Записки научных
семинаров ПОМИ
Том 421, 2014 г.

А. Л. Чистов

ДЕТЕРМИНИРОВАННЫЙ АЛГОРИТМ ПОЛИНОМИАЛЬНЫЙ СЛОЖНОСТИ ДЛЯ ПЕРВОЙ ТЕОРЕМЫ БЕРТИНИ. II

Данная статья продолжает [21] и является второй частью в серии из трёх. Во всех частях нумерация теорем (соответственно лемм, разделов и т.д.) единая. Она продолжается из [21] и далее из настоящей статьи в третьей части, которая подготовлена к печати. Список литературы в данной статье (за исключением ссылки на [21], которая здесь добавлена) совпадает со списком литературы из [21].

§2. Некоторые факты из линейной алгебры

По определению в любой характеристике основного поля существует только одна (0×0)-матрица, её определитель равен 1. Далее для всякого целого числа $m_1 \geqslant 0$ существует только одна $(m_1 \times 0)$-матрица (соответственно $(0 \times m_1)$-матрица). Пусть $m_2 \geqslant 0$ – целое число. Если A_1 является $(m_1 \times m_2)$-матрицей и A_2 является $(m_2 \times 0)$-матрицей, то A_1A_2 – $(m_1 \times 0)$-матрица. Если A_1 является $(0 \times m_1)$-матрицей и A_2 является $(m_1 \times m_2)$-матрицей, то A_1A_2 – $(0 \times m_2)$-матрица.

Согласно [16] для всех целых чисел $m_1 \geqslant m_2 \geqslant 0$ можно построить за время полиномиальное от m_1 семейство $((m_1 - m_2) \times m_1)$-матриц A_i, $1 \leqslant i \leqslant m_2(m_1 - m_2) + 1$ (они зависят от m_1 и m_2), удовлетворяющих следующим условиям.

- Все матрицы A_i имеют целые коэффициенты с длинами записи $O(m_1)$ (здесь и ниже константа в $O(\dots)$ является абсолютной), и ранг матрицы $\mathrm{rank}(A_i) = m_1 - m_2$.
- Для всякой $(m_2 \times m_1)$-матрицы A с коэффициентами из поля нулевой характеристики (фактически в [16] рассматривается случай произвольной характеристики) и рангом $\mathrm{rank}(A) = m_2$ существует $1 \leqslant i \leqslant m_2(m_1 - m_2) + 1$ такое, что определитель

$$\det \begin{pmatrix} A \\ A_i \end{pmatrix} \neq 0.$$

Ключевые слова: первая теорема Бертини, полиномиальный алгоритм.

Следовательно, можно построить за время полиномиальное от m_1 некоторую $(m_1 \times m_1)$-матрицу B_i с целыми коэффициентами с длинами записи $O(m_1)$ такую, что $A_i B_i = (0, \Delta_i)$, где Δ_i является диагональной $(m_1 - m_2) \times (m_1 - m_2)$-матрицей, все ненулевые коэффициенты матрицы Δ_i совпадают, и определитель $\det\Delta_i \neq 0$. Представим $B_i = (C_i, C'_i)$, где C_i (соответственно C'_i) является матрицей с m_2 (соответственно $m_1 - m_2$) столбцами. Мы будем обозначать через $A_{m_1,m_2,i}$, $B_{m_1,m_2,i}$, $C_{m_1,m_2,i}$ $C'_{m_1,m_2,i}$ матрицы A_i, B_i, C_i C'_i соответственно, если зависимость от m_1, m_2 существенна.

Лемма 15. *Пусть m_1, m_2, m_3 – произвольные целые числа такие, что $m_1 \geqslant m_3$, $m_2 \geqslant m_3$, $m_3 \geqslant 0$. Пусть $A = (a_{i,j})$ является $(m_2 \times m_1)$-матрицей с коэффициентами из $\overline{k_\alpha}$, где поле $k_\alpha = k(\varepsilon_1, \ldots, \varepsilon_\alpha)$,* [21, см. раздел 1], *$\alpha \geqslant 0$. Предположим, что $\operatorname{rank}(A) = m_3$. Пусть Δ является $(m_3 \times m_3)$-минором матрицы A (здесь это с точностью до знака определитель матрицы (a_{i_v,j_w}) для некоторых целых чисел $1 \leqslant i_1 < \ldots < i_{m_3} \leqslant m_2$, $1 \leqslant j_1 < \ldots < j_{m_3} \leqslant m_3$) таким, что $\Delta \neq 0$ и для всякого другого $(m_3 \times m_3)$-минора Δ_1 матрицы A элемент Δ_1/Δ не является бесконечно большим относительно поля k. Тогда справедливы следующие утверждения*

(i) *Существуют целые числа i, j такие, что $1 \leqslant j \leqslant m_3(m_1 - m_3) + 1$, $1 \leqslant i \leqslant m_3(m_2 - m_3) + 1$, определитель $\Delta_{i,j} = \det(C^T_{m_2,m_3,i} A C_{m_1,m_3,j}) \neq 0$ (здесь T обозначает транспонирование матриц), и $\Delta/\Delta_{i,j}$ не является бесконечно большим относительно поля k. Следовательно, стандартная часть $\operatorname{st}_\alpha(\Delta/\Delta_{i,j})$ является ненулевым элементом из $\overline{k}$.*

(ii) *Предположим, что $m_2 = m_3$. Тогда существует $1 \leqslant j \leqslant m_3(m_1 - m_3) + 1$ такое, что определитель $\Delta_j = \det(AC_{m_1,m_3,j} \neq 0$ и Δ/Δ_j не является бесконечно большим относительно поля k. Следовательно, стандартная часть $\operatorname{st}_\alpha(\Delta/\Delta_j)$ является ненулевым элементом из $\overline{k}$.*

(iii) *Предположим, что $m_2 = m_3$. Тогда существует $(m_1 \times m_1)$-матрица $G = (g_{i,j})$ такая, что всякий коэффициент $g_{i,j} \in \overline{k_\alpha}$ не является бесконечно большим относительно поля k; $\det(G) \neq 0$ и $\det(G)$ не является бесконечно малым относительно поля k; матрица $AG = (A', 0)$, где A' имеет m_3 столбцов. Определитель $\det(A') \neq 0$, и $\Delta/\det(A')$ не является бесконечно большим относительно поля k.*

Доказательство. Мы будем предполагать без ограничения общности, что $m_3 \geqslant 1$. Покажем, что из (ii) следует (i). Действительно, обозначим через A''' подматрицу в A, состоящую из строк с индексами $i_1, \ldots, i_{m_3}$. Применим (ii) к A'''. Тогда $A'''C_{m_1,m_3,j}$ является подматрицей в $AC_{m_1,m_3,j}$, определитель

$$\det(A'''C_{m_1,m_3,j}) \neq 0, \quad \text{и} \quad \Delta/\det(A'''C_{m_1,m_3,j})$$

не является бесконечно большим относительно поля k. Так что, чтобы доказать (i) достаточно применить (ii) во второй раз к матрице $(AC_{m_1,m_3,j})^T$. Требуемое утверждение доказано.

Докажем (iii). Заметим, что, см. [15], для всех $z_1, z_2 \in \overline{k_\alpha}$ таких, что $z_1 \neq 0$ и z_2/z_1 не является бесконечно большим относительно поля k, существует $c \in \overline{k}$ такое, что $(z_2 - cz_1)/z_1$ является бесконечно малой величиной относительно поля k. Положим $Q = A$ в качестве базы рекурсии. Мы опишем рекурсию по $(m_3 \times m_1)$-матрице $Q = (q_{i,j})$ с коэффициентами из $\overline{k_\alpha}$. На каждом шаге этой рекурсии мы используем элементарные преобразования столбцов матрица Q над полем $\overline{k_\alpha}$ и перестановки строк (престановки строк используются для удобства обозначений) такие, что все коэффициенты матриц, соответствующих этим преобразованиям столбцов не являются бесконечно большими относительно поля k. В конце рекурсии мы получим матрицу Q, которая имеет вид $(A', 0)$. Этого достаточно для доказательства утверждения (iii).

Пусть $0 \leqslant i < m_3$ – целое число. Рекурсивное предположение состоит в том, что в начале $(i+1)$-ого шага

$$Q = Q_i = \begin{pmatrix} Q'_i, & 0 \\ Q''_i & Q'''_i \end{pmatrix}, \tag{28}$$

где $Q'_i = (q'_{i,j})$ является $(i \times i)$-матрицей, коэффициенты $q'_{1,1}, \ldots, q'_{i,i}$ – ненулевые, $q'_{i,j} = 0$, если $j > i$, и для всех j, j_1, i_1, удовлетворяющих неравенствам $0 \leqslant j \leqslant i$, $j \leqslant j_1 \leqslant m_1$, $1 \leqslant i_1 \leqslant m_2$, частное $q_{i_1,j_1}/q_{j,j}$ не является бесконечно большим относительно поля k. Матрица $Q'''_i \neq 0$.

Опишем $(i+1)$-ый шаг рекурсии. Выберем ненулевой коэффициент z матрицы Q'''_i такой, что для любого другого коэффициента z' матрицы Q'''_i элемент z'/z не является бесконечно большим относительно поля k. Применяя престановки строк и столбцов, мы будем предполагать без ограничения общности, что $z = q_{i+1,i+1}$. Теперь при помощи подходящих элементарных преобразований столбцов мы переводим Q'''_i в

$\widetilde{Q}_i$, где первая строка матрицы $\widetilde{Q}_i$ равна $(q_{i+1,i+1}, 0, \dots, 0)$. По определению образ матрицы Q_i после всех этих преобразований есть Q_{i+1} (чтобы определить Q'_{i+1}, Q''_{i+1}, Q'''_{i+1} следует заменить i на $i+1$ в (28)). Поскольку ранг $\mathrm{rank}(A) = m_3$ матрица $Q'''_{i+1} \neq 0$ или $i+1 = m_3$. Таким образом, если $i+1 < m_3$, то переходим к следующему шагу рекурсии. Если $i+1 = m_3$, то мы полагаем $A' = Q'_{m_3}$. Существование матриц G и A' доказано. Мы имеем $A = (A', 0)G^{-1}$. Следовательно, минор $\Delta = \det(A')\det(G')$ для некоторой $(m_3 \times m_3)$-подматрицы G' матрицы G^{-1}. Отсюда следует последнее утверждение. Таким образом, (iii) доказано.

Докажем (ii). Мы будем использовать обозначения из доказательства (iii). Пусть $G_0 = \mathrm{st}_\alpha(G) = (\mathrm{st}_\alpha(g_{i,j}))$ – стандартная часть матрицы G (это матрица с коэффициентами из $\overline{k}$). Следовательно, согласно (iii) определитель $\det(\mathrm{st}_\alpha(G)) \neq 0$. По (iii) и формуле для присоединённой матрицы $(E+H)G = G_0$, где E – единичная матрица и все ненулевые коэффициенты матрицы H являются элементами из $\overline{k_\alpha}$, которые являются бесконечно малыми относительно поля k. Существует $1 \leqslant i \leqslant m_3(m_1 - m_3) + 1$ такое, что

$$\det\begin{pmatrix} (A', 0)G_0^{-1} \\ A_{m_1,m_3,i} \end{pmatrix} = c\det(A'),$$

где $0 \neq c \in \overline{k}$. Тогда

$$\det\begin{pmatrix} A \\ A_{m_1,m_3,i} \end{pmatrix} = \det\begin{pmatrix} (A', 0)G_0^{-1}(E+H) \\ A_{m_1,m_3,i} \end{pmatrix} = c_1\det(A'),$$

где $0 \neq c_1 \in \overline{k_\alpha}$, и c_1, c_1^{-1} не является бесконечно большими относительно поля k. Следовательно, $\det(AC_{m_1,m_3,i}) = c_2\det(A')$, где $0 \neq c_2 \in \overline{k_\alpha}$, и c_2, c_2^{-1} не являются бесконечно большими относительно поля k. Согласно (iii) $\Delta/\det(A')$ не является бесконечно большим относительно поля k. Отсюда следует (ii). Лемма доказана. □

Пусть элемент $(c_1, \lambda_1, L^{(1)})$ задан при помощи (17, 18, 19), см. введение. Теперь мы будем предполагать без ограничения общности, что n_1 минимально возможное и, следовательно, $n_1 \leqslant \nu$, см. введение, и ν ограничено сверху полиномом от $r(d'+1)^n$, см. введение. Рассмотрим системы полиномиальных уравнений и неравенств с квадратами абсолютных величин, содержащие общие однородные многочлены. Напомним, что в [12, 13] предложен метод для решения таких систем (только общие линейные формы появлялись в [12, 13]). Сейчас мы собираемся усилить этот метод на случай системы, удовлетворяющей следующим условиям.

1) Коэффициенты всех уравнений и неравенств этой системы являются элементами из конечного расширения некоторого поля $k_\alpha = k(\varepsilon_1, \dots, \varepsilon_\alpha)$, см. раздел 1, где $\alpha = O(1)$.
2) Неизвестные этой системы суть $\tau_1, \dots, \tau_{n_1}$; $X_{i,j}$, $0 \leqslant j \leqslant n$, $1 \leqslant i \leqslant \nu_2$, где $\nu_2 = O(1)$ (рассматривается как константа, $\nu_2 < n$); и некоторые другие $O(n)$ переменных. Обозначим их через Y_γ, $\gamma \in \Gamma$.
3) Эта система содержит неравенство $\sum\limits_{1 \leqslant i \leqslant n_1} |\tau_i|^2 \leqslant \varepsilon_1$. Все другие уравнения и неравенства этой системы имеют коэффициенты в конечном расширении k' поля $k(\varepsilon_2, \dots, \varepsilon_\alpha)$.
4) Каждое уравнение или неравенство этой системы, за исключением $\sum\limits_{1 \leqslant i \leqslant n_1} |\tau_i|^2 \leqslant \varepsilon_1$, эквивалентно $A \geqslant 0$ или $A = 0$, где A принадлежит наименьшему классу функций, удовлетворяющему следующим свойствам. Этот класс замкнут относительно операций сложения двух функций, умножения двух функций, умножения функции на скаляр из $\overline{k(\varepsilon_2, \dots, \varepsilon_\alpha)}$. Для произвольной функции B из этого класса функция $|B|^2$ принадлежит этому классу. Наконец, этот класс содержит все скаляры из $\overline{k(\varepsilon_2, \dots, \varepsilon_\alpha)}$; функции $X_{i,j}$, $0 \leqslant j \leqslant n$, $1 \leqslant i \leqslant \nu_2$; $e_{1,n+1}(X_{i,0}, \dots, X_{i,n})$, см. (20); $L_{1,j}(X_{i,0}, \dots, X_{i,n})$, $s+1 \leqslant j \leqslant \sigma$; $e_w^{(1)}(X_{i,0}, \dots, X_{i,n})$, $w \in \{0, \sigma+1, \dots, n\}$, где $1 \leqslant i \leqslant \nu_2$; и Y_γ, $\gamma \in \Gamma$.

Обозначим через $(\star)$ рассматриваемую систему для краткости.

Теперь предположим, что для всякого $1 \leqslant i \leqslant \nu_2$ алгебраические многообразия $V^{(i)}$, $W^{(i)}$ аналогичны (и заданы аналогичным образом) многообразиям V, W из введения. Нас интересует имеет ли система $(\star)$ решение $\tau_w = \tau_w^*$, $X_{i,j} = x_{i,j}^*$, $Y_\gamma = y_\gamma^*$ такое, что все τ_w^*, $x_{i,j}^*$, y_γ^* являются элементами из $\overline{k_\alpha}$, и

$$(x_{i,0}^* : \ldots : x_{i,n}^*) \in W^{(i)}(\overline{k_\alpha}), \quad 1 \leqslant i \leqslant \nu_2. \tag{29}$$

Полное число переменных системы $(\star)$ может быть $\geqslant \mathcal{P}(r(d'+1)^n)$ для некоторого полинома $\mathcal{P}$. Следовательно, применяя общие алгоритмы для построения описанного решения таких систем, см. [15], теорему 2 [10], мы получаем оценку экспоненциальную от числа переменных, т.е., экспоненциальную от $\mathcal{P}(r(d'+1)^n)$ для времени работы разрешающего алгоритма и построения решения системы $(\star)$. Предлагаемый метод позволяет уменьшить число переменных и редуцировать время работы алгоритма.

Именно, пусть $1 \leqslant n_3 \leqslant \min\{n_1, \nu_2(n-s+2)\}$ – целое число. Пусть $B_{n_1,n_3,j}$, $C_{n_1,n_3,j}$, $1 \leqslant j \leqslant n_3(n_1-n_3)+1$, – матрицы, определённые в начале раздела. Положим

$$\begin{pmatrix} T_{1,n_3,j} \\ \vdots \\ T_{n_1,n_3,j} \end{pmatrix} = B^{-1}_{n_1,n_3,j} \begin{pmatrix} \tau_1 \\ \vdots \\ \tau_{n_1} \end{pmatrix}.$$

Для произвольной линейной формы $H = \sum_{1 \leqslant i \leqslant n_1} h_i \tau_i$ относительно τ_1, $\ldots, \tau_{n_1}$ представим $H = \sum_{1 \leqslant i \leqslant n_1} h_{i,n_3,j} T_{i,n_3,j}$ (следовательно, все $h_{i,n_3,j}$ – линейные формы от h_i с целыми коэффициентами). По определению положим

$$H_{n_3,j} = \sum_{1 \leqslant i \leqslant n_3} h_{i,n_3,j} T_{i,n_3,j}.$$

Таким образом, определены $e_{1,n+1,n_3,j}$; $L_{1,w_1,n_3,j}$, $s+1 \leqslant w_1 \leqslant \sigma$; $L^{(1)}_{w_2,n_3,j}$, $w_2 \in \{0, \sigma+1, \ldots, n\}$.

Заменим в системе $(\star)$ во всех уравнениях и неравенствах $e_{1,n+1}$; L_{1,w_1}; $e^{(1)}_{w_2}$ на $e_{1,n+1,n_3,j}$; $L_{1,w_1,n_3,j}$, $s+1 \leqslant w_1 \leqslant \sigma$; $e^{(1)}_{w_2,n_3,j}$, $w_2 \in \{0, \sigma+1, \ldots, n\}$ соответственно. Заменим неравенство $\sum_{1 \leqslant i \leqslant n_1} |\tau_i|^2 \leqslant \varepsilon_1$ на $\sum_{1 \leqslant i \leqslant n_3} |T_{i,n_3,j}|^2 \leqslant \varepsilon_1$. Заменим переменные $\tau_1, \ldots, \tau_{n_1}$ системы $(\star)$ на $T_{1,n_3,j}, \ldots, T_{n_3,n_3,j}$. Обозначим через $(\star, n_3, j)$ полученную систему. Следовательно, система $(\star, n_3, j)$ имеет $O(n)$ неизвестных $T_{1,n_3,j}, \ldots$, $T_{n_3,n_3,j}$; $X_{i,j}$, $0 \leqslant j \leqslant n$, $1 \leqslant i \leqslant \nu_2$; Y_γ, $\gamma \in \Gamma$.

Аналогично системе $(\star)$ мы будем рассматривать решение $T_{i,n_3,j} = T'_{i,n_3,j}$, $X_{i,j} = x^*_{i,j}$, $Y_\gamma = y^*_\gamma$ такое, что все $T'_{i,n_3,j}$, $x^*_{i,j}$, y^*_γ являются элементами из $\overline{k_\alpha}$ и выполняется (29).

Лемма 16. *Система $(\star)$ имеет решение над полем $\overline{k_\alpha}$, удовлетворяющее (29) тогда и только тогда, когда существует $0 \leqslant n_3 \leqslant \min\{n_1, \nu_2(n-s+2)\}$ и $1 \leqslant j \leqslant n_3(n_1-n_3)+1$ такое, что система*

$(\star, n_3, j)$ имеет решение над $\overline{k_\alpha}$, удовлетворяющее (29). Кроме того, используя доказательство леммы, для заданного решения системы $(\star, n_3, j)$ над полем $\overline{k_\alpha}$, удовлетворяющего (29), можно построить явно решение системы $(\star)$ над полем $\overline{k_\alpha}$, удовлетворяющее (29).

Доказательство. Предположим, что система $(\star, n_3, j)$ имеет решение над полем $\overline{k_\alpha}$, удовлетворяющее (29) для некоторых $0 \leqslant n_3 \leqslant \min\{n_1,\, \nu_2(n-s+2)\}$ и $1 \leqslant j \leqslant n_3(n_1-n_3)+1$. Положим $T'_{i,n_3,j}=0$ для всех $n_3+1 \leqslant i \leqslant n_1$. Тогда линейная система $T_{i,n_3,j}=T'_{i,n_3,j}$, $1 \leqslant i \leqslant n_1$, относительно $\tau_1,\dots,\tau_{n_1}$ имеет решение $\tau_i=\tau_i^* \in \overline{k(\varepsilon_2,\dots,\varepsilon_\alpha)}$, $1 \leqslant i \leqslant n_1$. Поэтому $\sum\limits_{1\leqslant i\leqslant n_1} |\tau_i|^2 \leqslant c\varepsilon_1$ для некоторого целого числа $c \neq 0$ с длиной записи $O(n_1)$. Теперь для того, чтобы получить решение системы $(\star)$, удовлетворяющее (29), достаточно осуществить замену $\varepsilon_1 \mapsto c^{-1}\varepsilon_1$. Таким образом, система $(\star)$ имеет решение над полем $\overline{k_\alpha}$, удовлетворяющее (29).

Обратно, предположим, что система $(\star)$ имеет решение, удовлетворяющее (29). Согласно 3) и принципу переноса, см. [17], можно предполагать без ограничения общности, что все τ_w^*, $x_{i,j}^*$, y_γ^* являются элементами из $\overline{k(\varepsilon_2,\dots,\varepsilon_\alpha)}$. Положим $e_{1,n+1}(x_{i,0}^*,\dots,x_{i,n}^*)=e_{1,n+1,i}^*$, $L_{1,j}(x_{i,0}^*,\dots,x_{i,n}^*)=L_{1,j,i}^*$, $e_w^{(1)}(x_{i,0}^*,\,\dots,x_{i,n}^*)=e_{w,i}^{(1,*)}$ для всех j,w,i. Следовательно, $e_{1,n+1,i}^*$, $L_{1,j,i}^*$, $e_{w,i}^{(1,*)}$ являются линейными формами от $\tau_1,\dots,\tau_{n_1}$ с коэффициентами из $\overline{k(\varepsilon_2,\dots,\varepsilon_n)}$. Пусть A является $((n-s+2)\nu_2\times n_1)$-матрицей, состоящей из коэффициентов из $\overline{k(\varepsilon_2,\dots,\varepsilon_n)}$ линейных форм $e_{1,n+1,i}^*$, $1\leqslant i\leqslant \nu_2$; $L_{1,j,i}^*$, $s+1\leqslant j\leqslant\sigma$, $1\leqslant i\leqslant\nu_2$; $e_{w,i}^{(1,*)}$, $w\in\{0,\sigma+1,\dots,n\}$, $1\leqslant i\leqslant\nu_2$. Положим $n_3=\operatorname{rank}(A)$. Следовательно, $0\leqslant n_3\leqslant\min\{n_1,\nu_2(n-s+2)\}$.

Применим лемму 15 (i) к матрице A с $m_1=n_1$, $m_2=\nu_2(n-s+2)$, $m_3=n_3$. Таким образом, матрицы $B_{n_1,n_3,j}$ и $C_{n_1,n_3,j}$ определены согласно этой лемме. В дальнейшем j фиксировано в доказательстве.

Положим $T_{i,n_3,j}^*=T_{i,n_3,j}(\tau_1^*,\dots,\tau_{n_1}^*)$ для всех $1\leqslant i\leqslant n_1$. Определим линейные формы $\widetilde{e}_{1,n+1,i}$, $\widetilde{L}_{1,w_1,i}$, $\widetilde{e}_{w_2,i}^{(1)}$ равенствами

$$\begin{aligned}
&\widetilde{e}_{1,n+1,i}(T_{1,n_3,j},\dots,T_{n_1,n_3,j})=e_{1,n+1,i}^*,\\
&\widetilde{L}_{1,w_1,i}(T_{1,n_3,j},\dots,T_{n_1,n_3,j})=L_{1,w_1,i}^*,\\
&\widetilde{e}_{w_2,i}^{(1)}(T_{1,n_3,j},\dots,T_{n_1,n_3,j})=e_{w_2,i}^{(1,*)}.
\end{aligned}$$

Положим

$$e^*_{1,n+1,i}(\tau^*_1,\dots,\tau^*_{n_1}) = l^*_{1,n+1,i}, L^*_{1,w_1,i}(\tau^*_1,\dots,\tau^*_{n_1}) = l^*_{1,w_1,i},$$
$$e^{(1,*)}_{w_2,i}(\tau^*_1,\dots,\tau^*_{n_1}) = l^{(1,*)}_{w_2,i}$$

для всех w_1, w_2, i.

Рассмотрим линейную систему относительно переменных $T_{1,n_3,j}$, …, $T_{n_1,n_3,j}$

$$\begin{cases} \widetilde{e}_{1,n+1,i}(T_{1,n_3,j},\dots,T_{n_1,n_3,j}) = l^*_{1,n+1,i}, & \\ \widetilde{L}_{1,w_1,i}(T_{1,n_3,j},\dots,T_{n_1,n_3,j}) = l^*_{1,w_1,i}, & s+1 \leqslant w_1 \leqslant \sigma,\ 1 \leqslant i \leqslant \nu_2, \\ \widetilde{e}^{(1)}_{w_2,i}(T_{1,n_3,j},\dots,T_{n_1,n_3,j}) = l^{(1,*)}_{w_2,i}, & w_2 \in \{0, \sigma+1,\dots,n\}, 1 \leqslant i \leqslant \nu_2. \end{cases} \tag{30}$$

Система (30) имеет решение $T_{i,n_3,j} = T^*_{i,n_3,j}$, $1 \leqslant i \leqslant n_1$. Представим матрицу $AB_{n_1,n_3,j} = (A', A'')$, где A' имеет n_3 столбцов. По лемме 15 мы имеем $A'' = A'Z$, где $Z = (z_{i,w})$, и каждый коэффициент $z_{i,w} \in \overline{k(\varepsilon_2,\dots,\varepsilon_\alpha)}$ не является бесконечно большим относительно поля k. Следовательно, существует также решение линейной системы (30) $T_{i,n_3,j} = T'_{i,n_3,j}$, $1 \leqslant i \leqslant n_3$, и $T_{i,n_3,j} = 0$, $n_3 + 1 \leqslant i \leqslant n_1$, где $T'_{i,n_3,j} = T^*_{i,n_3,j} + \sum\limits_{n_3+1 \leqslant w \leqslant n_1} z_{i,w} T^*_{w,n_3,j}$. Поэтому система $(\star, n_3, j)$ имеет решение над полем $\overline{k_\alpha}$, удовлетворяющее (29). Лемма доказана. $\square$

Замечание 11. В дальнейшем, применяя лемму 16 для рассматриваемых j и n_3, мы будем выяснять, верно ли, что система $(\star, n_3, j)$ имеет решение, и строить это решение, если оно существует, при помощи теоремы 2 [10] и теоремы 2 [9].

§3. Разрешающий алгоритм для свойства (∗)

Напомним, что свойство $(*)$ было определено во введении из [21]. В этом разделе задана точка $(c_1, \lambda_1, L^{(1)})$, удовлетворяющая $(**)$, см. введение. Следующие наблюдения будут использоваться в алгоритме для утверждения (e) из теоремы 2 [21], описанном в этом разделе и разделе 6 в следующей части. Предположим, что $k_i \subset K$ для некоторого i.

- Предположим, что $(c_4, \lambda_4, L^{(4)}) \in \mathcal{L}_{c_1,\lambda_1,L^{(1)}} \otimes \overline{k_i}$ удовлетворяет условиям леммы 1 [21] (вместо $(c_0, \lambda_0, L^{(0)})$). Тогда, используя алгоритмы из [4, 9], можно вычислить число элементов

$\#(e_{4,n+1}/e_0^{(4)})(A_{\lambda_4,L^{(4)}})$. В частности, это может быть сделано, если выполняются условия 1), 2) из $(*)$ для $(c_4,\lambda_4,L^{(4)})$.

- Предположим, что $(c_4,\lambda_4,L^{(4)}) \in \mathcal{L}_{c_1,\lambda_1,L^{(1)}} \otimes \overline{k_i}$ удовлетворяет условиям леммы 2 [21] (вместо $(c_0,\lambda_0,L^{(0)})$). Тогда, используя алгоритм из [10], можно вычислить $\deg W'(c_4,\lambda_4,L^{(4)})$. В частности, это может быть сделано, если выполняются условия 1)–3) из $(*)$ для $(c_4,\lambda_4,L^{(4)})$.
- Предположим, что $(c_4,\lambda_4,L^{(4)}) \in \mathcal{L}_{c_1,\lambda_1,L^{(1)}} \otimes \overline{k_i}$ удовлетворяет условиям леммы 2 [21] (в частности, это верно, если выполняются условия 1)–3) из $(*)$ для $(c_4,\lambda_4,L^{(4)})$), и $\deg W'(c_4,\lambda_4,L^{(4)}) = \deg W'(c_1,\lambda_1,L^{(1)})$. Тогда, см. определение 4 и лемму 3 [21], согласно алгоритмам из [4, 9, 10] можно вычислить $W'(c_4,\lambda_4,L^{(4)},*)$ и после этого $\deg W'(c_4,\lambda_4,\ L^{(4)},*)$.
- Предположим, что $(c_4,\lambda_4,L^{(4)}) \in \mathcal{L}_{c_1,\lambda_1,L^{(1)}} \otimes \overline{k_i}$ удовлетворяет условиям леммы 2 [21] и
$$\deg W'(c_4,\lambda_4,L^{(4)}) = \deg W'(c_1,\lambda_1,L^{(1)})$$
$$= \deg W'(c_4,\lambda_4,L^{(4)},*) = \deg W'(c_1,\lambda_1,L^{(1)},*)$$
(в частности, это верно, если свойство $(*)$ выполняется для $(c_4,\lambda_4,L^{(4)})$ и
$$\deg W'(c_4,\lambda_4,L^{(4)}) = \deg W'(c_1,\lambda_1,L^{(1)}),$$
$$\deg W'(c_4,\lambda_4,L^{(4)},*) = \deg W'(c_1,\lambda_1,L^{(1)},*)).$$
Тогда $\Phi_{c_4,\lambda_4,L^{(4)},*} = \Phi_{c_4,\lambda_4,L^{(4)},+}$ и, следовательно, согласно алгоритмам из [4,9,10] можно вычислить многочлены $\Phi_{c_4,\lambda_4,L^{(4)},*}$, $R_{c_4,\lambda_4,L^{(4)},*}$, и $R_{c_4,\lambda_4,L^{(4)},*,0}$. Поэтому также можно найти целое число $a(c_4,\lambda_4,L^{(4)})$.

Предположим, что выполнено свойство $(**)$, см. введение. Сначала наша цель выяснить, верно ли, что справедливы условия 1)–3) из $(*)$ для $(c_1,\lambda_1,L^{(1)})$. Если 1)–3) выполняются для $(c_1,\lambda_1,L^{(1)})$, то мы построим $(c_5,\lambda_5,L^{(5)})$ аналогичную $(c_3,\lambda_3,L^{(3)})$ и такую, что условия 1)–3) из $(*)$ выполняются для $(c_5,\lambda_5,L^{(5)})$. В дальнейшем в этом и следующих разделах мы будем предполагать, что $c_5,\lambda_5,L^{(5)}$ получаются подстановкой в (17, 19) значений $\tau_i = \tau_{5,i}$, $1 \leqslant i \leqslant n_1$.

Мы опишем рекурсивный алгоритм по $(c_5,\lambda_5,L^{(5)})$. В качестве базы рекурсии положим $(c_5,\lambda_5,L^{(5)}) = (c_3,\lambda_3,L^{(3)})$. Опишем общий шаг этой рекурсии. Вычислим $\deg p'_v \deg W'$ точек из множества

$S = A_{\lambda_5, L^{(5)}} = (W_{\lambda_5} \setminus \mathcal{Z}(e_0, \ldots, e_r)) \cap \mathcal{Z}(e^{(5)}_{\sigma+1}, \ldots, e^{(5)}_n)$. Свойства 1) и 2) из $(*)$ для $(c_5, \lambda_5, L^{(5)})$ влекут трансверсальность пересечения (22) с $j = 5$, см. лемму 13 (ii) [13]. Вычислим число элементов $\#(e_{5,n+1}/e^{(5)}_0)(S)$. Если $\#(e_{5,n+1}/e^{(5)}_0)(S) < \deg p'_v \deg W'$, то мы строим пару различных точек $x_1, x_2 \in S$ таких, что $(e_{5,n+1}/e^{(5)}_0)(x_1) \neq (e_{5,n+1}/e^{(5)}_0)(x_2)$. Построим линейную форму $L_{1,0} \in k[X_0, \ldots, X_n]$ с целыми коэффициентами с длинами записи $O(1)$ такую, что $L_{1,0}(x_j) \neq 0$ для $j = 1, 2$. Для краткости положим $X^{(j)} = (X_{j,0}, \ldots, X_{j,n})$, $j = 1, 2$, и для произвольного многочлена p от $X_0, \ldots, X_n$ обозначим $p(X^{(j)}) = p(X_{j,0}, \ldots, X_{j,n})$. Рассмотрим систему полиномиальных уравнений и неравенств относительно неизвестных $X_{j,0}, \ldots, X_{j,n}$, $j = 1, 2$; $\tau_1, \ldots, \tau_{n_1}$ с коэффициентами из поля $\overline{k_3}$

$$\left\{\begin{array}{ll} \sum\limits_{1 \leqslant i \leqslant n_1} |\tau_i|^2 \leqslant \varepsilon_1, & \\ \sum\limits_{0 \leqslant i \leqslant n} |X_{j,i} - (X_i/L_{1,0})(x_j) L_{1,0}|^2 \leqslant \varepsilon_2, & j = 1, 2, \\ \sum\limits_{0 \leqslant i \leqslant n} |(e_{5,n+1} - e_{0,n+1} + e_{1,n+1})(X^{(1)}) - & \\ (e_{5,n+1} - e_{0,n+1} + e_{1,n+1})(X^{(2)})|^2 \geqslant \varepsilon_3, & \\ (L_{5,i} - L_{0,i} + L_{1,i})(X^{(j)}) = 0, & s+1 \leqslant i \leqslant \sigma, j = 1, 2, \\ (e^{(5)}_w - e^{(0)}_w + e^{(1)}_w)(X^{(j)}) = 0, & \sigma+1 \leqslant w \leqslant n, j = 1, 2, \\ (e^{(5)}_0 - e^{(0)}_0 + e^{(1)}_0)(X^{(j)}) = 1, & j = 1, 2. \end{array}\right. \tag{31}$$

Лемма 17. *Если $(c_1, \lambda_1, L^{(1)})$ удовлетворяет условиям 1)–3) из $(*)$, то система (31) имеет решение $X_{j,w} = x^*_{j,w}$, $\tau_i = \tau^*_i$ в поле $\overline{k_3}$ такое, что*

$$(x^*_{j,0} : \ldots : x^*_{j,n}) \in W(\overline{k_3}), \quad j = 1, 2. \tag{32}$$

Доказательство. Существует элемент $\varepsilon' > 0$ такой, что ε' – бесконечно малая величина относительно поля k_2 и ε_3 – бесконечно малая величина относительно поля $k_2(\varepsilon')$. По принципу переноса, см. [17], достаточно построить решение системы (31) с $\overline{k(\varepsilon')}$ вместо $\overline{k_3}$ в (32). Положим в лемме 4 [21] элемент $(c_0, \lambda_0, L^{(0)})$ равным общей точке $(c_1, \lambda_1, L^{(1)})$ подпространства $\mathcal{L}_{c_1, \lambda_1, L^{(1)}}$ (здесь следует расширить основное поле k до $k(\tau_1, \ldots, \tau_{n_1})$). Применяя последовательно n_1 раз лемму 4 [21], мы получаем точку $(c_3, \lambda_3, L^{(3)}) \in \mathcal{L}_{c_1, \lambda_1, L^{(1)}}$, удовлетворяющую условиям 1)–3) из $(*)$ и такую, что она получается из $(c_1, \lambda_1, L^{(1)})$ подстановкой τ'_i вместо τ_i в [17–19]. Рассмотрим прямую

$\mathfrak{l}$, содержащую $(c_5, \lambda_5, L^{(5)})$ и $(c_3, \lambda_3, L^{(3)})$. Выберем точку $(c_*, \lambda_*, L^*) \in \mathfrak{l}(\overline{k(\varepsilon')})$, которая бесконечно близка к $(c_5, \lambda_5, L^{(5)})$. Пусть $\tau_i = \tau_i^*$, $1 \leqslant i \leqslant n_1$, соответствуют (c_*, λ_*, L^*). Тогда очевидно для рассматриваемых τ_i^*, $1 \leqslant i \leqslant n_1$, существует решение (32) системы (31) с $\overline{k(\varepsilon')}$ вместо $\overline{k_3}$. Лемма доказана. □

Отметим, что система (31) удовлетворяет условиям 1)–4) из раздела 2. Поэтому, применяя лемму 16 и замечание 11, мы выясняем, верно ли, что система (31) имеет решение, удовлетворяющее (32), и, если оно существует, строим такое решение. Предположим, что такого решения не существует. Тогда по лемме 17 точка $(c_1, \lambda_1, L^{(1)})$ не удовлетворяет 3), и, следовательно, $(*)$ не выполняется.

Предположим, что мы построили решение системы (31), удовлетворяющее (32). Подставляя в (17)–(19) и (20) $\tau_{5,i} + \tau_i^*$ вместо τ_i, $1 \leqslant i \leqslant n_1$, мы получаем точку (c_*, λ_*, L^*) и многочлен e_{n+1}^* с коэффициентами из подполя k' поля $\overline{k_3}$, где расширение $k' \supset k$ является конечно порождённым. Мы можем предполагать без ограничения общности, что $k' \subset \overline{K}$. Мы имеем $L^{(5)} \in \mathcal{U}_0''$, $A_{\lambda_5, L^{(5)}} \cap \mathcal{Z}(e_0^{(5)}) = \varnothing$ и $A_{\lambda_5, L^{(5)}} \cap \overline{V \setminus W} = \varnothing$ согласно 1) и 2). Поэтому $L^* \in \mathcal{U}_0''$ (где $\mathcal{U}_0''$ определено для основного поля $\overline{k'}$, см. замечание 2 [11]), $A_{\lambda_*, L^*} \cap \mathcal{Z}(e_0^*) = \varnothing$ и $A_{\lambda_*, L^*} \cap \overline{V \setminus W} = \varnothing$. Поскольку пересечение (22) трансверсально для $j = 5$, из теоремы о неявной функции следует, что пересечение (22) трансверсально с λ_*, L^* вместо λ_j, $L^{(j)}$, и $\# A_{\lambda_*, L^*} = \deg p_v' \deg W'$. Мы имеем $\#(e_{n+1}^*/e_0^*)(A_{\lambda_*, L^*}) > \#(e_{5,n+1}/e_0^{(5)})(A_{\lambda_5, L^{(5)}})$. Теперь выполнены условия леммы 4 [21] для (c_*, λ_*, L^*) вместо $(c_0, \lambda_0, L^{(0)})$.

По лемме 4 [21] и наблюдениям в начале раздела можно применить алгоритм редукции к целым коэффициентам, см. предложение 2 [10], и заменить последовательно все значения τ_i^* на целые числа τ_i' с длинами записи $O(n \log d + (n - \sigma) \log(d'))$. Обозначим через (c', λ, L') полученную точку. Тогда $L' \in \mathcal{U}_0''$, число элементов $\# A_{\lambda, L'} = \deg p_v' \deg W'$, $A_{\lambda, L'} \cap \mathcal{Z}(e_0') = \varnothing$, и $A_{\lambda, L'} \cap \overline{V \setminus W} = \varnothing$, размерности $\dim W_\lambda = n - \sigma$, $\dim(W_\lambda \setminus \mathcal{Z}(e_0, \ldots, e_r)) \cap \mathcal{Z}(e_{\sigma+1}', \ldots, e_{n-1}') = 1$, число элементов

$$\#(e_{n+1}'/e_0')(A_{\lambda, L'}) \geqslant \#(e_{n+1}^*/e_0^*)(A_{\lambda_*, L^*}) > \#(e_{5,n+1}/e_0^{(5)})(A_{\lambda_5, L^{(5)}}),$$

морфизмы $p_{\lambda, L'}$, $p_{\lambda, L', *}$ являются доминантными. Применим лемму 8 [21] к случаю, когда $\iota(\mathbb{A}^1(\overline{k}))$ является прямой, содержащей (c', λ, L') и $(c_5, \lambda_5, L^{(5)})$, и $\iota(0) = (c_5, \lambda_5, L^{(5)})$. Тогда, применяя теорему 1 (f) [12], лемму 8 и лемму 4 [21], мы строим точку (c'', λ', L'') аналогичную $(c_5, \lambda_5, L^{(5)})$ и такую, что $\#(e''_{n+1}/e''_0)(A_{\lambda', L''}) \geqslant \#(e'_{n+1}/e'_0)(A_{\lambda, L'}) > \#(e_{5,n+1}/e_0^{(5)})(A_{\lambda_5, L^{(5)}})$. После этого мы заменяем $(c_5, \lambda_5, L^{(5)})$ на (c'', λ', L'') и переходим к следующему шагу рекурсии. Таким образом, в конце мы придём к случаю, когда число элементов $\#(e_{5,n+1}/e_0^{(5)})(S) = \deg p'_v \deg W'$. Тогда $(c_1, \lambda_1, L^{(1)})$ и $(c_5, \lambda_5, L^{(5)})$ удовлетворяют условиям 1)–3). Этот шаг описываемой рекурсии является заключительным.

В дальнейшем мы будем предполагать без ограничения общности, что $(c_1, \lambda_1, L^{(1)})$ удовлетворяет условиям 1)–3). Сейчас мы опишем новую рекурсию по $(c_5, \lambda_5, L^{(5)})$. В качестве базы рекурсии мы возьмём построенную точку $(c_5, \lambda_5, L^{(5)})$. В конце этой рекурсии мы получим $(c_5, \lambda_5, L^{(5)})$ такую, что условия 1)–3) из $(*)$ выполняются для $(c_5, \lambda_5, L^{(5)})$ и $\deg W'(c_5, \lambda_5, L^{(5)}) = \deg W'(c_1, \lambda_1, L^{(1)})$.

Опишем общий шаг этой рекурсии. В начале шага задана точка $(c_5, \lambda_5,\ L^{(5)})$, удовлетворяющая условиям 1)–3) из $(*)$. Пусть морфизмы $r_{c_5, \lambda_5, L^{(5)}}$, $p_{c_5, \lambda_5, L^{(5)}}$, $q_{c_5, \lambda_5, L^{(5)}}$, $p_{\lambda_5, L^{(5)}}$ аналогичны морфизмам $r_{c_0, \lambda_0, L^{(0)}}$, $p_{c_0, \lambda_0, L^{(0)}}$, $q_{c_0, \lambda_0, L^{(0)}}$, $p_{\lambda_0, L^{(0)}}$, см. доказательство леммы 1 и введение [21]. Сначала наша цель построить линейно независимые линейные формы $\widetilde{L}_j \in k[X_0, \ldots,\ X_{n-\sigma}]$, $j \in \{0, \sigma+1, \ldots, n\}$ с целыми коэффициентами с длинами записи $O(n^2 \log(dd'))$ (дополнительно, применяя алгоритм редукции к целым коэффициентам, см. предложение 2 [10], можно получить оценку $O(n \log d + (n-\sigma)\log(d'))$, но это сейчас не принципиально) и целое число t с той же самой длиной записи, удовлетворяющие следующим условиям.

(i) $(n-\sigma+1)$-набор линейных форм $(\widetilde{L}_0,\ \widetilde{L}_{\sigma+1}, \ldots,\ \widetilde{L}_{n-1},\ \widetilde{L}_n + tX_{n-\sigma+1})$ удовлетворяет утверждению теоремы 1 [10] для морфизма $q_{c_5, \lambda_5, L^{(5)}}$ (вместо $(n-\sigma+1)$-набора L' для p'). Поэтому $\#W'(c_5, \lambda_5,\ L^{(5)}) \cap \mathcal{Z}(\widetilde{L}_{\sigma+1}, \ldots,\ \widetilde{L}_{n-1}, \widetilde{L}_n + tX_{n-\sigma+1}) = \deg W'(c_5, \lambda_5, L^{(5)})$, $W'(c_5, \lambda_5, L^{(5)}) \cap \mathcal{Z}(\widetilde{L}_{\sigma+1}, \ldots,\ \widetilde{L}_{n-1},\ \widetilde{L}_n + tX_{n-\sigma+1}) \cap \mathcal{Z}(\widetilde{L}_0) = \varnothing$ (здесь мы предполагаем, что $X_0, \ldots, X_{n-\sigma+1}$ являются координатными функциями на $\mathbb{P}^{n-\sigma+1}(\overline{k})$), для всякого
$$z \in W'(c_5, \lambda_5, L^{(5)}) \cap \mathcal{Z}(\widetilde{L}_{\sigma+1}, \ldots, \widetilde{L}_{n-1}, \widetilde{L}_n + tX_{n-\sigma+1})$$
обратный образ $q^{-1}_{c_5, \lambda_5, L^{(5)}}(z)$ состоит из одной точки z_1, и z_1 является гладкой точкой многообразия W_{λ_5}, см. [10].

(ii) Положим

$$L_j = \widetilde{L}_j(L_0^{(5)}, L_{\sigma+1}^{(5)}, \dots, L_n^{(5)}),$$

и $L = (L_0, L_{\sigma+1}, \dots, L_n)$, $j \in \{0, \sigma+1, \dots, n\}$. Тогда элемент (c_5, λ_5, L) удовлетворяет условиям 1)–3) из $(*)$.

(iii) Для всякого

$$z \in W'(c_5, \lambda_5, L^{(5)}) \cap \mathcal{Z}(\widetilde{L}_{\sigma+1}, \dots, \widetilde{L}_{n-1}, \widetilde{L}_n + tX_{n-\sigma+1})$$

положим $L_z = (L_0, L_{\sigma+1}, \dots, L_{n-1}, L_n - (\widetilde{L}_n/\widetilde{L}_0)(z)L_0)$. Тогда (c_5, λ_5, L_z) (вместо $(c_0, \lambda_0, L^{(0)})$) удовлетворяет условиям леммы 2 [21].

(iv) Положим $\eta_j^{(5)} = \widetilde{L}_j(e_0^{(5)}, e_{\sigma+1}^{(5)}, \dots, e_n^{(5)}) = L_j(e_0, \dots, e_r)$ для всех $j \in \{0, \sigma+1, \dots, n\}$. Для всякого

$$z \in W_{\lambda_5} \cap \mathcal{Z}(\eta_{\sigma+1}^{(5)}, \dots, \eta_{n-1}^{(5)}, \eta_n^{(5)} + te_{5,n+1}) \setminus \mathcal{Z}(e_0, \dots, e_r)$$

число элементов $\# p_{\lambda_5,L}^{-1} p_{\lambda_5,L}(z) = \deg p'_v \deg W'$, и пересечение $p_{\lambda_5,L}^{-1} p_{\lambda_5,L}(z) \cap (\overline{V \setminus W}) = \varnothing$. Поэтому по лемме 2 [10] дифференциал $d_z p_{\lambda_5,L}$ является изоморфизмом. Следовательно, снова по этой лемме и (i) дифференциалы $d_z q_{c_5,\lambda_5,L}$ являются изоморфизмами для всех рассматриваемых z. Отсюда следует, см. ниже, что дифференциалы $d_z q_{c_5,\lambda_5,L^{(5)}}$ являются изоморфизмами для всех рассматриваемых z.

Применяя теорему 1 [10] и замечание 2 [21] к морфизму $q_{c_5,\lambda_5,L^{(5)}}$, мы строим линейные формы $\widetilde{L}_j \in k[X_0, \dots, X_{n-\sigma}]$, $j \in \{0, \sigma+1, \dots, n\}$ и целое число t', удовлетворяющие (i) с t' вместо t. Согласно утверждению (d) теоремы 1 [10] мы будем предполагать без ограничения общности, что $\widetilde{L}_j$, $j \in \{0, \sigma+1, \dots, n\}$ являются линейно независимыми линейными формами. Рассмотрим замену $\widetilde{L}_0$ на $\widetilde{L}_0 + t''X_0$ и $\widetilde{L}_j$ на $\widetilde{L}_j + t''X_{j-\sigma}$, $j \in \{\sigma+1, \dots, n\}$, с целым числом t'' с длиной записи $O(n \log d + (n-\sigma)\log d')$. По теореме 1 (f) [12] и лемме 8 [21], используя такую замену с подходящим t'' (он строится при помощи перебора), мы будем предполагать без ограничения общности дополнительно, что элемент (c_5, λ_5, L) удовлетворяет (ii). Заметим, что морфизм $p_{\lambda_5,L}$ отличается от $p_{\lambda_5,L^{(5)}}$ только автоморфизмом проективного пространства $\mathbb{P}^{n-\sigma}(\overline{k})$. Аналогично $p_{c_5,\lambda_5,L}$ отличается от $p_{c_5,\lambda_5,L^{(5)}}$ только автоморфизмом проективного пространства $\mathbb{P}^{n-\sigma+1}(\overline{k})$. Поэтому алгебраическое многообразие $W'(c_5, \lambda_5, L)$ отличается от $W'(c_5, \lambda_5, L^{(5)})$

только автоморфизмом проективного пространства $\mathbb{P}^{n-\sigma+1}(\overline{k})$. Следовательно, $\deg W'(c_5,\lambda_5,L^{(5)}) = \deg W'(c_5,\lambda_5,L)$. Отметим также, что $W'(c_5,\ \lambda_5,L^{(5)}) = \mathcal{Z}(\Phi_{c_5,\lambda_5,L^{(5)}}(X_0,\dots,X_{n-\sigma+1}))$, $W'(c_5,\lambda_5,L) = \mathcal{Z}(\Phi_{c_5,\lambda_5,L}(X_0,\dots,X_{n-\sigma+1})))$ и

$$\Phi_{c_5,\lambda_5,L^{(5)}}(X_0,\dots,X_{n-\sigma+1}) = \mu\Phi_{c_5,\lambda_5,L}(\widetilde{L}_0,\widetilde{L}_{\sigma+1},\dots,\widetilde{L}_n,X_{n-\sigma+1}), \tag{33}$$

где $0\neq\mu\in\overline{k}$.

Теперь по (i) всякая неприводимая компонента многообразия $C_{\lambda_5,L} = W_{\lambda_5}\cap\mathcal{Z}(\eta^{(5)}_{\sigma+1},\dots,\ \eta^{(5)}_{n-1})\setminus\mathcal{Z}(e_0,\dots,e_r)$ является кривой. Согласно условиям 1)–3) из $(*)$ для (c_5,λ_5,L) морфизм $p_{\lambda_5,L,*}$ – доминантный, для всех точек $z\in C_{\lambda_5,L}$, за исключением самое большее полиномиального от $d^n(d')^{n-\sigma}$ числа, дифференциал $d_zp_{\lambda_5,L}$ является изоморфизмом, $\#p^{-1}_{\lambda_5,L}p_{\lambda_5,L}(z) = \deg p'_v\deg W'$, пересечение $p^{-1}_{\lambda_5,L}p_{\lambda_5,L}(z)\cap(\overline{V\setminus W}) = \varnothing$. Пусть $z\in C_{\lambda_5,L}$ и $z' = q_{c_5,\lambda_5,L^{(5)}}(z)$. Тогда по лемме 2 [21] для всех точек $z\in C_{\lambda_5,L}$, за исключением самое большее полиномиального от $d^n(d')^{n-\sigma}$ числа, точка $(c_5,\lambda_5,L_{z'})$ (вместо $(c_0,\lambda_0,L^{(0)})$) удовлетворяет условиям леммы 2 [21]. Заметим, что согласно [4] для всякого целого числа t можно вычислить алгебраическое многообразие $C_{\lambda_5,L}\cap\mathcal{Z}(\widetilde{e}_n+te_{5,n+1})$. Поэтому можно построить целое число t с длиной записи $O(n^2\log(dd'))$ такое, что выполняются (i) и (ii), многообразие $C_{\lambda_5,L}\cap\mathcal{Z}(\widetilde{e}_n+te_{5,n+1})$ является нульмерным, и выполняются условия (iii) и (iv). Таким образом требуемые линейные формы $\widetilde{L}_j$ и целое число t построены.

Для краткости положим $\eta_j = \widetilde{L}_j(e^{(5)}_0 - e^{(0)}_0 + e^{(1)}_0,\ e^{(5)}_{\sigma+1} - e^{(0)}_{\sigma+1} + e^{(1)}_{\sigma+1},\dots,\ e^{(5)}_n - e^{(0)}_n + e^{(1)}_n)$, $j\in\{0,\sigma+1,\dots,n\}$. Пусть $\tau^*_i\in\overline{K}$ – произвольные (в дальнейшем мы будем предполагать, что $K\supset k_3$). Определим $(c_*,\lambda_*,L^*)\in\mathcal{L}_{c_1,\lambda_1,L^{(1)}}\otimes\overline{K}$, подставляя в (17)–(19) значения $\tau_i = \tau_{5,i}+\tau^*_i$, $1\leqslant i\leqslant n_1$. Пусть $\lambda_* = (L_{*,s+1},\dots,L_{*,\sigma})$, $L^* = (L^*_0,L^*_{\sigma+1},\dots,L^*_n)$, $e^*_j = L^*_j(e_0,\dots,e_r)$, $j\in\{0,\sigma+1,\dots,n\}$. Положим $\eta^*_j = \widetilde{L}_j(e^*_0,e^*_{\sigma+1},\dots,e^*_n)$, $j\in\{0,\sigma+1,\dots,n\}$. Таким образом, $\eta^*_j = \eta_j|_{\tau_i=\tau^*_i,\,1\leqslant i\leqslant n_1}$ и $\eta^{(5)}_j = \eta_j|_{\tau_i=0,\,1\leqslant i\leqslant n_1}$. Положим $\overline{L}_j = \widetilde{L}_j(L^*_0,L^*_{\sigma+1},\dots,L^*_n)$, $j\in\{0,\sigma+1,\dots,n\}$, и $\overline{L} = (\overline{L}_0,\overline{L}_{\sigma+1},\dots,\overline{L}_n)$. Поэтому $\eta^*_j = \overline{L}_j(e_0,\dots,e_r)$ для всех $j\in\{0,\sigma+1,\dots,n\}$.

Рассмотрим систему уравнений и неравенств относительно неизвестных $X_0,\dots,X_n,Y_{\sigma+1},\dots,Y_n,\tau_1,\dots,\tau_{n_1}$ с коэффициентами из поля

k_2

$$
\left\{
\begin{array}{ll}
\sum\limits_{1\leqslant i\leqslant n_1} |\tau_i|^2 \leqslant \varepsilon_1, & \\
\eta_j - Y_j\eta_0 = 0, & \sigma+1\leqslant j\leqslant n-1, \\
\eta_n - Y_n\eta_0 + & \\
+t(e_{5,n+1} - e_{0,n+1} + e_{1,n+1}) = 0, & \\
\eta_0 = 1, & \\
L_{5,j} - L_{0,j} + L_{1,j} = 0, & s+1\leqslant j\leqslant \sigma, \\
\sum\limits_{\sigma+1\leqslant i\leqslant n} |Y_i|^2 \leqslant \varepsilon_2, & \\
\sum\limits_{0\leqslant i\leqslant n} |e_i|^2 \geqslant \varepsilon_2^{-1}. &
\end{array}
\right.
\tag{34}
$$

Лемма 18. *Предположим, что $(c_1, \lambda_1, L^{(1)})$ удовлетворяет условиям* 1)–3) *из* $(*)$, *справедливы условия* (i)–(iv), $\deg W'(c_1,\ \lambda_1, L^{(1)}) > \deg W'(c_5, \lambda_5,\ L^{(5)})$. *Тогда система* (34) *имеет решение $X_w = x_w^*$, $0\leqslant w\leqslant n$; $\tau_i = \tau_i^*$, $1\leqslant i\leqslant n_1$; $Y_j = y_j^*$, $\sigma+1\leqslant j\leqslant n$, в поле $\overline{k_2}$ такое, что*

$$
(x_0^* : \ldots : x_n^*) \in W(\overline{k_2}). \tag{35}
$$

Для произвольного решения (35) *системы* (34) *точка (c_*, λ_*, L^*) удовлетворяет условиям леммы* 2 *[21] (вместо $(c_0, \lambda_0, L^{(0)})$) и* $\deg W'(c_*, \lambda_*, L^*) > \deg W'(c_5, \lambda_5, L^{(5)})$.

Доказательство. Очевидно достаточно доказать эту лемму с k_3 вместо k_2. Положим $S' = W'(c_5, \lambda_5, L^{(5)}) \cap \mathcal{Z}(\widetilde{L}_{\sigma+1}, \ldots, \widetilde{L}_{n-1}, \widetilde{L}_n + tX_{n+1})$. Пусть $\tau_i^*, y_j^* \in \overline{k_3}$, $1\leqslant i\leqslant n_1$, $\sigma+1\leqslant j\leqslant n$ является произвольными (не обязательно относящимися к решению системы (34)) такими, что $\sum\limits_{1\leqslant i\leqslant n_1} |\tau_i^*|^2 \leqslant \varepsilon_1$ и $\sum\limits_{\sigma+1\leqslant j\leqslant n} |y_j^*|^2 \leqslant \varepsilon_2$. Заметим, что согласно наблюдениям в начале раздела 1 [21] точка (c_*, λ_*, L^*) удовлетворяет (D) и условиям леммы 2 [21]. Следовательно, определены объекты q_{c_*,λ_*,L^*}, $W'(c_*, \lambda_*, L^*)$ и т.д. Пусть $z \in S'$ и $q_{c_5,\lambda_5,L^{(5)}}(z_1) = z$, см. (i).

Покажем, что для всякого $z \in S'$ существует единственная точка $z^* \in S^* = W'(c_*, \lambda_*, L^*) \cap \mathcal{Z}(\widetilde{L}_{\sigma+1} - y_{\sigma+1}^*\widetilde{L}_0, \ldots, \widetilde{L}_{n-1} - y_{n-1}^*\widetilde{L}_0, \widetilde{L}_n - y_n^*\widetilde{L}_0 + tX_{n+1})$ такая, что $q_{c_*,\lambda_*,L^*}^{-1}(z^*)$ содержит точку z_1^*, которая бесконечно близка к z_1 (поэтому также z^* является бесконечно близкой к z). Заметим, что по (i) $\widetilde{L}_{\sigma+1}/\widetilde{L}_0, \ldots, \widetilde{L}_{n-1}/\widetilde{L}_0, (\widetilde{L}_n+tX_{n+1})/\widetilde{L}_0$ порождают линейное пространство $\mathfrak{m}_z/\mathfrak{m}_z^2$, где $\mathfrak{m}_z$ является максимальным идеалом локального кольца $\mathcal{O}_{z,W'(c_5,\lambda_5,L^{(5)})}$ алгебраического многообразия $W'(c_5,\lambda_5,L^{(5)})$ в точке z. По (iv) дифференциал $d_{z_1}q_{c_5,\lambda_5,L^{(5)}}$ является изоморфизмом. Следовательно, двойственное отображение к $d_{z_1}q_{c_5,\lambda_5,L^{(5)}}$ также является изоморфизмом

$$\eta^{(5)}_{\sigma+1}/\eta^{(5)}_0, \ldots, \eta^{(5)}_{n-1}/\eta^{(5)}_0, (\eta^{(5)}_n + te_{5,n+1})/\eta^{(5)}_0$$

порождает линейное пространство $\mathfrak{m}_{z_1}/\mathfrak{m}_{z_1}^2$, где $\mathfrak{m}_{z_1}$ – максимальный идеал локального кольца $\mathcal{O}_{z_1,W_{\lambda_5}}$ алгебраического многообразия W_{λ_5} в точке z_1. Поэтому z_1 является гладкой точкой гиперповерхностей $\mathcal{Z}(\eta^{(5)}_j)$, $\sigma+1 \leqslant j \leqslant n-1$; $\mathcal{Z}(\eta^{(5)}_n + te_{5,n+1})$, и пересечение касательных пространств алгебраических многообразий W_{λ_5},$\mathcal{Z}(\eta^{(5)}_{\sigma+1})$,…, $\mathcal{Z}(\eta^{(5)}_{n-1})$, $\mathcal{Z}(\eta^{(5)}_n + te_{5,n+1})$ в точке z_1 трансверсально.

С другой стороны, по лемме 13 (ii) и (iii) [13] пересечение $W \cap \mathcal{Z}(L_{5,s+1}, \ldots, L_{5,\sigma}) \cap \mathcal{Z}(\eta^{(5)}_{\sigma+1}, \ldots, \eta^{(5)}_{n-1}, \eta^{(5)}_n - (\widetilde{L}_n/\widetilde{L}_0)(z)\eta^{(5)}_0)$ трансверсально в точке z_1. Поэтому пересечение $W \cap \mathcal{Z}(L_{5,s+1}, \ldots, L_{5,\sigma})$ также трансверсально в точке z_1. Следовательно, пересечение

$$W \cap \mathcal{Z}(L_{5,s+1}, \ldots, L_{5,\sigma}) \cap \mathcal{Z}(\eta^{(5)}_{\sigma+1}) \cap \ldots \cap \mathcal{Z}(\eta^{(5)}_{n-1}) \cap \mathcal{Z}(\eta^{(5)}_n + te_{5,n+1})$$

трансверсально в точке z_1. Наконец, по теореме о неявной функции существует только одна точка $z_1^* \in q^{-1}_{c_*,\lambda_*,L^*}(S^*)$ такая, что z_1^* бесконечно близка к z_1. Требуемое утверждение доказано. $\square$

Теперь предположим, что $y \in S^*$, $q_{c_*,\lambda_*,L^*}(y_1) = y$, и y_1 не является бесконечно близкой к $\mathcal{Z}(e_0, \ldots, e_r)$. Тогда очевидно y_1 бесконечно близка к $q^{-1}_{c_5,\lambda_5,L^{(5)}}(S')$ и, поэтому y является бесконечно близкой к S'. Обратно предположим, что y_1 бесконечно близка к $\mathcal{Z}(e_0, \ldots, e_r)$. Покажем, что y не является бесконечно близкой к S'. Действительно, предположим противное, что y бесконечно близка к $z \in S'$. Следовательно, $\widetilde{L}_0(y) \neq 0$. Положим $\overline{L}_y = (\overline{L}_0, \overline{L}_{\sigma+1}, \ldots, \overline{L}_{n-1}, \overline{L}_n - (\widetilde{L}_n/\widetilde{L}_0)(y)\overline{L}_0)$. Заметим, что коэффициенты линейных форм из $\overline{L}_y$ являются бесконечно близкими к коэффициентам, соответствующих линейных форм из L_z, см. условие (iii). По свойству (D) для (c_5, λ_5, L_z), см. (iii), пересечение $(W \setminus \mathcal{Z}(e_0, \ldots, e_r)) \cap \mathcal{Z}(L_{5,s+1}, \ldots, L_{5,\sigma}) \cap \mathcal{Z}(\eta^{(5)}_{\sigma+1}) \cap \ldots \cap \mathcal{Z}(\eta^{(5)}_{n-1}) \cap \mathcal{Z}(\eta^{(5)}_n - (\widetilde{L}_n/\widetilde{L}_0)(z)\eta^{(5)}_0) = A_{\lambda_5,L_z}$ трансверсально и состоит из $\deg p'_v \deg W'$

точек. По лемме 13 [13] и теореме о неявной функции пересечение $(W\setminus\mathcal{Z}(e_0,\ldots,e_r))\cap\mathcal{Z}(L_{*,s+1},\ldots,L_{*,\sigma})\cap\mathcal{Z}(\eta^*_{\sigma+1})\cap\ldots\cap\mathcal{Z}(\eta^*_{n-1})\cap\mathcal{Z}(\eta^*_n-(\widetilde{L}_n/\widetilde{L}_0)(y)\eta^*_0)=A_{\lambda_*,\overline{L}_y}$ трансверсально и состоит из $\deg p'_v\deg W'$ точек. По теореме о неявной функции точки из $A_{\lambda_*,\overline{L}_y}$ бесконечно близки к соответствующим точкам из A_{λ_5,L_z}. Но согласно (i) $q^{-1}_{c_5,\lambda_5,L^{(5)}}(z)$ состоит из одно точки, и $q^{-1}_{c_5,\lambda_5,L^{(5)}}(z)\subset A_{\lambda_5,L_z}$, $q^{-1}_{c_*,\lambda_*,L^*}(y)\subset A_{\lambda_*,\overline{L}_y}$. Поэтому $q^{-1}_{c_*,\lambda_*,L^*}(y)$ также состоит из одной точки, которая бесконечно близка к точке из $q^{-1}_{c_5,\lambda_5,L^{(5)}}(z)$. Таким образом, y_1 не является бесконечно близкой к $\mathcal{Z}(e_0,\ldots,e_r)$. Данное противоречие доказывает требуемое утверждение.

Покажем, что $\widetilde{L}_0$ не обращается в нуль тождественно ни на какой неприводимой компонентой многообразия $W'(c_*,\lambda_*,L^*)$. Действительно, по (ii) каждая неприводимая компонента многообразия W_{λ_5} содержит точку из $A_{\lambda_5,L}$, и $\eta_0^{(5)}$ не обращается в нуль ни в какой точке из $A_{\lambda_5,L}$. Отметим, что коэффициенты линейных форм $\overline{L}_j$ являются бесконечно близкими к соответствующим коэффициентам линейных форм L_j, $j\in\{0,\sigma+1,\ldots,n\}$. Следовательно, по лемме 13 [13] и теореме о неявной функции, см. последнее наблюдение, относящееся к свойству (D), в начале раздела 1 [21], каждая неприводимая компонента многообразия W_{λ_*} содержит точку из $A_{\lambda_5,\overline{L}}$, и $\eta^*_0=\widetilde{L}_0(e^*_0,e^*_{\sigma+1},\ldots,e^*_n)$ не обращается в нуль ни в какой точке из $A_{\lambda_5,\overline{L}}$. Следовательно, каждая неприводимая компонента многообразия $W'(c_*,\lambda_*,L^*)$ содержит точку из $q_{c_*,\lambda_*,L^*}(A_{\lambda_5,\overline{L}})$, и $\widetilde{L}_0$ не обращается в нуль ни в какой точке из $q_{c_*,\lambda_*,L^*}(A_{\lambda_5,\overline{L}})$. Отсюда следует требуемое утверждение.

Докажем существование требуемого решения системы (34). По лемме 4 [21] и алгоритму редукции к целым коэффициентам, ср. доказательство существования (c_*,λ_*,L^*) в лемме 17, существуют $\tau^*_i\in k(\varepsilon_3)$, которые являются бесконечно малыми величинами относительно поля k такими, что (c_*,λ_*,L^*) удовлетворяет условиям леммы 4 [21] (для любой прямой $\mathfrak{l}$, содержащей (c_*,λ_*,L^*)) вместо $(c_0,\lambda_0,L^{(0)})$, и $\deg W'(c_*,\lambda_*,L^*)=\deg W'(c_1,\lambda_1,L^{(1)})$. Мы имеем $\deg W'(c_*,\lambda_*,L^*)>\deg W'(c_5,\lambda_5,L^{(5)})$. Поэтому, как мы только что доказали, из теоремы Безу следует существование точки $z\in W'(c_*,\lambda_*,L^*)\cap\mathcal{Z}(\widetilde{L}_{\sigma+1},\ldots,\widetilde{L}_{n-1},\widetilde{L}_n+tX_{n-\sigma+1})$, которая не является бесконечно близкой к S'. Далее, существует точка $y\in W'(c_*,\lambda_*,L^*)$ с координатами из

$\overline{k(\varepsilon_3)}$ такая, что y бесконечно близка к z относительно поля k, обратный образ $q^{-1}_{c_*,\lambda_*,L^*}(y) \neq \emptyset$ и $\widetilde{L}_0(y) \neq 0$. Положим $y^*_j = (\widetilde{L}_j/\widetilde{L}_0)(y)$ для $\sigma+1 \leqslant j \leqslant n-1$ и $y^*_n = ((\widetilde{L}_n + tX_{n-\sigma+1})/\widetilde{L}_0)(y)$. Тогда всякое ненулевое $y^*_j \in \overline{k(\varepsilon_3)}$, $j \in \{\sigma+1,\ldots,n\}$, является бесконечно малым относительно поля k. Пусть $y_1 \in q^{-1}_{c_*,\lambda_*,L^*}(y)$. Согласно предыдущим рассуждениям точка y_1 бесконечно близка к $\mathcal{Z}(e_0,\ldots,e_r)$. Таким образом, система (34) имеет решение, удовлетворяющее (35) (с k_3 вместо k_2).

Обратно, если (34) имеет решение, удовлетворяющее (35), то по предыдущим рассуждениям и теореме Безу

$$\deg W'(c_*,\lambda_*,L^*) > \deg W'(c_5,\lambda_5,L^{(5)}).$$

Лемма доказана.

Вернёмся к описанию общего шага рассматриваемой рекурсии. Заметим, что система (34) удовлетворяет условиям 1)–4) из раздела 2. Поэтому, используя лемму 16 и замечание 11, мы выясняем, верно ли, что система (34) имеет решение, удовлетворяющее (35), и, если такое решение существует, строим его. Предположим, что такого решения не существует. Тогда по лемме 18 степень $\deg W'(c_1,\lambda_1,L^{(1)}) = \deg W'(c_5,\lambda_5,L^{(5)})$ и рассматриваемый шаг является заключительным.

Предположим, что мы построили решение системы (34), удовлетворяющее (35), см. формулировку леммы 18. Тогда $\deg W'(c_*,\lambda_*,L^*) > \deg W'(c_5,\ \lambda_5,L^{(5)})$ по этой лемме. Аналогично предыдущей рекурсии условия леммы 4 [21] выполнены для (c_*,λ_*,L^*) вместо $(c_0,\lambda_0,L^{(0)})$. По лемме 4 [21] и наблюдениям в начале раздела можно применить алгоритм редукции к целым коэффициентам, см. предложение 2 [10], и заменить последовательно все значения τ^*_i на целые числа τ'_i с длинами записи $O(n\log d + (n-\sigma)\log(d'))$. Обозначим через (c',λ,L') полученную точку. Тогда $L' \in \mathcal{U}''_0$, число элементов $\#A_{\lambda,L'} = \deg p'_v \deg W'$, $A_{\lambda,L'} \cap \mathcal{Z}(e'_0) = \varnothing$, и $A_{\lambda,L'} \cap \overline{V \setminus W} = \varnothing$, размерности $\dim W_\lambda = n-\sigma$, $\dim(W_\lambda \setminus \mathcal{Z}(e_0,\ldots,e_r)) \cap \mathcal{Z}(e'_{\sigma+1},\ldots,e'_{n-1}) = 1$, число элементов $\#(e'_{n+1}/e'_0)(A_{\lambda,L'}) = \#(e_{5,n+1}/e^{(5)}_0)(A_{\lambda_5,L^{(5)}})$, морфизмы $p_{\lambda,L'}$, $p_{\lambda,L',*}$ являются доминантными, и $\deg W'(c',\lambda,L') \geqslant \deg W'(c_*,\lambda_*,L^*)$. Применим лемму 8 [21] к случаю, когда $\iota(\mathbb{A}^1(\overline{k}))$ является прямой, содержащей (c',λ,L') и $(c_5,\lambda_5,L^{(5)})$, и $\iota(0) = (c_5,\lambda_5,L^{(5)})$. Тогда, применяя теорему 1 (f) [12], лемму 8 и лемму 4 [21], мы строим точку (c'',λ',L''), которая аналогична $(c_5,\lambda_5,L^{(5)})$, и $\deg W'(c'',\lambda',L'') \geqslant \deg W'(c',\lambda,L') > \deg W'(c_5,\lambda_5,L^{(5)})$. После этого мы заменяем $(c_5,\lambda_5,L^{(5)})$ на (c'',λ',L'')

и переходим к следующему шагу рекурсии. Общий шаг и вся рекурсия описаны.

Теперь мы опишем ещё одну рекурсию. В качестве базы рекурсии мы возьмём построенную точку $(c_5, \lambda_5, L^{(5)})$. В конце этой рекурсии мы получим точку $(c_5, \lambda_5, L^{(5)})$ такую, что условия 1)–3) из $(*)$ выполняются для $(c_5, \lambda_5, L^{(5)})$ и $\deg W'(c_5, \lambda_5, L^{(5)}) = \deg W'(c_1, \lambda_1, L^{(1)})$, $\deg W'(c_5, \lambda_5, L^{(5)}, *) = \deg W'(c_1, \lambda_1, L^{(1)}, *)$.

Опишем общий шаг этой рекурсии. В начале шага дана $(c_5, \lambda_5, L^{(5)})$, удовлетворяющая условиям 1)–3) из $(*)$, и $\deg W'(c_5, \lambda_5, L^{(5)}) = \deg W'(c_1, \lambda_1, L^{(1)})$. Применяя алгоритм из [4] вычислим, см. наблюдения в начале раздела, многообразие $W'(c_5, \lambda_5, L^{(5)}, *)$ и многочлен $\Phi_{c_5,\lambda_5,L^{(5)},+}$, см. лемму 3 [21]. Следовательно,

$$W'(c_5, \lambda_5, L^{(5)}, *) = \mathcal{Z}(\Phi_{c_5,\lambda_5,L^{(5)},+}(X_0, X_1, X_2))$$

по лемме 3 [21]. Согласно свойствам 1) и 2) из $(*)$ для $(c_5, \lambda_5, L^{(5)})$ пересечение $(W_{\lambda_5} \setminus \mathcal{Z}(e_0, \ldots, e_r)) \cap \mathcal{Z}(e^{(5)}_{\sigma+1}) \cap \ldots \cap \mathcal{Z}(e^{(5)}_n) = A_{\lambda_5,L^{(5)}}$ трансверсально в каждой его точке, состоит из $\deg p'_v \deg W'$ изолированных точек, и $A_{\lambda_5,L^{(5)}} \cap \mathcal{Z}(e^{(5)}_0) = \varnothing$. По свойству 3) из $(*)$, см. [21], и лемме 2 [10] пересечение $W'(c_5, \lambda_5, L^{(5)}) \cap \mathcal{Z}(X_1, \ldots, X_{n-\sigma})$ также трансверсально в каждой точке из $q_{c_5,\lambda_5,L^{(5)}}(A_{\lambda_5,L^{(5)}})$, число элементов $\#q_{c_5,\lambda_5,L^{(5)}}(A_{\lambda_5,L^{(5)}}) = \deg p'_v \deg W'$, и для всякого $z \in A_{\lambda_5,L^{(5)}}$ дифференциал $d_z q_{c_5,\lambda_5,L^{(5)}}$ является изоморфизмом.

Определим морфизмы $r_{c_5,\lambda_5,L^{(5)},*}$, $p_{\lambda_5,L^{(5)},*}$, $q_{c_5,\lambda_5,L^{(5)},*}$ подобно морфизмам $r_{c_0,\lambda_0,L^{(0)},*}$, $p_{\lambda_0,L^{(0)},*}$, $q_{c_0,\lambda_0,L^{(0)},*}$, см. доказательство леммы 3 и введение [21]. По лемме 11 [10] всякая неприводимая компонента многообразия $(W_{\lambda_5} \setminus \mathcal{Z}(e_0, \ldots, e_r)) \cap \mathcal{Z}(e^{(5)}_{\sigma+1}, \ldots, e^{(5)}_{n-1}) = C_{\lambda_5,L^{(5)}}$ содержит точку из $A_{\lambda_5,L^{(5)}}$. Следовательно, пересечение

$$(W_{\lambda_5} \setminus \mathcal{Z}(e_0, \ldots, e_r)) \cap \mathcal{Z}(e^{(5)}_{\sigma+1}) \cap \ldots \cap \mathcal{Z}(e^{(5)}_{n-1}) \tag{36}$$

трансверсально, каждая неприводимая компонента многообразие $C_{\lambda_5,L^{(5)}}$ является кривой, и многообразие $W'(c_5, \lambda_5, L^{(5)}, *)$ является объединением всех неприводимых компонент E пересечения $W'(c_5, \lambda_5, L^{(5)}) \cap \mathcal{Z}(X_1, \ldots, X_{n-\sigma-1})$ таких, что $E \cap q_{c_5,\lambda_5,L^{(5)}}(A_{\lambda_5,L^{(5)}}) \neq \varnothing$. Поэтому пересечение $W'(c_5, \lambda_5, L^{(5)}) \cap \mathcal{Z}(X_1, \ldots, X_{n-\sigma-1})$ трансверсально во всякой неприводимой компоненте E многообразия

$W'(c_5, \lambda_5, L^{(5)}, *)$. Мы имеем

$$\begin{aligned}\deg p_{\lambda_5, L^{(5)}, *} &= \deg r_{c_5, \lambda_5, L^{(5)}, *} = \deg p_{\lambda_5, L^{(5)}}\\ &= \deg r_{c_5, \lambda_5, L^{(5)}} = \deg p'_v \deg W'.\end{aligned}$$

Следовательно, морфизм $q_{c_5, \lambda_5, L^{(5)}, *}$ индуцирует изоморфизм алгебр рациональных функций на $C_{\lambda_5, L^{(5)}}$ и $W'(c_5, \lambda_5, L^{(5)}, *)$ соответственно (по определению эти алгебры изоморфизмы прямым произведениям полей рациональных функций всех неприводимых компонент кривой $C_{\lambda_5, L^{(5)}}$ и $W'(c_5, \lambda_5, L^{(5)}, *)$ соответственно). Аналогично $q_{c_5, \lambda_5, L^{(5)}}$ индуцирует бирациональный изоморфизм. Далее, $q_{c_5, \lambda_5, L^{(5)}, *}$ (соответственно $q_{c_5, \lambda_5, L^{(5)}}$) является изоморфизмом в окрестности относительно топологии Зарисского конечного множества $A_{\lambda_5, L^{(5)}}$. Пусть $z \in W'(c_5, \lambda_5, L^{(5)}, *)$ и $X_0(z) \neq 0$. Положим

$$L_z^{(5)} = (L_0^{(5)}, L_{\sigma+1}^{(5)}, \ldots, L_{n-1}^{(5)}, L_n^{(5)} - (X_{n-\sigma}/X_0)(z) L_0^{(5)}).$$

Пусть $z \in C_{\lambda_5, L^{(5)}}$ и $z' = q_{c_5, \lambda_5, L^{(5)}}(z)$. Тогда по теореме Безу (мы оставляем подробности читателю) для всех $z \in C_{\lambda_5, L^{(5)}}$, за исключением самое большее полиномиального от $d^n (d')^{n-\sigma}$ числа, морфизмы $q_{c_5, \lambda_5, L^{(5)}, *}$ и $q_{c_5, \lambda_5, L^{(5)}}$ являются изоморфизмами в некоторых окрестностях точки z относительно топологии Зарисского, $z \notin \overline{V \setminus W}$, пересечение (36) трансверсально в точке z (в частности, z является гладкой точкой кривой $C_{\lambda_5, L^{(5)}}$), число элементов $\# p^{-1}_{\lambda_5, L^{(5)}} p_{\lambda_5, L^{(5)}}(z) = \deg p'_v \deg W'$, $e_0^{(5)}(z) \neq 0$, элемент $(c_5, \lambda_5, L_{z'}^{(5)})$ удовлетворяет условиям леммы леммы 2 [21] (вместо $(c_0, \lambda_0, L^{(0)})$).

Пусть t', t'' – целые числа. Положим $B_{\lambda_5, L^{(5)}} = C_{\lambda_5, L^{(5)}} \cap \mathcal{Z}(e_0^{(5)} + t' e_n^{(5)} + t'' e_{5,n+1})$ в $\mathbb{P}^n(\overline{k})$. Напомним, что мы знаем явно многочлен $\Phi_{c_5, \lambda_5, L^{(5)}, +}$. Следовательно, можно построить целые числа t', t'' с длинами записи ограниченными сверху $O(n \log d + (n-\sigma) \log(d'))$ такие, что:

(v) для всякого $z \in B_{\lambda_5, L^{(5)}}$ морфизм $q_{c_5, \lambda_5, L^{(5)}, *}$ (соответственно $q_{c_5, \lambda_5, L^{(5)}}$) является изоморфизмом в окрестности относительно топологии Зарисского точки z,

(vi) для всякого $z \in B_{\lambda_5, L^{(5)}}$ число элементов $\# p^{-1}_{\lambda_5, L^{(5)}} p_{\lambda_5, L^{(5)}}(z) = \deg p'_v \deg W'$.

(vii) для всякого $z \in B_{\lambda_5, L^{(5)}}$ пересечение (36) трансверсально в точке z,

(viii) $q_{c_5,\lambda_5,L^{(5)}}(B_{\lambda_5,L^{(5)}}) = W'(c_5,\lambda_5,L^{(5)},*) \cap \mathcal{Z}(X_0+t'X_1+t''X_2)$, число элементов $\#q_{c_5,\lambda_5,L^{(5)}}(B_{\lambda_5,L^{(5)}}) = \deg W'(c_5,\lambda_5,L^{(5)},*)$, и $q_{c_5,\lambda_5,L^{(5)}}(B_{\lambda_5,L^{(5)}}) \cap \mathcal{Z}(X_0) = \varnothing$,

(ix) для всякого $z \in q_{c_5,\lambda_5,L^{(5)}}(B_{\lambda_5,L^{(5)}})$ элемент $(c_5,\lambda_5,L^{(5)}_z)$ удовлетворяет условиям леммы 2 [21] (вместо $(c_0,\lambda_0,L^{(0)})$).

Рассмотрим систему уравнений и неравенств относительно неизвестных $X_0,\dots,X_n$, Y_0, $\tau_1,\dots,\tau_{n_1}$ с коэффициентами из поля k_2

$$\left\{\begin{array}{ll}
\sum\limits_{1\leqslant i\leqslant n_1} |\tau_i|^2 \leqslant \varepsilon_1, & \\
e^{(5)}_j - e^{(0)}_j + e^{(1)}_j = 0, & \sigma+1\leqslant j\leqslant n-1,\\
e^{(5)}_0 - e^{(0)}_0 + e^{(1)}_0 + & \\
+t'(e^{(5)}_n - e^{(0)}_n + e^{(1)}_n) + & \\
+t''(e_{5,n+1} - e_{0,n+1} + e_{1,n+1}) = Y_0, & \\
e^{(5)}_0 - e^{(0)}_0 + e^{(1)}_0 = 1, & \\
L_{5,j} - L_{0,j} + L_{1,j} = 0, & s+1\leqslant j\leqslant \sigma,\\
|Y_0|^2 \leqslant \varepsilon_2, & \\
\sum\limits_{0\leqslant i\leqslant n} |e_i|^2 \geqslant \varepsilon_2^{-1}. &
\end{array}\right. \tag{37}$$

Лемма 19. *Предположим, что* $(c_1,\lambda_1,L^{(1)})$ *удовлетворяет условиям* 1)–4) *из* $(*)$, *выполняются условия* (v)–(ix), $\deg W'(c_1,\lambda_1,L^{(1)}) = \deg W'(c_5,\ \lambda_5,L^{(5)})$, $\deg W'(c_1,\lambda_1,L^{(1)},*) > \deg W'(c_5,\lambda_5,L^{(5)},*)$. *Тогда система* (34) *имеет решение* $X_w = x^*_w$, $0\leqslant w\leqslant n$; $\tau_i=\tau^*_i$, $1\leqslant i\leqslant n_1$; $Y_0 = y^*_0$, *из поля* $\overline{k_2}$ *такое, что*

$$(x^*_0:\ldots:x^*_n) \in W(\overline{k_2}). \tag{38}$$

Для произвольного решения (38) *системы* (37) *точка* (c_*,λ_*,L^*) *удовлетворяет условиям леммы* 2 *cite21* (*вместо* $(c_0,\lambda_0,L^{(0)})$), $\deg W'(c_1,\lambda_1,L^{(1)}) = \deg W'(c_5,\lambda_5,L^{(5)})$ *и*

$$\deg W'(c_*,\lambda_*,L^*) > \deg W'(c_5,\lambda_5,L^{(5)}).$$

Доказательство. Очевидно достаточно доказать эту лемму с полем k_3 вместо k_2. Для краткости положим $S' = q_{c_5,\lambda_5,L^{(5)}}(B_{\lambda_5,L^{(5)}})$ (в доказательстве этой леммы обозначения S' и S^* отличны от обозначений, введённых в доказательстве леммы 18, но они имеют аналогичный смысл). Пусть $\tau^*_i, y^*_0 \in \overline{k_3}$, $1\leqslant i\leqslant n_1$, являются произвольными (но не обязательно относящимися к решению системы (37)) такими, что

$\sum_{1 \leqslant i \leqslant n_1} |\tau_i^*|^2 \leqslant \varepsilon_1$ и $|y_0^*|^2 \leqslant \varepsilon_2$. Заметим, что согласно наблюдениям в начале раздела 1 [21] точка (c_*, λ_*, L^*) удовлетворяет (D) и условиям леммы 2 [21]. Следовательно, определены объекты q_{c_*,λ_*,L^*}, $W'(c_*, \lambda_*, L^*)$ и т.д. Пусть $z \in S'$ и $q_{c_5,\lambda_5,L^{(5)}}(z_1) = z$.

Покажем, что для всякой точки $z \in S'$ существует единственная $z^* \in S^* = W'(c_*, \lambda_*, L^*, *) \cap \mathcal{Z}(X_0 + t'X_1 + t''X_2 - y_0^* X_0)$ такая, что $q^{-1}_{c_*,\lambda_*,L^*}(z^*)$ содержит точку z_1^*, которая бесконечно близка к z_1 (поэтому также z^* бесконечно близка к z). Отметим, что по (v) и (viii) пересечение $C_{\lambda_5,L^{(5)}} \cap \mathcal{Z}(e_0^{(5)} + t'e_n^{(5)} + t''e_{5,n+1})$ трансверсально в точке z_1. Следовательно, по (vii) пересечение $(W_{\lambda_5} \setminus \mathcal{Z}(e_0, \ldots, e_r)) \cap \mathcal{Z}(e^{(5)}_{\sigma+1}) \cap \ldots \cap \mathcal{Z}(e^{(5)}_{n-1}) \cap \mathcal{Z}(e_0^{(5)} + t'e_n^{(5)} + t''e_{5,n+1})$ трансверсально в точке z_1 (в частности, z_1 является гладкой точкой всех рассматриваемых многообразий).

С другой стороны, по лемме 13 (ii) и (ix) [13] пересечение $W \cap \mathcal{Z}(L_{5,s+1}, \ldots, L_{5,\sigma}) \cap \mathcal{Z}(e^{(5)}_{\sigma+1}, \ldots, e^{(5)}_{n-1}, e_n^{(5)} - (X_{n-\sigma}/X_0)(z)e_0^{(5)})$ трансверсально в точке z_1. Поэтому пересечение $W \cap \mathcal{Z}(L_{5,s+1}, \ldots, L_{5,\sigma})$ также трансверсально в точке z_1. Следовательно, пересечение $W \cap \mathcal{Z}(L_{5,s+1}, \ldots, L_{5,\sigma}) \cap \mathcal{Z}(e^{(5)}_{\sigma+1}) \cap \ldots \cap \mathcal{Z}(e^{(5)}_{n-1}) \cap \mathcal{Z}(e_0^{(5)} + t'e_n^{(5)} + t''e_{5,n+1})$ трансверсально в точке z_1. Наконец, по теореме о неявной функции существует только одна точка $z_1^* \in q^{-1}_{c_*,\lambda_*,L^*,*}(S^*)$ такая, что z_1^* бесконечно близка к z_1. Требуемое утверждение доказано. □

Теперь предположим, что $y \in S^*$, $q_{c_*,\lambda_*,L^*,*}(y_1) = y$ и y_1 не является бесконечно близкой к $\mathcal{Z}(e_0, \ldots, e_r)$. Тогда очевидно y_1 бесконечно близка к $q^{-1}_{c_5,\lambda_5,L^{(5)},*}(S')$ и, поэтому y бесконечно близка к S'. Обратно, предположим, что y_1 бесконечно близка к $\mathcal{Z}(e_0, \ldots, e_r)$. Покажем, что y не является бесконечно близкой к S'. Действительно, предположим противное, что y бесконечно близка к $z \in S'$. Следовательно, $X_0(y) \neq 0$. Положим $L_y^* = (L_0^*, \ldots, L_{n-1}^*, L_n^* - (X_{n-\sigma}/X_0)(y)L_0^*)$. Тогда ненулевые коэффициенты линейных форм L_y^* бесконечно близки к коэффициентам соответствующих линейных форм из $L_z^{(5)}$.

Согласно свойству (D) для $(c_5, \lambda_5, L_z^{(5)})$, см. (ix), пересечение

$$
\begin{aligned}
&(W \setminus \mathcal{Z}(e_0, \ldots, e_r)) \cap \mathcal{Z}(L_{5,s+1}, \ldots, L_{5,\sigma}) \cap \mathcal{Z}(e^{(5)}_{\sigma+1}) \cap \ldots \cap \mathcal{Z}(e^{(5)}_{n-1}) \\
&\cap \mathcal{Z}(e_n^{(5)} - (X_{n-\sigma}/X_0)(z)e_0^{(5)}) = A_{\lambda_5, L_z^{(5)}}
\end{aligned}
$$

трансверсально и состоит из $\deg p'_v \deg W'$ точек. По лемме 13 [13] и теореме о неявной функции пересечение

$$(W \setminus \mathcal{Z}(e_0, \ldots, e_r)) \cap \mathcal{Z}(L_{*,s+1}, \ldots, L_{*,\sigma}) \cap \mathcal{Z}(e^*_{\sigma+1}) \cap \ldots \cap \mathcal{Z}(e^*_{n-1})$$
$$\cap \mathcal{Z}(e^*_n - (X_{n-\sigma}/X_0)(y)e^*_0) = A_{\lambda_*, L^*_y}$$

трансверсально и состоит из $\deg p'_v \deg W'$ точек. По теореме о неявной функции точки из A_{λ_*, L^*_y} бесконечно близки к соответствующим точкам из A_{λ_5, L_z}. Но согласно (v) $q^{-1}_{c_5,\lambda_5,L^{(5)}}(z)$ состоит из одной точки. Далее, прообраз $q^{-1}_{c_5,\lambda_5,L^{(5)}}(z) \subset A_{\lambda_5, L^{(5)}_z}$, $q^{-1}_{c_*,\lambda_*,L^*}(y) \subset A_{\lambda_*, L^*_y}$. Поэтому $q^{-1}_{c_*,\lambda_*,L^*}(y)$ также состоит из одной точки, которая бесконечно близка к точке из $q^{-1}_{c_5,\lambda_5,L^{(5)}}(z)$. Таким образом, y_1 не является бесконечно близкой к $\mathcal{Z}(e_0, \ldots, e_r)$. Это противоречие доказывает требуемое утверждение.

Покажем, что X_0 не обращается в нуль тождественно ни на какой неприводимой компонентой многообразия $W'(c_*, \lambda_*, L^*, *)$. Действительно, как мы видели, каждая неприводимая компонента многообразия $C_{\lambda_5, L^{(5)}}$ содержит точку из $A_{\lambda_5, L^{(5)}}$, и $e^{(5)}_0$ не обращается в нуль ни в какой точке из $A_{\lambda_5, L^{(5)}}$. Заметим, что коэффициенты линейных форм L^*_j бесконечно близки к соответствующим коэффициентам линейных форм $L^{(5)}_j$, $j \in \{0, \sigma+1, \ldots, n\}$. Следовательно, по лемме 13 [13] и теореме о неявной функции, см. наблюдения, относящиеся к свойству (D) в начале раздела 1 [21], каждая неприводимая компонента многообразия $(W_{\lambda_*} \setminus \mathcal{Z}(e_0, \ldots, e_r)) \cap \mathcal{Z}(e^*_{s+1}, \ldots, e^*_\sigma)$ содержит точку из A_{λ_*, L^*}, и $e^*_0 = \widetilde{L}_0(e^*_0, e^*_{\sigma+1}, \ldots, e^*_n)$ не обращается в нуль ни в какой точке из A_{λ_*, L^*}. Следовательно, всякая неприводимая компонента многообразия $W'(c_*, \lambda_*, L^*, *)$ содержит точку из $q_{c_*,\lambda_*,L^*,*}(A_{\lambda_*, L^*})$, и X_0 не обращается в нуль ни в какой точке из $q_{c_*,\lambda_*,L^*,*}(A_{\lambda_*, L^*})$. Требуемое утверждение доказано.

Докажем существование требуемого решения системы (37). По лемме 4, лемме 6 [21] и алгоритму редукции к целым коэффициентам, ср. доказательство существования (c_*, λ_*, L^*) в лемме 17, существуют $\tau^*_i \in k(\varepsilon_3)$, которые являются бесконечно малыми величинами относительно поля k или нулями такие, что (c_*, λ_*, L^*) удовлетворяет условиям леммы 4, леммы 6 [21] (для прямой $\mathfrak{l}$, содержащей (c_*, λ_*, L^*)) вместо $(c_0, \lambda_0, L^{(0)})$, и $\deg W'(c_*, \lambda_*, L^*) = \deg W'(c_1, \lambda_1, L^{(1)})$, $\deg W'(c_*, \lambda_*,$

$L^*, *) = \deg W'(c_1, \lambda_1, L^{(1)}, *)$. Мы имеем

$$\deg W'(c_*, \lambda_*, L^*, *) > \deg W'(c_5, \lambda_5, L^{(5)}, *).$$

Поэтому, как мы доказали, из теоремы Безу вытекает существование точки $z \in W'(c_*, \lambda_*, L^*, *) \cap \mathcal{Z}(X_0 + t'X_1 + t''X_2)$, которая не является бесконечно близкой к S'. Далее, существует точка $y \in W'(c_*, \lambda_*, L^*, *)$ с координатами из $\overline{k(\varepsilon_3)}$ такая, что y бесконечно близка к z относительно поля k, обратный образ $q^{-1}_{c_*, \lambda_*, L^*, *}(y) \neq \varnothing$ и $X_0(y) \neq 0$. Положим $y_0^* = ((X_0 + t'X_1 + t''X_2)/X_0)(y)$. Тогда $y_0^* \in \overline{k(\varepsilon_3)}$ бесконечно мала относительно поля k. Пусть $y_1 \in q^{-1}_{c_*, \lambda_*, L^*, *}(y)$. Согласно предыдущим рассуждениям точка y_1 бесконечно близка к $\mathcal{Z}(e_0, \ldots, e_r)$. Таким образом, система (37) имеет решение, удовлетворяющее (38) (с k_3 вместо k_2).

Обратно, если (37) имеет решение, удовлетворяющее (38), то согласно предыдущим рассуждениям и теореме Безу $\deg W'(c_*, \lambda_*, L^*, *) > \deg W'(c_5, \lambda_5, L^{(5)}, *)$. Лемма доказана.

Вернёмся к описанию общего шага рассматриваемой рекурсии. Заметим, что система (37) удовлетворяет условиям 1)–4) из раздела 2. Следовательно, применяя лемму 16 и замечание 11, мы выясним, верно ли, что система (37) имеет решение, удовлетворяющее (38), и, если такое решение существует, то мы строим его. Предположим, что такого решения не существует. Тогда по лемме 19 степень $\deg W'(c_1, \lambda_1, L^{(1)}, *) = \deg W'(c_5, \lambda_5, L^{(5)}, *)$ и рассматриваемый шаг является последним. В этом случае мы можем выяснить верно ли, что $\deg W'(c_1, \lambda_1, L^{(1)}) = \deg W'(c_1, \lambda_1, L^{(1)}, *)$. Если $\deg W'(c_1, \lambda_1, L^{(1)}) \neq \deg W'(c_1, \lambda_1, L^{(1)}, *)$, то условие 4) из $(*)$ не выполняется для $(c_1, \lambda_1, L^{(1)})$, и поэтому $(*)$ также не выполняется для $(c_1, \lambda_1, L^{(1)})$. Если $\deg W'(c_1, \lambda_1, L^{(1)}) = \deg W'(c_1, \lambda_1, L^{(1)}, *)$, то условие 4) из $(*)$ справедливо для $(c_1, \lambda_1, L^{(1)})$, и, следовательно, $(*)$ также выполняется для $(c_1, \lambda_1, L^{(1)})$.

Предположим, что мы построили решение системы (37), удовлетворяющее (38), см. формулировку леммы 19. Тогда степень $\deg W'(c_*, \lambda_*, L^*, *) > \deg W'(c_5, \lambda_5, L^{(5)}, *)$ по этой лемме. Аналогично предыдущим рекурсиям условия леммы 4 [21] и леммы 6 [21] выполняются для (c_*, λ_*, L^*) вместо $(c_0, \lambda_0, L^{(0)})$. Согласно лемме 4, лемме 6 [21] и наблюдениям в начале раздела можно применить алгоритм редукции к целым коэффициентам, см. [10], предложение 2, и заменить последовательно все τ_i^* на целые числа τ_i' с длинами записи $O(n\log d + (n-\sigma)\log(d'))$. Обозначим через (c',λ,L') полученную точку. Тогда $L' \in \mathcal{U}_0''$, число элементов $\#A_{\lambda,L'} = \deg p_v' \deg W'$, $A_{\lambda,L'} \cap \mathcal{Z}(e_0') = \varnothing$, и $A_{\lambda,L'} \cap \overline{V\setminus W} = \varnothing$, размерности $\dim W_\lambda = n-\sigma$, $\dim(W_\lambda \setminus \mathcal{Z}(e_0,\dots,e_r)) \cap \mathcal{Z}(e'_{\sigma+1},\dots,e'_{n-1}) = 1$, число элементов $\#(e'_{n+1}/e'_0)(A_{\lambda,L'}) = \#(e_{5,n+1}/e_0^{(5)})(A_{\lambda_5,L^{(5)}})$, морфизмы $p_{\lambda,L'}$, $p_{\lambda,L',*}$ являются доминантными, $\deg W'(c',\lambda,L') = \deg W'(c_5,\lambda_5,L^{(5)})$, и $\deg W'(c',\lambda,L',*) \geqslant \deg W'(c_*,\lambda_*,L^*,*)$. Применим лемму 8 [21] к случаю, когда $\iota(\mathbb{A}^1(\overline{k}))$ является прямой, содержащей (c',λ,L') и $(c_5,\lambda_5,L^{(5)})$, и $\iota(0) = (c_5,\lambda_5,L^{(5)})$. Тогда, пользуясь теоремой 1 (f) [12], леммой 8 и леммой 4, леммой 6 [21], мы строим точку (c'',λ',L''), которая аналогична $(c_5,\lambda_5,L^{(5)})$, и такую, что

$$\deg W'(c'',\lambda',L'',*) \geqslant \deg W'(c',\lambda,L',*) > \deg W'(c_5,\lambda_5,L^{(5)},*).$$

После этого мы заменяем $(c_5,\lambda_5,L^{(5)})$ на (c'',λ',L'') и переходим к следующему шагу рекурсии. Общий шаг и вся рекурсия описаны. Разрешающий алгоритм для свойства $(*)$ полностью описан. Требуемая оценка на время работы этого алгоритма (она такая же, как и для утверждения (e) теоремы 2, см. введение [21]) следует немедленно из оценок на времена работы использованных алгоритмов.

§4. Монодромия и неприводимость

Бóльшая часть этого раздела и его обозначения независимы от предыдущих разделов и введения. Пусть $n \geqslant 1$ и $1 \leqslant s \leqslant n$ – целые числа. Пусть k – произвольное поле нулевой характеристики, V_s – определённое над k проективное алгебраическое многообразие в $\mathbb{P}^n(\overline{k})$, $1 \leqslant s \leqslant n-1$, и все неприводимые компоненты многообразия V_s имеют одну и ту же размерность $n-s$, т.е. V_s является равноразмерностным. Пусть $T_0, T_{s+1}, T_{s+2},\dots,T_{n+1}$ – линейные формы от $X_0,\dots,X_n$ с коэффициентами из k. Рассмотрим определённые над k морфизмы

$$\begin{aligned} &p : V_s \setminus \mathcal{Z}(T_0,T_{s+1},T_{s+2},\dots,T_n) \to \mathbb{P}^{n-s}(\overline{k}),\\ &(X_0:\dots:X_n) \mapsto (T_0 : T_{s+1} : T_{s+2} : \dots : T_n), \qquad (39)\\ &p' : V_s \setminus \mathcal{Z}(T_0,T_{s+1},T_{s+2},\dots,T_{n+1}) \to \mathbb{P}^{n-s+1}(\overline{k}),\\ &(X_0:\dots:X_n) \mapsto (T_0 : T_{s+1} : T_{s+2} : \dots : T_{n+1}) \qquad (40)\end{aligned}$$

(не следует путать эти морфизмы p и p' с морфизмами из введения). В этом разделе мы будем предполагать, что $T_0, T_{s+1}, T_{s+2}, \dots, T_n$, (соответственно $T_0, T_{s+1}, T_{s+2}, \dots, T_{n+1}$) являются координатными функциями в $\mathbb{P}^{n-s}(\overline{k})$, (соответственно $\mathbb{P}^{n-s+1}(\overline{k})$). Мы будем предполагать, что морфизм p является доминантным, т.е., по определению для всякой неприводимой компоненты W многообразия V_s ограничение $p|_W$ является доминантным морфизмом. Тогда замыкание в топологии Зарисского

$$\overline{p'(V_s \setminus \mathcal{Z}(T_0, T_{s+1}, T_{s+2}, \dots, T_{n+1}))} = \mathcal{Z}(\Phi),$$

где $\Phi \in k[T_0, T_{s+1}, T_{s+2}, \dots, T_{n+1}]$ – однородный ненулевой сепарабельный многочлен, который однозначно определён с точностью до ненулевого множителя из k. Мы фиксируем Φ. Обозначим через $q : V_s \setminus \mathcal{Z}(T_0, T_{s+1}, T_{s+2}, \dots, T_n) \to \mathcal{Z}(\Phi)$ морфизм, индуцированный (40). Обозначим через $k(V_s)$ и $k(\mathcal{Z}(\Phi))$ алгебры определённых над k рациональных функций на V_s и $\mathcal{Z}(\Phi)$ соответственно (по определению эти алгебры изоморфны прямым произведениям полей рациональных функций всех определённых над k компонент V_s и $\mathcal{Z}(\Phi)$ соответственно). Мы будем предполагать, что морфизм q является бирациональным изоморфизмом в том смысле, что он индуцирует изоморфизм сепарабельных алгебр $k(\mathcal{Z}(\Phi)) \simeq k(V_s)$. Пусть $r : \mathcal{Z}(\Phi) \setminus \mathcal{Z}(T_0, T_{s+1}, T_{s+2}, \dots, T_n) \to \mathbb{P}^{n-s}(\overline{k})$ – морфизм линейной проекции на координаты $T_0, T_{s+1}, T_{s+2}, \dots, T_n$. Следовательно, $p = r \circ q$. Морфизм r определён над k.

По определению степень $\deg p$ морфизма p равна степени расширения алгебр рациональных функций

$$[k(V_s) : k(\mathbb{P}^{n-s}(\overline{k}))] = \dim_{k(\mathbb{P}^{n-s}(\overline{k}))} k(V_s).$$

Аналогично определяется степень произвольного доминантного морфизма. В частности, определена $\deg r$. Мы имеем $\deg p = \deg r = \deg_{T_{n+1}} \Phi$, поскольку q является бирациональным морфизмом. Обратно, если $\deg p = \deg_{T_{n+1}} \Phi$, то q – бирациональный морфизм. Положим $\deg p = D$. Следовательно, целое число $D \geqslant 1$.

Обозначим через

$$R = \mathrm{Res}_{T_{n+1}}(\Phi, \partial\Phi/\partial T_{n+1}) \in k[T_0, T_{s+1}, T_{s+2}, \dots, T_n]$$

дискриминант относительно T_{n+1} многочлена Φ, см. замечание выше об определении дискриминанта в введении. Следовательно, $0 \neq$

R является однородным относительно $T_0, T_{s+1}, T_{s+2}, \dots, T_n$ многочленом. Пусть R_0 – бесквадратная часть полинома R, т.е. R_0 сепарабелен и $\mathcal{Z}(R) = \mathcal{Z}(R_0)$. Многочлен R_0 однозначно определён с точностью до ненулевого множителя из k. Мы выбираем и фиксируем R_0. Пусть $\Phi_D \in k[T_0, T_{s+1}, \dots, T_n]$ равен коэффициенту при T_{n+1}^D многочлена Φ. Следовательно, Φ_D делит R.

Обозначим через $A^{(s)}$ множество всех изолированных точек многообразия $V_s \cap \mathcal{Z}(T_{s+1}, \dots, T_n)$ в $\mathbb{P}^n(\overline{k})$. Рассмотрим условие

$$A^{(s)} \cap \mathcal{Z}(T_0) = \varnothing, \ \& \ \#(T_{n+1}/T_0)(A^{(s)}) = \deg p. \tag{41}$$

Пусть $T_0, T_{s+1}, T_{s+2}, \dots, T_{n+1}$ – произвольные линейные формы с коэффициентами из поля k такие, что p является доминантным и выполнено условие (41) (мы не предполагаем сейчас заранее, что q бирационален). Тогда по лемме 2 [10] морфизм q является бирациональным изоморфизмом. Мы будем предполагать до конца доказательства теоремы 3, что p является доминантным и выполняется условие (41).

Лемма 20. *Пусть V_s, p, q, D и Φ, Φ_D – такие же, как и выше. Предположим, что для точки $z \in \mathbb{P}^{n-s}(\overline{k}) \setminus \mathcal{Z}(T_0, T_{s+1}, \dots, T_n)$, число элементов $\#p^{-1}(z) = D$. Тогда $\Phi_D(z) \neq 0$.*

Доказательство. Доказательство этой леммы аналогично доказательству леммы 2 [21] с $d' = 1$. Достаточно заменить в лемме 2 [21] объекты W, $p_{\lambda,L'}$, $r_{c',\lambda,L'}$, $q_{c',\lambda,L'}$ на V_s, p, q, r. Единственное отличие здесь состоит в том, что многообразие V_s не обязательно неприводимо над k. Лемма доказана. $\square$

Предположим, что морфизм p – регулярный доминантный и конечный. Тогда $p'(V_s) = q(V_s) = \mathcal{Z}(\Phi)$, $\deg \Phi = \deg_{T_{n+1}} \Phi = D$, $\deg p = \deg V_s = \deg q(V_s) = D$, и морфизмы q и r – также конечные. В этом случае мы выбираем старший коэффициент $\mathrm{lc}_{T_{n+1}} \Phi = 1$. Теперь $A^{(s)} = V_s \cap \mathcal{Z}(T_{s+1}, \dots, T_n)$. Рассмотрим условие

$$\begin{aligned} A^{(s)} = V_s \cap \mathcal{Z}(T_{s+1}, \dots, T_n), \& \ A^{(s)} \cap \mathcal{Z}(T_0) \\ = \varnothing, \& \ \#(T_{n+1}/T_0)(A^{(s)}) = \deg V_s. \end{aligned} \tag{42}$$

Если $T_0, T_{s+1}, T_{s+2}, \dots, T_{n+1}$ – произвольные линейные формы с коэффициентами из k, удовлетворяющие условию (42) (мы не предполагаем сейчас, что p является доминантным и q бирационален), то морфизм p является регулярным доминантным конечным и q является бирациональным конечным, см. например, раздел 2 [5]. Кроме того, из (42) следует, что $\#A^{(s)} = D$ и пересечение $V_s \cap \mathcal{Z}(T_{s+1}, \dots, T_n)$ трансверсально в каждой точке по теореме Безу. Условие (41) является следствием (42).

Для произвольного многочлена $g \in \overline{k}[T_0, T_{s+1}, \dots, T_{n+1}]$ положим $g_* = g(T_0, 0, \dots, 0,\ T_n, T_{n+1})$. Мы будем предполагать в дальнейшем, что $R_{0,*}$ является ненулевым. Далее, предполагаем без ограничения общности, что T_0 не делит $R_{0,*}$, заменяя, если это необходимо, T_0 на $T_0 + \lambda T_n$ с подходящим целым числом λ. Поскольку $R_{0,*} \neq 0$, то многочлен $\Phi_{D,*} \neq 0$. Поэтому $\deg_{T_{n+1}} \Phi_* = \deg_{T_{n+1}} \Phi$. Пусть $\varphi \in k[T_0, T_n]$ равен наибольшему общему делителю коэффициентов при T_{n+1}^j, $0 \leqslant j \leqslant D$, многочлена Φ_*. Полином φ однозначно определён с точностью до ненулевого множителя из k. Выберем и зафиксируем φ. Положим $\Phi_+ = \Phi_*/\varphi$, $R_+ = R_*/\varphi^{2D-1}$. Следовательно, $\deg_{T_{n+1}} \Phi_+ = \deg_{T_{n+1}} \Phi$.
Замечание 12. Фактически по лемме 11 [10] равенство $\deg_{T_{n+1}} \Phi = \deg_{T_{n+1}} \Phi_+$ следует непосредственно из (41)

Отождествим $\mathcal{Z}(T_{s+1}, \dots, T_{n-1}) \subset \mathbb{P}^n(\overline{k})$ (соответственно $\subset \mathbb{P}^{n-s+1}(\overline{k})$, $\subset \mathbb{P}^{n-s}(\overline{k})$) с $\mathbb{P}^{s+1}(\overline{k})$ (соответственно $\mathbb{P}^2(\overline{k})$, $\mathbb{P}^1(\overline{k})$). Обозначим через $V_{s,+}$ объединение всех неприводимых компонент W пересечения $V_s \cap \mathcal{Z}(T_{s+1}, \dots,\ T_{n-1}) \subset \mathbb{P}^{s+1}(\overline{k})$ таких, что $W \not\subset \mathcal{Z}(g)$ для всякого $0 \neq g \in k[T_0, T_n]$. Повторим описанную конструкцию для $V_{s,+} \subset \mathbb{P}^{s+1}(\overline{k})$ вместо $V_s \subset \mathbb{P}^n(\overline{k})$. Теперь n и s заменяются на $s+1$ и s соответственно. По лемме 2 [10], условию (41), и поскольку $\deg_{T_{n+1}} \Phi_+ = \deg_{T_{n+1}} \Phi$, можно заменить линейные формы $T_0, T_{s+1}, T_{s+2}, \dots, T_{n+1}$ на T_0, T_n, T_{n+1}. Новое множество $A_+^{(s)} = A^{(s)}$ является тем же самым, что и первоначальное. Мы получаем объекты p_+, q_+, r_+, Φ_+, R_+, $R_{0,+}$, $A_+^{(s)}$, которые аналогичны p, q, r, Φ, R, R_0, $A^{(s)}$ и удовлетворяют аналогичным свойствам по тем же причинам. В частности, $\deg p = \deg p_+$. Отметим, что если p является конечным, то $\varphi \in k$ и $V_{s,+} = V_s \cap \mathcal{Z}(T_{s+1}, \dots, T_{n-1})$.

Теперь мы можем сформулировать наш критерий неприводимости.

Теорема 3. *Пусть $n \geqslant 3$ и $1 \leqslant s \leqslant n-2$ – целые числа. Пусть V_s – равноразмерностное проективное алгебраическое многообразие в $\mathbb{P}^n(\overline{k})$ с $\dim V_s = n - s$. Пусть $T_0, T_{s+1},\ T_{s+2}, \dots, T_{n+1}$ – линейные формы из $k[X_0, \dots, X_n]$ такие, что морфизм p – доминантный и выполняется условие* (41). *Пусть многочлен Φ и его дискриминант R – такие же, как и выше. Предположим, что многочлен $R_{0,*} =$*

$R_0(T_0, 0, \dots, 0, T_n)$ является ненулевым и сепарабельным. Тогда $\deg p = \deg p_+$ и неприводимые над $\overline{k}$ (соответственно k) компоненты алгебраических многообразий V_s и $V_{s,+}$ находятся во взаимно однозначном соответствии по правилу $W \mapsto W_1$, где W_1 – единственная неприводимая над $\overline{k}$ (соответственно k) компонента многообразия $V_{s,+}$ такая, что $W_1 \subset W \cap \mathcal{Z}(T_{s+1}, \dots, T_{n-1})$. В частности, если p конечен, то $V_{s,+} = V_s \cap \mathcal{Z}(T_{s+1}, \dots, T_{n-1})$ и $W_1 = W \cap \mathcal{Z}(T_{s+1}, \dots, T_{n-1})$.

Доказательство. Поскольку V_s и $V_{s,+}$ определены над k, то достаточно доказать только утверждение, относящееся к неприводимым над $\overline{k}$ компонентам. Обозначим через N (соответственно N_+) число всех неприводимых над $\overline{k}$ компонент многообразия V_s (соответственно $V_{s,+}$). Равенство $A^{(s)} = A_+^{(s)}$ влечёт, что для всякой неприводимой компоненты W многообразия V_s существует неприводимая компонента W_1 многообразия $V_{s,+}$ такая, что W_1 является неприводимой компонентой пересечения $W \cap \mathcal{Z}(T_{s+1}, \dots, T_{n-1})$. Из условия (41), леммы 2 [10] и равенства $A^{(s)} = A_+^{(s)}$ следует, что пересечение $V_s \cap \mathcal{Z}(T_{s+1}, \dots, T_{n-1})$ трансверсально во всякой неприводимой компоненте многообразия $V_{s,+}$. Поэтому справедливо неравенство $N_+ \geqslant N$, и если $N_+ = N$, то имеет место требуемое взаимно однозначное соответствие. Так что достаточно доказать, что $N = N_+$. Заметим, что N (соответственно N_+) является числом неприводимых над $\overline{k}$ компонент многообразия $\mathcal{Z}(\Phi)$ (соответственно $\mathcal{Z}(\Phi_+)$), поскольку q (соответственно q_+) является бирациональным изоморфизмом.

Мы будем предполагать без ограничения общности, что k является подполем поля комплексных чисел $\mathbb{C}$. Напомним, что $R_{0,*} \in k[T_0, T_n]$ – ненулевой однородный многочлен, и T_0 не делит $R_{0,*}$. Пусть $y_1, \dots, y_u$ – все попарно различные корни многочлена $R_{0,*}(1, T_n)$. Следовательно, $u = \deg R_0$ по условию леммы. Выберем точку $y \in \mathbb{C}$ такую, что $R_{0,*}(y) \neq 0$ и для всех $1 \leqslant i_1 \neq i_2 \leqslant u$ точки y, y_{i_1}, y_{i_2} не принадлежат одной и той же прямой в $\mathbb{C}$ (отождествляемом здесь с $\mathbb{R}^2$). Пусть $0 < m_1 \in \mathbb{R}$. Обозначим через b_i замкнутый круг с радиусом m_1 и центром y_i, $1 \leqslant i \leqslant u$. Выберем m_1 столь малым, что всякая прямая в $\mathbb{C}$, проходящая через точку y, пересекает самое большее один круг b_i, $1 \leqslant i \leqslant u$, и $|y_i - y_j| > 3m_1$, $|y - y_i| > m_1$ для всех $1 \leqslant i \neq j \leqslant u$. Обозначим через c_i, $1 \leqslant i \leqslant u$, окружность с радиусом m_1 и центром y_i. Обозначим через z_i пересечение интервала $[y, y_i]$ с c_i. Обозначим через

e_i объединение интервала $[y, z_i]$ и c_i. Обозначим через γ_i, $1 \leqslant i \leqslant u$, путь из точки y в z_i вдоль $[y, z_i]$, затем по c_i вокруг y_i против часовой стрелки, и назад из точки z_i в точку y вдоль интервала $[z_i, y]$. Положим $e = \cup_{1 \leqslant i \leqslant u} e_i$ и $E_z = (T_{n+1}/T_0)(r_+^{-1}(1 : z))$ для всякого $z \in \mathbb{C}$. Заметим, что для всякого $z \in \mathbb{C} \setminus \mathcal{Z}(R)$ число элементов $\# E_z = D$.

Положим $E = E_y$. Следовательно, $\# E = D$. Пусть $a \in E$. Обозначим через ξ_a аналитическую функцию от Z, определённую в окрестности точки y, такую, что $\Phi_+(1, Z, \xi_a) = 0$ и $\xi_a(y) = a$. Результат аналитического продолжения функции ξ_a вдоль пути γ_i есть $\xi_{\sigma_i(a)}$, где σ_i однозначно определённая перестановка множества E. Обозначим через S_D группу перестановок множества E и через G подгруппу в S_D, порождённую всеми σ_i, $1 \leqslant i \leqslant u$. Тогда известно, см., например, [3, 19], что число N_+ неприводимых над $\overline{k}$ компонент многообразия $V_{s,+}$ совпадает с числом классов транзитивности G на E.

Пусть $\mu_i, \nu_i \in k$, $s+1 \leqslant i \leqslant n-1$ и $0 < \delta \in \mathbb{R}$. Обозначим через $\mathcal{A}_\delta$ условие $\sum\limits_{s+1 \leqslant i \leqslant n-1} (|\mu_i|^2 + |\nu_i|^2) < \delta$. Положим $\widetilde{T}_i = T_i$, $i = 0, n, n+1$ и $\widetilde{T}_i = T_i - \mu_i T_0 - \nu_i T_n$ для всех $s+1 \leqslant i \leqslant n-1$. По лемме 2 [10] существует $0 < \delta_0 \in \mathbb{R}$ такое, что при условии $\mathcal{A}_{\delta_0}$ линейные формы $\widetilde{T}_i$ удовлетворяют тем же самым свойствам (рассмотренным выше), что и T_i, $i \in \{0, s+1, s+2, \ldots, n+1\}$. В дальнейшем мы будем предполагать, что выполняется свойство $\mathcal{A}_{\delta_0}$. Тогда для $\widetilde{T}_i$ определены объекты $\widetilde{A}^{(s)}$, $\widetilde{\Phi}$, $\widetilde{R}$ и т.д. Они соответствуют $A^{(s)}$, Φ, R и т.д. Отметим, что $\Phi = \widetilde{\Phi}$, $R = \widetilde{R}$ (как многочлены от $X_0, \ldots, X_n$), $N = \widetilde{N}$, $u = \widetilde{u} = \deg R_0$ и

$$\widetilde{\Phi}_* = \Phi(T_0, \mu_{s+1}T_0 + \nu_{s+1}T_n, \ldots, \mu_{n-1}T_0 + \nu_{n-1}T_n, T_n, T_{n+1}), \tag{43}$$

$$\widetilde{R}_* = R(T_0, \mu_{s+1}T_0 + \nu_{s+1}T_n, \ldots, \mu_{n-1}T_0 + \nu_{n-1}T_n, T_n), \tag{44}$$

$$\widetilde{\Phi}_* = \widetilde{\varphi}\widetilde{\Phi}_+, \tag{45}$$

где $\widetilde{\varphi} \in k[T_0, T_n]$ делит $\widetilde{\Phi}_{D,*}$ и $\widetilde{\Phi}_{D,*}$ делит $\widetilde{R}_{0,*}$. Следовательно, по лемме 1 [9], применённой к многочлену $R_*(1, Z)/\mathrm{lc}_Z(R_*(1, Z))$ существует $0 < \delta_1 < \delta_0$ такое, что из $\mathcal{A}_{\delta_1}$ вытекает, что $|\widetilde{y}_i - y_i| < m_1/2$ для всякого $1 \leqslant i \leqslant u$. Мы будем предполагать в дальнейшем, что выполняется свойство $\mathcal{A}_{\delta_1}$. Теперь мы выбираем $\widetilde{y} = y$ и $\widetilde{m}_1 = m_1/2$.

Пусть $m_2 = \inf\{|a_1 - a_2| \, : \, a_1, a_2 \in E_z \,\&\, a_1 \neq a_2 \,\&\, z \in e\}$. Тогда $m_2 > 0$ согласно компактности множества e. По лемме 20 для всякого $z \in e$ многочлен $\Phi_*(1, z, Z)/\mathrm{lc}_Z \Phi_*(1, z, Z) = \Phi_+(1, z, Z)/\mathrm{lc}_Z \Phi_+(1, z, Z)$.

Поэтому по лемме 1 [9], применённой к многочленам

$$\Phi_*(1,z,Z)/\mathrm{lc}_Z\Phi_*(1,z,Z), z\in e,$$

по (43), (45) и согласно компактности множества e существует $0<\delta_2\leqslant\delta_1$ такое, что из $\mathcal{A}_{\delta_2}$ следует, что для всякого $z\in e$ для всякого $a\in E_z$ существует единственное $\widetilde{a}\in\widetilde{E}_z$ такое, что $|a-\widetilde{a}|<m_2/3$. Мы будем предполагать в дальнейшем, что выполняется свойство $\mathcal{A}_{\delta_2}$.

Теперь существует биекция $\tau : E\to\widetilde{E}$, $a\mapsto\widetilde{a}$, $|a-\widetilde{a}|<m_2/3$. Поэтому τ индуцирует изоморфизм $S_D\to\widetilde{S}_D$. Согласно нашей конструкции путь γ_i гомотопен пути $\widetilde{\gamma}_i$ в $\mathbb{C}\setminus\mathcal{Z}(\widetilde{R}_*)$, для всякого $1\leqslant i\leqslant u$. Следовательно, $\widetilde{\sigma}_i=\tau\circ\sigma_i\circ\tau^{-1}$, для всякого $1\leqslant i\leqslant u$. Поэтому группы $G\simeq\widetilde{G}$ изоморфны и $N_+=\widetilde{N}_+$.

Обозначим через $\mathcal{L}_{n-s+1}$, (соответственно $\mathcal{L}_{n-s-1}$) векторное пространство линейных форм с коэффициентами из $\overline{k}$ с базисом $T_0,T_{s+1},\dots,T_n$ (соответственно $T_{s+1},,\dots,T_{n-1}$). Пусть $\mathcal{L}$ – линейное подпространство пространства $\mathcal{L}_{n-s+1}$. Обозначим через $I(\mathcal{L})\subset\overline{k}[T_0,T_{s+1},,\dots,T_{n+1}]$ идеал, порождённый $\mathcal{L}$. Для всякого многочлена $g\in\overline{k}[T_0,T_{s+1},\dots,T_{n+1}]$ положим

$$g \bmod \mathcal{L}=g \bmod I(\mathcal{L})\in\bigl(\overline{k}[T_0,T_{s+1},,\dots,T_n]/I(\mathcal{L})\bigr)[T_{n+1}]=A_{\mathcal{L}}.$$

Кольцо $A_{\mathcal{L}}$ изоморфно кольцу многочленов от $n-s+2-\dim\mathcal{L}$ переменных над $\overline{k}$. Для всякого $\psi\in A_{\mathcal{L}}$ естественным образом определена степень $\deg_{T_{n+1}}\psi$. Согласно первой теореме Бертини, применённой последовательно $n-s-1$ раз (следует каждый раз удалять фиксированные компоненты) в каждой окрестности в классической топологии векторного подпостранства) $\mathcal{L}_{n-s-1}\subset\mathcal{L}_{n-s+1}$ (окрестность подпространства $\mathcal{L}_{n-s-1}$ рассматривается здесь в соответствующем грассмановом многообразии) существует $(n-s-1)$-мерное векторное подпространство $\mathcal{L}\subset\mathcal{L}_{n-s+1}$, удовлетворяющее следующим свойствам.

- Многочлен $R \bmod \mathcal{L}\neq 0$. Поэтому $\Phi_D \bmod \mathcal{L}\neq 0$, $\deg_{T_{n+1}}\Phi=D$, и многочлен $\Phi \bmod \mathcal{L}$ не имеет кратных множителей ψ с $\deg_{T_{n+1}}\psi\geqslant 1$.
- Для всякого неприводимого над $\overline{k}$ множителя Ψ многочлена Φ степени $\deg_{T_{n+1}}\Psi\geqslant 1$ многочлен $\Psi \bmod \mathcal{L}$ имеет только один неприводимый над $\overline{k}$ множитель ψ с $\deg_{T_{n+1}}\psi\geqslant 1$, и поэтому $\deg_{T_{n+1}}\psi=\deg_{T_{n+1}}\Psi$.

Следовательно, можно выбрать $\mathcal{L}$ равным линейному подпространству, порождённому $\widetilde{T}_{s+1}, \ldots, \widetilde{T}_{n-1}$ для некоторых μ_i, ν_i, $s+1 \leqslant i \leqslant n-1$, удовлетворяющих свойству $\mathcal{A}_{\delta_2}$. В этом случае $\widetilde{N}_+ = \widetilde{N}$. Таким образом, $N = \widetilde{N} = \widetilde{N}_+ = N_+$. Теорема доказана. $\square$

Пусть $n \geqslant 1$ и $1 \leqslant s \leqslant n-1$ – целые числа. До конца раздела мы будем предполагать, что выполняется условие (41). Далее, предполагаем также, что p является доминантным морфизмом и q бирациональным изоморфизмом. Теперь пусть $L \in k[T_0, T_{s+1}, T_{s+2}, \ldots, T_n]$ – ненулевая линейная форма. Положим $A_L = k[T_0, T_{s+1}, T_{s+2}, \ldots, T_n]/(L)$. Так что A_L изоморфно кольцу многочленов от $n-s$ переменных. Следующие условия (i), (ii) и (iii) попарно эквивалентны.

(i) $R_0 \bmod L \in A_L$ сепарабелен,

(ii) Пересечение $\mathcal{Z}(R) \cap \mathcal{Z}(L)$ в $\mathbb{P}^{n-s}(\overline{k})$ трансверсально.

(iii) Степень $\deg \mathcal{Z}(R) = \deg(\mathcal{Z}(R) \cap \mathcal{Z}(L))$ в $\mathbb{P}^{n-s}(\overline{k})$.

Более того, существует непустое открытое в топологии Зарисского подмножество $\mathcal{U}_{s,1}$ пространства линейных форм от $T_0, T_{s+1}, \ldots, T_n$ такое, что для всякого $L \in U_{s,1}$ выполняются условия (i)–(iii).

Обозначим через $V_{s,L}$ объединение всех неприводимых компонент W многообразия $V_s \cap \mathcal{Z}(L)$ таких, что $W \not\subset \mathcal{Z}(g)$ для всякого ненулевого элемента $g \in k[T_0, T_{s+1}, \ldots, T_n]/(L)$.

Следующие условия (iv) и (v) эквивалентны по лемме 2 [10].

(iv) Размерность $\dim V_{s,L} = n-s-1$, p индуцирует рациональный морфизм $p_L : V_{s,L} \to \mathbb{P}^{n-s-1}(\overline{k})$ (т.е., $p_L|_W$ является рациональным доминантным морфизмом для всякого неприводимой компоненты W многообразия $V_{s,L}$), и $\deg p_L = \deg p$.

(v) Размерность $\dim V_{s,L} = n-s-1$ и существует точка $z \in \mathcal{Z}(L) \subset \mathbb{P}^{n-s}(\overline{k})$ такая, что число элементов $\#p^{-1}(z) = \deg p$.

Более того, существует непустое открытое в топологии Зарисского подмножество $\mathcal{U}_{s,2}$ пространства линейных форм от $T_0, T_{s+1}, \ldots, T_n$ такое, что для всякого $L \in U_{s,2}$ выполняются условия (iv), (v).

Обозначим через $V_{s,1}$ объединение всех неприводимых над $\overline{k}$ замкнутых подмногообразий W многообразия V_s таких, что $\dim W = n-s-1$ и размерность замыкания

$$\dim \overline{p(W \setminus \mathcal{Z}(T_0, T_{s+1}, \ldots, T_n))} < n-s-1.$$

Заметим, что существует только конечное число таких подмногообразий W, и многообразие $V_{s,1}$ определено над k (оно может быть пустым). Условия (vi) и (vii) эквивалентны.

(vi) $V_{s,L} = V_s \cap \mathcal{Z}(L)$.

(vii) $\dim V_{s,1} \cap \mathcal{Z}(L) \leqslant n-s-2$, т.е., для всякого неприводимой компоненты W многообразия $V_{s,1}$ алгебраическое многообразие $W \cap \mathcal{Z}(L) \neq W$.

Кроме того, существует ненулевая линейная форма L, удовлетворяющая (vi) и (vii), в том и только в том случае, если

$$\dim(V_s \cap \mathcal{Z}(T_0, T_{s+1}, \ldots, T_n)) \leqslant \dim(V_s) - 2.$$

Более того, если справедливо последнее условие, то существует непустое открытое в топологии Зарисского подмножество $\mathcal{U}_{s,3}$ пространства линейных форм от $T_0, T_{s+1}, \ldots, T_n$ такое, что для всякой $L \in U_{s,3}$ выполняются условия (vi) и (vii).

Следствие 1. *Пусть $n \geqslant 1$ и $1 \leqslant s \leqslant n-1$ – целые числа. Пусть V_s – равноразмерностное проективное алгебраическое многообразие в $\mathbb{P}^n(\overline{k})$ с $\dim V_s = n-s$. Пусть $T_0, T_{s+1}, T_{s+2}, \ldots, T_{n+1}$ – линейные формы из $k[X_0, \ldots, X_n]$ такие, что морфизм p является доминантным и q является бирациональным, см. выше. Пусть $L \in k[T_0, T_{s+1}, T_{s+2}, \ldots, T_n]$ – ненулевая линейная форма. Предположим, что выполняются эквивалентные условия* (i)–(iii), *и также имеют место эквивалентные условия* (iv) *и* (v), *см. выше. Тогда неприводимые над $\overline{k}$ (соответственно неприводимые над k) компоненты многообразий V и $V_{s,L}$ находятся во взаимно однозначном соответствии по правилу $W \mapsto W_1$, где W_1 однозначно определённая неприводимая над $\overline{k}$ (соответственно k) компонента многообразия $V_{s,L}$ такая, что $W_1 \subset W \cap \mathcal{Z}(L)$. Кроме того, если справедливы эквивалентные условия* (vi) *и* (vii), *то $\dim(V_s \cap \mathcal{Z}(T_0, T_{s+1}, \ldots, T_n)) \leqslant \dim(V_s) - 2$. Множество ненулевых линейных форм L, удовлетворяющих* (i)–(iii) (*соответственно* (iv)–(vi)) *является непустым открытым в топологии Зарисского подмножеством $\mathcal{U}_{s,1}$ (соответственно $\mathcal{U}_{s,2}$) пространства всех линейных форм от $T_0, T_{s+1}, \ldots, T_n$. Если $\dim(V_s \cap \mathcal{Z}(T_0, T_{s+1}, \ldots, T_n)) \leqslant \dim(V_s) - 2$, то множество ненулевых линейных форм L, удовлетворяющих* (vi) *и* (vii) *является является непустым открытым в топологии Зарисского подмножеством $\mathcal{U}_{s,3}$ пространства всех линейных форм от $T_0, T_{s+1}, \ldots, T_n$.*

Доказательство. Пусть $\mathbb{P}^{n+1}(\overline{k})$ имеет однородные координаты $X_0, \ldots, X_{n+1}$. Отождествим $\mathbb{P}^n(\overline{k}) = \mathcal{Z}(X_{n+1}) \subset \mathbb{P}^{n+1}(\overline{k})$. Пусть $I(V_s)$ – однородный идеал многообразия V_s. Обозначим через $\widetilde{V}_s \subset \mathbb{P}^{n+1}(\overline{k})$ проективное алгебраическое многообразие, которое является множеством всех общих нулей идеала $I(V_s)$. Следовательно, $V_s = \widetilde{V}_s \cap \mathcal{Z}(X_{n+1})$ в $\mathbb{P}^{n+1}(\overline{k})$. Положим $\widetilde{T}_{s+1} = L$ (не следует путать волну в обозначениях здесь и ниже с волной из обозначений в доказательстве теоремы). По (v) и лемме 20 существуют линейные формы $\widetilde{T}_0, \widetilde{T}_{s+2}, \ldots, \widetilde{T}_n$ от $T_0, T_{s+1}, T_{s+2}, \ldots, T_n$ с коэффициентами из k такие, что линейные формы $\widetilde{T}_0, \widetilde{T}_{s+1}, \ldots, \widetilde{T}_n$ являются линейно независимыми, число элементов $\#r^{-1}(\mathcal{Z}(\widetilde{T}_{s+1}, \ldots, \widetilde{T}_n)) = \deg \Phi$ и $r^{-1}(\mathcal{Z}(\widetilde{T}_{s+1}, \ldots, \widetilde{T}_n)) \cap \mathcal{Z}(\widetilde{T}_0) = \varnothing$. Заменим в (41) n, V_s, T_0, $T_{s+1}, \ldots, T_n$ и T_{n+1} на $n+1$, $\widetilde{V}_s$, $\widetilde{T}_0$, $\widetilde{T}_{s+1}, \ldots, \widetilde{T}_n$, X_{n+1} и T_{n+1} соответственно. Тогда выполняется вновь полученное условие. Мы получаем многочлены $\widetilde{\Phi}$, $\widetilde{R}$, соответствующие $\widetilde{V}_s$, и новые линейные формы согласно конструкции теоремы 3. Очевидно $\widetilde{\Phi} = \Phi$ и $\widetilde{R} = R$ как многочлены от $X_0, \ldots, X_{n+1}$. Теперь, применяя теорему 3 в рассматриваемой ситуации, мы получаем все утверждения следствия. Следствие доказано. □

Литература

1. М. Бальдассарри, *Алгебраические многообразия*, Изд-во иностр. лит., М., 1961.
2. Н. Бурбаки, *Коммутативная алгебра*, Мир, М., 1971.
3. Н. Г. Чеботарев, *Теория алгебраических функций*, ОГИЗ, М.-Л., 1948.
4. А. Л. Чистов, *Алгоритм полиномиальной сложности для разложения многочленов на неприводимые множители и нахождение компонент многообразия в субэкспоненциальное время*, Зап. научн. семин. ЛОМИ, **137** (1984), 124–188.
5. А. А. Чистов, *Вычисление степеней алгебраических многообразий над полем нулевой характеристики за полиномиальное время и его приложения*, Зап. научн. семин. ПОМИ, **258** (1999), 7–59.
6. А. Л. Чистов, *Эффективная конструкция локальных параметров неприводимых компонент алгебраического многообразия*, Тр. С.-Пет. матем. общества, **7** (1999), 230–266.
7. А. Л. Чистов, *Сильная версия основного разрешающего алгоритма для экзистенциональной теории первого порядка вещественно замкнутых полей*, Зап. научн. семин. ПОМИ, **256** (1999), 168–211.
8. А. Л. Чистов, *Эффективная гладкая стратификация алгебраического многообразия в нулевой характеристике и её приложения*, Зап. научн. семин. ПОМИ, **266** (2000), 254–311.

9. А. Л. Чистов, *Монодромия и критерии неприводимости с алгоритмическими приложениями в нулевой характеристике*, Зап. научн. семин. ПОМИ, **292**, (2002), 130–152.
10. А. Л. Чистов, *Вычисление степени доминантного морфизма в нулевой характеристике за полиномиальное время I*, Зап. научн. семин. ПОМИ, **307** (2004), 189–235.
11. А. Л. Чистов, *Вычисление степени доминантного морфизма в нулевой характеристике за полиномиальное время II*, Зап. научн. семин. ПОМИ, **325** (2005), 181–224.
12. А. Л. Чистов, *Вычисление степени доминантного морфизма в нулевой характеристике за полиномиальное время III*, Зап. научн. семин. ПОМИ, **344** (2007), 203–239.
13. А. Л. Чистов, *Вычисление степени доминантного морфизма в нулевой характеристике за полиномиальное время IV*, Зап. научн. семин. ПОМИ, **360** (2008), 260–294.
14. А. Л. Чистов, *Оценка степени системы уравнений, задающей многообразие приводимых многочленов*, Алгебра и анализ **24**, №. 3 (2012), 199–222.
15. A. L. Chistov, *Polynomial–time computation of the dimensions of components of algebraic varieties in zero-characteristic*, J. Pure and Applied Algebra, **117** & **118** (1997), 145–175.
16. A. Chistov, H. Fournier, L. Gurvits, P. Koiran, *Vandermonde Matrices, NP-Completeness, and Transversal Subspaces*, Foundations of Computational Mathematics, **3** #4 (2003), 421–427.
17. J. Bochnak, M. Coste, M.-F. Roy, *Géométrie algébrique réelle*, Springer–Verlag, Berlin, Heidelberg, New York, 1987.
18. R. Hartshorne, *Algebraic geometry*, Springer–Verlag, New York, Heidelberg, Berlin, 1977.
19. C. Jordan, *Traité des substitutions et des équations algébriques*, Paris 1870, 277–279.
20. O. Zariski, *Pencils on an algebraic variety and a new proof of a theorem of Bertini*, Trans. Amer. Math. Soc., **50** (1941), 48–70.
21. А. Л. Чистов, *Детерминированный алгоритм полиномиальный сложности для первой теоремы Бертини. I*, Зап. научн. семин. ПОМИ, **411** (2013), 191–239.

Chistov A. L. A deterministic polynomial–time algorithm for the first Bertini theorem. II.

Consider a projective algebraic variety W which is an irreducible component of a set of all common zeroes of a family of homogeneous polynomials of degrees less than d in $n+1$ variables in zero–characteristic. Consider a linear system on W given by homogeneous polynomials of degree d'. Under the conditions of the first Bertini theorem for W and this linear system we show how to construct an irreducible divisor in general position from the

statement of this theorem. This algorithm is deterministic and polynomial in $(dd')^n$ and the size of input. This paper is the second in the tree-part series.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН, Фонтанка 27,
191023 С.-Петербург, Россия
E-mail: alch@pdmi.ras.ru

Поступило 12 ноября 2013 г.