A BOUND FOR THE DEGREE OF A SYSTEM OF EQUATIONS DETERMINING THE VARIETY OF REDUCIBLE POLYNOMIALS

A. L. CHISTOV

ABSTRACT. Let \( \mathbb{A}^N(K) \) denote the affine space of homogeneous polynomials of degree \( d \) in \( n+1 \) variables with coefficients from the algebraic closure \( \bar{K} \) of a field \( K \) of arbitrary characteristic; so \( N = \binom{n+d}{n} \). It is proved that the variety of all reducible polynomials in this affine space can be given by a system of polynomial equations of degree less than \( 56d^7 \) in \( N \) variables. This result makes it possible to formulate an efficient version of the first Bertini theorem for the case of a hypersurface.

INTRODUCTION

Let \( K \) be an arbitrary field of characteristic \( \text{char}(K) = p \) with algebraic closure \( \bar{K} \) (in what follows for any field \( E \) we denote by \( \bar{E} \) the 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 assume that \( H \subset K \).

It is well known that the discriminant \( \Delta_f \) 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 \( \bar{K}[X_1] \), i.e., it has no multiple factors in the ring \( \bar{K}[X_1] \) or, which is the same, the polynomial \( f \) is separable. In the present paper we consider a polynomial \( f = \sum_{i_1,...,i_n} f_{i_1,...,i_n} X_1^{i_1} \cdots X_n^{i_n} \in K[X_1,\ldots,X_n] \), \( n \geq 2 \), with all \( f_{i_1,...,i_n} \) in \( K \), of degree \( \deg_{X_1,\ldots,X_n} f = d \geq 2 \) and construct an analog \( A_f \) of the discriminant \( \Delta_f \) in the following sense. The discriminant \( \Delta_f \) of the polynomial in one variable corresponds to the property “\( f \) is separable”. In a similar way, \( A_f \) corresponds to the property “\( f \) is absolutely irreducible”.

The element \( A_f \) belongs to \( K_{w,v,u} \) where \( K_{w,v,u} \) is a purely transcendental extension of the field \( K \), see §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 in these families. Actually, \( A_f \in \bar{K}[w,v,u] \), where \( \bar{K}[w,v,u] \) is the ring of polynomials in all the elements of the families \( w, v, u \).

Next, \( A_f \) corresponds to \( f \) canonically: it is a polynomial in all the coefficients \( f_{i_1,...,i_n} \) of \( f \). The degree of this polynomial in \( f_{i_1,...,i_n} \) is bounded from above by \( 56d^7 \); see a more precise estimate in §3. Finally, we state the main property: \( A_f \neq 0 \) if and only if the polynomial \( f \) is irreducible in the ring \( \bar{K}[X_1,\ldots,X_n] \).

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

2010 Mathematics Subject Classification. Primary 14Q15; Secondary 14M99, 12Y05, 12E05, 13P05.

Key words and phrases. Absolute irreducibility, lattices, Bertini theorem.
Theorem 1. (i) Let \( n \geq 2 \) and \( d \geq 1 \) be integers. The set \( \mathcal{V}_{d,n} \) of all reducible polynomials in \( K[X_1, \ldots, X_n] \) of degree \( d \) is closed in \( \mathcal{U}_{d,n} \) with respect to the Zariski topology, and \( \mathcal{V}_{d,n} \) can be given as the set of all roots in \( \mathcal{U}_{d,n} \) of a system of polynomial equations with coefficients in 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 in the affine space \( \mathbb{A}^{N_1}(\bar{K}) \) of homogeneous polynomials of degree \( d \) is closed in \( \mathbb{A}^{N_1}(\bar{K}) \) with respect to the Zariski topology, and \( \mathcal{W}_{d,n} \) is the set of all roots of a system of polynomial equations with coefficients in the primitive field \( H \) in \( N_1 \) variables. The degree of this system is less than \( 56d^7 \).

For more precise statements for \( n \geq 2 \) and \( d \geq 2 \), see Lemma 11 in §3. Theorem 1 follows from Lemma 11 immediately. The proof of Lemma 11 reduces to the case of two variables. This reduction is described in §3.

The case of two variables, \( f \in K[X,T] \), is treated in §2. Here, we suggest a criterion for absolute irreducibility: \( R_{\rho,f} \neq 0 \), see (15) and Lemma 6. To obtain this criterion, we describe a formal (or universal) version of the Hensel lemma, then introduce a lattice corresponding to \( f \) over the ring of polynomials \( \bar{K}[T] \), and consider a minimal vector in it. It should be emphasized that Lemma 5 in §2 is one of the most important results of the paper.

Estimates for a minimal vector in an arbitrary lattice over \( K[T] \) are obtained in §1. The idea to consider lattices for questions related to irreducibility of polynomials dates back to [9], 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 \( f \in K[X_1, \ldots, X_n, Y] \), \( n \geq 2 \), be a polynomial of degree \( \deg_Y f \) at least 1. Assume that \( f \) is absolutely irreducible, i.e., irreducible in the ring \( \bar{K}[X_1, \ldots, X_n, Y] \). Suppose that for its discriminant with respect to the variable \( Y \) we have

\[
\Delta = \text{Res}_Y \left( f, \frac{\partial f}{\partial Y} \right) \neq 0,
\]

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

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

(a) The polynomial \( f \) does not belong to \((L_1, L_2)\), and for all \( \mu_1, \mu_2 \in \bar{K} \) 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 \( \Delta \).

(b) The discriminant \( \Delta \) does not belong to \((L_1, L_2)\).

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

Theorem 2. Let \( f \in \bar{K}[X_1, \ldots, X_n, Y], n \geq 2 \), be an irreducible polynomial such that \( \deg_Y f \geq 1 \), \( \deg_{X_1, \ldots, X_n,Y} f \leq d \) for an integer \( d \geq 1 \), and (1) is satisfied. Then the following assertions hold true.

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

(ii) Suppose that \( L \) is a linear subspace of the space of all linear forms in \( X_1, \ldots, X_n \) with coefficients in \( K \), with \( \dim L \geq 3 \) (hence, also \( n \geq 3 \)). Then there are \( L_1, L_2 \in L \) satisfying condition (b) (and, therefore, also (a)). More precisely, let \( L'_1, L'_2, L'_3 \in L \) be three linearly independent linear forms, and let \( I \subset K \) be a finite set such that the number of elements \( \#I \) is equal to \( 1 + \deg_{X_1, \ldots, X_n} \Delta \). Then there are \( \alpha_1, \alpha_2 \in I \) such that \( L_1 = L'_1 - \alpha_1 L'_3 \) and \( L_2 = L'_2 - \alpha_2 L'_3 \) satisfy condition (b).

We describe how to prove this theorem. Let \( L_1, L_2, L_3, \ldots, L_n \) be a basis of the space of all linear forms in \( X_1, \ldots, X_n \). 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 \( K(t)[L_1, L_3, \ldots, L_n, Y] \). This follows from Lemma 12 with \( Y, L_3, \ldots, L_n, L_1, L_2 \) in place of \( X_1, \ldots, X_{n+1} \) (below in the Introduction we also refer to Lemma 13, Lemma 14, and Corollary 3; a similar replacement of variables should be done there).

Next, assume that \( f \) is irreducible in the ring \( K(t)[L_1, L_3, \ldots, L_n, Y] \). Then \( f \) is an irreducible element of the ring \( K(t)[L_1, L_3, \ldots, L_n, Y] \) if and only if the field \( K(t) \) is algebraically closed in the field \( K \); 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 \( K(t) \) is algebraically closed in \( K \). In spite of simplicity, probably this result is new.

Finally, now assertion (i) follows from Corollary 3 of Lemma 14 immediately. We prove (ii). Performing a nondegenerate linear transformation of the variables \( X_1, \ldots, X_n \), we can suppose without loss of generality that \( L'_1 = X_{n-1}, L'_2 = X_n, \) and \( L'_3 = X_1 \). Then \( \Delta \notin (L_1, L_2) \) if and only if

\[ \Delta(X_1, \ldots, X_{n-2}, \alpha_1 X_1, \alpha_2 X_1) \neq 0. \]

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

Remark 1. In accordance with the construction described in §§1–3, the number of equations in the polynomial system in Theorem 1 (i) (respectively, (ii)) is bounded from above by \( d^{(d+n)O(1)} \).

A system with a smaller number of equations can be obtained as follows. In Theorem 1, replace the field \( H \) by an infinite extension \( H_1 \) of \( H \), assuming that \( H_1 \subset K \). Then there is a modified system given by \( \mathcal{W}_{d,n} \) (respectively, \( \mathcal{W}_{d,n}' \)) similar to that in statement (i) (respectively, (ii)) of Theorem 1 and consisting of \( N+1 \) (respectively, \( N_1+1 \)) polynomial equations with coefficients in \( H_1 \). To get such a system, it suffices to take linear combinations with coefficients in \( H_1 \) 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, the results of [5] can be used to construct explicitly elements \( A_{i,f} \in K, 1 \leq i \leq N_2 = d^{O(n)} \), with the following properties. Every

\[ A_{i,f} = A_f \Bigg|_{w = w_i^*, v = v_i^*, u = u_i^*} \]

is obtained by substitution in \( A_f \) of some special values \( w_i^*, v_i^*, u_i^* \) of the families \( w, v, u \) such that the elements of \( w_i^*, v_i^*, u_i^* \) are in the field \( H_1 \). Then \( A_f \neq 0 \) if and only if \( A_{i,f} \neq 0 \) for some \( 1 \leq i \leq N_2 \). If the field \( K \) is finitely generated over \( H \) (with a fixed transcendence degree), and is given like the ground field in the Introduction in [2], then, for a polynomial \( f \), all \( A_{i,f} \) can be computed 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 $56d^8$ in assertion (i) of Theorem 2 (or the similar sharper upper bound in Corollary 3) for an arbitrary characteristic of the ground field. This is possible if char($K$) = 0. In this case, $56d^8$ can be replaced by $4d^4$. This can be deduced from the irreducibility criterion given in the Introduction of [4].

Note also that in the zero-characteristic case, the estimate $56d^7$ in Theorem 1 cannot be refined in a similar way.

The present paper is important. In future, we hope to consider the effective version of the first Bertini theorem from the algorithmic point of view, in the general case and for an arbitrary characteristic of the ground field. Still, there we are able to get only results weaker those obtained in [4] in the zero-characteristic case. As an application, the main result of [4] 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 $A = (a_{i,j})_{1 \leq i \leq n_1, 1 \leq j \leq n_2}$ be an $(n_1 \times n_2)$-matrix with the elements $a_{i,j}$ in the ring $B = K[T]$, where $T$ is a transcendental element over the field $K$. Let $a_i = (a_{i,1}, \ldots, a_{i,n_2}) \in B^{n_2}$, $1 \leq i \leq n_1$, be the rows of the matrix $A$. Denote by $M$ the $B$-submodule of $B^{n_2}$ generated by all rows $a_i$ of $A$ (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 $|A| = \max_{1 \leq i \leq n_1, 1 \leq j \leq n_2} |a_{i,j}|$ and set $|y| = \max_{1 \leq j \leq n_2} |y_i|$ for an arbitrary vector $y = (y_1, \ldots, y_{n_2}) \in B^{n_2}$. In what follows in this section we assume that $|A| = D$.

Let $r = \rank(A)$ 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 $|q| \leq D$, and we can write

$$q = \sum_{1 \leq i \leq n_1} \lambda_i a_i,$$

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

Proof. Obviously, $|q| \leq |A| = D$. Permuting the columns of the matrix $A$, we may assume without loss of generality that the first $r$ columns of $A$ are linearly independent over the field $K(T)$. Let $A = (A_1, A_2)$, where the matrix $A_1$ has $r$ columns and $A_2$ has $n_2 - r$ columns. Then $\rank(A_1) = r$. There is a matrix $A_3$ of size $n_1 \times (n_1 - r)$ such that $\rank(A_1, A_3) = n_1$ and each column of $A_3$ contains only one nonzero entry 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 nonsingular square matrix, its determinant $\det(A_4)$ is nonzero, and $|\det(A_4)| \leq rD$.

The ring $B$ is Euclidean. It is well known that then there is a matrix $Q \in \GL_{n_1}(B)$ (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 $QA_4 = A' = (a'_{i,j})_{1 \leq i, j \leq n_1}$ is an upper triangular matrix (this means that $a'_{i,j} = 0$ for all $1 \leq j < i \leq n_1$). Moreover, applying (if necessary) elementary transformations of rows to the resulting upper triangular matrix, we may assume without loss of generality that $|a_{i,j}'| < |a_{j,i}'|$ for all $1 \leq i < j \leq n_1$.

Since $Q \in \GL_{n_1}(B)$, we have $\det(A') = \alpha \det(A_4)$ for an element $0 \neq \alpha \in K$. Hence,

$$\sum_{1 \leq j \leq n_1} \max_{1 \leq i \leq n_1} |a_{i,j}'| = \sum_{1 \leq j \leq n_1} |a_{j,i}'| = |\det(A_4)| \leq rD.$$
Of course, this implies $|A'| \leq |\det(A_4)|$. We have $Q = A_4^{-1}A'$. Put $\Delta_1 = \det(A_4)$. Now,

$$|\Delta_1Q| \leq |\Delta_1A_4^{-1}| + |A'| \leq rD + |\Delta_1|,$$

(if $n_2 = n_1 = r$, then here we can replace $rD$ by $(n_1 - 1)D$, but in the next section we have $n_1 > n_2$, so that we ignore this minor improvement). Hence, $|Q| \leq rD$.

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

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

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

Note that $\det((a''_{i,j})_{1 \leq i, j \leq r}) \neq 0$. Using Cramer’s rule and (3), we get

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

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

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

The lemma is proved. \hfill \Box

Under the conditions of Lemma 1, we write $\lambda_i = \sum_{0 \leq \gamma \leq (2r + 1)D} \lambda_i, \gamma T_\gamma^\gamma$, $1 \leq i \leq n_1$, and $a_{i,j} = \sum_{0 \leq \gamma \leq (2r + 1)D} a_{i,j, \gamma} T_\gamma^\gamma$, $1 \leq i \leq n_1$, $1 \leq j \leq n_2$, where $\lambda_i, \gamma \in K$, $a_{i,j, \gamma} \in K$ (if $\gamma > D$, then $a_{i,j, \gamma} = 0$ for all $i, j$).

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

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

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 $(\mu, j)$ (respectively, $(i, \nu)$); see (4). We order the pairs $(\mu, j)$ lexicographically: $(\mu_1, j_1) > (\mu_2, j_2)$ if and only if $\mu_1 > \mu_2$ or $\mu_1 = \mu_2$ and $j_1 > j_2$. The pairs $(i, \nu)$ are ordered similarly. Next, we identify the linearly ordered set of pairs $(\mu, j)$ (respectively, $(i, \nu)$) and $\{1, \ldots, \nu_1\}$ (respectively, $\{1, \ldots, \nu_2\}$). Now the matrix $C_{A,-1}$ has the form $C_{A,-1} = (c_{i,j})_{1 \leq i \leq \nu_1, 1 \leq j \leq \nu_2}$, where the elements $c_{i,j}$ are uniquely determined by (4) and by these identifications of linearly ordered sets. Let $c_1, \ldots, c_{\nu_1}$ be all the rows of the matrix $C_{A,-1}$.

Let $-1 \leq \rho \leq D$ 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 the matrix $C_{A,-1}$. These are the rows $c_{\nu_3}, \ldots, c_{\nu_2}$, 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 $u = \{u_{i,j}\}_{1 \leq i \leq \nu_1 + \nu_2, 1 \leq j \leq \nu_0}$ be a family of elements algebraically independent over the field $K$. Denote by $K_u = K(u)$ the extension of the field
Let $K_n$ by all the elements of the family $u$. Hence, the transcendence degree of $K_n$ over $K$ is $(\nu_1 + \nu_2)\nu_0$. Put

$$h_{i,j} = \sum_{\nu_3 \leq i \leq \nu_1, 1 \leq j \leq \nu_2} u_{i,i} u_{j+j,1,1}, \quad \nu_3 \leq i \leq \nu_1, 1 \leq j \leq \nu_2;$$

$$h'_{i,j} = \sum_{1 \leq i \leq \nu_1, 1 \leq j \leq \nu_2} u_{i,i} u_{j+j,1,1}, \quad 1 \leq i \leq \nu_1, 1 \leq j \leq \nu_2.$$

Then all $h_{i,j}, h'_{i,j}$ are in $K_n$. In other words, the matrix $(h'_{i,j})_{i,j}$ is obtained from $C_{A,-1}$ in two steps. First, we take $\nu_1$ generic linear combinations $c'_1, \ldots, c'_{\nu_1}$ of the rows of $C_{A,-1}$, obtaining a matrix $C'$ with rows $c'_1, \ldots, c'_{\nu_1}$. After that, we take $\nu_2$ generic linear combinations $c''_1, \ldots, c''_{\nu_2}$ of the columns of the matrix $C'$ and get a matrix $C'' = (h'_{i,j})_{i,j}$.

In a similar way, we build a matrix $(h_{i,j})_{i,j}$ starting with $C_{A,\rho}$.

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

$$\Delta_{A,\rho,\gamma} = \det((h_{i,j})_{1 \leq i \leq \nu_1, 1 \leq j \leq \nu_2}), \quad \Delta'_{A,\gamma} = \det((h'_{i,j})_{1 \leq i \leq \nu_1, 1 \leq j \leq \nu_2}).$$

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

Lemma 2. Under the 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 $1 \leq \gamma \leq r_1$ such that $\Delta_{A,\rho,\gamma} \neq 0$ and $\Delta'_{A,\gamma+1} = 0$.

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

Proof. This follows from the considerations above and Lemma 1. \hfill \Box

§2. Irreducibility criterion: The case of two variables

Let $K, T, B = K[T]$ be the same as in the preceding section. Let $X$ be a variable, and let $f \in K[X, T]$ be a polynomial such that $0 \leq \deg_T f \leq \rho$ for an integer $\rho \geq 1$. Next, suppose that $\deg_X f = \deg_X f(X,0) = m \geq 2$ and the leading coefficient $\text{lc}_X f$ belongs to $K$ (the last condition means that $\deg_X (f - f(X,0)) < \deg_X f$). Put

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

(5)

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

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

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

where all $g_i$ are in $B_1$ (respectively, all $g_i$ are in $B_2$). We shall use the notation $\cdots$ for polynomials, elements of $B_1^n$, $B_2^n$, matrices, and so on, see the preceding section. So, now $|g| = \deg_T g$ for any polynomial $g$. We shall apply the results of the preceding section to the ring $B_1$ in place of $B$.

Setting $f_0 = f(X,0)$, we write $f_0 = f_0(Z) + (X - Z)g_0$ for a polynomial $g_0 \in K[Z, X]$. Notice that $g_0(Z, Z) = f_0'(Z) = \frac{df_0}{dZ}$. Put $\delta = f_0'(Z)$.

We represent $f$ in the form $f = \sum_{i \geq 0} f_i T^i$, where all $f_i$ are in $K[X]$ (hence, if $i > |f|$, then $f_i = 0$). Set $\bar{f}_i = \delta^{2i-2} f_i$ for all $i \geq 1$. Put $\bar{z}_0 = Z$. 
For all \( i \geq 1 \), we define recursively polynomials \( \bar{g}_{i,j} \in K[Z] \), \( 0 \leq j \leq m - 2 \), and \( \bar{z}_i \in K[Z] \). Put \( \bar{g}_i = \sum_{0 \leq j \leq m-2} \bar{g}_{i,j}X^j \in K[Z,X] \).

Assume that \( \bar{g}_j \) and \( \bar{z}_j \) are defined for all \( 0 \leq j < i \) for some \( i \geq 1 \). Then

\[
(X - Z)\bar{g}_i - g_0\bar{z}_i = \delta \left( \bar{f}_i + \sum_{1 \leq w \leq i-1} \bar{g}_w \bar{z}_{i-w} \right).
\]

Now, to find all \( \bar{g}_{i,j} \in K(Z) \), \( 0 \leq j \leq m - 2 \), and \( -\bar{z}_i \in K(Z) \), one should use (7) and solve a linear system with coefficients in \( K(Z) \) by Cramer’s rule. The coefficient 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 \( \delta \). Hence, actually, all \( \bar{g}_{i,j} \) are in \( K[Z] \) and \( \bar{z}_i \in K[Z] \). The recursive step for determining the \( \bar{g}_i \) and \( \bar{z}_i \) is described.

**Lemma 3.** (i) For all \( i \geq 1 \),

\[
\deg_Z \bar{g}_i \leq (2i - 1)(2m - 2), \quad \deg_Z \bar{z}_i \leq (2i - 1)(2m - 2).
\]

(ii) Let us extend the field \( K \) up to the field \( K(t) \), where \( t \) is a new variable. Assume that \( f \in K[t,X,T] \), and using (7) like this was done above one can prove that \( \bar{g}_i \in K[t,Z,X] \) and \( \bar{z}_i \in K[t,Z] \) for all \( i \geq 1 \). Assume additionally that \( \deg_t f \leq s \) for an integer \( s \). Then for all \( i \geq 1 \) we have

\[
\deg_{t} \bar{g}_i \leq (3i - 1)s, \quad \deg_{t} \bar{z}_i \leq (3i - 1)s.
\]

**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 \( \deg_Z \bar{f}_i \leq (2i - 2)(m - 1) \). Now the claim follows by induction on \( i \) with the use of 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 \( \deg_{t} \bar{f}_i \leq (2i - 1)s \). Now, (ii) follows by induction on \( i \) with the use of Cramer’s rule. The lemma is proved. \( \Box \)

Consider the separable \( K \)-algebra \( K' = K[Z]/(f_0(Z)) \). Put \( z = Z \mod f_0(Z) \in K' \). Then \( f_0 = (X - z)g_0(z,X) \), where \( g_0(z,X) \in K'[X] \). Note that \( \delta(z) = g_0(z,z) \) is an invertible element of \( K' \), because the polynomial \( f_0 \) is separable. Let \( K'[[T]] \) be the ring of formal power series in \( T \) over the algebra \( K' \). We can apply Hensel’s lifting to the decomposition \( f(X,0) = (X - z)g_0(z,X) \), obtaining

\[
f = \left( X - \sum_{i \geq 0} z_i T^i \right) \left( g_0(z,X) + \sum_{i \geq 1} g_i T^i \right)
\]

in the ring \( K'[[T]][X] \). Here \( z_0 = z \), all \( z_i \) are in \( K' \), the polynomials \( g_i \) belong to \( K'[X] \), \( \deg_X g_i \leq m - 2 \), for all \( i \geq 1 \).

**Lemma 4.** For all \( i \geq 1 \), we have

\[
z_i = \frac{\bar{z}_i(z)}{\delta(z)^{2i-1}}, \quad g_i = \frac{\bar{g}_i(z,X)}{\delta(z)^{2i-1}}.
\]

**Proof.** Formula (8) implies that for all \( i \geq 1 \) the polynomials \( g_i \) and the elements \( z_i \) satisfy the recursive relation

\[
(X - z)g_i - g_0(z,X)z_i = f_i + \sum_{1 \leq w \leq i-1} g_w z_{i-w}.
\]

Now, (9) is obtained by induction on \( i \) with the help of (10) and (7). \( \Box \)
Remark 3. Like (8) and (9), we can obtain the expansion
\[ f - f_0(Z) = \left( X - Z - \sum_{i \geq 1} \frac{z_i}{\delta^{2i-1}} T^i \right) \left( g_0 + \sum_{i \geq 1} \frac{\bar{g}_i}{\delta^{2i-1}} T^i \right) \]
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
\[
\eta = \delta^{2D-3} X - \delta^{2D-3} \left( Z + \sum_{1 \leq i \leq D - 1} \frac{z_i}{\delta^{2i-1}} T^i \right) = \delta^{2D-3} X - \left( \delta^{2D-3} Z + \sum_{1 \leq i \leq D - 1} z_i \delta^{2(D-1-i)} T^i \right) \in K[Z, X, T],
\]
(11)

Let $x \in \bar{K}$ be a root of the polynomial $f(X, 0)$, i.e., $f(x, 0) = 0$. Put
\[
a_i = \eta(x, X, T) X^{i-1}, \quad \bar{a}_i = \eta X^{i-1}, \quad 1 \leq i \leq m - 1,
\]
\[
a_i = T^D X^{i-m}, \quad \bar{a}_i = T^D X^{i-m}, \quad m \leq i \leq 2m - 1.
\]
Hence, $a_i \in B_1^m$ and $\bar{a}_i \in B_2^m$, under the identification (6). Put $n_1 = 2m - 1$. Let $A$ (respectively, $\tilde{A}$) be the matrix with the rows $a_1, \ldots, a_{n_1}$ (respectively, $\tilde{a}_1, \ldots, \tilde{a}_{n_1}$).

Consequently, $D = |A| = |\tilde{A}|$. We apply the construction of §1 to the matrices $A$ and $\tilde{A}$ (replacing there the ground field $K$ by $K[x]$ and $K(Z)$, respectively). Now the following objects corresponding to $A$ and $\tilde{A}$ are defined; see §1: the integers $\nu_i, 0 \leq i \leq 3, r_1$, the matrices $C_{A, -1}, C_{A, \rho}, \tilde{C}_{\tilde{A}, -1}, \tilde{C}_{\tilde{A}, \rho}$, the determinants $\Delta_{A, \rho, i}, \Delta'_{\tilde{A}, i+1} \in K_u[x]$, $\Delta_{\tilde{A}, \rho, i}, \Delta'_{\tilde{A}, i+1} \in K_u[Z]$ for all $1 \leq i \leq r_1$. Note that $r = \text{rank}(A) = \text{rank}(\tilde{A}) = m$ by (12).

Lemma 5. Let $f$ be a polynomial satisfying all the conditions formulated at the beginning of the section, and let matrices $C_{A, -1}, C_{\tilde{A}, -1}$ correspond to $f$. Then
\[
\text{rank}(C_{A, -1}) = \text{rank}(C_{\tilde{A}, -1}) = ((2m + 2)D + 1)m - D.
\]
Put $r_0 = ((2m + 2)D + 1)m - D$ (recall that $D = (2m - 1)\rho + 1$).

Proof. We prove this for the matrix $C_{A, -1}$. Since the proof for $C_{\tilde{A}, -1}$ is similar, it is left to the reader. It suffices to show that $r_0$ is the maximal number of linearly independent equations of system (4) from §1 with $\mu_0 = -1$. By (12), this system has the form
\[
\begin{cases}
Z_{j+m-1, \mu - D} + \sum_{0 \leq \nu \leq \mu} \sum_{1 \leq i \leq m - 1} Z_{i, \nu} a_{i,j,\mu - \nu} = 0, & 0 \leq \mu \leq (2r + 2)D, \\
Z_{j-1, \mu} \delta^{2D-3}(x) = 0, & 0 \leq \mu < D, \quad j = m, \\
Z_{j-1, \mu} \delta^{2D-3}(x) + \sum_{0 \leq \nu \leq \mu} Z_{j, \nu} a_{j,j,\mu - \nu} = 0, & 0 \leq \mu < D, \quad 2 \leq j \leq m - 1, \\
\sum_{0 \leq \nu \leq \mu} Z_{j, \nu} a_{j,j,\mu - \nu} = 0, & 0 \leq \mu < D, \quad j = 1.
\end{cases}
\]
(13)

From system (13) we delete $D$ equations
\[
Z_{1, \nu} a_{1,1,\mu - \nu} = 0, \quad 0 \leq \mu < D,
\]
and denote by $(*)$ the resulting system. Then system $(*)$ has a trapezoidal form (after a permutation of equations and variables) with the elements $Z_{j+m-1, \mu - D}$ for $D \leq \mu \leq (2r + 2)D, 1 \leq j \leq m$, and the elements $Z_{j-1, \mu} \delta^{2D-3}(x), 0 \leq \mu < D, 2 \leq j \leq m,$
on the slanting side of the trapezoid. Hence, all equations of system (\textasterm{*}) are linearly independent. The number of equations in (\textasterm{*}) is \( r_0 \). Finally, (\textasterm{*}) implies that \( Z_{j,\mu} = 0 \) for all \( 1 \leq j \leq m-1, \, 0 \leq \mu < D \). Therefore, equations (14) are linear combinations of those in system (\textasterm{*}). The lemma is proved. \hfill \Box

Let \( f_1 \) and \( f_2 \) be two polynomials in the variable \( Z \). Denote by \( \text{Res}_Z(f_1, f_2) \) the resultant with respect to \( Z \) of the polynomials \( f_1 \) and \( f_2 \). Usually, this resultant is defined as the determinant of the Sylvester matrix for nonzero polynomials \( f_1, f_2 \) (in the case where \( \deg Z f_1 = \deg Z f_2 = 0 \) the Sylvester matrix is empty, and its determinant is 1 in the natural way). If \( f_1 = 0 \) or \( f_2 = 0 \), then \( \text{Res}_Z(f_1, f_2) = 0 \) by definition.

Put

\begin{equation}
R_{\rho, f} = \text{Res}_Z(\Delta_{\gamma', \rho, r_0}, f(Z, 0)) \in K_u.
\end{equation}

Thus, \( R_{\rho, f} \) depends on \( \rho \) and the coefficients of the polynomial \( f \in K[X, T] \). Denote by \( M \) the lattice in \( B_1^n \) generated by the rows of the matrix \( A \). The minimal vector of the lattice \( M \) is defined as in \( \S \! 1 \) (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 this 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 \( \bar{K}[X, T] \).

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

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

Conversely, suppose that \( |q| \leq \rho \). Consider the resultant

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

of the polynomials \( q \) and \( f \) with respect to \( X \). It is well known that there are polynomials \( p_1, p_2 \in K[x][X, T] \) such that \( R = p_1 q + p_2 f \). Since \( q \in M \), the linear polynomial \( \eta(x, X, T) \) mod \( T^D \) divides \( q \) mod \( T^D \) in the ring \( B_1/(T^D)[X] \). By (8), (9), and (11), also \( \eta(x, X, T) \) mod \( T^D \) divides \( f \) mod \( T^D \) in the ring \( B_1/(T^D)[X] \). Therefore, \( \eta(x, X, T) \) mod \( T^D \) divides \( R \) mod \( T^D \) in the last ring. But \( \deg X R \leq 0 \). Consequently, \( R \) mod \( T^D \) = 0, whence \( |R| \geq D \) or \( R = 0 \).

On the other hand, the conditions \( |f| \leq \rho \), \( |q| \leq \rho \) imply that \( |z| \leq \rho \) 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, \( |R| \leq (2m - 1)\rho = D - 1 \). Thus, \( R = 0 \). This means that \( \text{GCD}(f, q) \neq 1 \) in the ring \( K[x][X, T] \). Hence, \( f \) is a reducible polynomial in \( \bar{K}[X, T] \) and (i) is proved.

(ii) Recall that \( \Delta_{\gamma', \rho, r_0} \in K_u[x] \), \( \Delta_{\overline{\gamma'}, \rho, r_0} \in K_u[Z] \), and, in accordance with our definitions, \( \Delta_{\gamma', \rho, r_0}(x) = \Delta_{\gamma, \rho, r_0} \). By Lemma 2 (with the ring \( B_1 \) in place of \( B \)) and Lemma 5, \( \Delta_{\gamma', \rho, r_0} \neq 0 \) if and only if \( |q| > \rho \) for a minimal vector \( q \) of \( M \). Hence, by (i), \( \Delta_{\gamma', \rho, r_0} \neq \Delta_{\overline{\gamma'}, \rho, r_0}(x) \neq 0 \) if and only if the polynomial \( f \) is irreducible in the ring \( \bar{K}[X, T] \). But \( x \) is an arbitrary root of the polynomial \( f_0(Z) \). Consequently, \( f \) is irreducible in the ring \( \bar{K}[X, T] \) if and only if the polynomials \( \Delta_{\overline{\gamma'}, \rho, r_0} \) and \( f_0(Z) \) are relatively prime in the ring \( K_u[Z] \), i.e., if and only if their resultant \( R_{\rho, f} \) is not equal to zero. Assertion (ii) and the entire lemma are proved. \hfill \Box
Lemma 7. Let $f \in K[X,T]$ be a polynomial satisfying all the conditions formulated at the beginning of this section. Then the following assertions hold true.

(i) We have

$$\deg Z \Delta_{A,\rho,r_0} \leq 2(m - 1)(4m\rho - 2\rho - 1) \left(4m^3\rho + 2m^2\rho + 2m^2 - 4m\rho + 3m + \rho - 1\right).$$

(ii) Under the conditions of assertion (ii) in Lemma 3,

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

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

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

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

Proof. There is no loss of generality in assuming that the conditions of assertion (ii) of Lemma 3 are fulfilled. Using Lemma 3 and (11), we get

$$\deg Z \eta \leq (2D - 3)(2m - 2), \quad \deg_t \eta \leq (3D - 4)s$$

Let $C_{A,\rho} = (\overline{c}_{i,j})_{i,j}$ be the matrix corresponding to $\overline{A}$. By (12) and (19), we also have

$$\deg Z \overline{c}_{i,j} \leq (2D - 3)(2m - 2)$$

and $\deg_t \overline{c}_{i,j} \leq (3D - 4)s$ for all $i, j$. Hence, $\deg Z \Delta_{A,\rho,r_0} \leq r_0(2D - 3)(2m - 2)$ and $\deg_t \Delta_{A,\rho} \leq r_0(3D - 4)s$ (it can be checked directly that $r_0$ does not exceed the number $((2r + 2)D - \rho)m$ of the rows of $C_{A,\rho}$, but we even do not use this). This implies (i) and (16).

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

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

This implies (17).

The right-hand side of (17) is a monotone increasing function of $m$ and $\rho$ for $m \geq 2$, $\rho \geq 1$. 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 those of assertion (ii) in Lemma 3. Suppose that the polynomial $f \in K[t,X,T]$ is irreducible in the ring $K(t)[X,T]$. Then there are at most

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

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 $\deg_t \Delta_f \leq (2m - 1)s$ values $t^* \in \overline{K}$ of $t$ such that $\Delta f|_{t=t^*} = 0$. In what follows we assume that $\deg_X f_0 = \deg_X f(t^*,X,0)$ and $f(t^*,X,0)$ is separable. The resultant $R_{\rho,f}$ belongs to $K[t]$ and, by our definitions, $R_{\rho,f}(t^*) = R_{\rho,f}(t^*,X,T)$. Now (20) follows from Lemma 6 (ii) and (17).
§3. Irreducibility criterion: The general case

Let $K$ be an arbitrary field, and let $f \in K[X_1, \ldots, X_n]$, $n \geq 2$, be a polynomial such that $\deg X_1, \ldots, X_n f = d \geq 2$. These conditions will be assumed throughout this section.

Let $v = \{v_i\}_{2 \leq i \leq n}$ and $w = \{w_{i,j}\}_{1 \leq i \leq n, 0 \leq j \leq n}$ be two families of transcendental elements over $K$ such that the field $K_{w,v,u}$ generated over $K$ by all the elements of $w, v, u$ has the maximal possible transcendence degree $n - 1 + n(n + 1) + \nu_0(\nu_1 + \nu_2)$; see §1 (the integers $\nu_i$, $0 \leq i \leq 2$, will be specified in the definition of $A_f$ below). We write $K_v = K(v_2, \ldots, v_n)$, $K_w = K(v_1, \ldots, v_n)$, and denote by $K_w$ (respectively, $K_{w,v}$) the extension of the field $K$ by all elements of the family $w$ (respectively, the families $w$ and $v$). Let $K[w]$ (respectively, $K[w, v]; K[w, v, u]$) be the ring of polynomials in all the transcendental elements of the family $w$ (respectively, the families $w, v; w, v, u$) with coefficients from $K$. A similar notation will be used with other constant fields in place of $K$ and other families of transcendental elements.

Set $f_v = f(X, v_2T, \ldots, v_nT) \in K_v[X, T]$.

**Lemma 8.** Assume that $\deg X_1 f = \deg X_1 f(X_1, 0, \ldots, 0) = d$ and that the polynomial $f(X_1, 0, \ldots, 0)$ has $d$ pairwise distinct roots in the field $K$. The following assertions are equivalent.

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

(ii) The polynomial $f_v$ is irreducible in the ring $K_v[X, T]$.

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

**Proof.** Obviously, (iii) implies (ii). Assume that $f_v$ is reducible in the ring $K_v[X, T]$ and a polynomial $h \in K_v[X, T]$ divides $f_v$, $\deg_X h < \deg_X f_v$. Then $h(X, 0)$ divides $f_v(X, 0)$. Multiplying $h$ by a nonzero constant from $K_v$, we may assume without loss of generality that $h(X, 0) \in \bar{K}[X]$. The uniqueness of a Hensel lifting shows that $h \in \bar{K}_v[[T]][X]$. Therefore, $h \in \bar{K}_v[[T]][X] \cap \bar{K}_v[X, T] = \bar{K}_v[X, T]$, where intersection is taken in $\bar{K}_v[[T]][X]$. Thus, $f_v$ is reducible in the ring $K_v[X, T]$. Hence, (ii) implies (iii).

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

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

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

$$f_w = f(W_1, W_2, \ldots, W_n) \in K[w][X_1, \ldots, X_n],$$

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

Notice that

$$\deg X_1 f_w = \deg X_1 f_{w,v} = \deg X f_{w,v} = \deg X_T f_{w,v} = \deg X_T f_w = d.$$  

**Lemma 9.** The following assertions are equivalent.

(i) The polynomial $f$ has no multiple factors in $\bar{K}[X_1, \ldots, X_n]$.

(ii) The polynomial $f_v(X_1, 0, \ldots, 0)$ has no multiple factors in $\bar{K}_w[X_1]$.

(iii) The polynomial $f_{w,v}(X, 0)$ has no multiple factors in $\bar{K}_{w,v}[X]$.

**Proof.** Assume that (i) is true. Then, by the Bézout theorem, a generic line intersects the hypersurface $Z(f)$ (of all the roots of $f$ in the affine space $\mathbb{A}^n(\bar{K})$) at $d$ points. Hence, the polynomial $f(w_{1,0} + w_{1,1}X_1, \ldots, w_{n,0} + w_{n,1}X_1)$ has $d$ pairwise distinct roots in $\bar{K}_w$. This implies the equivalence of (i) and (ii). The equivalence of (ii) and (iii) follows from the relation $f_{w,v}(X, 0) = f_w(X, 0, \ldots, 0)$. \[\square\]
We put
\[ A_f = \Delta_{f,v,w} R_{d,f,w,v} \in K[w,v,u], \]
see (5), (15); now \( \rho = d \) and the ground field is equal to \( K_{w,v} \) in place of \( K \). Also, here we modify the definition of the resultant \( R_{d,f,w,v} \) as follows. Suppose the matrix \( \tilde{A}_{w,v} \) and the element \( \Delta_{\tilde{A}_{w,v},d,r_0} \) correspond to the polynomial \( f_{w,v} \) like \( \tilde{A} \) and \( \Delta_{\tilde{A},\rho,r_0} \) correspond to \( f \) in \( \S 2 \). Set \( d' = \max f \deg Z \Delta_{\tilde{A}_{w,v},d,r_0} \), where the maximum is taken over all the polynomials \( f \) satisfying the conditions listed at the beginning of the of the section and such that \( \Delta_{f,v,w} \neq 0 \). We regard \( \Delta_{\tilde{A}_{w,v},d,r_0} \) as a polynomial of degree at most \( d' \) with respect to \( Z \) (some higher order coefficients of this polynomial may be equal to zero), construct the Sylvester matrix \( \text{Syl}(\Delta_{\tilde{A}_{w,v},d,r_0}, f_{w,v}(Z,0)) \) of size \( d' + d \) for these two polynomials with respect to \( Z \). Finally, we define the modified resultant \( R_{d,f,w,v} \) to be the determinant of this matrix. It is easy to check that \( R_{d,f,w,v} \neq 0 \) if and only if the resultant in the usual sense \( \text{Res}_Z(\Delta_{\tilde{A}_{w,v},d,r_0}, f_{w,v}(Z,0)) \) is nonzero. This modification is necessary to make the definition of \( A_f \) canonical, because we do not prove that \( \deg Z \Delta_{\tilde{A}_{w,v},d,r_0} \) depends only on \( n \) and \( d \) if \( f_{w,v} \) is separable.

**Lemma 10.** Suppose \( f \in K[X_1, \ldots, X_n] \), \( \deg X_1, \ldots, X_n f = d \geq 2, n \geq 2 \). Then the polynomial \( f \) is irreducible in the ring \( K[X_1, \ldots, X_n] \) if and only if \( A_f \neq 0 \).

**Proof.** Suppose that \( f \in K[X_1, \ldots, X_n] \) is irreducible. Then the polynomial \( f_{w,v}(X,0) \) has no multiple factors in \( K_{w,v}[X] \) by Lemma 9. Therefore, \( \Delta_{f,v,w} \neq 0 \). Next, the polynomial \( f \) is irreducible in the ring \( K_{w,v}[X_1, \ldots, X_n] \). Hence, also \( f_w \) is irreducible in this ring. By Lemma 8 with the ground field \( K_w \) in place of \( K \), the polynomial \( f_{w,v} \) is irreducible in the ring \( K_{w,v}[X, T] \). 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 \( \Delta_{f,v,w} \neq 0 \) and the polynomial \( f_{w,v}(X,0) \) has no multiple factors in \( K_{w,v}[X] \). 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 \( f_{w,v} \in K_{w,v}[X, T] \) is irreducible. By Lemma 8 with the ground field \( K_w \) in place of \( K \), the polynomial \( f_w \in K_{w}[X_1, \ldots, X_n] \) is irreducible. Therefore, the polynomial \( f \) is irreducible in the ring \( K[X_1, \ldots, X_n] \). \( \Box \)

Let \( I_{d,n} = \{(i_1, \ldots, i_n) \in \mathbb{Z}^n : i_1 + \cdots + i_n \leq d; i_j \geq 0 \forall j \} \) be a set of multiindices, and let \( J_{d,n} = I_{d,n} \setminus \{i_1 \cdots i_n \mid d \geq 2, n \geq 2 \}. \) Notice that for the number of elements we have \( \#I_{d,n} = \binom{n+d}{d} = N, \#J_{d,n} = \binom{n+d-1}{n-1} = N_1 \). Now, let \( \Phi \) (respectively, \( \Psi \)) be a generic polynomial (respectively, a generic homogeneous polynomial) of degree \( d \) in \( n \) variables for a given characteristic \( p \) of the ground field. This means that

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

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

We identify the set of all polynomials (respectively, the linear space of all homogeneous polynomials) of degree \( d \) in \( K[X_1, \ldots, X_n] \) with a Zariski open subset \( U_{d,n} \subset K^{N_1}(K) \) (respectively, with the affine space \( A^{N_1}(K) \)), where \( K^{N_1}(K) \) has the coordinate functions in the family \( \varphi \) (respectively, \( A^{N_1}(K) \) has the coordinate functions in the family \( \psi \)).

Recall that \( H[\varphi] \) and \( H[\psi] \) are the rings of polynomials with coefficients in \( H \) in all the variables from the families \( \varphi \) and \( \psi \) respectively. We have \( \Phi \in H[\varphi][X_1, \ldots, X_n], \Psi \in H[\psi][X_1, \ldots, X_n] \). Then \( A_{\Phi} \in H[\varphi, w, v, u], A_{\Psi} \in H[\psi, w, v, u] \). We can represent
these elements uniquely in the form

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

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

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

\[ f = \sum_{(i_1, \ldots, i_n) \in I} \lambda_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n} \]

be an arbitrary polynomial (respectively, a homogeneous polynomial) of degree \( d \) with all coefficients \( \lambda_{i_1, \ldots, i_n} \) lying 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, in accordance with our definitions for the case where \( I = I_{d,n} \), we have

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

(21)

we leave the checking of the details to the reader), i.e., \( A_f \) is obtained by substituting in \( A_\Phi \) 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 \( f \) and \( I = J_{d,n} \),

\[ A_f = A_\Psi \big|_{\psi = \lambda'} = A_\Psi \big|_{\psi_{i_1, \ldots, i_n} = \lambda_{i_1, \ldots, i_n} \forall (i_1, \ldots, i_n) \in J_{d,n}} \]

Also, we have \( A_\Psi \big|_{\psi_{i_1, \ldots, i_n} = 0} = 0 \) \( \forall (i_1, \ldots, i_n) \in J_{d,n} \).

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 of the family \( \varphi \) (respectively, \( \psi \)).

**Lemma 11.** (i) Let \( n \geq 2 \) and \( d \geq 2 \) be integers. Then the set \( \mathcal{W}_{d,n} \) of all reducible polynomials in \( \bar{K}[X_1, \ldots, X_n] \) 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 zeros in \( \bar{K}^N(\bar{K}) \) of the polynomials belonging to the family \( \{A_{\Phi,\mu}\}_{\mu \in M_\Phi} \).

Also, the set \( \mathcal{W}_{d,n} \) of all reducible polynomials in the affine space \( \bar{K}^{N_1}(\bar{K}) \) of homogeneous polynomials of degree \( d \) is identified with the Zariski closed subset \( \mathcal{Z}(\{A_{\Psi,\mu}\}_{\mu \in M_\Psi}) \) of \( \bar{K}^{N_1}(\bar{K}) \).

(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

\[ 56d^7 - 32d^6 - 54d^5 + 96d^4 - 72d^3 + 15d^2 + 9d - 3 < 56d^7. \]

**Proof.** (i) This follows immediately from our definitions, Lemma 10, and (21), (22).

(ii) It suffices to prove the claims related to \( \deg_\varphi A_\Phi \) and \( \deg_\psi A_\Psi \). We treat the case of \( \deg_\varphi A_\Phi \). Let \( t \) be a new variable. Without loss of generality we may assume that the ground field \( K \) includes \( H[t, \varphi] \). Consider the polynomial \( \Phi = t\Phi \in H[t, \varphi] \). Then the definitions imply immediately that \( \deg_t A_\Phi = \deg_\varphi A_\Phi \) and \( \deg_t A_{\Psi,\mu} = \deg_t (\Delta_{\Phi_{w,v}, R_{d,\Phi_{w,v}}}) \) (now, in the definition of \( R_{d,\Phi_{w,v}} \) 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 \( \Phi_{w,v} \) over the ground field \( K_{w,v,u}(t) \). Denote by \( c(s, m, \rho) \) the right-hand side of (20). Now \( s = 1 \) and \( m = \rho = d \). Hence,

\[ \deg_t (\Delta_{\Phi_{w,v}, R_{d,\Phi_{w,v}}}) \leq c(1, d, d) \]

This implies (23) for \( \deg_\varphi A_\Phi \). The proof of the estimate for \( \deg_\psi A_\Psi \) is similar. \( \square \)
Corollary 2. Let \( f \in K[t, X_1, \ldots, X_n] \), \( n \geq 2 \), be a polynomial irreducible in the ring \( \overline{K}(t)[X_1, \ldots, X_n] \) with \( \deg_t f \leq d \), \( \deg_{X_1,\ldots,X_n} f = d \) for an integer \( d \geq 2 \). Then there are at most
\[
\deg_t A_f \leq 56d^8 - 32d^7 - 54d^6 + 96d^5 - 72d^4 + 15d^3 + 9d^2 - 3d < 56d^8
\]
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 \( \Delta f\big|_{t=t^*} = 0 \). Notice also that \( \Delta f\big|_{t=t^*} = 0 \) if and only if
\[
\deg_{X_1} f(t^*, X_1, \ldots, X_n) < \deg_{X_1} f \quad \text{or} \quad \Delta_f(t^*,X_1,\ldots,X_n) = 0.
\]

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), \( \deg_t A_f \leq d \deg_v A_f \). Now the required assertion follows from Lemma 10 and (23) immediately. \( \square \)

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

Our aim in this section is to prepare for the proof of Theorem 2; see the Introduction. Let \( K \) be an arbitrary field, and let \( f \in K[X_1, \ldots, X_{n+1}] \), \( n \geq 2 \), 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 \( X_1 \) is nonzero:
\[
\Delta = \text{Res}_{X_1} \left( f, \frac{\partial f}{\partial X_1} \right) \neq 0.
\]
All these conditions are assumed 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 (the details are left to the reader). \( \square \)

The next lemma follows from Lemma 4 in \( [7] \). For completeness, we give a simple direct independent proof of this fact (in a similar way one can prove Lemma 4 in \( [7] \) 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 \( \theta \notin \overline{K}(t) \).

Moreover, if (i) and (ii) are satisfied, then the element \( \theta \) 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 this ring and such that some coefficient of \( f_1 \) is equal to 1. 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 \( \overline{K}(t) \). Using interpolation by the elements \( x_2, \ldots, x_n \), we conclude 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 \( \text{Gal}(E/\overline{K}(t)) = G \) 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 absolute irreducible factors has the form $f = \lambda_0 f_1 \cdots f_\nu$, $\nu > 1$, where $f_1, \ldots, f_\nu \in E[X_1, \ldots, X_n]$ are pairwise distinct polynomials conjugate to $f_1$ over the field $\overline{K}(t)$, and $0 \neq \lambda_0 \in \overline{K}(t)$.

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

On the other hand, we show (of course, it is known again) that every $E$-vector subspace $V \subset E \otimes_{\overline{K}(t)} K$ is invariant under the action of $E$. Therefore, the degree of the minimal polynomial of the element $\epsilon_i$, $i \in I_2$ is smaller than $\deg_{X_1} f$. Consequently, condition (ii) 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 $\Delta$.

**Proof.** By Lemma 2, there is a finite separable algebraic extension of fields $E_1 \supset \overline{K}(t)$ such that $[E_1 : \overline{K}(t)] > 1$ and $E_1$ is contained in the field $K$. The extension $E_1 \supset \overline{K}(t)$ corresponds to the morphism $C \to \mathbb{P}^1(\overline{K})$ of 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 $v_1$, that 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 determined by a uniformizing element

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

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

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
The elements $X_2, \ldots, X_{n-1}, \mu_3 X_n + \mu_4 X_{n+1}$ are algebraically independent over the field $E_1$. Therefore (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 $v_2(X_i) = 0$, $1 \leq i \leq n - 1$, $v_2(\mu_3 X_n + \mu_4 X_{n+1}) = 0$. Hence, (26) implies $v_2(\mu_1 X_n + \mu_2 X_{n+1}) = 1$. Observe that $E_2 \supset K(X_2, \ldots, X_{n+1})$.

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

Corollary 3. Let $f \in K[X_1, \ldots, X_{n+1}]$, $n \geq 2$, be an irreducible polynomial such that $\deg_{X_1} f \geq 1$, $\deg_{X_1, \ldots, X_{n+1}} f \leq d$ for an integer $d \geq 1$, and (24) is satisfied. Suppose that $f$ is irreducible in the ring $K[X_1, \ldots, X_{n+1}]$, the polynomial $f$ does not belong to the ideal $(X_1, X_{n+1})$, and for all $\mu_1, \mu_2 \in K$ 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 $\Delta$. Then for all $t^* \in K$ except at most

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

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

Proof. This follows immediately from Lemmas 12–14 and Corollary 2 in §3. □

References


ST. PETERSBURG BRANCH, STEKLOV MATHEMATICAL INSTITUTE, RUSSIAN ACADEMY OF SCIENCES, FONTANKA 27, SAINT PETERSBURG 191023, RUSSIA

E-mail address: alch@pdmi.ras.ru

Received 1/NOV/2011

Translated by THE AUTHOR