Записки научных
семинаров ПОМИ
Том 373, 2009 г.

A. L. Chistov

AN OVERVIEW OF EFFECTIVE NORMALIZATION OF A NONSINGULAR IN CODIMENSION ONE PROJECTIVE ALGEBRAIC VARIETY

Abstract. Let V be a nonsingular in codimension one projective algebraic variety of degree D and of dimension n. Then the construction of the normalization of V can be reduced canonically within the time polynomial in the size of the input and $D^{n^{O(1)}}$ to solving a linear equation $aX + bY + cZ = 0$ over a polynomial ring. We describe a plan with all lemmas to prove this result.

Introduction

Let k be a field with algebraic closure $\overline{k}$. Let $V \subset \mathbb{P}^N(\overline{k})$ be a projective algebraic variety defined over k and irreducible over $\overline{k}$ of dimension n and degree D. Then the construction of the normalization of V can be divided into two parts:

(I) construction of a finite birational isomorphism $V' \to V$ such that the variety V' is nonsingular in codimension one; this means by definition that the dimension $\dim \operatorname{Sing}(V') \leqslant n-2$, where $\operatorname{Sing}(V')$ is the variety of singular points of V',

(II) construction of the normalization of V'.

In the case of zero-characteristic $\operatorname{char}(k) = 0$ one can solve (I) within the polynomial time using the ideas from [1]. Everything is reduced here to the case of the curves $n = 1$. We hope to describe this construction in detail in another paper. To obtain a similar effective algorithm for (I) in the case of nonzero characteristic is an open problem.

In this paper, we concentrate ourself on the problem (II). So we shall suppose in what follows that $V = V'$ is nonsingular in codimension one. We shall show that the construction of the normalization of V can be reduced canonically within the time polynomial in the size of the input

Key words and phrases. algebraic variety, projective variety, normalization, complexity.

and $D^{n^{O(1)}}$ to solving a linear equation $aX+bY+cZ=0$ over a polynomial ring. We describe a plan with statements of main lemmas to prove this result. We hope that the detailed publication with all proofs will appear later (we are going also to describe there how to solve (I) for a zero-characteristic ground field).

In the case of surfaces $n=2$ problem (II) can be solved within the polynomial time without difficulties (it is not our aim now). Besides that, the case $n=2$ can be easily reduced to $n=3$. So we shall suppose in what follows without loss of generality that $n \geqslant 3$. We assume that V is given by its generic point, see [2]. Notice also here that constructing an appropriate linear projection one can always reduce the general case to the particular one: $N=n+2$ (but we don't give the details now).

So we shall suppose in what follows that $N=O(n)$.

For arbitrary polynomials $g_1,\dots,g_m \in \overline{k}[X_0,\dots,X_N]$ we shall denote by $\mathcal{Z}(g_1,\dots,g_m)$ the set of all common zeroes of these polynomials in $\mathbb{P}^N(\overline{k})$ (in what follows we shall use the similar notations for the sets of common zeroes of others polynomials or polynomial ideals in projective or affine spaces).

Definition 1. *Let $\rho : E \to W$ be a morphism of algebraic varieties defined over the field $\overline{k}$. Suppose that $\rho(E)$ is closed in the Zariski topology in W, the total quotient rings of the rings of regular functions $\overline{k}(E) = \overline{k}(\rho(E))$ and ρ induces the finite morphism $E \to \rho(E)$. Then the variety $\mathrm{Si}\,(\rho)$ of self-intersection of ρ is the closure in the Zariski topology of the subset of $\rho(E)$ consisting of all points z such that the number of elements $\#\rho^{-1}(z) > 1$. Let W be an arbitrary algebraic variety, $\widetilde{W}$ be normalization of W and $\rho : \widetilde{W} \to W$ be the morphism of normalization. Then the variety $\mathrm{Si}\,(W)$ of self-intersection of W is $\mathrm{Si}\,(\rho)$.*

Let the integer a_0 be equal to 2 if $\mathrm{char}\,(k) \neq 2$ and 3 if $\mathrm{char}\,(k)=2$. Let $u=\{u_{i,j}\}$, $0 \leqslant i \leqslant n+1$, $1 \leqslant j \leqslant \binom{N+a_0}{a_0}$, be a family of elements algebraically independent over k. Let us fix a one-to-one correspondence between the set of integers $\{1,\dots,\binom{N+a_0}{a_0}\}$ and the set of monomials in $X_0,\dots,X_N$ with coefficient 1 of degree a_0. Denote by H_i, $0 \leqslant i \leqslant n+1$, the generic homogeneous polynomial of degree a_0. The coefficients of this polynomial are from the family $\{u_{i,j}\}$, $1 \leqslant j \leqslant \binom{N+a_0}{a_0}$ according to the fixed one-to-one correspondence. Denote by $k_u = k(u)$ the extension of the field k by all the elements of the family u. Hence $H_i \in k_u[X_0,\dots,X_N]$, $0 \leqslant i \leqslant n+1$. In what follows we shall denote the algebraic variety $V(\overline{k_u})$

again by V (this will not lead to an ambiguity). Denote by

$$q_H : V \to \mathbb{P}^{n+1}(\overline{k_u}), \qquad (X_0 : \ldots : X_N) \mapsto (H_0 : \ldots : H_{n+1})$$
$$p_H : V \to \mathbb{P}^{n}(\overline{k_u}), \qquad (X_0 : \ldots : X_N) \mapsto (H_0 : \ldots : H_{n})$$

the rational morphisms of projective algebraic varieties over the field $\overline{k_u}$. Further, let

$$p_0 : \mathbb{P}^{n+1}(\overline{k}) \to \mathbb{P}^{n}(\overline{k}), \quad (X_0 : \ldots : X_{n+1}) \mapsto (X_0 : \ldots : X_n)$$

be the morphism of the linear projection (we shall use the same notation for this morphism over the field $\overline{k_u}$).

Theorem 1. *Let $V \subset \mathbb{P}^N(\overline{k})$ be a defined over k and irreducible over $\overline{k}$ nonsingular in codimension one projective algebraic variety of dimension $n \geqslant 3$ and degree D. Then the following properties hold.*

(a) *The morphism p_H is regular finite dominant separable and defined over the field k_u. The degree of p_H is $a_0^n D$, i.e., the degree of the extension of fields of rational functions $[k_u(V) : k_u(H_1/H_0, \ldots, H_n/H_0)] = a_0^n D$.*

(b) *The morphism q_H is defined over the field k_u and induces the finite birational isomorphism $V \to q_H(V)$ where $q_H(V) \subset \mathbb{P}^{n+1}(\overline{k_u})$ is a closed affine algebraic variety defined over the field k_u. For every smooth point $z \in V$ the differential $d_z q_H$ (of the morphism q_H at the point z) is a monomorphism. Further, $q_H(z)$ is a smooth point of the algebraic variety $q_H(V)$ if and only if $q_H(z) \notin \mathrm{Si}\,(q_H)$.*

(c) *The algebraic variety $q_H^{-1}(\mathrm{Si}\,(q_H))$ is defined over the field k_u, irreducible over $\overline{k_u}$ and is of dimension $n-1$. Hence the algebraic variety $\mathrm{Si}\,(q_H)$ is defined over the field k_u, irreducible over $\overline{k_u}$ and is of dimension $n-1$. In particular $\mathrm{Si}\,(q_H) \neq \emptyset$.*

(d) *The equality $q_H(V) = \mathcal{Z}(\Phi_H)$ holds where $\Phi_H \in k_u[X_0, \ldots, X_{n+1}]$ is an irreducible over $\overline{k_u}$ homogeneous polynomial such that $\deg_{X_i} \Phi_H = \deg_{X_0,\ldots,X_{n+1}} \Phi_H = a_0^n D$ for all $1 \leqslant i \leqslant n+1$, in particular, leading coefficients $\mathrm{lc}_{X_i} \Phi_H \in k_u$ for all $1 \leqslant i \leqslant n+1$. Besides that, for every $0 \leqslant i \leqslant n+1$ the polynomial Φ_H is separable with respect to X_i, i.e., $\partial \Phi_H / \partial X_i \neq 0$.*

There is a nonempty open in the Zariski topology subset $\mathcal{V}$ of $\mathrm{Si}\,(q_H)$ satisfying the following properties.

(e) *For every* $z \in \mathcal{V}$ *the inverse image* $q_H^{-1}(z) = \{z_1, z_2\}$ *consists of two distinct points such that* z_1 *and* z_2 *are smooth points of* V, *the differentials* $d_{z_1} q_H$ *and* $d_{z_2} q_H$ *are monomorphisms, and the intersection* $d_{z_1} q_H(T_{z_1,V}) \cap d_{z_2} q_H(T_{z_2,V})$ *of the images of the tangent spaces* $T_{z_1,V}$ *and* $T_{z_2,V}$ *(of* V *in the points* z_1 *and* z_2*) is transversal, i.e., the dimension*

$$\dim d_{z_1} q_H(T_{z_1,V}) \cap d_{z_2} q_H(T_{z_2,V}) = n - 1.$$

(f) *For every* $z \in p_0(\mathcal{V})$ *the inverse image* $p_H^{-1}(z)$ *consists of* $a_0^n D$ *distinct smooth points of* V *and for every* $y \in p_H^{-1}(z)$ *the differential* $d_y p_H$ *of the morphism* p_H *in the point*

y *is an isomorphism. Moreover,* $\mathcal{V} = p_0^{-1} p_0(\mathcal{V}) \cap \mathrm{Si}\,(q_H)$ *and* $p_0(\mathcal{V})$ *is an open in the Zariski topology subset of the closed irreducible over* $\overline{k}$ *projective algebraic variety* $p_0(\mathrm{Si}\,(q_H))$.

(g) *The morphism of defined over* k_u *and irreducible over* $\overline{k_u}$ *algebraic varieties* $q_H^{-1}(\mathrm{Si}\,(q_H)) \to \mathrm{Si}\,(q_H)$ *induced by* q_H *is finite dominant and separable of degree* 2. *The morphism of defined over* k_u *projective algebraic varieties* $q_1 : \mathrm{Si}\,(q_H) \to p_0(\mathrm{Si}\,(q_H))$ *induced by* p_0 *is a finite birational isomorphism. For every* $y \in \mathcal{V}$ *the point* $q_1(y)$ *is a smooth point of* $p_0(\mathrm{Si}\,(q_H))$ *and the differential* $d_y q_1$ *is an isomorphism.*

Let $\mathrm{ver}_{a_0} : \mathbb{P}^N(\overline{k}) \to \mathbb{P}^{N_1}(\overline{k})$, $N_1 = \binom{N+a_0}{a_0} - 1$ be the Veronese mapping of degree a_0. We have $\deg \mathrm{ver}_{a_0}(V) = a_0^n D$ and the projective algebraic varieties V and $\mathrm{ver}_{a_0}(V)$ are isomorphic. Hence it is sufficient to construct the normalization of $\mathrm{ver}_{a_0}(V) = W$.

Denote by B the homogeneous ring over the field k_u of the projective algebraic variety W. To obtain the normalization of W it is sufficient now to construct the integral closure $\overline{B}$ of B in its field of fractions. By the natural isomorphism $V \to W$ one can identify B with the subring of the homogeneous ring of V over the field k_u generated by all the homogeneous polynomials in $X_0, \ldots, X_N$ of degree a_0 with coefficients from k_u. Hence we have a homomorphism of k_u-algebras $k_u[X_0, \ldots, X_{n+1}] \to B$, $X_i \mapsto H_i$, $0 \leqslant i \leqslant n+1$, which induces the inclusion

$$k_u[X_0, \ldots, X_{n+1}]/(\Phi_H) \subset B, \tag{1}$$

see the proof of Theorem 1. Denote for brevity $A = k_u[X_0, \ldots, X_n]$, $\Phi = \Phi_H \in A$, and $\omega = X_{n+1} \bmod \Phi \in B$ according to inclusion (1).

The projective variety $p_0(\mathrm{Si}\,(q_H)) = \mathcal{Z}(\Delta_0)$, see Theorem 1, where $\Delta_0 \in A$ is an irreducible polynomial over the field $\overline{k_u}$ dividing the discriminant of the polynomial Φ with respect to X_{n+1}.

Set the ring $A^{(0)} = A/(\Delta_0)$. Denote by $K^{(0)}$ the field of fractions of $A^{(0)}$. Put $A^{(1)}$ to be the integral closure of the ring $A^{(0)}$ in $K^{(0)}$. Denote by $\Delta_1 \in k_u[X_0, \ldots, X_{n-1}]$ the discriminant of the polynomial Δ_0 with respect to X_n. Consider the element $\Delta_1 \bmod \Delta_0 \in k_u[X_0, \ldots, X_n]/(\Delta_0)$. Therefore we have $A^{(1)} \subset (1/\Delta_1 \bmod \Delta_0)A/(\Delta_0)$.

We shall suppose without loss of generality that $\mathrm{lc}_{X_{n+1}}\Phi = 1$. By Theorem 1, the polynomial $\Phi \bmod \Delta_0 = F_0(X_{n+1} - \eta)^2$ where $F_0 \in A^{(1)}[X_{n+1}]$ is a separable polynomial over $K^{(0)}$ with leading coefficients $\mathrm{lc}_{X_{n+1}}F_0 = 1$ and the element $\eta \in A^{(1)}$. Set $F_1 = X_{n+1} - \eta$. Put $m_0 = \deg_{X_{n+1}} F_0F_1 = a_0^n D - 1$. Now the homogeneous ring of the algebraic variety $\mathrm{Si}\,(q_H)$ over the field k_u is $A^{(0)}[\eta]$.

Let $b \in \overline{B}$. Then one can prove that $b = (\sum_{0 \leqslant i \leqslant m_0} b_i\omega^i)/\Delta_0$ where all $b_i \in A$. Denote by $\mathfrak{I}$ the ideal of A generated by the elements b_{m_0} for all $b \in \overline{B}$. Since $\omega^{m_0} \in \overline{B}$ the ideal $(\Delta_0) \subset \mathfrak{I}$. Let us define the homomorphisms of A-modules

$$e : \overline{B} \to \mathfrak{I}/(\Delta_0), \quad e(b) = b_{m_0} \bmod \Delta_0,$$
$$\epsilon : \overline{B} \to \mathfrak{I}, \quad \epsilon(b) = b_{m_0}.$$

Set $A' = \sum_{0 \leqslant i \leqslant m_0 - 1} A\omega^i \subset A[\omega]$. Hence A' is a free A-module with the basis $1, \omega, \ldots, \omega^{m_0 - 1}$.

Theorem 2. *The kernels* $\mathrm{Ker}\,(e) = A[\omega]$ *and* $\mathrm{Ker}\,(\epsilon) = A'$. *Hence we have the natural exact sequences of* A*-modules*

$$0 \longrightarrow A[\omega] \longrightarrow \overline{B} \xrightarrow{e} \mathfrak{I}/(\Delta_0) \longrightarrow 0,$$
$$0 \longrightarrow A' \longrightarrow \overline{B} \xrightarrow{\epsilon} \mathfrak{I} \longrightarrow 0.$$

Further, the equalities

$$\mathfrak{I} = \{z \in A : zF_1F_0 \in A^{(0)}[X_{n+1}]\},$$
$$\mathfrak{I} = \{z \in A : zA^{(0)}[\eta] \subset A^{(0)}\}$$

hold (notice that if q_1 *is not bijective then* $\eta \notin A^{(0)}$ *and* $\mathfrak{I} \neq A$*).*

For $z \in \mathfrak{I}$ one can find an element from $\epsilon^{-1}(z)$ as follows. Let $g \in A[X_{n+1}]$ be an arbitrary polynomial such that $zF_1F_0 = g \bmod \Delta_0 \in A^{(0)}[X_{n+1}]$. Then $g(\omega)/\Delta_0 \in \epsilon^{-1}(z)$.

If $\mathfrak{I} \neq A$ then every associated prime ideal $\mathfrak{p}$ of $\mathfrak{I}$ is an associated prime ideal of the ideal (Δ_0, Δ_1) and hence the height $\operatorname{ht}\mathfrak{p} = 2$.

Note that by the given generic point of V one can construct Δ_0, Δ_1, F_0, F_1 within the time polynomial in $D^{n^{O(1)}}$ and the size of the input, cf. [2]. Let us represent

$$\eta^i = \frac{\eta_i}{\Delta_1} \bmod \Delta_0, \quad 0 \leqslant i \leqslant m_0,$$

where $\eta_i \in A$. The inclusion $zA^{(0)}[\eta] \subset A^{(0)}$, $z \in A$ holds if and only if there are $x_i, y_i \in A$ such that

$$z\eta_i = x_i\Delta_1 + y_i\Delta_0 \tag{2}$$

for all $0 \leqslant i \leqslant m_0$. Let T_0, T_1 be new variables. Now (2) is equivalent to

$$z \sum_{0 \leqslant i \leqslant m_0} T_0^i T_1^{m_0-i}\eta_i = \Delta_1 \sum_{0 \leqslant i \leqslant m_0} T_0^i T_1^{m_0-i}x_i + \Delta_0 \sum_{0 \leqslant i \leqslant m_0} T_0^i T_1^{m_0-i}y_i.$$

Put $a = \Delta_1$, $b = \Delta_0$, $c = -\sum_{0 \leqslant i \leqslant m_0} T_0^i T_1^{m_0-i}\eta_i$ and consider the linear equation $aX + bY + cZ = 0$ over the polynomial ring $A[T_0, T_1] = A^{(2)}$. Let (x_j, y_j, z_j), $j \in J$, be a finite system of generators of the module of solutions of the equation $aX + bY + cZ = 0$ over $A^{(2)}$. Since the coefficients a, b, c are homogeneous with respect to T_0, T_1 we shall suppose without loss of generality that all x_j, y_j, z_j are also homogeneous with respect to T_0, T_1. Put $J_1 = \{j \in J : \deg_{T_0,T_1} z_j = 0\}$. Now obviously z_j, $j \in J_1$, is a system of generators of the A-module $\mathfrak{I}$. Thus, the normalization of V is reduced to solving the linear equation $aX + bY + cZ = 0$ over the polynomial ring $A^{(2)}$.

Notice that we get a system of generators of the $k_u[H_0, \ldots, H_n]$-module $\overline{B}$. But the algebraic varieties V and W are defined over the field k. Denote by B' the homogeneous ring of the algebraic variety W over the field k. So we have $B = k_u \otimes_k B'$. If the field k is infinite (or finite but has sufficiently many elements) then one can obtain the integral closure $\overline{B'}$ in the similar way replacing the field k_u by k and all generic polynomials H_i by homogeneous H_i' with coefficients from k in general position (they

can be constructed within the time polynomial in $D^{n^{O(1)}}$ and the size of the input using, e.g., the algorithms from [2] at least in the case of zero-characteristic).

One can also construct $\overline{B'}$ directly knowing $\overline{B}$.

We don't specify $O(1)$ in $D^{n^{O(1)}}$ since, see [3], the known upper bound for the complexity of solving the considered linear equation $aX+bY+cZ = 0$ is polynomial in $D^{2^{n^{O(1)}}}$ and the size of a, b, c.

Finally, we would like to note that there is also an analog of the described construction for affine algebraic varieties. It is less canonical but actually we consider it to reduce the projective case to affine one.

1. Lemmas of general position

Let $N \geqslant 0$ and $r \geqslant 0$ be integers. Let $\mathbb{A}^N(\overline{k})$ be the affine space with coordinate functions $X_1, \ldots, X_N$. We shall identify the set of all r-tuples $(L_1, \ldots, L_r)$ of linear forms $L_i \in \overline{k}[X_1, \ldots, X_N]$, $1 \leqslant i \leqslant r$ with the algebraic variety $\mathbb{A}^{Nr}(\overline{k})$. If $r \leqslant N$ then by $S^{(r)}$ denote the set of all r-tuples $(L_1, \ldots, L_r) \in \mathbb{A}^{Nr}(\overline{k})$ such that $L_1, \ldots, L_r$ are linearly independent over $\overline{k}$. Hence $S^{(r)}$ is a nonempty open in the Zariski topology subset of $\mathbb{A}^{Nr}(\overline{k})$.

In this and next section, $L = (L_1, \ldots, L_{n+1})$ is a $(n+1)$-tuple of linear forms. The following lemma is known.

Lemma 1. *Let $V \subset \mathbb{A}^N(\overline{k})$ be a closed affine algebraic variety irreducible over $\overline{k}$ of dimension $\dim V = n$. Denote by $\overline{V}$ the closure in the Zariski topology of V in the projective space $\mathbb{P}^N(\overline{k})$ where $\mathbb{A}^N(\overline{k}) = \mathbb{P}^N(\overline{k}) \setminus \mathcal{Z}(X_0)$ and $\mathbb{P}^N(\overline{k})$ has homogeneous coordinates $X_0, \ldots, X_N$. By $\mathcal{V}_1 \subset \mathbb{A}^{Nn}(\overline{k})$ denote the subset of all n-tuples $(L_1, \ldots, L_n)$ of linear forms such that*

$$\overline{V} \cap \mathcal{Z}(X_0, L_1, \ldots, L_n) = \emptyset \tag{3}$$

in $\mathbb{P}^N(\overline{k})$. Then $\mathcal{V}_1$ is a nonempty open in the Zariski topology subset of $\mathbb{A}^{Nn}(\overline{k})$. Further, there is a nonempty open in the Zariski topology subset $\mathcal{V}_2 \subset \mathbb{A}^{N(n+1)}(\overline{k})$ such that $L = (L_1, \ldots, L_{n+1}) \in \mathcal{V}_2$ if and only if the following properties are satisfied.

(1) *The corresponding n-tuple $(L_1, \ldots, L_n) \in \mathcal{V}_1$.*

(2) *The morphism*

$$p_L : V \longrightarrow \mathbb{A}^n(\overline{k}), \quad (X_1, \ldots, X_N) \mapsto (L_1, \ldots, L_n) \tag{4}$$

is finite dominant and separable.

(3) *Consider the morphism*

$$q_L : V \longrightarrow \mathbb{A}^{n+1}(\overline{k}), \quad (X_1, \ldots, X_N) \mapsto (L_1, \ldots, L_{n+1}). \qquad (5)$$

Then $q_L(V) = \mathcal{Z}(\Phi_L)$ *where* $\Phi_L \in \overline{k}[X_1, \ldots, X_{n+1}]$ *is an irreducible polynomial with leading coefficient* $\mathrm{lc}_{X_{n+1}} \Phi_L = 1$ *and* Φ_L *is separable with respect to* X_{n+1}, *i.e., the partial derivative* $\partial \Phi_L / \partial X_{n+1} \neq 0$.

(4) *By* q_2 *denote the morphism* $V \longrightarrow \mathcal{Z}(\Phi_L)$ *induced by* q_L. *Then* q_2 *is a finite birational isomorphism, i.e., there is a nonempty open in the Zariski topology subset* $U \subset V$ *such that* q_2 *induces the isomorphism of algebraic varieties* $U \to q_2(U)$.

Further, the degree $\deg_{X_{n+1}} \Phi_L = D = \deg \overline{V}$ *coincides with the degree of the projective algebraic variety* $\overline{V}$ *and hence does not depend on the choice of* $L \in \mathcal{V}_2$.

Remark 1. One can slightly generalize Lemma 1. One can consider an algebraic variety V such that all the irreducible components of V have the same dimension n, cf. the next lemma. Then by definition q_2 is a birational isomorphism if and only if it induces the isomorphism of total quotient rings of the rings of regular functions of corresponding algebraic varieties.

Lemma 2. *Let* $\gamma : W \to \mathbb{A}^n(\overline{k})$ *be a finite dominant morphism of defined over* $\overline{k}$ *algebraic varieties of dimension* $n \geqslant 0$. *Suppose that the irreducible components of the algebraic variety* W *have the same dimension. Let* $\overline{k}(W)$ *be the total quotient ring of the ring of regular functions of the algebraic variety* W *and by definition* $\deg \gamma = [\overline{k}(W) : \overline{k}(X_1, \ldots, X_n)]$ *is the dimension of* $\overline{k}(W)$ *over the field* $\overline{k}(X_1, \ldots, X_n)$. *Let* $z \in \mathbb{A}^1(\overline{k})$.

(1) *Suppose that for every point* $x \in \gamma^{-1}(z)$ *the differential* $d_x\gamma$ *is an isomorphism (and hence the point* x *is a smooth point of* W). *Then the morphism* γ *is separable (which means by definition that* $\overline{k}(W)$ *is a separable* $\overline{k}(X_1, \ldots, X_n)$ *algebra) and the number of elements*

$$\#\gamma^{-1}(z) = \deg \gamma = [\overline{k}(W) : \overline{k}(X_1, \ldots, X_n)]. \qquad (6)$$

(2) *Conversely, suppose that* (6) *holds and* γ *is a separable morphism. Then for every point* $x \in \gamma^{-1}(z)$ *the differential* $d_x\gamma$ *is an isomorphism. In particular,* x *is a smooth point of* W

Besides that, if γ is separable then the set of points $z \in \mathbb{A}^n(\overline{k})$ such that (2) *holds is open in the Zariski topology in $\mathbb{A}^n(\overline{k})$.*

Let $\psi_1, \ldots, \psi_m$ be a basis of the linear space of all the polynomials of degree at most a_0, see the Introduction, in $X_1, \ldots, X_N$ with coefficients from $\overline{k}$. Let

$$\psi = (\psi_1, \ldots, \psi_m) \, : \, \mathbb{A}^N(\overline{k}) \longrightarrow \mathbb{A}^m(\overline{k}) \tag{7}$$

be the morphism of algebraic varieties. Let $\mathbb{A}^m(\overline{k})$ has coordinate functions $X_1, \ldots, X_m$. Denote $V_0 = \psi(V)$. Hence V_0 is isomorphic to V.

Let $\mathbb{A}^N(\overline{k}) \times \mathbb{A}^N(\overline{k})$ has coordinate functions $X_1, \ldots, X_N$, $Y_1, \ldots, Y_N$. Let V be an affine algebraic variety from the formulation of Lemma 1. By

$$D(V \times V) = \Big\{ (z, z) \, : \, z \in V \Big\} \tag{8}$$

the diagonal subvariety of $V \times V$ is denoted. Hence $(V \times V) \setminus D(V \times V)$ is a quasiprojective algebraic variety. Consider the morphism

$$\begin{aligned} &p_\psi \, : \, (V \times V) \setminus D(V \times V) \to \mathbb{A}^m(\overline{k}), \\ &(X_1, \ldots, X_N, \, Y_1, \ldots, Y_N) \mapsto \\ &(\psi_1(X_1, \ldots, X_N) - \psi_1(Y_1, \ldots, Y_N), \ldots, \psi_m(X_1, \ldots, X_N) \\ &- \psi_m(Y_1, \ldots, Y_N)). \end{aligned}$$

Lemma 3. *Let V be a closed affine algebraic variety defined over $\overline{k}$ and irreducible over $\overline{k}$ in $\mathbb{A}^N(\overline{k})$ and the dimension $\dim V = n$. Then the following assertions hold.*

(a) *Let $x_1, x_2, x_3 \in \mathbb{A}^N(\overline{k})$ be arbitrary three distinct points Then $\psi(x_1)$, $\psi(x_2)$, $\psi(x_3)$ do not belong to the same line in $\mathbb{A}^m(\overline{k})$.*

(b) *There are pairwise distinct integers $1 \leqslant i_1, \ldots, i_{2n} \leqslant m$ such that the family*

$$\psi_i(X_1, \ldots, X_N) - \psi_i(Y_1, \ldots, Y_N), \quad i \in \{i_1, \ldots, i_{2n}\}$$

is a separable basis of transcendency of the field $\overline{k}(V \times V)$ over $\overline{k}$ or, which is the same, the extension of fields

$$\overline{k}(V_0 \times V_0) \supset \overline{k}(X_{i_1} - Y_{i_1}, \ldots, X_{i_{2n}} - Y_{i_{2n}}) \tag{9}$$

is finite and separable.

(c) *If characteristic* $\operatorname{char}(\overline{k}) \neq 2$ *then for every point* $z \in \mathbb{A}^m(\overline{k})$ *the number of elements of the inverse image* $\#p_\psi^{-1}(z) \leqslant 1$. *If characteristic* $\operatorname{char}(\overline{k}) = 2$ *then for every point* $z \in \mathbb{A}^m(\overline{k})$ *the number of elements* $\#p_\psi^{-1}(z) \leqslant 2$ *and if this inverse image is nonempty then* $p_\psi^{-1}(z) = \{(x,y),\,(y,x)\}$ *for some distinct* $x, y \in V$.

For an arbitrary set E by $\#E = \operatorname{Card}(E)$ we denote the cardinality of E.

Lemma 4. *Let* $V \subset \mathbb{A}^N(\overline{k})$ *be a closed affine algebraic variety irreducible over* $\overline{k}$ *of dimension* n. *Let* $n+1 \leqslant N$. *Suppose that any three distinct points from* V *do not belong to the same line in* $\mathbb{A}^N(\overline{k})$. *Let* $L = (L_1, \ldots, L_{n+1}) \in S^{(n+1)}$. *Let* q_L *be the morphism defined in Lemma* 1. *By* F'_L *denote the closure in the Zariski topology of the set*

$$\Big\{ z \in \mathbb{A}^{n+1}(\overline{k}) \,:\, \#q_L^{-1}(z) > 2 \Big\}.$$

There is a nonempty open in the Zariski topology subset $\mathcal{V}'_3 \subset S^{(n+1)}$ *such that* $L = (L_1, \ldots, L_{n+1}) \in \mathcal{V}'_3$ *if and only if the dimension* $\dim F'_L \leqslant n-2$.

Lemma 5. *Let* $V \subset \mathbb{A}^N(\overline{k})$ *be a closed affine algebraic variety irreducible over* $\overline{k}$ *of dimension* n. *Let* $n+1 \leqslant N$. *Let* $L = (L_1, \ldots, L_{n+1}) \in S^{(n+1)}$. *By* F''_L *denote the closure in the Zariski topology of the set of all smooth point* z *of* V *such that the differential* $d_z q_L$ *in the point* z *of the morphism* q_L *is not a monomorphism. Then there is a open in the Zariski topology subset* $\mathcal{V}''_3$ *of* $S^{(n+1)}$ *such that* $L \in \mathcal{V}''_3$ *if and only if the dimension* $\dim F''_L \leqslant n-2$.

Remark 2. We shall denote $\mathcal{V}_1 = \mathcal{V}_1(V)$, $\mathcal{V}_2 = \mathcal{V}_2(V)$, $\mathcal{V}'_3 = \mathcal{V}'_3(V)$ and $\mathcal{V}''_3 = \mathcal{V}''_3(V)$ when it will be necessary to indicate explicitly the algebraic variety V from the formulations of Lemma 1, Lemma 4, and Lemma 5.

Lemma 6. *Under conditions of Lemma* 5 *suppose that* $z \notin F''_L$ *is a smooth point of* V *such that the number of elements of the inverse image* $\#q_L^{-1}q_L(z) = 1$. *Suppose that* $L \in \mathcal{V}_2$, *see Lemma* 1 *(and hence* $q_L(V)$ *is closed in the Zariski topology in* $\mathbb{A}^{n+1}(\overline{k})$ *since the morphism* q_L *is finite). Then* $q_L(z)$ *is a smooth point of* $q_L(V)$ *and hence by Lemma* 5 *the tangent space in the point* $q_L(z)$ *of* $q_L(V)$

$$T_{q_L(z),\,q_L(V)} = d_z q_L(T_{z,V}).$$

Lemma 7. *Under conditions of Lemma 6 suppose that* $L \in \mathcal{V}_2 \cap \mathcal{V}_3''$. *Then* $F_L'' \subset q_L^{-1}(\mathrm{Si}\,(q_L))$. *Hence for every smooth point* $z \in V$ *the point* $q_L(z)$ *is a smooth point of* $\mathcal{Z}(\Phi_L)$ *if and only if* $z \notin \mathrm{Si}\,(q_L)$.

2. Irreducibility of self-intersection

Let V be an algebraic variety satisfying conditions of Lemma 3. Let us replace N by m and the algebraic variety V by the isomorphic variety $V_0 = \psi(V)$. So we replace also the notation: denote m by N and V_0 by V. Hence now V and N satisfy all the assertions of Lemma 3 in place of V_0 and m. Therefore V and N satisfy the conditions of Lemma 4 and Lemma 5.

Let $L_1, \dots, L_{2n} \in \overline{k}[X_1, \dots, X_N]$ be linear forms. Denote for brevity

$$M_i = L_i(X_1, \dots, X_N) - L_i(Y_1, \dots, Y_N), \tag{10}$$

for every $1 \leqslant i \leqslant 2n$.

Recall that $D(V \times V)$ is the the diagonal subvariety of $V \times V$ defined by (8). By

$$\begin{aligned} &p_M \,:\, (V \times V) \setminus D(V \times V) \to \mathbb{A}^{2n}(\overline{k}), \\ &(X_1, \dots, X_N, Y_1, \dots, Y_N) \mapsto (M_1, \dots, M_{2n}) \end{aligned} \tag{11}$$

and

$$\begin{aligned} &p_{X-Y} \,:\, (V \times V) \setminus D(V \times V) \to \mathbb{A}^{N}(\overline{k}), \\ &(X_1, \dots, X_N, Y_1, \dots, Y_N) \mapsto (X_1 - Y_1, \dots, X_N - Y_N) \end{aligned} \tag{12}$$

denote the morphisms of quasiprojective algebraic varieties. Set $V_1 = (V \times V) \setminus D(V \times V)$. By V_1' denote the subvariety of $\mathbb{A}^N(\overline{k})$ which is closure in the Zariski topology of $p_{X-Y}(V_1)$. Hence the open in the Zariski topology set of linear forms $\mathcal{V}_1(V_1')$ is defined, see Remark 2.

Recall that $\mathcal{V}_2$, $\mathcal{V}_3'$, and $\mathcal{V}_3''$ are open in the Zariski topology subset of $(n+1)$-tuples of linear forms from Lemma 1, Lemma 4, and Lemma 5, respectively. By $\mathcal{W}_3$ denote the subset of $2n$-tuples of linear forms $(L_1, \dots, L_{2n})$ such that for every permutation σ of the set $\{1, \dots, 2n\}$ the $(n+1)$-tuple $(L_{\sigma(1)}, \dots, L_{\sigma(n+1)}) \in \mathcal{V}_2 \cap \mathcal{V}_3' \cap \mathcal{V}_3''$. Hence $\mathcal{W}_3$ is a nonempty open in the Zariski topology subset of $\mathbb{A}^{2Nn}(\overline{k})$.

Let $L_1, \dots, L_{2n} \in \overline{k}[X_1, \dots, X_N]$ be linear forms. Then linear forms M_i, $1 \leqslant i \leqslant 2n$ are defined by (10). Denote by $L = (L_1, \dots, L_{n+1}) \in \mathbb{A}^{N(n+1)}$ the $(n+1)$-tuple of linear forms. Recall that the morphisms p_L,

q_L, p_M and p_{X-Y} are defined, see (4), (5), (11), and (12). Recall that the degree $D = \deg \overline{V}$ where $\overline{V}$ is closure in the Zariski topology of V in $\mathbb{P}^N(\overline{k})$, see Lemma 1.

Set $p'_{X-Y} = p_M$ for the special case when $M_i = X_i - Y_i$ for all $1 \leqslant i \leqslant 2n$.

Define also the morphism

$$p_0 : \mathbb{A}^{n+1}(\overline{k}) \to \mathbb{A}^n(\overline{k}), \quad (X_1, \ldots, X_{n+1}) \mapsto (X_1, \ldots, X_n). \tag{13}$$

Note that if one performs an appropriate linear transformation γ of $X_1, \ldots, X_N$ and replaces V by $\gamma(V)$ then the algebraic variety V satisfies all the conditions of the next lemma.

Lemma 8. *Let V be an irreducible over $\overline{k}$ affine algebraic variety which is a closed subvariety $\mathbb{A}^N(\overline{k})$. Let the dimension $\dim V = n \geqslant 3$ and $N \geqslant 2n$. Suppose that any three distinct points of V do not belong to the same line in $\mathbb{A}^N(\overline{k})$. Consider the affine algebraic variety $V \times V \subset \mathbb{A}^N(\overline{k}) \times \mathbb{A}^N(\overline{k})$ where $\mathbb{A}^N(\overline{k}) \times \mathbb{A}^N(\overline{k})$ has coordinates functions $X_1, \ldots, X_N, Y_1, \ldots, Y_N$. Suppose that linear forms $X_1 - Y_1, \ldots, X_{2n} - Y_{2n}$ are algebraically independent in the field of rational functions $\overline{k}(V \times V)$ and the extension of fields*

$$\overline{k}(V \times V) \supset \overline{k}(X_1 - Y_1, \ldots, X_{2n} - Y_{2n}) \tag{14}$$

is separable and finite. Suppose that for every $z \in \mathbb{A}^N(\overline{k})$ the number of elements of the inverse image $\#p^{-1}_{X-Y}(z) \leqslant a_0 - 1$. Suppose that the $2n$-tuple $(X_1, \ldots, X_{2n}) \in \mathcal{V}_1(V'_1)$, see Remark 2 and (12), and hence the morphism

$$V'_1 \to \mathbb{A}^{2n}(\overline{k}), \quad (X_1, \ldots, X_N) \mapsto (X_1, \ldots, X_{2n}) \tag{15}$$

is finite separable (consequently for every point $z \in \mathbb{A}^{2n}(\overline{k})$ the number of elements of the inverse image $\#p^{-1}_M(z) < +\infty$, i.e., the morphism p_M is quasifinite dominant separable). Suppose that the $2n$-tuple $(L_1, \ldots, L_{2n}) \in \mathcal{W}_3$. Set $L_i = X_i$, $M_i = X_i - Y_i$ for all $n + 2 \leqslant i \leqslant 2n$. Finally, assume that there is $(L_1, \ldots, L_{n+1}) \in \mathcal{V}_2(V)$ such that all linear forms $L_i \in \overline{k}[X_1, \ldots, X_{2n}]$ for all $1 \leqslant i \leqslant 2n$.

Then there is a nonempty open in the Zariski topology subset $\mathcal{W}_4 \subset \mathcal{V}_1(V'_1)$ such that $\mathcal{W}_4 \subset \mathcal{W}_3$ and for every $(L_1, \ldots, L_{2n}) \in \mathcal{W}_4$ the following properties hold.

(a) *The morphism p_L is finite dominant separable. The degree of p_L is D, i.e., the degree of the extension of fields of rational functions $[\overline{k}(V) : \overline{k}(L_1, \dots, L_n)] = D$.*

(b) *The morphism q_L induces the finite birational isomorphism $V \to q_L(V)$ where $q_L(V) \subset \mathbb{A}^{n+1}(\overline{k})$ is a closed affine algebraic variety. The closure in the Zariski topology F''_L of the subset of smooth points $z \in V$ such that the differential $d_z q_L$ (of the morphism q_L in the point z) is not a monomorphism has dimension $\dim F''_L \leqslant n-2$. For every smooth point $z \in V$ the point $q_L(z)$ is a smooth point of $q_L(V)$ if and only if $z \notin \mathrm{Si}\,(q_L)$.*

(c) *The algebraic variety $q_L^{-1}(\mathrm{Si}\,(q_L))$ is irreducible over $\overline{k}$ of dimension $n-1$. Hence the algebraic variety $\mathrm{Si}\,(q_L)$ is irreducible over $\overline{k}$ of dimension $n-1$. In particular $\mathrm{Si}\,(q_L) \neq \emptyset$.*

(d) *There is a nonempty open in the Zariski topology subset $\mathcal{V}_5$ of $\mathrm{Si}\,(q_L)$ such that for every $z \in \mathcal{V}_5$ the inverse image $q_L^{-1}(z) = \{z_1, z_2\}$ consists of two distinct points such that z_1 and z_2 are smooth points of V, the differentials $d_{z_1} q_L$ and $d_{z_2} q_L$ are monomorphisms, and the intersection $d_{z_1} q_L(T_{z_1,V}) \cap d_{z_2} q_L(T_{z_2,V})$ of the images of the tangent spaces $T_{z_1,V}$ and $T_{z_2,V}$ (of V in the points z_1 and z_2) is transversal, i.e., the dimension*

$$\dim d_{z_1} q_L(T_{z_1,V}) \cap d_{z_2} q_L(T_{z_2,V}) = n-1. \tag{16}$$

We shall denote also $\mathcal{V}_5 = \mathcal{V}_5(L)$ when the dependence on L will be essential.

(e) *Further for every $z \in p_0(\mathcal{V}_5)$ the inverse image $p_L^{-1}(z)$ consists of D distinct smooth points of V and for every $y \in p_L^{-1}(z)$ the differential $d_y p_L$ of the morphism p_L in the point y is an isomorphism. Besides that, $\mathcal{V}_5 = p_0^{-1} p_0(\mathcal{V}_5) \cap \mathrm{Si}\,(q_L)$ and $p_0(\mathcal{V}_5)$ is an open in the Zariski topology subset of the closed irreducible over $\overline{k}$ affine algebraic variety $p_0(\mathrm{Si}\,(q_L))$.*

(f) *The morphism of irreducible over $\overline{k}$ algebraic varieties $q_L^{-1}(\mathrm{Si}\,(q_L)) \to \mathrm{Si}\,(q_L)$ induced by q_L is finite dominant and separable of degree 2. The morphism of irreducible over $\overline{k}$ affine algebraic varieties $q_4 : \mathrm{Si}\,(q_L) \to p_0(\mathrm{Si}\,(q_L))$ induced by p_0 is finite separable. For every $y \in \mathcal{V}_5$ the point $q_4(y)$ is a smooth point of $p_0(\mathrm{Si}\,(q_L))$ and the differential $d_y q_4$ is an isomorphism.*

(g) *Let $D(V\times V)$ be the diagonal subvariety of $V\times V$, see above, and the linear form M_i, $1\leqslant i\leqslant n+1$ be defined by* (10). *Then for every $1\leqslant j\leqslant n+1$ the algebraic variety*

$$\big((V\times V)\setminus D(V\times V)\big)\cap\mathcal{Z}(M_1,\ldots,M_j) \tag{17}$$

is irreducible over $\overline{k}$ and there is a nonempty open in the Zariski topology subset $\mathcal{U}_j$ of the algebraic variety (17) *such that for every $z\in\mathcal{U}_j$ the point z is a smooth point of $\mathcal{U}_j$, the point z is a smooth point of $V\times V\setminus D(V\times V)$ and the intersection of tangent spaces*

$$T_{z,V\times V\setminus D(V\times V)}\cap\mathcal{Z}(M_1,\ldots,M_j) \tag{18}$$

in the point z of the algebraic varieties $(V\times V)\setminus D(V\times V)$ and $\mathcal{Z}(M_1,\ldots,M_j)$ is transversal, i.e.,

$$\dim T_{z,V\times V\setminus D(V\times V)}\cap\mathcal{Z}(M_1,\ldots,M_j)=2n-j.$$

(h) *The equality $q_L(V)=\mathcal{Z}(\Phi_L)$ holds where $\Phi_L\in\overline{k}[X_1,\ldots,X_{n+1}]$ is an irreducible over $\overline{k}$ polynomial such that*

$$\deg_{X_i}\Phi_L=\deg_{X_1,\ldots,X_{n+1}}\Phi_L=D$$

for all $1\leqslant i\leqslant n+1$, in particular, leading coefficients $\operatorname{lc}_{X_i}\Phi_L\in\overline{k}$ for all $1\leqslant i\leqslant n+1$. Besides that, for every $1\leqslant i\leqslant n+1$ the polynomial Φ_L is separable with respect to X_i, i.e., $\partial\Phi_L/\partial X_i\neq 0$.

(i) *The morphism p_M is quasifinite separable dominant. Let $\mathcal{Z}(L_1,\ldots,L_j)\subset\mathbb{P}^{2n}(\overline{k})$ be the linear subspace of the projective space. Then the morphism p_M induces for every $1\leqslant j\leqslant n+1$ the morphism*

$$V_1\cap\mathcal{Z}(M_1,\ldots,M_j))\to\mathcal{Z}(L_1,\ldots,L_j)$$

such that the extension of fields

$$\overline{k}(V_1\cap\mathcal{Z}(M_1,\ldots,M_j))\supset\overline{k}(\mathcal{Z}(L_1,\ldots,L_j)),\quad 1\leqslant j\leqslant n+1. \tag{19}$$

is finite separable.

Proof. Denote by $\pi_1 : V\times V\to V$ the projection to the first direct factor. Notice that $q_L^{-1}(\operatorname{Si}(q_L))$ is equal to the closure with respect to the Zariski topology of

$\pi_1(V_1\cap\mathcal{Z}(M_1,\ldots,M_{n+1}))$. Let us represent $V_1=\bigcup_{\iota\in I}U_\iota$ where U_ι is a nonempty open in the Zariski topology affine subset of V_1 for every $\iota\in I$ and the number of elements $\#I<+\infty$. Now actually everything follows straightforwardly from Theorem 3, see the Appendix, applied j (recall that $1\leqslant j\leqslant n+1$) times to the restrictions $p'_{X-Y}|_{U_\iota}$ of the morphism p'_{X-Y} to U_ι, cf. also the Introduction from [4], and further from Lemmas 1, 2, 3, 4, 5, and 6. The lemma is proved.

3. The case of a projective nonsingular in codimension one algebraic variety

Now we can give a sketch of the proof of Theorem 1. We have $\deg \mathrm{ver}_{a_0}(V) = a_0^n D$ and the projective algebraic varieties V and $\mathrm{ver}_{a_0}(V)$ are isomorphic. Let us replace V by $\mathrm{ver}_{a_0}(V)$. Then $H_0, \ldots, H_{n+1}$ are replaced by generic linear forms in $X_0, \ldots, X_{N_1}$ (we denote them again by $H_0, \ldots, H_{n+1}$; the morphism q_H and p_H are defined as previously). By Lemma 3 any three distinct points of $\mathrm{ver}_{a_0}(V)$ do not belong to any line in $\mathbb{P}^{N_1}(\overline{k_u})$. Now all the required assertions are direct consequences of Lemma 8. They are obtained by considering the restrictions of the morphisms p_H and q_H to the affine algebraic varieties $V \setminus \mathcal{Z}(H_i)$, $0 \leqslant i \leqslant n$, with the coordinate functions X_j/H_i, $1 \leqslant j \leqslant N$. After that one can glue everything without difficulties. The theorem is proved.

4. A modification of the Serre criterion for normal algebraic varieties

Let $V \subset \mathbb{A}^N(\overline{k})$ be a closed affine irreducible over $\overline{k}$ normal algebraic variety of dimension n. Denote for brevity the ring of regular functions $\overline{k}[V] = B$. Let $\mathfrak{P}$ be a prime ideal of B. By $B_{\mathfrak{P}} = (B \setminus \mathfrak{P})^{-1}B$ denote the localization of B with respect to the prime ideal $\mathfrak{P}$. The following characterization, the Serre criterion, of normal affine algebraic varieties is known. The affine algebraic variety V is normal if and only if the following two conditions are satisfied

- for every prime ideal $\mathfrak{P}$ of the ring B with height $\mathrm{ht}\,(\mathfrak{P}) = 1$ the localization $B_{\mathfrak{P}}$ is integrally closed,
- for every prime ideal $\mathfrak{P}$ of the ring B with height $\mathrm{ht}\,(\mathfrak{P}) \geqslant 2$ there are two distinct elements $u, v \in (B \setminus \mathfrak{P})^{-1}\mathfrak{P}$ such that u, v is regular sequence (of length two) of the local ring $B_{\mathfrak{P}}$.

The last condition means that v is not a zero-divisor in $B_{\mathfrak{P}}/uB_{\mathfrak{P}}$. The first one means that V is nonsingular in codimension one.

Denote $A = \overline{k}[X_1, \ldots, X_n]$. Suppose that the extension of rings $B \supset A$ is integral. Let $\mathfrak{p}$ be a prime ideal of A. By $B_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1}B$ denote the localization of B with respect to the multiplicatively closed set $A \setminus \mathfrak{p}$. We shall need also the following characterization of normal algebraic varieties.

Lemma 9. *The affine irreducible algebraic variety V is normal if and only if the following two conditions hold*

(i) *for every prime ideal* $\mathfrak{p}$ *of the ring* A *with height* $\operatorname{ht}(\mathfrak{p}) = 1$ *the localization* $B_{\mathfrak{p}}$ *is integrally closed,*

(ii) *for every prime ideal* $\mathfrak{p}$ *of the ring* A *with height* $\operatorname{ht}(\mathfrak{p}) \geqslant 2$ *there are two distinct elements* $u, v \in (A \setminus \mathfrak{p})^{-1}\mathfrak{p}$ *such that* u, v *is a regular sequence of length two of the semilocal ring* $B_{\mathfrak{p}}$.

Proof. Suppose that V is a normal algebraic variety. Then B is integrally closed. Hence (i) holds. Let $\mathfrak{p}$ be a prime ideal of the ring A with height $\operatorname{ht}(\mathfrak{p}) \geqslant 2$. Therefore there is $0 \neq u \in \mathfrak{p}$. Let $\operatorname{Ass}(B/uB)$ be the set of all associated prime ideals of the ring B of the ideal uB. Then for every $\mathfrak{p}_1 \in \operatorname{Ass}(B/uB)$ the height $\operatorname{ht}(\mathfrak{p}_1) = 1$ since B is integrally closed, see [??]. Hence $\operatorname{ht}(\mathfrak{p}_1 \cap A) = 1$ where $\mathfrak{p}_1 \cap A$ is a prime ideal of A. Therefore there is

$$v \in \mathfrak{p} \setminus \bigcup_{\mathfrak{p}_1 \in \operatorname{Ass}(B/uB)} (\mathfrak{p}_1 \cap A).$$

Consequently u, v is the required regular sequence of the ring $B_{\mathfrak{p}}$ which proves (ii).

Conversely, let (i) and (ii) hold. Let $\mathfrak{P}$ be a prime ideal of the ring B with $\operatorname{ht}(\mathfrak{P}) = 1$. Set $\mathfrak{p} = \mathfrak{P} \cap A$. Then $\operatorname{ht}(\mathfrak{p}) = 1$ in A. Hence by (i) the ring $B_{\mathfrak{p}}$ is integrally closed. Therefore $B_{\mathfrak{P}} = (B \setminus \mathfrak{P})^{-1}B_{\mathfrak{p}}$ is also integrally closed.

Let $\mathfrak{P}$ be a prime ideal of the ring B with $\operatorname{ht}(\mathfrak{P}) \geqslant 2$. Set $\mathfrak{p} = \mathfrak{P} \cap A$. Then $\operatorname{ht}(\mathfrak{p}) \geqslant 2$ in A. By (ii), there are two distinct elements $u, v \in (A \setminus \mathfrak{p})^{-1}\mathfrak{p}$ such that u, v is regular sequence of length two of the semilocal ring $B_{\mathfrak{p}}$. But $B_{\mathfrak{P}} = (B \setminus \mathfrak{P})^{-1}B_{\mathfrak{p}}$. The multiplication to $v : B_{\mathfrak{p}}/uB_{\mathfrak{p}} \to B_{\mathfrak{p}}/uB_{\mathfrak{p}}$ is a monomorphism. Hence the multiplication to $v : B_{\mathfrak{P}}/uB_{\mathfrak{P}} \to B_{\mathfrak{P}}/uB_{\mathfrak{P}}$ is also a monomorphism. Consequently u, v is regular sequence in $B_{\mathfrak{P}}$. Thus, by the Serre criterion, the algebraic variety V is normal. The lemma is proved.

5. A new representation of a normal algebraic variety

Now we shall formulate two lemmas for the proof of Theorem 2. We use the notation from the Introduction.

Let $h \in A$ be a homogeneous irreducible polynomial. Set the ideal $\mathfrak{p} = (h) \subset A$. Denote by $S_{\mathfrak{p}} = A \setminus \mathfrak{p}$ the multiplicatively closed set. For an arbitrary A-module M denote by $M_{\mathfrak{p}} = S_{\mathfrak{p}}^{-1}M$ the localization of M with respect to the multiplicatively closed set $S_{\mathfrak{p}}$.

Lemma 10. *For every prime ideal of height one* $\mathfrak{p} = (h) \subset A$ *such that* $\mathfrak{p} \neq (\Delta_0)$ *the inclusion* (1) *induces the identification ring*

$$B_{\mathfrak{p}} = A_{\mathfrak{p}}[X_{n+1}]/(\Phi).$$

Proof. Recall that $\Delta \in \overline{k_u}[X_0, \ldots, X_n]$ is the discriminant of the polynomial Φ with respect to X_{n+1}. Suppose that the irreducible polynomial h does not divide Δ. Then

$$B_{\mathfrak{p}} \supset \frac{1}{\Delta} A_{\mathfrak{p}}[\omega] = A_{\mathfrak{p}}[\omega].$$

Hence the ring $B_{\mathfrak{p}} = A_{\mathfrak{p}}[\omega]$ is integrally closed.

Suppose that h divides Δ and $h \neq c\Delta_0$ for every $c \in \overline{k_u}$. It is sufficient to show that the ring $A_{\mathfrak{p}}[\omega]$ is integrally closed. Let $\mathfrak{P}_\gamma$, $\gamma \in \Gamma$, be the family of all prime ideals $\mathfrak{P}$ of the ring $A[\omega]$ such that $\mathfrak{P} \cap A = \mathfrak{p}$. Let $S_{\mathfrak{P}_\gamma} = A[\omega] \setminus \mathfrak{P}_\gamma$ be the multiplicatively closed set. For a $A[\omega]$-module M denote by $M_{\mathfrak{P}_\gamma}$ the localization of $S^{-1}_{\mathfrak{P}_\gamma} M$. Then the ring $A[\omega]_{\mathfrak{P}_\gamma}$ is integrally closed since the algebraic variety $\mathcal{Z}(\Phi_H) \setminus \mathcal{Z}(\Delta_0)$ is nonsingular in codimension one. Now it is sufficient to show that $A[\omega]_{\mathfrak{p}} \supset \bigcap_{\gamma \in \Gamma} A[\omega]_{\mathfrak{P}_\gamma}$. Let $z \in \bigcap_{\gamma \in \Gamma} A[\omega]_{\mathfrak{P}_\gamma}$. Then one can represent $z = z_\gamma / s_\gamma$, where $z \in A[\omega]$, $s_\gamma \in S_\gamma$ for every $\gamma \in \Gamma$. Let K_1 be the field of fractions B. Hence one can represent $z = z'/s$, where $z' \in A[\omega]$,

$$s \in A[\omega] \setminus \bigcup_{\gamma \in \Gamma} \mathfrak{P}_\gamma. \tag{20}$$

and s is primitive element of the extension $K_1 \supset \overline{k_u}(X_0, \ldots, X_n)$ Let $\mathcal{N}$ be the mapping of the norm from the field of fractions K_1 to $\overline{k_u}(X_0, \ldots, X_n)$. Then

$$s = \mathcal{N}(s)/s' = \left(\prod_\sigma s^\sigma \right) \Big/ s',$$

where σ runs over all the pairwise distinct embeddings of K_1 to the algebraic closure of $\overline{k_u}(X_0, \ldots, X_n)$ over $\overline{k_u}(X_0, \ldots, X_n)$.

Suppose that $\mathcal{N}(s) \in \mathfrak{p}$. Let $v : \overline{k_u}(X_0, \ldots, X_n) \to \mathbb{Q} \cup \{+\infty\}$ be the discrete valuation of the field $\overline{k_u}(X_0, \ldots, X_n)$ with the center $\mathfrak{p}$ on A. Since $\mathcal{N}(s) \in \mathfrak{p}$ there is an extension w of v to the least normal over $\overline{k_u}(X_0, \ldots, X_n)$ extension K_2 of K_1 such that $w(\mathcal{N}(s)) > 0$. Obviously

$w(s^\sigma) \geqslant 0$ for every σ. Hence there is σ such that $w(s^\sigma) > 0$. Hence s^σ belongs to a prime ideal $\mathfrak{P}$ of $A[\omega]^\sigma$ such that $\mathfrak{P} \cap A = \mathfrak{p}$. But then $\mathfrak{P} = \mathfrak{P}_\gamma^\sigma$ for some $\gamma \in \Gamma$. On the other hand, by (20) we have $s^\sigma \notin \bigcup_{\gamma\in\Gamma} \mathfrak{P}_\gamma^\sigma$. We get a contradiction. Therefore, $\mathcal{N}(s) \in S_\mathfrak{p}$.

Let us show that $s' \in A[\omega]$. Indeed, let $Z^\nu + \sum_{0\leqslant i\leqslant \nu-1} b_i Z^i$, be the minimal polynomial of s over the field $\overline{k_u}(X_0, \dots, X_n)$. Then all $b_i \in A$ and $b_0 = (-1)^\nu \mathcal{N}(s)$ since s is a primitive element of the extension $K_1 \supset \overline{k_u}(X_0, \dots, X_n)$. Thus, $s' = (-1)^{\nu+1}(s^{\nu-1} + \sum_{1\leqslant i\leqslant \nu-1} b_i s^{i-1}) \in A[\omega]$.

Now $z = z's'/\mathcal{N}(s) \in A_\mathfrak{p}[\omega]$. The lemma is proved.

Lemma 11. *Let $\mathfrak{p} = (\Delta_0)$. The polynomial*

$$F_0 F_1 \in (\overline{k_u}[X_0, \dots, X_n]/\Delta_0)_\mathfrak{p}[X_{n+1}].$$

Let $G \in A_\mathfrak{p}[X_{n+1}]$ be an arbitrary polynomial such that $G \bmod \Delta_0 = F_0F_1$, the degree $\deg_{X_{n+1}} G = m_0$ and the leading coefficient $\mathrm{lc}_{X_{n+1}} G = 1$. (one can choose $G \in (1/\Delta_1)A[X_{n+1}]$ but we don't fix it now). Set $\theta = G(X_0, \dots, X_n, \omega)/\Delta_0$. Then $\theta \in B_\mathfrak{p}$, and $B_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module with the basis

$$1, \omega, \dots, \omega^{m_0-1}, \theta. \tag{21}$$

Corollary 1. *Denote by $\overline{B}$ the integral closure of B in its field of fractions. The ring*

$$\overline{B} \subset \frac{1}{\Delta_0} A[\omega].$$

Proof. By Lemmas 10 and 11,

$$\overline{B} \subset \left(\frac{1}{\Delta_0} \sum_{0\leqslant i\leqslant a_0^n D-1} A_{(\Delta_0)}\omega^i \right) \cap \bigcap_{\substack{\mathfrak{p}\neq(\Delta_0),\\ \mathrm{ht}\,\mathfrak{p}=1}} \left(\sum_{0\leqslant i\leqslant a_0^n D-1} A_\mathfrak{p}\omega^i \right)$$

$$= \sum_{0\leqslant i\leqslant a_0^n D-1} \left(\frac{1}{\Delta_0} A_{(\Delta_0)} \cap \bigcap_{\substack{\mathfrak{p}\neq(\Delta_0),\\ \mathrm{ht}\,\mathfrak{p}=1}} A_\mathfrak{p} \right) \omega^i = \sum_{0\leqslant i\leqslant a_0^n D-1} \left(\frac{1}{\Delta_0} A \right) \omega^i;$$

here with all the terms of the considered intersections are subsets of the field of fractions of $A[\omega]$. The corollary is proved.

Corollary 2. *Let $z \in A$ and θ be an arbitrary element from the statement of Lemma 11. Then $z\theta \in (1/\Delta_0)A[\omega]$ if and only if $z\theta \in \overline{B}$.*

Using these lemmas and corollaries one can prove without difficulties all the assertions of Theorem 2.

Appendix: An irreducibility theorem

We use in this paper an irreducibility theorem from the Appendix of [4]. So in this section we formulate it for completeness of presentation. Actually it is a version of the first Bertini theorem, see for details [4].

Let B be an arbitrary commutative Noetherian integral ring. We shall denote by B' the integral closure of B in the field of fractions of B. For a finitely generated B-module M denote by $\mathrm{Ass}\,(M)$ the set of all associated prime ideals of M (they are prime ideals of B). Recall that an ideal of B is called radical if it coincides with its nil-radical. In what follows the morphisms of algebraic varieties are regular morphisms if it is not stated otherwise.

Let $n \geqslant 2$ be an integer. Let $\mathbb{A}^n(\overline{k})$ be affine space over the field $\overline{k}$ with the coordinate functions $X_1, \ldots, X_n$. Let $x \in \mathbb{A}^n(\overline{k})$ be the point with the coordinates $X_i(x) = 0$, $1 \leqslant i \leqslant n$.

Let V be an affine algebraic variety defined over $\overline{k}$ and irreducible over $\overline{k}$. Let $p : V \to \mathbb{A}^n(\overline{k})$ be a dominant separable morphism. We shall identify the ring $\overline{k}[X_1, \ldots, X_n] \subset \overline{k}[V]$. For an element $g \in \overline{k}[X_1, \ldots, X_n]$ we shall denote by $\mathcal{Z}(g)$ the subset of all zeroes of the polynomial g in $\mathbb{A}^n(\overline{k})$. By $V \cap \mathcal{Z}(g)$ we shall denote for convenience of notation the subset $p^{-1}(\mathcal{Z}(g)) \subset V$.

We shall suppose additionally that

$$\dim p^{-1}(x) \leqslant n - 2. \tag{22}$$

By $B = \overline{k}[V]$ denote the ring of regular functions of the algebraic variety V. Let $z \in V$ be a point. By $\mathfrak{M}_z$ denote the maximal ideal of B corresponding to the point z.

Let $y \in B$ be a primitive element of the separable algebraic extension $\overline{k}(V) \supset \overline{k}(X_1, \ldots, X_n)$, i.e.,

$$\overline{k}(V) = \overline{k}(X_1, \ldots, X_n)[y]. \tag{23}$$

Let $f \in \overline{k}[X_1, \ldots, X_n, Y]$ be minimal polynomial of y over $\overline{k}(X_1, \ldots, X_n)$ (here Y is a new variable) and f be irreducible in the ring $\overline{k}[X_1, ..., X_n, Y]$. So the degree $D = \deg_Y f \geqslant 1$. Let $\deg_{X_1,\ldots,X_n,Y} f = m_1$ and $f^{(m_1)}$ be the homogeneous in $X_1, \ldots, X_n, Y$ form of degree m_1 of the polynomial f.

The element y is integral over $\overline{k}[X_1, \ldots, X_n]$ if the morphism p is finite. Denote by $\mathrm{lc}_Y f$ the leading coefficient of the polynomial f with respect to Y. We choose f such that $\mathrm{lc}_Y f = 1$ if p is finite.

Besides that we shall suppose that if $n = 2$ then p is finite.

Denote by

$$\Delta = \mathrm{Res}_Y(f, \partial f/\partial Y) \in \overline{k}[X_1, \ldots, X_n] \tag{24}$$

the discriminant of the polynomial f with respect to Y. So $\Delta \neq 0$ since f is separable.

Remark 3. Recall that by definition the discriminant Δ is the determinant of the $(2D-1) \times (2D-1)$ Sylvester matrix of the resultant. Although in the case of nonzero characteristic of the ground field the degree $\deg_Y \partial f/\partial Y$ may be less than $D-1$ the partial derivative $\partial f/\partial Y$ is considered formally as a polynomial of degree $D-1$ in this matrix. Some higher coefficients of $\partial f/\partial Y$ may be equals to zero in this representation.

Let us identify the set of all linear forms from $\overline{k}[X_1, \ldots, X_n]$ with $\mathbb{A}^n(\overline{k})$. Let $\mathfrak{P}$ be a prime ideal of $\overline{k}[X_1, \ldots, X_n]$ (respectively, B, B'). Suppose that

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

where $\mathcal{Z}(X_1, \ldots, X_n)$ and $\mathcal{Z}(\mathfrak{P})$ are considered as subvarieties of $\mathbb{A}^n(\overline{k})$ (respectively, V, the normalization of V). Then the set $S_{\mathfrak{P}}$ of linear forms $L \in \overline{k}[X_1, \ldots, X_n]$ such that $L \notin \mathfrak{P}$ is open in the Zariski topology in $\mathbb{A}^n(\overline{k})$ since

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

Consider B'/B as a B-module. Set

$$\mathcal{B}_1 = \mathrm{Ass}\,(B'/B), \quad \mathcal{B}_2 = \{\mathfrak{P} \in \mathcal{B}_1 \,:\, \mathcal{Z}(\mathfrak{P}) \subset p^{-1}(x)\},$$
$$\mathcal{B}_3 = \{\mathfrak{P} \in \mathcal{B}_1 \,:\, \dim \mathcal{Z}(\mathfrak{P}) = n-1\}.$$

Consider the set $\mathcal{U}_1$ (respectively, $\mathcal{U}_2$) of linear forms L in $X_1, \ldots, X_n$ such that $L \notin \mathfrak{P}$ for every $\mathfrak{P} \in \mathcal{B}_1 \setminus \mathcal{B}_2$ (respectively, $\mathcal{B}_3$). Then $\mathcal{U}_1$ (respectively, $\mathcal{U}_2$) is a nonempty open in the Zariski topology subset of $\mathbb{A}^n(\overline{k})$ and $\mathcal{U}_1 \subset \mathcal{U}_2$. Note that $\mathcal{U}_1 = \mathcal{U}_2 = \mathbb{A}^n(\overline{k})$ if $\mathcal{B}_1 = \mathcal{B}_2$, in particular if $B = B'$ (i.e., if V is normal) since in the latter case $\mathrm{Ass}\,(B'/B) = \emptyset$. Note also that if the set of singular points of V has dimension at most $n-2$ then $\mathcal{B}_3 = \emptyset$ and $\mathcal{U}_2 = \mathbb{A}^n(\overline{k})$.

Let $L \in \overline{k}[X_1, \ldots, X_n]$ be a nonzero linear form. Consider B/LB as a B-module. Set

$$\mathcal{B}_{1,L} = \mathcal{B}_2 \cap \mathrm{Ass}\,(B/LB), \quad \mathcal{B}_{2,L} = (\mathcal{B}_1 \setminus \mathcal{B}_3) \cap \mathrm{Ass}\,(B/LB).$$

Let us show that there is a nonzero element $\Delta_1 \in \overline{k}[X_1, \dots, X_n]$ such that the extensions of rings

$$B[\Delta_1^{-1}] \supset \overline{k}[X_1, \dots, X_n, \Delta_1^{-1}][y] \supset \overline{k}[X_1, \dots, X_n][\Delta_1^{-1}] \qquad (25)$$

are integral. Indeed, by (23), one can choose Δ_1 to be the product of $\mathrm{lc}_Y f$ and all the leading coefficients of minimal polynomials over $\overline{k}[X_1, \dots, X_n]$ of the elements a finite system of generators of the ring B over $\overline{k}[X_1, \dots, X_n]$. In the case, where p is finite we choose $\Delta_1 = 1$. Fix such an element Δ_1.

Set $\mathcal{B}_4 = \mathrm{Ass}\,(B'/\Delta_1 B')$ where $B'/\Delta_1 B'$ is considered as a B'-module. Hence the elements of $\mathcal{B}_4$ are prime ideals of B'. By $\mathcal{U}_3$ denote the set of all linear forms $L \in \overline{k}[X_1, \dots, X_n]$ such that $L \notin \mathfrak{P}$ for every $\mathfrak{P} \in \mathcal{B}_4$. Since B' is integrally closed the dimension $\dim \mathcal{Z}(\mathfrak{P}) = n - 1$ for every $\mathfrak{P} \in \mathcal{B}_4$. Therefore $\mathcal{U}_3$ is a nonempty open in the Zariski topology subset of $\mathbb{A}^n(\overline{k})$. Note that if p is finite then $\mathcal{U}_3 = \mathbb{A}^n(\overline{k})$. Note also that if $L \in \mathcal{U}_3$ then L does not divide Δ_1 in the ring $\overline{k}[X_1, \dots, X_n]$.

Theorem 3. *Let $n \geqslant 2$. Let V, B, $p : V \to \mathbb{A}^n(\overline{k})$, y, f, Δ, Δ_1, m_1, $f^{(m_1)}$, $\mathcal{U}_1$, $\mathcal{U}_2$, $\mathcal{U}_3$, $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$ and $\mathcal{B}_4$ be as above.*

(i) *Then there is a nonzero linear form $L \in \overline{k}[X_1, \dots, X_n]$ in $X_1, \dots, X_n$ such that the ideal $(f, L) \subset \overline{k}[X_1, \dots, X_n, Y]$ is radical and if $n \geqslant 3$ it is prime. The element $\Delta \bmod L \in \overline{k}[X_1, \dots, X_n]/(L)$ is nonzero (i.e., L does not divide Δ) and*

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

is also nonzero.

(ii) *The set of linear forms L satisfying the properties from* (i) *contains a nonempty open in the Zariski topology subset $\mathcal{U}_4$ of $\mathbb{A}^n(\overline{k})$.*

(iii) *Let $L \in \mathcal{U}_1 \cap \mathcal{U}_3 \cap \mathcal{U}_4$ (respectively, $L \in \mathcal{U}_2 \cap \mathcal{U}_3 \cap \mathcal{U}_4$). Then the ideal*

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

where the ideal $\mathfrak{p}$ is the radical of the ideal LB and if $n \geqslant 3$ it is prime. The ideal $\mathfrak{q}$ is an intersection of $\mathfrak{P}$-primary ideals for all prime ideals $\mathfrak{P} \in \mathcal{B}_{1,L}$ (respectively, $\mathfrak{P} \in \mathcal{B}_{2,L}$), herewith we suppose that the intersection over the empty set (when $\mathcal{B}_{1,L} = \emptyset$ or $\mathcal{B}_{2,L} = \emptyset$) is B. Hence if p is finite then $\mathfrak{q}$ is an intersection of $\mathfrak{M}_z$-primary

ideals for some $z \in p^{-1}(x)$ *or* $\mathfrak{q} = B$. *Besides that, for every* $\mathfrak{P} \in \mathcal{B}_{1,L}$ *(respectively,* $\mathfrak{P} \in \mathcal{B}_{2,L}$*) the dimension* $\dim \mathcal{Z}(\mathfrak{P}) \leqslant n-2$ *and therefore, the* $\mathfrak{P}$*-primary component of the ideal* LB *is embedded.*

(iv) *Let* $L \in \mathcal{U}_2 \cap \mathcal{U}_3 \cap \mathcal{U}_4$. *Then the algebraic variety* $V \cap \mathcal{Z}(L)$ *has dimension* $\dim V - 1$ *and if* $n \geqslant 3$ *then* $V \cap \mathcal{Z}(L)$ *is irreducible over* $\overline{k}$. *Further, the projection induced by* p

$$V \cap \mathcal{Z}(L) \to \mathcal{Z}(L) \tag{26}$$

is a dominant and separable morphism of affine algebraic varieties (here $\mathcal{Z}(L) \subset \mathbb{A}^n(\overline{k})$*). Besides that if* p *is a finite morphism then morphism* (26) *is also finite.*

Denote by $\overline{k}(V \cap \mathcal{Z}(L))$ *the total quotient ring of the ring of regular functions of the algebraic variety* $V \cap \mathcal{Z}(L)$, *hence it is the field of rational functions of this algebraic variety if* $n \geqslant 3$. *Then*

$$\big[\,\overline{k}(V \cap \mathcal{Z}(L)) : \overline{k}(\mathcal{Z}(L))\,\big] = \big[\,\overline{k}(V) : \overline{k}(X_1, \ldots, X_n)\big], \tag{27}$$

herewith the left part of this equality is the dimension of the total quotient ring over the field $\overline{k}(\mathcal{Z}(L))$ *and the right part is the degree of extension of fields of rational functions* $\overline{k}(V) \supset \overline{k}(\mathbb{A}^n(\overline{k}))$. *Denote by* $y \bmod L$ *the image of the element* y *in* $\overline{k}[V \cap \mathcal{Z}(L)]$.

Then minimal polynomial of the element $y \bmod L$ *over* $\overline{k}(\mathcal{Z}(L))$ *is* $f \bmod L$ *and* $y \bmod L$ *is a primitive element of the separable algebra* $\overline{k}(V \cap \mathcal{Z}(L))$ *over* $\overline{k}(\mathcal{Z}(L))$.

(v) *Let* $n \geqslant 3$. *Let* $\mathcal{L}$ *be a linear subspace of the space of all linear forms from* $\overline{k}[X_1, \ldots, X_n]$ *with* $\dim \mathcal{L} \geqslant 3$. *Suppose that for every* $\mathfrak{P} \in \mathcal{B}_4$ *such that* $\dim \mathcal{Z}(\mathfrak{P}) = n-1$ *the dimension*

$$\dim \overline{p(\mathcal{Z}(\mathfrak{P}))} \geqslant n-2, \tag{28}$$

where the bar means closure with respect to the Zariski topology. Then $\mathcal{L} \cap \mathcal{U}_2 \cap \mathcal{U}_3 \neq \emptyset$.

(vi) *Let* $n \geqslant 3$. *Let* $\mathcal{L}$ *be a linear subspace of the space of all linear forms from* $\overline{k}[X_1, \ldots, X_n]$ *with* $\dim \mathcal{L} \geqslant 3$. *Then* $\mathcal{L} \cap \mathcal{U}_4 \neq \emptyset$.

The proof of this theorem see in the Appendix of [4].

References

1. A. L. Chistov, *Polynomial complexity of the Newton–Puiseux algorithm.* — Lecture Notes in Computer Science, Vol. 233, Springer, New York, Berlin, Heidelberg, 1986, pp. 247–255.
2. A. L. Chistov, *Polynomial complexity algorithm for factoring polynomials and constructing components of a variety in subexponential time.* — Zap. Nauchn. Semin. LOMI **137** (1984), 124–188.
3. A. L. Chistov, *Double-exponential lower bound for the degree of a system of generators of a polynomial prime ideal.* — Algebra Analiz **20**, (6), (2008), 186–213.
4. A. L. Chistov, *A deterministic polynomial-time algorithm for the first Bertini theorem.* Preprint of St.Petersburg Mathematical Society (2004), `http://www.MathSoc.spb.ru`.

С.-Петербургское отделение
Математического института
им. В.А. Стеклова РАН,
наб. р. Фонтанки 27,
191023 Санкт-Петербург, Россия

E-mail: alch@pdmi.ras.ru

Поступило 11 сентября 2009 г.