SPb. Math. Society Preprint 2011-06 05 Dec 2011, rev. 29 Jan 2012

A Bound for the Degree of a System of Equations Giving the Variety of Reducible Polynomials

Alexander L. Chistov

St. Petersburg Department of Steklov Mathematical Institute
of the Academy of Sciences of Russia
Fontanka 27, St. Petersburg 191023, Russia,
e-mail: alch@pdmi.ras.ru

Abstract

Consider the affine space $\mathbb{A}^N(\overline{K})$ of homogeneous polynomials of degree d in $n+1$ variables with coefficients from an algebraic closure $\overline{K}$ of a field K of arbitrary characteristic, so $N = \binom{n+d}{n}$. We prove that the variety of all reducible polynomials from this affine space can be given by a system of polynomial equations of degree less than $56d^7$ in N variables. Using this result we formulate an effective version of the first Bertini theorem for the case of a hypersurface.

Introduction

Let K be an arbitrary field of characteristic $\mathrm{char}(K) = p$ with an algebraic closure $\overline{K}$ (in what follows for any field E we denote by $\overline{E}$ an algebraic closure of E). Let H be the primitive field of characteristic p, i.e., $H = \mathbb{Q}$ if $p = 0$ or $H = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ if $p > 0$. We shall assume that $H \subset K$.

It is well known that the discriminant Δ_f of a polynomial $f \in K[X_1]$ is a polynomial in the coefficients of f and $\Delta_f \neq 0$ if and only if f is square free in $\overline{K}[X_1]$, i.e., it does not have multiple factors in the ring $\overline{K}[X_1]$ or which is the same the polynomial f is separable. In the present paper we consider a polynomial $f = \sum_{i_1,\ldots,i_n} f_{i_1,\ldots,i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n} \in K[X_1, \ldots, X_n]$, $n \geqslant 2$, all $f_{i_1,\ldots,i_n} \in K$, of degree $\deg_{X_1,\ldots,X_n} f = d \geqslant 2$ and construct an analog A_f of the discriminant Δ_f in the following sense. The discriminant Δ_f of the polynomial in one variable corresponds to the property "f is separable". In the similar way A_f corresponds to the property "f is absolutely irreducible".

The element $A_f \in K_{w,v,u}$ where $K_{w,v,u}$ is a purely transcendental extension of the field K, see Section 3. Here w, v, u are families of transcendental elements over the field K and the field $K_{w,v,u}$ is generated over K by all the elements from these families. Actually $A_f \in K[w, v, u]$ where $K[w, v, u]$ is the ring of polynomials in all the elements from families w, v, u.

Key words and phrases: absolute irreducibility, lattices, the Bertini theorem.
UDK 513.6+518.5
2000 Mathematics Subject Classification: 14Q15, 14M99, 12Y05, 12E05, 13P05.

Further, A_f corresponds to f canonically: it is a polynomial in all the coefficients $f_{i_1,\dots,i_n}$ of f. The degree of this polynomial in $f_{i_1,\dots,i_n}$ is bounded from above by $56d^7$, see a more precise estimate in Section 3. Finally, the main property: $A_f \neq 0$ if and only if the polynomial f is irreducible in the ring $\overline{K}[X_1,\dots,X_n]$.

Consider the affine space $\mathbb{A}^N(\overline{K})$, $N = \binom{n+d}{n}$, (respectively $\mathbb{A}^{N_1}(\overline{K})$, $N_1 = \binom{n+d-1}{n-1}$) of polynomials (respectively homogeneous polynomials) from $\overline{K}[X_1, \dots, X_n]$ of degree at most d (respectively of degree d) in n variables with coefficients from an algebraic closure $\overline{K}$ of a field K. In this paper we regard 0 as a reducible polynomial. Although 0 belongs to the linear space of the homogeneous polynomial of degree d by definition $\deg 0 = -1$. The set $\mathcal{U}_{d,n}$ of polynomials of degree d from $\mathbb{A}^N(\overline{K})$ is an open in the Zariski topology subset of this affine space. As a consequence of the construction for the element A_f we get the following result.

THEOREM 1 *(i) Let $n \geqslant 2$ and $d \geqslant 1$ be integers. The set $\mathcal{V}_{d,n}$ of all reducible polynomials from $\overline{K}[X_1,\dots,X_n]$ of degree d is closed in $\mathcal{U}_{d,n}$ with respect to Zariski topology and $\mathcal{V}_{d,n}$ can be given as a set of all roots from $\mathcal{U}_{d,n}$ of a system of polynomial equations with coefficients from a primitive field H in N variables. The degree of this system is less than $56d^7$.*

(ii) Similarly the set $\mathcal{W}_{d,n}$ of all reducible polynomials from the affine space $\mathbb{A}^{N_1}(\overline{K})$ of homogeneous polynomials of degree d is closed in $\mathbb{A}^{N_1}(\overline{K})$ with respect to Zariski topology and $\mathcal{W}_{d,n}$ is a set of all roots of a system of polynomial equations with coefficients from the primitive field H in N_1 variables. The degree of this system is less than $56d^7$.

More precise statements for $n \geqslant 2$ and $d \geqslant 2$, see in Lemma 11 Section 3. Theorem 1 follows from Lemma 11 immediately. The proof of Lemma 11 is reduced to the case of two variables. This reduction is described in Section 3.

The case of two variables: $f \in K[X,T]$ is considered in Section 2. We suggest here a criterion for absolute irreducibility: $R_{\rho,f} \neq 0$, see (15) and Lemma 6. To get this criterion we describe a formal (or universal) version of the Hensel lemma, introduce a lattice corresponding to f over the ring of polynomials $\overline{K}[T]$ and consider a minimal vector in it. We would like to emphasize that Lemma 5 from Section 2 is one of the most important in the paper.

Estimates for a minimal vector in an arbitrary lattice over $K[T]$ are obtained in Section 1. The idea to consider lattices for questions related to irreducibility of polynomials is originated from [6] but in the present paper we have quite different accents.

As an application of Theorem 1 we get an efficient version of the first Bertini theorem for the case of a hypersurface. Let $f \in K[X_1,\dots,X_n,Y]$, $n \geqslant 2$, be a polynomial of degree $\deg_Y f \geqslant 1$. Assume that f is absolutely irreducible, i.e., irreducible in the ring $\overline{K}[X_1,\dots,X_n,Y]$. Suppose that its discriminant with respect to the variable Y

$$\Delta = \mathrm{Res}_Y\left(f, \frac{\partial f}{\partial Y}\right) \neq 0, \tag{1}$$

i.e., the polynomial f is separable with respect to Y. Denote by $\mathcal{K}$ the field of fractions of the ring $\overline{K}[X_1,\dots,X_n,Y]/(f)$.

Let $L_1, L_2 \in \overline{K}[X_1, \dots, X_n]$ be two linearly independent over $\overline{K}$ linear forms in $X_1, \dots, X_n$. Denote by $(L_1, L_2) \subset \overline{K}[X_1, \dots, X_n, Y]$ the ideal of the last ring of polynomials generated by L_1 and L_2. Consider the following conditions.

(a) The polynomial $f \notin (L_1, L_2)$ and for all $\mu_1, \mu_2 \in \overline{K}$ such that $\mu_1 \neq 0$ or $\mu_2 \neq 0$ the linear form $\mu_1 L_1 + \mu_2 L_2$ does not divide Δ.

(b) The discriminant $\Delta \notin (L_1, L_2)$.

The discriminant Δ is the the determinant of the Sylvester matrix of the polynomials $f, \partial f/\partial Y \in \overline{K}(X_1, \dots, X_n)[Y]$. Hence if $f \in (L_1, L_2)$ then $\Delta \in (L_1, L_2)$. Therefore, condition (b) implies (a).

THEOREM 2 *Let $f \in \overline{K}[X_1, \dots, X_n, Y]$, $n \geqslant 2$, be an irreducible polynomial such that $\deg_Y f \geqslant 1$, $\deg_{X_1,\dots,X_n,Y} f \leqslant d$ for an integer $d \geqslant 1$ and (1) is satisfied. Then the following assertions hold.*

(i) Assume that condition (a) or condition (b) holds for linearly independent linear forms L_1, L_2. Let $t^* \in \overline{K}$ and $L = L_2 - t^* L_1$. So the ring $\overline{K}[X_1, \dots, X_n]/(L)$ is isomorphic to the ring of polynomials in $n-1$ variables. Then for all $t^* \in \overline{K}$, except at most $56d^8$, the polynomial $f \bmod L \in \overline{K}[X_1, \dots, X_n]/(L)[Y]$ is irreducible in the last ring and $\Delta \bmod L \neq 0$. This means that the intersection of the hypersurface $\mathcal{Z}(f)$ and the hyperplane $\mathcal{Z}(L)$ in the affine space $\mathbb{A}^{n+1}(\overline{K})$ is transversal and irreducible over $\overline{K}$.

(ii) Suppose that $\mathcal{L}$ is a linear subspace of the space of all linear forms in $X_1, \dots, X_n$ with coefficients from $\overline{K}$ and the dimension $\dim \mathcal{L} \geqslant 3$ (hence also $n \geqslant 3$). Then there are $L_1, L_2 \in \mathcal{L}$ satisfying condition (b) (and therefore also (a)). More precisely, let $L_1', L_2', L_3' \in \mathcal{L}$ be three linearly independent linear forms and $I \subset \overline{K}$ be a finite set such that the number of elements $\#I = 1 + \deg_{X_1,\dots,X_n} \Delta$. Then there are $\alpha_1, \alpha_2 \in I$ such that $L_1 = L_1' - \alpha_1 L_3'$, $L_2 = L_2' - \alpha_2 L_3'$ satisfy condition (b).

Let us describe how to prove this theorem. Let $L_1, L_2, L_3, \dots, L_n$ be a basis of the space of all linear forms in $X_1, \dots, X_n$. Put $t = L_2/L_1$. Then $f \notin (L_1, L_2)$ if and only if the polynomial f is irreducible in the ring $\overline{K}(t)[L_1, L_3 \dots, L_n, Y]$. This follows from Lemma 12 with $Y, L_3, \dots, L_n, L_1, L_2$ in place of $X_1, \dots, X_{n+1}$ (in the sequel we refer in the Introduction also to Lemma 13, Lemma 14 and Corollary 3; one should do the similar replacement of variables there).

Further, assume that f is irreducible in the ring $\overline{K}(t)[L_1, L_3, \dots, L_n, Y]$. Then f is an irreducible element of the ring $\overline{K(t)}[L_1, L_3, \dots, L_n, Y]$ if and only if the field $\overline{K}(t)$ is algebraically closed in the field $\mathcal{K}$, see [7], Lemma 4. We give a simple direct independent proof of this fact in Lemma 13.

In Lemma 14 we prove that *if condition (a) or condition (b) is satisfied then the field $\overline{K}(t)$ is algebraically closed in $\mathcal{K}$.* In spite of the simplicity of this assertion probably this result is new.

Finally now assertion (i) follows from Corollary 3 of Lemma 14 immediately. Let us prove assertion (ii). Performing a nondegenerate linear transformation of variables $X_1, \dots, X_n$ one can suppose without loss of generality that $L_1' = X_{n-1}$, $L_2' = X_n$, $L_3' = X_1$. Then $\Delta \notin (L_1, L_2)$ if and only if

$$\Delta(X_1, \dots, X_{n-2}, \alpha_1 X_1, \alpha_2 X_1) \neq 0.$$

Thus the required $\alpha_1, \alpha_2 \in I$ exist. Theorem 2 is proved (modulo Lemmas 12—14 and Corollary 3).

REMARK 1 According to the construction described Sections 1–3 the number of equations in the polynomial system from Theorem 1 (i) (respectively (ii)) is bounded from above by $d^{(d+n)^{O(1)}}$.

One can obtain a system with a smaller number of equations as follows. Let us replace in the formulation of Theorem 1 the field H by an infinite extension H_1 of H. We assume that $H_1 \subset \overline{K}$. Then there is a modified system giving $\mathcal{V}_{d,n}$ (respectively $\mathcal{W}_{d,n}$) similar to the one from the statement (i) (respectively (ii)) of Theorem 1 and consisting of $N + 1 - \dim \mathcal{V}_{d,n}$ (respectively $N_1 + 1 - \dim \mathcal{W}_{d,n}$) polynomial equations with coefficients from H_1. To get the last system it is sufficient to take linear combinations with coefficients from H_1 of the initial equations from Theorem 1 (i) (respectively (ii)) in general position. Still these linear combinations are given not efficiently. It is difficult to construct them.

On the other hand, using [5] one can construct explicitly the elements $A_{i,f} \in K$, $1 \leqslant i \leqslant N_2 = d^{O(n)}$ satisfying the following properties. Every

$$A_{i,f} = A_f|_{w=w_i^*, v=v_i^*, u=u_i^*}$$

is obtained by the substitution in A_f some special values w_i^*, v_i^*, u_i^* of families w, v, u such that the elements of w_i^*, v_i^*, u_i^* are from the field H_1. The element $A_f \neq 0$ if and only if $A_{i,f} \neq 0$ for some $1 \leqslant i \leqslant N_2$. If the field K is finitely generated over H (of fixed transcendency degree) and given similarly to the ground field from the Introduction of [2] then for a polynomial f one can compute all $A_{i,f}$ within the time polynomial in the size of the polynomial f and d^n. We shall not prove and use this result in the present paper.

REMARK 2 It would be interesting to improve the upper bound $56d^8$ from assertion (i) of Theorem 2 (or the similar more precise upper bound from Corollary 3) for an arbitrary characteristic of the ground field. It is possible if $\mathrm{char}(K) = 0$. In this case one can replace $56d^8$ by $4d^4$. It can be deduced from the Irreducibility Criterion given in the Introduction of [4].

Note also that in zero–characteristic one can not improve the estimate $56d^7$ from Theorem 1 in the similar way.

The present paper is important. In future we hope to consider from the algorithmic point of view the effective version of the first Bertini theorem in general case and in arbitrary characteristic of the ground field. Still there we are able to obtain only less strong results than the ones from [4] in zero–characteristic. As an application the main result of [3] will be improved for the case of a finite ground field.

1 Estimates for a minimal vector in a lattice

Let K be an arbitrary field. Let $A = (a_{i,j})_{1 \leqslant i \leqslant n_1,\, 1 \leqslant j \leqslant n_2}$ be an $(n_1 \times n_2)$-matrix with the elements $a_{i,j}$ from the ring $B = K[T]$ where T is a transcendental element over the field K. Let $a_i = (a_{i,1}, \ldots, a_{i,n_2}) \in B^{n_2}$, $1 \leqslant i \leqslant n_1$, be the rows of the matrix A. Denote by M the B-submodule of B^{n_2} generated by all the rows a_i of the matrix A (in other words M is a lattice in B^{n_2}).

For an element $b \in B$ set $|b| = \deg_T b$ (we assume that $\deg_T 0 = -1$). So $|a_{i,j}| = \deg_T a_{i,j}$. Put $|A| = \max_{1 \leqslant i \leqslant n_1,\, 1 \leqslant j \leqslant n_2} |a_{i,j}|$ and for an arbitrary vector $y = (y_1, \ldots, y_{n_2}) \in B^{n_2}$ set $|y| = \max_{1 \leqslant j \leqslant n_2} |y_i|$. We shall suppose in what follows in this section that $|A| = D$. Let $r = \mathrm{rank}(A)$ be the rank of the matrix A.

The minimal vector of M is an arbitrary nonzero element $q \in M$ such that $|q| = \min\{|y| : 0 \neq y \in M\}$, i.e., $|q|$ is minimal possible.

LEMMA 1 *Let q be an arbitrary minimal vector of the lattice M. Then $|q| \leqslant D$ and one can represent*

$$q = \sum_{1 \leqslant i \leqslant n_1} \lambda_i a_i, \tag{2}$$

where $\lambda_i \in B$ and $|\lambda_i| \leqslant (2r+1)D$ for all $1 \leqslant i \leqslant n_1$.

PROOF Obviously $|q| \leqslant |A| = D$. Permuting the columns of the matrix A we shall suppose without loss of generality that the first r columns of the matrix A are linearly independent over the field $K(T)$. Let us represent $A = (A_1, A_2)$ where the matrix A_1 has r columns and A_2 has $n_2 - r$ columns. So $\mathrm{rank}(A_1) = r$. There is a matrix A_3 of the size $n_1 \times (n_1 - r)$ such that $\mathrm{rank}(A_1, A_3) = n_1$ and each column of the matrix A_3 contains only one nonzero entry and this entry is equal to 1 (if $r = n_1$ then A_3 has 0 columns, i.e., it is empty). Hence $(A_1, A_3) = A_4$ is a nondegenerate square matrix, its determinant $\det(A_4) \neq 0$ and $|\det(A_4)| \leqslant rD$.

The ring B is Euclidean. Hence as it is well known there is a matrix $Q \in \mathrm{GL}_{n_1}(B)$ (the matrix Q is a product of the elementary matrices over the ring B corresponding to the some elementary transformations of the rows of the matrix A_4) such that $QA_4 = A' = (a'_{i,j})_{1 \leqslant i,j \leqslant n_1}$ is an upper triangular matrix (this means that $a'_{i,j} = 0$ for all $1 \leqslant j < i \leqslant n_1$). Moreover, applying (if it is necessary) elementary transformations of rows to the obtained upper triangular matrix we shall suppose without loss of generality in the sequel that $|a'_{i,j}| < |a'_{j,j}|$ for all $1 \leqslant i < j \leqslant n_1$.

Since $Q \in \mathrm{GL}_{n_1}(B)$ the determinant $\det(A') = \alpha \det(A_4)$ for an element $0 \neq \alpha \in K$. Hence

$$\sum_{1 \leqslant j \leqslant n_1} \max_{1 \leqslant i \leqslant n_1} \{|a'_{i,j}|\} = \sum_{1 \leqslant j \leqslant n_1} |a'_{j,j}| = |\det(A_4)| \leqslant rD. \tag{3}$$

This implies of course $|A'| \leqslant |\det(A_4)|$. We have $Q = A_4^{-1} A'$. Put $\Delta_1 = \det(A_4)$. Now

$$|\Delta_1 Q| \leqslant |\Delta_1 A_4^{-1}| + |A'| \leqslant rD + |\Delta_1|.$$

(if $n_2 = n_1 = r$ then one can replace here rD by $(n_1 - 1)D$ but in the next section we have $n_1 > n_2$; so we don't take into account this minor improvement). Hence $|Q| \leqslant rD$.

Put $QA = A'' = (a''_{i,j})_{1 \leqslant i \leqslant n_1,\, 1 \leqslant j \leqslant n_2}$. Let $a''_1, \ldots, a''_{n_1}$ be the rows of the matrix A'' and A''_1 be the matrix consisting of the first r rows of the matrix A''. Now according to our construction $a''_1, \ldots, a''_r$ is the basis of the module M (it is a free module) over the ring B, $a''_i = 0$ for all $r+1 \leqslant i \leqslant n_1$ and $a''_{i,j} = a'_{i,j}$ for all $1 \leqslant i, j \leqslant r$.

Therefore there are $\mu_i \in B$, $1 \leqslant i \leqslant r$, such that $q = \sum_{1 \leqslant i \leqslant r} \mu_i a''_i$. Henceforth

$$q_j = \sum_{1 \leqslant i \leqslant r} \mu_i a'_{i,j}, \quad 1 \leqslant j \leqslant r.$$

Notice that $\det((a'_{i,j})_{1\leqslant i,j\leqslant r}) \neq 0$. Therefore, using Cramer's rule and (3) we get

$$|\mu_i| \leqslant |q| + \sum_{1\leqslant j\leqslant r} \max_{1\leqslant i\leqslant r}\{|a'_{i,j}|\} \leqslant D + rD = (r+1)D.$$

Let Q_1 be the matrix consisting of the first r rows of the matrix Q. Then $Q_1A = A''_1$ and $(\mu_1,\dots,\mu_r)Q_1A = q$. Put $(\lambda_1,\dots,\lambda_{n_1}) = (\mu_1,\dots,\mu_r)Q_1$. Now (2) holds and for all $1 \leqslant i \leqslant n_1$

$$|\lambda_i| \leqslant \max_{1\leqslant i\leqslant r} |\mu_i| + |Q_1| \leqslant (2r+1)D.$$

The lemma is proved.

Under conditions of Lemma 1 let us represent $\lambda_i = \sum_{0\leqslant\gamma\leqslant(2r+1)D} \lambda_{i,\gamma}\, T^\gamma$, $1 \leqslant i \leqslant n_1$, and $a_{i,j} = \sum_{0\leqslant\gamma\leqslant(2r+1)D} a_{i,j,\gamma}\, T^\gamma$, $1 \leqslant i \leqslant n_1$, $1 \leqslant j \leqslant n_2$, where all the coefficients $\lambda_{i,\gamma} \in K$, $a_{i,j,\gamma} \in K$ (if $\gamma > D$ then $a_{i,j,\gamma} = 0$ for all i,j).

Let $Z_{i,\nu}$, $1 \leqslant i \leqslant n_1$, $0 \leqslant \nu \leqslant (2r+1)D$, be new variables. Let $-1 \leqslant \mu_0 \leqslant D$ be an integer. Consider the homogeneous linear system with coefficients from the field K with respect to the variables $Z_{i,\nu}$

$$\sum_{0\leqslant\nu\leqslant\mu} \sum_{1\leqslant i\leqslant n_1} Z_{i,\nu}\, a_{i,j,\mu-\nu} = 0, \quad \mu_0 < \mu \leqslant (2r+2)D,\ 1 \leqslant j \leqslant n_2. \qquad (4)$$

Let $C_{A,-1}$ be the matrix of system (4) with $\mu_0 = -1$. It has $\nu_1 = ((2r+2)D+1)n_2$ rows and $\nu_2 = ((2r+1)+1)Dn_1$ columns. The rows (respectively columns) of the matrix $C_{A,-1}$ correspond to different pairs (μ,j) (respectively (i,ν)), see (4). We order pairs (μ,j) lexicographically: $(\mu_1,j_1) > (\mu_2,j_2)$ if and only if $\mu_1 > \mu_2$ or $\mu_1 = \mu_2$ and $j_1 > j_2$. Similarly we order pairs (i,ν). Next, we identify the linear ordered set of pairs (μ,j) (respectively (i,ν)) and $\{1,\dots,\nu_1\}$ (respectively $\{1,\dots,\nu_2\}$). Now the matrix $C_{A,-1}$ has the form $C_{A,-1} = (c_{i,j})_{1\leqslant i\leqslant\nu_1,\,1\leqslant j\leqslant\nu_2}$ where elements $c_{i,j}$ are uniquely defined by (4) and these identifications of linear ordered sets. Let $c_1,\dots,c_{\nu_1}$ be all the rows of the matrix $C_{A,-1}$.

Let $-1 \leqslant \rho \leqslant D$ be an arbitrary integer. Then the matrix $C_{A,\rho}$ of system (4) with $\mu_0 = \rho$ is identified with a submatrix of $C_{A,-1}$. Namely, $C_{A,\rho}$ consists of $((2r+2)D-\rho)n_2$ rows of matrix $C_{A,-1}$. These are rows $c_{\nu_3},\dots,c_{\nu_1}$ where $\nu_3 = 1+\nu_1-((2r+2)D-\rho)n_2 = (\rho+1)n_2+1$.

Set $\nu_0 = \max\{\nu_1,\nu_2\}$. Let $u = \{u_{i,j}\}_{1\leqslant i\leqslant\nu_1+\nu_2,\,1\leqslant j\leqslant\nu_0}$ be a family of algebraically independent over the field K elements. Denote by $K_u = K(u)$ the extension of the field K by all the elements from the family u. Hence the transcendency degree of K_u over K is $(\nu_1+\nu_2)\nu_0$. Put

$$h_{i,j} = \sum_{\nu_3\leqslant i_1\leqslant\nu_1,\,1\leqslant j_1\leqslant\nu_2} u_{i,i_1}u_{j+\nu_1,j_1}c_{i_1,j_1}, \quad \nu_3 \leqslant i \leqslant \nu_1,\ 1 \leqslant j \leqslant \nu_2,$$

$$h'_{i,j} = \sum_{1\leqslant i_1\leqslant\nu_1,\,1\leqslant j_1\leqslant\nu_2} u_{i,i_1}u_{j+\nu_1,j_1}c_{i_1,j_1}, \quad 1 \leqslant i \leqslant \nu_1,\ 1 \leqslant j \leqslant \nu_2.$$

So all $h_{i,j}, h'_{i,j} \in K_u$. In other words the matrix $(h'_{i,j})_{i,j}$ is obtained from $C_{A,-1}$ in two steps. At first one takes ν_1 generic linear combinations $c'_1,\dots,c'_{\nu_1}$ of the rows of the matrix $C_{A,-1}$ and get the matrix C' with the rows $c'_1,\dots,c'_{\nu_1}$. After that one takes ν_2 generic linear combinations $c''_1,\dots,c''_{\nu_2}$ of the columns of the matrix C' and get the matrix $C'' = (h'_{i,j})_{i,j}$. In the similar way one obtains the matrix $(h_{i,j})_{i,j}$ starting from $C_{A,\rho}$.

Let $0 \leqslant \gamma \leqslant \min\{\nu_1 - \nu_3 + 1, \nu_2\} = r_1$ be an integer. Put

$$\Delta_{A,\rho,\gamma} = \det((h_{i,j})_{1 \leqslant i,j \leqslant \gamma}), \quad \Delta'_{A,\gamma} = \det((h'_{i,j})_{1 \leqslant i,j \leqslant \gamma}).$$

Set $\Delta'_{A,r_1+1} = 0$. We have $\mathrm{rank}(C_{A,-1}) = \mathrm{rank}(C_{A,\rho}) = \gamma$ if and only if $\Delta_{A,\rho,\gamma} \neq 0$ and $\Delta'_{A,\gamma+1} = 0$.

LEMMA 2 *Under conditions of Lemma 1 let q be a minimal vector of the lattice M. Then $|q| > \rho$ if and only if every solution of system (4) with $\mu_0 = \rho$ is a solution of system (4) with $\mu_0 = -1$, i.e., if and only if there is $1 \leqslant \gamma \leqslant r_1$ such that $\Delta_{A,\rho,\gamma} \neq 0$ and $\Delta'_{A,\gamma+1} = 0$.*

Assume additionally that $\mathrm{rank}(C_{A,-1}) = r_0$. Then $|q| > \rho$ if and only if $\Delta_{A,\rho,r_0} \neq 0$.

PROOF This follows from the previous considerations and Lemma 1. The lemma is proved.

2 An irreducibility criterion: the case of two variables

Let K, T, $B = K[\,T\,]$ be the same as in the previous section. Let X be a variable and $f \in K[\,X,T]$ be a polynomial such that the degree $0 \leqslant \deg_T f \leqslant \rho$ for an integer $\rho \geqslant 1$. Further, let $\deg_X f = \deg_X f(X,0) = m \geqslant 2$ and the leading coefficient $\mathrm{lc}_X f \in K$ (the last condition means that $\deg_X(f - f(X,0)) < \deg_X f$). Put

$$\Delta_f = \mathrm{Res}_X(f(X,0), f'(X,0)) \in K \tag{5}$$

to be the discriminant of the polynomial $f(X,0)$. We shall assume that $\Delta_f \neq 0$, i.e., the polynomial $f(X,0)$ is has m pairwise distinct roots in the algebraic closure $\overline{K}$. We shall suppose that all these conditions are satisfied throughout this section.

Set $n_2 = m$. Put the ring $B_1 = \overline{K}[\,T\,]$, $B_2 = B_1[Z]$ where Z is a variable. We shall identify the set of polynomials $g \in \overline{K}[\,X,T]$ (respectively $g \in \overline{K}[\,Z,X,T]$) of degree $\deg_X g < m$ with B_1^m (respectively B_2^m). Under this identification

$$g = g_0 + g_1 X + \ldots + g_{m-1} X^{m-1} \mapsto (g_0, g_1, \ldots, g_{m-1}), \tag{6}$$

here all $g_i \in B_1$ (respectively all $g_i \in B_2$). We shall use the notation $|...|$ for polynomials, elements of B_1^m, B_2^m, matrices and so on, see the previous section. So at present $|g| = \deg_T g$ for any polynomial g. We shall apply the results of the previous section for the ring B_1 in place of B.

Set $f_0 = f(X,0)$. Let us represent $f_0 = f_0(Z) + (X - Z)g_0$ for a polynomial $g_0 \in K[Z,X]$. Notice that $g_0(Z,Z) = f'_0(Z) = \frac{d\,f_0}{dZ}$. Write $\delta = f'_0(Z)$.

Let us represent $f = \sum_{i \geqslant 0} f_i\, T^i$ where all $f_i \in K[X]$ (hence if $i > |f|$ then $f_i = 0$). Set $\overline{f}_i = \delta^{2i-2} f_i$ for all $i \geqslant 1$. Put $\overline{z}_0 = Z$.

For all $i \geqslant 1$ let us define recursively polynomials $\overline{g}_{i,j} \in K[Z]$, $0 \leqslant j \leqslant m-2$, and $\overline{z}_i \in K[Z]$. Put $\overline{g}_i = \sum_{0 \leqslant j \leqslant m-2} \overline{g}_{i,j} X^j \in K[Z,X]$.

Assume that $\overline{g}_j$ and $\overline{z}_j$ are defined for all $0 \leqslant j < i$ for some $i \geqslant 1$. Then

$$(X - Z)\overline{g}_i - g_0 \overline{z}_i = \delta\Big(\overline{f}_i + \sum_{1 \leqslant w \leqslant i-1} \overline{g}_w \overline{z}_{i-w}\Big). \tag{7}$$

Now to find all $\overline{g}_{i,j} \in K(Z)$, $0 \leqslant j \leqslant m-2$ and $-\overline{z}_i \in K(Z)$ one should solve using (7) a linear system with coefficients from $K(Z)$ by Cramer's rule. The coefficients matrix of this system is the Sylvester matrix of the polynomials $X - Z$ and g_0. Its determinant is $\pm\delta$. All the free terms of this system are divisible by δ. Hence actually all $\overline{g}_{i,j} \in K[Z]$ and $\overline{z}_i \in K[Z]$. The recursive step for the definition of $\overline{g}_i$ and $\overline{z}_i$ is described.

LEMMA 3 *(i) For all $i \geqslant 1$ the degrees*

$$\deg_Z \overline{g}_i \leqslant (2i-1)(2m-2), \quad \deg_Z \overline{z}_i \leqslant (2i-1)(2m-2).$$

(ii) Let us extend the field K till the field $K(t)$ where t is a new variable. Assume that $f \in K[t, X, T]$. Now $g_0 \in K[t, Z, X]$ and using (7) in the similar way as it was above one can prove that $\overline{g}_i \in K[t, Z, X]$, $\overline{z}_i \in K[t, Z]$ for all $i \geqslant 1$. Assume additionally that $\deg_t f \leqslant s$ for an integer s. Then for all $i \geqslant 1$ the degrees

$$\deg_t \overline{g}_i \leqslant (3i-1)s, \quad \deg_t \overline{z}_i \leqslant (3i-1)s.$$

PROOF (i) The degrees with respect to Z of all the minors of the Sylvester matrix of the polynomials $g_0, X-Z$ are bounded from above by $2m-3$. We have $\deg_Z \overline{f}_i \leqslant (2i-2)(m-1)$. Now the required assertion follows by the induction on i using Cramer's rule.

(ii) The degrees with respect to t of all the minors of the Sylvester matrix of the polynomials $g_0, X - Z$ are bounded from above by s. We have $\deg_t \overline{f}_i \leqslant (2i-1)s$. Now the required assertion follows by the induction on i using Cramer's rule. The lemma is proved.

Consider the separable K-algebra $K' = K[Z]/(f_0(Z))$. Put $z = Z \bmod f_0(Z) \in K'$. Then $f_0 = (X - z)g_0(z, X)$ where $g_0(z, X) \in K'[X]$. Notice that $\delta(z) = g_0(z, z)$ is an invertible element of K' since the polynomial f_0 is separable. Let $K'[[\,T\,]]$ be the ring of formal power series in T over the algebra K'. One can apply Hensel's lifting to the decomposition $f(X, 0) = (X - z)g_0(z, X)$ and get

$$f = \Big(X - \sum_{i \geqslant 0} z_i\, T^i\Big)\Big(g_0(z, X) + \sum_{i \geqslant 1} g_i\, T^i\Big) \tag{8}$$

in the ring $K'[[\,T\,]][X]$. Here $z_0 = z$, all $z_i \in K'$, the polynomials $g_i \in K'[X]$, $\deg_X g_i \leqslant m-2$, for all $i \geqslant 1$.

LEMMA 4 *For all $i \geqslant 1$*

$$z_i = \frac{\overline{z}_i(z)}{\delta(z)^{2i-1}}, \quad g_i = \frac{\overline{g}_i(z, X)}{\delta(z)^{2i-1}}. \tag{9}$$

PROOF Equality (8) implies that for all $i \geqslant 1$ the polynomials g_i and the elements z_i satisfy the recursive relation

$$(X - z)g_i - g_0(z, X)z_i = f_i + \sum_{1 \leqslant w \leqslant i-1} g_w z_{i-w}. \tag{10}$$

Now (9) is obtained by the induction on i using (10) and (7). The lemma is proved.

REMARK 3 Similarly to (8) and (9) one can obtain the decomposition

$$f - f_0(Z) = \Big(X - Z - \sum_{i\geqslant 1} \frac{\overline{z}_i}{\delta^{2i-1}}\, T^i\Big)\Big(g_0 + \sum_{i\geqslant 1} \frac{\overline{g}_i}{\delta^{2i-1}}\, T^i\Big)$$

in the ring $K(Z)[[T]][X]$. This is a formal (or universal) version of the Hensel lemma.

Set $D = (2m-1)\rho + 1$ and

$$\eta = \delta^{2D-3}X - \delta^{2D-3}\Big(Z + \sum_{1\leqslant i\leqslant D-1} \frac{\overline{z}_i\, T^i}{\delta^{2i-1}}\Big) = \tag{11}$$
$$\delta^{2D-3}X - \Big(\delta^{2D-3}Z + \sum_{1\leqslant i\leqslant D-1} \overline{z}_i \delta^{2(D-1-i)} T^i\Big) \in K[\,Z, X, T],$$

Let $x \in \overline{K}$ be a root of the polynomial $f(X,0)$, i.e., $f(x,0) = 0$. Put

$$\begin{array}{llll} a_i = \eta(x,X,T)X^{i-1}, & \widetilde{a}_i = \eta X^{i-1}, & 1 \leqslant i \leqslant m-1, \\ a_i = T^D X^{i-m}, & \widetilde{a}_i = T^D X^{i-m}, & m \leqslant i \leqslant 2m-1. \end{array} \tag{12}$$

Hence all $a_i \in B_1^m$, $\widetilde{a}_i \in B_2^m$ under identification (6). Put $n_1 = 2m-1$. Let A (respectively $\widetilde{A}$) be the matrix with the rows $a_1, \ldots, a_{n_1}$ (respectively $\widetilde{a}_1, \ldots, \widetilde{a}_{n_1}$). Hence $D = |A| = |\widetilde{A}|$. Let us apply the construction of Section 1 to the matrices A and $\widetilde{A}$ (replacing there the ground field K by $K[\,x\,]$ and $K(Z)$ respectively). Now the following objects corresponding to A and $\widetilde{A}$ are defined, see Section 1: the integers ν_i, $0 \leqslant i \leqslant 3$, r_1, the matrices $C_{A,-1}$, $C_{A,\rho}$, $C_{\widetilde{A},-1}$, $C_{\widetilde{A},\rho}$, the determinants $\Delta_{A,\rho,i}, \Delta'_{A,i+1} \in K_u[\,x\,]$, $\Delta_{\widetilde{A},\rho,i}, \Delta'_{\widetilde{A},i+1} \in K_u[Z]$ for all $1 \leqslant i \leqslant r_1$. Notice that $r = \mathrm{rank}(A) = \mathrm{rank}(\widetilde{A}) = m$ by (12).

LEMMA 5 *Let f be a polynomial satisfying all the conditions formulated at the beginning of the section and the matrices $C_{A,-1}$, $C_{\widetilde{A},-1}$ correspond to f. Then the ranks of matrices*

$$\mathrm{rank}(C_{A,-1}) = \mathrm{rank}(C_{\widetilde{A},-1}) = ((2m+2)D+1)m - D.$$

Put $r_0 = ((2m+2)D+1)m - D$ (recall that $D = (2m-1)\rho + 1$).

PROOF We shall prove this assertion for the matrix $C_{A,-1}$. The proof for $C_{\widetilde{A},-1}$ is similar and left to the reader. It is sufficient to show that r_0 is the maximal number of linearly independent equations of system (4) from Section 1 with $\mu_0 = -1$. By (12) the last system has the form

$$\left\{\begin{array}{ll} Z_{j+m-1,\mu-D} + & \\ \sum_{0\leqslant\nu\leqslant\mu}\sum_{1\leqslant i\leqslant m-1} Z_{i,\nu}a_{i,j,\mu-\nu} = 0, & D \leqslant \mu \leqslant (2r+2)D,\ 1 \leqslant j \leqslant m, \\ Z_{j-1,\mu}\delta^{2D-3}(x) = 0, & 0 \leqslant \mu < D,\ j = m, \\ Z_{j-1,\mu}\delta^{2D-3}(x) + & \\ \sum_{0\leqslant\nu\leqslant\mu} Z_{j,\nu}a_{j,j,\mu-\nu} = 0, & 0 \leqslant \mu < D,\ 2 \leqslant j \leqslant m-1, \\ \sum_{0\leqslant\nu\leqslant\mu} Z_{j,\nu}a_{j,j,\mu-\nu} = 0, & 0 \leqslant \mu < D,\ j = 1. \end{array}\right. \tag{13}$$

Let us delete from system (13) D equations

$$\sum_{0\leqslant\nu\leqslant\mu} Z_{1,\nu}a_{1,1,\mu-\nu}=0,\quad 0\leqslant\mu<D. \tag{14}$$

and denote by (*) the new obtained system. Then system (*) has the trapezoidal form (after a permutation of equations) with the elements $Z_{j+m-1,\mu-D}$, $D\leqslant\mu\leqslant(2r+2)D$, $1\leqslant j\leqslant m$; $Z_{j+1,\mu}\delta^{2D-3}(x)$, $0\leqslant\mu<D$, $2\leqslant j\leqslant m-1$, on the slanting side of the trapezoid. Hence all the equations of system (*) are linearly independent. The number of equation of system (*) is r_0. Finally (*) implies that $Z_{j,\mu}=0$ for all $1\leqslant j\leqslant m-1$, $0\leqslant\mu<D$. Hence equations (14) are linear combinations of the ones from system (*). The lemma is proved.

Let f_1 and f_2 be two polynomials in the variable Z. Denote by $\mathrm{Res}_Z(f_1,f_2)$ the resultant with respect to Z of the polynomials f_1 and f_2. This resultant is defined usually as the determinant of the Sylvester matrix for nonzero polynomials f_1, f_2 (in the case $\deg_Z f_1=\deg_Z f_2=0$ one obtains the empty Sylvester matrix, its determinant is 1 in the natural way). If $f_1=0$ or $f_2=0$ then by definition $\mathrm{Res}_Z(f_1,f_2)=0$.

Put

$$R_{\rho,f}=\mathrm{Res}_Z(\Delta_{\widetilde{A},\rho,r_0},f(Z,0))\in K_u. \tag{15}$$

Thus $R_{\rho,f}$ depends on ρ and the coefficients of the polynomial $f\in K[X,T]$. Denote by M the lattice in B_1^m generated by the rows of the matrix A. The minimal vector of the lattice M is defined as in Section 1 (now with the ring B_1 in place of B).

LEMMA 6 *Let $f\in K[X,T]$ be a polynomial satisfying all the conditions formulated at the beginning of the Section. Then the following assertions hold true.*

(i) Let q be an arbitrary minimal vector of M. Then $|q|>\rho$ if and only if the polynomial f is irreducible in the ring $\overline{K}[X,T]$.

(ii) The element $R_{\rho,f}\neq 0$ if and only if the polynomial f is irreducible in the ring $\overline{K}[X,T]$.

PROOF (i) Suppose that f is reducible in $\overline{K}[X,T]$. Then there is a divisor $g\in\overline{K}[X,T]$ of f such that the degree $1\leqslant\deg_X g<m$ and $X-x$ divides $g(X,0)$. The definition of the lattice M and the uniqueness of the the decomposition into the irreducibles in the ring $K[x]((T))[X]$ (here $K((T))$ is the field of fractions of the ring $K[[T]]$) imply that $g\in M$ (under identification (6)). We have $|q|\leqslant|g|\leqslant|f|\leqslant\rho$.

Conversely, suppose that $|q|\leqslant\rho$. Consider the resultant

$$R=\mathrm{Res}_X(q,f)\in K[x][T]$$

of the polynomials q and f with respect to X. As it is well known there are polynomials $p_1,p_2\in K[x][X,T]$ such that $R=p_1q+p_2f$. Since $q\in M$ the linear polynomial $\eta(x,X,T)\bmod T^D$ divides $q\bmod T^D$ in the ring $B_1/(T^D)[X]$. By (8), (9) and (11) also $\eta(x,X,T)\bmod T^D$ divides $f\bmod T^D$ in the ring $B_1/(T^D)[X]$. Therefore, $\eta(x,X,T)\bmod T^D$ divides $R\bmod T^D$ in the last ring. But $\deg_X R\leqslant 0$. Consequently $R\bmod T^D=0$ and hence $|R|\geqslant D$ or $R=0$.

On the other hand, the conditions $|f| \leqslant \rho$, $|q| \leqslant \rho$ imply that $|z| \leqslant \rho$ for each element z of the Sylvester matrix of the resultant R. The size of this matrix is bounded from above by $2m-1$. Therefore, $|R| \leqslant (2m-1)\rho = D-1$. Thus $R = 0$. This means that $\mathrm{G\,C\,D}\,(f,q) \neq 1$ in the ring $K[\,x\,][X,T]$. Hence f is a reducible polynomial in $\overline{K}[X,T]$ and (i) is proved.

(ii) Recall that $\Delta_{A,\rho,r_0} \in K_u[\,x\,]$, $\Delta_{\widetilde{A},\rho,r_0} \in K_u[Z]$ and according to our definitions $\Delta_{\widetilde{A},\rho,r_0}(x) = \Delta_{A,\rho,r_0}$. By Lemma 2 (with the ring B_1 in place of B) and Lemma 5 we have $\Delta_{A,\rho,r_0} \neq 0$ if and only if $|q| > \rho$ for a minimal vector q of M. Hence by (i) $\Delta_{A,\rho,r_0} = \Delta_{\widetilde{A},\rho,r_0}(x) \neq 0$ if and only if the polynomial f is irreducible in the ring $\overline{K}[\,X,T]$. But x is an arbitrary root of the polynomial $f_0(Z)$. Hence f is irreducible in the ring $\overline{K}[\,X,T]$ if and only if the polynomials $\Delta_{\widetilde{A},\rho,r_0}$ and $f_0(Z)$ are relatively prime in the ring $K_u[Z]$, i.e., if and only if their resultant $R_{\rho,f} \neq 0$. Assertion (ii) and all the lemma are proved.

LEMMA 7 *Let $f \in K[X,T]$ be a polynomial satisfying all the conditions formulated at the beginning of the Section. Then the following assertions hold.*

(i) The degree

$$\deg_Z \Delta_{\widetilde{A},\rho,r_0} \leqslant 2(m-1)(4m\rho - 2\rho - 1) \times \\ \left(4m^3\rho + 2m^2\rho + 2m^2 - 4m\rho + 3m + \rho - 1\right).$$

(ii) Under conditions of assertion (ii) of Lemma 3 the degrees

$$\deg_t \Delta_{\widetilde{A},\rho,r_0} \leqslant s(6m\rho - 3\rho - 1) \times \\ \left(4m^3\rho + 2m^2\rho + 2m^2 - 4m\rho + 3m + \rho - 1\right), \tag{16}$$

$$\deg_t R_{\rho,f} \leqslant s\left(14m^2\rho - 15m\rho - 3m + 4\rho + 2\right) \times \\ \left(4m^3\rho + 2m^2\rho + 2m^2 - 4m\rho + 3m + \rho - 1\right). \tag{17}$$

Hence if $2 \leqslant \deg_X f = m = d$, $1 \leqslant \deg_T f \leqslant \rho = d$, $\deg_t f \leqslant s = d$ then

$$\deg_t R_{\rho,f} \leqslant d\left(14d^3 - 15d^2 + d + 2\right)\left(4d^4 + 2d^3 - 2d^2 + 4d - 1\right). \tag{18}$$

PROOF We shall suppose without loss of generality that the conditions of assertion (ii) of Lemma 3 hold. From Lemma 3 and (11) we get

$$\deg_Z \eta \leqslant (2D-3)(2m-2), \quad \deg_t \eta \leqslant (3D-4)s \tag{19}$$

Let $C_{\widetilde{A},\rho} = (\widetilde{c}_{i,j})_{i,j}$ be the matrix corresponding to $\widetilde{A}$. According to (12) and (19) we have also $\deg_Z \widetilde{c}_{i,j} \leqslant (2D-3)(2m-2)$, $\deg_t \widetilde{c}_{i,j} \leqslant (3D-4)s$ for all i,j. Hence $\deg_Z \Delta_{\widetilde{A},\rho,r_0} \leqslant r_0(2D-3)(2m-2)$, $\deg_t \Delta_{\widetilde{A},\rho} \leqslant r_0(3D-4)s$ (one can check direcly that r_0 is no more than the number of the rows $((2r+2)D-\rho)m$ of the matrix $C_{\widetilde{A},\rho}$ but we even do not use this). This implies (i) and (16).

Finally considering the Sylvester matrix for the resultant of the polynomials $\Delta_{\widetilde{A},\rho,r_0}$ and $f_0(Z)$ we get

$$\deg_t R_{\rho,f} \leqslant \deg_Z \Delta_{\widetilde{A},\rho,r_0} \cdot \deg_t f_0 + \deg_Z f_0 \cdot \deg_t \Delta_{\widetilde{A},\rho,r_0} \leqslant \\ r_0(2D-3)(2m-2)s + mr_0(3D-4)s.$$

This implies (17).

The right part of (17) is a monotone increasing function of m and ρ for $m \geqslant 2$, $\rho \geqslant 1$. Now substituting $m = d$ and $\rho = d$ in (17) we get (18). The lemma is proved.

COROLLARY 1 *Let f be a polynomial satisfying the conditions of Lemma 7 and the ones from assertion (ii) of Lemma 3. Suppose that the polynomial $f \in K[t, X, T]$ is irreducible in the ring $\overline{K(t)}[X, T]$. Then there are at most*

$$\deg_t(\Delta_f R_{\rho,f}) \leqslant s(2m-1) + s\left(14m^2\rho - 15m\rho - 3m + 4\rho + 2\right) \times \quad (20)$$
$$\left(4m^3\rho + 2m^2\rho + 2m^2 - 4m\rho + 3m + \rho - 1\right)$$

values $t^* \in \overline{K}$ of t such that the polynomial $f(t^*, X, T)$ is reducible in the ring $\overline{K}[X, T]$ or $\Delta_f|_{t=t^*} = 0$. Note that $\Delta_f|_{t=t^*} = 0$ if and only if $\deg_X f_0 > \deg_X f(t^*, X, 0)$ or the polynomial $f(t^*, X, 0)$ is not separable.

PROOF Recall that $f_0 = f(t, X, 0)$. There are at most $\deg_t \Delta_f \leqslant (2m-1)s$ values $t^* \in \overline{K}$ of t such that $\Delta_f|_{t=t^*} = 0$. In what follows we shall assume that $\deg_X f_0 = \deg_X f(t^*, X, 0)$ and $f(t^*, X, 0)$ is separable. The resultant $R_{\rho,f} \in K[t]$ and according to our definitions $R_{\rho,f}(t^*) = R_{\rho,f(t^*,X,T)}$. Now (20) follows from Lemma 6 (ii) and (17). The corollary is proved.

3 An irreducibility criterion: general case

Let K be an arbitrary field and $f \in K[X_1, \ldots, X_n]$, $n \geqslant 2$, be a polynomial such that $\deg_{X_1,\ldots,X_n} f = d \geqslant 2$. We shall suppose that these conditions hold throughout this section

Let $v = \{v_i\}_{2 \leqslant i \leqslant n}$ and $w = \{w_{i,j}\}_{1 \leqslant i \leqslant n,\, 0 \leqslant j \leqslant n}$ be two families of transcendental elements over K such that the field $K_{w,v,u}$ generated over K by all the elements from families w, v, u has the maximal possible transcendency degree $n - 1 + n(n+1) + \nu_0(\nu_1 + \nu_2)$, see Section 1 (the integers ν_i, $0 \leqslant i \leqslant 2$, will be specified in the definition of A_f below). Write $K_v = K(v_2, \ldots, v_n)$, $\overline{K}_v = \overline{K}(v_2, \ldots, v_n)$. Denote by K_w (respectively $K_{w,v}$) the extension of the field K by all the elements from the family w (respectively families w and v). We shall denote by $K[w]$ (respectively $K[w, v]$; $K[w, v, u]$) the ring of polynomials in all the transcendental elements from the family w (respectively families w, v; w, v, u) with coefficients from K. We shall use the similar notation with other constant fields in place of K and other families of transcendental elements.

Set $f_v = f(X, v_2 T, \ldots, v_n T) \in K_v[X, T]$.

LEMMA 8 *Assume that the degree $\deg_{X_1} f = \deg_{X_1} f(X_1, 0, \ldots, 0) = d$ and the polynomial $f(X_1, 0, \ldots, 0)$ has d pairwise distinct roots in the field $\overline{K}$. The following assertions are equivalent.*

(i) The polynomial f is irreducible in the ring $\overline{K}[X_1, \ldots, X_n]$.

(ii) The polynomial f_v is irreducible in the ring $\overline{K}_v[X, T]$.

(iii) The polynomial f_v is irreducible in the ring $\overline{K_v}[X, T]$ where $\overline{K_v}$ is the algebraic closure of the field K_v.

PROOF Obviously (iii) implies (ii). Assume that f_v is reducible in the ring $\overline{K_v}[X, T]$ and a polynomial $h \in \overline{K_v}[X, T]$ divides f_v, $\deg_X h < \deg_X f_v$. Then

$h(X,0)$ divides $f_v(X,0)$. Hence multiplying h by a nonzero constant from $\overline{K_v}$ we can suppose without loss of generality that $h(X,0) \in \overline{K}[X]$. Now by the uniqueness of the Hensel's lifting $h \in \overline{K}_v[[\,T\,]][X]$. Therefore $h \in \overline{K}_v[[\,T\,]][X] \cap \overline{K_v}[\,X,T] = \overline{K}_v[\,X,T]$ where the last intersection is taken in $\overline{K_v}[[\,T\,]][X]$. Thus, f_v is reducible in the ring $\overline{K}_v[\,X,T]$. Hence (ii) implies (iii).

Assume that f_v is reducible in the ring $\overline{K}_v[\,X,T]$. Then the polynomial $f_v(X,1)$ is reducible in the ring $\overline{K}_v[X]$. By the Gauss lemma the polynomial $f(X,v_2,\ldots,v_n)$ is reducible in the ring $\overline{K}[X,v_2,\ldots,v_n]$. Hence (i) implies (ii).

Conversely, if f is reducible in the ring $\overline{K}[X_1,\ldots,X_n]$ then f_v is reducible in the ring $\overline{K}_v[\,X,T]$. Thus, (ii) implies (i). The lemma is proved.

Put the linear polynomials $W_i = w_{i,0} + \sum_{1 \leqslant i \leqslant n} w_{i,j}X_j$, $1 \leqslant i \leqslant n$. Set

$$f_w = f(W_1,W_2,\ldots,W_n) \in K[w][X_1,\ldots,X_n],$$
$$f_{w,v} = f_w(X,v_2T,\ldots,v_nT) \in K[w,v][\,X,T].$$

Notice that $\deg_{X_1} f_w = \deg_{X_1,\ldots,X_n} f_w = d$, $\deg_X f_{w,v} = \deg_T f_{w,v} = \deg_{X,T} f_{w,v} = d$.

LEMMA 9 *The following assertions are equivalent.*

(i) The polynomial f does not have multiple factors in $\overline{K}[X_1,\ldots,X_n]$.

(ii) The polynomial $f_w(X_1,0,\ldots,0)$ does not have multiple factors in $\overline{K_w}[X_1]$.

(iii) The polynomial $f_{w,v}(X,0)$ does not have multiple factors in $\overline{K_{w,v}}[X]$.

PROOF Assume that (i) is satisfied. Then by the Bézout theorem the generic line intersects the hypersurface $\mathcal{Z}(f)$ (of all the roots of the polynomial f in the affine space $\mathbb{A}^n(\overline{K})$) in d points. Hence the polynomial $f(w_{0,1}+w_{1,1}X_1,\ldots,w_{n,1}+w_{n,1}X_1)$ has d pairwise distinct roots in $\overline{K_w}$. This implies the equivalence of (i) and (ii). The equivalence of (ii) and (iii) follows from the equality $f_{w,v}(X,0) = f_w(X,0,\ldots,0)$. The lemma is proved.

Put

$$A_f = \Delta_{f_{w,v}} R_{d,f_{w,v}} \in K[w,v,u],$$

see (5), (15), now $\rho = d$ and the ground field is equal to $K_{w,v}$ in place of K.

LEMMA 10 *Let $f \in K[X_1,\ldots,X_n]$, $\deg_{X_1,\ldots,X_n} f = d \geqslant 2$, $n \geqslant 2$. Then the polynomial f is irreducible in the ring $\overline{K}[X_1,\ldots,X_n]$ if and only if the element $A_f \neq 0$.*

PROOF Suppose that $f \in \overline{K}[X_1,\ldots,X_n]$ is irreducible. Then the polynomial $f_{w,v}(X,0)$ does not have multiple factors in $\overline{K_{w,v}}[X]$ by Lemma 9. Therefore, $\Delta_{f_{w,v}} \neq 0$. Further, the polynomial f is irreducible in the ring $\overline{K_w}[X_1,\ldots,X_n]$. Hence also f_w is irreducible in the last ring. By Lemma 8 with the ground field K_w in place of K the polynomial $f_{w,v}$ is irreducible in the ring $\overline{K_{w,v}}[X,T]$. Now by Lemma 6 (ii) with the ground field $K_{w,v}$ in place of K we have $R_{d,f_{w,v}} \neq 0$. Thus $A_f \neq 0$.

Conversely, let $A_f \neq 0$. Then $\Delta_{f_{w,v}} \neq 0$ and the polynomial $f_{w,v}(X,0)$ does not have multiple factors in $\overline{K_{w,v}}[X]$. We have $R_{d,f_{w,v}} \neq 0$. Hence by Lemma 6 (ii) with the ground field $K_{w,v}$ in place of K the polynomial $f_{w,v} \in \overline{K_{w,v}}[\,X,T]$ is irreducible. Further by Lemma 8 with the ground field K_w in place of K the

polynomial $f_w \in \overline{K_w}[X_1, \ldots, X_n]$ is irreducible. Therefore, the polynomial f is irreducible in the ring $\overline{K}[X_1, \ldots, X_n]$. The lemma is proved.

Put $I_{d,n} = \{(i_1, \ldots, i_n) \in \mathbb{Z}^n : i_1 + \ldots + i_n \leqslant d;\, i_j \geqslant 0\, \forall j\}$ to be the set of multiindices, and $J_{d,n} = I_{d,n} \setminus I_{d-1,n}$, $d \geqslant 2$, $n \geqslant 2$. Notice that the number of elements $\#I_{d,n} = \binom{n+d}{n} = N$, $\#J_{d,n} = \binom{n+d-1}{n-1} = N_1$. Now let Φ (respectively Ψ) be a generic polynomial (respectively generic homogeneous polynomial) of degree d in n variables for a given characteristic p of the ground field. This means that

$$\Phi = \sum_{(i_1,\ldots,i_n)\in I_{d,n}} \varphi_{i_1,\ldots,i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}, \quad \Psi = \sum_{(i_1,\ldots,i_n)\in J_{d,n}} \psi_{i_1,\ldots,i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n},$$

where the family of coefficients $\varphi = \{\varphi_{i_1,\ldots,i_n}\}_{(i_1,\ldots,i_n)\in I_{d,n}}$ (respectively $\psi = \{\psi_{i_1,\ldots,i_n}\}_{(i_1,\ldots,i_n)\in J_{d,n}}$) consists of $\binom{n+d}{n}$ (respectively $\binom{n+d-1}{n-1}$) algebraically independent over the field H elements (recall that H is the primitive subfield of K).

We shall identify the set of all polynomial (respectively the linear space of all homogeneous polynomials) of degree d from $\overline{K}[X_1, \ldots, X_n]$ with an open in the Zariski topology subset $\mathcal{U}_{d,n} \subset \mathbb{A}^N(\overline{K})$ (respectively with the affine space $\mathbb{A}^{N_1}(\overline{K})$) where $\mathbb{A}^N(\overline{K})$ has the coordinate functions from the family φ (respectively $\mathbb{A}^{N_1}(\overline{K})$ has the coordinate functions from the family ψ).

Recall that $H[\varphi]$ and $H[\psi]$ are the rings of polynomials with coefficients from H in all the variables from the families φ and ψ respectively. The polynomials $\Phi \in H[\varphi][X_1, \ldots, X_n]$, $\Psi \in H[\psi][X_1, \ldots, X_n]$. The elements $A_\Phi \in H[\varphi, w, v, u]$, $A_\Psi \in H[\psi, w, v, u]$. One can uniquely represent

$$A_\Phi = \sum_{\mu\in M_\Phi} A_{\Phi,\mu}\, \mu, \quad A_\Psi = \sum_{\mu\in M_\Psi} A_{\Psi,\mu}\, \mu,$$

where all $A_{\Phi,\mu} \in H[\varphi]$ (respectively $A_{\Psi,\mu} \in H[\psi]$) are nonzero, μ runs over a set M_Φ (respectively M_Ψ) of pairwise distinct monomials with the coefficient 1 in the elements from the families w, v, u.

Put $I = I_{d,n}$ (respectively $I = J_{d,n}$). Now let

$$f = \sum_{(i_1,\ldots,i_n)\in I} \lambda_{i_1,\ldots,i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}$$

be an arbitrary polynomial (respectively homogeneous polynomial) of degree d with all coefficients $\lambda_{i_1,\ldots,i_n} \in K$. Denote by $\lambda = \{\lambda_{i_1,\ldots,i_n}\}_{(i_1,\ldots,i_n)\in I_{d,n}}$ (respectively $\lambda' = \{\lambda_{i_1,\ldots,i_n}\}_{(i_1,\ldots,i_n)\in J_{d,n}}$) the family of coefficients of this polynomial. Then according to the given definitions (we leave to check the details to the reader) for the case $I = I_{d,n}$

$$A_f = A_\Phi|_{\varphi=\lambda} = A_\Phi|_{\varphi_{i_1,\ldots,i_n}=\lambda_{i_1,\ldots,i_n}\, \forall (i_1,\ldots,i_n)\in I_{d,n}}, \tag{21}$$

i.e., A_f is obtained by the substitution in A_Φ the coefficients $\lambda_{i_1,\ldots,i_n}$ in place of the transcendental elements $\varphi_{i_1,\ldots,i_n}$ for all multiindices $(i_1, \ldots, i_n) \in I_{d,n}$. Similarly for the case of a nonzero homogeneous polynomial f when $I = J_{d,n}$

$$A_f = A_\Psi|_{\psi=\lambda'} = A_\Psi|_{\psi_{i_1,\ldots,i_n}=\lambda_{i_1,\ldots,i_n}\, \forall (i_1,\ldots,i_n)\in J_{d,n}}. \tag{22}$$

We have also $A_\Psi|_{\psi_{i_1,\ldots,i_n}=0\,\forall(i_1,\ldots,i_n)\in J_{d,n}}=0$.

For an arbitrary polynomial $z\in H[\varphi,w,v,u]$, (respectively $z\in H[\psi,w,v,u]$) denote by $\deg_\varphi z$ (respectively $\deg_\psi z$) the degree of z with respect to all the elements from the family φ (respectively ψ).

LEMMA 11 *(i) Let $n\geqslant 2$ and $d\geqslant 2$ be integers. Then the set $\mathcal{V}_{d,n}$ of all reducible polynomials from $\overline{K}[X_1,\ldots,X_n]$ of degree d is identified with the intersection $\mathcal{U}_{d,n}\cap\mathcal{Z}(\{A_{\Phi,\mu}\}_{\mu\in M_\Phi})$ where $\mathcal{Z}(\{A_{\Phi,\mu}\}_{\mu\in M_\Phi})$ is the set of all common zeroes in $\mathbb{A}^N(\overline{K})$ of the polynomials from the family $\{A_{\Phi,\mu}\}_{\mu\in M_\Phi}$.*

Similarly the set $\mathcal{W}_{d,n}$ of all reducible polynomials from the affine space $\mathbb{A}^{N_1}(\overline{K})$ of homogeneous polynomials of degree d is identified with the closed with respect to Zariski topology subset $\mathcal{Z}(\{A_{\Psi,\mu}\}_{\mu\in M_\Psi})\subset\mathbb{A}^{N_1}(\overline{K})$.

(ii) The degrees $\deg_\varphi A_\Phi$, $\deg_\psi A_\Psi$; $\deg_\varphi A_{\Phi,\mu}$, $\mu\in M_\Phi$; $\deg_\psi A_{\Psi,\mu}$, $\mu\in M_\Psi$, are bounded from above by

$$56d^7-32d^6-54d^5+96d^4-72d^3+15d^2+9d-3<56d^7. \tag{23}$$

PROOF (i) This follows immediately from the given definitions, Lemma 10 and (21), (22).

(ii) It is sufficient to prove the assertions related to $\deg_\varphi A_\Phi$ and $\deg_\psi A_\Psi$. Let us prove it for $\deg_\varphi A_\Phi$. Let t be a new variable. We shall suppose without loss of generality that the ground field $K\supset H[t,\varphi]$. Consider the polynomial $\widetilde{\Phi}=t\Phi\in H[t,\varphi]$. Then the definitions imply immediately $\deg_t A_{\widetilde{\Phi}}=\deg_\varphi A_\Phi$ and $\deg_t A_{\widetilde{\Phi}}=\deg_t(\Delta_{\widetilde{\Phi}_{w,v}}R_{d,\widetilde{\Phi}_{w,v}})$ (at present in the definition of $R_{d,\widetilde{\Phi}_{w,v}}$ the ground field is equal to $K_{w,v,u}(t)$ in place of K, see (15)). We can apply Corollary 1 to the polynomial $\widetilde{\Phi}_{w,v}$ over the ground field $K_{w,v,u}(t)$. Denote by $c(s,m,\rho)$ the right part of (20). Now $s=1$, $m=\rho=d$. Hence

$$\deg_t(\Delta_{\widetilde{\Phi}_{w,v}}R_{d,\widetilde{\Phi}_{w,v}})\leqslant c(1,d,d).$$

This implies (23) for $\deg_\varphi A_\Phi$. The proof of the estimate for $\deg_\psi A_\Psi$ is similar. The lemma is proved.

COROLLARY 2 *Let $f\in K[t,X_1,\ldots,X_n]$, $n\geqslant 2$, be a polynomial irreducible in the ring $\overline{K(t)}[X_1,\ldots,X_n]$ with $\deg_t f\leqslant d$, $\deg_{X_1,\ldots,X_n} f=d$ for an integer $d\geqslant 2$. Then there are at most*

$$\deg_t A_f\leqslant 56d^8-32d^7-54d^6+96d^5-72d^4+15d^3+9d^2-3d<56d^8$$

values $t^*\in\overline{K}$ of t such that the polynomial $f(t^*,X_1,\ldots,X_n)$ is reducible in the ring $\overline{K}[X_1,\ldots,X_n]$ or $\Delta_f|_{t=t^*}=0$. Notice also that $\Delta_f|_{t=t^*}=0$ if and only if $\deg_{X_1} f(t^*,X_1,\ldots,X_n)<\deg_{X_1} f$ or $\Delta_{f(t^*,X_1,\ldots,X_n)}=0$.

PROOF We have $A_f\in K_{w,v,u}[\,t\,]$ and if $A_f(t^*)\neq 0$ then $A_f(t^*)=A_{f(t^*,X_1,\ldots,X_n)}$. By (21) the degree $\deg_t A_f\leqslant d\deg_\varphi A_\Phi$. Now the required assertion follows from Lemma 10 and (23) immediately. The corollary is proved.

4 Effective version of the first Bertini theorem: the case of a hypersurface over a field of arbitrary characteristic

The aim of this section is to prepare everything for the proof of Theorem 2, see the Introduction. Let K be an arbitrary field and $f\in K[X_1,\ldots,X_{n+1}]$,

$n \geqslant 2$, be a polynomial irreducible in the ring $\overline{K}[X_1, \ldots, X_{n+1}]$ and such that $\deg_{X_1} f > 0$, $\deg_{X_1,\ldots,X_{n+1}} f = d$ and the discriminant of f with respect to X_1

$$\Delta = \mathrm{Res}_{X_1}\left(f, \frac{\partial f}{\partial X_1}\right) \neq 0. \tag{24}$$

We shall assume that all these conditions are satisfied throughout this section.

Put $t = X_{n+1}/X_n$. Then $f = f(X_1, \ldots, X_n, X_n t) \in K[t, X_1, \ldots, X_n]$. Denote by $(X_n, X_{n+1}) \subset K[X_1, \ldots, X_{n+1}]$ the ideal generated by X_n, X_{n+1}.

LEMMA 12 *The polynomial f is irreducible in the ring $\overline{K}(t)[X_1, \ldots, X_n]$ if and only if $f \notin (X_n, X_{n+1})$.*

PROOF This follows from the Gauss lemma (we leave the details to the reader). The lemma is proved.

The assertion of the following lemma follows from Lemma 4 [7]. Still at present it is useful to give a simple direct independent proof of this fact for the completeness (in the similar way one can prove Lemma 4 [7] in full generality).

LEMMA 13 *Let f be a polynomial satisfying all the conditions formulated at the beginning of the section. Suppose that the polynomial f is irreducible in the ring $\overline{K}(t)[X_1, \ldots, X_n]$. Then the following conditions are equivalent.*

(i) The polynomial f is reducible in the ring $\overline{K(t)}[X_1, \ldots, X_n]$.

(ii) The field $\overline{K}(t)$ is not algebraically closed in the field of fractions $\mathcal{K}$ of the ring $K[X_1, \ldots, X_{n+1}]/(f)$, i.e., there is an element $\theta \in \mathcal{K}$ algebraic over $\overline{K}(t)$ and such that $\theta \notin \overline{K}(t)$.

More than that, if (i) and (ii) are satisfied then the element θ is separable over the field $\overline{K}(t)$.

PROOF Suppose that (i) is satisfied. Let $f_1 \in \overline{K(t)}[X_1, \ldots, X_n]$ be a factor of f irreducible in the last ring such that some coefficient of f_1 is equal to 1. Now for all $x_2, \ldots, x_n \in \overline{K}(t)$ if $\Delta(x_2, \ldots, x_n, tx_n) \neq 0$ then the polynomial $f(X_1, x_2, \ldots, x_n, tx_n) \in \overline{K}(t)[X_1]$ is separable, $f_1(X_1, x_2, \ldots, x_n)$ divides $f(X_1, x_2, \ldots, x_n, tx_n)$ and, therefore, the coefficients of the polynomial $f_1(X_1, x_2, \ldots, x_n)$ are separable over the field $\overline{K}(t)$. From here using the interpolation by the elements $x_2, \ldots, x_n$ we get that the coefficients of the polynomial f_1 from $\overline{K(t)}$ are separable over $\overline{K}(t)$.

This implies that there is a finite Galois extension $E \supset \overline{K}(t)$ with the Galois group $\mathrm{Gal}(E/\overline{K}(t)) = G$ such that each absolutely irreducible factor of the polynomial f is equal to $\lambda\sigma(f_1)$ where $0 \neq \lambda \in \overline{K(t)}$ and $\sigma \in G$. Hence the decomposition of f into the absolute irreducible factors has the form $f = \lambda_0 f_1 \cdot \ldots \cdot f_\nu$, $\nu > 1$, where $f_1, \ldots, f_\nu \in E[X_1, \ldots, X_n]$ are all pairwise distinct conjugated to the polynomial f_1 over the field $\overline{K}(t)$ and $0 \neq \lambda_0 \in \overline{K}(t)$.

Now $E \otimes_{\overline{K}(t)} \mathcal{K}$ is a separable E-algebra and $E \otimes_{\overline{K}(t)} \mathcal{K} \simeq \prod_{1 \leqslant i \leqslant \nu} \mathcal{K}_i$ where $\mathcal{K}_i$ is a field of fractions of the ring $E[X_1, \ldots, X_n]/(f_i)$. Hence $E \otimes_{\overline{K}(t)} \mathcal{K} \supset \prod_{1 \leqslant i \leqslant \nu} E = E'$ and E' is a finite dimensional E-algebra which is invariant with respect to the action of the Galois group G.

On the other hand, let us show (again it is known of course) that every E-vector subspace $V \subset E \otimes_{\overline{K}(t)} \mathcal{K}$ which is invariant with respect to the action

of the Galois group G has the form $V = E \otimes_{\overline{K}(t)} V^G$ where $V^G \subset \mathcal{K}$ is a $\overline{K}(t)$-vector space of the invariant with respect to the action of G elements of V. Indeed, suppose contrary. Let e_i, $i \in I_1 \cup I_2$, be a $\overline{K}(t)$-basis of $\mathcal{K}$ such that e_i, $i \in I_2$ is a $\overline{K}(t)$-basis of V^G. Since $V \setminus (E \otimes_{\overline{K}(t)} V^G) = \widetilde{V} \neq \emptyset$ there is a vector

$$q = \sum_{1 \leqslant j \leqslant \mu} q_j e_{i_j} \in \widetilde{V} \tag{25}$$

such that all $i_1, \ldots, i_\mu \in I_1$, all $0 \neq q_j \in E$ and the integer μ is minimal possible. We have $\mu \geqslant 2$ and there is $1 < \alpha \leqslant \mu$ such that $q_\alpha/q_1 \notin \overline{K}(t)$ since otherwise we get a contradiction: $q_1^{-1}q \in V^G$ is a nontrivial linear combination of the elements e_i, $i \in I_1$, with coefficients from $\overline{K}(t)$.

Therefore, there is $\sigma \in G$ such that $\sigma(q_\alpha/q_1) \neq q_\alpha/q_1$. Put $\widetilde{q} = q_1^{-1}q - \sigma(q_1^{-1}q)$. Then $0 \neq \widetilde{q} \in \widetilde{V}$ and $\widetilde{q}$ has representation (25) with μ' in place of μ such that $\mu' < \mu$. This is a contradiction. Henceforth $V = E \otimes_{\overline{K}(t)} V^G$

Thus $E_1 = (E')^G \subset \mathcal{K}$ is a field and the degree of the extension $[E_1 : \overline{K}(t)] = \nu > 1$. One can choose $\theta \in E_1 \setminus \overline{K}(t)$. Hence condition (ii) is fulfilled.

Conversely, suppose that condition (ii) holds true. Let $X_1 \bmod f \in \overline{K}[X_1, \ldots, X_{n+1}]/(f) \subset \mathcal{K}$. Let $E_1 \supset \overline{K}(t)$ be an algebraic extension of the field $\overline{K}(t)$ such that $E_1 \subset \mathcal{K}$ and $E_1 \neq \overline{K}(t)$. Hence $\overline{K}(t)(X_2, \ldots, X_n) \neq E_1(X_2, \ldots, X_n) \subset \mathcal{K}$ and the extention $E_1 \supset \overline{K}(t)$ is separable. Therefore the degree of the minimal polynomial of the element $X_1 \bmod f \in \mathcal{K}$ over the field $E_1(X_2, \ldots, X_n)$ is less than $\deg_{X_1} f$. Henceforth using the Gauss lemma we get that there is a polynomial $f_1 \in E_1[X_1, \ldots, X_n]$ such that $\deg_{X_1} f_1 < \deg_{X_1} f$ and f_1 divides f in the ring $E_1[X_1, \ldots, X_n]$. Thus condition (i) is fulfilled. The lemma is proved.

LEMMA 14 *Suppose that the polynomial f is irreducible in the ring $\overline{K}(t)[X_1, \ldots, X_n]$ but f is reducible in the ring $\overline{K(t)}[X_1, \ldots, X_n]$. Then there are elements $\mu_1, \mu_2 \in \overline{K}$ such that $(\mu_1, \mu_2) \neq (0, 0)$ and $\mu_1 X_n + \mu_2 X_{n+1}$ divides the discriminant Δ.*

PROOF By Lemma 2 there is a finite separable algebraic extension of fields $E_1 \supset \overline{K}(t)$ such that the degree $[E_1 : \overline{K}(t)] > 1$ and E_1 is contained in the field $\mathcal{K}$. The extention of the fields $E_1 \supset \overline{K}(t)$ corresponds to the morphism $C \to \mathbb{P}^1(\overline{K})$ of the smooth projective curves defined over the field $\overline{K}$. The degree of this morphism is $\nu > 1$. The Hurwitz formula for the genus of the curve C implies that there is a discrete valuation $v : \overline{K}(t) \to \mathbb{Z} \cup \{+\infty\}$ of the field $\overline{K}(t)$ over $\overline{K}$ (or which is the same v is zero on $\overline{K} \setminus \{0\}$) and a discrete valuation v_1 which is an extension of v to the field E_1 such that v_1 is ramified over v, i.e., there is an element $\xi \in E_1$ with $v_1(\xi) = 1/e$ for an integer $e > 1$. The valuation v is defined by a uniformizing element

$$\pi = \frac{\mu_1 X_n + \mu_2 X_{n+1}}{\mu_3 X_n + \mu_4 X_{n+1}} \tag{26}$$

such that $\mu_1, \mu_2, \mu_3, \mu_4 \in \overline{K}$, $\mu_1\mu_4 - \mu_3\mu_2 \neq 0$ and $v(\pi) = 1$.

The elements $X_2, \ldots, X_{n-1}$, $\mu_3 X_n + \mu_4 X_{n+1}$ are algebraically independent over the field E_1. Hence, see [1], there is a discrete valuation v_2 of the field $E_1(X_2, \ldots, X_{n-1}, \mu_3 X_n + \mu_4 X_{n+1}) = E_2$ such that $v_2|_{E_1} = v_1$ and $v_2(X_i) = 0$, $1 \leqslant i \leqslant n-1$, $v_2(\mu_3 X_n + \mu_4 X_{n+1}) = 0$. Hence (26) implies $v_2(\mu_1 X_n + \mu_2 X_{n+1}) = 1$. Notice that $E_2 \supset \overline{K}(X_2, \ldots, X_{n+1})$.

The extension of fields $\mathcal{K} \supset \overline{K}(X_2, \ldots, X_{n+1})$ is finite separable since $\Delta \neq 0$. Therefore the extension $\mathcal{K} \supset E_2$ is also finite separable. Hence there is a discrete valuation v_3 of the field $\mathcal{K}$ such that $v_3|_{E_2} = v_2$. Denote by v_4 the restriction of v_3 to the field $\overline{K}(X_2, \ldots, X_{n+1})$. By the described construction $v_4(z) \geqslant 0$ for every $z \in \overline{K}[X_2, \ldots, X_{n+1}]$, $v_4(\mu_1 X_n + \mu_2 X_{n+1}) = 1$ and $v_4(\overline{K}(X_2, \ldots, X_{n+1}) \setminus \{0\}) = \mathbb{Z}$, see [1]. The valuation v_3 is ramified over v_4 since since $v_3(\xi) = v_1(\xi) = 1/e$. This implies that $\mu_1 X_n + \mu_2 X_{n+1}$ divides the discriminant Δ. The lemma is proved.

COROLLARY 3 *Let $f \in \overline{K}[X_1, \ldots, X_{n+1}]$, $n \geqslant 2$, be an irreducible polynomial such that $\deg_{X_1} f \geqslant 1$, $\deg_{X_1, \ldots, X_{n+1}} f \leqslant d$ for an integer $d \geqslant 1$ and (24) is satisfied. Suppose that f is irreducible in the ring $\overline{K}[X_1, \ldots, X_{n+1}]$, the polynomial f does not belong to the ideal (X_n, X_{n+1}) and for all $\mu_1, \mu_2 \in \overline{K}$ such that $\mu_1 \neq 0$ or $\mu_2 \neq 0$ the linear form $\mu_1 X_n + \mu_2 X_{n+1}$ does not divide Δ. Then for all $t^* \in \overline{K}$, except at most*

$$56d^8 - 32d^7 - 54d^6 + 96d^5 - 72d^4 + 15d^3 + 9d^2 - 3d < 56d^8$$

the polynomial $f(X_1, \ldots, X_n, t^* X_n) \in \overline{K}[X_1, \ldots, X_n]$ is irreducible in the last ring.

PROOF This follows immediately from Lemmas 12—14 and Corollary 2 from Section 3. The corollary is proved.

References

[1] **Bourbaki N.**, *"Algèbre commutative", Chap. 1–7* Actualités Sci. Indust., nos. 1290, 1293, 1308, 1314, Paris 1961, 1964, 1965.

[2] **Chistov A. L.:** *"Polynomial complexity algorithm for factoring polynomials and constructing components of a variety in subexponential time"*, Zap. Nauchn. Semin. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) v.137 (1984), p. 124–188 (in Russian) [English transl.: J. Sov. Math. v.34, No.4, (1986) p. 1838–1882].

[3] **Chistov A. L.:** *"Double-Exponential Lower Bound for the Degree of a System of Generators of a Polynomial Prime Ideal"*, Algebra i Analiz 20, (6), (2008) p. 186–213 (in Russian) [English transl.: St. Petersburg Math. J. v.20, (2009), p. 983–1001].

[4] **Chistov A. L.:** *"A deterministic polynomial–time algorithm for the first Bertini theorem"*, Preprint of St.Petersburg Mathematical Society (2004), http://www.mathsoc.spb.ru/preprint/2004/index.html

[5] **Chistov A.L., Fournier H., Gurvits L., Koiran P.:** *"Vandermonde Matrices, NP-Completeness, and Transversal Subspaces"*, Foundations of Computational Mathematics 3, (4), (2003) p. 421–427.

[6] **Lenstra A. K., Lenstra H. W., Lovasz L.:** *"Factoring Polynomials with Rational Coefficients"*, Mathematische Annalen 261, (1982) p. 515–534.

[7] **Zariski O.:** *"Pencils on an algebraic variety and a new proof of a theorem of Bertini"*, Trans. Amer. Math. Soc., v. 50 (1941) p. 48–70.