Записки научных
семинаров ПОМИ
Том 432, 2015 г.

А. Л. Чистов

ДЕТЕРМИНИРОВАННЫЙ АЛГОРИТМ ПОЛИНОМИАЛЬНОЙ СЛОЖНОСТИ ДЛЯ ПЕРВОЙ ТЕОРЕМЫ БЕРТИНИ. III

Данная статья продолжает серию работ [21,22] и является заключительной. Во всех частях нумерация теорем (соответственно лемм, разделов и т.д.) единая, и здесь она продолжается из предыдущих работ. Список литературы в данной статье (за исключением добавленных ссылок на [21, 22]) совпадает со списком литературы из [21].

§5. Доказательство теоремы 1 из работы [21]

По лемме 11 из [21] для того, чтобы доказать (a), достаточно показать, что $\mathcal{U}^{(\mathrm{v})}_{c_1,\lambda_1,0}$ является подмножеством в $\mathcal{U}_0$. Заменяя поле k на $k(\tau_1,\ldots,\tau_{n_1})$, можно предполагать без ограничения общности, что $n_1 = 0$ и $(c_1,\lambda_1) = (c',\lambda)$, где (c',λ) – из введения и удовлетворяет свойству $(*)$, см. [21].

Пусть $L' \in \mathcal{U}^{(\mathrm{v})}_{c',\lambda,0}$. Используя изоморфизм Веронезе степени d', см. [18], мы можем предполагать, не умаляя общности, что $d' = 1$, т.е. что $e'_0, e'_{\sigma+1}, \ldots, e'_{n+1}$ являются линейными формами от $X_0,\ldots,X_n$ с коэффициентами из k. Заменим в теореме 3 из [22] объекты V_s, s и T_j для всех j на W_λ, σ и e'_j соответственно и применим эту теорему.

Тогда неприводимые над $\overline{k}$ компоненты многообразий

$$W_\lambda \quad \text{и} \quad W_{\lambda,n-1}(L')$$

находятся во взаимно однозначном соответствии, задаваемом правилом

$$E \mapsto \overline{E \cap \mathcal{Z}(e'_{\sigma+1},\ldots,e'_{n-1}) \setminus \mathcal{Z}(e_0,\ldots,e_r)}. \tag{46}$$

Неприводимые над $\overline{k}$ компоненты многообразий

$$W \quad \text{и} \quad W \cap \mathcal{Z}(L_{s+1},\ldots,L_\sigma)$$

находятся во взаимно однозначном соответствии, задаваемом правилом

$$E \mapsto E \cap \mathcal{Z}(L_{s+1},\ldots,L_\sigma), \quad \text{см. [11–13].}$$

Ключевые слова: первая теорема Бертини, полиномиальный алгоритм.

Пересечения

$$(W \setminus \mathcal{Z}(e_0, \dots, e_r)) \cap \mathcal{Z}(e'_{\sigma+1}, \dots, e'_{n-1})$$

и

$$(W \setminus \mathcal{Z}(e_0, \dots, e_r)) \cap \mathcal{Z}(L_{s+1}, \dots, L_\sigma) \cap \mathcal{Z}(e'_{\sigma+1}, \dots, e'_{n-1})$$

трансверсальны, см. [11–13]. Следовательно, неприводимые над $\overline{k}$ компоненты многообразий W и $W_{\lambda,n-1}(L')$ находятся во взаимно однозначном соответствии, задаваемом правилом

$$E \mapsto \overline{E \cap \mathcal{Z}(L_{s+1}, \dots, L_\sigma) \cap \mathcal{Z}(e'_{\sigma+1}, \dots, e'_{n-1}) \setminus \mathcal{Z}(e_0, \dots, e_r)}.$$

Таким образом, неприводимые над $\overline{k}$ компоненты многообразий W и $W_{n-1}(L')$ находятся во взаимно однозначном соответствии согласно (46). Поэтому $L' \in \mathcal{U}_0$. Утверждение (a) доказано.

Докажем (e). Мы можем предполагать без ограничения общности, что $n_1 = n_2+1$ и выполняются условия леммы 12 из [21]. Для краткости положим $\Phi_i = \Phi_{c_i,\lambda_i,L^{(i)}}$, $R_i = R_{c_i,\lambda_i,L^{(i)}}$, $i = 1, 2$; $\overline{\Phi_1} = \Phi_1|_{\{\tau_{n_1}=\tau'_{n_1}\}}$, $\overline{R_1} = R_1|_{\{\tau_{n_1}=\tau'_{n_1}\}}$, $\overline{R_{1,0}} = R_{1,0}|_{\{\tau_{n_1}=\tau'_{n_1}\}}$, $\overline{R_{1,*}} = R_{1,*}|_{\{\tau_{n_1}=\tau'_{n_1}\}}$ (здесь индекс 0 означает операцию взятия бесквадратной части, индекс $*$ также определён во введении). Положим $\delta = \deg p'_v \deg W'$. Тогда по лемме 12 из [21] мы имеем $\overline{\Phi_1} = \varphi\Phi_2$, где $0 \neq \varphi \in \overline{k}[\tau_1, \dots, \tau_{n_2}, Z_0, Z_{\sigma+1}, \dots, Z_n]$. Поэтому

$$\deg_{Z_0,Z_{\sigma+1},\dots,Z_{n+1}} \Phi_{c_2,\lambda_2,L^{(2)}} \leqslant \deg_{Z_0,Z_{\sigma+1},\dots,Z_{n+1}} \Phi_{c_1,\lambda_1,L^{(1)}}.$$

Далее, $\overline{R_1} = \varphi^{2\delta-1}R_2$. Следовательно, $\overline{R_{1,0}} \neq 0$, и $R_{2,0}$ делит $\overline{R_{1,0}}$. Поэтому $b(c_2, \lambda_2, L^{(2)}) \leqslant b(c_1, \lambda_1, L^{(2)})$.

Мы имеем $R_{1,*} \neq 0$ по лемме 2 из [21]. Согласно лемме 13 из [21]

$$(\,\Phi_{1,*}/(\tau_{n_1} - \tau'_{n_1})^{\gamma}\,)|_{\{\tau_{n_1}=\tau'_{n_1}\}}$$

$$= \varphi_1\Phi_{2,*}, (\,R_{1,*}/(\tau_{n_1} - \tau'_{n_1})^{\gamma(2\delta-1)}\,)|_{\{\tau_{n_1}=\tau'_{n_1}\}} = \varphi_1^{2\delta-1}R_{2,*},$$

где $\varphi_1 \in \overline{k}(\tau_1, \dots, \tau_{n_2}, Z_0, Z_n)$. По условию 4) из $(*)$ для Φ_2 имеем $\varphi_1 \in \overline{k}[\tau_1, \dots, \tau_{n_2}, Z_0, Z_n]$. Поэтому $\deg R_{1,*,0} \geqslant \deg R_{2,*,0}$. Таким образом, $a(c_2, \lambda_2, L^{(2)}) \leqslant a(c_1, \lambda_1, L^{(2)})$. Утверждение (e) доказано.

Утверждение (d) немедленно следует из леммы 8 работы [21] и теоремы Безу.

Докажем (b) и (c) с помощью индукции по n_1. Пусть $n_2 + 1 = n_1$ и точка (c_2, λ_2) получается из (c_1, λ_1) подстановкой целого числа τ'_{n_1} вместо τ_{n_1} в (17), (18). По (d) существует τ'_{n_1} с длиной записи

$O(n\log d+(n-\sigma)\log d')$, такое, что (c_2,λ_2,L') удовлетворяет тем же самым свойствам, что и (c_1,λ_1,L'). Таким образом, можно заменить (c_1,λ_1,L') на (c_2,λ_2,L'), и утверждения (b) и (c) доказаны по индукции.

Докажем (g). Рассмотрим точку (c_1,λ_1,U). Если расширить основное поле, то $U\in\mathcal{U}^{(\mathrm{v})}_{c_1,\lambda_1,0}$. Следовательно, по теореме Безу и лемме 8 из [21], используя алгоритм редукции к целым коэффициентам, см. предложение 2 из [10], можно последовательно заменить все коэффициенты линейных форм U_j, $j\in\{0,\sigma+1,\dots,n\}$, на целые числа с длинами записи $O(n\log d+(n-\sigma)\log d')$ и получить требуемое L'. Утверждение (g) доказано.

Докажем (f). Неравенства из (f) являются частными случаями неравенств из (e), см. определения из введения. Предположим, что

$$\deg W'(c_2,\lambda_2)=\deg W'(c_1,\lambda_1)\quad\text{и}\quad b(c_2,\lambda_2)=b(c_1,\lambda_1).$$

Пусть $L'\in\mathcal{U}^{(\mathrm{v})}_{c_2,\lambda_2,0}$. Согласно (c) мы можем предполагать без ограничения общности, что $(c_2,\lambda_2)=(c',\lambda)$. Тогда по лемме 9 из [21] свойство $(*)$ выполняется для (c_1,λ_1,L'). Далее, (ii) и (iii) из определения 2 работы [21] для (c',λ,L') влекут свойства (ii) и (iii) для (c_1,λ_1,L'). Таким образом, $L'\in\mathcal{U}^{(\mathrm{v})}_{c_1,\lambda_1,0}$. Утверждение (f) доказано. Теорема доказана.

§6. Доказательство теоремы 2 из работы [21]

Очевидно, утверждение (a) этой теоремы следует из (e) и определения 2 работы [21]. Утверждение (b) следует из (a). Утверждение (c) следует из (e) и определения 2 работы [21]. Утверждение (d) является частным случаем утверждения (c). Так что достаточно доказать только (e).

Заметим, что

$$\deg W'(c_1,\lambda_1,U)=\deg W'(c_1,\lambda_1)\quad\text{и}\quad b(c_1,\lambda_1)=b(c_1,\lambda_1,U)$$

по определению, а $b(c_1,\lambda_1,U)=a(c_1,\lambda_1,U)$ по лемме 10 из [21]. Поэтому достаточно доказать все части утверждения (e) кроме относящейся к вычислению $\deg W'(c_1,\lambda_1)$ и $b(c_1,\lambda_1)$. После этого для вычисления $\deg W'(c_1,\lambda_1)$ и $b(c_1,\lambda_1)$ можно взять $L^{(1)}=U$.

При условиях из раздела 3 работы [22] пусть

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

и

$$(c_5, \lambda_5, L^{(5)}) \in \mathcal{L}_{c_1,\lambda_1,L^{(1)}}$$

– элемент, построенный при помощи разрешающего алгоритма из раздела 3 работы [22]. Тогда $\deg W'(c_1, \lambda_1, L^{(1)}) = \deg W'(c_5, \lambda_5, L^{(5)}) = \deg W'(c_5, \lambda_5, L^{(5)}, *)$, и оба элемента $(c_1, \lambda_1, L^{(1)})$, $(c_5, \lambda_5, L^{(5)})$ удовлетворяют свойству $(*)$. Далее, условие 5), см. введение, выполняется для $(c_5, \lambda_5, L^{(5)})$.

Мы опишем рекурсивный алгоритм по $(c_5, \lambda_5, L^{(5)})$. В конце рекурсии мы получим элемент $(c_5, \lambda_5, L^{(5)})$, такой, что $a(c_5, \lambda_5, L^{(5)}) = a(c_1, \lambda_1, L^{(1)})$. В качестве базы рекурсии возьмём элемент $(c_5, \lambda_5, L^{(5)})$, построенный в разделе 3 работы [22].

Опишем общий шаг этой рекурсии. Вычислим число $a(c_5, \lambda_5, L^{(5)})$ и $R_{c_5,\lambda_5,L^{(5)},*,0}$, см. наблюдения в начале раздела 3 работы [22]. Заменяя, если это необходимо, $e_0^{(5)}$ на $e_0^{(5)} + \mu e_n^{(5)}$ для подходящего целого числа μ с длиной записи $O(n \log d + (n-\sigma)\log(d'))$, мы будем предполагать в дальнейшем без ограничения общности, что Z_0 не делит $R_{c_5,\lambda_5,L^{(5)},*,0}$. Для краткости положим $\xi_j = e_j^{(5)} - e_j^{(0)} + e_j^{(1)}$, $j \in \{0, \sigma+1, \ldots, n\}$, и $e_{n+1} = e_{5,n+1} - e_{0,n+1} + e_{1,n+1}$ (однородные многочлены $e_j^{(5)}, e_j^{(0)}, e_j^{(1)}$, $e_{5,n+1}, e_{0,n+1}, e_{1,n+1}$ определены во введении и разделе 3 работы [22]). Пусть $X^{(j)}$ есть семейство переменных $X_{j,0}, \ldots, X_{j,n}$, $1 \leqslant j \leqslant 4$. Для произвольного многочлена p от $n+1$ переменных для краткости обозначим $p(X^{(j)}) = p(X_{j,0}, \ldots, X_{j,n})$. Положим

$$\begin{aligned}
&A_0 = \varepsilon_4 - |e_{n+1}(X^{(1)}) - e_{n+1}(X^{(2)})|^2, \quad A_1 = |e_{n+1}(X^{(1)})|^2 - \varepsilon_4^{-1},\\
&B_0 = \varepsilon_4 - |e_{n+1}(X^{(3)}) - e_{n+1}(X^{(4)})|^2, \quad B_1 = |e_{n+1}(X^{(3)})|^2 - \varepsilon_4^{-1},\\
&I_0 = \{1,2\}, \quad I_1 = \{1\}, \quad J_0 = \{3,4\}, \quad J_1 = \{3\}.
\end{aligned}$$

Пусть $(w_1, w_2) \in \{(0,0), (0,1), (1,1)\}$. Рассмотрим следующую систему полиномиальных уравнений и неравенств с квадратами абсолютных величин относительно переменных $\tau_1, \ldots, \tau_{n_1}$, $X_{j,0}, \ldots, X_{j,n}$, $j \in I_{w_1} \cup J_{w_2}$, с коэффициентами из поля k_4:

$$\begin{cases} \sum_{1\leqslant i\leqslant n_1} |\tau_i|^2 \leqslant \varepsilon_1, & \\ \sum_{\sigma+1\leqslant i\leqslant n-1} |\xi_i|^2 \leqslant \varepsilon_2, & \\ \varepsilon_3 \leqslant |\xi_n(X^{(1)}) - \xi_n(X^{(3)})|^2 \leqslant \varepsilon_2, & \\ A_{w_1} = 0, & \\ B_{w_2} = 0, & \\ \xi_i(X^{(j)}) = 0, & j \in I_{w_1} \cup J_{w_2},\ \sigma+1 \leqslant i \leqslant n-1, \\ \xi_n(X^{(j_1)}) = \xi_n(X^{(j_2)}), & (j_1, j_2) \in I^2_{w_1} \cup J^2_{w_2}, \\ \xi_0(X^{(j)}) = 1, & j \in I_{w_1} \cup J_{w_2}, \\ L_j(X^{(j)}) = 0, & j \in I_{w_1} \cup J_{w_2},\ s+1 \leqslant j \leqslant \sigma. \end{cases} \tag{47}$$

Лемма 21. *Неравенство* $a(c_5, \lambda_5, L^{(5)}) < a(c_1, \lambda_1, L^{(1)})$ *выполнено в том и только в том случае, если существует пара* $(w_1, w_2) \in \{(0,0),(0,1),(1,1)\}$*, такая, что система* (47) *имеет решение* $X_{j,i} = x^*_{j,i}$, $0 \leqslant j \leqslant n$, $j \in I_{w_1} \cup J_{w_2}$, *удовлетворяющее условию*

$$(x^*_{j,0} : \ldots : x^*_{j,n}) \in W(\overline{k_5}), \quad j \in I_{w_1} \cup J_{w_2}. \tag{48}$$

Доказательство. Предположим, что $a(c_5, \lambda_5, L^{(5)}) < a(c_1, \lambda_1, L^{(1)})$. Существует такой элемент ε', что $\varepsilon' > 0$ является бесконечно малой величиной относительно поля k_2 и ε_3 является бесконечно малой величиной относительно поля $k_2(\varepsilon')$. По принципу переноса, см. [17], достаточно построить решение (48) системы (47) с коэффициентами в поле $\overline{k(\varepsilon', \varepsilon_4)}$ вместо $\overline{k_4}$.

Согласно лемме 4, лемме 6, лемме 7 из [21] и алгоритму редукции к целым коэффициентам (ср. доказательство существования (c_*, λ_*, L^*) в лемме 17) существуют $\tau^*_i \in k(\varepsilon')$, которые являются бесконечно малыми величинами относительно поля k и таковы, что (c_*, λ_*, L^*) удовлетворяет условиям леммы 4, леммы 6, леммы 7 из [21] (для всякой прямой $\mathfrak{l}$, содержащей (c_*, λ_*, L^*)) вместо $(c_0, \lambda_0, L^{(0)})$,

$$\deg W'(c_*, \lambda_*, L^*) = \deg W'(c_1, \lambda_1, L^{(1)}),$$
$$\deg W'(c_*, \lambda_*, L^*, *) = \deg W'(c_1, \lambda_1, L^{(1)}, *)$$

и

$$a(c_*, \lambda_*, L^*) = a(c_1, \lambda_1, L^{(1)})$$

(напомним, что точка (c_*, λ_*, L^*) определена в разделе 3 работы [22] перед системой (34)). Выберем многочлен $\Phi_{c_*, \lambda_*, L^*}$ (он однозначно определён с точностью до множителя из $\overline{k(\varepsilon')}$), такой, что справедливо следующее свойство. Каждый коэффициент многочлена Φ_{c_*,λ_*,L^*} не является бесконечно большим относительно поля k, и некоторый ненулевой коэффициент φ многочлена Φ_{c_*,λ_*,L^*} не является бесконечно малым относительно поля k. Напомним, что в общей ситуации если определено отображение стандартной части $\mathrm{st} : K \setminus \{$бесконечно большие элементы$\} \to k$, то для произвольного многочлена f с коэффициентами из $K \setminus \{$бесконечно большие элементы$\}$ стандартная часть $\mathrm{st}(f)$ является многочленом с коэффициентами из k, такими, что все ненулевые коэффициенты многочлена $f - \mathrm{st}(f)$ являются бесконечно малыми величинами относительно поля k. Теперь по лемме 14 из [21] (с полем $k(\varepsilon')$ и $\mathrm{st}_{\varepsilon'}$ вместо поля k_i и st_i соответственно) и поскольку $\deg W'(c_*, \lambda_*, L^*) = \deg W'(c_5, \lambda_5, L^{(5)})$, стандартная часть $\mathrm{st}_{\varepsilon'}(\Phi_{c_*,\lambda_*,L^*})$ совпадает с $\Phi_{c_5,\lambda_5,L^{(5)}}$ с точностью до ненулевого множителя из $\overline{k}$. Поэтому по лемме 1 из [21], применённой к $\Phi_{c_5,\lambda_5,L^{(5)}}$, также $\mathrm{st}_{\varepsilon'}(\Phi_{c_*,\lambda_*,L^*,*})$ совпадает с $\Phi_{c_5,\lambda_5,L^{(5)},*}$ с точностью до ненулевого множителя из k. Мы имеем

$$\begin{aligned}\deg_{Z_0,Z_n,Z_{n+1}} \Phi_{c_*,\lambda_*,L^*,*} &= \deg_{Z_0,Z_n,Z_{n+1}} \Phi_{c_5,\lambda_5,L^{(5)},*}\\ &= \deg W'(c_1, \lambda_1, L^{(1)}, *),\end{aligned}$$

и

$$\deg_{Z_{n+1}} \Phi_{c_*,\lambda_*,L^*,*} = \deg_{Z_{n+1}} \Phi_{c_5,\lambda_5,L^{(5)},*} = \deg p'_v \deg W'$$

согласно нашей конструкции. Следовательно,

$$\mathrm{st}_{\varepsilon'}(R_{c_*,\lambda_*,L^*,*}) = R_{c_5,\lambda_5,L^{(5)},*}.$$

Так как $a(c_5, \lambda_5, L^{(5)}) < a(c_*, \lambda_*, L^*)$, многочлен $R_{c_*,\lambda_*,L^*,*}$ имеет больше попарно различных корней, чем $R_{c_5,\lambda_5,L^{(5)},*}$. Следовательно, существуют два различных бесконечно близких корня $\xi_{n,0}, \xi_{n,1}$ многочлена $R_{c_*,\lambda_*,L^*,*}(1, Z_n) \in \overline{k(\varepsilon')}[Z_n]$. Поэтому $\xi_{n,0} - \xi_{n,1} \in \overline{k(\varepsilon')}$ является бесконечно малой величиной относительно поля k.

Следовательно, для всякого $i = 0, 1$ имеет место один из двух случаев:

1) многочлен $\Phi_{c_*,\lambda_*,L^*,*}(1, \xi_{n,i}, Z_{n+1})$ имеет кратный корень
$$Z_{n+1} = \xi_{n+1,i},$$

2) $(\mathrm{lc}_{Z_{n+1}}(\Phi_{c_*,\lambda_*,L^*,*}))(1, \xi_{n,i}) = 0$ (напомним, что
$$\mathrm{lc}_{Z_{n+1}}(\Phi_{c_*,\lambda_*,L^*,*}) \in \overline{k}[Z_0, Z_n]\ ).$$

Переставляя $i = 0, 1$, можно предполагать без ограничения общности, что если 1) выполняется для некоторого $i = 0, 1$, то 1) справедливо для $i = 0$.

Для удобства обозначений положим $I_{1,1} = I_0$, $I_{1,2} = I_1$, $I_{2,1} = J_0$, $I_{2,2} = J_1$. Если выполнено w) (здесь w = 1 или w = 2) для i, то по принципу переноса существуют $\widetilde{\xi}_{n,i} \in \overline{k(\varepsilon', \varepsilon_4)}$ и $\widetilde{\xi}_{n+1,j} \in \overline{k(\varepsilon', \varepsilon_4)}$, $j \in I_{i,w}$, удовлетворяющие следующим условиям:

(a) элемент $\widetilde{\xi}_{n,i}$ является бесконечно близким к $\xi_{n,i}$ относительно поля $\overline{k(\varepsilon')}$,

(b) если $w = 1$, то $|\widetilde{\xi}_{n+1,j_1} - \widetilde{\xi}_{n+1,j_2}|^2 = \varepsilon_4$, где $j_1, j_2 \in I_{i,1}$, $j_1 \neq j_2$, и каждый элемент $\widetilde{\xi}_{n+1,j}$, $j \in I_{i,w}$, является бесконечно близким к $\xi_{n+1,i}$,

(c) если $w = 2$, то $|\widetilde{\xi}_{n+1,j}|^2 = \varepsilon_4^{-1}$, где $j \in I_{i,2}$.

Заметим, что $(1 : \widetilde{\xi}_{n,i} : \widetilde{\xi}_{n+1,j})$ является общей точкой многообразия $W'(c_1, \lambda_1, L^{(1)}, *)$ для всех рассматриваемых i, w, j. Далее, $q_{c_*,\lambda_*,L^*,*}$ – доминантный морфизм кривых, и $\deg q_{c_*,\lambda_*,L^*,*} = 1$. Поэтому

(d) $\#q^{-1}_{c_*,\lambda_*,L^*,*}((1 : \widetilde{\xi}_{n,i} : \widetilde{\xi}_{n+1,j})) = 1$ для всех $j \in I_{i,w}$.

Теперь для $i = 0, 1$ положим $w_i = 0$, если выполняется 1), и $w_i = 1$, если выполняется 2). Положим $(x^*_{j,0} : \ldots : x^*_{j,n}) \in q^{-1}_{c_*,\lambda_*,L^*,*}((1 : \widetilde{\xi}_{n,i} : \widetilde{\xi}_{n+1,j}))$, $j \in I_{w_1} \cup I_{w_2}$. Тогда согласно нашей конструкции $X_{j,i} = x^*_{j,i}$, $0 \leqslant j \leqslant n$, $j \in I_{w_1} \cup J_{w_2}$, является решением системы (47), удовлетворяющим условию (48) (с полем $k(\varepsilon', \varepsilon_4)$ вместо k_4).

Обратно, предположим, что существует решение (48) системы (47). Тогда, как это следует из описания алгоритма для рассматриваемой рекурсии, см. ниже, выполняется неравенство

$$a(c_5, \lambda_5, L^{(5)}) < a(c_1, \lambda_1, L^{(1)}).$$

Лемма доказана. □

Вернёмся к описанию общего шага рекурсии. Заметим, что система (47) удовлетворяет условиям 1)–4) из раздела 2 работы [22]. Поэтому, используя лемму 16 и замечание 11 из [22], мы выясняем, верно ли, что система (47) имеет решение, удовлетворяющее (48), и, если такое решение существует, строим его. Предположим, что такого решения не существует. Тогда по лемме 21 имеем $a(c_5, \lambda_5, L^{(5)}) = a(c_1, \lambda_1, L^{(1)})$, и рассматриваемый шаг является последним. Положим в этом случае

$(c_4, \lambda_4, L^{(4)}) = (c_5, \lambda_5, L^{(5)})$. Точка $(c_4, \lambda_4, L^{(4)})$ удовлетворяет утверждению (e) из теоремы 2 работы [21].

Предположим, что мы построили решение системы (47), удовлетворяющее (48), см. формулировку леммы 21. Тогда из системы (47) и (48) мы немедленно получаем, ср. доказательство леммы 21, что $a(c_*, \lambda_*, L^*) > a(c_5, \lambda_5,\ L^{(5)})$ по этой лемме. Как и для предыдущих рекурсий, условия леммы 4 из [21], леммы 6 и леммы 7 из [21] выполняются для (c_*, λ_*, L^*) вместо $(c_0, \lambda_0, L^{(0)})$. Согласно лемме 4, лемме 6, лемме 7 из [21] и наблюдениям в начале раздела 3 работы [22] можно применить алгоритм редукции к целым коэффициентам, см. [10, предложение 2], и последовательно заменить 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 $L' \in \mathcal{U}_0''$,

$$\#A_{\lambda,L'} = \deg p_v' \deg W', \quad A_{\lambda,L'} \cap \mathcal{Z}(e_0') = \varnothing \quad \text{и} \quad A_{\lambda,L'} \cap \overline{V \setminus W} = \varnothing,$$

$$\dim W_\lambda = n - \sigma, \quad \dim(W_\lambda \setminus \mathcal{Z}(e_0, \ldots, e_r)) \cap \mathcal{Z}(e_{\sigma+1}', \ldots, e_{n-1}') = 1,$$

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

морфизмы $p_{\lambda,L'}$, $p_{\lambda,L',*}$ являются доминантными,

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

и

$$a(c', \lambda, L') \geqslant a(c_*, \lambda_*, L^*).$$

Применим лемму 8 из [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, используя теорему 1 (f) из [12], лемму 8 и лемму 4, лемму 6, лемму 7 из [21], мы строим точку (c'', λ', L''), которая аналогична $(c_5, \lambda_5, L^{(5)})$ и такова, что $a(c'', \lambda', L'') \geqslant a(c', \lambda, L') > a(c_5, \lambda_5,\ L^{(5)})$. 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.

Требуемая оценка на время работы данного алгоритма для утверждения (e) теоремы 2 работы [21] немедленно следует из оценок на времена работы использованных алгоритмов. Утверждение (e) теоремы 2 из [21] доказано. Таким образом, теорема 2 работы [21] доказана, см. начало раздела.

Приложение: доказательство некоторой версии первой теоремы Бертини в произвольной характеристике

Для того чтобы сделать наше изложение в [9–13] и настоящей статье замкнутым в себе, мы дадим независимое доказательство первой теоремы Бертини (и некоторых других относящихся к ней результатов) для случая аффинных алгебраических многообразий в произвольной характеристике основного поля, см. теорему 4 ниже. Отметим здесь, что в нашем изложении имеют место только две ссылки на первую теорему Бертини и только на частный случай гиперповерхностей в аффинном пространстве в нулевой характеристике. Именно, они имеются в доказательствах теоремы 3 из [22] и теоремы 3 из [9]. Всё же для удобства читателя и возможных приложений в будущем мы решили рассмотреть в теореме 4 более общую ситуацию аффинного алгебраического многообразия над алгебраически замкнутым полем произвольной характеристики. Из леммы 24 следует общая версия первой теоремы Бертини, сформулированная во введении.

В этом разделе мы пользуемся обозначениями, которые могут отличаться от обозначений из введения. Пусть k – совершенное поле произвольной характеристики с алгебраическим замыканием $\overline{k}$. Пусть B – произвольное коммутативное нётерово целостное кольцо. Мы будем обозначать через B' целое замыкание кольца B в его поле частных. Для конечно порождённого B-модуля M обозначим через $\mathrm{Ass}_B(M)$ множество всех ассоциированных простых идеалов модуля M (они являются простыми идеалами в B). Напомним, что идеал кольца B называется радикальным, если он совпадает со своим нильрадикалом. В дальнейшем морфизмы алгебраических многообразий являются регулярными, если не оговорено противное.

Пусть $n \geqslant 2$ – целое число. Пусть $\mathbb{A}^n(\overline{k})$ – аффинное пространство над полем $\overline{k}$ с координатными функциями $X_1, \ldots, X_n$. Пусть $x \in \mathbb{A}^n(\overline{k})$ – точка с координатами $X_i(x) = 0$, $1 \leqslant i \leqslant n$.

Пусть V – аффинное алгебраическое многообразие, определённое и неприводимое над $\overline{k}$. Пусть $p : V \to \mathbb{A}^n(\overline{k})$ – доминантный сепарабельный морфизм. Мы будем отождествлять кольцо $\overline{k}[X_1, \ldots, X_n]$ с подкольцом в $\overline{k}[V]$. Для элемента $g \in \overline{k}[X_1, \ldots, X_n]$ обозначим через $\mathcal{Z}(g)$ подмножество всех нулей многочлена g в $\mathbb{A}^n(\overline{k})$. Для удобства обозначений мы будем обозначать через $V \cap \mathcal{Z}(g)$ подмножество $p^{-1}(\mathcal{Z}(g)) \subset V$.

Мы будем предполагать дополнительно, что

$$\dim p^{-1}(x) \leqslant n-2. \tag{49}$$

Обозначим через $B = \overline{k}[V]$ кольцо регулярных функций алгебраического многообразия V. Пусть $z \in V$. Обозначим через $\mathfrak{M}_z$ максимальный идеал кольца B, соответствующий точке z.

Пусть $y \in B$ – примитивный элемент сепарабельного алгебраического расширения $\overline{k}(V) \supset \overline{k}(X_1, \dots, X_n)$, т.е.

$$\overline{k}(V) = \overline{k}(X_1, \dots, X_n)[y]. \tag{50}$$

Пусть $f \in \overline{k}[X_1, \dots X_n, Y]$–минимальный многочлен элемента y над полем $\overline{k}(X_1, \dots, X_n)$ (здесь Y является новой переменной) и f неприводим в кольце $\overline{k}[X_1, \dots, X_n, Y]$. Тогда $D = \deg_Y f \geqslant 1$. Пусть $\deg_{X_1,\dots,X_n,Y} f = m_1$ и $f^{(m_1)}$ – однородная относительно $X_1, \dots, X_n, Y$ форма степени m_1 многочлена f.

Элемент y цел над $\overline{k}[X_1, \dots, X_n]$, если морфизм p конечен. Обозначим через $\mathrm{lc}_Y f$ старший коэффициент многочлена f относительно Y. Мы выбираем f так, что $\mathrm{lc}_Y f = 1$, если p конечен.

Кроме того, мы будем предполагать, что *если $n = 2$, то p конечен.*

Обозначим через

$$\Delta_1 = \mathrm{Res}_Y(f, \partial f/\partial Y) \in \overline{k}[X_1, \dots, X_n] \tag{51}$$

дискриминант многочлена f относительно Y. Тогда $\Delta_1 \neq 0$, поскольку f является сепарабельным.

Замечание 13. По определению дискриминант Δ_1 является определителем $(2D-1)\times(2D-1)$ матрицы Сильвестра результанта. Хотя в случае ненулевой характеристики основного поля степень $\deg_Y \partial f/\partial Y$ может быть меньше чем $D-1$, частная производная $\partial f/\partial Y$ рассматривается здесь формально как многочлен степени $D-1$ в представлении этой матрицы. Некоторые старшие коэффициенты производной $\partial f/\partial Y$ могут быть равны нулю в этом представлении. Напомним ещё раз, что это определение дискриминанта отличается от общепринятого на множитель $\mathrm{lc}_Y f$, но оно более удобно для нас.

Отождествим множество всех линейных форм из $\overline{k}[X_1, \dots, X_n]$ с $\mathbb{A}^n(\overline{k})$. Пусть $\mathfrak{P}$ – простой идеал кольца $\overline{k}[X_1, \dots, X_n]$ (соответственно B, B'). Предположим, что

$$\mathcal{Z}(\mathfrak{P}) \not\subset \mathcal{Z}(X_1, \dots, X_n),$$

где $\mathcal{Z}(X_1,\ldots,X_n)$ и $\mathcal{Z}(\mathfrak{P})$ рассматриваются как подмногообразия в $\mathbb{A}^n(\overline{k})$ (соответственно V, нормализации многообразия V). Тогда множество $S_{\mathfrak{P}}$ линейных форм $L \in \overline{k}[X_1,\ldots,X_n]$, таких, что $L \notin \mathfrak{P}$, является непустым и открытым в топологии Зарисского в $\mathbb{A}^n(\overline{k})$, поскольку

$$S_{\mathfrak{P}} = \bigcup_{z\in\mathcal{Z}(\mathfrak{P})} \Big\{L \in \mathbb{A}^n(\overline{k}) \,:\, L(z) \neq 0\Big\}.$$

Рассмотрим B'/B как B-модуль. Положим

$$\mathcal{B}_0 = \operatorname{Ass}_B(B'/B), \qquad \mathcal{B}_1 = \{\mathfrak{P} \in \mathcal{B}_0 \,:\, \mathcal{Z}(\mathfrak{P}) \not\subset p^{-1}(x)\},$$
$$\mathcal{B}_2 = \{\mathfrak{P} \in \mathcal{B}_0 \,:\, \dim \mathcal{Z}(\mathfrak{P}) = n-1\}.$$

Рассмотрим множество $\mathcal{U}_1$ (соответственно $\mathcal{U}_2$) линейных форм L от $X_1,\ \ldots,X_n$, таких, что $L \notin \mathfrak{P}$ для всякого $\mathfrak{P} \in \mathcal{B}_1$ (соответственно $\mathcal{B}_2$). Тогда $\mathcal{U}_1$ (соответственно $\mathcal{U}_2$) является непустым открытым в топологии Зарисского подмножеством в $\mathbb{A}^n(\overline{k})$, и $\mathcal{U}_1 \subset \mathcal{U}_2$. Заметим, что $\mathcal{U}_1 = \mathcal{U}_2 = \mathbb{A}^n(\overline{k})$, если $\mathcal{B}_1 = \varnothing$, в частности, если $B = B'$ (т.е. если V является нормальным), так как в последнем случае $\operatorname{Ass}_B(B'/B) = \varnothing$. Отметим также, что если множество особых точек многообразия V имеет размерность не больше $n-2$, то $\mathcal{B}_2 = \varnothing$ и $\mathcal{U}_2 = \mathbb{A}^n(\overline{k})$.

Пусть $L \in \overline{k}[X_1,\ldots,X_n]$ – ненулевая линейная форма. Рассмотрим B/LB как B-модуль. Положим

$$\mathcal{B}_{1,L} = (\mathcal{B}_0 \setminus \mathcal{B}_1) \cap \operatorname{Ass}_B(B/LB), \quad \mathcal{B}_{2,L} = (\mathcal{B}_0 \setminus \mathcal{B}_2) \cap \operatorname{Ass}_B(B/LB).$$

Покажем, что существует ненулевой элемент $\Delta_3 \in \overline{k}[X_1,\ldots,X_n]$, такой, что расширения колец

$$B[\Delta_3^{-1}] \supset \overline{k}[X_1,\ldots,X_n,\, \Delta_3^{-1}][y] \supset \overline{k}[X_1,\ldots,X_n][\Delta_3^{-1}] \tag{52}$$

являются целыми. Действительно, согласно (50) можно выбрать Δ_3 равным произведению $\operatorname{lc}_Y f$ и всех старших коэффициентов минимальных многочленов над $\overline{k}[X_1,\ldots,X_n]$ элементов конечной системы образующих кольца B над $\overline{k}[X_1,\ldots,X_n]$. В случае, когда p является конечным, мы выбираем $\Delta_3 = 1$. Зафиксируем элемент Δ_3.

Положим $\mathcal{B}_3 = \operatorname{Ass}_{B'}(B'/\Delta_3 B')$, где $B'/\Delta_3 B'$ рассматривается как B'-модуль. Тогда элементы из $\mathcal{B}_3$ являются простыми идеалами кольца B'. Обозначим через $\mathcal{U}_3$ множество всех линейных форм $L \in \overline{k}[X_1,\ldots,$ $X_n]$, таких, что $L \notin \mathfrak{P}$ для всякого $\mathfrak{P} \in \mathcal{B}_3$. Поскольку B' является целозамкнутым, $\dim \mathcal{Z}(\mathfrak{P}) = n-1$ для всякого $\mathfrak{P} \in \mathcal{B}_3$, см. [2]. Следовательно, $\mathcal{U}_3$ является непустым открытым в топологии Зарисского подмножеством пространства $\mathbb{A}^n(\overline{k})$. Отметим также, что если p конечен, то $\mathcal{U}_3 = \mathbb{A}^n(\overline{k})$. Заметим, что если $L \in \mathcal{U}_3$, то L не делит Δ_3 в кольце $\overline{k}[X_1, \ldots, X_n]$.

Теорема 4. *Пусть $n \geqslant 2$. Пусть V, B, $p : V \to \mathbb{A}^n(\overline{k})$, y, f, Δ_1, Δ_3, m_1, $f^{(m_1)}$, $\mathcal{U}_1$, $\mathcal{U}_2$, $\mathcal{U}_3$, $\mathcal{B}_0$, $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$, $\mathcal{B}_{1,L}$ и $\mathcal{B}_{2,L}$ – такие же, как и выше.*

(i) *Тогда существует ненулевая линейная форма $L \in \overline{k}[X_1, \ldots, X_n]$ от $X_1, \ldots, X_n$, такая, что идеал $(f, L) \subset \overline{k}[X_1, \ldots, X_n, Y]$ радикален, а если $n \geqslant 3$, то он простой. Элемент $\Delta_1 \bmod L \in \overline{k}[X_1, \ldots, X_n]/(L)$ является ненулевым (т.е. L не делит Δ_1), и элемент*

$$f^{(m_1)} \bmod L \in (\,\overline{k}[X_1, \ldots, X_n]/(L)\,)[Y]$$

также является ненулевым.

(ii) *Множество $\mathcal{U}_4$ линейных форм L, удовлетворяющих свойствам из* (i)*, является непустым открытым в топологии Зарисского подмножеством аффинного пространства $\mathbb{A}^n(\overline{k})$.*

(iii) *Пусть $L \in \mathcal{U}_1 \cap \mathcal{U}_3 \cap \mathcal{U}_4$ (соответственно $L \in \mathcal{U}_2 \cap \mathcal{U}_3 \cap \mathcal{U}_4$). Тогда*

$$LB = \mathfrak{p} \cap \mathfrak{q},$$

где идеал $\mathfrak{p}$ является радикалом идеала LB и если $n \geqslant 3$, то он простой. Идеал $\mathfrak{q}$ является пересечением $\mathfrak{P}$-примарных идеалов для всех простых идеалов $\mathfrak{P} \in \mathcal{B}_{1,L}$ (соответственно $\mathfrak{P} \in \mathcal{B}_{2,L}$), причём здесь мы предполагаем, что пересечение по пустому множеству (когда $\mathcal{B}_{1,L} = \varnothing$ или $\mathcal{B}_{2,L} = \varnothing$) равно B. Поэтому если $L \in \mathcal{U}_1 \cap \mathcal{U}_3 \cap \mathcal{U}_4$ и p конечен, то $\mathfrak{q}$ является пересечением $\mathfrak{M}_z$-примарных идеалов для некоторых $z \in p^{-1}(x)$ или $\mathfrak{q} = B$. Кроме того, для всякого $\mathfrak{P} \in \mathcal{B}_{1,L}$ (соответственно $\mathfrak{P} \in \mathcal{B}_{2,L}$) $\dim \mathcal{Z}(\mathfrak{P}) \leqslant n-2$, и, следовательно, $\mathfrak{P}$-примарная компонента идеала LB является вложенной.

(iv) *Пусть $L \in \mathcal{U}_2 \cap \mathcal{U}_3 \cap \mathcal{U}_4$. Тогда алгебраическое многообразие $V \cap \mathcal{Z}(L)$ имеет размерность $\dim V - 1$, и если $n \geqslant 3$, то $V \cap \mathcal{Z}(L)$ неприводимо над $\overline{k}$. Далее, проекция*

$$V \cap \mathcal{Z}(L) \to \mathcal{Z}(L), \tag{53}$$

индуцированная морфизмом p, является доминантным сепарабельным морфизмом алгебраических многообразий (здесь

$\mathcal{Z}(L) \subset \mathbb{A}^n(\overline{k})$). *Кроме того, если p конечен, то морфизм* (53) *также является конечным.*

Обозначим через $\overline{k}(V \cap \mathcal{Z}(L))$ *полное кольцо частных кольца регулярных функций алгебраического многообразия* $V \cap \mathcal{Z}(L)$; *оно является полем рациональных функций этого алгебраического многообразия, если* $n \geqslant 3$. *Тогда*

$$[\overline{k}(V \cap \mathcal{Z}(L)) : \overline{k}(\mathcal{Z}(L))] = [\overline{k}(V) : \overline{k}(X_1, \ldots, X_n)], \qquad (54)$$

причём левая часть этого равенства равна размерности полного кольца частных над полем $\overline{k}(\mathcal{Z}(L))$, *а правая часть равна степени расширения полей рациональных функций* $\overline{k}(V) \supset \overline{k}(\mathbb{A}^n(\overline{k}))$. *Обозначим через* $y \bmod L$ *образ элемента* y *в* $\overline{k}[V \cap \mathcal{Z}(L)]$. *Тогда минимальный многочлен элемента* $y \bmod L$ *над* $\overline{k}(\mathcal{Z}(L))$ *равен* $f \bmod L$, *и* $y \bmod L$ *является примитивным элементом сепарабельной алгебры* $\overline{k}(V \cap \mathcal{Z}(L))$ *над* $\overline{k}(\mathcal{Z}(L))$.

(v) *Пусть* $n \geqslant 3$. *Пусть* $\mathcal{L}$ – *линейное подпространство пространства всех линейных форм из* $\overline{k}[X_1, \ldots, X_n]$ *с* $\dim \mathcal{L} \geqslant 3$. *Предположим, что для всякого* $\mathfrak{P} \in \mathcal{B}_3$, *такого, что* $\dim \mathcal{Z}(\mathfrak{P}) = n - 1$,

$$\dim \overline{p(\mathcal{Z}(\mathfrak{P}))} \geqslant n - 2. \qquad (55)$$

Тогда $\mathcal{L} \cap \mathcal{U}_2 \cap \mathcal{U}_3 \neq \varnothing$.

(vi) *Пусть* $n \geqslant 3$. *Пусть* $\mathcal{L}$ – *линейное подпространство пространства всех линейных форм из* $\overline{k}[X_1, \ldots, X_n]$ *с* $\dim \mathcal{L} \geqslant 3$. *Тогда* $\mathcal{L} \cap \mathcal{U}_4 \neq \varnothing$.

Доказательство. Пусть $n = 2$. Тогда мы определяем $\mathcal{U}_4$ как множество всех линейных форм $L \in \overline{k}[X_1, X_2]$, таких, что L не делит $\Delta_1 f^{(m_1)}$. Следовательно, в этом случае $\mathcal{U}_4$ является непустым открытым в топологии Зарисского подмножеством пространства $\mathbb{A}^2(\overline{k})$. Напомним, что согласно нашим предположениям $\mathrm{lc}_Y f = 1$, если $n = 2$. Поэтому если $L \in \mathcal{U}_4$, то $\Delta_1 \bmod L \neq 0$ и, значит, многочлен $f \bmod L$ является сепарабельным. Следовательно, идеал (f, L) радикален. Кроме того, $f^{(m_1)} \bmod L \neq 0$. Утверждения (i) и (ii) доказаны для $n = 2$.

Теперь наша цель – свести (iii), (iv) и (v) к (i) и (ii) для $n \geqslant 3$ (утверждения (i) и (ii) для $n \geqslant 3$ будут доказаны позже). Так что мы сейчас предполагаем, что (i) и (ii) выполняются для $n \geqslant 3$. Пусть $\widetilde{V}$ – нормализация многообразия V. Следовательно, $\overline{k}[\widetilde{V}] = B'$.

Обозначим через $S_1 = \{\Delta_3^N \,:\, 0 \leqslant N \in \mathbb{Z}\}$ мультипликативно замкнутое подмножество в $\overline{k}[X_1, \dots, X_n]$. Для краткости положим $A = \overline{k}[X_1, \dots, X_n]$. Обозначим через V_1 аффинное алгебраическое многообразие с кольцом регулярных функций $A[Y]/(f)$.

Лемма 22. *Пусть $L \in \mathcal{U}_3 \cap \mathcal{U}_4$. Тогда идеал LB' кольца B' – радикальный (соответственно простой, если $n \geqslant 3$), и естественные гомоморфизмы*

$$B'/LB' \to S_1^{-1}(B'/LB'), \tag{56}$$

$$A[Y]/(f, L) \to S_1^{-1}A[Y]/(f, L) \tag{57}$$

являются мономорфизмами. Естественный гомоморфизм $A[Y]/(f, L) \to B'/LB'$ также является мономорфизмом. Следовательно, можно отождествить $A[Y]/(f, L)$ с подалгеброй в B'/LB'. Наконец, при этом отождествлении алгебры $A[Y]/(f, L)$ и B'/LB' имеют одно и то же полное кольцо частных, т.е. можно отождествить полные кольца частных, $\overline{k}(\widetilde{V} \cap \mathcal{Z}(L))$ и $\overline{k}(V_1)$, колец регулярных функций алгебраических многообразий $\widetilde{V} \cap \mathcal{Z}(L)$ и V_1.

Доказательство. Докажем, что (56) является мономорфизмом. Достаточно показать, что умножение на $\Delta_3 \,:\, B'/LB' \to B'/LB'$ является мономорфизмом, см. [2]. Пусть $z \in B'$ и $\Delta_3 z = L z_1$ для некоторого $z_1 \in B'$. Поскольку $L \in \mathcal{U}_3$, умножение на $L \,:\, B'/\Delta_3 B' \to B'/\Delta_3 B'$ – мономорфизм. Следовательно, существует элемент $z_2 \in B'$, такой, что $z_1 = \Delta_3 z_2$. Поскольку B' целостно, $z = L z_2$. Поэтому (56) – мономорфизм.

Так как $L \in \mathcal{U}_3$, линейная форма L не делит Δ_3. Следовательно, гомоморфизм (57) является мономорфизмом.

Расширения колец (52) являются целыми, и элемент y сепарабелен над $\overline{k}(X_1, \dots, X_n)$. Поэтому, см., например, [2], в этом случае можно отождествить $S_1^{-1}B'$ с подкольцом в $\frac{1}{\Delta_1} S_1^{-1}A[Y]/(f, L)$. Покажем, что при этом отождествлении

$$L\, S_1^{-1}B' = \Big(\frac{L}{\Delta_1} S_1^{-1}A[Y]/(f, L) \Big) \cap S_1^{-1}B'. \tag{58}$$

Действительно, пусть $(L/\Delta_1)a_1 = a_2$, где $a_1 \in S_1^{-1}A[Y]/(f, L)$ и $a_2 \in S_1^{-1}B'$. Положим $a = a_2/L$. Тогда $La \in S_1^{-1}B'$ и $\Delta_1 a \in S_1^{-1}A[Y]/(f, L)$.

Рассмотрим минимальный многочлен $\psi \in A[Z]$ (здесь Z – новая переменная) элемента a над $\overline{k}(X_1,\dots,X_n)$, такой, что ψ является неприводимым элементом кольца $A[Z]$. Тогда старший коэффициент $\mathrm{lc}_Z\psi$ делит $\mathrm{G\,C\,D}\,(L^D,\Delta_1^D)$ в кольце $S_1^{-1}A$. Поэтому $\mathrm{lc}_Z\psi=\lambda\Delta_3^N$, где $0\neq\lambda\in\overline{k}$ и целое число N неотрицательно. Следовательно, $a\in S_1^{-1}B'$, поскольку последнее кольцо целозамкнуто. Требуемое утверждение доказано.

Покажем, что $(\,LS_1^{-1}B'\,)\cap(\,S_1^{-1}A[Y]/(f,L)\,) = LS_1^{-1}A[Y]/(f,L)$. Действительно, L не делит Δ_1, и $S_1^{-1}A[Y]/(f,L)$ является свободным $S_1^{-1}(A/(L))$-модулем. Поэтому требуемое утверждение следует из (58). Теперь можно рассмотреть отождествления

$$\begin{aligned} S_1^{-1}A[Y]/(f,L) &\subset S_1^{-1}(B'/LB') \\ &\subset \frac{1}{\Delta_1 \operatorname{mod} L}S_1^{-1}A[Y]/(f,L)\subset \overline{k}(V_1\cap\mathcal{Z}(L)). \end{aligned} \tag{59}$$

Поскольку (56) и (57) – мономорфизмы, из (59) следует, что $A[Y]/(f,L)\to B'/LB'$ также является мономорфизмом. Таким образом, первое и последнее утверждения леммы снова следуют из (59). Лемма доказана. □

Теперь мы собираемся доказать (iii) и (iv). По лемме 22 идеал LB' кольца B' является радикальным и если $n\geqslant 3$, то он простой. Поэтому идеал $LB'\cap B$ радикален в B и если $n\geqslant 3$, то он простой. Поскольку кольцо B' цело над B, идеал $LB'\cap B$ является радикалом идеала LB кольца B. Рассмотрим морфизм $\gamma : B/LB\to B'/LB'$, индуцированный включением $B\subset B'$. Обозначим $E_1=\mathrm{Ker}\gamma$ и $E_2=\mathrm{Im}\gamma$, так что мы имеем точную последовательность

$$0\to E_1\to B/LB\to E_2\to 0.$$

Поэтому $\mathrm{Ass}_B(B/LB)\subset\mathrm{Ass}_B(E_1)\cup\mathrm{Ass}_B(E_2)$. Мы имеем $\mathrm{Ass}_B(E_2) = \mathrm{Ass}_B(B/(LB'\cap B))$, так как $E_2\simeq B/(LB'\cap B)$.

Включение $B\subset B'$ и умножение на $L : B'\to B'$ индуцируют коммутативную диаграмму гомоморфизмов B-модулей

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & B' & \longrightarrow & B'/B & \longrightarrow & 0 \\ & & \big\downarrow L & & \big\downarrow L & & \big\downarrow L & & \\ 0 & \longrightarrow & B & \longrightarrow & B' & \longrightarrow & B'/B & \longrightarrow & 0 \end{array}$$

с точными строками. Рассматривая Ker–Coker последовательность, соответствующую этой диаграмме, мы получаем точную последовательность

$$0 \longrightarrow E_1 \longrightarrow B'/B \xrightarrow{L} B'/B \longrightarrow 0,$$

т.е. E_1 может быть отождествлено с ядром гомоморфизма умножения на $L : B'/B \to B'/B$. Но $L \in \mathcal{U}_1$ (соответственно $L \in \mathcal{U}_2$). Поэтому $\mathrm{Ass}_B(E_1) \subset \mathcal{B}_{1,L}$ (соответственно $\mathrm{Ass}_B(E_1) \subset \mathcal{B}_{2,L}$). Далее, $\mathrm{Ass}_B(B/(LB' \cap B)) \cap (\mathcal{B}_0 \setminus \mathcal{B}_2) = \varnothing$, поскольку для всякого $\mathfrak{P} \in \mathrm{Ass}_B(B/(LB' \cap B))$ имеем $\dim \mathcal{Z}(\mathfrak{P}) = n-1$ и для всякого $\mathfrak{P} \in \mathcal{B}_0 \setminus \mathcal{B}_2$ имеем $\dim \mathcal{Z}(\mathfrak{P}) \leqslant n-2$. Отметим, что $\mathcal{B}_0 \setminus \mathcal{B}_1 \subset \mathcal{B}_0 \setminus \mathcal{B}_2$. Следовательно, $\mathrm{Ass}_B(E_1) = \mathcal{B}_{1,L}$ (соответственно $\mathrm{Ass}_B(E_1) = \mathcal{B}_{2,L}$), и также для всякого $\mathfrak{P} \in \mathrm{Ass}_B(E_1)$ множество $\mathcal{Z}(\mathfrak{P})$ не является неприводимой компонентой многообразия $\mathcal{Z}(LB' \cap B)$.

Таким образом,

$$\overline{k}[V \cap \mathcal{Z}(L)] \simeq B/(B \cap LB') \subset B'/LB' \simeq \overline{k}[\widetilde{V} \cap \mathcal{Z}(L)]. \tag{60}$$

Теперь из (60) и леммы 22 следует, что можно рассмотреть отождествления

$$A[Y]/(f, L) \subset B/(B \cap LB') \subset B'/LB'$$

и кольца $A[Y]/(f, L)$, $B/(B \cap LB')$, B'/LB' имеют одно и то же полное кольцо частных.

Наконец, нам требуется доказать (54). Достаточно показать, что

$$[\overline{k}(V_1 \cap \mathcal{Z}(L)) : \overline{k}(\mathcal{Z}(L))] = [\overline{k}(V_1) : \overline{k}(X_1, \ldots, X_n)]. \tag{61}$$

Но это эквивалентно равенству $\deg_Y f = \deg_Y (f \bmod L)$, которое выполняется, поскольку L не делит Δ_1.

Таким образом, утверждения (iii) и (iv) (по модулю (i) и (ii) для $n \geqslant 3$) доказаны. Докажем (v). Если $\mathfrak{P} \in \mathcal{B}_2 \setminus \mathcal{B}_3$, то $\dim \overline{p(\mathcal{Z}(\mathfrak{P}))} = \dim \mathcal{Z}(\mathfrak{P}) = n-1$, поскольку расширения колец (52) являются целыми. Следовательно, для всякого $\mathfrak{P} \in \mathcal{B}_2 \cup \mathcal{B}_3$ имеем $\dim \overline{p(\mathcal{Z}(\mathfrak{P}))} \geqslant n-2$. Поэтому $\dim(\mathfrak{P} \cap \mathcal{L}) \leqslant 2$ всякого $\mathfrak{P} \in \mathcal{B}_2 \cup \mathcal{B}_3$. Таким образом, $\mathcal{L} \setminus \mathfrak{P} \neq \varnothing$ для всякого $\mathfrak{P} \in \mathcal{B}_2 \cup \mathcal{B}_3$. Отсюда следует (v) (по модулю (i) и (ii) для $n \geqslant 3$).

Теперь наша цель – доказать утверждение (i) теоремы 4 для $n \geqslant 3$. Пусть $L_1, L_2 \in \overline{k}[X_1, \ldots, X_n]$ – две линейно независимые над $\overline{k}$ линейные формы от $X_1, \ldots, X_n$. Обозначим через $(L_1, L_2) \subset \overline{k}[X_1, \ldots, X_n, Y]$ идеал последнего кольца полиномов, порождённый L_1 и L_2. Рассмотрим следующие условия:

(a) $f \notin (L_1, L_2)$, и для всех $\mu_1, \mu_2 \in \overline{k}$, таких, что $\mu_1 \neq 0$ или $\mu_2 \neq 0$, линейная форма $\mu_1 L_1 + \mu_2 L_2$ не делит Δ_1;

(b) $\Delta_1 \notin (L_1, L_2)$.

Дискриминант Δ_1 является определителем матрицы Сильвестра многочленов $f, \partial f/\partial Y \in \overline{k}(X_1, \dots, X_n)[Y]$. Следовательно, если $f \in (L_1, L_2)$, то $\Delta_1 \in (L_1, L_2)$. Поэтому из условия (b) следует (a).

Пусть $L_1, L_2, L_3, \dots, L_n$ – базис пространства всех линейных форм от $X_1, \dots, X_n$. Положим $t = L_2/L_1$. Тогда

$$f \in \overline{k}[t, L_1, L_3, \dots, L_n, Y].$$

Более точно, существует многочлен $\widetilde{f} \in \overline{k}[X_1, \dots, X_n, Y]$, такой, что $f = \widetilde{f}(t, L_1, L_3, \dots, L_n, Y)$. Тогда $f \notin (L_1, L_2)$ в том и только в том случае, когда многочлен f является неприводимым в кольце

$$\overline{k}(t)[L_1, L_3, \dots, L_n, Y].$$

Это следует из леммы 12 работы [14] с $Y, L_3, \dots, L_n, L_1, L_2$ вместо $X_1, \dots, X_{n+1}$ (в дальнейшем мы ссылаемся также на леммы 13 и 14 из [14]; здесь следует осуществить аналогичную замену переменных).

Обозначим через $\mathcal{K}$ поле частных кольца $\overline{k}[X_1, \dots, X_n, Y]/(f)$. Далее, предположим, что многочлен f неприводим в кольце

$$\overline{k}(t)[L_1, L_3, \dots, L_n, Y]$$

. Тогда f является неприводимым элементом кольца

$$\overline{k(t)}[L_1, L_3, \dots, L_n, Y]$$

в том и только в том случае, если поле $\overline{k}(t)$ алгебраически замкнуто в $\mathcal{K}$, см. [20, лемма 4]. Простое прямое доказательство этого факта имеется также в лемме 13 работы [14].

В лемме 14 работы [14] мы доказываем, что если *выполняется условие* (a) *или условие* (b), *то поле* $\overline{k}(t)$ *алгебраически замкнуто в* $\mathcal{K}$.

Пусть $L_1', L_2', L_3' \in \overline{k}[X_1, \dots, X_n]$ – три произвольные линейно независимые линейные формы. Обозначим через $\mathcal{L}$ линейное пространство над $\overline{k}$ с базисом L_1', L_2', L_3'. Мы дополнительно покажем, что в утверждении (i) можно выбрать $L \in \mathcal{L}$. Осуществляя невырожденное линейное преобразование переменных $X_1, \dots, X_n$, можно предполагать без ограничения общности, что $L_1' = X_{n-1}$, $L_2' = X_n$, $L_3' = X_1$. Тогда существуют $\alpha_1, \alpha_2 \in k$, такие, что

$$(f^{(m_1)}\Delta_1)(X_1, \dots, X_{n-2}, \alpha_1 X_1, \alpha_2 X_1) \neq 0.$$

Положим $L_1 = X_1 - \alpha_1 X_{n-1}$, $L_2 = X_2 - \alpha_2 X_n$. Теперь очевидно выполняется условие (a). Следовательно, многочлен $f \in \overline{k(t)}[L_1, L_3, \dots, L_n, Y]$ является неприводимым. Кроме того, $\Delta_1 \bmod (L_1, L_2) \neq 0$ и $f^{(m_1)} \bmod (L_1, L_2) \neq 0$.

Рассмотрим аффинное пространство $\mathbb{A}^N(\overline{k(t)})$, $N = \binom{m_1+n}{n}$, многочленов от $X_1, \dots, X_n, Y$ степени не выше m_1. Известно (см., например, [18]), что множество всех неприводимых над $\overline{k(t)}$ многочленов степени m_1 от $X_1, \dots, X_n, Y$ с коэффициентами из $\overline{k(t)}$ является непустым открытым в топологии Зарисского подмножеством пространства $\mathbb{A}^N(\overline{k(t)})$. Следовательно, для всех $t^* \in \overline{k(t)}$, за исключением, может быть, конечного числа, многочлен $f|_{t=t^*} = \widetilde{f}(t^*, L_1, L_3, \dots, L_n, Y)$ является неприводимым в $\overline{k(t)}[L_1, L_3, \dots, L_n, Y]$. В частности, это верно для всех $t^* \in \overline{k}$, за исключением, может быть, конечного числа. Выберем и зафиксируем t^*, удовлетворяющее этому свойству. Положим $L = L_2 - t^* L_1$. Очевидно, согласно нашей конструкции для этой линейной формы L справедливо утверждение (i). Таким образом, утверждение (i) доказано, и дополнительно $L \in \mathcal{L}$.

Теперь наша цель – доказать утверждение (ii) теоремы 4 для $n \geqslant 3$. Напомним, что V_1 является аффинным алгебраическим многообразием с кольцом регулярных функций $A[Y]/(f)$ и $A = \overline{k}[X_1, \dots, X_n]$.

Обозначим через $\mathcal{U}'_n$ множество линейных форм $L = \sum\limits_{1 \leqslant i \leqslant n} l_i X_i \in \overline{k}[X_1, \dots, X_n]$, таких, что $l_1, \dots, l_n \in \overline{k}$ и $l_n \neq 0$. Для всякого $L \in \mathcal{U}'_n$ имеет место изоморфизм

$$\overline{k}[X_1, \dots, X_n]/(L) \simeq \overline{k}[X_1, \dots, X_{n-1}], \tag{62}$$

индуцированный подстановкой $X_n = -(l_1 X_1 + \ldots + l_n X_n)/l_n$. В дальнейшем для всякой линейной формы $L \in \mathcal{U}'_n$ мы будем отождествлять кольца в левой и правой частях (62) с помощью этого изоморфизма. Очевидно, $\mathcal{U}'_n$ является открытым в топологии Зарисского подмножеством аффинного пространства всех линейных форм от $X_1, \dots, X_n$ с коэффициентами из $\overline{k}$.

Можно определить аналогичным образом подмножества $\mathcal{U}'_i$ для $1 \leqslant i \leqslant n-1$ (мы оставляем подробности читателю). Согласно симметрии индексов $1, 2, \dots, n$ достаточно доказать следующую лемму.

Лемма 23. *Множество $\mathcal{U}_4 \cap \mathcal{U}'_n$ является открытым в топологии Зарисского подмножеством аффинного пространства всех линейных форм от $X_1, \dots, X_n$ с коэффициентами из $\overline{k}$.*

Доказательство. Линейная форма L принадлежит $\mathcal{U}_4$ тогда и только тогда, когда выполняются следующие два условия:

1) идеал (f, L) является простым в $\overline{k}[X_1, \ldots, X_n, Y]$,
2) L не делит $f^{(m_1)}\Delta_1$.

Очевидно, множество линейных форм, удовлетворяющих условию 2), является открытым в топологии Зарисского подмножеством аффинного пространства $\mathbb{A}^n(\overline{k})$. Поэтому достаточно доказать, что множество всех $L \in \mathcal{U}'_n$, удовлетворяющих условию 1), является открытым в топологии Зарисского подмножеством пространства $\mathbb{A}^n(\overline{k})$.

Рассмотрим аффинное пространство $\mathbb{A}^{N_1}(\overline{k})$, $N_1 = \binom{m_1+n-1}{n-1}$, многочленов от $X_1, \ldots, X_{n-1}, Y$ степени не выше m_1. Известно (см., например, [18]), что множество $\mathcal{V}$ всех неприводимых над $\overline{k}$ многочленов степени m_1 от $X_1, \ldots, X_{n-1}, Y$ с коэффициентами из $\overline{k}$ является открытым в топологии Зарисского подмножеством пространства $\mathbb{A}^{N_1}(\overline{k})$. Пусть $L = l_1 X_1 + \ldots + l_n X_n \in \mathcal{U}'_n$, где все коэффициенты l_i лежат в $\overline{k}$. Тогда $L \in \mathcal{U}_4 \cap \mathcal{U}'_n$ в том и только в том случае, если выполнено условие 2) и

$$f\left(X_1, \ldots, X_{n-1}, -\sum_{1 \leqslant i \leqslant n-1} l_n^{-1} l_i X_i\right) \in \mathcal{V}.$$

Лемма доказана. □

Отсюда немедленно следует (ii).

Мы доказали выше, что существует $L \in \mathcal{L} \cap \mathcal{U}_4$. Отсюда вытекает (vi). Теорема доказана. □

Замечание 14. Множества $\mathcal{U}_i$, $1 \leqslant i \leqslant 4$, из утверждения теоремы 4 удовлетворяют следующему свойству. Для всех $0 \neq \lambda \in \overline{k}$ и $L \in \mathcal{U}_i$ линейная форма λL лежит в $\mathcal{U}_i$.

Следствие 2. *В условиях теоремы* 4 *пусть* $L \in \mathcal{U}_2 \cap \mathcal{U}_3 \cap \mathcal{U}_4$ *– линейная форма. Пусть* W *– множество всех гладких точек алгебраического многообразия* $V \cap \mathcal{Z}(L) \setminus p^{-1}(x)$. *Тогда* W *является плотным открытым в топологии Зарисского подмножеством алгебраического многообразия* $V \cap \mathcal{Z}(L)$, *всякая точка* $z \in W$ *– гладкая точка многообразия* V, *локальное кольцо* $\mathcal{O}_{z, V \cap \mathcal{Z}(L)}$ *алгебраического многообразия* $V \cap \mathcal{Z}(L)$ *в точке* z *изоморфно* $\mathcal{O}_{z,V}/L\mathcal{O}_{z,V}$. *В частности,* *если $V \subset \mathbb{A}^N(\overline{k})$ для некоторого N и p – линейная проекция на первые n координат, то пересечение касательных пространств*

$$T_{z,V} \cap \mathcal{Z}(L) \tag{63}$$

многообразий V и $\mathcal{Z}(L)$ (мы отождествляем $T_{z,\mathcal{Z}(L)}$ с $\mathcal{Z}(L)$) в точке z трансверсально, т.е. $\dim T_{z,V} \cap \mathcal{Z}(L) = n-1$, и существует система локальных параметров $h_1, \ldots, h_{N-n}$ многообразия V в точке z, такая, что $L, h_1, \ldots, h_{N-n}$ является системой локальных параметров пересечения $V \cap \mathcal{Z}(L)$ в точке z.

Доказательство. Мы можем предполагать без ограничения общности, что $V \subset \mathbb{A}^N(\overline{k})$ и p является линейной проекцией на первые n координат. Очевидно, W является плотным открытым в топологии Зарисского подмножеством пересечения $V \cap \mathcal{Z}(L)$. Пусть $z \in W$ – гладкая точка многообразия $V \cap \mathcal{Z}(L)$. Обозначим через $\mathcal{O}_z$ локальное кольцо в точке z алгебраического многообразия $\mathbb{A}^N(\overline{k})$. Обозначим через $I(V)$ идеал аффинного алгебраического многообразия $V \subset \mathbb{A}^N(\overline{k})$. Таким образом, $\overline{k}[V] = A_1/I(V)$, где $A_1 = \overline{k}[X_1, \ldots, X_N]$. Тогда согласно утверждению (iii) справедливо равенство

$$\mathcal{O}_{z,V\cap\mathcal{Z}(L)} = \mathcal{O}_z/(I(V)\mathcal{O}_z + L\mathcal{O}_z).$$

Поэтому L является одним из локальных параметров в точке z алгебраического многообразия $V \cap \mathcal{Z}(L)$ (рассматриваемого как подмногообразие в $\mathbb{A}^N(\overline{k})$), и другие такие локальные параметры могут быть выбраны из $I(V)$. Следовательно, существует система локальных параметров $L, h_1, \ldots, h_{N-n}$ в точке z пересечения $V \cap \mathcal{Z}(L)$, такая, что $h_1, \ldots, h_{N-n} \in I(V)$.

Отсюда следует, что точка z является гладкой точкой многообразия V, касательное пространство $T_{z,V}$ есть $\mathcal{Z}(d_z h_1, \ldots, d_z h_{N-n})$ и пересечение касательных пространств (63) трансверсально. Следствие доказано. □

Следствие 3. *Пусть $n \geqslant 3$. Пусть $f \in \overline{k}[X_1, \ldots, X_n]$ – неприводимый многочлен с $\deg f \geqslant 1$. Предположим, что f не является однородным многочленом относительно $X_1, \ldots, X_n$ или $n \geqslant 4$. Пусть $\mathcal{L}$ – линейное подпространство пространства всех линейных форм от $X_1, \ldots, X_n$ с коэффициентами из $\overline{k}$. Предположим, что $\dim \mathcal{L} \geqslant 3$. Тогда существует непустое открытое в топологии Зарисского подмножество*

$\mathcal{U}'''$ подпространства $\mathcal{L}$, такое, что для всякого $L \in \mathcal{U}'''$ элемент $f \bmod L \in \overline{k}[X_1, \ldots, X_n]/(L)$ является неприводимым.

Доказательство. Предположим, что f не является однородным многочленом относительно $X_1, \ldots, X_n$. Рассмотрим многочлен

$$F = Y^{\deg_{X_1,\ldots,X_n} f} f(X_1/Y, \ldots, X_n/Y).$$

Тогда многочлен $F \in \overline{k}[X_1, \ldots, X_n, Y]$ неприводим. Многочлен $F \bmod L$ неприводим тогда и только тогда, когда $f \bmod L$ является неприводимым. Если $\mathrm{char}(\overline{k}) = 0$, то положим $F_1 = F$. Если $\mathrm{char}(\overline{k}) = p > 0$, то пусть $s \geqslant 0$ – максимальное целое число, такое, что $F \in \overline{k}[X_1, \ldots, X_n, Y^{p^s}]$, и положим $F_1 = F(X_1, \ldots, X_n, Y^{p^{-s}})$. Тогда многочлен $F_1 \in \overline{k}[X_1, \ldots, X_n, Y]$ неприводим и $\partial F/\partial Y \neq 0$. Если $\mathrm{char}(\overline{k}) > 0$ и $s \geqslant 1$, то существует такое i, $\quad 1 \leqslant i \leqslant n$, $\quad$ что $\partial F/\partial X_i \neq 0$, поскольку f неприводим и, следовательно, сепарабелен. Мы можем предполагать без ограничения общности, осуществляя линейное преобразование переменных $X_1, \ldots, X_n$, что $i = n$.

Применяя теорему 4 (vi) к алгебраическому многообразию $\mathcal{Z}(F_1)$ и многочлену F_1 (вместо V и f), мы заключаем, что существует непустое открытое в топологии Зарисского подмножество $\mathcal{U}' \subset \mathcal{L}$, такое, что для всякой формы $L \in \mathcal{U}'$ многочлен $F_1 \bmod L$ является неприводимым и $\partial(F_1 \bmod L)/\partial Y \neq 0$. Пусть $L = l_1X_1 + \ldots + l_nX_n$, где все l_i лежат в $\overline{k}$ и $l_n \neq 0$. Тогда (см. выше) $F_1 \bmod L \in \overline{k}[X_1, \ldots, X_{n-1}]$. Известно (см., например, [4]), что в рассматриваемом случае многочлен $F \bmod L$ является неприводимым тогда и только тогда, когда он сепарабелен относительно $X_1, \ldots, X_{n-1}, Y$. Если $\mathrm{char}(\overline{k}) = 0$ или $s = 0$, то выполняется последнее условие. Если $\mathrm{char}(\overline{k}) > 0$ и $s \geqslant 1$, то $\partial F/\partial X_n \neq 0$. Следовательно, в этом случае условие $\partial(F \bmod L)/\partial X_{n-1} \neq 0$ определяет открытое в топологии Зарисского подмножество $\mathcal{U}'' \subset \mathcal{L}$. Положим $\mathcal{U}''' = \mathcal{U}' \cap \mathcal{U}''$. Таким образом, $\mathcal{U}'''$ является требуемым открытым в топологии Зарисского подмножеством подпространства $\mathcal{L}$.

В случае, когда $n \geqslant 4$, можно осуществить невырожденное линейное преобразование первых $X_1, \ldots, X_n$ и предполагать без ограничения общности, что $\mathrm{lc}_{X_n} f = 1$ и $\partial F/\partial X_1 \neq 0$. Кроме того, мы можем предполагать, не умаляя общности, что $X_n \notin \mathcal{L}$, если $\dim \mathcal{L} < n$. После этого мы полагаем $X_n = Y$ и, применяя лемму 23, получаем линейную форму L, удовлетворяющую требуемым условиям. Теперь аналогично доказательству леммы 23 мы устанавливаем существование требуемого открытого в топологии Зарисского подмножества $\mathcal{U}'''$ подпространства $\mathcal{L}$ в рассматриваемом случае. Следствие доказано. □

Лемма 24. *Пусть k – совершенное поле произвольной характеристики. В обозначениях из введения для всякого α, $\sigma+1 \leqslant \alpha \leqslant n-1$, множество $\mathcal{U}_\alpha$ является непустым открытым в топологии Зарисского подмножеством в $\mathbb{A}^{(r+1)(\alpha-\sigma)}(\overline{k})$.*

Доказательство. Используя вложение Веронезе, мы будем предполагать без ограничения общности, что $d'=1$. По теореме 4 существует $\lambda=(L_{s+1},\dots,L_\sigma)$, см. введение, такое, что неприводимые над $\overline{k}$ компоненты алгебраических многообразий W и $W\cap\mathcal{Z}(L_{s+1},\dots,L_\sigma)$ находятся во взаимно однозначном соответствии, задаваемом правилом $E\mapsto E\cap\mathcal{Z}(L_{s+1},\dots,L_\sigma)$, и пересечение $W\cap\mathcal{Z}(L_{s+1},\dots,L_\sigma)$ трансверсально (всё это условия общего положения для λ). Заменяя W на W_λ, мы будем в дальнейшем предполагать, не умаляя общности, что $s=\sigma$.

В случае ненулевой характеристики, заменяя k на совершенное замыкание $k(t)^{p^{-\infty}}$ некоторого чисто трансцендентного расширения $k(t)$ поля k, мы будем предполагать без ограничения общности, что поле k является бесконечным.

Рассмотрим сначала случай нулевой характеристики (в конце доказательства мы вернёмся к случаю ненулевой характеристики). Покажем, что $\mathcal{U}_\alpha\neq\varnothing$. Пусть $L''\in\mathcal{U}_0''$. Положим $p_{L''}=p_{\lambda,L''}$ (сейчас $\lambda=()$, поскольку $s=\sigma$). Предположим, что для целого числа i, $\sigma\leqslant i<\alpha$,

(∗) существуют линейные формы $L'_{\sigma+1},\dots,L'_i$, $\sigma+1\leqslant i<\alpha$, такие, что все L'_j, $s+1\leqslant j\leqslant i$, являются линейными комбинациями форм $L''_0,L''_{\sigma+1},\dots,L''_n$ с целыми коэффициентами из k и $(L'_{\sigma+1},\dots,L'_i)\in\mathcal{U}_i$.

Тогда по леммам 11 и 14 работы [10] морфизм $W\cap\mathcal{Z}(L'_{\sigma+1},\dots,L'_i)\to\mathcal{Z}(X_1,\dots,X_{i-\sigma})=\mathbb{P}^{n-i}(\overline{k})$, индуцированный морфизмом $p_{L''}$, является доминантным. Он индуцирует морфизм алгебраических многообразий $\operatorname{con}(W)\cap\mathcal{Z}(L'_{\sigma+1},\dots,L'_i)\to\mathbb{A}^{n-i+1}(\overline{k})$. Пусть

$$\operatorname{con}(W)\cap\mathcal{Z}(L'_{\sigma+1},\dots,L'_i)\setminus\mathcal{Z}(L''_0,L''_{\sigma+1},\dots,L''_n)=\bigcup_{j\in J}E_j,$$

где E_j, $J\in J$, – конечное семейство аффинных непустых открытых в топологии Зарисского подмножеств многообразия $\operatorname{con}(W)\cap$

$\mathcal{Z}(L'_{\sigma+1}, \ldots, L'_i) \setminus \mathcal{Z}(L''_0, L''_{\sigma+1}, \ldots, L''_n)$. Тогда по теореме 4, применённой к каждому морфизму $E_j \to \mathbb{A}^{n-i+1}(\overline{k})$, $j \in J$, существует линейная форма L''_{i+1} (из пересечения по всем $j \in J$ открытых в топологии Зарисского подмножеств из утверждения теоремы 4), такая, что выполняется свойство $(*)$ с $i+1$ вместо i. Таким образом, мы доказали существование $(L'_{\sigma+1}, \ldots, L'_\alpha) \in \mathcal{U}_\alpha$ индукцией по i.

Докажем, что $\mathcal{U}_\alpha$ является открытым в топологии Зарисского подмножеством в $\mathbb{A}^{(n-\alpha)(n+1)}(\overline{k})$. Сначала покажем, что $\mathcal{U}_\alpha$ является конструктивным подмножеством пространства $\mathbb{A}^{(n-\alpha)(n+1)}(\overline{k})$. Вероятно, это может быть доказано при помощи теории первого порядка алгебраически замкнутых полей. Но мы дадим прямое доказательство.

Напомним, что по определению подмножество алгебраического многообразия F является конструктивным в том и только в том случае, если оно является объединением $\cup_{\gamma \in \Gamma}(F'_\gamma \cap F''_\gamma)$, где число индексов $\#\Gamma$ конечно, все F'_γ являются открытыми в топологии Зарисского подмножествами множества F и все F''_γ являются замкнутыми в топологии Зарисского подмножествами множества F. Мы будем использовать следующий критерий.

- *Предположим, что $E \subset F$ и для всякого замкнутого подмногообразия $E' \subset F$, такого, что $E' \cap E$ является плотным относительно топологии Зарисского в E', существует непустое открытое в топологии Зарисского подмножество $E'' \subset E'$, такое, что $E'' \subset E$. Тогда E является конструктивным подмножеством множества F.*

Доказательство этого критерия осуществляется индукцией по $\dim \overline{E}$ (здесь $\overline{E}$ – замыкание E относительно топологии Зарисского). В самом деле, существует плотное открытое в топологии Зарисского подмножество $E''' \subset \overline{E}$, такое, что $E''' \subset E$. Можно заменить E на $E \setminus E'''$. Очевидно, $\dim \overline{E \setminus E'''} < \dim \overline{E}$. В данном критерии можно предполагать дополнительно, что E' является неприводимым над алгебраическим замыканием основного поля.

Покажем, что $\mathcal{U}_\alpha$ удовлетворяет сформулированному критерию. Пусть E' – замкнутое неприводимое над $\overline{k}$ подмногообразие в $\mathbb{A}^{(n-\alpha)(n+1)}(\overline{k})$ и $(L'_{\sigma+1}, \ldots, L'_\alpha) \in E' \cap \mathcal{U}_\alpha$. Расширим основное поле k до k_u, см. введение. Мы будем предполагать без ограничения общности, что все коэффициенты линейных форм U_i, $\sigma+1 \leqslant i \leqslant \alpha$, являются бесконечно близкими к соответствующим коэффициентам линейных форм L'_i. Предположим, что $(L''_{\sigma+1}, \ldots, L''_\alpha) \in E' \cap \mathcal{U}_\alpha$, все линейные формы $L''_i - L'_i$, $\sigma + 1 \leqslant i \leqslant \alpha$, имеют коэффициенты из $\overline{k_u}$, которые бесконечно малы относительно поля k (или равны нулю). Тогда по лемме 9 работы [12] $(L''_{\sigma+1}, \ldots, L''_\alpha) \in \mathcal{U}''_\alpha$. По лемме 11 из [12] $\mathrm{st}(W(L''_{\sigma+1}, \ldots, L''_\alpha)) = W(L'_{\sigma+1}, \ldots, L'_\alpha)$. Поэтому по лемме 1 из [12] степень каждой неприводимой над $\overline{k_u}$ компоненты многообразия $W(L''_{\sigma+1}, \ldots, L''_\alpha)$ не меньше $\deg W(L'_{\sigma+1}, \ldots, L'_\alpha)$. Следовательно, многообразие $W(L''_{\sigma+1}, \ldots, L''_\alpha)$ является неприводимым над $\overline{k_u}$.

Далее можно выбрать $(L''_{\sigma+1}, \ldots, L''_\alpha)$ так, что дополнительно $\xi = (L''_{\sigma+1}, \ldots, L''_\alpha)$ является общей точкой многообразия E'. Обозначим через $\overline{k}(\xi)$ поле, порождённое над $\overline{k}$ координатами точки ξ. Мы будем отождествлять его с $\overline{k}(E')$. Существует линейная проекция $\pi : W(L''_{\sigma+1}, \ldots, L''_\alpha) \to \mathbb{P}^{n-\alpha+1}(\overline{k})$, $(X_0 : \ldots : X_n) \mapsto (Z_0 : \ldots : Z_{n-\alpha+1})$, такая, что все Z_j, $0 \leqslant j \leqslant n - \alpha + 1$, являются линейными формами с коэффициентами из k, образ $\pi(W(L''_{\sigma+1}, \ldots, L''_\alpha))$ равен $\mathcal{Z}(H)$ для сепарабельного многочлена $H \in \overline{k}(\xi)[X_0, \ldots, X_{n-\alpha+1}]$, морфизм $W(L''_{\sigma+1}, \ldots, L''_\alpha) \to \mathcal{Z}(H)$, индуцированный морфизмом π, является конечным и $\deg W(L''_{\sigma+1}, \ldots, L''_\alpha) = \deg H$ (это всё условия общего положения для линейной проекции). Следовательно, число элементов неприводимых над $\overline{k(\xi)}$ множителей многочлена H равно числу неприводимых над $\overline{k}$ компонент многообразия W. Заменяя H и все L''_j на cH и cL''_j с подходящим ненулевым $c \in \overline{k}[E']$, мы будем предполагать без ограничения общности, что $H \in \overline{k}[E'][X_0, \ldots, X_{n-\alpha+1}]$ и $L''_j \in \overline{k}[E'][X_0, \ldots, X_n]$ для всех j. Очевидно, многочлен $H(Z_0, \ldots, Z_{n-\alpha+1})$ обращается в нуль тождественно на $W(L''_{\sigma+1}, \ldots, L''_\alpha)$. Теперь рассмотрим гомоморфизм $\overline{k}[E'] \to \overline{k}$, задающий точку $\widetilde{\xi} \in E'$. Этот гомоморфизм продолжается естественным образом до гомоморфизма колец многочленов

$$\overline{k}[E'][X_1, \ldots, X_n] \to \overline{k}[X_1, \ldots, X_n].$$

Обозначим через $\widetilde{H}$ и $\widetilde{L}_j$ образы многочленов H и L'_j при этом гомоморфизме. Существует непустое открытое в топологии Зарисского подмножество $E^{(1)} \subset E'$, такое, что если $\widetilde{\xi} \in E^{(1)}$, то $(\widetilde{L}_{\sigma+1}, \ldots, \widetilde{L}_\alpha) \in \mathcal{U}''_\alpha$, образ $\pi(W(\widetilde{L}_{\sigma+1}, \ldots, \widetilde{L}_\alpha))$ равен $\mathcal{Z}(\widetilde{H})$, морфизм $W(\widetilde{L}_{\sigma+1}, \ldots, \widetilde{L}_\alpha) \to \mathcal{Z}(\widetilde{H})$, индуцированный морфизмом π, конечен и $\deg W(\widetilde{L}_{\sigma+1}, \ldots, \widetilde{L}_\alpha) = \deg \widetilde{H}$, $\widetilde{H} \in \overline{k}[X_0, \ldots, X_{n-\alpha+1}]$ сепарабелен. Это утверждение доказывается непосредственно (мы оставляем детали читателю). Наконец, существует непустое открытое в топологии Зарисского подмножество

$E^{(2)} \subset E^{(1)}$, такое, что для всякой точки $\widetilde{\xi} \in E^{(2)}$ число неприводимых над $\overline{k}$ множителей многочлена $\widetilde{H}$ равно числу неприводимых над $\overline{k(\xi)}$ множителей многочлена H. Действительно, в лемме 23 мы доказали, что $\mathcal{U}_4 \cap \mathcal{U}'_n$ является открытым в топологии Зарисского, и последнее утверждение доказывается аналогичным образом.

Таким образом, множество $\mathcal{U}_\alpha$ является конструктивным. Наконец, как мы видели в доказательстве, для всякой точки $L' \in \mathcal{U}_\alpha$ существует бесконечно малая окрестность $\mathcal{W}$ точки L' в $\mathcal{U}''_\alpha$, такая, что $\mathcal{W} \subset \mathcal{U}_\alpha$. Очевидно, это возможно только в случае, если $\mathcal{U}_\alpha$ является открытым в топологии Зарисского. Лемма доказана в нулевой характеристике.

В случае ненулевой характеристики достаточно обобщить все леммы из [10–13], которые использовались в доказательстве, на случай ненулевой характеристики при условии, что расширение полей $k(W) \supset k(W')$ является сепарабельным. Это возможно сделать без затруднений. Мы оставляем подробности читателю. Можно определить бесконечно малые величины в случае ненулевой характеристики при помощи нормирований, см. [2]. Например, в наиболее простом случае для трансцендентного над k элемента ε мы имеем нормирование $v : k(\varepsilon) \to \mathbb{Z} \cup \{+\infty\}$ над k, такое, что $v(\varepsilon) = 1$. Оно может быть продолжено до нормирования $\overline{v} : \overline{k(\varepsilon)} \to \mathbb{Q} \cup \{+\infty\}$. По определению ненулевой элемент $a \in \overline{k(\varepsilon)}$ является бесконечно малым тогда и только тогда, когда $\overline{v}(a) > 0$. Лемма доказана. □

Литература

1. М. Бальдассарри, *Алгебраические многообразия.* М., Издательство иностранной литературы, 1961.
2. Н. Бурбаки, *Коммутативная алгебра.* М., Мир, 1971.
3. Н. Г. Чеботарев, *Теория алгебраических функций.* М.-Л., ОГИЗ, 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. Л. 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.* — Труды Санкт-Петербургского мат. общества **7** (1999), 230–266.
7. А. Л. Чистов, *Сильная версия основного разрешающего алгоритма для экзистенциальной 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**, вып. 3 (2012), 199–222.
15. A. L. Chistov, *Polynomial-time computation of the dimensions of components of algebraic varieties in zero-characteristic.* — J. Pure Appl. Algebra **117, 118** (1997), 145–175.
16. A. Chistov, H. Fournier, L. Gurvits, P. Koiran, *Vandermonde matrices, NP-completeness, and transversal subspaces.* — Found. Comput. Math. **3**, No. 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, pp. 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.
22. А. Л. Чистов, *Детерминированный алгоритм полиномиальный сложности для первой теоремы Бертини. II.* — Зап. научн. семин. ПОМИ **421** (2014), 214–249.

Chistov A. L. A deterministic polynomial-time algorithm for the first Bertini theorem. III.

Consider a projective algebraic variety W that is an irreducible component of the set of all common zeros 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 the input. This work concludes a tree-part series of papers.

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

Поступило 6 октября 2014 г.