскольку многочлен f_0 сепарабелен. Пусть $k'_v[[T]]$ – кольцо формальных степенных рядов от T над алгеброй k'_v. Можно применить подъём по лемме Гензеля к разложению $f(X,0) = (X-z)g_0(z,X)$ и получить

$$f = \Big(X - \sum_{i\geqslant 0} z_i\, T^i\Big)\Big(g_0(z,X) + \sum_{i\geqslant 1} g_i\, T^i\Big) \tag{14}$$

в кольце $k'_v[[T]][X]$. Здесь $z_0 = z$, все z_i лежат в k'_v, многочлены g_i лежат в $k'_v[X]$, $\deg_X g_i \leqslant m-2$ для всех $i \geqslant 1$.

Для всех $i \geqslant 1$

$$z_i = \frac{\overline{z}_i(z)}{\delta(z)^{2i-1}}, \quad g_i = \frac{\overline{g}_i(z,X)}{\delta(z)^{2i-1}}. \tag{15}$$

Это следует из леммы 4 работы [2].

Положим $D = (2d-1)\rho + 1$ и

$$\begin{aligned}\eta &= \delta^{2D-3}X - \delta^{2D-3}\Big(Z + \sum_{1\leqslant i\leqslant D-1} \frac{\overline{z}_i\, T^i}{\delta^{2i-1}}\Big) \\ &= \delta^{2D-3}X - \Big(\delta^{2D-3}Z + \sum_{1\leqslant i\leqslant D-1} \overline{z}_i \delta^{2(D-1-i)} T^i\Big) \in K[\,Z,X,T].\end{aligned} \tag{16}$$

Пусть $x \in \overline{k}$. Будем рассматривать x как параметр. Если $f(x,0) \neq 0$, то по определению выходом описываемой конструкции будет $(\varnothing,1,1,1,1,1)$, подробности см. ниже в разделе 5. В дальнейшем, если не оговорено противное, мы будем предполагать, что $f(x,0) = 0$. Следовательно, каждый элемент из $k[x]$ может быть представлен в виде $\sum\limits_{0\leqslant i<d} a_i x^i$, где $a_i \in k$. Всё же при алгебраических операциях $\times, +, -$ с элементами из $k[x]$ мы не будем использовать соотношение $f(x,0) = 0$,

если не оговорено противное. Поэтому мы будем представлять элементы из $k[x]$ в виде $\sum\limits_{0\leqslant i\leqslant N} a_i x^i$, где $a_i \in k$ и N произвольное, т.е. в этих вычислениях x аналогичен трансцендентному элементу над k (конечно, такое представление с произвольным N не единственно, но оно появляется естественным образом из контекста).

Положим

$$\begin{aligned} a_i &= \eta(x, X, T)X^{i-1}, && 1 \leqslant i \leqslant d-1, \\ a_i &= T^D X^{i-m}, && d \leqslant i \leqslant 2d-1. \end{aligned} \tag{17}$$

Положим $B_1 = \overline{k_v}[T]$. Мы будем отождествлять множество многочленов $g \in \overline{k_v}[X, T]$, таких, что $\deg_X g < d$, с B_1^d. При этом отождествлении

$$g = g_0 + g_1 X + \cdots + g_{d-1} X^{d-1} \mapsto (g_0, g_1, \ldots, g_{d-1}); \tag{18}$$

здесь $g_i \in B_1$ для всех i.

Следовательно, при отождествлении (18) все a_i лежат в B_1^d.

Положим $n_1 = d, n_2 = 2d-1$. Пусть A является $(n_1 \times n_2)$-матрицей со строками $a_1, \ldots, a_{2m-1}$. Следовательно, элементы матрицы A принадлежат B_1. Обозначим через M решётку в B_1^d, порождённую строками матрицы A.

Пусть $g = (g_0, \ldots, g_{d-1}) \in M$. Положим

$$|g| = \sup\{\deg_T g_i \,:\, 0 \leqslant i \leqslant d-1\}$$

и $\deg_X g = \sup(\{i \,:\, g_i \neq 0 \,\&\, 0 \leqslant i \leqslant d-1\} \cup \{-1\})$.

Для любых двух элементов $g, h \in M$ положим $g < h$ в том и только в том случае, если $|g| < |h|$ или $|g| = |h|$, но $\deg_X g < \deg_X h$. Минимальный элемент из M – это произвольный ненулевой элемент $q \in M$, такой, что для всякого ненулевого элемента $g \in M$ не верно, что $g < q$, т.е. либо $q < g$, либо $|q| = |g|$ и $\deg_X q = \deg_X g$.

Лемма 3. *Предположим, что $f(x, 0) = 0$ и q – минимальный элемент из M. Тогда q является неприводимым множителем многочлена f_v в кольце $\overline{k_v}[X, T]$, таким, что $X - x$ делит $q(X, 0)$ в кольце $\overline{k_v}[X]$. Далее, $\mathrm{lc}_X q \in \overline{k_v}$, поскольку $\mathrm{lc}_X f_v \in k$. Поэтому тогда $q/\mathrm{lc}_X q \in \overline{k_v}[X, T]$.*

Доказательство. Это следует из доказательства леммы 6 работы [1] (мы оставляем подробности читателю). □

Пусть $q^{(1)} \in M$ – произвольный ненулевой элемент, такой, что $|q^{(1)}| \leqslant D$. По лемме 1 работы [1] можно представить $q^{(1)}$ в виде

$$q^{(1)} = \sum_{1 \leqslant i \leqslant 2d-1} \lambda_i a_i, \tag{19}$$

где $\lambda_i \in \overline{k_v}[T]$ и $\deg_T \lambda_i \leqslant (2d+1)D$ при $1 \leqslant i \leqslant 2d-1$. Следовательно, $\lambda_i = \sum\limits_{0 \leqslant j \leqslant (2d+1)D} \lambda_{i,j} T^j$, где $\lambda_{i,j} \in \overline{k_v}$.

Для целого числа α, $0 \leqslant \alpha \leqslant D$, обозначим через $\mathcal{E}_\alpha$ следующее утверждение. Существует ненулевой элемент $q^{(1)} \in M$ с $|q| \leqslant \alpha$. Тогда однородная линейная система $\mathcal{S}_\alpha$ над полем $k_v[x]$ соответствует $\mathcal{E}_\alpha$ и удовлетворяет следующим свойствам. Это система относительно неизвестных $\lambda_{i,j}$, $1 \leqslant i \leqslant 2d-1$, $0 \leqslant j \leqslant (2d+1)D$. Система $\mathcal{S}_\alpha$ имеет матрицу коэффициентов с элементами из $k[x][v]$. Эта система имеет ненулевое решение тогда и только тогда, когда справедливо утверждение $\mathcal{E}_\alpha$. Фактически, ненулевое решение системы $\mathcal{S}_\alpha$ определяет элемент $q^{(1)}$, такой, что $|q^{(1)}| \leqslant \alpha$, согласно (19). Можно легко построить систему $\mathcal{S}_\alpha$ (мы оставляем подробности читателю).

Для целых чисел α_1, α_2, где $0 \leqslant \alpha_1 \leqslant D, 0 \leqslant \alpha_2 \leqslant d$, обозначим через $\mathcal{E}_{\alpha_1,\alpha_2}$ следующее утверждение. Существует такой ненулевой элемент $q^{(1)} \in M$, что $|q^{(1)}| \leqslant \alpha_1$ и $\deg_X q^{(1)} \leqslant \alpha_2$. Тогда однородная линейная система $\mathcal{S}_{\alpha_1,\alpha_2}$ над полем $k_v[x]$ соответствует $\mathcal{E}_{\alpha_1,\alpha_2}$ и удовлетворяет следующим свойствам. Это система относительно неизвестных $\lambda_{i,j}$, $1 \leqslant i \leqslant 2d-1$, $0 \leqslant j \leqslant (2d+1)D$. Система $\mathcal{S}_{\alpha_1,\alpha_2}$ имеет матрицу коэффициентов с элементами из $k[x][v]$. Эта система имеет ненулевое решение тогда и только тогда, когда выполняется утверждение $\mathcal{E}_{\alpha_1,\alpha_2}$. Фактически, ненулевое решение системы $\mathcal{S}_{\alpha_1,\alpha_2}$ определяет элемент $q^{(1)}$, такой, что $|q^{(1)}| \leqslant \alpha_1$ и $\deg_X q^{(1)} \leqslant \alpha_2$, согласно (19). Можно легко построить систему $\mathcal{S}_{\alpha_1,\alpha_2}$ (мы оставляем подробности читателю).

Пусть $0 \leqslant \alpha_1 \leqslant D$, $1 \leqslant \alpha_2 \leqslant d$. Теперь элемент q с $|q| = \alpha_1$, $\deg_X q = \alpha_2$ является минимальным в том и только в том случае, если выполняются следующие условия:

(a) система $\mathcal{S}_{\alpha_1,\alpha_2}$ имеет ненулевое решение,
(b) если $\alpha_1 \geqslant 1$, то система $\mathcal{S}_{\alpha_1-1}$ имеет только нулевое решение,
(c) система $\mathcal{S}_{\alpha_1,\alpha_2-1}$ имеет только нулевое решение.

В этом случае ненулевое решение системы $\mathcal{S}_{\alpha_1,\alpha_2}$ определяет элемент q согласно (19) (с q вместо $q^{(1)}$). Следовательно, существует минимальный элемент $q \in M$, такой, что $q \in k[x][v][X,T]$.

Неприводимый над $\overline{k_v}$ множитель q многочлена f однозначно определён с точностью до множителя из $\overline{k_v}$. Поэтому если выполняются условия (a), (b) и (c), то система $\mathcal{S}_{\alpha_1,\alpha_2}$ имеет только одно линейно независимое над $k_v[x]$ решение.

Число неизвестных однородных линейных систем из (a), (b) и (c) равно $r' = (2d-1)((2d+1)D+1)$. Обозначим через S_{α_1,α_2}, S_{α_1-1} (если $\alpha_1 \geqslant 1$), S_{α_1,α_2-1} матрицы однородных линейных систем из (a), (b) и (c) соответственно.

Условие (a) выполняется в том и только в том случае, если все миноры порядка r' матрицы S_{α_1,α_2} равны 0.

Условие (b) выполняется в том и только в том случае, если $\alpha_1 = 0$ или не все миноры порядка r' матрицы S_{α_1-1} равны 0.

Условие (c) выполняется в том и только в том случае, если не все миноры порядка r' матрицы S_{α_1,α_2-1} равны 0.

Обозначим $\Delta_1, \ldots, \Delta_{m_1}$ все миноры порядка r' матрицы S_{α_1,α_2}. Обозначим $\Delta_{m_1+1}, \ldots, \Delta_{m_2}$ все миноры порядка r' матрицы S_{α_1-1} (если $\alpha_1 = 0$, то $m_1 = m_2$). Обозначим $\Delta_{m_2+1}, \ldots, \Delta_{m_3}$ все миноры порядка r' матрицы S_{α_1,α_2-1}.

Пусть символы $\wedge$, $\vee$ обозначают логическую конъюнкцию и дизъюнкцию. Теперь конъюнкция (a) $\wedge$ (b) $\wedge$ (c) эквивалентна условию

$$\begin{aligned}&(\Delta_1 = \cdots = \Delta_{m_1} = 0) \wedge ((\Delta_{m_1+1} \neq 0) \vee \cdots \vee (\Delta_{m_2} \neq 0))\\ &\wedge((\Delta_{m_2+1} \neq 0) \vee \cdots \vee (\Delta_{m_3} \neq 0)).\end{aligned} \tag{20}$$

Применяя результат из [4], можно заменить миноры Δ_i на некоторые их линейные комбинации и считать в дальнейшем без ограничения общности, что $m_3 = d^{O(1)}$.

Обозначим через J_{m_1,m_2,m_3} множество всех пар (i_2, i_3), таких, что $m_1 < i \leqslant m_2$, $m_2 < j \leqslant m_3$. Упорядочим пары J_{m_1,m_2,m_3} лексикографически, т.е. положим $(i', j') < (i, j)$ тогда и только тогда, когда $i' < i$ или $i' = i$, но $j' < j$. Пусть $(i, j) \in J_{m_1,m_2,m_3}$. Обозначим через $\mathcal{E}_{\alpha_1,\alpha_2,i,j}$ следующее условие:

$$(\Delta_1 = \cdots = \Delta_{m_1} = 0) \wedge \bigwedge_{\substack{(i',j') \in J_{m_1,m_2,m_3},\\ (i',j') < (i,j)}} (\Delta_{i'}\Delta_{j'} = 0) \wedge (\Delta_i \Delta_j \neq 0). \tag{21}$$

Тогда условие (20) эквивалентно дизъюнкции $\bigvee_{(i,j) \in J_{m_1,m_2,m_3}} \mathcal{E}_{\alpha_1,\alpha_2,i,j}$.

Кроме того, если выполнено условие (20), то можно выбрать решение системы $\mathcal{S}_{\alpha_1,\alpha_2}$ в виде $\lambda_{i,j} = \Delta'_{i,j}$, где каждое $\Delta'_{i,j}$ равно с точностью до знака некоторому минору порядка $r' - 1$ матрицы S_{α_1,α_2}.

Минимальный элемент q вычисляется по формуле

$$q = \sum_{1\leqslant i\leqslant 2d-1}\ \sum_{0\leqslant j\leqslant (2d+1)D} \Delta'_{i,j} T^j a_i,$$

см. (19).

Заметим, что $\Delta_i \in k[x][v]$, $1 \leqslant i \leqslant m_3$. Более точно, можно представить Δ_i в виде $\Delta_i = \sum\limits_{0\leqslant j\leqslant N} \Delta_{i,j} x^j$, где $\Delta_{i,j} \in k[v]$ и N ограничено сверху величиной $d^{O(1)}$ с абсолютной константой в $O(1)$ (мы предоставляем читателю вычислить такую константу $O(1)$). Положим $\widetilde{\Delta}_i = \sum\limits_{0\leqslant j\leqslant N} \Delta_{i,j} X^j \in k[v][X]$, $1 \leqslant i \leqslant m_3$.

Если все $\tilde{\Delta}_i$, $1 \leqslant i \leqslant m_3$, равны нулю, то положим $\psi^{(1)} = f(X,0)$. Предположим, что не все многочлены $\tilde{\Delta}_i$, $1 \leqslant i \leqslant m_3$, равны нулю. Существует инъективная функция $\varkappa : \{1,2,\dots,m_3+m_3^2\} \to \mathbb{Z}^n$, такая, что если $\varkappa(i) = (j_1,\dots,j_n)$, то все j_α неотрицательны и $j_1+\dots+j_n \leqslant N$, где $N = d^{O(1)}$. Определим

$$\psi^{(1)} = \mathrm{G\,C\,D}_{Y_1,\dots,Y_n,X,v_3,\dots,v_n}\Big(\sum_{1\leqslant i\leqslant m_1} Y_1^{j_1}\dots Y_n^{j_n}\tilde{\Delta}_i, f(X,0)\Big) \in k[v][X],$$

где $(j_1,\dots,j_n) = \varkappa(i)$ для каждого слагаемого $Y_1^{j_1}\dots Y_n^{j_n}\tilde{\Delta}_i$. Далее, положим

$$\psi^{(2)} = \mathrm{G\,C\,D}_{Y_1,\dots,Y_n,X,v_3,\dots,v_n}\Big(\psi^{(1)}, \sum_{\substack{m_1<i_2\leqslant m_2,\\ m_2<i_3\leqslant m_3}} Y_1^{j_1}\dots Y_n^{j_n}\tilde{\Delta}_{i_2}\tilde{\Delta}_{i_3}\Big) \in k[v][X],$$

где $(j_1,\dots,j_n) = \varkappa(i_2+m_3 i_3)$ для каждого слагаемого $Y_1^{j_1}\dots Y_n^{j_n}\tilde{\Delta}_{i_2}\tilde{\Delta}_{i_3}$. Теперь $\psi^{(2)} \neq 0$ и $\psi^{(2)}$ делит $\psi^{(1)}$ в кольце $k[v][X]$. Применяя нётерову нормализацию и лемму 2 (ср. с разделом 2), мы вычисляем многочлен $\psi^{(3)} \in k[v][X]$, совпадающий с $\psi^{(1)}/\psi^{(2)}$ с точностью до ненулевого множителя из k.

Отметим, что $\mathrm{lc}_X \psi^{(3)} \in k[v]$. Далее, $\psi^{(4)} = \psi^{(3)}/\mathrm{lc}_X\psi^{(3)} \in k[X]$, поскольку $\psi^{(4)}$ делит многочлен $f(X,0)$ в кольце $k_v[X]$ и $f(X,0) \in k[X]$. Применяя лемму 2, мы вычисляем многочлен $\psi \in k[X]$, совпадающий с $\psi^{(4)}$ с точностью до ненулевого множителя из k. Мы имеем $\psi(x) = 0$, поскольку иначе условие (20) не выполняется. Следовательно, $\deg_X \psi = \alpha_3 \geqslant 1$ и $\deg_X \psi^{(1)} > \deg_X \psi^{(2)} \geqslant 0$. Мы представляем ψ

в виде $\psi = \sum\limits_{0\leqslant i\leqslant\alpha_3} \psi_i X^i$, где $\psi_i \in k$. Согласно описанной конструкции все ψ_i являются многочленами степени $d^{O(1)}$ от коэффициентов полинома f. Эти многочлены имеют коэффициенты из кольца K_0.

При отождествлении (18) элемент q имеет вид $q = \sum\limits_{0\leqslant i\leqslant\alpha_2} q_i X^i$, где $q_i \in k[x][v][T]$. Заметим, что $q_{\alpha_2} = \mathrm{lc}_X q \in k[x][v]$, поскольку q делит f_v в кольце $k_v[x][X,T]$ и $\mathrm{lc}_X f_v = \mathrm{lc}_X f(X,0) \in k$. Далее, $q/\mathrm{lc}_X q \in k[x][v][X,T]$, поскольку этот многочлен делит f_v в кольце $k_v[x][X,T]$ и $\mathrm{lc}_X f_v \in k$.

Применяя нётерову нормализацию и лемму 2 (здесь мы оставляем подробности читателю), мы вычисляем многочлен q', совпадающий с $q/\mathrm{lc}_X q$ с точностью до ненулевого множителя из $k[x]$. Так что, заменяя q на q', мы будем предполагать в дальнейшем без ограничения общности, что $\mathrm{lc}_X q \in k[x]$.

Согласно описанной конструкции можно представить q в виде

$$q = \sum_{0\leqslant s\leqslant \deg_T q} \sum_{0\leqslant i\leqslant\alpha_2} \sum_{0\leqslant j\leqslant N} q_{s,i,j} X^i x^j T^s,$$

где $q_{s,i,j} \in k[v]$, целое число N ограничено сверху величиной $d^{O(1)}$ и все $q_{i,j,s}$ являются многочленами от коэффициентов из $k[v]$ полинома f_v. Эти многочлены имеют коэффициенты в кольце K_0. Положим $q_{i,j} = \sum\limits_{0\leqslant s\leqslant \deg_T q} q_{s,i,j} T^s$ для всех i,j. Теперь $q_i = \sum\limits_{0\leqslant j\leqslant N} q_{i,j} x^j$ для всех i.

Пусть $q(X,0) = q|_{T=0}$. Тогда $q(X,0) \in k[x][X]$, поскольку $q(X,0)$ делит $f(X,0)$ в кольце $k_v[x][X]$ и $\mathrm{lc}_X q(X,0) \in k[X]$.

Пусть $A = k[Z]/(\psi(Z))$ – сепарабельная алгебра и $z_1 = Z \bmod \psi \in A$. Тогда $1, z_1, \ldots, z_1^{\deg\psi-1}$ – базис алгебры A над k. Положим $\nu_0 = \mathrm{lc}_X\, \psi$. Пусть $N \geqslant \alpha_3$ и все $a_i \in k$, $0 \leqslant i \leqslant N$, произвольные. Заметим, что элемент $\sum\limits_{0\leqslant i\leqslant N} a_i z_1^i$ может быть представлен в виде $\sum\limits_{0\leqslant i<\alpha_3} b_i z_1^i$ с $b_i \in k$ согласно лемме 2. Именно, всякий элемент $\nu_0^{N-\alpha_3+1} b_i$ является полиномом от $\psi_0, \ldots, \psi_{\alpha_3}$ и $a_0, \ldots, a_N$ с коэффициентами из кольца K_0.

Элемент q_{α_2} обратим в $k[x]$ для всякого корня x многочлена ψ, поскольку $\deg_X q(X,0) = \alpha_2$ для всякого корня x многочлена ψ. Мы собираемся найти $q_{\alpha_2}^{-1}$. Положим $\widetilde{q}_{\alpha_2} = \sum\limits_{0\leqslant j\leqslant N} q_{0,\alpha_2,j} z_1^j$, где $q_{0,\alpha_2,j} \in k[x]$.

Тогда $\widetilde{q}_{\alpha_2}$ обратим в A. Пусть $\widetilde{q}_{\alpha_2}^{-1} = \sum\limits_{0\leqslant i<\alpha_3} b_i z_1^i$, где $b_i \in k$. Тогда

$$\left(\sum_{0\leqslant i\leqslant N} q_{0,\alpha_2,j} z_1^j\right)\left(\sum_{0\leqslant i<\alpha_3} b_i z_1^i\right) = 1.$$

Отсюда, применяя лемму 2, мы получаем соотношение

$$\sum_{0\leqslant i<\alpha_3}\sum_{0\leqslant j<\alpha_3} L_{i,j} b_j z_1^i = \nu_0^{N+1},$$

где все $L_{i,j}$ являются многочленами от $\psi_0,\dots,\psi_{\alpha_3}$, $q_{\alpha_2,0},\dots,q_{\alpha_2,N}$ с коэффициентами из кольца K_0. Следовательно, мы получаем линейную систему для того, чтобы найти $b_0,\dots,b_{\alpha_3-1}$. Мы решаем её по правилу Крамера. Положим $\nu_1 = \det(\{L_{i,j}\}_{0\leqslant i,j<\alpha_3})$. Таким образом, можно записать

$$q_{\alpha_2}^{-1} = \sum_{0\leqslant i<\alpha_3} a_i \nu_0^{N+1} x^i/\nu_1, \tag{22}$$

где все a_i, ν_1 являются многочленами от $\psi_0,\dots,\psi_{\alpha_3}$, $q_{\alpha_2,0},\dots,q_{\alpha_2,N}$ с коэффициентами из кольца K_0.

Положим $q'' = (\nu_1/q_{\alpha_2})q$. Пусть

$$q'' = \sum_{0\leqslant s\leqslant \deg_T q''}\sum_{0\leqslant i\leqslant\alpha_2}\sum_{0\leqslant j<\alpha_3} q''_{s,i,j} X^i x^j T^s,$$

где $q''_{s,i,j} \in k$. Тогда, согласно (22) и лемме 2, старший коэффициент $\mathrm{lc}_X q''$ лежит в k и все $q_{s,i,j}$ являются многочленами от $\psi_0,\dots,\psi_{\alpha_3}$, $q_{i,0},\dots,q_{i,N}$ с коэффициентами из кольца K_0. Можно вычислить все $q''_{i,j}$ при помощи (22) и леммы 2. Теперь, заменяя $(N, q, \{q_{s,i,j}\}_{\forall i,j})$ на $(\alpha_3-1, q'', \{q''_{s,i,j}\}_{\forall i,j})$, мы будем предполагать в дальнейшем без ограничения общности, что $\mathrm{lc}_X q \in k$ и $N = \alpha_3 - 1$.

§4. Завершение конструкции разложения многочленов на абсолютно неприводимые множители.

В этом разделе мы построим примитивные элементы полей, порождённых коэффициентами абсолютно неприводимых множителей многочлена f. Здесь, как и в предыдущем разделе, требуется подробное описание для того, чтобы получить алгоритм, соответствующий лесу вычислений, в следующем разделе.

Пусть $q(X,0) = \sum\limits_{0\leqslant i\leqslant\alpha_2} Q_{0,i}X^i$, где $Q_{0,i}\in k[x]$. Тогда $Q_{0,\alpha_2} = q_{\alpha_2}\in k$. Далее, для всякого i из интервала $0\leqslant i<\alpha_3$ вычисляется представление $Q_{0,i} = \sum\limits_{0\leqslant j<\alpha_3} q_{0,i,j}x^j$, где $q_{0,i,j}\in k$. Пусть Y – новая переменная. Положим

$$\theta_i = \sum_{0\leqslant j<\alpha_3} q_{0,i,j}z_1^j \in A, \quad 0\leqslant i\leqslant\alpha_2,$$
$$\theta = \sum_{0\leqslant i\leqslant\alpha_2} \theta_i Y^i \in A[Y].$$

Тогда для всякого корня x многочлена ψ имеем $\theta_i|_{z_1=x} = q_{0,i}$ при $0\leqslant i\leqslant\alpha_2$, и $\theta|_{z_1=x} = \sum\limits_{0\leqslant i\leqslant\alpha_2} Q_{0,i}Y^i = q(Y,0)$.

Для целых чисел α_3, α_4, где $0\leqslant\alpha_4\leqslant\alpha_3$, обозначим через $\mathcal{E}'_\delta$ следующее утверждение. Элементы $1,\theta,\dots,\theta^{\alpha_4}\in A\otimes_k k(Y)$ линейно независимы над полем $k(Y)$. Запишем $\nu_0^{(\alpha_3-1)^2+1}\theta^i = \sum\limits_{0\leqslant j<\alpha_3}\theta_{i,j}z_1^j$, где все $\theta_{i,j}$ лежат в $k[Y]$ и по лемме 2 являются полиномами от Y, $\psi_0,\dots,\psi_{\alpha_3}$ и всех $q_{0,i,j}$ с коэффициентами из K_0. Обозначим через $\mathcal{S}'_{\alpha_4}$ следующую однородную систему над полем $k(Y)$ относительно неизвестных Z_i, $0\leqslant i\leqslant\alpha_4$:

$$\sum_{0\leqslant i\leqslant\alpha_4} Z_i\theta_{i,j} = 0, \quad 0\leqslant j<\alpha_3. \tag{23}$$

Тогда условие $\mathcal{E}'_{\alpha_4}$ выполняется в том и только в том случае, если система $\mathcal{S}'_{\alpha_4}$ имеет ненулевое решение. Обозначим через S'_{α_4} матрицу однородной системы $\mathcal{S}'_{\alpha_4}$; ее элементы лежат в $k[Y]$.

Обозначим через $H\in k(Y)[Z]$ минимальный многочлен элемента $\theta\in A\otimes_k k(Y)$ над $k(Y)$, такой, что $H\in k[Y,Z]$. Пусть $\deg_Z H = \alpha_4$ и, следовательно, $H = \sum\limits_{0\leqslant i\leqslant\alpha_4} H_iZ^i\in k[Y,Z]$, где $H_i\in k[Y]$. Поэтому $H(Y,\theta)=0$.

Степень $\deg_Z H$ равна α_4 тогда и только тогда, когда выполняются следующие два условия:

(c) однородная линейная система $\mathcal{S}'_{\alpha_4}$ имеет ненулевое решение,
(d) однородная линейная система $\mathcal{S}'_{\alpha_4-1}$ имеет только нулевое решение.

Если выполнены условия (c) и (d), то любое ненулевое решение из $k[Y]^{\alpha_4+1}$ системы $\mathcal{S}'_{\alpha_4}$ задаёт коэффициенты $(H_0,\dots,H_{\alpha_4})$ минимального многочлена H (такой многочлен однозначно определён с точностью до ненулевого множителя из $k[Y]$).

Условие (c) выполняется тогда и только тогда, когда все миноры порядка α_4+1 матрицы S'_{α_4} равны 0. Условие (d) выполняется тогда и только тогда, когда не все миноры порядка α_4 матрицы S'_{α_4-1} равны 0.

Обозначим через $\Delta_{m_3+1},\dots,\Delta_{m_4}$ все миноры порядка α_4+1 матрицы S'_{α_4}. Обозначим через $\Delta_{m_4+1},\dots,\Delta_{m_5}$ все миноры порядка α_4 матрицы S'_{α_4-1}. Заметим, что $\Delta_i\in k[Y]$ для всех i, $m_3<i\leqslant m_5$.

Теперь конъюнкция (c) $\wedge$ (d) эквивалентна условию

$$(\Delta_{m_3+1}=\dots=\Delta_{m_4}=0)\wedge((\Delta_{m_4+1}\neq 0)\vee\dots\vee(\Delta_{m_5}\neq 0)). \qquad (24)$$

Кроме того, если выполнено условие (24), то можно выбрать решение системы $\mathcal{S}'_{\alpha_4}$ в виде $Z_i=\Delta'_i$, где каждое Δ'_i равно с точностью до знака некоторому минору порядка α_4-1 матрицы S'_{α_4} и Δ'_{α_4} является ненулевым минором матрицы S'_{α_4-1}. Миноры Δ'_i, $0\leqslant i\leqslant\alpha_4$, выбираются из одних и тех же строк с индексами $0\leqslant i_0<\dots<i_{\alpha_4-1}<\alpha_3$ матрицы S'_{α_4}.

Положим $H_i=\Delta'_i$, $0\leqslant i\leqslant\alpha_4$, $\nu_2=\Delta'_{\alpha_4}$. Заметим, что выполнено неравенство $\deg_Y\Delta'_{\alpha_4}<\alpha_2\alpha_4\leqslant d^2$.

Для всякого корня x многочлена ψ элемент $q(Y,0)$ является целым над $k[Y]$. Поэтому существует минимальный многочлен $\widetilde{H}_x\in k(Y)[Z]$ элемента $q(Y,0)$ над полем $k(Y)$, такой, что $\widetilde{H}_x\in k[Y,Z]$ и $\mathrm{lc}_Z\widetilde{H}_x\in k$. Отметим, что каждый полином $\widetilde{H}_x$ сепарабелен относительно Z.

Обозначим через $\widetilde{H}$ произведение всех попарно различных многочленов $\widetilde{H}_x$, где x пробегает множество всех корней многочлена ψ; т.е. $\widetilde{H}$ является бесквадратной частью многочлена $\prod\limits_{\{x\,:\,\psi(x)=0\}}\widetilde{H}_x$. Тогда многочлен $\widetilde{H}$ совпадает с H/H_{α_4} с точностью до ненулевого множителя из k. Поэтому $H/H_{\alpha_4}\in k[Y,Z]$. Применяя лемму 2, мы вычисляем многочлен $H'\in k[Y,Z]$, такой, что H/H_{α_4} и H' совпадают с точностью до ненулевого множителя из k. Заменяя H на H', мы будем предполагать в дальнейшем без ограничения общности, что $\mathrm{lc}_Z H\in k$.

Далее, для всякого корня x многочлена ψ поле $k(Y)[q_{0,0},\dots,q_{0,\alpha_2}]$ имеет примитивный элемент $q(Y,0)$. Следовательно, по китайской теореме об остатках сепарабельная алгебра $k(Y)[\theta_0,\dots,\theta_{\alpha_2}]$ (это подалгебра в $A\otimes_k k(Y)$) имеет примитивный элемент θ. Поэтому существует

единственное представление

$$\theta_i = \sum_{0\leqslant j<\alpha_4} c_{i,j}\theta^j, \quad 0 \leqslant i \leqslant \alpha_2,$$

где $c_{i,j} \in k(Y)$.

Для того чтобы найти коэффициенты $c_{i,j}$, заметим, что

$$\theta_i = \sum_{0\leqslant j<\alpha_4} c_{i,j}\theta^j = \sum_{0\leqslant s<\alpha_3}\sum_{0\leqslant j<\alpha_4} c_{i,j}\theta_{j,s}z_1^s\nu_0^{-(\alpha_3-1)^2-1}$$

и $\theta_i = \sum\limits_{0\leqslant s<\alpha_3} q_{0,i,s}z_1^s$. Поэтому $\sum\limits_{0\leqslant j<\alpha_4} c_{i,j}\theta_{j,s} = q_{0,i,s}\nu_0^{(\alpha_3-1)^2+1}$ для всех i, s.

Теперь рассмотрим линейную систему

$$\sum_{0\leqslant j<\alpha_4} Z_j\theta_{j,s} = q_{0,i,s}\nu_0^{(\alpha_3-1)^2+1}, \quad s = i_0, \ldots, i_{\alpha_4-1}, \tag{25}$$

для всякого i, $0 \leqslant i < \alpha_2$. Тогда $Z_j = c_{i,j}$, $0 \leqslant j < \alpha_4$, является единственным решением системы (25). Оно может быть найдено при помощи правила Крамера. Следовательно, можно записать $c_{i,j} = a_{i,j}/\nu_2$, где $a_{i,j} \in k[Y]$, и вычислить все $a_{i,j}$.

Перебирая элементы из множества $\mathcal{J}_{d^2-1}$, мы находим такой элемент $y^* \in \mathcal{J}_{d^2-1}$, что $\nu_2(y^*) \neq 0$. Положим $\xi = \theta|_{Y=y^*}$.

Покажем, что ξ является примитивным элементом сепарабельной алгебры $k[\theta_0, \ldots, \theta_{\alpha_2}]$ (это подалгебра в A) над полем k. Действительно, элементы $1, \xi, \ldots, \xi^{\alpha_4-1}$ линейно независимы над k, поскольку $\nu_2(y^*) \neq 0$. Многочлен $H(y^*, Z)$ является минимальным полиномом элемента ξ, поскольку $H(y^*, \xi) = 0$, $0 \neq \mathrm{lc}_Z H \in k$ и $\deg_Z H(y^*, Z) = \alpha_4$. Наконец, $\theta_i = \sum\limits_{0\leqslant j<\alpha_4} \theta^*_{i,j}\cdot\xi^j$, где $\theta^*_{i,j} = a_{i,j}(y^*)/\nu_2(y^*)$ для всех i, j. Требуемое утверждение доказано.

Каждый элемент из $k[\xi]$ может быть представлен в виде $\sum\limits_{0\leqslant i<\alpha_4} a_i\xi^i$, где $a_i \in k$. Всё же при алгебраических операциях $\times, +, -$ с элементами из $k[\xi]$ мы не будем использовать соотношение $H(y^*, \xi) = 0$, если не оговорено противное. Поэтому мы будем представлять элементы из $k[\xi]$ в виде $\sum\limits_{0\leqslant i\leqslant N} a_i\xi^i$, где $a_i \in k$ и N произвольное, т.е. в этих вычислениях ξ аналогичен трансцендентному элементу над k (конечно, такое представление с произвольным N не единственно, но оно появляется естественным образом из контекста).

Положим $Q_0 = q(X,0)\nu_2(y^*)$. Тогда $Q_0 \in k[\xi][X]$ и $\mathrm{lc}_X Q_0 \in k$. Применяя лемму 2, находим многочлен $U_0 \in k[\xi][X]$, такой, что Q_0U_0 совпадает с $f(X,0)$ с точностью до ненулевого множителя из k. Более точно, $Q_0U_0 = \lambda_0 f(X,0)$, где $0 \neq \lambda_0 = (\mathrm{lc}_X Q_0)^{d-\alpha_2+1} \in k$.

Пусть $\lambda_0 f_v = \sum\limits_{i\geqslant 0} \Phi_i T^i$, где $\Phi_i \in k[v][X]$, $\Phi_0 = \lambda_0 f(X,0)$ (здесь имеем $\Phi_i = 0$, если $i \geqslant \deg_T f_v$). Теперь мы собираемся применить лемму Гензеля. Именно, мы построим разложение

$$\Big(Q_0 + \sum_{i\geqslant 1} Q_i T^i\Big)\Big(U_0 + \sum_{j\geqslant 1} U_j T^j\Big) = \Phi_0 + \sum_{i\geqslant 1} \Phi_i T^i, \tag{26}$$

где $Q_i, U_j \in k[\xi][v][X]$. Более точно, пусть $R_0 = \mathrm{Res}_X(Q_0, U_0) \in k$ – результант многочленов Q_0 и U_0. Пусть R_1 (соответственно R_2, R_3) – дискриминант многочлена $\lambda_0 f(X,0)$ (соответственно Q_0, U_0). Следовательно,

$$R_1 = R_2 R_3 R_0^2. \tag{27}$$

Элементы R_0, R_2, R_3 не являются делителями нуля в $k[\xi]$, поскольку $0 \neq R_1 \in k$.

Положим $\overline{Q}_i = R_0^{2i-1} Q_i$, $\overline{U}_j = R_0^{2i-1} U_i$, $\overline{\Phi}_i = R_0^{2i-2}\Phi_i$ при $i, j \geqslant 1$. Мы докажем, что имеют место представления $\overline{Q}_i = \sum\limits_{0\leqslant j\leqslant \alpha_2-1} \overline{Q}_{i,j} X^j$, $\overline{U}_i = \sum\limits_{0\leqslant j\leqslant d-\alpha_2-1} \overline{U}_{i,j} X^j$, где $\overline{Q}_{i,j}, \overline{U}_{i,j} \in k[\xi][v]$.

Предположим, что для некоторого $i \geqslant 1$ элементы $\overline{Q}_j$ и $\overline{U}_j$ уже определены для $0 \leqslant j < i$ и $\overline{Q}_j, \overline{U}_j \in k[\xi][v][X]$. Тогда

$$U_0\overline{Q}_i + Q_0\overline{U}_i = R_0\Big(\overline{\Phi}_i + \sum_{1\leqslant w\leqslant i-1} \overline{Q}_w \overline{U}_{i-w}\Big). \tag{28}$$

Теперь, чтобы найти все $\overline{Q}_{i,j}$, $0 \leqslant j \leqslant \alpha_2 - 1$, и $\overline{U}_{i,j}$, $0 \leqslant j \leqslant d - \alpha_2 - 1$, следует решить линейную систему с коэффициентами из $k[\xi][v]$, соответствующую соотношению (28). Она имеет единственное решение. Его можно получить по правилу Крамера. Матрица коэффициентов этой системы является матрицей Сильвестра многочленов Q_0 и U_0. Её определитель $\pm R_0$ не является делителем нуля в $k[\xi][v]$. Все свободные члены этой системы делятся на R_0. Поэтому $\overline{Q}_{i,j} \in k[\xi][v]$, $\overline{U}_{i,j} \in k[\xi][v]$ для всех i, j, и фактически они являются полиномами от коэффициентов из $k[\xi][v]$ многочленов $Q_0, U_0, \lambda_0 f_v$. Рекурсивный шаг для определения и построения $\overline{Q}_i$ и $\overline{U}_i$ описан.

Напомним, что $\deg_T q = \alpha_1$. Положим $q''' = q\nu_2(y^*)R_1^{\alpha_1} \in k[\xi][v][T,X]$. Теперь из (27) следует, что $q''' \in k[\xi][v][T,X]$. Старший коэффициент $\mathrm{lc}_X q'''$ лежит в k, и согласно описанной конструкции подъёма по лемме Гензеля все коэффициенты из $k[\xi]$ многочлена q''' являются полиномами от коэффициентов из $k[\xi][v]$ многочленов q_0 и $\lambda_0 f_v$. Степени этих полиномов ограничены сверху величиной $d^{O(1)}$ с абсолютной константой в $O(\dots)$.

Мы имеем $q''' = q'''(v_3,\dots,v_n,T,X) \in k[\xi][v_3,\dots,v_n,T,X]$. Положим

$$Q''' = q'''(X_3/X_2,\dots,X_n/X_2,X_2,X_1).$$

Тогда $Q''' \in k[\xi][X_1,\dots,X_n]$ по лемме Гаусса (мы оставляем подробности читателю). Положим

$$Q^{(4)} = Q'''(X_1, X_2 - \alpha_2 X_1 - \beta_2, \dots, X_n - \alpha_n X_1 - \beta_n),$$

см. формулу (12) в начале раздела 3.

Согласно описанной конструкции можно представить $Q^{(4)}$ в виде

$$Q^{(4)} = \sum_{0\leqslant i\leqslant N_1} \sum_{i_1,\dots,i_n} Q^{(4)}_{i,i_1,\dots,i_n} X_1^{i_1}\cdot\dots\cdot X_n^{i_n}\xi^i,$$

где $Q^{(4)}_{i,i_1,\dots,i_n} \in k$ и N_1 является минимально возможным, таким, что $N_1 \geqslant \alpha_4 - 1$. Тогда целое число N_1 ограничено сверху величиной $d^{O(1)}$ с абсолютной константой в $O(\dots)$. Более того, все $Q^{(4)}_{i,i_1,\dots,i_n}$ являются полиномами от коэффициентов многочлена f. Эти полиномы имеют коэффициенты из кольца K_0.

Положим $Q = H_{\alpha_4}^{N_1-\alpha_4+1} Q^{(4)}$. Тогда по лемме 2 можно найти представление

$$Q = \sum_{0\leqslant i<\alpha_4} \sum_{i_1,\dots,i_n} Q_{i,i_1,\dots,i_n} X_1^{i_1},\dots,X_n^{i_n}\xi^i,$$

где $Q_{i,i_1,\dots,i_n} \in k$. Более того, все $Q_{i,i_1,\dots,i_n}$ являются полиномами от коэффициентов многочлена f. Эти полиномы имеют коэффициенты из кольца K_0.

Положим

$$\varepsilon = q_{\alpha_2}\nu_2(y^*)R_1^{\alpha_1} H_{\alpha_4}^{N_1-\alpha_4+1}. \tag{29}$$

Тогда $\varepsilon = H_{\alpha_4}^{N_1-\alpha_4+1}\mathrm{lc}_X q'''(X,0)$.

Для всякого корня $Z = \xi^*$ многочлена $H(y^*,Z)$ положим $Q^* = Q|_{\xi=\xi^*}$. Тогда многочлен Q^* неприводим в кольце $\overline{k}[X_1,\dots,X_n]$ и Q^* делит F в кольце $k[\xi^*][X_1,\dots,X_n]$ (здесь мы оставляем подробности

читателю). Так что Q^* является абсолютно неприводимым множителем многочлена F.

§5. Деревья вычислений, покрытия и стратификации

В этом разделе мы получим требуемое разложение многочлена f на абсолютно неприводимые множители.

В дальнейшем мы не будем предполагать, что $f(x,0)=0$. Пусть $k=\overline{k}$. Положим $\widetilde{P}_{n,d}=\bigcup_{-1\leqslant d'\leqslant d}P_{n,d}$, $d\geqslant 0$ (мы считаем, что здесь $\deg_{X_1,\dots,X_n}0=-1$). По определению $\widetilde{P}^0_{n,d}=\{\varnothing\}$ (это одноэлементное множество). Обозначим через P_{2,d_2,d_3} множество всех многочленов Φ из $\overline{k}[Y,Z]$, таких, что $\deg_Z\Phi=d_2$, $\deg_Y\Phi=d_3$.

Конструкция, описанная в предыдущих разделах, задаёт функцию

$$\mathfrak{t}:\bigcup_{d\geqslant 2}(P_{\mathrm{spr},n,d}\times\overline{k})\to\bigcup_{d_1\geqslant 0,\ d_2\geqslant 0,\ d_3\geqslant 0}(\widetilde{P}^{d_2}_{n,d_1}\times P_{2,d_2,d_3}\times\overline{k}^4)$$

по формуле

$$\mathfrak{t}(F,x)=\begin{cases}((Q_0,\dots,Q_{\alpha_4-1}),H(Y,Z),\varepsilon,q_{\alpha_2},c,y^*), & \text{если}\quad f(x,0)=0,\\ (\varnothing,1,1,1,1,1), & \text{если}\quad f(x,0)\neq 0,\end{cases}$$

где $Q=\sum\limits_{0\leqslant i<\alpha_4}Q_i\xi^i$ и $Q_i\in k[X_1,\dots,X_n]$. Напомним, что $c=\mathrm{lc}_X f(X,0)$, $q_{\alpha_2}=\mathrm{lc}_X q(X,0)$, $y^*\in\mathcal{J}_{d^2-1}$ и ε определено в (29), см. разделы 3, 4. Мы оставляем читателю доказательство того, что эта функция является алгоритмом, соответствующим лесу вычислений (это следует непосредственно из конструкции, описанной в предыдущих двух разделах). Обозначим этот лес через $\{T'''_d\}_{d\geqslant 2}$ (мы сейчас предполагаем, что n фиксировано).

Замечание 2. В определении функции $\mathfrak{t}$ можно опустить $\overline{k}^4$. Действительно, предположим, что $((Q_0,\dots,Q_{\alpha_4-1}),\ H(Y,Z))$ вычисляются на выходе, соответствующем листу w дерева вычислений. Это дерево получено из конструкции, описанной в двух предыдущих разделах. Тогда все элементы $\varepsilon,q_{\alpha_2},c,y^*$ также вычислены в некоторых вершинах v_1,v_2,v_3,v_4, которые являются предками вершины w в этом дереве вычислений. Так что мы вводим $\overline{k}^4$ в определении функции $\mathfrak{t}$ только для удобства.

Обозначим через $b_1, \dots, b_\mu, Z$ координатные функции пространства параметров $P_{\mathrm{spr},n,d} \times \overline{k}$. Здесь $\mu = \binom{n+d}{n}$ и Z – координатная функция на $\overline{k}$.

Напомним, что в обозначениях работы [1] условие $\mathcal{A}_w$ соответствует каждой вершине w дерева T_d'''. Для удобства читателя и лучшего понимания здесь мы хотели бы отметить, что, например, для всех возможных α_1, α_2, $(i,j) \in J_{m_1,m_3,m_3}$ существует вершина w дерева T_d''', такая, что $\mathcal{A}_w = \mathcal{E}_{\alpha_1,\alpha_2,i,j}$ (сейчас все Δ_i в (21) являются многочленами с коэффициентами из $k[b_1, \dots, b_\mu]$).

Пусть $L(T_d''')$ – множество листьев дерева T_d'''. В обозначениях работы [1] условие $\overline{\mathcal{A}}_w$ соответствует каждому листу $w \in L(T_d''')$ (не следует путать это w с w из предыдущих разделов). Из конструкции, описанной в разделах 3, 4, следует, что каждое $\overline{\mathcal{A}}_w$ эквивалентно условию

$$(\varphi_{w,1} = \dots = \varphi_{w,\mu_{w,1}} = 0) \wedge ((\varphi_{w,\mu_{w,1}+1} \neq 0) \vee \dots \vee (\varphi_{w,\mu_{w,2}} \neq 0),$$

где существует в точности одно число j_0, $1 \leqslant j_0 \leqslant \mu_{w,2}$, такое, что $\varphi_{w,j_0} \in k[b_1, \dots, b_\mu, Z] \setminus k[b_1, \dots, b_\mu]$. Более того, $j_0 = 1$ или $j_0 = \mu_{w,1}+1$. Все другие многочлены $\varphi_{w,j}$, $1 \leqslant j \leqslant \mu_{w,2}$, $j \neq j_0$, лежат в $k[b_1, \dots, b_\mu]$. Фактически, если $j_0 = 1$, то многочлен φ_{w,j_0} соответствует $\psi(Z)$, и если $j_0 = \mu_{w,1} + 1$, то φ_{w,j_0} соответствует $f(Z, 0)$, см. раздел 3.

Если $j_0 \neq \mu_{w,1} + 1$, то по определению w является листом первого рода, в противном случае w является листом второго рода.

В обозначениях работы [1] имеем квазипроективное алгебраическое многообразие

$$\mathcal{W}_w = \mathcal{Z}(\varphi_{w,1}, \dots, \varphi_{w,\mu_{w,1}}) \setminus \mathcal{Z}(\varphi_{w,\mu_{w,1}+1}, \dots, \varphi_{w,\mu_{w,2}}) \subset P_{\mathrm{spr},n,d} \times \overline{k}.$$

Пусть w – лист первого рода. Тогда по определению имеем квазипроективное алгебраическое многообразие

$$\mathcal{W}_w' = \mathcal{Z}(\varphi_{w,2}, \dots, \varphi_{w,\mu_{w,1}}) \setminus \mathcal{Z}(\varphi_{w,\mu_{w,1}+1}, \dots, \varphi_{w,\mu_{w,2}}) \subset P_{\mathrm{spr},n,d}.$$

Степени всех многочленов $\varphi_{w,j}$ относительно $b_1, \dots, b_\mu, Z$ ограничены сверху величиной $d^{O(1)}$ с абсолютной константой в $O(\dots)$ (читатель может вычислить такую константу). Далее, дерево $L(T_d''')$ имеет уровень $l(T_d''')$, ограниченный сверху величиной $d^{O(1)}$, снова с абсолютной константой в $O(\dots)$.

Выходные данные, соответствующие листу $w \in L(T_d''')$ первого рода, имеют вид $((Q_{w,0},\dots,Q_{w,d_2-1}), H_w, \varepsilon_w, e_w, c_w, y_w)$, где

$$H_w \in k[b_1,\dots,b_\nu][Y,Z], \quad \deg_Y H = d_3 \geqslant 1, \quad \deg_Z H_w = d_2 \geqslant 1,$$
$$Q_{w,i} \in k[b_1,\dots,b_\mu][X_1,\dots,X_n], \quad \max_{0\leqslant i\leqslant d_2-1} \deg_{X_1,\dots,X_n} Q_{w,i} = d_1 \geqslant 1,$$
$$0 \neq \varepsilon_w, e_w, c_w \in k[b_1,\dots,b_\mu], \quad y_w \in k.$$

Имеем $1 \leqslant d_1 \leqslant d$, $1 \leqslant d_2 \leqslant d$, $1 \leqslant d_3 \leqslant d^2$. Степени $\deg_{b_1,\dots,b_\mu} Q_{w,i}$ для всех i, а также $\deg_{b_1,\dots,b_\mu} H_w$, $\deg_{b_1,\dots,b_\mu} e_w$, $\deg_{b_1,\dots,b_\mu} \varepsilon_w$, $\deg_{b_1,\dots,b_\mu} c_w$ ограничены сверху величиной $d^{O(1)}$ с абсолютной константой в $O(\dots)$.

Кроме того, многочлены e_w, c_w, $\mathrm{lc}_Z H_w$ не имеют нулей на $\mathcal{W}_w$ и $\mathcal{W}_w'$, т.е. $\mathcal{W}_w \cap \mathcal{Z}(\varepsilon_w e_w c_w \mathrm{lc}_Z H_w) = \varnothing$ и $\mathcal{W}_w' \cap \mathcal{Z}(\varepsilon_w e_w c_w \mathrm{lc}_Z H_w) = \varnothing$. Это следует из конструкции, описанной в разделах 3, 4.

Выходные данные, соответствующие листу $w \in L(T_d''')$ второго рода, имеют вид $(\varnothing, 1, 1, 1, 1, 1)$.

Положим $\mathcal{P}_{i,d_{i,1},d_{i,2},d_{i,3}} = \widetilde{P}^{d_{i,2}}_{n,d_{i,1}} \times P_{2,d_{i,2},d_{i,3}} \times \overline{k}^4$, $1 \leqslant i \leqslant d$. Теперь рассмотрим функцию

$$\mathfrak{T} : \bigcup_{d\geqslant 2} (P_{\mathrm{spr},n,d} \times \overline{k}^d) \to \bigcup_{d\geqslant 1} \bigcup_{\substack{d_{i,1}\geqslant 0,\, d_{i,2}\geqslant 0,\\ d_{i,3}\geqslant 0\ \forall\, 1\leqslant i\leqslant d}} \prod_{1\leqslant i\leqslant d} \mathcal{P}_{i,d_{i,1},d_{i,2},d_{i,3}},$$

заданную формулой

$$\mathfrak{T}(F,(x_1,\dots,x_d)) = (\mathfrak{t}(F,x_1),\dots,\mathfrak{t}(F,x_d)).$$

Функция $\mathfrak{T}$ является алгоритмом, соответствующим лесу вычислений $\{T_d^{(4)}\}_{d\geqslant 2}$. Для всякого d дерево $T_d^{(4)}$ строится при помощи деревьев T_d''' аналогично конструкции набора из d деревьев вычислений, см. [1, раздел 2] (здесь мы оставляем подробности читателю). Мы будем предполагать, что координатные функции на $P_{\mathrm{spr},n,d} \times \overline{k}^d$ суть $b_1,\dots,b_\mu$, $Z_1,\dots,Z_d$.

Фактически, мы будем использовать только следующие свойства дерева $T_d^{(4)}$. Множество листьев $L(T_d^{(4)})$ может быть отождествлено с $L(T_d''')^d$, где $L(T_d''')$ является множеством листьев дерева T_d'''. Пусть $w = (w_1,\dots,w_d) \in L(T_d^{(4)})$, где $w_i \in L(T_d''')$. Предположим, что алгебраическое многообразие параметров $\mathcal{W}_{w_i}$ соответствует w_i, $1 \leqslant i \leqslant d$, см. выше и определения в [1]. Так что $\mathcal{W}_{w_i} \subset P_{\mathrm{spr},n,d} \times \overline{k}$. Тогда многообразие параметров $\mathcal{W}_w$, соответствующее w, равно

$$\{(z,(x_1,\dots,x_n)) : (z,x_i) \in \mathcal{W}_{w_i}, \quad 1 \leqslant i \leqslant d\}.$$

Следовательно, если $w_1, \dots, w_d \in L(T_d''')$ – листья первого рода, то

$$\mathcal{W}_w = \mathcal{Z}(\psi_{w,1}, \dots, \psi_{w,\mu_{w,1}}) \setminus \mathcal{Z}(\psi_{w,\mu_{w,1}+1}, \dots, \psi_{w,\mu_{w,2}}) \tag{30}$$

для некоторых целых чисел $\mu_{w,1}$ и $\mu_{w,2}$, где $\mu_{w,2} \geqslant \mu_{w,1} \geqslant d$, и многочленов $\psi_{w,i}$, таких, что

$$\begin{aligned} &\psi_{w,i} \in k[b_1, \dots, b_\mu, Z_i] \setminus k[b_1, \dots, b_\mu], && 1 \leqslant i \leqslant d, \\ &\psi_{w,i} \in k[b_1, \dots, b_\mu], && d+1 \leqslant i \leqslant \mu_{w,2}. \end{aligned} \tag{31}$$

Для всех i степени $\deg_{b_1,\dots,b_\mu,Z_1,\dots,Z_d} \psi_{w,i}$ ограничены сверху величиной $d^{O(1)}$ с абсолютной константой в $O(\dots)$. Уровень $l(T_d^{(4)})$ также ограничен сверху величиной $d^{O(1)}$.

Далее, если все $w_1, \dots, w_d \in L(T_d''')$ – листья первого рода, то $\bigcap_{1 \leqslant i \leqslant d} \mathcal{W}'_{w_i}$ совпадает с множеством z, таких, что существует $(x_1, \dots, x_d)$ с $(z, (x_1, \dots, x_d)) \in \mathcal{W}_w$.

Пусть $\mathcal{U} \subset \prod\limits_{1 \leqslant i \leqslant d} \mathcal{P}_{i,d_{i,1},d_{i,2},d_{i,3}}$ – открытое в топологии Зарисского подмножество всех элементов $(Q^{(i)}, H^{(i)}, \varepsilon^{(i)}, e^{(i)}, c^{(i)}, y^{(i)})_{1 \leqslant i \leqslant d}$, таких, что $Q^{(i)} \in \widetilde{P}^{d_{i,2}}_{n,d_{i,1}}$, $H^{(i)} \in \overline{k}[Y, Z]$, $H^{(i)} \in P_{2,d_{i,2},d_{i,3}}$, $0 \neq \varepsilon^{(i)}, e^{(i)}, c^{(i)} \in \overline{k}$, $y^{(i)} \in \overline{k}$ и $\operatorname{lc}_Z H^{(i)} \in \overline{k}$ при $1 \leqslant i \leqslant d$. Следовательно, $\mathcal{U}$ зависит от d и $d_{j,i}$, $1 \leqslant j \leqslant 3$, $1 \leqslant i \leqslant d$. Для краткости обозначим $\mathcal{U} = \mathcal{U}(d, d_{j,i})$. Положим $\mathcal{P}_{i,d_{i,1},d_{i,2}} = \widetilde{P}^{d_{i,2}}_{n,d_{i,1}} \times P_{1,d_{i,2}} \times \overline{k}^2$.

Теперь введём функцию

$$\mathfrak{S} : \bigcup_{d \geqslant 1} \bigcup_{\substack{d_{i,1} \geqslant 0,\ d_{i,2} \geqslant 0,\\ d_{i,3} \geqslant 0\ \forall\, 1 \leqslant i \leqslant d}} \mathcal{U}(d, d_{j,i}) \to \bigcup_{d \geqslant 1} \bigcup_{\substack{d_{i,1} \geqslant 0,\ d_{i,2} \geqslant 0,\\ d_{i,3} \geqslant 0\ \forall\, 1 \leqslant i \leqslant d}} \prod_{1 \leqslant i \leqslant d} \mathcal{P}_{i,d_{i,1},d_{i,2}},$$

заданную формулой

$$\mathfrak{S}((Q^{(i)}, H^{(i)}, \varepsilon^{(i)}, e^{(i)}, y^{(i)})_{1 \leqslant i \leqslant d}) = (\widetilde{Q}^{(i)}, \widetilde{G}^{(i)}, \widetilde{\varepsilon}^{(i)}, c^{(i)})_{1 \leqslant i \leqslant d},$$

где $\widetilde{Q}^{(i)} \in \widetilde{P}^{\alpha_{i,2}}_{n,\alpha_{i,1}}$, $\widetilde{G}^{(i)} \in P_{1,\alpha_{i,2}}$, $\widetilde{\varepsilon}^{(i)} \in \overline{k}$, $\alpha_{i,1}, \alpha_{i,2} \geqslant 0$, вычисляются следующим образом.

Если $\deg_Z H^{(i)} = 0$ по крайней мере для одного i, $1 \leqslant i \leqslant d$, то положим $\alpha_{i,1} = \alpha_{i,2} = 0$, $\widetilde{Q}^{(i)} = \varnothing$ для всех i и $\widetilde{G}^{(i)} = 1$, $\widetilde{\varepsilon}^{(i)} = \varepsilon^{(i)}$ для всех i (фактически, этот случай нас не интересует).

Предположим, что $\deg_Z H^{(i)} \geqslant 1$ при $1 \leqslant i \leqslant d$. Тогда вычислим многочлен

$$E^{(i)} = \mathrm{G\,C\,D}_{Y,Z}\Big(H^{(i)}(Y, e^{(i)} Z)), \prod_{1 \leqslant j < i} H^{(j)}(Y, e^{(j)} Z)\Big)$$

и, используя лемму 2, многочлен $\widetilde{H}^{(i)}$, совпадающий с $H^{(i)}/E^{(i)}$ с точностью до ненулевого множителя из k.

Положим $\alpha_{i,2} = \deg_Z \widetilde{H}^{(i)}$. Если $\alpha_{i,2} = 0$, то положим $\alpha_{1,i} = 0$ и $\widetilde{G}^{(i)} = \widetilde{H}^{(i)}$, $\widetilde{Q}^{(i)} = \varnothing \in \widetilde{P}_0^0$, $\widetilde{\varepsilon}^{(i)} = \varepsilon^{(i)}$.

Предположим, что $\alpha_{i,2} > 0$. Пусть $\widetilde{H}^{(i)}(y^{(i)}, Z) = \sum\limits_{0 \leqslant j \leqslant \alpha_{i,2}} \widetilde{H}_j^{(i)} Z^j$, где $\widetilde{H}_j^{(i)} \in \overline{k}$. Тогда положим

$$\widetilde{G}^{(i)} = \sum_{0 \leqslant j \leqslant \alpha_{i,2}} \widetilde{H}_j^{(i)} \cdot (e^{(i)})^{\alpha_{i,2}-j} Z^j.$$

Пусть $\nu_{i,2} = \mathrm{lc}_Z \widetilde{G}^{(i)}$ (отметим, что $\mathrm{lc}_Z \widetilde{G}^{(i)} = \widetilde{H}_{\alpha_2}^{(i)} = \mathrm{lc}_Z \widetilde{H}^{(i)} \in \overline{k}$). Тогда, применяя лемму 2, для всякого i, $0 \leqslant i \leqslant d-1$, мы записываем представление

$$\nu_{i,2}^{d_{i,2}-\alpha_{i,2}+1} \sum_{0 \leqslant j < d_{i,2}} Q_j^{(i)} Z^j = A^{(i)} \widetilde{G}^{(i)} + B^{(i)},$$

где $A^{(i)}, B^{(i)} \in \overline{k}[X_1, \ldots, X_n][Z]$ и $\deg_Z B^{(i)} < \alpha_{i,2}$. Пусть

$$B^{(i)} = \sum_{0 \leqslant j < \alpha_{i,2}} B_j^{(i)} Z^j, \quad B_j^{(i)} \in \overline{k}[X_1, \ldots, X_n] \quad \text{для всех} \quad i, j.$$

Положим $\widetilde{Q}^{(i)} = (B_0^{(i)}, \ldots, B_{\alpha_{i,2}-1}^{(i)})$ и $\alpha_{1,i} = \max_{1 \leqslant j < \alpha_{i,2}} \deg_{X_1,\ldots,X_n} B_j^{(i)}$. Наконец, полагаем $\widetilde{\varepsilon}^{(i)} = \nu_{i,2}^{d_{i,2}-\alpha_{i,2}+1} \varepsilon^{(i)}$. Таким образом, элемент $(\widetilde{Q}^{(i)}, \widetilde{H}^{(i)}, \widetilde{\varepsilon}^{(i)}, c^{(i)})_{1 \leqslant i \leqslant d}$ определён.

Согласно описанной конструкции функция $\mathfrak{S}$ является алгоритмом, соответствующим лесу вычислений. Обозначим через

$$T^{(5)} = \{T_{d,d_{i,j}}^{(5)}\}_{\forall d, d_{i,j}}$$

этот лес вычислений.

Теперь определена композиция $T^{(5)} \circ T^{(4)}$ лесов вычислений $T^{(5)}$ и $T^{(4)}$, см. [1]. Напомним, что $T^{(5)} \circ T^{(4)}$ соответствует функции $\mathfrak{S} \circ \mathfrak{T}$. Пусть $T^{(6)} = T^{(5)} \circ T^{(4)}$. Так что $T^{(6)} = \{T_d^{(6)}\}_{d \geqslant 2}$, где каждое $T_d^{(6)}$ является деревом вычислений.

Выход, соответствующий листу $w \in L(T_d^{(6)})$ дерева $T_d^{(6)}$, имеет вид $(Q_w^{(i)}, G_w^{(i)}, \varepsilon_w^{(i)}, c_w)_{1 \leqslant i \leqslant d}$, где

$$G_w^{(i)} \in k[b_1, \ldots, b_\mu][Z], \quad \deg_Z G_w^{(i)} = \alpha_{w,i,2} \geqslant 0,$$

если $\alpha_{w,i,2} > 0$, то $Q_w^{(i)} = (Q_{w,0}^{(i)}, \dots, Q_{w,\alpha_{w,i,2}-1}^{(i)})$, где

$$Q_{w,j}^{(i)} \in k[b_1, \dots, b_\mu][X_1, \dots, X_n]$$

и $\alpha_{w,i,1} = \max_{1 \leqslant j \leqslant \alpha_{w,i,2}-1} \deg_{X_1,\dots,X_n} Q_{w,j}^{(i)}$, если $\alpha_{w,i,2} = 0$, то $\alpha_{w,i,1} = 0$ и $Q_w^{(i)} = \varnothing$. Имеем $0 \neq \varepsilon_w^{(i)}, c_w \in k[b_1, \dots, b_\mu]$ (здесь c_w не зависит от i).

Степени относительно $b_1, \dots, b_\mu$ всех многочленов $G_w^{(i)}, \varepsilon_w^{(i)}, c_w$ и $Q_{w,j}^{(i)}$ (если $\alpha_{w,i,2} > 0$) ограничены сверху величиной $d^{O(1)}$ с абсолютной константой в $O(\dots)$.

Алгебраическое многообразие $\mathcal{W}_w$, соответствующее любому листу $w \in L(T_d^{(6)})$, имеет вид (30), где $\psi_{w,i}$ является многочленом из $k[b_1, \dots, b_\mu]$ или $k[b_1, \dots, b_\mu, Z_j]$ для некоторого j, $1 \leqslant j \leqslant d$. Фактически, все многочлены $\psi_{w,i}$ имеют коэффициенты из K_0. Для всех i степени $\deg_{b_1,\dots,b_\mu,Z_1,\dots,Z_d} \psi_{w,i}$ ограничены сверху величиной $d^{O(1)}$ с абсолютной константой в $O(\dots)$. Уровень $l(T_d^{(6)})$ также ограничен сверху величиной $d^{O(1)}$.

Кроме того, все $\varepsilon_w^{(i)}$, c_w, $\mathrm{lc}_Z G_w^{(i)}$ не имеют нулей на $\mathcal{W}_w$, т.е.

$$\mathcal{W}_w \cap \mathcal{Z}\Big(c_w \prod_{1 \leqslant i \leqslant d} (\varepsilon_w^{(i)} \mathrm{lc}_Z G_w^{(i)})\Big) = \varnothing.$$

Это немедленно следует из нашей конструкции.

Обозначим через $L'(T_d^{(6)})$ множество листьев w дерева $T_d^{(6)}$, удовлетворяющих следующим свойствам:

- для w существуют листья $w_1, \dots, w_d \in L(T_d''')$ первого рода, такие, что w является потомком листа $(w_1, \dots, w_d) \in L(T^{(4)})$,
- $\sum\limits_{1 \leqslant i \leqslant d} \alpha_{w,i,1}\alpha_{w,i,2} = d$.

Алгебраическое многообразие $\mathcal{W}_w$, соответствующее любому листу $w \in L'(T_d^{(6)})$, имеет вид (30) для некоторых целых чисел $\mu_{w,1}$, $\mu_{w,2}$, где $\mu_{w,2} \geqslant \mu_{w,1} \geqslant d$, и многочленов $\psi_{w,i}$, удовлетворяющих условиям (31). Положим

$$\mathcal{W}'_w = \mathcal{Z}(\psi_{w,d+1}, \dots, \psi_{w,\mu_{w,1}}) \setminus \mathcal{Z}(\psi_{w,\mu_{w,1}+1}, \dots, \psi_{w,\mu_{w,2}}) \subset P_{\mathrm{spr},n,d}.$$

Для всякого $w \in L'(T_d^{(6)})$ обозначим через I_w множество всех i, таких, что $1 \leqslant i \leqslant d$ и $\alpha_{w,i,1}\alpha_{w,i,2} \neq 0$. Для всякого $i \in I_w$ положим

$$F_{w,i} = \sum_{0 \leqslant j < \alpha_{w,i,2}} Q_{w,j}^{(i)} Z^j \in k[b_1, \dots, b_\mu, Z, X_1, \dots, X_n].$$

Для всякой точки $(b_1^*, \dots, b_\mu^*) \in \mathcal{W}'_w$ обозначим через $\Xi_{w,i}$ множество всех корней многочлена $G_w^{(i)}(b_1^*, \dots, b_\mu^*, Z) \in \overline{k}[Z]$. Таким образом, $\#\Xi_{w,i} = \alpha_{w,i,2}$.

Пусть теперь $F \in \overline{k}[b_1, \dots, b_\mu, X_1, \dots, X_n]$ – общий многочлен степени $\deg_{X_1,\dots,X_n} F = d \geqslant 2$. Как полином от $X_1, \dots, X_n$ он имеет все коэффициенты из семейства $b_1, \dots, b_\mu$.

Лемма 4. *Справедливы следующие утверждения.*

(a) *Объединение* $\bigcup_{w \in L'(T_d^{(6)})} \mathcal{W}'_w$ *есть* $P_{\mathrm{spr},n,d}$, *т.е.* $\{\mathcal{W}'_w\}_{w \in L'(T_d^{(6)})}$ *является покрытием пространства* $P_{\mathrm{spr},n,d}$.

(b) *Для всякого* $w \in L'(T_d^{(6)})$ *для всякой точки* $(b_1^*, \dots, b_\mu^*) \in \mathcal{W}'_w$ *для всякого корня* $\xi \in \Xi_{w,i}$ *многочлен*

$$F_{w,i}(b_1^*, \dots, b_\mu^*, \xi, X_1, \dots, X_n) \in \overline{k}[X_1, \dots, X_n]$$

неприводим в последнем кольце, т.е. он абсолютно неприводим.

(c) *Семейство* $\{F_{w,i}(b_1^*, \dots, b_\mu^*, \xi, X_1, \dots, X_n)\}_{\substack{\xi \in \Xi_{w,i} \\ i \in I_w}}$ *содержит* $\sum\limits_{i \in I_w} \alpha_{w,i,2}$ *попарно взаимно простых в кольце* $\overline{k}[X_1, \dots, X_n]$ *многочленов.*

(d) *Имеем*

$$c_w(b_1^*, \dots, b_\mu^*) \prod_{i \in I_w} \prod_{\xi \in \Xi_{w,i}} F_{w,i}(b_1^*, \dots, b_\mu^*, \xi, X_1, \dots, X_n)$$
$$= \Big(\prod_{i \in I_w} (\varepsilon_w^{(i)}(b_1^*, \dots, b_\mu^*))^{\alpha_{w,i,2}} \Big) F(b_1^*, \dots, b_\mu^*, X_1, \dots, X_n). \qquad (32)$$

Следовательно, (32) *является разложением многочлена* $F(b_1^*, \dots, b_\mu^*, X_1, \dots, X_n)$ *на абсолютно неприводимые множители с точностью до ненулевого множителя из* $\overline{k}$.

Доказательство. Нетрудно заметить, что всякий корень многочлена $H(Y, q_{\alpha_2} Z) \in \overline{k}(Y)[Z]$ имеет вид $q(Y,0)/q_{\alpha_2} \in k[x][Y]$ для некоторого корня x многочлена $f(X,0)$. Значит, $\mathrm{lc}_Y q(Y,0)/q_{\alpha_2} = 1$. С другой стороны, существует единственный абсолютно неприводимый множитель φ многочлена f, такой, что $\mathrm{lc}_{X_1} \varphi = 1$ и $\varphi(Y, 0, \dots, 0) = q(Y,0)/q_{\alpha_2}$. Обратно, согласно описанной конструкции, для всякого абсолютно неприводимого множителя φ многочлена f, такого, что $\mathrm{lc}_{X_1} \varphi = 1$, существует корень x многочлена $f(X,0)$, такой, что $\varphi(Y, 0, \dots, 0) =$

$q(Y,0)/q_{\alpha_2}$. Отсюда легко вывести все утверждения леммы (мы оставляем подробности читателю). $\square$

§6. Лемма о покрытии и стратификации

В следующей общей лемме мы показываем, как получить стратификацию некоторого многообразия, если известно его покрытие. Но сначала нам требуется дать несколько определений, ср. [1].

Пусть аффинное пространство $\mathbb{A}^\mu(\overline{k})$ имеет координатные функции $b_1,\dots,b_\mu$. Пусть $V \subset \mathbb{A}^\mu(\overline{k})$ – квазипроективное алгебраическое многообразие и $\overline{V}$ – замыкание относительно топологии Зарисского многообразия V в $\mathbb{A}^\mu(\overline{k})$. Предположим, что $\overline{V} = \bigcup\limits_{0\leqslant a\leqslant\mu} V_a$ – разложение многообразия $\overline{V}$ в объединение равноразмерностных аффинных алгебраических многообразий V_a, т.е. для всякого целого числа a, $0 \leqslant a \leqslant \mu$, размерность всякой неприводимой компоненты E алгебраического многообразия V_a равна a и E является неприводимой компонентой многообразия $\overline{V}$. Пусть $\deg V_a = D_a$ (степень аффинного алгебраического многообразия равна степени его замыкания относительно топологии Зарисского в соответствующем проективном пространстве). По определению $D_a(V) = D_a$. Для всякого целого числа $D \geqslant 2$ положим

$$\begin{aligned}
&\deg V = \sum_{0\leqslant a\leqslant\mu} D_a,\\
&\delta_0(V) = D_a(V), \quad \text{где} \quad a = \dim(V),\\
&\delta_1(V,D) = \sum_{0\leqslant a\leqslant\mu} D_a(V)D^a,\\
&\delta(V,D) = \sum_{0\leqslant a\leqslant\mu} D_a(V)(D^{a+1}-1)/(D-1).
\end{aligned}$$

Зафиксируем целое число $D \geqslant 2$. Пусть $V_1, V_2 \subset \mathbb{A}^\mu(\overline{k})$ – два квазипроективных алгебраических многообразия. Положим $V_1 < V_2$ тогда и только тогда, когда $V_1 \subset V_2$, $\dim V_1 < \dim V_2$ или $V_1 \subset V_2$, $\dim V_1 = \dim V_2$, но $\delta_0(V_1) < \delta_0(V_2)$. Тогда $<$ является частичным порядком на множестве всех квазипроективных алгебраических многообразий в $\mathbb{A}^\mu(\overline{k})$.

Лемма 5. *Пусть V – квазипроективное алгебраическое многообразие в $\mathbb{A}^\mu(\overline{k})$. Пусть $\{\mathcal{W}_\gamma\}_{\gamma\in\Gamma}$ – семейство квазипроективных алгебраических многообразий в $\mathbb{A}^\mu(\overline{k})$. Предположим, что для всякого $\gamma\in\Gamma$*

$$\mathcal{W}_\gamma = \mathcal{Z}(\psi_{\gamma,1},\dots,\psi_{\gamma,\mu_{\gamma,1}}) \setminus \mathcal{Z}(\psi_{\gamma,\mu_{\gamma,1}+1},\dots,\psi_{\gamma,\mu_{\gamma,2}}) \subset \mathbb{A}^\mu(\overline{k})$$

для некоторых многочленов $\psi_{\gamma,i}\in\overline{k}[b_1,\dots,b_\mu]$, таких, что для всех i

$$\deg_{b_1,\dots,b_\mu}\psi_{\gamma,i}\leqslant D$$

для некоторого $D\geqslant 2$. Предположим, что $\bigcup_{\gamma\in\Gamma}\mathcal{W}_\gamma\supset V$. Тогда существует семейство квазипроективных алгебраических многообразий $\{\mathcal{W}_\beta\}_{\beta\in B}$, удовлетворяющее следующим свойствам.

(a) *Для всякого $\beta\in B$*

$$\mathcal{W}_\beta = \mathcal{Z}(\psi^{(1)}_{\beta,1},\dots,\psi^{(1)}_{\beta,\mu_{\beta,1}}) \setminus \bigcup_{2\leqslant j\leqslant m_\beta} \mathcal{Z}(\psi^{(j)}_{\beta,1},\dots,\psi^{(j)}_{\beta,\mu_{\beta,j}}) \subset \mathbb{A}^\mu(\overline{k})$$

для некоторого $m_\beta\geqslant 2$ и некоторых многочленов $\psi^{(j)}_{\beta,i}\in\overline{k}[b_1,\dots,b_\mu]$, таких, что $\deg_{b_1,\dots,b_\mu}\psi_{\beta,i}\leqslant D$ для всех i,j.

(b) *Для всякого $\beta\in B$ целое число m_β ограничено сверху величиной $\delta_1(V,D)$.*

(c) *$\{V\cap\mathcal{W}_\beta\}_{\beta\in B}$ является стратификацией алгебраического многообразия V, т.е. $\bigcup_{\beta\in B}(V\cap\mathcal{W}_\beta)=V$ и для всех попарно различных β_1,β_2 имеем $(V\cap\mathcal{W}_{\beta_1})\cap(V\cap\mathcal{W}_{\beta_2})=\varnothing$.*

(d) *Для всякого $\beta\in B$ существует индекс $\gamma\in\Gamma$, такой, что $\mathcal{W}_\beta\subset\mathcal{W}_\gamma$.*

(e) *$\#B\leqslant\delta(V,D)$.*

Доказательство. Доказательство использует рекурсию по V. Именно, мы будем предполагать, что лемма доказана для всех квазипроективных алгебраических многообразий V', таких, что $V'<V$. База рекурсии $V=\varnothing$ очевидна, поскольку в этом случае $\delta(V,D)=0$ и можно взять $B=\varnothing$.

Для всякого $\gamma\in\Gamma$ положим

$$\mathcal{W}^{(1)}_\gamma = \mathcal{Z}(\psi_{\gamma,1},\dots,\psi_{\gamma,\mu_{\gamma,1}}),\quad \mathcal{W}^{(2)}_\gamma = \mathcal{Z}(\psi_{\gamma,\mu_{\gamma,1}+1},\dots,\psi_{\gamma,\mu_{\gamma,2}}).$$

Обозначим через $V^{(1)}_\gamma$ объединение всех неприводимых компонент E многообразия V, таких, что $E\subset\mathcal{W}^{(1)}_\gamma$ и $E\not\subset\mathcal{W}^{(2)}_\gamma$.

Обозначим через $V_\gamma^{(2)}$ объединение всех неприводимых компонент E многообразия V, таких, что $E \subset \mathcal{W}_\gamma^{(1)} \cap \mathcal{W}_\gamma^{(2)}$.

Обозначим через V'_γ объединение всех неприводимых компонент E многообразия V, таких, что $E \not\subset \mathcal{W}_\gamma^{(1)}$.

Положим $V''_\gamma = (V_\gamma^{(1)} \cap \mathcal{W}_\gamma^{(2)}) \cup V_\gamma^{(2)}$.

Опишем шаг рекурсии. Существует индекс $\gamma_0 \in \Gamma$, такой, что $\dim V_{\gamma_0}^{(1)} = \dim V$. Выберем и зафиксируем такой индекс γ_0. Теперь $V'_{\gamma_0} < V$ и $V''_{\gamma_0} < V$. Применим рекурсивное предположение к алгебраическим многообразиям V'_{γ_0} и V''_{γ_0}. Получим семейство $\{\mathcal{W}'_\beta\}_{\beta\in B'}$ (соответственно $\{\mathcal{W}''_\beta\}_{\beta\in B''}$), удовлетворяющее свойствам (a)–(d) с (V'_{γ_0}, B') (соответственно (V''_{γ_0}, B'')) вместо (V, B).

Можно предполагать без ограничения общности, что $\gamma_0 \notin B' \cup B''$ и $B' \cap B'' = \varnothing$. Положим $B = B' \cup B'' \cup \{\gamma_0\}$ и

$$\mathcal{W}_\beta = \begin{cases} \mathcal{W}_{\gamma_0}, & \text{если} \quad \beta = \gamma_0, \\ \mathcal{W}_\beta \setminus \mathcal{W}_{\gamma_0}^{(1)}, & \text{если} \quad \beta \in B', \\ \mathcal{W}_\beta \cap \mathcal{W}_{\gamma_0}^{(1)} \cap \mathcal{W}_{\gamma_0}^{(2)}, & \text{если} \quad \beta \in B''. \end{cases}$$

Очевидно, выполняются свойства (a), (c) и (d). Далее, имеем

$$\delta_1(V''_{\gamma_0}, D) \leqslant \delta_1(V, D)$$

по теореме Безу, и, очевидно, $\delta_1(V'_{\gamma_0}, D) < \delta_1(V, D)$. Отсюда, используя рекурсивное предположение, получаем (b).

Пусть $E \subset \mathbb{A}^\mu(\overline{k})$ – неприводимое над k квазипроективное алгебраическое многообразие и $g \in \overline{k}[X_1, \ldots, X_n]$ – многочлен степени не больше D. Тогда из теоремы Безу следует, что $\delta(E \cap \mathcal{Z}(g), D) \leqslant \delta(E, D)$ и если $E \cap \mathcal{Z}(g) \neq E$, то $\deg E + \delta(E \cap \mathcal{Z}(g), D) \leqslant \delta(E, D)$.

Применяя последнее утверждение несколько раз, выводим, что

$$1 + \delta(V_{\gamma_0}^{(1)} \cap \mathcal{W}_{\gamma_0}^{(2)}, D) \leqslant \deg V_{\gamma_0}^{(1)} + \delta(V_{\gamma_0}^{(1)} \cap \mathcal{W}_{\gamma_0}^{(2)}, D) \leqslant \delta(V_{\gamma_0}^{(1)}, D),$$

ср. с доказательством леммы 1 в [1] (здесь мы оставляем подробности читателю).

Следовательно, используя рекурсивное предположение, мы получаем, что

$$\begin{aligned} \#B &\leqslant 1 + \#B' + \#B'' \leqslant 1 + \delta(V', D) + \delta(V'', D) \\ &\leqslant 1 + \delta(V_{\gamma_0}^{(1)} \cap \mathcal{W}_{\gamma_0}^{(2)}, D) + \delta(V_{\gamma_0}^{(2)}, D) + \delta(V'_{\gamma_0}, D) \\ &\leqslant \delta(V_{\gamma_0}^{(1)}, D) + \delta(V_{\gamma_0}^{(2)}, D) + \delta(V'_{\gamma_0}, D) = \delta(V, D). \end{aligned}$$

Это доказывает утверждение (e). Лемма доказана. □

Например, применяя лемму 5 к покрытию $\{\mathcal{W}'_w\}_{w\in L'(T_d^{(6)})}$ пространства $P_{\mathrm{spr},n,d}$ из леммы 4 (i), можно получить стратификацию $\{\mathcal{W}_\beta\}_{w\in B}$ пространства $P_{\mathrm{spr},n,d}$.

§7. Общий случай

Напомним, что в разделе 2 определена функция $\mathrm{SQF}_{X_1,\dots,X_n}$, соответствующая лесу вычислений $\{T'_d\}_{d\geqslant 0}$. Мы имеем $\mathrm{SQF}_{X_1,\dots,X_n} = \{\mathrm{SQF}_{i,X_1,\dots,X_n}\}_{1\leqslant i\leqslant d}$, см. конец раздела 2.

Пусть d – целое число, $d \geqslant 2$, $F \in \overline{k}[X_1,\dots,X_n]$ – произвольный многочлен степени $\deg_{X_1,\dots,X_n} F \leqslant d$ и $x_i = (x_{i,1},\dots,x_{i,d}) \in \overline{k}^d$, $1 \leqslant i \leqslant d$. Тогда положим $F' = \mathrm{RDP}_{X_1,\dots,X_n}(F)$, см. замечание 1. Пусть $\deg_{X_1,\dots,X_n} F' = d_1$. Если $d_1 \leqslant 0$, то положим $\mathfrak{D}(F,(x_1,\dots,x_d)) = F'$.

Предположим, что $d_1 \geqslant 1$. Тогда положим $F''_i = \mathrm{SQF}_{i,X_1,\dots,X_n}(F')$, $1 \leqslant i \leqslant d_1$. Пусть $d_{i,1} = \deg_{X_1,\dots,X_n} F''_i$. Если $d_{i,1} \leqslant 1$, то положим $G_i = F''_i$ при $1 \leqslant i \leqslant d_{i,1}$. Если $d_{i,1} \geqslant 2$, то положим

$$G_i = (\mathfrak{S}\circ\mathfrak{T})(F''_i,(x_{i,1},\dots,x_{i,d_{i,1}}))$$

при $1 \leqslant i \leqslant d_{i,1}$. Положим $\mathfrak{D}(F,(x_1,\dots,x_d)) = (G_1,\dots,G_{d_1})$.

Теперь $\mathfrak{D}$ – функция с областью определения $\bigcup_{d\geqslant 2}(\overline{k}^{N(n,d)}\times\overline{k}^{d^2})$. Мы предоставляем читателю определить область значений функции $\mathfrak{D}$. Она соответствует лесу вычислений $T^{(7)} = \{T_d^{(7)}\}_{d\geqslant 2}$.

Следующие утверждения о деревьях $T_d^{(7)}$ аналогичны утверждениям из раздела 5, относящимся к $T_d^{(6)}$. Их доказательства только немного сложнее, чем доказательства аналогичных утверждений из раздела 5, так что мы оставляем подробности читателю.

Уровень $l(T_d^{(7)})$ дерева $T_d^{(7)}$ ограничен сверху величиной $d^{O(1)}$. Для всякого листа $w \in L(T_d^{(7)})$ степени относительно $b_1,\dots,b_\mu$ всех многочленов из выхода, соответствующего w, ограничены сверху величиной $d^{O(1)}$. Квазипроективное алгебраическое многообразие $\mathcal{W}_w$ может быть представлено в виде (30), где $\psi_{w,r} \in k[b_1,\dots,b_\mu,\{Z_{i,j}\}_{1\leqslant i,j\leqslant d}]$ и для всякого (i,j) существует не более одного многочлена $\psi_{w,r}$, такого, что $\deg_{Z_{i,j}}\psi_{w,r} > 0$. В этом случае мы будем обозначать $r = r_{i,j}$. Кроме того, если $\deg_{Z_{i,j}}\psi_{w,r} > 0$, то $\psi_{w,r} \in k[b_1,\dots,b_\mu,Z_{i,j}]$. Степени всех многочленов $\psi_{w,r}$ ограничены сверху величиной $d^{O(1)}$.

Пусть $w \in L(T_d^{(7)})$. Предположим, что для всех (i,j) мы имеем $1 \leqslant r_{i,j} \leqslant \mu_{w,1}$, если $r_{i,j}$ определено. В этом случае по определению w является листом первого рода. Для всякого листа первого рода квазипроективное алгебраическое многообразие $\mathcal{W}'_w$ по определению является проекцией многообразия $\mathcal{W}_w$ в $\mathbb{A}^\mu(\overline{k})$ (здесь это аффинное пространство имеет координатные функции $b_1, \ldots, b_\mu$).

Доказательство теоремы 1. Сначала рассмотрим случай, когда

$$((a_1, \ldots, a_\nu), f) = ((b_1, \ldots, b_\mu), F),$$

где F – общий многочлен степени d (т.е. семейство его коэффициентов есть $\{b_j\}_{1 \leqslant j \leqslant \mu}$)). Тогда аналогом леммы 4 является в точности теорема 1 (заметим только, что в формулировке теоремы используются несколько другие обозначения). Дерево $T_d^{(7)}$ сейчас аналогично $T_d^{(6)}$.

Можно определить подмножество $L'(T_d^{(7)}) \subset L(T_d^{(7)})$ листьев w первого рода, таких, что для всякой точки $(b_1^*, \ldots, b_\mu^*) \in \mathcal{W}'_w$ выход, соответствующий w, определяет разложение многочлена

$$F(b_1^*, \ldots, b_\mu^*, X_1, \ldots, X_n)$$

на абсолютно неприводимые множители. Семейство $\{\mathcal{W}'_w\}_{w \in L'(T_d^{(7)})}$ является покрытием пространства $\overline{k}^{N(n,d)}$ для всякого $d \geqslant 2$. Можно получить стратификацию $\{\mathcal{W}_\beta\}_{\beta \in B_1}$ этого пространства, применяя лемму 5 к рассматриваемому покрытию.

Далее, аналогично доказательству леммы 4, комбинируя результаты из предыдущих разделов, несложно установить все требуемые утверждения в случае общего многочлена F. В частности, можно вычислить точные значения $\lambda_{\alpha,0}$ и $\lambda_{\alpha,1}$ в терминах из разделов 2–4, ср. с формулировкой леммы 4.

Теперь, чтобы доказать теорему для исходных входных данных $((a_1, \ldots, a_\nu), f)$, достаточно рассмотреть дерево $T_d^{(7)}(f)$, см. определение в [1] (грубо говоря, чтобы получить $T_d^{(7)}(f)$, следует подставить коэффициенты из $k[a_1, \ldots, a_\nu]$ многочлена f вместо $b_1, \ldots, b_\mu$ во все объекты дерева $T_d^{(7)}$). Листья $L(T_d^{(7)}(f))$ находятся во взаимно однозначном соответствии с $L(T_d^{(7)})$. Имеем $l(T_d^{(7)}(f)) = l(T_d^{(7)}) + 1$. Для всякого $w \in L(T_d^{(7)}(f))$ степени относительно $a_1, \ldots, a_\nu$ всех многочленов из выхода, соответствующего w, ограничены сверху величиной

$d'd^{O(1)}$. Квазипроективное алгебраическое многообразие $\mathcal{W}_w$ может быть представлено в виде (30), где

$$\psi_{w,r} \in k[a_1, \dots, a_\nu, \{Z_{i,j}\}_{1 \leqslant i,j \leqslant d}].$$

Степени всех многочленов $\psi_{w,r}$ ограничены сверху величиной $d'd^{O(1)}$.

Для всякого листа $w \in L(T_d^{(7)}(f))$, соответствующего листу первого рода из $L(T_d^{(7)})$, квазипроективное алгебраическое многообразие $\mathcal{W}'_w$ по определению является проекцией многообразия $\mathcal{W}_w$ в $\mathbb{A}^\nu(\overline{k})$ (здесь это аффинное пространство имеет координатные функции $a_1, \dots, a_\nu$).

Обозначим через $L'(T_d^{(7)}(f))$ множество листьев w из $L(T_d^{(7)}(f))$, таких, что w соответствует листу из $L'(T_d^{(7)})$. Для всякого листа w из $L'(T_d^{(7)}(f))$ для всякой точки $(a_1^*, \dots, a_\nu^*) \in \mathcal{W}'_w$ выход, соответствующий w, определяет разложение многочлена $f(a_1^*, \dots, a_\nu^*, X_1, \dots, X_n)$ на абсолютно неприводимые множители.

Наконец, заменим дерево $T_d^{(7)}(f)$ на несократимое дерево $\mathrm{IRD}(T_d^{(7)}(f))$, см. [1]. Число листьев дерева $\mathrm{IRD}(T_d^{(7)}(f))$ ограничено сверху величиной $(d')^\nu d^{O(\nu)}$ по теореме 1 работы [1]. Теперь положим $T_d^{(8)} = \mathrm{IRD}(T_d^{(7)}(f))$ и $L'(T_d^{(8)}) = L(\mathrm{IRD}(T_d^{(7)}(f))) \cap L'(T_d^{(7)}(f))$.

Семейство $\{\mathcal{W}'_w\}_{w \in L'(T_d^{(8)})}$ является покрытием пространства $\mathbb{A}^\nu(\overline{k})$. Можно получить стратификацию $\{\mathcal{W}_\beta\}_{\beta \in B_2}$ этого пространства, применяя лемму 5 к рассматриваемому покрытию. По лемме 5 (e) число элементов $\#B_2$ ограничено сверху величиной $(d')^\nu d^{O(\nu)}$. Теперь можно взять A равным подмножеству всех $\beta \in B_2$, таких, что $\mathcal{W}_\beta \neq \varnothing$ (здесь обозначение $(\beta, \mathcal{W}_\beta)$ соответствует обозначению $(\alpha, \mathcal{W}_\alpha)$ из формулировки теоремы 1). Таким образом, исходный случай $((a_1, \dots, a_\nu), f)$ сводится к общему случаю $((b_1, \dots, b_\mu), F)$. Теорема доказана. $\square$

Список литературы

1. А. Л. Чистов, *Вычисления с параметрами: теоретическое обоснование.* — Зап. научн. семин. ПОМИ **436** (2015), 219–239.
2. А. Л. Чистов, *Оценка степени системы уравнений, задающей многообразие приводимых многочленов.* — Алгебра и анализ **24**, вып. 3 (2012), 199–222; и *“Исправление...”*, Алгебра и анализ **25**, вып. 2 (2013), 279.
3. G. E. Collins, *Subresultants and reduced polynomial remainder sequences.* — J. ACM **14**, No. 1 (1967), 128–142.

4. A. Chstov, H. Fournier, L. Gurvits, P. Koiran, *Vandermonde matrices, NP-completeness, and transversal subspaces.* — Found. Comput. Math. **3**, No. 4 (2003), 421–427.

Chistov A. L. Efficient absolute factorization of polynomials with parametric coefficients.

Consider a polynomial with parametric coefficients. We show that the variety of parameters can be represented as a union of strata. For values of the parameters from each stratum, the decomposition of this polynomial into absolutely irreducible factors is given by algebraic formulas depending only on the stratum. Each stratum is a quasiprojective algebraic variety. This variety and the corresponding output are given by polynomials of degrees at most D with $D = d'd^{O(1)}$ where d', d are bounds on the degrees of the input polynomials. The number of strata is polynomial in the size of the input data. This solves a long-standing problem of avoiding a double exponential growth of the degrees of coefficients for this problem.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН,
191023 С.-Петербург, Россия
E-mail: alch@pdmi.ras.ru

Поступило 3 октября 2016 г.