COROLLARY 2. If $f \in \mathbb{Q}[x_1, \ldots, x_n]$ and $f(x) > 0$ for any $x \in \mathbb{R}^n$, then $f(x') > 1/\gamma$.

Proof. The function f achieves local minima and, in particular, a global minimum at its critical points. If $K \subset \mathbb{R}^n$ is the set of critical points of f, then the set $V = (K \times f(K)) \subset \mathbb{R}^{n+1}$ is an algebraic variety, defined by the system $\partial f/\partial x_1 = \ldots = \partial f/\partial x_n = 0$, $f = x_{n+1}$. The set of points defined by the system $\partial f/\partial x_1 = \ldots = \partial f/\partial x_n = 0, f = \min_{x \in \mathbb{R}^n} f(x)$ is an algebraic subvariety of the variety V, and by Corollary 1, contains a point $x' = (x'_1, \ldots, x'_{n+1})$ such that $|x'_{n+1}| > 1/\gamma$.

LITERATURE CITED

1. D. Yu. Grigor'ev, "Decomposition of polynomials over a finite field and solution of systems of algebraic equations," J. Sov. Math., 34, No. 4 (1986).
2. J. Thorpe, First Chapters of Differential Geometry [Russian translation], Moscow (1982).
3. M. Hirsch, Differential Topology [Russian translation], Moscow (1979).
4. W. Hodge and D. Pedoe, Methods of Algebraic Geometry [Russian translation], Vol. 2, Moscow (1954).
5. D. Lazard, "Résolutions des systèmes d'équations algébriques," Theor. Comput. Sci., 15, 77-110 (1981).
6. J. Milnor, "On the Betti numbers of real varieties," Proc. Am. Math. Soc., 15, No. 2, 275-280 (1964).
7. H. R. Wûthrich, "Ein Entsceidungsverfahren für die Theorie der reell-abgeschlossenen Körper," Lect. Notes Comput. Sci., 43, 138-162 (1976).

FACTORIZATION OF POLYNOMIALS OVER A FINITE FIELD AND THE SOLUTION OF SYSTEMS OF ALGEBRAIC EQUATIONS

D. Yu. Grigor'ev

UDC 518.5+512.46

An algorithm is constructed for factoring polynomials in several variables over a finite field $\mathbb{F}_q \varkappa$, which works in polynomial time in the size of the polynomial and q. Previously this result was known in the case of one variable. An algorithm is given for the solution (over the algebraic closure $\bar{F}$ of the field F) of systems of algebraic equations $f_0 = \cdots = f_k = 0$, where $f_0, \ldots, f_k \in F[X_0, \ldots, X_n]$ with working time of order $L^{n^2(n+\ell)}(q+1)$, where L is the size of a representative of the original system, ℓ is the degree of transcendence of the field F over the prime subfield, q = char(F). Previously the estimate $L^{2^n}(q+1)$ was known for ℓ = 0.

INTRODUCTION

In the present paper we give algorithms for solving two problems of computational commutative algebra, the estimate of whose complexity is better in order of growth than those known previously, In Chapter I an algorithm is described for factoring polynomials in several variables into irreducible factors over a finite field, which works in polynomial time.

Translated from Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR, Vol. 137, pp. 20-79, 1984.

0090-4104/86/3404-1762$12.50 © 1986 Plenum Publishing Corporation

In Chapter II an algorithm is constructed for solving systems of algebraic equations of arbitrary degree, working in subexponential time.

The problem of constructing an algorithm for factoring polynomials into factors goes back all the way to Gauss. Up to now it has attracted the attention of many mathematicians. The Kronecker algorithm is widely known [1]. Unfortunately, Kronecker's algorithm, as well as all other algorithms known until most recently, required exponential time (in the length of the description of the original polynomial) in general. The first step was made by D. K. Faddeev and independently A. I. Skopin at the end of the fifties for factoring polynomials in one variable over a finite field $F=\mathbb{F}_q$; in the literature this algorithm is known as Berlekamp's algorithm [5], which he published in the sixties. After this, in the course of nearly 20 years there was no essential progress. Only in 1982, Lenstra et al. [20] constructed a polynomial algorithm for factoring polynomials in one variable over the field of rational numbers $F=\mathbb{Q}$, which reduced the factoring to the search for a vector of sufficiently small norm in a given lattice over the ring of integers $\mathbb{Z}$, with subsequent application of Berlekamp's algorithm and Hensel's lemma. Independently, in [15], the reduction of the factoring of polynomials in several variables over $F=\mathbb{Q}$ to the factoring of polynomials in two variables was obtained, which was polynomial for a fixed number of variables, and, in addition, in [16] a polynomial reduction of the factoring of polynomials in two variables over $F=\mathbb{Q}$ to the factoring of polynomials in one variable was found. Finally, an algorithm of polynomial complexity for factoring polynomials in several variables over a finite field was first given by the author in [8], and an account of it constitutes Chapter I of the present paper (cf. Theorem 1.4 of Sec. 3). Afterwards, Chistov constructed an algorithm of polynomial complexity for factoring polynomials in several variables over global fields [8] and extended this result to fields which are finitely generated over their prime subfields [4].

In Chapter I we consider a polynomial $f\in\mathbb{F}_q\varkappa[X_1,\ldots,X_n]$. Here we assume that $\deg_{X_i}(f)<r, 1\leqslant i\leqslant n$. Then f can be represented by the vector of length r^n of its coefficients from the finite field $\mathbb{F}_q\varkappa$. The bit length of the description of elements of the field $\mathbb{F}_q\varkappa$ does not exceed $\varkappa\log_2 q$. Hence, by the size of the polynomial f in Chapter I we mean the quantity $r^n\varkappa\log_2 q$. In Chapter I an algorithm is described for factoring f into factors which are irreducible over $\mathbb{F}_q\varkappa$ in polynomial time in the size of f.

Section 1 of Chapter I is preparatory for Sec. 2, although it has independent interest. A polynomial algorithm is given for finding a minimal vector in a lattice over the ring $\mathbb{F}_q\varkappa[t]$.

In Sec. 2 a polynomial algorithm is constructed for factoring polynomials from $\mathbb{F}_q\varkappa[X_1,X]$.

In Sec. 3 the proof of the basic result of Chapter I is completed with the help of reduction to the case of two variables (n = 2).

The problem of solving systems of algebraic equations also has a long history. The fundamental possibility of solving systems over an algebraically closed field was already established in the 19th century on the basis of elimination theory (cf., e.g., [1]). Many papers were devoted to this problem, especially in the last two decades in connection with the development of programming and the theory of complexity of computations. In a number of papers (cf., e.g., [14]) an upper bound for the working time was found in which the quantity d^{2^n} appeared, where n is the number of variables, and (d − 1) is the maximal degree of the equations. Despite the immense progress in algebraic geometry, up to now there has been no success in overcoming the considerable difficulties in the path toward lowering the estimate mentioned.

The first essentially better estimate was established by Lazard in [18] in the case when the system has a finite number of solutions in projective space (i.e., the variety of all roots is zero-dimensional). On the other hand, one can consider the algorithm from [8] as an algorithm for solving systems of algebraic equations in the case when the variety of roots of the system is a hypersurface, i.e., has codimension one. This algorithm is used repeatedly in the present paper. One can even consider the present paper as continuation of [8]. We note that the algorithm from [18] is also based on the factoring of polynomials.

In Chapter II the author's algorithm for solving systems of algebraic equations with an estimate of complexity which is polynomial in d^{n^3} is described (Theorem 2.4; cf. also Secs. 2-4 of [9, 10]). Further, Chistov constructed an algorithm with an essentially better estimate which is polynomial in d^{n^2} (cf. Secs. 5-7 of [10]; also [4]).

Let the ground field $F = H(T_1,\dots,T_\ell)[\eta]$, where either $H=\mathbb{Q}$ or $H=\mathbb{F}_{q^{\varkappa}}$, $q = char(H)$ the elements $T_1,\dots,T_\ell$ being algebraically independent over H; the element η is separable and algebraic over $H(T_1,\dots,T_\ell)$, and by $\varphi = \sum_{0\le i<\deg_Z(\varphi)} (\varphi_i^{(1)}/\varphi^{(2)})Z^i \in H(T_1,\dots,T_\ell)[Z]$ we denote its minimal polynomial over $H(T_1,\dots,T_\ell)$ with leading coefficient $\ell c_Z(\varphi) = 1$, where $\varphi_i^{(1)}, \varphi^{(2)} \in H[T_1,\dots,T_\ell]$ and $\deg(\varphi^{(2)})$ is the smallest possible. Any element $f \in F[X_0,\dots,X_n]$ can be represented uniquely in the form

$$f = \sum_{0\le i<\deg_Z(\varphi); i_0,\dots,i_n} (a_{i,i_0,\dots,i_n}/b)\eta^i X_0^{i_0}\cdots X_n^{i_n},$$

where $a_{i,i_0,\dots,i_n}$, $b \in H[T_1,\dots,T_\ell]$ and deg(b) is as small as possible, the polynomials $a_{i,i_0,\dots,i_n}, b$ are uniquely defined up to a factor from H*. We let $\deg_{T_1,\dots,T_\ell}(f) =$

$$\max_{i,i_0,\dots,i_n}\{\deg_{T_1,\dots,T_\ell}(a_{i,i_0,\dots,i_n}), \deg_{T_1,\dots,T_\ell}(b)\}$$

By the length of description ℓ(h) if $h \in \mathbb{Q}$ we shall mean its bit length, and $h \in \mathbb{F}_{q^{\varkappa}}$ the quantity $\varkappa \log_2 q$. By ℓ(f) we denote the maximum length of description of coefficients from H of the monomials $T_1,\dots,T_\ell$ in the polynomials $a_{i,i_0,\dots,i_n}, b$.

Suppose given an input system $f_0 = \cdots = f_{k-1} = 0$ of algebraic equations (we assume, without loss of generality, that $f_0,\dots,f_{k-1}$ are linearly independent). In fact, in Chapter II we give an algorithm which decomposes an arbitrary projective algebraic variety into irreducible components, so we can assume that $f_0,\dots,f_{k-1} \in F[X_0,\dots,X_n]$ are homogeneous polynomials with respect to $X_0,\dots,X_n$. Throughout Chapter II we assume that

$$\deg_{T_1,\dots,T_\ell,Z}(\varphi) < d_1, \deg_{X_0,\dots,X_n}(f_i) < d, \deg_{T_1,\dots,T_\ell}(f_i) < d_2, \ell(\varphi) \le M_1, \ell(f_i) \le M_2.$$

In Chapter II by the size of the polynomial f_i we mean the quantity $\binom{d+n}{n} d_1 d_2^l l(f_i)$.

The projective variety $\{f_0 = \cdots = f_{k-1} = 0\} \subset \mathbb{P}^n(\bar{F})$ of common roots of the system $f_0 = \cdots = f_{k-1} = 0$ decomposes into components $\{f_0 = \cdots = f_{k-1}\} = \bigcup_\alpha W_\alpha \subset \mathbb{P}^n(\bar{F})$ [7], where a component is defined and irreducible over a maximal purely inseparable [6] extension $F^{q^{-\infty}}$ of the field F [6]. The algorithm given in Chapter II finds all the components W_α. Any component W_α will be representable in the following two ways: by means of its generic point [3], and, on the other hand, by some system of algebraic equations such that the variety of its roots coincides with the component considered; in such a case we shall say that the system defines the variety.

Section 1 of Chapter II has an auxiliary character; its results are used later in Secs. 3 and 4 for the construction of a transcendence basis in general for fields of rational functions over the ground field F for all components of the variety.

In Sec. 2 we recount a certain modification of Lazard's algorithm [18] for finding all roots of a system of algebraic equations if there are finitely many of them in projective space (the original method of Lazard works in appropriate time only for a finite ground field F). The estimate of the working time (cf. Theorem 2.3) is polynomial in M_1, M_2, $(d^n d_1 d_2)^{l+1}$

In Sec. 3 we give a method for finding generic points of the components W_α. Here we also introduce the construction of the tree of components which is important for our approach.

In Sec. 4 we describe the construction of a system of equations defining each of the components W_α, which completes the proof of the basic result of Chapter II (Theorem 2.4).

Chapter I

FACTORIZATION OF POLYNOMIALS OVER A FINITE FIELD

1. Finding a Minimal Vector in a Lattice Over $\mathbb{F}_q[t]$

We let $F = \mathbb{F}_q(t)$, $A = \mathbb{F}_q[t] \subset F$, where t is algebraically independent over $\mathbb{F}_q$. Considering A as a polynomial ring, we define the order $|a|$ for $a \in A$ as follows: $|a| = \deg_t a$, i.e., the degree of the polynomial a with respect to the variable t. The order of a vector $(a_1, \ldots, a_k) \in A^k$ is defined as follows: $|(a_1, \ldots, a_k)| = \max_{1 \le i \le k} |a_i|$.

In the present section we consider lattices over the ring A (i.e., finitely generated free A-modules). We assume that the lattice is defined by some system of generators (not necessarily free) and each generator is a k-dimensional vector in A^k.

A minimal vector of a lattice is defined as a nonzero vector of minimal order in the lattice. We also assume that the elements of A can be described as polynomials over $\mathbb{F}_q$ and the elements of $\mathbb{F}_q$ as integers from 0 to q − 1. Hence the length of description of a vector (and consequently of the lattice) is polynomial with respect to log q, the order of the vector, and k (respectively, the maximum of the orders of generators of the lattice and the number of all the coefficients).

<u>THEOREM 1.1</u>. A minimal vector of a lattice can be found in polynomial time.

We note that the theorem is an analog for nonzero characteristic of the basic result (1.26) of Sec. 1 of [20] and, moreover, it is stronger since, in the case of characteristic zero, in general one constructs a nonminimal vector.

<u>Proof</u>. We write the generators of the lattice as the rows of a matrix over $\mathbb{F}_q[t]$, which we denote by M.

<u>LEMMA 1.1</u>. The matrix M can be reduced by a permutation of the columns followed by elementary row transformations to trapezoidal form in polynomial time:

$$YMS = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1k} \\ & b_{22} & & \vdots \\ 0 & & \ddots b_{\mu\mu} \dots & b_{\mu k} \\ & 0 & & \end{pmatrix} = B \quad ,$$

where $0 \neq \det Y \in \mathbb{F}_q$; the product $\prod_{1 \leq i \leq \mu} b_{ii} \neq 0$, S is some permutation matrix, i.e., is obtained from the identity by a permutation of the rows.

Now, assuming that Lemma 1.1 is proved, we complete the proof of the theorem. We find a vector $u = (u_1, \dots)$ over A such that uB is a minimal vector in the lattice corresponding to the matrix B. Then uBS^{-1} is a minimal vector of the original lattice.

We now proceed to find the vector u. We let $\rho = \max_{ij} |b_{ij}|$. Obviously, $|uB| \leq |(b_{11}, \dots, b_{1k})| \leq \rho$. Hence $|u_1 b_{11}| \leq \rho$ and, consequently, $|u_1| \leq \rho$ Then $|u_1 b_{12} + u_2 b_{22}| \leq \rho$ and $|u_1 b_{12}| \leq 2\rho$, so $|u_2| \leq 2\rho$. Arguing in the same way, we get a sequence $|u_3| \leq 3\rho, \dots, |u_\mu| \leq \mu\rho$. Hence the question of whether it is true that $|uB| = \rho'$, for any given $\rho' \leq \rho$ reduces to the solution of a linear system over $\mathbb{F}_q$, in which the unknowns are the coefficients of the polynomials $u_1, \dots, u_\mu$. The algorithm gives, successively, $\rho' = 0, 1, \dots$ up to the value of ρ' for which the system mentioned is solvable (such a $\rho' \leq \rho$).

<u>Proof of Lemma 1.1</u>. In what follows we shall use the fact that the rank of a matrix over * can be calculated in polynomial time (cf. also [12, 21]). Since the order of an arbitrary minor of the matrix is no greater than the sum of the orders of the elements of this matrix (we denote this sum by s), substituting for t any s + 1 pairwise distinct elements of the finite extension $\mathbb{F}_q\varkappa \supset \mathbb{F}_q$, where $q^\varkappa > s$, we get that the rank of the original matrix is equal to the maximum of the ranks of the s + 1 matrices constructed. The ranks of the latter matrices are easily calculated by reducing these matrices with coefficients from $\mathbb{F}_q\varkappa$ to trapezoidal form.

Based on what was just said, we choose a maximal linearly independent set of columns of the matrix M and a matrix S which moves them to the beginning. Then $MS = (M_1, M_2)$, where M_1 consists of the columns mentioned above. We arbitrarily complete the matrix M_1 to a nonsingular mtrix $\mathfrak{D} = (M_1, M_3)$. This can be done, for example, by adding a sequence of columns with unique nonzero component equal to one, keeping track of the rank of the matrices obtained.

*Something is missing in the Russian original – Publisher.

Now we reduce the matrix D to upper-triangular form in polynomial time by row transformations, i.e., we find a matrix Y with coefficients from A, such that

$$Y\mathcal{D} = \begin{pmatrix} c_{11} & \cdots & c_{1\omega} \\ & c_{22} \ddots & \vdots \\ 0 & & c_{\omega\omega} \end{pmatrix} = C \quad \text{and} \quad 0 \neq \det Y \in \mathbb{F}_q .$$

Since the ring A is Euclidean, such a matrix exists. It is easy to verify that Y is the matrix which had to be constructed in Lemma 1.1.

We rewrite the last equation in the form $Y = C\mathcal{D}^{-1}$ and we write $\mathcal{D}^{-1} = (g_{ij} / \det \mathcal{D})$, where $g_{ij} \in A \, (1 \leq i, j \leq \omega)$. Since $\prod_{1 \leq i \leq \omega} c_{ii} = \det \mathcal{D} \det(Y)$ one has $|c_{ii}| \leq |\det \mathcal{D}| \; (1 \leq i \leq \omega)$ and by some appropriate row transformation we can arrange that $|c_{ij}| \leq |c_{jj}| \; (1 \leq i \leq j \leq \omega)$. Hence, without loss of generality, we shall assume that, for the matrix C, which must be constructed, one has $|c_{ij}| \leq |\det \mathcal{D}| \; (1 \leq i \leq j \leq \omega)$.

We fix some $1 \leq m \leq \omega$ and we consider the condition that all components of the vector $(0, \ldots, 0, c'_{m,m}, \ldots, c'_{m,\omega}) \times \mathcal{D}^{-1}$ for some polynomials $c'_{m,m}, \ldots, c'_{m,\omega}$ are also polynomials (i.e., belong to A), and in addition the order $\rho_m = |c'_{m,m}|$ is the smallest possible and the leading coefficients of the polynomials $c'_{m,m}$ are equal to 1. The condition just formulated is equivalent to the following system of equations

$$\sum_{m \leq i \leq \omega} c'_{m,i} \, g_{ij} \qquad (\det \mathcal{D}) h_j \; (1 \leq j \leq \omega), \text{ where } h_j \in A \; (1 \leq j \leq \omega)$$

The last system in its own right is equivalent with a system of linear equations over $\mathbb{F}_q$, in which the unknowns are the coefficients of the polynomials $c'_{m,i}$, h_j. The determinant det D and the elements of the matrix $\mathcal{D}^{-1}$ can be calculated with the help of interpolation, substituting for t an appropriate number of elements of some finite extension $\mathbb{F}_{q^{\varkappa}}$ (analogously to the construction of the calculation of the rank given above, cf. also [12, 21]).

From the linear system considered we find all $c'_{m,i} \; (m \leq i \leq \omega)$, setting $\rho_m = 0, 1, \ldots$ successively. Doing this for all $1 \leq m \leq \omega$, we get a matrix

$$Y' = \begin{pmatrix} c'_{11} & c'_{12} & \cdots & c'_{1\omega} \\ & \ddots & & \vdots \\ 0 & & & c'_{\omega\omega} \end{pmatrix} \mathcal{D}^{-1} .$$

We show that Y' is the matrix required in Lemma 1.1. First, the elements of Y' are polynomials (i.e., belong to A). Further, according to the condition on ρ_m formulated above, we have $0 = |\det Y| = \sum_{1 \leq m \leq \omega} |c_{mm}| - |\det \mathcal{D}| \geq \sum_{1 \leq m \leq \omega} \rho_m - |\det \mathcal{D}| = |\det Y'| \geq 0$. From this it follows that Y'is the matrix sought, which concludes the proof of Lemma 1.1 and of Theorem 1.1.

The following proposition is nowhere used in the present paper, but nevertheless it closely touches on the questions considered in this section and has some independent interest.

Proposition 1.1 [8]. Let K be a field and A = K[t]. Let M = (m_{ij}) be some nonsingular $n \times n$ matrix (i.e., det M ≠ 0) with coefficients from A. Then for some suitable nonzero vector $u \in A^n$ one has $|uM| \leqslant (1/n)|\det M|$ (to the end of this section, $|(u_1, \ldots, u_n)| = \max_{1 \leqslant i \leqslant n} \deg_t (u_i)$).

We note that this inequality is sharp.

The proof of the proposition from [8] is effective and is based on the following lemma.

LEMMA 1.2. If the field K is infinite, then for some matrices $U' \in GL_n(A)$, $V' \in GL_n(K)$ the matrix

$$M' = U'MV' = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ & \ddots & \vdots \\ 0 & & \alpha_{nn} \end{pmatrix}$$

is upper triangular and, moreover, $\alpha_{ss} = g.c.d. \{\alpha_{ij} : s \leqslant i \leqslant j \leqslant n\}$ for any $1 \leqslant s \leqslant n$, in particular $\alpha_{11} = g.c.d. \{ m_{ij} : 1 \leqslant i, j \leqslant n \}$.

2. Factorization of Polynomials in One Variable into Factors Over the Ring

As in Sec. 1, we assume that $F = \mathbb{F}_q(t)$, $A = \mathbb{F}_q[t]$ and the order $|a|$ for $a \in A$ has the same meaning. Let $\sum_{0 \leqslant i \leqslant r} a_i X^i = f \in A[X]$. Our goal is to decompose f into irreducible factors over the field F (or over A, which is equivalent by Gauss' lemma [1]). We defined the order $|f| = \max_{0 \leqslant i < r} |a_i|$.

First we reduce everything to the case when the polynomial f is separable. If this is not so, then either $f'_X = 0$ or $0 < \deg_X g.c.d.(f, f'_X) < \deg_X f$. In the first case we let f = $\sum_{i,j} a_{qi}^{(j)} t^j X^i$. We set $f_1 = \sum_{i,j} a_{qi}^{(j)} t^j X^i$. Since $\deg_X f_1 < \deg_X f$ (if $\deg_X f = 0$, everything is trivial), we can assume that we have already decomposed f$_1$ over F. Let $f_1 = \prod_s \varphi_s$, where $\varphi_s \in A[X]$ and φ_s is irreducible over F for any s. Then $f = \prod_s \varphi_s(X^q)$. We fix s at some time and we let $\varphi_s(X) = \sum_{i,j} b_i^{(j)} t^j X^i$. Then either $b_i^{(j)} = 0$ for any i, j such that $q \nmid j$, and in this case $\varphi_s(X^q) = (\sum_{i,j} b_i^{(jq)} t^j X^i)^q$, or if not, it is easy to show that $\varphi_s(X^q)$ is irreducible over F. Finally, we get that either f is irreducible or we find some proper divisor of f and we continue to apply the procedure described to the factors of the polynomial f. If $0 < \deg_X g.c.d.(f, f'_X) < \deg_X f$, then we also get some proper divisor of f. Thus, in what follows, we consider only separable polynomials f.

Let $(p) \subset A$ be a maximal ideal of the ring A, generated by some irreducible polynomial $p \in A$. The only requirement on the choice of p is that p be relatively prime with the discriminant $R = \mathrm{Res}_X(f, f'_X) \in A$ in the ring A. Further, considering the polynomial mod (p), we write it, choosing in A[X] a representative for which the order of all coefficients is less than $|p|$.

We show that p can be found in polynomial time. For each s and for any factor φ_j of the separable polynomial $t^{q^s} - t = \prod_i \varphi_i$, which is irreducible over $\mathbb{F}_q$, one has the relation $\deg \varphi_j \mid s$, since the splitting field of this polynomial is $\mathbb{F}_{q^s}$ and, consequently, $\mathbb{F}_q \subset \mathbb{F}_q[t]/(\varphi_j) \subset \mathbb{F}_{q^s}$ and the degree of the field extension $[\mathbb{F}_q[t]/(\varphi_j) : \mathbb{F}_q] = \deg \varphi_j$ (cf. also [1]). Let $q^s \geqslant 2r|f| > |R|$ and $q^{s-1} < 2r|f|$ for some s. Then there exists an irreducible polynomial

$p\in A$, such that $p\nmid R$ and $|p|\leq s$. If not, $(t^{q^s}-t)\mid R$, which leads to a contradiction. Such a polynomial p can be found, looking at all elements of A of order not greater than s and verifying whether it is true that $p\nmid R$ and p is irreducible (the latter can be verified with the help of Berlekamp's algorithm [5]; cf. also below). The upper bound on s shows that p can be found in polynomial time.

Below we need an algorithm (which is a slight modification of the Berlekamp algorithm just mentioned [5]) for factoring a polynomial $g\in\mathbb{F}_{q^m}[t]$ over $K=\mathbb{F}_{q^m}$ in time which is polynomial in q, m, s = deg g (direct application of Berlekamp's algorithm gives time which is polynomial in q^m, s).

We consider the ring $\mathbb{D}=K[t]/(g)$. We let $\psi_q(\alpha)=\alpha^q$ be the Frobenius automorphism $(\psi_q:\mathbb{D}\rightarrow\mathbb{D})$. Arguing as above at the beginning of this section, without loss of generality we can assume that g is separable.

Thus, let $g=g_1\cdots g_\varkappa$ be the factorization required. Then $\mathbb{D}=\bigoplus_{1\leq i\leq\varkappa}K[t]/(g_i)=\bigoplus_{1\leq i\leq\varkappa}\mathbb{F}_{q^{s_i}}$ (here and below, $\oplus$ denotes the direct sum of rings) by the residue theorem [6], since g_i are relatively prime in pairs in view of the separability of g (s_i = deg g_i). We consider the subring $E=\{\alpha\in\mathbb{D}:\psi_q(\alpha)=\alpha\}\subset\mathbb{D}$. It is easy to verify that the construction of a basis of E over $\mathbb{F}_q$ reduces to the solution of a suitable linear system over $\mathbb{F}_q$ (it is necessary to describe the decomposition of α in the basis D over $\mathbb{F}_q$ with parametric coefficients, then the direct action of ψ_q and the equation $\psi_q(\alpha)=\alpha$ provide a linear system with respect to the parametric coefficients).

It is well known that the subfield $\{\alpha\in\mathbb{F}_{q^m}:\psi_q(\alpha)=\alpha\}$ is isomorphic with $\mathbb{F}_q$ [1]. Consequently, $E=\bigoplus_{1\leq i\leq\varkappa}\mathbb{F}_q$, where the i-th copy of $\mathbb{F}_q$ is contained in $\mathbb{F}_{q^{s_i}}$. We find this decomposition of E explicitly. We take any two elements $\alpha,\beta\in E$ which are linearly independent over $\mathbb{F}_q$. Considering the elements $\alpha+\gamma\beta$ consecutively for all $\gamma\in\mathbb{F}_q$, we find among them a zero divisor. For this, for any fixed γ we consider multiplication by $\alpha+\gamma\beta$ as a linear operator on E and we consider its kernel $E_\gamma\subset E$. For some γ we have $E_\gamma\neq 0$, if $\varkappa>1$. Then $E=E_\gamma\oplus(\alpha+\gamma\beta)E$ and we continue to apply the decomposition procedure described to both direct summands separately.

Let $\xi\in\mathbb{F}_q\subset E$ belong to one of the direct summands of the decomposition of E. Then the polynomial which represents ξ in K[t] has a nontrivial divisor in common with the polynomial g if $\varkappa>1$ (for $\varkappa=1$ the polynomial g is irreducible). Repeating this process recursively, we factor g into irreducible factors in time which is polynomial in q, m, s.

Now, analogously to [20], we factor f mod p over the finite field A/(p), and let the polynomial $h_1\in A[X]$ be such that h_1 mod p is irreducible over A/(p), $(h_1 \bmod p)\mid(f \bmod p)$ and the leading coefficient $lc_X(h_1)=1$. One can find the polynomial h_1 in time which is polynomial in $q,|p|, r>\deg f=\deg_X f$, based on the modified Berlekamp algorithm given above. For what follows we fix some natural number k (it will be made more precise below in the description of the algorithm).

Now we construct a polynomial $h \in A[X]$, such that $h \equiv h_1 (\mathrm{mod}\, p), (h \bmod p^k) | (f \bmod p^k)$, $\deg h = \deg h_1$ and $lc_X h = 1$. As in Hensel's lemma (cf., e.g., [5]) we shall seek h in the form $h = \sum_{1 \le i \le k} h_i p^{i-1}$, where $h_i \in A[X]$, $\deg h_i < \deg h_1 = \ell_1$ for $i > 1$ and $|h_i| < |p|$ for any i. One can show that a polynomial h, satisfying all these conditions, is unique.

Let $f \bmod p = (h_1 \bmod p)(g_1 \bmod p)$, where $g_1 \in A[X]$, such that $\deg f = \deg h_1 + \deg g_1$ and $lc_X g_1 = lc_X f$. Then $u_1 = f - h_1 g_1 = p v_1$ for some $v_1 \in A[X]$ and $\deg v_1 < \deg f$. We construct recursively for any $j \ge 2$ three polynomials $h_j, g_j, v_j \in A[X]$, which have the following properties:

1) $|h_j| < |p|, |g_j| < |p|, \deg h_j < \deg h_1 = \ell_1, \deg g_j < \deg g_1, \deg v_j < \deg f$;

2) $f - \left(\sum_{1 \le i \le j} h_i p^{i-1}\right)\left(\sum_{1 \le i \le j} g_i p^{i-1}\right) = v_j p^j$.

Let us assume that for all $i < j$ the polynomials h_i, g_i, v_i are already constructed. We let

$$h^{(j-1)} = \sum_{1 \le i \le j-1} h_i p^{i-1}, \quad g^{(j-1)} = \sum_{1 \le i \le j-1} g_i p^{i-1}.$$

Then by the inductive hypothesis and 2) we have $f - h^{(j-1)} g^{(j-1)} = v_{j-1} p^{j-1}$. We find $h_j, g_j \in A[X]$ such that property 1) holds for them and, in addition, $v_{j-1} \equiv h_j g_1 + g_j h_1 (\mathrm{mod}\, p)$. This can be done with the help of Euclid's algorithm in the ring of polynomials A/(p)[X], applying it to h_1, g_1 and keeping in mind that the polynomials h_1 mod p and g_1 mod p are relatively prime, since f mod p is separable according to the choice of p. Let $1 \equiv \bar{h}_j g_1 + \bar{g}_j h_1 (\mathrm{mod}\, p)$ for some suitable $\bar{h}_j, \bar{g}_j \in A[X]$. Then $v_{j-1} = v_{j-1} \bar{h}_j g_1 + v_{j-1} \bar{g}_j h_1 \equiv h_j g_1 + (v_{j-1} \bar{g}_j - \bar{v}_{j-1}) h_1 (\mathrm{mod}\, p)$, where $v_{j-1} \bar{h}_j \equiv \bar{v}_{j-1} h_1 + h_j (\mathrm{mod}\, p)$ and $|h_j| < |p|$, $\deg h_j < \deg h_1$. Since $\deg v_{j-1} < \deg f$ by 1) and $\deg h_j g_1 < \deg h_1 g_1 = \deg f$, we deduce from this that for the polynomial $g_j \equiv v_{j-1} \bar{g}_j - \bar{v}_{j-1} (\mathrm{mod}\, p)$ and such that $|g_j| < |p|$ one has $\deg g_j < \deg f - \deg h_1 = \deg g_1$.

Then we get $v_{j-1} p^{j-1} \equiv (h_j g_1 + g_j h_1) p^{j-1} \equiv (h_j g^{(j-1)} + g_j h^{(j-1)}) p^{j-1} + h_j g_j p^{2j-2} (\mathrm{mod}\, p^j)$. Consequently, $f \equiv h^{(j)} g^{(j)} (\mathrm{mod}\, p^j)$, i.e., $f - h^{(j)} g^{(j)} = v_j p^j$ for some $v_j \in A[X]$ such that $\deg v_j < \deg f$. For j = k, the constructed polynomial $h = h^{(k)}$ is the one sought.

Analogously to Proposition 2.5 of [20], there exists a unique (up to multiplication by an element from $A^* = F^*$, i.e., an invertible element of A) irreducible polynomial $h_0 \in A[X]$ such that $h_0 | f$ and $(h \bmod p) | (h_0 \bmod p)$. For the proof one can consider the factorization of f in A[X], reduce it mod p, and choose the unique factor h_0 from the factorization of f over A, which mod p is divisible by the irreducible polynomial h mod p. As in 2.5 of [20], if $g | f$ and $g \in A[X]$, then the following three assertions are equivalent:

$$(i)\ (h \bmod p) | (g \bmod p); \quad (ii)\ (h \bmod p^k) | (g \bmod p^k); \quad (iii)\ h_0 | g.$$

We reproduce here the proof of the implication $(i) \Longrightarrow (ii)$ (the rest is proved more easily). Since the polynomial f(mod p) is separable, the polynomials (h mod p) and ((f/g) mod p) are relatively prime. Consequently, $\lambda_1 h + \mu_1 f/g \equiv 1 (\mathrm{mod}\, p)$ for some suitable $\lambda_1, \mu_1 \in A[X]$.

Consequently, $\lambda_1 h + \mu_1 f/g = 1 - pv_1$ for some $v_1 \in A[X]$. Multiplying this equation by the polynomial $(1 + pv_1 + \dots + p^{k-1} v_1^{k-1})g$, we get $\lambda_2 h + \mu_2 f \equiv g \pmod{p^k}$ for the corresponding $\lambda_2, \mu_2 \in A[X]$. The left side of the latter is divisible by h(mod p^k) according to the construction of h, and hence finally we get $(h \bmod p^k) | (g \bmod p^k)$.

In what follows in this section our goal is the construction of the polynomial h_0. For the arguments we fix an integer $\ell_1 \leqslant m < \deg f$. Analogously to [20], we introduce the following lattice L over the ring A:

$$L = \{ v \in A[X] : \deg v \leqslant m \; \& \; (h \bmod p^k) | (v \bmod p^k) \}.$$

We identify the polynomial $v = \sum_{0 \leqslant i \leqslant m} v_i X^{l} \in A[X]$ with the vector $(v_0, \dots, v_m) \in A^{m+1}$. The following theorem is the analog of Proposition 2.7 of [20].

<u>THEOREM 1.2</u>. Let $0 \neq b \in L$ and for the element b suppose $|p| k \ell_1 > m|f| + (\deg f)|b|$. Then the polynomial h_0 divides b in the ring A[X].

<u>Proof</u>. We shall follow the proof of 2.7 of [20]. We let $g = g.c.d.(f, b) \in A[X]$. Then $p \nmid lc_X(g)$. We need only prove that $(h \bmod p) | (g \bmod p)$ according to the equivalence proved above. Hence let us assume the contrary. Then there exist $\lambda_1, \mu_1, w \in A[X]$ such that

$$\lambda_1 h + \mu_1 g = 1 - pw. \tag{1.1}$$

Further, we show that from (1.1) one gets a contradiction.

We let e = deg g, m' = deg b. Obviously, $0 \leqslant e \leqslant m' \leqslant m$. We introduce the A-lattice

$$M = \{ \lambda f + \mu b : \lambda, \mu \in A[X],\ 0 \leqslant \deg \lambda < m' - e,\ 0 \leqslant \deg \mu < (\deg f) - e \}.$$

Then $M \subset A + AX + \dots + AX^{(\deg f) + m' - e - 1} = V$. Let M' be the projection of the lattice M to the direct summand $\mathcal{U} = AX^e + \dots + AX^{(\deg f) + m' - e - 1}$ of the lattice V. Let us assume that some element $\lambda f + \mu b \in M$ projects to zero in M'. Then $\deg(\lambda f + \mu b) < e$. Since $g | (\lambda f + \mu b)$ and deg g = e, one has $\lambda f + \mu b = 0$. Consequently, μ = 0, since $\deg \mu < (\deg f) - e = \deg(f/g)$ and (f/g)/μ. Consequently, λ = 0.

Consequently, by what was just proved, the elements of the system of generators $\{ X^i f : 0 \leqslant i < m' - e \} \cup \{ X^l b : 0 \leqslant i < (\deg f) - e \}$ of the lattice M over A project into elements of an A-basis of the lattice M' which are linearly independent over A. Hence $rg_A M = rg_A M' = \deg f + m' - 2e$.

Now we show that under the assumption (1.1) one has the following inclusion:

$$\{ v \in M : \deg v < e + \ell_1 \} \subset p^k A[X] \tag{1.2}$$

Let $v \in M$, $\deg v < e + \ell_1$. Then $g | v$. Multiplying both sides of (1.1) by the polynomial $(1 + pw + (pw)^2 + \dots + (pw)^{k-1})(v/g)$, we get $\lambda_2 h + \mu_2 v \equiv (v/g) \pmod{p^k}$ for some suitable $\lambda_2, \mu_2 \in$ A[X]. We note that $(h \bmod p^k) | (v \bmod p^k)$, since $v \in M$, $b \in L$. From this, $(h \bmod p^k) | ((v/g) \bmod p^k)$. But on the other hand, $\deg(h \bmod p^k) = \ell_1$ (since $lc_X(h) = 1$) and $\deg((v/g) \bmod p^k) \leqslant \deg(v/g) < e + \ell_1 - e = \ell_1$. Consequently, $(v/g) \in p^k A[X]$ and, in particular, $v \in p^k A[X]$, which proves (1.2).

We denote by $\Delta_u(M')$ the determinant of the matrix whose columns are the coordinates in an A-basis of the lattice U of the elements of some A-basis of the lattice M'. Under change of bases the determinant $\Delta_u(M')$ can only be multiplied by some invertible element of the ring A (i.e., an element of $\mathbb{F}_q^*$).

First we estimate the order $|\Delta_u(M')|$ from above. Considering the basis of M' of which we spoke previously, we get

$$|\Delta_u(M')| \leqslant \sum_{0\leqslant i<m'-e} |X^i f| + \sum_{0\leqslant i<(\deg f)-e} |X^i b| = (m'-e)|f| + ((\deg f)-e)|b| \leqslant m|f| + (\deg f)|b|.$$

Now, based on (1.2), we estimate $|\Delta_u(M')|$ from below. Since A is a Euclidean ring [1], there exists a triangular basis $b_e,\ldots,b_{(\deg f)+m'-e-1}$ of the lattice M' over A, i.e., a basis such that deg bj = j for $e\leqslant j<(\deg f)+m'-e$. According to (1.2), $lc_X(b_e),\ldots,lc_X(b_{e+l_1-1})\in$ (p^k). We note that $e+l_1-1 \leqslant m'+(\deg f)-e-1$, since $g|b$ and (h mod p) $|((f/g) \bmod p)$ according to the assumptions made at the beginning of the proof of the theorem. Consequently,

$$|\Delta_u(M')| = \sum_{l_1\leqslant j<(\deg f)+m'-e} |lc_X(b_j)| \geqslant l_1 k|p| > m|f| + (\deg f)|b|$$

by the hypothesis of the theorem. This leads to a contradiction with the upper bound established above and completes the proof of Theorem 1.2.

To conclude the section we briefly recount the general scheme of the algorithm for factoring a polynomial $f\in A[X]$. First of all we choose $p\in A$ relatively prime with the discriminant $\mathrm{Res}_X(f, f'_X)$ (cf. the remark above on the choice of p). Then we decompose f mod p over the field A/(p) and we choose some $h_1\in A[X]$, such that $(h_1 \bmod p)|(f \bmod p)$; $(h_1 \bmod p)$ is irreducible, $l_1=\deg h_1$. We set successively $m=l_1, l_1+1,\ldots,(\deg f)-1$. We find the minimal integer k, satisfying $|p|kl_1> (m+\deg f)|f|$. Then we construct h according to the process of Hensel's lemma, described above. Finally, we determine whether there exists (and if so we find it) a nonzero vector $b\in L$ for which $|p|kl_1>m|f|+(\deg f)|b|$. This can be done with the help of Theorem 1.1 of Sec. 1 in polynomial time. Actually, $b=h_0\beta$ for some $\beta\in A^*=\mathbb{F}_q^*$. In fact, one has $|h_0|<|f|$. Consequently, $h_0|b$, and at the step when m = deg h_0, by Theorem 1.2 the algorithm described gives $b=h_0\beta$, since $h_0\in L$ and the polynomial h_0 has minimal order equal to $|h_0|$ among all nonzero elements of L again by Theorem 1.2.

3. The Case of Several Variables Over a Finite Field

Let $f\in \mathbb{F}_q\text{æ}[X, u_1,\ldots,u_n]$, where $n\geqslant 2$, $\rho=\deg_X(f)<r$, $a=lc_X(f)$, and $\deg_{u_i}(f)<r$. First we reduce consideration to the case when f is square-free and $lc_X(f)=1$.

In what follows, the original field $F=\mathbb{F}_q\text{æ}$ is extended in the course of the work of the algorithm, so that, as a result, we get a factorization $f=\prod_i f_i$ over some field $F_1\supset F$. One can pass to a factorization over F by considering the norm $N_{F_1/F}(f_i)|f$, which is irreducible over F.

We make the change of variables $g(X, U_1, \ldots, U_n) = a^{\delta-1} f(X/a, U_1, \ldots, U_n) \in F[X, U_1, \ldots, U_n]$. Then $lc_X(g) = 1$. From a factorization of g it is easy to pass to a factorization of f. Hence we shall assume that $lc_X(f) = 1$.

Let $\mathcal{D}(U_1, \ldots, U_n) = \mathrm{Res}_X(f, \partial f/\partial X)$ be the discriminant. If $\mathcal{D} = 0$ (the polynomial $\mathcal{D}$ can be calculated on the basis of [21] in time which is polynomial in the size of f), then on the basis of the construction from [4] we single out the repeated factors in the factorization of f considered as a polynomial in one variable over the field $F(U_1, \ldots, U_n)$. We note that for this, in the construction of Sec. 1 of [4], point c) for the field $F(U_1, \ldots, U_n)$ was not used to the full extent, but only for extracting roots of degree q in it, and in the field $F(U_1, \ldots, U_n)$ we have to extract q-th roots on the basis of the algorithm for extracting q-th roots in F.

Let $\mathcal{D} \not\equiv 0$. We set $\delta = \deg_{U_1, \ldots, U_n} \mathcal{D}$ and consider the set $I = \{y_0, \ldots, y_\delta\}^n$, where $y_0, \ldots, y_\delta$ are pairwise distinct and belong to the field F or some finite extension $F_1 \supset F$ of it. Then one can find an element $(\alpha_1, \ldots, \alpha_n) \in I$, such that $\mathcal{D}(\alpha_1, \ldots, \alpha_n) \neq 0$.

We replace $f(X, U_1, \ldots, U_n)$ by the polynomial $f(X, U_1 - \alpha_1, \ldots, U_n - \alpha_n)$. Obviously, getting the factorization of the latter polynomial, we get the factorization of f, and hence, in what follows, we shall assume that the polynomial $f(X, 0, \ldots, 0)$ is separable.

Let $\mathrm{char}\, F = q \neq 2$ and $2^k > 2rn \geqslant 2^{(k-1)}$. We extend the field $F = \mathbb{F}_{q^{\varkappa}}$ to the field $\mathbb{F}_{q^{\varkappa \cdot 2^k}}$ successively (k times) by adjoining the square root of some element which is not a square, from the current field. We describe the process of seeking such an element μ in the field F_1. Let $\mu_1 \in F_1$, and $\mu_2^2 = \mu_1$ (we find the element μ_2 with the help of the modified Berlekamp algorithmn, cf. Sec. 2), for μ_2 and $-\mu_2$ we arbitrarily choose $\mu_3^{(1)}$, $\mu_3^{(2)}$, so that $(\mu_3^{(1)})^2 = \mu_2$ and $(\mu_3^{(2)})^2 = -\mu_2$; then we choose some square roots of $\mu_3^{(1)}$ and $\mu_3^{(2)}$, etc. In no more than $\log_2 \mathrm{card}\, F_1$ steps, one of the two elements considered $\mu_s^{(i)} \in F_1^* \setminus (F_1^*)^2$, where $i = 1, 2$; $s \leqslant \log_2 \mathrm{card}\, F_1$.

Now let char F = 2. One can assume that $3 \mid \mathrm{card}\, F - 1$. If this is not so, then we imbed F in the field $\mathbb{F}_{2^{2\beta}} = F_2 \supset F = \mathbb{F}_{2^{2\beta - 1}}$ with the help of the polynomial $Z^2 + Z + 1$ which is irreducible over F. Then we perform a construction, analogous to the construction above, "replacing 2 by 3," i.e., we assume that $3^k > 2rn \geqslant 3^{k-1}$ and we extract cube roots, as a result of which we get the field $\mathbb{F}_{2^{2\beta \cdot 3^k}}$.

One can now assume that $F = \mathbb{F}_{q^{\varkappa \cdot 2^k}}$ or $F = \mathbb{F}_{2^{2\beta \cdot 3^k}}$, respectively; then the splitting field of the polynomial f(X, 0, ..., 0) due to the choice of k has odd degree over F, if $q = \mathrm{char}\, F \neq 2$, or degree not divisible by 3, if char F = 2. As above, we choose an element $\mu \in F^* \setminus (F^*)^2$ in the first case and $\mu \in F^* \setminus (F^*)^3$ in the second.

For any s the polynomial $Z^{2^s} - \mu$ or, respectively, $Z^{3^s} - \mu$ is irreducible over F because, as is known [6], the polynomial $Z^m - a$ is irreducible over an arbitrary field G, if $a \notin G^p$ for any prime $p \mid m$ and $a \notin -4G^4$ if $4 \mid m$. We let s = kn and let θ be a root of one of the two polynomials considered, respectively.

Before the theorem we need the following version of Hensel's lemma. We let $I=(i_1,\dots,i_n)$ be a multiindex, where $0\leqslant i_\alpha\in\mathbb{Z}$ for any α and $U^I=U_1^{i_1}\cdots U_n^{i_n}$, the weight $|I|=i_1+\dots+i_n$, K be a field. We introduce a partial ordering relation on the multiindices, by setting $I=(i_1,\dots,i_n)\preccurlyeq J=(j_1,\dots,j_n)$ if $i_1\leqslant j_1,\dots,i_n\leqslant j_n$.

HENSEL'S LEMMA. Let $f\in K[X,U_1,\dots,U_n]$, the leading coefficient for X in f be equal to 1, and the polynomial $f_0=f(X,0,\dots,0)\in K[X]$ be separable. Let us assume that $f_0=g_0h_0$, where $g_0,h_0\in K[X]$ are polynomials with leading coefficients equal to 1. Then for each multiindex I with $|I|\geqslant 1$ there exist unique polynomials $g_I,h_I\in K[X]$, such that $\deg g_I<g_0$, $\deg h_I<\deg h_0$ and in the ring $K[[U_1,\dots,U_n]][X]$ one has

$$\Big(g_0+\sum_{\beta_1=1}^{\infty}\sum_{|I|=\beta_1}g_IU^I\Big)\Big(h_0+\sum_{\beta_2=1}^{\infty}\sum_{|J|=\beta_2}h_JU^J\Big)=f.$$

Proof. The left side of this equation transforms to the form

$$g_0h_0+\sum_{\beta=1}^{\infty}\sum_{|I|=\beta}\Big(g_0h_I+h_0g_I+\sum_{I_1+I_2=I,I_1\prec I,I_2\prec I}g_{I_1}h_{I_2}\Big)U^I.$$

Considering, by induction, that we have already found $\sum_{I_1+I_2=I,I_1\prec I,I_2\prec I}g_{I_1}h_{I_2}$, we can, using the Euclidean algorithm (cf. Sec. 2), find h_I and g_I.

We note that the lemma extends in an obvious way to a factorization $f_0=g_0^{(1)}g_0^{(2)}\cdots g_0^{(j)}$ into more factors, and here the monomial with multiindex $I=(i_1,\dots,i_n)$ is constructed in time which is polynomial in $i_1\dots i_n,\varrho=\deg_Xf$.

THEOREM 1.3. Let $f\in F[X,U_1,\dots,U_n]$ be irreducible over $F=F_{q^{\varkappa 2^{\kappa}}}$ for q ≠ 2 and $F=\mathbb{F}_{2^{\varkappa 3^{\kappa}}}$, if ϰ is even, or $F=\mathbb{F}_{2^{2\varkappa 3^{\kappa}}}$, if ϰ is odd, for q = 2, and in addition let $lc_X(f)=1$ and $f_0=f(X,0,\dots,0)\in F[X]$ be separable. Moreover, let $f_0\mid\tilde f$ for some $\tilde f\in\mathbb{F}_{q^\varkappa}[X]$, such that $0\leqslant\deg\tilde f<\varkappa$. Then the polynomial $\hat f=f(X,U,\theta^{\beta}U,\theta^{\beta^2}U,\dots,\theta^{\beta^{n-1}}U)\in F_1[X,U]$ is irreducible over the field $F_1=F[\theta]$, where $\beta=2^{\kappa}$ for q ≠ 2 and $\beta=3^{\kappa}$ for q = 2; here $\theta^{\beta^n}\in F\setminus F^2$ for q ≠ 2 and $\theta^{\beta^n}\in F\setminus F^3$ for q = 2.

Proof. Let $\bar F$ be the algebraic closure of F. It follows from Hensel's lemma that $f=\prod_{1\leqslant i\leqslant\varrho}(X-X_i(U_1,\dots,U_n)),\varrho=\deg_Xf$ for some $X_i(U_1,\dots,U_n)\in\bar F[[U_1,\dots,U_n]]$ $(1\leqslant i\leqslant\varrho)$.

Let us assume that $\bar f=g^{(1)}g^{(2)}$, where $0<\deg_Xg^{(1)}=\varrho_1<\varrho$, since $lc_X\bar f=lc_Xf=1$ and $g^{(1)},g^{(2)}\in F_1[X,U]$; further, it is possible to compute that $\overline{G^{(1)}}=g^{(1)}$ and $\overline{G^{(2)}}=g^{(2)}$, where $G^{(1)}=\prod_{1\leqslant i\leqslant\varrho_1}(X-X_i(U_1,\dots,U_n)),G^{(2)}=f/G^{(1)}$ by the factoriality of the ring $\bar F[[U]][X]$, since $\bar f=\prod_{1\leqslant i\leqslant\varrho}(X-\overline{X_i(U)})$ is the factorization of $\bar f$ into irreducibles in this ring. We let

$$G^{(1)}=\sum_{0\leqslant i\leqslant\varrho_1}\sum_{0\leqslant\alpha_1,\dots,\alpha_n<\infty}b^{(1)}_{i,\alpha_1,\dots\alpha_n}X^iU_1^{\alpha_1}\cdots U_n^{\alpha_n},$$

$$G^{(2)}=\sum_{0\leqslant i\leqslant\varrho-\varrho_1}\sum_{0\leqslant\alpha_1,\dots,\alpha_n<\infty}b^{(2)}_{i,\alpha_1,\dots,\alpha_n}X^iU_1^{\alpha_1}\cdots U_n^{\alpha_n},$$

where $b^{(1)}_{i,\alpha_1,\ldots\alpha_n}, b^{(2)}_{i,\alpha_1,\ldots\alpha_n} \in \overline{F}$. Since $f(X,0,\ldots 0) = \bar{f}(X,0) = g^{(1)}(X,0)g^{(2)}(X,0)|\tilde{f}$, the coefficients of the polynomials $g^{(1)}(X,0)$, $g^{(2)}(X,0)$ lie in the splitting field F_0 of the polynomial $\bar{f}$. By the choice of k, the degree of the composite $[F_0F:F]$ is odd for $q \neq 2$ or is not divisible by 3 for q = 2 and, consequently, is relatively prime with $\beta^n = [F_1:F]$. Since, on the other hand, $g^{(1)}(X,0), g^{(2)}(X,0) \in F_1[X]$, we get that $g^{(1)}(X,0), g^{(2)}(X,0) \in F[X]$.

To the factorization $f(X,0,\ldots,0) = g^{(1)}(X,0)\, g^{(2)}(X,0)$ we apply the process of Hensel's lemma, and since $G^{(1)}(X,0,\ldots,0) = g^{(1)}(X,0)$ and $G^{(2)}(X,0,\ldots,0) = g^{(2)}(X,0)$, we get as a result the factorization $f = G^{(1)}G^{(2)}$ due to the uniqueness condition from Hensel's lemma. Hence, in fact $b^{(1)}_{i,\alpha_1,\ldots,\alpha_n}, b^{(2)}_{i,\alpha_1,\ldots\alpha_n} \in F$ again by Hensel's lemma.

We let $g^{(1)} = \sum_{0\leq i\leq \rho_1;\alpha} a^{(1)}_{i,\alpha} X^i \mathcal{U}^\alpha$, $g^{(2)} = \sum_{0\leq i\leq \rho-\rho_1;\alpha} a^{(2)}_{i,\alpha} X^i \mathcal{U}^\alpha$, where $a^{(1)}_{i,\alpha}, a^{(2)}_{i,\alpha} \in F_1$.

We show that there exists at least one coefficient $b^{(1)}_{i,\alpha_1,\ldots,\alpha_n}$ or $b^{(2)}_{i,\alpha_1,\ldots,\alpha_n}$ which is nonzero, such that $nr < \alpha_1 + \ldots + \alpha_n \leq 2nr$. We assume the contrary and we let $G^{(1)} = V_1 + W_1$, $G^{(2)} = V_2 + W_2$, where $\deg V_1 = \deg_{\mathcal{U}_1,\ldots\mathcal{U}_n} V_1 \leq nr$, $\deg V_2 \leq nr$, and in W_1, W_2 there only appear monomials of degree greater than 2nr in $\mathcal{U}_1,\ldots,\mathcal{U}_n$. Then $f = G^{(1)}G^{(2)} = V_1V_2 + (V_1W_2 + W_1V_2 + W_1W_2)$, and since $\deg f \leq nr$, $\deg(V_1V_2) \leq 2nr$, and in $(V_1W_2 + W_1V_2 + W_1W_2)$ there only appear monomials of degree greater than 2nr, we get that $f = V_1V_2$, which contradicts the irreducibility of f. Thus, for definiteness let $b^{(1)}_{i,\alpha_1,\ldots\alpha_n} \neq 0$ for some $i, \alpha_1, \ldots, \alpha_n$, such that $nr < \alpha_0 = \alpha_1 + \ldots + \alpha_n \leq 2nr$.

We show that $a^{(1)}_{i,\alpha_0} \neq 0$. We consider $h(X,\mathcal{U},Z_1,\ldots,Z_n) = G^{(1)}(X,Z_1\mathcal{U},\ldots,Z_n\mathcal{U}) = \sum_{0\leq i\leq \rho_1;\gamma_1,\ldots\gamma_n} b^{(1)}_{i,\gamma_1,\ldots\gamma_n} X^i \mathcal{U}^{\gamma_1+\ldots+\gamma_n} Z_1^{\gamma_1}\ldots Z_n^{\gamma_n}$. We let $h_{i,\alpha_0} = \sum_{\gamma_1+\ldots+\gamma_n=\alpha_0} b^{(1)}_{i,\gamma_1,\ldots\gamma_n} Z_1^{\gamma_1}\ldots Z_n^{\gamma_n}$. Obviously, $h(X,\mathcal{U},1,\theta^\beta,\theta^{\beta^2},\ldots,\theta^{\beta^{n-1}}) = g^{(1)}(X,\mathcal{U})$, and moreover $a^{(1)}_{i,\alpha_0} = h_{i,\alpha_0}(1,\theta^\beta,\theta^{\beta^2},\ldots,\theta^{\beta^{n-1}})$. By what was proved above, $h_{i,\alpha_0} \not\equiv 0$, since in it there appears the monomial $b^{(1)}_{i,\alpha_1,\ldots,\alpha_n} \times Z_1^{\alpha_1}\ldots Z_n^{\alpha_n} \neq 0$. Since $0 \leq \gamma_1 \leq 2nr < \beta$, for different vectors $(\gamma_1,\ldots\gamma_n)$, such that $\gamma_1+\ldots+\gamma_n = \alpha_0$, the corresponding numbers $\beta\gamma_2 + \beta^2\gamma_3 + \ldots + \beta^{n-1}\gamma_n$ are different, so $h_{i,\alpha_0}(1,\theta^\beta,\theta^{\beta^2},\ldots\theta^{\beta^{n-1}}) = \varphi_1(\theta)$, where $0 \not\equiv \varphi_1(Z) \in F\,[Z]$ and $\deg_Z(\varphi_1) \leq \beta\gamma_2 + \beta^2\gamma_3 + \ldots + \beta^{n-1}\gamma_n \leq \beta^{n-1}\alpha_0 < \beta^n$. But the degree $[F_1:F] = \beta^n$, so $\varphi_1(\theta) \neq 0$, and consequently $a^{(1)}_{i,\alpha_0} \neq 0$. From this, $\deg_{\mathcal{U}} g^{(1)} \geq \alpha_0 > nr$ but, on the other hand, $g^{(1)} | \bar{f}$ and hence $\deg_{\mathcal{U}}(g^{(1)}) \leq \deg_{\mathcal{U}}(\bar{f}) \leq nr$. The contradiction obtained completes the proof of the theorem.

The theorem was found jointly with A. L. Chistov (cf. [4]).

We describe the algorithm for factoring f. We consider two cases.

I) $r \leq n$. Let $f(X,0,\ldots,0) = \prod_{i\in I} \varphi_i$ be the factorization of $f(X,0,\ldots,0)$ over F and let $f(X,\mathcal{U}_1,\ldots,\mathcal{U}_n) = f_1\cdots f_\sigma$ be the factorization of $f(X,\mathcal{U}_1,\ldots,\mathcal{U}_n)$ over F, where $lc_X(\varphi_i) = lc_X(f_i) = 1$ for all i. Then for some partition $I = I_1 \cup \cdots \cup I_\sigma$ one has $f_j(X,0,\ldots,0) = \prod_{i\in I_j} \varphi_i$ for all $1 < j \leq \delta$. Hence the algorithm in the case considered finds a factorization $f(X,0,\ldots,0) = \prod_{i \in I} \varphi_i$ and looks at all subsets $\emptyset \neq I_1 \subsetneqq I$. We let $\prod_{i \in I_1} \varphi_i = \varphi_{I_1}$ and $\bar{I}_1 = I \setminus I_1$. We apply the process of Hensel's lemma (cf. above) to the factorization $f(X,0,\ldots,0) = \varphi_{I_1} \varphi_{\bar{I}_1}$ up to the construction of monomials for which the degree in each variable does not exceed r, and then we verify whether f is equal to the product of the two polynomials obtained. As a result we find a nontrivial factorization of f, if f is reducible, or we establish its irreducibility.

The procedure described requires no more than time which is polynomial in $2^r r^n$, q (since $\operatorname{card} I < r$), i.e., polynomial in q and in the size of $L_1(f)$, since in the case considered $2^r \leq r^n \leq L_1(f)$.

II) $r > n$. We find a factorization of $f(X, u, \theta^{\beta} u, \theta^{\beta^2} u, \ldots, \theta^{\beta^{n-1}} u) = \bar{f}(X, u)$ over $F_1 = F[\theta]$ using Sec. 3, in time which is polynomial in $L_1(\bar{f})$, the degree $[F_1 : F]$, and q. Let $\bar{f} = \prod_i \varphi_i$. We let $\varphi_i = \varphi_{i,0} + \sum_j \varphi_{i,j} u^j$, where $\varphi_{i,j} \in F_1[X]$, $j \geq 0$, and moreover $\deg_X \varphi_{i,j} < \deg_X \varphi_{i,0}$ for $j > 0$, since $lc_X \bar{f} = 1$ and one can require that $lc_X(\varphi_i) = 1$ for all i.

We note that $f(X,0,\ldots,0) = \bar{f}(X,0) = \prod_i \varphi_i(X,0) = \prod_i \varphi_{i,0}$. Analogously to the way it was established in the proof of Theorem 1.3 that the coefficients of the polynomials $\overline{G^{(1)}}(X,0,\ldots,0)$, $\overline{G^{(2)}}(X,0,\ldots,0)$ lie in F, one can show here that $\varphi_{i,0} \in F[X]$ for all i.

By Hensel's lemma applied to the factorization $f(X,0,\ldots,0) = \prod_i \varphi_{i,0}$, , there exist $\Phi_i(X, u_1, \ldots, u_n) \in F[[u_1, \ldots, u_n]][X]$, such that $\Phi_i(X,0,\ldots,0) = \varphi_{i,0}$ for all i and $f = \prod_i \Phi_i$. We show that $\Phi_i \in F[X, u_1, \ldots, u_n]$ for all i. Let $f = \prod_j \Psi_j$ be a factorization of f over F, i.e., $\Psi_j \in F[X, u_1, \ldots, u_n]$ and $lc_X \Psi_j = 1$ for any j. Applying Theorem 1.3, we get that $\Psi_j(X, u, \theta^{\beta} u, \theta^{\beta^2} u, \ldots, \theta^{\beta^{n-1}} u)$ is irreducible over F_1. Hence, for any j there also exists a unique i, such that $\Psi_j(X, u, \theta^{\beta} u, \theta^{\beta} u, \ldots, \theta^{\beta^{n-1}} u) = \varphi_i(X, u)$, and, in particular, $\Psi_j(X,0,\ldots,0) = \varphi_{i,0}$. Hence by the uniqueness condition in Hensel's lemma, we have $\Psi_j = \Phi_i$ i.e., Φ_i is a polynomial which is irreducible over F.

The algorithm for constructing each Φ_i following the process of Hensel's lemma, concludes its work in the construction of monomials of degree no higher than r in each variable $u_1, \ldots, u_n$. The description of the algorithm for factoring f is concluded.

Finally, we estimate the time for the work of the algorithm in case II). The process of Hensel's lemma works in polynomial time (in the case considered here of a finite field F, this follows from the fact that the calculation of the coefficients of the factors requires only a polynomial number of operations). Hence it suffices to estimate the degree $[F_1 : F]$ from above as well as the size of the polynomial $\bar{f}$. By construction $[F_1 : F] = \beta^n \leq (6rn)^n \leq 6^n r^{2n}$, i.e., it does not exceed some polynomial in the size of the polynomial f (cf. Introduction). Further, the size of the polynomial $\bar{f}$ is not greater than a suitable polynomial in the size of the polynomial f and $[F_1 : F]$, since $\bar{f}$ is obtained from f by substituting elements $\theta^{\beta^i} u$ for u_{i+1} (for $i \geq 1$) and the variable u for u_1, and then reducing similar terms, the latter does not increase the size. Consequently, the algorithm given for factoring f works in time which is polynomial in q and in the size of the polynomial f.

This completes the proof of the last basic result of Chapter I.

THEOREM 1.4. One can construct an algorithm which decomposes any polynomial $f \in \mathbb{F}_q\varkappa[X_1, \dots, X_n]$ into factors which are irreducible over the finite field $\mathbb{F}_q\varkappa$ in time which is polynomial in $r^n, \varkappa, q$, where $\deg_{X_i}(f) < r$ for $1 \leq i \leq n$, i.e., in time which is polynomial in q and in the size of the polynomial f.

Chapter II

SOLUTION OF SYSTEMS OF ALGEBRAIC EQUATIONS IN SUBEXPONENTIAL TIME

1. Choice of a Transcendence Basis for All Components of Highest Dimension

Suppose given a system $f_0 = \dots = f_{k-1} = 0$ of equations, in which $f_0, \dots, f_{k-1} \in F[X_1, \dots, X_n]$ are polynomials of degree $d_0, \dots, d_{k-1}$, respectively. We denote by $\tilde{f}_i = Z_0^{\deg(f_i)} f_i \cdot (Z_1/Z_0, \dots, Z_n/Z_0)$ the homogeneous polynomial of degree f_i with respect to the variables $Z_0, \dots, Z_n$. The system $f_0 = \dots = f_{k-1} = 0$ defines an affine algebraic variety $V = \{(\vartheta_1, \dots, \vartheta_n) \in \mathbb{A}^n(\bar{F}) : f_0(\vartheta_1, \dots, \vartheta_n) = \dots = f_{k-1}(\vartheta_1, \dots \vartheta_n) = 0\} \subset \mathbb{A}^n(\bar{F}) = \bar{F}^n$. The system $\tilde{f}_0 = \dots = \tilde{f}_{k-1} = 0$ in its own right defines a projective algebraic variety

$$\bar{V} = \{(\vartheta_0 : \dots : \vartheta_n) \in \mathbb{P}^n(\bar{F}) : \tilde{f}_0(\vartheta_0, \dots, \vartheta_n) = \dots = \tilde{f}_{k-1}(\vartheta_0, \dots \vartheta_n) = 0\} \subset \mathbb{P}^n(\bar{F}).$$

(Cf., e.g., [3, 7] for the basic concepts and notation from algebraic geometry which are needed here and later.) As is well known, the affine space $\mathbb{A}^n(\bar{F})$ can be imbedded in the projective space $\mathbb{P}^n(\bar{F})$, so that the point $(\vartheta_1, \dots, \vartheta_n) \in \mathbb{A}^n(\bar{F})$ is mapped into the point $(1 : \vartheta_1 : \dots : \vartheta_n) \in \mathbb{P}^n(\bar{F})$, where the image of $\mathbb{A}^n(\bar{F})$ in $\mathbb{P}^n(\bar{F})$ coincides with the open affine subset $\{(\vartheta_0 : \dots : \vartheta_n) : \vartheta_0 \neq 0\}$. In what follows, we sometimes identify $\mathbb{A}^n(\bar{F})$ with its image in $\mathbb{P}^n(\bar{F})$. We note that $V = \bar{V} \cap \mathbb{A}^n(\bar{F})$. We shall call the hyperplane $P_\infty = \{(0 : \vartheta_1 : \dots : \vartheta_n) \in \mathbb{P}^n\}$ the hyperplane at infinity.

We can uniquely represent the varieties $V = \bigcup_{i \in I} \mathcal{U}_i$, $\bar{V} = \bigcup_{j \in J} W_j$ as finite unions of closed subsets which are irreducible over $\bar{F}$ (components). Then we can assume without loss of generality that $J = I \cup J_1$, where $I \cap J_1 = \emptyset$, and moreover $W_i \cap \mathbb{A}^n(\bar{F}) = \mathcal{U}_i$, and the closure in the Zariski topology $\bar{\mathcal{U}}_i = W_i$ for any $i \in I$, besides this, $W_j \cap \mathbb{A}^n(\bar{F}) = \emptyset$ for any $j \in J_1$ (we shall call the varieties W_j the components at infinity).

Let $W \subset \mathbb{P}^n(\bar{F})$ or $W \subset \mathbb{A}^n(\bar{F})$ be some irreducible variety. By $\bar{F}(W)$ we denote the field of rational functions on W. One can consider any rational function on $\mathbb{P}^n$ as a ratio g/h, where $g, h \in \bar{F}[Z_0, \dots, Z_n]$ are homogeneous polynomials of identical degrees and $h \neq 0$. A rational function on W is the restriction to W of some rational function g/h, under the condition that h does not vanish identically on W. This function is defined on the nonempty open subset of the variety W, equal to $W \cap \{\vartheta : h(\vartheta) \neq 0\}$ (two rational functions coincide if and only if they are defined and coincide on some nonempty open subset of the variety W).

The transcendence degree $\deg tr_{\bar{F}} \bar{F}(W)$ is called the dimension dim W of the variety W; by the dimension m = dim $\bar{V}$ we mean $\max_{j \in J} \dim W_j$. We let $J_2 = \{j \in J : \dim W_j = m\}$. In the title of this section by components of highest dimension we mean the set of components W_j, when j runs through J_2.

We also note that the degree $\deg \bar{V} \leqslant d_0 \cdot \ldots \cdot d_{k-1}$, according to Bezout's inequality (cf. [7]). In [14] the upper bound $\deg \bar{V} \leqslant (1+n \max d_i)^n$ is established (it is best for large k). Hence, in what follows we shall sometimes give estimates for the upper bound in terms of the degree of the variety deg $\bar{V}$. We note that $\deg \bar{V} = \sum_{j \in J} \deg W_j$ [7], and, in particular, $\mathrm{card}(J) \leqslant \deg(\bar{V})$.

The goal of the present section is to construct a certain family $\mathfrak{M} = \mathfrak{M}_{n,m,d}$ of collections, each of which consists of m + 1 linear forms $\sum_{0 \leqslant i \leqslant n} \lambda_{\ell i} Z_i$, $0 \leqslant \ell \leqslant m$, such that $\lambda_{\ell i} \in F$ if F is infinite, or $\lambda_{\ell i}$ belongs to some suitable finite extension of F, when F is a finite field and, moreover, the intersection $\bar{V} \cap \{\sum_{0 \leqslant i \leqslant n} \lambda_{0i} Z_i = \ldots = \sum_{0 \leqslant i \leqslant n} \lambda_{mi} Z_i = 0\}$ of a variety $\bar{V}$ for which $\deg \bar{V} \leqslant d$ with the set of common zeros of the linear forms $\sum_{0 \leqslant i \leqslant n} \lambda_{\ell i} \cdot Z_i$, $0 \leqslant \ell \leqslant m$, is empty.

In what follows we shall more than once need the following construction of a set from N (for arbitrary N) vectors $u_1, \ldots, u_N \in H^{\ell+1}$, where H = F or $H \supset F$ is a suitable finite extension of F, such that $\mathrm{card}(H) > N$, if $\mathrm{card}(F) < \infty$. Let $\alpha_1, \ldots \alpha_N \in H$ be pairwise distinct elements. We define the vector $u_i = (1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^\ell)$.

LEMMA 2.1. Any (ℓ + 1) vectors from the constructed set $u_1, \ldots, u_N$ are linearly independent over H.

We now return to the construction of the family $\mathfrak{M}$ of collections of linear forms. We let N = 1 + nd and let $(u_{10}, \ldots, u_{1n}), \ldots, (u_{N0}, \ldots u_{Nn}) \in H^{n+1}$ be vectors, any (n + 1) of which are linearly independent. For brevity we let $L_j = \sum_{0 \leqslant i \leqslant n} u_{ji} Z_i$. We show that as $\mathfrak{M}$ one can take the family of collections $(L_{j_0}, \ldots L_{j_m})$, where $j_0, \ldots, j_m$ run through all values such that $1 \leqslant j_0 < j_1 \ldots < j_m \leqslant N$.

By induction we shall prove a somewhat stronger assertion. Namely, we show that for any $0 \leqslant \ell \leqslant m$ one can find $1 \leqslant j_0 < j_1 < \ldots < j_\ell \leqslant N$ such that $\dim \bar{V} \cap \{L_{j_0} = \ldots = L_{j_\ell} = 0\} = m - \ell - 1$ (in particular, for m = ℓ we have $\bar{V} \cap \{L_{j_0} = \ldots = L_{j_m} = 0\} = \emptyset$). Suppose this assertion is already proved for ℓ − 1 (if ℓ = 0 we assume that nothing has yet been proved). We must show that one can find a linear form Lj, where $1 \leqslant j \leqslant N$, such that Lj does not vanish identically on any component of the variety $\bar{V} \cap \{L_{j_0} = \ldots = L_{j_{\ell-1}} = 0\}$. If this is not so, then by Dirichlet's principle, since $\deg \bar{V} \cap \{L_{j_0} = \ldots = L_{j_{\ell-1}} = 0\} \leqslant \deg \bar{V}$, one can find some component W of the variety $\bar{V} \cap \{L_{j_0} = \ldots = L_{j_{\ell-1}} = 0\}$ and n + 1 different linear forms $L_{s_0}, \ldots, L_{s_n}$, vanishingly identically on W, and then $W \subset \{L_{s_0} = \cdots = L_{s_n} = 0\} = \emptyset$. The contradiction obtained proves the existence of the required form Lj. Arranging the indices $j_0, \ldots, j_{\ell-1}, j$ in increasing order, we get some new indices $j_0, \cdots, j_\ell$, such that $\dim \bar{V} \cap \{L_{j_0} = \ldots = L_{j_\ell} = 0\} = m - \ell - 1$ and thus our assertion is proved.

Now we prove the following lemma, which we shall use in the subsequent sections.

LEMMA 2.2. Let $\bar{V} = \{f_0 = \ldots = f_{k-1} = 0\}$ be the variety of common zeros in $\mathbb{P}^n(\bar{F})$ of homogeneous polynomials $f_0, \ldots, f_{k-1} \in F[Y_0, \ldots, Y_n]$. Then the following conditions are equivalent:

1) $\bar{V}\cap\{Y_0=\ldots=Y_m=0\}=\emptyset$

2) the system of equations

$$f(Y_0,t_1Y_0,\ldots,t_mY_0,Y_{m+1},\ldots Y_n)= \;=f_{k-1}(Y_0,t_1Y_0,\ldots,t_mY_0,Y_{m+1},\ldots,Y_n)=0$$

with coefficients from the field $F(t_1,\ldots,t_m)$, where $t_1,\ldots,t_m$ are algebraically independent over the field F, has only a finite number of solutions in $\mathbb{P}^{n-m}(\overline{F(t_1,\ldots,t_m)})$ and has no solutions at infinity, i.e., solutions with $Y_0 = 0$.

Proof. 1)$\Rightarrow$2). The system of equations $f_0=\ldots=f_{k-1}=0,\ Y_1-t_1Y_0=\ldots=Y_m-t_mY_0=0$ is equivalent with the system from point 2). Since $\emptyset=\bar{V}(\overline{F(t_1,\ldots,t_m)})\cap\{Y_0=\ldots=Y_m=0\}=\{f_0=\ldots=f_{k-1}=Y_1-t_1Y_0=\ Y_m-t_mY_0\ \ \{Y_0=0\}$, by the theorem on the dimension of an intersection (cf. [3, 7]), the system of equations from 2) has only a finite number of solutions. The system from point 2) cannot have solutions with $Y_0 = 0$, since, if it did, $\bar{V}(\overline{F(t_1,\ldots t_m)})\cap\{Y_0=\ldots=Y_m=0\}\neq\emptyset$ and from this, as is well known, it follows that $\bar{V}\cap\{Y_0=\ldots=Y_m=0\}\neq\emptyset$, which contradicts 1).

2)$\Rightarrow$1). Let us assume that $\bar{V}\cap\{Y_0=\ldots=Y_m=0\}\neq\emptyset$ and let $(0:\ldots:0:\xi_{m+1}:\ldots:\xi_n)\in\bar{V}\cap\{Y_0=\ldots=Y_m=0\}$. Then $(0:\xi_{m+1}:\ldots:\xi_n)\in\mathbb{P}^{n-m}(\overline{F(t_1,\ldots,t_m)})$ is a solution of the system from point 2) with $Y_0 = 0$. The lemma is proved.

We note that essentially at the same time we have proved that if the system from point 2) has no solutions with $Y_0 = 0$, then it has a finite number of solutions.

COROLLARY. Under the conditions of the lemma, for any component W_j of highest dimension m of the variety $\bar{V}$ the rational functions $Y_1/Y_0,\ldots,Y_m/Y_0$ form a transcendence basis of the field of rational functions $\bar{F}(W_j)$ over $\bar{F}$.

Proof. The linear form Y_0 is not identically equal to zero on W_j, since if it were, $\bar{V}\cap\{Y_0=\ldots=Y_m=0\}\supset W_j\cap\{Y_1=\ldots=Y_m=0\}\neq\emptyset$ by the theorem on the dimension of the intersection [7]. Hence it suffices to prove that the functions $Y_j/Y_0,\ 1\leqslant j\leqslant m$, are algebraically independent in $\bar{F}(W_j)$. Let us assume the contrary, and let there exist an algebraic dependence relation among $Y_1/Y_0,\ldots Y_m/Y_0$. Then there exists a nonzero homogeneous factor $\psi(Y_0,\ldots,Y_m)\in\bar{F}[Y_0,\ldots Y_m]$ which is identically equal to zero on W_j. There exist linear forms $S_0,\ldots,S_m$ in $Y_0,\ldots Y_m$ with coefficients from $\bar{F}$, which are a basis of the space of linear forms in $Y_0,\ldots,Y_m$ and such that for the polynomial $\psi_1(S_0,\ldots,S_m)=\psi(Y_0,\ldots Y_m)$ the leading coefficient $lc_{S_0}\psi_1=1$. Then we get by the dimension of intersection theorem $\emptyset\neq W_j\cap\{S_1=\ldots=S_m=0\}=W_j\cap\{S_1=\ldots=S_m=0\}\cap\{\psi_1(S_0,\ldots,S_m)=0\}=W_j\cap\{S_1=\ldots=S_m=0\}\cap\{S_0=0\}=W_j\cap\{Y_0=\ldots=Y_m=0\}$, which contradicts the hypothesis of the lemma and proves the corollary.

Now we estimate the number of elements of the family $\mathfrak{M}$. We have $card(\mathfrak{M})=\binom{n\deg\bar{V}+1}{m+1}\leqslant(n(\deg\bar{V}+1))^{m+1}/(m+1)!<(3n(\deg\bar{V}+1)/(m+1))^{m+1}$, the last number does not exceed $(3(n-m)(\deg\bar{V}+1))^{m+1}$, if $0\leqslant m<n/2$, and does not exceed $(6(\deg\bar{V}+1))^{m+1}$ if $n/2\leqslant m<n$. If we know (cf. Sec. 3 below) that $\deg\bar{V}\leqslant d^{n-m}$ then $card\ \mathfrak{M}$ can be estimated above by a polynomial in $d^{(n-m)(m+1)}$ for $d>1$.

We sum up the properties of the family $\mathfrak{M}$ in the form of the following lemma.

LEMMA 2.3. One can construct a family $\mathfrak{M}=\mathfrak{M}_{n,m,d}$, consisting of (m + 1)-tuples of linear forms in the variables $X_0,\ldots,X_n$ such that for any closed set $\bar{V}\subset\mathbb{P}^n(\bar{F})$, for which $\dim\bar{V}\leqslant m$, $\deg\bar{V}\leqslant d$, one can find an (m + 1)-tuple $(Y_0,\ldots,Y_m)\in\mathfrak{M}$, such that $\bar{V}\cap\{Y_0=\ldots=Y_m=0\}=\emptyset$. Here $\operatorname{card}\mathfrak{M}=\binom{n\deg\bar{V}+1}{m+1}$ and $\mathfrak{M}$ can be constructed in time which is polynomial in $\operatorname{card}\mathfrak{M}$.

We note finally that the coefficients of the linear forms of elements of $\mathfrak{M}$ can be chosen to be integral if card (F) = 0 or from a small finite field if $\operatorname{char}(F)>0$, so that the length of description of these coefficients is bounded above by a polynomial in n, $\log(\deg\bar{V})$.

2. Case of a Finite Number of Roots of the System in Projective Space

This case was considered in [17, 18]. In the present section we formulate the results of these papers with modifications necessary for our further goals. We consider systems of homogeneous equations and we use the concepts and notation introduced in the preceding section. In [17], with the help of homological methods the following theorem is proved (cf. also [18]).

THEOREM 2.1 [17]. Let $g_0,\ldots,g_{k-1}\in F[X_0,\ldots,X_n]$ and the system of homogeneous equations $g_0=\ldots=g_{k-1}=0$ have no roots in $\mathbb{P}^n(\bar{F})$. Then the ideal $(g_0,\ldots,g_{k-1})\supset(X_0,\ldots,X_n)^D$, for $D=\delta_0'+\sum_{1\leqslant i\leqslant\min(k-1,n)}(\delta_i'-1)$, where $\delta_0'=\deg g_0\geqslant\delta_1'=\deg g_1\geqslant\ldots$

This estimate is better than the estimate from [14]. We note that it is sharp.

Now let $f_0,\ldots,f_{k-1}\in F[X_0,\ldots,X_n]$ be homogeneous polynomials of degree $\delta_0'\geqslant\ldots\geqslant\delta_{k-1}'$, respectively. We introduce new variables $U_0,\ldots,U_n$, algebraically independent over $F(X_0,\ldots,X_n)$. We set $f_k=X_0U_0+\ldots+X_nU_n\in F(U_0,\ldots U_n)[X_0,\ldots,X_n]$ and $D=(\sum_{1\leqslant i\leqslant\min(k-1,n)}(\delta_i'-1))+\delta_0'$, where $\delta_k'=1$. We consider the map $\mathfrak{A}:\mathcal{H}_0\oplus\ldots\oplus\mathcal{H}_k\to\mathcal{H}$, which is linear over the field $F(U_0,\ldots,U_n)$ where $\mathcal{H}_i$ (respectively, $\mathcal{H}$) is the space of homogeneous polynomials in $X_0,\ldots,X_n$ over $F(U_0,\ldots,U_n)$ of degree $D-\delta_i'$ (respectively, D) for $0\leqslant i\leqslant k$, namely, $\mathfrak{A}(h_0,\ldots,h_k)=\sum_{0\leqslant i\leqslant k}h_if_i$. An arbitrary element $h=(h_0,\ldots,h_k)\in\mathcal{H}_0\oplus\ldots\oplus\mathcal{H}_k$ can be written in the form h $h=(h_{0,1},\ldots,h_{0,s_0},h_{1,1},\ldots,h_{1,s_1},\ldots,h_{k,1},\ldots h_{k,s_k})$, where $s_i=\binom{n+D-\delta_i'}{n}$ and $h_{i,1},\ldots,h_{i,s_i}$ are the coefficients of the polynomial h_i, under the condition that some enumeration of the polynomials of degree $D-\delta_i'$ is fixed. One describes the elements of the space $\mathcal{H}$ analogously. In the chosen coordinate systems the map $\mathfrak{A}$ has matrix A of size $\binom{n+D}{n}\times(\sum_{0\leqslant i\leqslant k}s_i)$. One can represent the matrix A in the form A = (A', A"), where A' contains $\sum_{0\leqslant i\leqslant k-1}\delta_i$ columns, A" contains s_k columns; moreover, the elements of A' belong to F. The elements of A" are linear forms over F in the variables $U_0,\ldots,U_n$. The following result is found in [18], based on Theorem 2.1.

THEOREM 2.2. 1) The system $f_0=\ldots=f_{k-1}=0$ has a finite number of solutions in $\mathbb{P}^n(\bar{F})$ if and only if $\mathrm{rg}(A)=\binom{n+D}{n}$ [we let $r=\binom{n+D}{n}$].

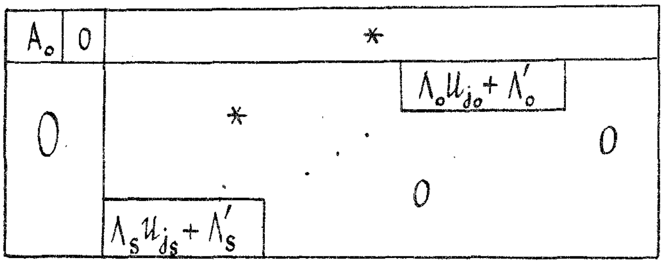
2) All $r \times r$ minors of the matrix A together generate a principal ideal, whose generator R is their greatest common divisor.

3) The homogeneous form R in $U_0, \dots, U_n$ decomposes into a product $R = \prod_{1 \leqslant i \leqslant \mathcal{D}_1} L_i$, where $L_i = \sum_{0 \leqslant j \leqslant n} \xi_j^{(i)} U_j$ is a linear form with coefficients from $\bar{F}$, besides this $(\xi_0^{(i)} : \dots : \xi_n^{(i)}) \in \mathbb{P}^n(\bar{F})$ is a root of the system, and the number of occurrences of forms proportional to L_i in the product is equal to the multiplicity of the corresponding root of the system $(1 \leqslant i \leqslant \mathcal{D}_1)$.

Thus, R coincides with the u-resultant [1] up to a factor from $\bar{F}$ if k = n.

Initially as the input of the algorithm given in [18] the system $f_0 = \dots = f_{k-1} = 0$ is given. On the basis of Theorem 2.2, the algorithm establishes whether the system has a finite number of roots in $\mathbb{P}^n(\bar{F})$ and if the answer is positive, then as output it lists all the roots together with their multiplicities.

The algorithm of [18] reduces the matrix A (cf. Sec. 2 of [13]) by elementary row and column transformations over F to the form


A_0
0
*
$\Lambda_0 U_{j_0} + \Lambda_0'$
0
*
0
0
$\Lambda_s U_{j_s} + \Lambda_s'$

where A_0 is a nonsingular upper triangular matrix with coefficients from F, the matrices $\Lambda_0, \dots \Lambda_s$ are diagonal nonsingular with coefficients from F of sizes $\lambda_0, \dots, \lambda_s$, respectively, the elements of the matrices Λ_i' are linear forms over F with respect to the variables U_j, $j > j_i$ (for all $0 \leqslant i \leqslant s$). Here and below we assume, without loss of generality, that $rg\, A = \binom{n+D}{n}$, since otherwise the algorithm detects that $rg\, A < \binom{n+D}{n}$ in the course of its work and stops.

The algorithm mentioned for reduction of the matrix works in a number of arithmetic operations over the elements of a field F which is a polynomial in the size of the matrix A. Consequently, we get a polynomial algorithm for the case of a finite field F. For other fields it is impossible in general to assert that the algorithm works in time which is proportional in the length of description of the matrix A, so some additional considerations are necessary.

In the given matrix each minor of maximal order det $\binom{n+D}{n}$ is divisible by the product $det(\Lambda_0 U_{j_0} + \Lambda_0') \cdot \dots \cdot det(\Lambda_s U_{j_s} + \Lambda_s')$. Consequently, $R = det(A_0) det(\Lambda_0 U_{j_0} + \Lambda_0') \cdot \dots \cdot det(\Lambda_s \cdot U_{j_s} + \Lambda_s')$. The number D_1 of roots, considering their multiplicities, of the original system is equal to $\sum_{0 \leqslant i \leqslant s} \lambda_s$ according to point 3) of Theorem 2.2. We fix some pair of indices $0 \leqslant \alpha_1 < \alpha_2 \leqslant n$. The form $R \in F[U_0, \dots, U_n]$ can be represented in the form of a product $R = R_1 R_2$, where R_2 is the product of all the linear forms L_i (cf. Theorem 2.2), for which one has $\xi_{\alpha_1}^{(i)} = \xi_{\alpha_2}^{(i)} = 0$. Then $R_2 \in F[U_0, \dots, U_{\alpha_1}, \dots, U_{\alpha_2}, \dots, U_n]$ and $R_1 \in F[U_0, \dots, U_n]$

up to an appropriate factor from $\bar{F}$, which we can assume equal to 1 without loss of generality (a roof over a variable indicates the absence of this variable).

We note that $\deg_{U_0,\dots U_n}(R)=r-rg(A')$ (we recall that A' is the matrix with coefficients from F consisting of the first $\sum_{0\leq i\leq k-1} s_i$ columns of the matrix A). It follows from this that R coincides (up to a factor from F^*) with any nonzero minor of size r of the matrix A, which contains rg(A') columns of the submatrix A'.

Our goal is to give an algorithm which is polynomial with respect to the length of description of the matrix A, which calculates $R_1(0,\dots,0,U_{\alpha_1},0,\dots,0,U_{\alpha_2},0,\dots,0)\in F[U_{\alpha_1},U_{\alpha_2}]$, or gives the answer that the original system has infinitely many solutions (by calculating a polynomial, we mean here and later calculating its coefficients). This algorithm works for a sufficiently broad class of fields F, in particular for finite primitive extensions of purely transcendental extensions of primitive fields. For convenience of notation we renumber the variables $U_0,\dots, U_n$ so that U_{α_1}, U_{α_2} get the indices 0 and 1, respectively. We start with the case when $F=H(T_1,\dots,T_\ell)$ is a purely transcendental extension $(\ell \geqslant 0)$.

Now let H_1 be some finite field such that $(n-2)D_1 < card(H_1) \leqslant q(n-1)\, D_1$, where q = char ($H_1$) if $q=char(F) > 0$. In this case we extend the field F to the composite of the fields F and H_1 and we assume further that $H_1 \subset F$. In the case of characteristic zero we let $H_1=\mathbb{Z}$.

Using Lemma 2.1 of Sec. 1, one can construct a family of $N=((n-2)D_1 + 1)$ vectors $v^{(1)}=(v_1^{(1)},\dots,v_{n-1}^{(1)}),\dots,v^{(N)}=(v_1^{(N)},\dots, v_{n-1}^{(N)})\in H_1^{n-1}$, any n − 1 of which are linearly independent. Now we show that for some $1 \leqslant i \leqslant N$ the polynomial $R(U_0,U_1,v_1^{(i)},\dots,v_{n-1}^{(i)})\in F(U_0,U_1)$ is different from zero. If this is not so, then by Dirichlet's principle for at least one of the linear forms $L_m={}_{0\leqslant j\leqslant n}\sum \xi_j^{(m)} U_j$ (cf. Theorem 2.2), for which $\xi_0^{(m)}=\xi_1^{(m)}=0$ and for (n − 1) vectors among $v^{(1)},\dots, v^{(N)}$ (let them be $v^{(1)},\dots,v^{(n-1)}$) one has $L_m(0,0,v_1^{(i)},\dots,v_{n-1}^{(i)})=0$, $1\leqslant i \leqslant n-1$, which contradicts the linear independence of the vectors $v^{(1)},\dots,v^{(n-1)}$.

The algorithm calculating $R_1(U_0,U_1,0,\dots, 0)$ considers in turn $v^{(1)},\dots, v^{(N)}$ and finds $R(U_0,U_1,v_1^{(i)},\dots,v_{n-1}^{(i)})$ for $1 \leqslant i \leqslant N$. For some i the polynomial $R(U_0,U_1,v_1^{(i)},\dots,v_{n-1}^{(i)})\neq 0$. Then $R_1(U_0,U_1,0,\dots,0)$ coincides with the form of highest degree of the polynomial $R(U_0,U_1, v_1^{(i)},\dots,v_{n-1}^{(i)})$ (up to a factor from H_1* or $\mathbb{Q}^*$). In the case of characteristic zero, by the construction of Lemma 2.1 one can take $v_j^{(i)}=i^j \leqslant N^{n-1}$, so the length of description $\ell(v_j^{(i)})$ is polynomial, and hence the vectors $v^{(1)},\dots,v^{(N)}$ can be substituted into R in polynomial time (analogously, the same thing is true in the case of nonzero characteristic). Further, we fix an index i and for brevity we let $v_1=v_1^{(i)},\dots,v_{n-1}=v_{n-1}^{(i)}$ and we shall calculate the polynomial $R(U_0,U_1,v_1,\dots,v_{n-1})$.

For this we apply Gauss' algorithm (cf. [14]) over the field $F(U_0,U_1)$ to the matrix $A(U_0,U_1,v_1,\dots,v_{n-1})$. The algorithm is determined by the sequence of choices of leading elements. If A_i is the result of performing the i-th step $(i\geqslant 0, A_0=A(U_0,U_1,v_1,\dots,v_{n-1}))$ and $0\neq a_{\alpha_i\beta_i}^{(i)}$ is the element of the matrix A_i chosen as the leading one at this step, then the element $a_{\gamma,\delta}^{(i+1)}=a_{j,\delta}^{(i)}-a_{\alpha_i\delta}^{(i)}a_{\gamma,\beta_i}^{(i)}/a_{\alpha_i,\beta_i}^{(i)}$ for $\gamma\neq\alpha_0,\dots,\alpha_i$. We denote by $\Delta_{i_1\dots i_m}^{j_1,\dots j_m}$ the determinant of the $m \times m$ submatrix of the matrix $A(U_0, U_1, V_1, \ldots, V_{n-1})$, spanned by the rows with indices $i_1, \ldots i_m$ and columns with indices $j_1, \ldots, j_m$.

LEMMA 2.4 (cf., e.g., [14]). One has $a^{(i+1)}_{\gamma\delta} = \Delta^{\beta_0, \ldots, \beta_i \delta}_{\alpha_0, \ldots, \alpha_i \gamma} / \Delta^{\beta_0, \ldots, \beta_i}_{\alpha_0, \ldots, \alpha_i}$ for $\gamma \neq \alpha_0, \ldots, \alpha_i$ and $\delta \neq \beta_0, \ldots, \beta_i$; further, $a^{(i+1)}_{\gamma, \beta_i} = 0$ for $\gamma \neq \alpha_0, \ldots \alpha_i$. Finally, $a^{(i+1)}_{\gamma\delta} = a^{(i)}_{\gamma\delta}$ for all other pairs γ, δ.

The lemma can be proved by induction on i.

Applying the Gauss algorithm to the matrix $A(U_0, U_1, V_1, \ldots, V_{n-1})$, we choose leading elements so that at the i-th step β_i should be as small as possible. Then if $rg(A(U_0, U_1, V_1, \ldots, V_{n-1}) = r$, one has $0 \neq R(U_0, U_1, V_1, \ldots, V_{n-1}) = \Delta^{\beta_0, \ldots, \beta_{r-1}}_{\alpha_0, \ldots \alpha_{r-1}}$ according to the remark above; we recall that A = (A', A"), where A' is a matrix with coefficients from F, the coefficients of the matrix A" are linear forms in $U_0, \ldots, U_n$. Now if $0 = R(U_0, U_1, V_1, \ldots, V_{n-1})$, then the algorithm turns to the consideration of the following vector $V^{(i+1)}$. The time of working in realizing the Gauss algorithm can be estimated by Lemma 2.4 by a polynomial in $(rd_2+1)^{\ell+1} M_2$, where, we recall, $r = \binom{D+n}{n}$, $deg_{T_1, \ldots, T_\ell}(f_i) \leq d_2$ and $\ell(f_i) \leq M_2$ (see Introduction).

There is another method for calculating $R(U_0, U_1, V_1, \ldots, V_{n-1})$ in Sec. 3 of [9]; it is based on interpolation [21] and uses the Gauss algorithm only for the case when F is a finite field.

We note that $deg_{T_1, \ldots, T_\ell} R(U_0, U_1, V_1, \ldots, V_{n-1}) \leq rd_2$ and on the basis of Hadamard's inequality one can deduce that $\ell(R(U_0, U_1, v_1, \ldots, v_{n-1})) \leq r(M_2 + \ell \log d_2 + \log r)$.

Now let $F = K[\eta]$ and $\varphi(\eta) = 0$, where $\varphi \in K[Z]$ and φ is irreducible over K, where K is a pure transcendental extension of transcendence degree ℓ over $\mathbb{Q}$ or over a finite field (cf. Introduction). We consider a transcendental extension $K \subset K(T)$ and we calculate the polynomial $R(U_0, U_1, v_1, \ldots, v_{n-1})$ under the condition that in the matrix A the element T is substituted for η. We assume that each element of the matrix A is represented as an element of K[T] of degree in T less than $deg(\varphi)$. Then we sustitute η in reverse for T in $R(U_0, U_1, v_1, \ldots, v_{n-1})$ and we reduce it mod φ. The calculation of $R(U_0, U_1, v_1, \ldots, v_{n-1})$ requires time no greater than some polynomial in $(r(d_1+d_2)+1)^{\ell+1}$ and the length of description of the initial data (including φ), i.e., of $(M_1+M_2)(r(d_1+d_2)+1)^{\ell+1}$ (we recall, cf. Introduction, that $deg_{T_1, \ldots, T_\ell}(\varphi) < d_1, \ell(\varphi) \leq M_1$). We note also that $deg_{T_1, \ldots, T_\ell}(R(U_0, U_1, v_1, \ldots, v_{n-1})) \leq r(d_1^2 + d_2)$ and $\ell(R(U_0, U_1, v_1, \ldots, v_{n-1})) \leq O(r d_1((\ell+1) \log d_1 + M_1) + d n r^2 \log(nr) + r(M_2 + \ell \log d_2))$.

Thus, we have finished the description of the process of calculating the polynomial $R_1(U_0, U_1, 0, \ldots, 0)$. Now we begin to calculate the linear forms $L_i = \sum_{0 \leq j \leq n} \xi^{(i)}_j U_j$ (cf. Theorem 2.2). We assume further that the field $F = H(T_1, \ldots, T_\ell)[\eta]$ is the same as in the Introduction.

In what follows, all arguments about nonseparability relate to the case $q = char(F) > 0$. We fix a pair of indices $0 \leq j'_0 < j'_1 \leq n$. Again, as above, one can assume without loss of generality that $j'_0 = 0, j'_1 = 1$. Since $(\xi^{(\varepsilon)}_0 U_0 + \xi^{(\varepsilon)}_1 U_1) | R_1(U_0, U_1, 0, \ldots, 0)$, we get that $R_1(\xi^{(\varepsilon)}_1, -\xi^{(\varepsilon)}_0, 0, \ldots, 0) = 0$. Considering that $R_1(U_0, U_1, 0, \ldots, 0)$ is a homogeneous polynomial of degree no greater than D_1, we get that the element $\xi^{(\varepsilon)}_1/\xi^{(\varepsilon)}_0$ (if $\xi^{(\varepsilon)}_0 \neq 0$) has degree over the field F no greater than D_1. Consequently, its degree of nonseparability over F is all the more no greater than D_1. Let $\mathcal{D}_1/q < q^{\mu} \leq \mathcal{D}_1$. If the characteristic q = 0, then here and below we set $q^{\mu}=1$ for convenience of notation. Then any element $(\xi^{(\varepsilon)}_{j_1}/\xi^{(\varepsilon)}_{j_0})^{q^{\mu}}$ is separable over F (if $\xi^{(\varepsilon)}_{j_0} \neq 0$). We consider further the new system of algebraic equations, obtained by replacing each coefficient of the original system by its q^{μ} power. After this change the degrees with respect to each T_i $(1 \leq i \leq \ell)$ if the coefficients of the system are multiplied by $q^{\mu} \leq \mathcal{D}_1$. For the new system the ratio of any pair of coordinates in the forms L_{ε} will be separable over F, namely, this ratio coincides with $(\xi^{(\varepsilon)}_{j_1}/\xi^{(\varepsilon)}_{j_0})^{q^{\mu}}$ for the corresponding j_0, j_1. If we solve the new system, then in order to find a solution of the original system we have to calculate the elements $(\xi^{(\varepsilon)}_{j_1}/\xi^{(\bar{\varepsilon})}_{j_0})$, starting from the elements $(\xi^{(\varepsilon)}_{j_1}/\xi^{(\varepsilon)}_{j_0})^{q^{\mu}} \in F[\theta']$ found, where θ' is a separable element over F, which will be constructed by the algorithm. Besides this, we show further that $[F[\theta'] : F] \leq \mathcal{D}_1$ and for the minimal polynomial $\Phi(Z)$ of the element θ' over F with leading coefficient $lc_Z(\Phi)=1$, the degree $\deg_{T_1,\dots,T_\ell}\Phi$ can be bounded above by a polynomial in $\tau=\binom{\mathcal{D}+n}{n}$, d_2, d_1, while the polynomial has degree 1 with respect to d_2 (we represent $\Phi=\sum_i \left(\sum_{0\leq j<\deg_Z(\varphi)} \frac{a_{ij}(T_1,\dots,T_\ell)}{b(T_1,\dots,T_\ell)}\eta^j\right) Z^i$, where $a_{ij}, b \in H[T_1,\dots,T_\ell]$ and $\deg_{T_1,\dots,T_\ell}(b)$ is the smallest possible, and we set $\deg_{T_1,\dots,T_\ell}\Phi = \max_{i,j}\{\deg_{T_1,\dots,T_\ell}(a_{ij}), \deg_{T_1,\dots,T_\ell}(b)\}$ (cf. Introduction). In what follows we write the elements of the field F[θ] in the form g(θ'), where $g \in F[Z]$ and $\deg_Z(g) < \deg_Z(\Phi)$.

We estimate the degrees with respect to $T_1,\dots,T_\ell$ of the element $(\xi^{(\varepsilon)}_1/\xi^{(\varepsilon)}_0)^{q^{\mu}} = \xi^{q^{\mu}}$. Since the polynomial $(Z-\xi^{q^{\mu}}) \mid R_1(Z,-1,0,\dots,0)$ (here the polynomial R_1 corresponds to the new system), we can apply Chapter I of [4] to the polynomial $R_1(Z,-1,0,\dots,0) \in F[\theta'][Z]$ and the separable extension $F \subset F[\theta']$. Then, keeping in mind that $\deg_{T_1,\dots,T_\ell}R_1(Z,-1,0,\dots,0) \leq \tau(d_1^2+d_2)$ and $\deg_Z R_1 (Z,-1,0,\dots,0) \leq \mathcal{D}_1$ according to Chapter I of [4] and the bounds on $\deg_{T_1,\dots,T_\ell}\Phi, \deg_Z\Phi$ mentioned above, one can also estimate $\deg_{T_1,\dots,T_\ell}(\xi^{q^{\mu}})$ from above by a polynomial in τ, d_1, d_2 of the first degree relative to d_2.

Now we decompose $Z^{q^{\mu}}-\xi^{q^{\mu}}$ into factors over the field F[θ'], applying Chapter I of [4] to the separable extension of the field $F \subset F[\theta']$. The decomposition has the form $Z^{q^{\mu}}-\xi^{q^{\mu}} = (Z^{q^{\nu}}-\xi^{q^{\nu}})^{q^{\mu-\nu}}$, where $\xi^{q^{\nu}} \in F[\theta']$; then $\xi^{q^{\nu-1}} \notin F[\theta']$ (here and below in similar cases we assume $q>0$). Then the extension of the original system corresponding to the linear form L_{ε}, can be represented by the vector $(\xi^{(\varepsilon)}_0,\dots,\xi^{(\varepsilon)}_n)$, where the elements $(\xi^{(\varepsilon)}_{j_1}/\xi^{(\varepsilon)}_{j_0})^{q^{\nu_{j_0 j_1}}} \in F[\theta']$ are given, while $\nu_{j_0 j_1}$ is such that $(\xi^{(\varepsilon)}_{j_1}/\xi^{(\varepsilon)}_{j_0})^{q^{\nu_{j_0 j_1}-1}} \notin F[\theta']$ (all of this under the condition that $\xi^{(\varepsilon)}_{j_0} \neq 0$). By what was just said, we shall assume in what follows, without loss of generality (raising the coefficients of the original system to the power q^{μ}, if this is necessary), that for any linear form $(\xi^{(\varepsilon)}_{j_0}U_{j_0}+\xi^{(\varepsilon)}_{j_1}U_{j_1}) \mid R_1(0,\dots,0,U_{j_0},0,\dots,0,U_{j_1},0,\dots,0)$ the element $\xi^{(\varepsilon)}_{j_1}/\xi^{(\varepsilon)}_{j_0}$ is separable over F (under the condition that $\xi^{(\varepsilon)}_{j_0} \neq 0$) for any ε, j_0, j_1.

Further, to solve the system we shall follow the general plan of [18]. First of all we calculate the polynomial $R_1(U_0,U_1,0,\dots,0)$ with the help of the algorithm given above. Then we decompose it over F into irreducible factors (cf. Chapter I of [4]). Let $h_1(U_0,U_1) \mid R_1(U_0,U_1,0,\dots,0)$ be some factor which is irreducible over F (the algorithm being described considers all irreducible factors) different from U_1 (in this case, if $(\xi_0^{(\varepsilon)}U_0 + \xi_1^{(\varepsilon)}U_1) \mid h_1$, $\xi_0^{(\varepsilon)} \neq 0$). We note that the construction of [4] leads to an upper bound on $\deg_{T_1,\ldots,T_\ell}(h_1)$ which is polynomial in r , d_2 , d_1 and in addition of the first degree with respect to d_2, and to an upper bound on the length $l(h_1)$ of description of the coefficients which is polynomial in $M_1 + M_2 + \ell d_2$, r, d_1, and this polynomial has degree 1 with respect to $M_1 + M_2 + \ell d_2$. The procedure given below finds all the forms L_ε satisfying the condition $\xi_0^{(\varepsilon)} \neq 0$. To find all forms, it suffices after this to find the forms satisfying the condition $\xi_1^{(\varepsilon)} \neq 0$ and to choose among them the forms for which $\xi_0^{(\varepsilon)} = 0$ (or one can add the equation $X_0 = 0$ to the original system), etc. We set $g_1(Z) = h_1(Z,-1) \in F[Z]$; then $g_1(\xi_1^{(\varepsilon)}/\xi_0^{(\varepsilon)}) = 0$. We let $F_1 = F[\theta_1] = F[Z]/(g_1(Z))$, where $g_1(\theta_1) = 0$ and $\theta_1' = \theta_1$, $\Phi_1 = g_1$. The construction of F_1, θ_1, θ_1', Φ_1 completes the description of the first step of the procedure. We can assume without loss of generality that $\operatorname{card}(H) \geqslant \delta = d_1 \mathfrak{D}_1$ (otherwise we can extend the finite field H, as before in similar situations).

Let (s − 1) steps of the procedure be made already. The following s-th step starts with the addition to the system obtained at the (s − 1)-st step of the equation $\theta_{s-1}X_0 - X_{s-1} = 0$ (throughout the s-th step the polynomial R_1 corresponds to this new system). Then we calculate the polynomial $R_1(U_0, 0, \ldots, 0, U_s, 0, \ldots, 0)$ and we find a factor $h_s(U_0, U_s) \mid R_1(U_0, 0, \ldots, 0, U_s, 0, \ldots, 0)$ which is irreducible over the field F_{s-1} , constructed at the (s − 1)-st step (cf. [4]); the algorithm considers all irreducible factors h_s. We let $g_s = h_s(Z,-1)$. Then $g_s(\xi_s^{(\varepsilon)}/\xi_0^{(\varepsilon)}) = 0$. Let $F_s = F_{s-1}[\theta_s] = F_{s-1}[Z]/(g_s(Z))$, where $g_s(\theta_s) = 0$ (as θ_i, of course, one can take $\xi_i^{(\varepsilon)}/\xi_0^{(\varepsilon)}$ for some ε and any $1 \leqslant i \leqslant s$).

We consider the elements $\theta_{s-1}' + c_1\theta_s, \ldots, \theta_{s-1}' + c_\delta\theta_s$, where $0 = c_1, \ldots, c_\delta \in H$ are pairwise distinct (in the case of characteristic zero we take $c_i = i-1$). At least one of these elements is a primitive element for F_s over F (cf. [6]). For each of $\theta_{s-1}' + c_{\gamma_\varkappa}\theta_s$, $1 \leqslant \gamma_\varkappa \leqslant \delta$ the algorithm constructs the minimal polynomial over F. For this it is necessary to solve the question of the linear dependence over F of the powers 1, $\theta_{s-1}' + c_{\gamma_\varkappa}\theta_s$, $(\theta_{s-1}' + c_{\gamma_\varkappa}\theta_s)^2, \ldots, (\theta_{s-1}' + c_{\gamma_\varkappa}\theta_s)^s$. These powers can be expanded with respect to the basis $(\theta_{s-1})^\alpha \theta_s^\beta$ where $0 \leqslant \alpha < \deg \Phi_{s-1}$, $0 \leqslant \beta < \deg g_s$ and the question reduces to the solution of a linear system over F. Moreover, the degrees with respect to $T_1, \ldots, T_\ell$ of solutions of the system, i.e., of the coefficients of the minimal polynomial, are bounded above by a polynomial (independent of i) in r, d_2, d_1 (of degree one with respect to d_2) and in $\max\{\deg_{T_1,\ldots,T_\ell}(\Phi_{s-1}), \deg_{T_1,\ldots,T_\ell}(g_s)\}$. Moreover, the length of description of the coefficients of the monomials in $T_1, \ldots, T_\ell, \eta$ can be bounded above by a polynomial in $r, d_1, (M_1 + M_2 + \ell d_2)$ of degree 1 with respect to $(M_1 + M_2 + \ell d_2)$. We denote by θ_s' the primitive element constructed of the form $\theta_{s-1}' + c_{\gamma_\varkappa}\theta_s$ of the field F_s over F, and by $\Phi_s(Z) \in F[Z]$ its minimal polynomial, $\Phi_s(\theta_s') = 0$.

Now we prove that the degrees $\deg_{T_1,\ldots,T_\ell}(\Phi_s)$ (the length of description of the coefficients $l(\Phi_s)$, respectively) can be bounded above by a polynomials in r, d_2, d_1 of degree 1 with respect to d_2 (in $r, d_1, (M_1 + M_2 + \ell d_2)$ of degree 1 with respect to $(M_1 + M_2 + \ell d_2)$, respectively), independent of s. We note that by construction $\theta_s' = \theta_1 + \sum_{2 \leqslant \varkappa \leqslant s} \gamma_\varkappa \theta_\varkappa$ and $\theta_\varkappa = \xi_\varkappa^{(\varepsilon)}/\xi_0^{(\varepsilon)}$ for some ε, where $\gamma_\varkappa \in H$ and $0 \leqslant \gamma_\varkappa \leqslant \delta - 1$, when char (F) = 0, for $1 \leqslant \varkappa \leqslant s$. We consider the auxiliary system of equations obtained from the original one by a nondegenerate linear change of variables under which $X_0 \rightarrow X_0$, $X_1 + \sum_{2 \leq \varkappa \leq s} \gamma_\varkappa X_\varkappa \longrightarrow X_1$. Then the roots of the auxiliary system are the vectors $(\xi_0^{(\rho)}, \xi_1^{(\rho)} + \sum_{2 \leq \varkappa \leq s} \gamma_\varkappa \xi_\varkappa^{(\rho)}, \dots)$ for all $1 \leq \rho \leq \mathcal{D}_1$. One can choose the linear substitution so that the length of description of the coefficients of the auxiliary system are bounded above by $\mathcal{O}(M_2 + l \log d_2 + \log \delta)$. For the auxiliary system the element $\theta_1 + \sum_{2 \leq \varkappa \leq s} \gamma_\varkappa \theta_\varkappa = \xi_1 / \xi_0 + \sum_{2 \leq \varkappa \leq s} \gamma_\varkappa \xi_\varkappa^{(\varepsilon)} / \xi_0^{(\varepsilon)}$ is a root of the polynomial $R_1(Z, -1, 0, \dots, 0)$, corresponding to the auxiliary system. Consequently, arguing as above, one can get the upper bound wanted, independent of s, by the degrees with respect to $T_1, \dots, T_l$ and the length of description of the coefficients of the polynomial Φ_s .

Now we let $\theta' = \theta'_n$, $\Phi = \Phi_n$. We show that the ratios sought $\xi_j^{(\rho)} / \xi_0^{(\rho)}$ of the original system can be expressed in terms of the basis $1, \theta', (\theta')^2, \dots$ with coefficients from the field F, and here the degrees with respect to $T_1, \dots, T_l$ of these coefficients are bounded above by a polynomial in r, d_2, d_1 of degree 1 with respect to d_2 and the lengths of description of the coefficients in the monomials in $T_1, \dots, T_l, \overset{2}{\theta}, \theta'$ are bounded above by a polynomial in $(M_1 + M_2 + l \quad d_2), d_1, r$ of degree 1 with respect to $(M_1 + M_2 + l \quad d_2)$. Moreover, the polynomials of these estimates are independent of ρ, j. For any s we decompose the polynomial $g_j(Z) = R_1(Z, 0, \dots, 0, -1, 0, \dots, 0)$ (here $j \leq s$) over the field $F_s = F[\theta'_s]$ according to Chapter I of [4]. Then $g_j(\theta_j) = 0$ for $j \leq s$, so $(Z - \theta_j) | g_j$. From this it follows [4] that the degrees $\deg_{T_1, \dots, T_l}(\theta_j)$ in the expressions of θ_j as an element of the field $F[\theta'_s]$ (the length of description of the coefficients of θ_j, respectively) can be bounded above by a polynomial in r, d_2, d_1 of degree 1 with respect to d_2 (by a polynomial in $(M_1 + M_2 + l \quad d_2), r, d_1$ of degree 1 with respect to $(M_1 + M_2 + l \quad d_2)$, respectively) and, moreover, these estimates are independent of s, j, ρ.

Now we show by induction on s that one can express θ_j $(1 \leq j \leq s)$ in terms of powers of the element θ_s' in time which is polynomial in $M_1 M_2 (r d_2 d_1)^{l+1}$, and, moreover, the polynomial giving the estimate is independent of s, j, ρ.

Let the expressions for θ_j $(1 \leq j \leq s-1)$, as elements of the field $F[\theta'_{s-1}]$, be found already. Since $\theta'_s = \theta'_{s-1} + \gamma_s \theta_s$, using the polynomials Φ_{s-1}, g_s (cf. above), we find decompositions of the elements $1, \theta'_s, (\theta'_s)^2, \dots$ with respect to the basis $(\theta'_{s-1})^\alpha \theta_s^\beta$ with coefficients from the field F, where $0 \leq \alpha < \deg(\Phi_{s-1})$, $0 \leq \beta < \deg(g_s)$. Solving a linear system over F, one can find the decompositions of θ_s, θ'_{s-1} with respect to the basis $1, \theta'_s, (\theta'_s)^2, \dots$. After this, substituting into the expressions for $\theta_1, \dots, \theta_{s-1}$ in the field $F[\theta'_{s-1}]$ the expression found for θ'_{s-1} , we get what is required. The expressions constructed for θ_j $(1 \leq j \leq n)$ satisfy the estimates given above, so the time of construction of all θ_j (as elements of the field $F[\theta']$) is polynimial in $M_1, M_2, (r d_2 d_1)^{l+1}, \kappa, q$.

Now we somewhat alter the primitive element $\theta' = \sum_{j'_0 < j \leq n} \gamma_j (\xi_j / \xi_{j'_0})^{q^\mu}$ (here $\xi_j = \xi_j^{(\varepsilon)}$ and $\xi_\varkappa^{(\varepsilon)} = 0$ for $\varkappa < j'_0$). Namely, we set $q^\nu = \max_j \{ q^{\nu_{j j'_0}} \}$ and $\theta'' = (\theta')^{q^{\nu - \mu}} = \sum_{j'_0 < j \leq n} \gamma_j^{q^{\nu - \mu}} (\xi_j / \xi_{j'_0})^{q^\nu}$. Then $F[\theta''] = F[\theta']$.

<u>Remark</u>. We note that if $F[(\xi_{j'_0+1}^{(\varepsilon)} / \xi_{j'_0}^{(\varepsilon)})^{q^\nu}, \dots, (\xi_n^{(\varepsilon)} / \xi_{j'_0}^{(\varepsilon)})^{q^\nu}] = F[(\xi_{j'_0+1}^{(\varepsilon)} / \xi_{j'_0}^{(\varepsilon)})^{q^\nu}]$, i.e., $\theta_1 = (\xi_{j'_0+1}^{(\varepsilon)} / \xi_{j'_0}^{(\varepsilon)})^{q^\mu}$ is a primitive element, then $\theta' = \theta_1$ according to our construction of a primitive element,

since $c_1 = 0$, while the polynomial $g_1^{(\varepsilon)} = g_1$ coincides with $\Phi_{n-j_0} = \Phi = \Phi^{(\varepsilon)}$ (cf. the notation above; the superscript ε means that we consider L_ε), is irreducible over F, and $g_1(\theta_1) = 0$. Moreover, if $\xi_0^{(\varepsilon)} \neq 0$ for any ε, i.e., for any root of the original system, then for any fixed pair of indices $j_0' = 0$, j_1' the corresponding polynomial $R_1 = R$. Moreover, if $(\xi_1^{(\varepsilon)} / \xi_0^{(\varepsilon)})^{q^\mu}$ is a primitive element for any ε, whose minimal polynomial over F is $\Phi^{(\varepsilon)} | R_1(Z, -1, 0, \ldots, 0)$ (here $R_1, g_1 = \Phi^{(\varepsilon)}$ correspond to the modified system obtained from the original by raising its coefficients to the q^μ-th power; see above), then $R = R_1$ for the pair $j_0' = 0$, $j_1' = 1$ and the product $\prod_{\bar{\varepsilon}} (\Phi^{(\varepsilon)})^{e_{\bar{\varepsilon}}} = R(Z, -1, 0, \ldots, 0)$ up to a factor from F^*, where $\bar{\varepsilon}$ runs through the set of conjugacy classes over F of roots of the system ($\bar{\varepsilon}$ corresponds to ε). Finally, according to the construction given above, to each conjugacy class over F of roots of the original system there corresponds a polynomial $\Phi^{(\varepsilon)}$ with suitable ε and, conversely, to each polynomial $\Phi^{(\varepsilon)}$ there corresponds here a conjugacy class of roots (not necessarily unique). The polynomials $\Phi^{(\varepsilon)}$ can coincide for different $\bar{\varepsilon}$. The exponents of the degrees $e_{\bar{\varepsilon}}$ are equal to the multiplicities of the linear form L_ε in the polynomial R (see Theorem 2.2 above).

This remark is due to A. L. Chistov and is not used here.

We summarize the results of the present section in the following theorem, which is a modification of the theorem of [18].

<u>THEOREM 2.3</u>. Suppose given a system of homogeneous equations $f_0 = \ldots = f_{k-1} = 0$, where $f_i \in F[X_0, \ldots, X_n]$, $\deg f_i = \delta_i'$, $\delta_0' \geqslant \delta_1' \geqslant \ldots \geqslant \delta_{k-1}'$ (without loss of generality, $n \leqslant k$), where the field $F = H(T_1, \ldots, T_\ell)[\eta]$; $H = \mathbb{Q}$ or H is a finite field of characteristic $q > 0$; $T_1, \ldots, T_\ell$ are algebraically independent over H; η is an algebraic and separable element over $H(T_1, \ldots, T_\ell)$ with minimal polynomial $\varphi(Z) \in H(T_1, \ldots, T_\ell)[Z]$, $\varphi(\eta) = 0$. We let $\mathcal{D} = \delta_0' + \sum_{1 \leqslant i \leqslant \min(k-1, n)} (\delta_i' - 1)$, $\tau = \binom{\mathcal{D}+n}{n}$, $(d_1 - 1) = \deg_{T_1, \ldots, T_\ell, Z}(\varphi)$; by $d_2 - 1$ we denote the degree with respect to $T_1, \ldots, T_\ell$ of the coefficients of the system (see Introduction), by M_2 (respectively, M_1) we denote the maximum of the lengths of description of the coefficients of the monomials in $T_1, \ldots \ldots, T_\ell, \eta$ in the system (respectively, in φ).

An algorithm is constructed which first determines whether the system has a finite number of solutions and, second, if it does, then it finds all the roots in the following form. The roots are divided into conjugacy classes over F, and the multiplicities of the roots are given. For each class the algorithm finds a polynomial $\Phi \in H(T_1, \ldots, T_\ell)[\eta][Z]$ which is separable and irreducible over F, with leading coefficient $lc_Z(\Phi) = 1$, let θ" be a root of the polynomial Φ. For each class, in addition the algorithm finds a $0 \leqslant j_0 \leqslant n$ such that $\xi_{j_0} \neq 0$ for any root $(\xi_0 : \ldots : \xi_n) \in \mathbb{P}^n$ of this class and $\xi_j = 0$ for $j < j_0$, and calculates the elements $(\xi_j / \xi_{j_0})^{q^{\nu_j}} \in F[\theta'']$ for $j_0 \leqslant j \leqslant n$ (in the case of characteristic q = 0, we assume $\nu_j = 0$ and $q^{\nu_j} = 1$ for notational convenience), where $1 \leqslant q^{\nu_j} \leqslant \mathcal{D}_1$ (we recall that $\mathcal{D}_1 \leqslant \tau$ is the number of all roots of the system; see Theorem 2.2), and here $(\xi_j / \xi_{j_0})^{q^{\nu_j - 1}} \notin F[\theta'']$ (when $q > 0, \nu_j > 0$). Further, $F[(\xi_{j_0+1}/\xi_{j_0})^{q^{\nu_{j_0+1}}}, \ldots, (\xi_n/\xi_{j_0})^{q^{\nu_n}}] = F[\theta'']$ and $\theta'' = \sum_{j_0 \leqslant j \leqslant n} \gamma_j' (\xi_j / \xi_{j_0})^{q^\nu}$, where $\gamma_j' \in H$ (we assume that $\operatorname{card} H \geqslant \mathcal{D}_1 d_1$ or we extend H; see above), $q^\nu = \max_j q^{\nu_j}$. The number of conjugate roots in a class (without considering multiplicities) is equal to

$deg_z \Phi$. The degrees $deg_{T_1,\dots,T_\ell}(\xi_j/\xi_{j_0})^{q^{\nu_j}}$, $deg_{T_1,\dots,T_\ell}\Phi$ (the lengths of description of the coefficients of the monomials in $T_1,\dots,T_\ell, h, \theta''$ of the elements $(\xi_j/\xi_{j_0})^{q^{\nu_j}}$ and of the coefficients of the polynomial Φ , respectively) can be bounded above by some polynomial in r, d_2, d_1 of degree 1 with respect to d_2 (by a polynomial in $(M_1+M_2+\ell d_2), r, d_1$ of degree 1 with respect to $(M_1+M_2+\ell d_2)$, respectively) and, moreover, these estimates are independent of j and of the conjugacy class of the roots. The algorithm constructed works in time which is polynomial in $M_1, M_2, (r d_2 d_1)^{\ell+1}$, k, q.

3. Direct Method for Finding the Tree of Components and Generic Points

As in Secs. 1 and 2, let $f_0,\dots,f_{k-1} \in F[X_0,\dots,X_n]$ be homogeneous polynomials. Further, without loss of generality we assume that $deg\, f_i = d$, by replacing each f_i by $\{f_i X_j^{d-deg f_i}\}_{0\leqslant j\leqslant n}$, where $d = \max_{0\leqslant i\leqslant k-1}\{deg\, f_i\}$. Moreover, without loss of generality we assume that $\{f_i\}_{0\leqslant i\leqslant k-1}$ are linearly independent, so $k \leqslant \binom{d+n}{n} \leqslant (d+1)^n$. We assume that the ground field F = $H(T_1,\dots,T_\ell)[h]$, where either $H = \mathbb{Q}$ or H is a finite field, q = char (F), the elements $T_1,\dots,T_\ell$ are algebraically independent over H, the element h is separable over $H(T_1,\dots,T_\ell)$ and $\varphi(T) \in H[T_1,\dots,T_\ell,T]$ is its minimal polynomial. We shall assume without loss of generality that $f_i \in H[T_1,\dots,T_\ell,h,X_0,\dots X_n]$ for $0 \leqslant i \leqslant k-1$. We denote by d_1 an upper bound on $deg_{T_1,\dots,T_\ell,T}(\varphi)$ and by M_1 an upper bound on the length of description of the coefficients from H of the polynomial φ in monomials in $T_1,\dots,T_\ell, h$. By d_2 we denote an upper bound on $deg_{T_1,\dots,T_\ell}(f_j), 0 \leqslant j \leqslant k-1$, by M_2 an upper bound on the length of description of the coefficients from H of the polynomials $f_0,\dots,f_{k-1}$ in the monomials in $T_1,\dots,T_\ell, h, X_0,\dots,X_n$ (see Introduction).

The goal of the present section is the construction of an algorithm for explicitly finding the irreducible components defined over a maximal purely inseparable extension $F^{q^{-\infty}}$ of the field F, of the variety $\mathbb{P}^n(\bar{F})$ defined by the system $f_0 = \dots = f_{k-1} = 0$. Namely, for any component the algorithm constructs a generic point of it (see below and also [3]), and, besides this, in Sec. 4 a certain family of equations with coefficients from F will be constructed, which gives the component as a set of points in $\mathbb{P}^n(\bar{F})$. For brevity we shall call a component which is defined and irreducible over $F^{q^{-\infty}}$ an irreducible component over F; such a component can be given as the set of points of a system of equations with coefficients from F. An upper bound on the time that the algorithm takes will be given below in Theorem 2.4 of Sec. 4.

We proceed to a description of the tree of components, which is constructed by the algorithm in the course of performing it. The tree of components has a root which is ascribed to projective space. Any vertex v, different from the root, is ascribed to some variety $W_v \subset \mathbb{P}^n(\bar{F})$ · which is irreducible over F. By the level m of the vertex v we mean the number of edges in branches going from the root to the vertex v. The algorithm constructs for any $1 \leqslant \underset{(m)}{m} \leqslant n+1$ the linear combination $h_m = \sum_{0\leqslant i\leqslant k-1} \varkappa_i^{(m)} f_i$, where $\varkappa_i \in H$ (if H is a finite field, then it is possible that it must be extended, so that $card(H) > kd^n$; see Secs. 1 and 2). Moreover, $codim_{\mathbb{P}^n}(W_v) = m$ for $1 \leqslant m \leqslant n+1$ (in particular, $W_v = \emptyset$ when m =

n + 1) and the family of components of the variety $\{h_1=\ldots=h_m=0\}\subset\mathbb{P}^n(\bar{F})$ of common roots of the polynomials $h_1,\ldots,h_m$, which are irreducible over F, coincides with the family of varieties W_v for all v of level m and of varieties W_{v_1} for all leaves v_1 of the tree of components of levels less than m, such that W_{v_1} is a component of the variety $\{f_0=\ldots=f_{k-1}=0\}$.

If v is a vertex of level m which is not a leaf, then h_{m+1} does not vanish identically on W_v. Moreover, for any son w of the vertex v in the tree the variety W_w coincides with a component of the variety $W_v\cap\{h_{m+1}=0\}$. Conversely, any component of the latter variety coincides with W_w for some son w of the vertex v, except for those components $W^{(i)}$ of the variety $W_v\cap\{h_{m+1}=0\}$, such that $W^{(i)}\subset W_{v_1}$ for some leaf v_1 of level not greater than m, such that W_{v_1} is a component of the variety $\{f_0=\ldots=f_{k-1}=0\}$. To any component W of codimension m of the latter variety there corresponds a leaf v_1 (in general not one) of level m, such that $W=W_{v_1}$. Conversely, there are two types of leaves of level not greater than n. For any leaf v_1 of level m of the first type W_{v_1} is a component of the variety $\{f_0=\ldots=f_{k-1}=0\}$ and $\operatorname{codim}W_{v_1}=m$. If v_2 is a leaf of level m of the second type, then h_{m+1} does not vanish on W_{v_2}, so $W_{v_2}\not\subset\{f_0=\ldots=f_{k-1}=0\}$, but, on the other hand, $W_{v_2}\cap\{h_{m+1}=0\}\subset\{f_0=\ldots=f_{k-1}=0\}$ and there does not exist a component of the variety $W_{v_2}\cap\{h_{m+1}=0\}$, which is a component of the variety $\{f_0=\ldots=f_{k-1}=0\}$.

First of all we estimate from above the number of vertices in the tree of components. Namely, we show by induction on m that $\sum_v \deg W_v\leqslant d^m$, where v runs through all vertices of level m. If $W_v\cap\{h_{m+1}=0\}=(\bigcup_w W_w)\cup(\bigcup_i W^{(i)})$ (see above) is the decomposition into irreducible components over F, where the components W_w are ascribed to the sons w of the vertex v of level m, then $\sum_w \deg W_w\leqslant d\cdot\deg W_v$ according to Bezout's inequality [7]. Summing these inequalities over all vertices v of level m, one can get the inequalities required for vertices of level m + 1. From this it follows that the number of all vertices of the tree of components is less than $(n+1)d^n+1$, since the depth of the tree is not greater than n + 1. Thus, it suffices to estimate in what follows the time the algorithm works for the construction of one vertex of the tree of components.

The algorithm given constructs $h_1,\ldots,h_{n+1}$, the tree, and the components W_v by induction on the level m of the vertex v. We write the first step (m = 1). We let $h_1=f_0$. Based on Chapter I of [4], we decompose $f_0=\prod_i g_i^{e_i}$, where g_i are irreducible over F for each i. We fix some index i. We let $W_1=\{g_i=0\}\subset\mathbb{P}^n(\bar{F})$ be a hypersurface which is a component of the hypersurface $\{f_0=0\}$.

Now we construct a generic point of the component W_1 [3]. Let $g_i=\tilde{g}_i(X_0^{q^{\nu_i'}},\ldots,X_n^{q^{\nu_i'}})$, where $\tilde{g}_i\in F[Z_0,\ldots,Z_n]$ and ν_i' are as large as possible, when $q>0$, and $q^{\nu_i'}=1$, when char (F) = 0 (the analogous remark is valid below in analogous situations). Obviously, $\tilde{g}_i$ is irreducible over F. Let $0\leqslant j_1\leqslant n$ be an index such that $(\partial\tilde{g}_i/\partial Z_{j_1})\not\equiv 0$ and let $j_0\neq j_1$ (let us assume $n>0$). For convenience of notation let us assume temporarily that $j_0=0$, $j_1=n$, and, moreover, we assume that $g_i\neq c\,X_{j_0}^{q^{\nu_i'}}$. We set $X_1/X_0=t_1,\ldots,X_{n-1}/X_0=t_{n-1}$, $(X_n/X_0)^{q^{\nu_i'}}=\theta_1$, where $t_1,\ldots,t_{n-1}$ are algebraically independent over F; we let $\Phi_1(Z)=\tilde{g}_i(1,t_1,\ldots,t_{n-1},Z)/a_0\in F(t_1,\ldots,t_{n-1})[Z]$, where $a_0=a_0(t_1,\ldots,t_{n-1})=lc_Z(\tilde{g}_i(1,t_1,\ldots,t_{n-1},Z))\in F[t_1,\ldots,t_{n-1}]$. We have

$\Phi_1(\theta_1)=0$ and, moreover, Φ_1 is the minimal polynomial for the element θ_1 over the field $F(t_1,\dots,t_{n-1})$. We consider the field $F(t_1,\dots,t_{n-1})[Z]/(\Phi_1)=F(t_1,\dots,t_{n-1})[\theta_1]$. Then the expressions given above for X_j/X_0 supply a generic point of the component W_1 in the following sense. An isomorphism of fields $F(X_1/X_0,\dots,X_{n-1}/X_0,(X_n/X_0)^{q^{\nu_i'}})\simeq F(t_1,\dots,t_{n-1})[\theta_1]$ (the field $F(X_1/X_0,\dots,X_{n-1}/X_0,(X_n/X_0)^{q^{\nu_i'}})$ here and later in similar situations, is a subfield of the field $F^{q^{-\infty}}(W_1)$, generated by F and the rational functions $X_1/X_0,\dots,X_{n-1}/X_0,(X_n/X_0)^{q^{\nu_i'}}$ on W_1) can be lifted uniquely to a field imbedding $\pi: F^{q^{-\infty}}(W_1)\hookrightarrow \overline{F(t_1,\dots,t_{n-1})}$ (in fact, the image of the field $F^{q^{-\infty}}(W_1)$ under the imbedding π is purely inseparable over the field $F(t_1,\dots,t_{n-1})[\theta_1]$), since the extension $F(X_1/X_0,\dots,X_{n-1}/X_0,(X_n/X_0)^{q^{\nu_i'}})\subset F^{q^{-\infty}}(W_1)$ is purely separable. Thus, π defines a generic point of the variety W_1 (see [3]).

Now we can describe the first level of components. It consists of all sons of a root. The vertices of the first level correspond bijectively to polynomials g_i. For uniformity we now introduce notation which will be used below in the inductive step. Let the polynomial g_i correspond to the vertex v of the first level. Then the component $W_v = W_1$ is ascribed to it in the tree of components $W_v=\{\psi_0^{(v)}=\dots=\psi_N^{(v)}=0\}$, where $\psi_0^{(v)}\equiv\dots\equiv\psi_N^{(v)}\equiv g_i$. A generic point of the component W_v is given by the equations $X_1/X_0=t_1,\dots,X_{n-1}/X_0=t_{n-1}$, $(X_n/X_0)^{q^{\nu_i'}}=\theta_v=\theta_1$; we set, finally, $\Phi_v=\Phi_1$ (see above).

Now we formulate the inductive hypothesis. Let $h_1,\dots,h_m$ and all the vertices v of level m (and also vertices of levels less than m) of the tree of components be constructed already; we assume $m\leqslant n$. Moreover, there is constructed a certain family of homogeneous polynomials $\psi_0^{(v)},\dots,\psi_N^{(v)}\in F[X_0,\dots,X_n]$, such that $W_v=\{\psi_0^{(v)}=\dots=\psi_{N'}^{(v)}=0\}$ and $N'\leqslant(3d^m)^n$. Moreover, there is given the field $F(t_1,\dots,t_{n-m})[\theta_v]$, where $t_1,\dots,t_{n-m}$ are algebraically independent over F, the minimal polynomial $\Phi_v\in F(t_1,\dots,t_{n-m})[Z]$ of the element θ_v over the field $F(t_1,\dots,t_{n-m})$ with leading coefficient $lc_Z(\Phi_v)=1$. Finally, there is constructed a generic point of the variety W_v, more precisely, there are written expressions $(X_j/X_{j_0})^{q^{\nu_j'}}\in F(t_1,\dots,t_{n-m})[Z]$, for some fixed j, and any j and suitable $q^{\nu_j'}\leqslant(d+d_1+d_2)^m d^m d_1$ (the numbers j_0, ν_j' actually depend on the vertex v, but we shall not state this explicitly in what follows). Here X_j/X_{j_0} are considered as rational functions on W_v, and these expressions define a field isomorphism (after suitable renumbering of the variables $X_0,\dots,X_n$)$F(X_1/X_0,\dots,X_{n-m}/X_0,(X_{n-m+1}/X_0)^{q^{\nu_{n-m+1}'}},\dots,(X_n/X_0)^{q^{\nu_n'}})\simeq F(t_1,\dots,t_{n-m})[\theta_v]$ also by the inductive hypothesis). Under this isomorphism $X_i/X_0\longrightarrow t_i$, $1\leqslant i\leqslant n-m$. Further, this isomorphism can be lifted uniquely to a field imbedding $F^{q^{-\infty}}(W_v)\hookrightarrow\overline{F(t_1,\dots t_{n-m})}$, i.e., to a generic point of the variety W_v.

We also formulate estimates on the parameters of all the elements indicated. The degrees $\deg_{X_0,\dots,X_n}(\psi_j^{(v)})\leqslant d_1(d+d_1+d_2)^m \deg W_v\leqslant(d+d_1+d_2)^{m+1}d^m$, $\deg_Z\Phi_v\leqslant\deg W_v\leqslant d^m$, moreover $\deg_{T_1,\dots,T_l}(\psi_j^{(v)})$ does not exceed a polynomial in $(d+d_1+d_2)^{m(n-m+1)}$ and $\deg_{T_1,\dots,T_l,t_1,\dots,t_{n-m}}(\Phi_v)$, $\deg_{T_1,\dots,T_l,t_1,\dots,t_{n-m}}(X_j/X_0)^{q^{\nu_j'}}$ are bounded above by some polynomial in $(d+d_1+d_2)^m$ (here and below in analogous situations the polynomial does not depend on the original system, the vertex v, etc.). We denote by $l(\psi_j^{(v)})$ the maximal length of description of the coefficients from H of the polynomials $\psi_j^{(v)}$. Then $l(\psi_j^{(v)}),l(\Phi_v),l((X_j/X_0)^{q^{\nu_j}})\leqslant(M_1+M_2+l)P((d+d_1+d_2)^{m^2n})$ for a suitable polynomial p.

Now we proceed to perform the following step of the algorithm for constructing the tree of components. We consider the polynomials $f_0, \dots, f_{k-1}$ and for each of them we verify whether it vanishes identically on the component W_v. Namely, we fix i and we substitute in the homogeneous polynomials $f_i^{q^\nu}$ the expression for $(X_j/X_0)^{q^{\nu'}}, 0 \leqslant j \leqslant n$ where $q^{\nu'} = \max_{0 \leqslant j \leqslant n} q^{\nu'_j}$. As a result we get an element of the field $F(t_1, \dots, t_{n-m})[\theta_v]$. If this element is equal to zero (in this case, see Lemma 2.7 below, f_i vanishes identically on W_v), then we pass to consideration of the next polynomial f_{i+1}; otherwise, if this element is different from zero, then v is not a leaf of the first type (see above), i.e., W_v is not a component of the variety $\{f_0 = \dots = f_{k-1} = 0\}$. Now if all f_i vanish identically on W_v, then v is a leaf of the first type and W_v is a component of the variety $\{f_0 = \dots = f_{k-1} = 0\}$

Now we construct $h_{m+1} = \sum_{0 \leqslant i \leqslant k-1} \varkappa_i^{(m+1)} f_i$. Using Lemma 2.1 of Sec. 1, we choose $N_1 = ((k-1)d^m + 1)$ vectors $\alpha_1, \dots, \alpha_{N_1} \in H^k$, any k of which are linearly independent. For any vector $\alpha = (\alpha^{(0)}, \dots, \alpha^{(k-1)})$ we let $h^{(\alpha)} = \sum_{0 \leqslant i \leqslant k-1} \alpha^{(i)} f_i$. We verify that at least one of the vectors $\alpha_1, \dots, \alpha_{N_1}$ can be taken as $(\varkappa_0^{(m+1)}, \dots, \varkappa_{k-1}^{(m+1)})$, so that h_{m+1} will not vanish identically on W_v for any vertex v of level m, which is not a leaf of the first type. In the opposite case, by Dirichlet's principle there exist at least k vectors among $\alpha_1, \dots, \alpha_{N_1}$ (let them be $\alpha_1, \dots, \alpha_k$), such that $h^{(\alpha_1)}, \dots, h^{(\alpha_k)}$ vanishes on W_v for some fixed vertex v of level m (which is not a leaf of the first type), since the number of vertices of level m is not greater than d^m according to what was proved above. Then all $f_0, \dots, f_{k-1}$ vanish on W_v, which contradicts the fact that v is not a leaf of the first type.

The algorithm considers $h^{(\alpha_i)}$ for $1 \leqslant i \leqslant N_1$ and for each vertex v of level m, which is not a leaf of the first type, substitutes into the homogeneous polynomials $(h^{(\alpha_i)})^{q^{\nu'}}$ the expressions for $(X_j/X_0)^{q^{\nu'}}$ (keeping in mind the renumbering of unknowns made above). As h_{m+1} we take an element $h^{(\alpha_i)}$, for which the results of the substitutions for all v are different from zero as elements of the field $F(t_1, \dots, t_{n-m})[\theta_v]$.

Now we fix a vertex v of level m, which is not a leaf of the first type and we let $W = W_v \cap \{h_{m+1} = 0\} = \{\psi_0^{(v)} = \dots = \psi_N^{(v)} = h_{m+1} = 0\}$. Obviously the dimension of each component of the variety W is equal to n − m − 1.

We apply the construction of Lemma 2.3 of Sec. 1 to our situation. It gives us a family $\mathfrak{M}$ of no more than $\binom{nd^{m+1}+1}{n-m}$ elements, each of which is an (n − m)-tuple of linear forms of the form $\left(\sum_{0 \leqslant i \leqslant n} \lambda_{si} X_i\right)$, where $0 \leqslant s \leqslant n-m-1$ and either $\lambda_{si} \in H$, if $H = \mathbb{Q}$, or λ_{si} belongs to some suitable extension of the finite field H, $0 \leqslant s \leqslant n-m-1$ (we assume here and later in analogous situations, without loss of generality and for convenience of notation, that this extension coincides with H). Moreover, the length of description of any of the λ_{si} can be bounded above by some polynomial in n, log (deg W) (cf. the construction of Sec. 1 and the remark at the end of Sec. 1). According to Lemma 2.3, at least one of the (n − m)-tuples of $\mathfrak{M}$ has the property that $W \cap \{\sum_{0 \leqslant i \leqslant n} \lambda_{0i} X_i = \dots = \sum_{0 \leqslant i \leqslant n} \lambda_{n-m-1,i} = 0\} = \emptyset$ and, consequently (cf. the corollary in Sec. 1), this (n − m)-tuple is a common transcendence basis for all components of the variety W.

The algorithm considers all elements of the family $\mathfrak{M}$. We fix an element $(\sum_{0\leqslant i\leqslant n}\lambda_{si}X_i)_{0\leqslant s\leqslant n-m-1}\in\mathfrak{M}$. We add the forms $\{\sum_{0\leqslant i\leqslant n}\lambda_{si}X_i\}_{0\leqslant s\leqslant n-m-1}$ (they are linearly independent by the construction of Sec. 1) to a basis of the space of F-linear forms in the variables $X_0,\dots,X_n$ and we denote this new basis by $Y_0,\dots,Y_n$, in particular, $Y_s = \sum_{0\leqslant i\leqslant n}\lambda_{si}X_i$ for $0\leqslant s\leqslant n-m-1$. As a result of taking the current step all sons of the vertex v will be constructed (under the condition that the fixed element of $\mathfrak{M}$ satisfies the condition $\{\sum_{0\leqslant i\leqslant n}\lambda_{0i}X_i=\dots=\sum_{0\leqslant i\leqslant n}\lambda_{n-m-1,i}X_i=0\}=\emptyset$ and for each son w there will be constructed homogeneous polynomials $\psi_0^{(w)},\dots,\psi_N^{(w)}\in F(Y_0,\dots,Y_n)$, $N\leqslant(3d^{(m+1)})^n$ such that the corresponding variety $W_w=\{\psi_0^{(w)}=\dots=\psi_N^{(w)'}=0\}$. Besides this the algorithm finds a generic point for W_w, i.e., the expressions $(Y_j/Y_0)^{q^{\nu_j'}}\in F(t_1,\dots,t_{n-m-1})[\theta_w']$ for $n-m\leqslant j\leqslant n$, defining a field isomorphism $F(t_1,\dots,t_{n-m-1})[\theta_w']\simeq F(Y_1/Y_0,\dots,Y_{n-m-1}/Y_0,(Y_{n-m}/Y_0)^{q^{\nu_{n-m}}},\dots,(Y_n/Y_0)^{q^{\nu_n}}]$. The variables $X_0,\dots,X_n$ can be expressed as linear forms in $Y_0,\dots,Y_n$ and conversely. Substituting these expressions in $\psi_j^{(w)}$ and $(Y_j/Y_0)^{q^{\nu_j}}$, one can get the polynomials desired (where the length of description of all these elements can increase no more than polynomially). For convenience we also represent the polynomials $\psi_0^{(v)},\dots,\psi_{N'}^{(v)},h_{m+1}$ as polynomials in $Y_0,\dots,Y_n$ and we preserve the same notation for them.

We shall assume in our arguments that the fixed element of $\mathfrak{M}$ satisfies the condition $W\cap\{Y_0=\dots=Y_{n-m-1}=0\}=\emptyset$, because otherwise the algorithm detects that this is false in the course of its work, and goes on to consider another element from $\mathfrak{M}$.

In what follows we shall consider the intersection of the variety $W(\bar{F}')$, where $F'=H(T_1,\dots,T_\ell,t_1,\dots,t_{n-m-1})[h]=F(t_1,\dots,t_{n-m-1})$ with the linear space $\Pi=\{Y_i-t_iY_0=0\}_{1\leqslant i\leqslant n-m-1}$, where $t_1,\dots,t_{n-m-1}$ are algebraically independent over F (here we consider varieties as subvarieties in $\mathbb{P}^n(\bar{F}')$). Since $W\cap\{Y_0=\dots=Y_{n-m-1}=0\}=\emptyset$, one has that $W(\bar{F}')\cap\Pi$ consists of a finite set of points, lying in an affine subspace $\{Y_0\neq 0\}\subset\mathbb{P}^n(\bar{F}'$ (by Lemma 2.2 of Sec. 1). Hence the zero-dimensional variety $W(\bar{F}')\cap\Pi$ is defined over the field $(F')^{q^{-\infty}}$.

We substitute T_iY_0 in the polynomials $\psi_0^{(v)},\dots,\psi_{N'}^{(v)},h$ for Y_i for $1\leqslant i\leqslant n-m-1$. The roots of the system of equations

$$\begin{aligned}&\psi_i^{(v)}(Y_0,t_1Y_0,\dots,t_{n-m-1}Y_0,Y_{n-m},\dots,Y_n)=0,\ 0\leqslant i\leqslant N'\\&h_{m+1}(Y_0,t_1Y_0,\dots,t_{n-m-1}Y_0,Y_{n-m},\dots,Y_n)=0\end{aligned}\tag{1}$$

in projective space $\mathbb{P}^{m+1}(\bar{F}')$ correspond bijectively to the roots of the system defining the intersection $W(\bar{F}')\cap\Pi\subset\mathbb{P}^n(\bar{F}')$. We apply Theorem 2.3 of Sec. 2 to (1), where the role of F of the theorem is played by F', respectively, the role of $T_1,\dots,T_\ell$ is played by $T_1,\dots,T_\ell,t_1,\dots,t_{n-m-1}$. If the algorithm of Theorem 2.3 detects that $W(\bar{F}')\cap\Pi$ is infinite or there exists a root of (1) with $Y_0 = 0$, then for the fixed element of $\mathfrak{M}$ the condition $W\cap\{Y_0=\dots=Y_{n-m-1}=0\}=\emptyset$ does not hold (see the remark on Lemma 2.2 of Sec. 1) and the algorithm goes on to the consideration of the next element of $\mathfrak{M}$ (namely, at this place the algorithm determines whether the condition $W\cap\{Y_0=\dots=Y_{n-m-1}==0\}=\emptyset$ holds).

We consider some conjugacy class over F' of roots of (1) and the polynomial $\Phi\in F'[Z]$ corresponding to this class which is irreducible over F' and $lc_Z(\Phi)=1$ (see Theorem 2.3). Our next goal is to establish a bijective correspondence between the components of the variety W and the conjugacy classes over F' of roots of (1), i.e., in particular, to any son of the vertex v there corresponds a uniquely determined polynomial Φ .

First we verify that the elements $Z_1,\dots,Z_{n-m-1}$ form a transcendence basis over the field F for the ring $\Lambda_v=F[Z_1,\dots,Z_n]/(\psi_0^{(v)}(1,Z_1,\dots,Z_n),\dots,\psi_{N'}^{(v)}(1,Z_1,\dots,Z_n),h_{m+1}(1,Z_1,\dots,Z_n))$. In fact, the kernel of the homomorphism $\Lambda_v\to F^{q^{-\infty}}[Y_1/Y_0,\dots,Y_n/Y_0]=F^{q^{-\infty}}[W\cap\{Y_0\neq 0\}]$ in the coordinate ring of the affine variety $W\cap\{Y_0\neq 0\}$ over $F^{q^{-\infty}}$ (under which $Z_i\to Y_i/Y_0,\ 1\leqslant i\leqslant n$) is the nilradical $\mathcal{R}(\Lambda_v)$ of the ring Λ_v . The components w_1 of the variety W correspond bijectively to minimal prime ideals I_{w_1} of the ring Λ_v (see [3]; also see the proof of Lemma 2.9 below). The elements $Z_1,\dots,Z_{n-m-1}$ are algebraically independent over F, since they are algebraically independent in the ring $F^{q^{-\infty}}[W_{w_1}\cap\{Y_0\neq 0\}]\supset\Lambda_v/I_{w_1}$. On the other hand, for any $\lambda\in\Lambda_v$ and any component W_{w_1} of the variety W, there exists a polynomial $0\neq P_{w_1}\in F[\tilde{Z}_1,\dots,\tilde{Z}_{n-m}]$ (here $\tilde{Z}_1,\dots,\tilde{Z}_{n-m}$ are algebraically independent over F), such that $P_{w_1}(Z_1,\dots,Z_{n-m-1},\lambda)\in I_{w_1}$. We let $P_v=\prod_{w_1}P_{w_1}$ be the product of the polynomials P_{w_1} over all components W_{w_1} of the variety W. Then $P_v(Z_1,\dots,Z_{n-m-1},\lambda)\in\mathcal{R}(\Lambda_v)$ (see [3]). Consequently, $P_v^{\ell}(Z_1,\dots,Z_{n-m-1},\lambda)=0$ for a suitable integral e, i.e., the family $\{Z_1,\dots,Z_{n-m-1}\}$ is a transcendence basis of the ring Λ_v over F.

We let $S=F[Z_1,\dots,Z_{n-m-1}]\setminus\{0\}\subset\Lambda_v$ be a multiplicatively closed subset. Keeping in mind that $I_{w_1}\cap S=\emptyset$ for each w_1, we get that the minimal prime ideals of the ring $S^{-1}\Lambda_v$ correspond bijectively to the ideals I_{w_1} and have the form $S^{-1}I_{w_1}$ (cf., e.g., [3]). On the other hand, $F(Z_1,\dots,Z_{n-m-1})\subset S^{-1}\Lambda_v$ and $S^{-1}\Lambda_v$ is a finite-dimensional algebra over the field $F(Z_1,\dots,Z_{n-m-1}$. Consequently, all prime ideals of the ring $S^{-1}\Lambda_v$ are simultaneously minimal and maximal.

LEMMA 2.5. Let $F\subset F_1\subset\overline{F}$ be field extensions and let $\Lambda'_v=F_1\otimes_F\Lambda_v$. Then there exists a bijective correspondence between the following three sets (we recall that $W\cap\{Y_0=Y_{n-m-1}=0\}=\emptyset$):

a) components W'_μ of the variety W which are irreducible over F_1;

b) classes of homomorphisms having the same kernel $S^{-1}\Lambda'_v\to\overline{F(t_1,\dots,t_{n-m-1})}$ of algebras over the field $\Omega=F_1(t_1,\dots,t_{n-m-1})$ (here the inclusion $\Omega\hookrightarrow S^{-1}\Lambda'_v$ is defined by the correspondences $t\to Z_i,\ 1\leqslant i\leqslant n-m-1$);

c) pairs, the first term of each of which is a conjugacy class over $F'=F(t_1,\dots,t_{n-m-1})$ of roots of (1), and if the polynomial $\Phi\in F'(Z)$ corresponds to this class (see Theorem 2.3 of Sec. 2), the second term is a factor $\Phi_u\in\Omega[Z]$ of the polynomial Φ which is irreducible over Ω .

Proof. First we construct a bijective correspondence between the sets of points a) and b). Let W_u' be a component of the variety W which is irreducible over F_1. It corresponds to a simultaneously minimal and maximal ideal $S^{-1}I'_u\subset S^{-1}\Lambda'_v$, where $I'_u\subset\Lambda'_v$ is a minimal ideal (see above). Since $\Omega\subset(S^{-1}\Lambda'_v/S^{-1}I'_u)$ is a finite field extension (analogously to the way this was proved above), there exists a field imbedding $(S^{-1}\Lambda'_v/S^{-1}I'_u) \hookrightarrow \overline{\Omega}$ under which the elements $Z_1, \ldots, Z_{n-m-1}$, which are algebraically independent over F_1, are mapped respectively into $t_1, \ldots, t_{n-m-1}$. Thus to the component W_u' corresponds the class of homomorphisms from b), containing the composition of the natural epimorphism $S^{-1}\Lambda'_v \longrightarrow S^{-1}\Lambda'_v/S^{-1}I'_u$ and the field imbedding just constructed.

Conversely, the kernel of the homomorphism from b) is a maximal ideal $S^{-1}I'_u \subset S^{-1}\Lambda'_v$ and to it there corresponds the component W_u'. It is straightforward to verify that the correspondences are well defined and that they are mutually inverse.

Now we construct a bijective correspondence between the sets of points b) and c). Suppose given a pair from point c). The field extension $\Omega \subset \Omega[Z]/(\Phi_u)$ is finite, from which it follows that there exists a field imbedding $\Omega[Z]/(\Phi_u) \hookrightarrow \overline{\Omega}$ which is the identity on Ω. By Theorem 2.3 of Sec. 2, applied to (1) over the field F', if $\Phi_u(\theta'_u) = 0$ and all the more $\Phi(\theta'_u)=0$, then $F'[\theta'_u]=F'[Z]/(\Phi)=F'[(\xi_{n-m}/\xi_0)^{q^{\nu_{n-m}}}, \ldots, (\xi_n/\xi_0)^{q^{\nu_n}}$, where $(\xi_0 : \xi_{n-m} : \ldots : \xi_n) \in \mathbb{P}^{m+1}(\overline{F'})$ is a solution of (1) ($\xi_0 \neq 0$ since $W \cap \{Y_0 = \ldots = Y_{n-m-1} = 0\} = \emptyset$ see Sec. 2), and taking the composite of this field with the field Ω, we get that $\Omega[Z]/(\Phi_u) = \Omega[\theta'_u] = \Omega[(\xi_{n-m}/\xi_0)^{q^{\nu_{n-m}}}, \ldots, (\xi_n/\xi_0)^{q^{\nu_n}}]$. The extension $\Omega[(\xi_{n-m}/\xi_0)^{q^{\nu_{n-m}}}, \ldots, (\xi_n/\xi_0)^{q^{\nu_n}}] \subset \Omega[\xi_{n-m}/\xi_0, \ldots, \xi_n/\xi_0]$ is purely inseparable. From this it follows that the imbedding indicated above $\Omega[(\xi_{n-m}/\xi_0)^{q^{\nu_{n-m}}}, \ldots, (\xi_n/\xi_0)^{q^{\nu_n}}] \hookrightarrow \overline{\Omega}$ can be extended uniquely to an imbedding $\sigma : \Omega[\xi_{n-m}/\xi_0, \ldots, \xi_n/\xi_0] \hookrightarrow \overline{\Omega}$.

By hypothesis and Theorem 2.3, the vector $(\xi_0 : \xi_{n-m} : \ldots : \xi_n)$ is a root of (1). Consequently, since $\xi_0 \neq 0$ according to Lemma 2.2, there exists a unique homomorphism $\pi : S^{-1}\Lambda'_v \longrightarrow \Omega[\xi_{n-m}/\xi_0, \ldots, \xi_n/\xi_0]$ of Ω-algebras, under which $\pi(Z_i) = \xi_i/\xi_0$, $n-m \leq i \leq n$. Thus, with the pair from point c) considered, we associate the composition $\sigma \circ \pi$.

Conversely, suppose given a homomorphism $\tau : S^{-1}\Lambda_v \to \overline{\Omega}$ over Ω. Then the vector of images $(1 : \tau(Z_{n-m}) : \ldots : \tau(Z_n))$ is a root of (1), belonging to some conjugacy class over F' of roots, to which corresponds a polynomial $\Phi \in F'[Z]$. Moreover, for suitable $\theta'_u \in \Omega$ such that $\Phi(\theta'_u) = 0$, one has the coincidence of fields $F'[\theta'_u] = F'[\tau(Z_{n-m})^{q^{\nu_{n-m}}}, \ldots, \tau(Z_n)^{q^{\nu_n}}]$. Consequently, $\Phi_u(\theta'_u) = 0$ for some factor $\Phi_u \in \Omega[Z]$ of the polynomial Φ which is irreducible over Ω. Thus, to the class containing τ there corresponds the class of conjugate roots considered as the first term of the pair and the polynomial Φ_u as the second term of the pair. It is straightforward to verify that the correspondences constructed are well defined and that they are mutually inverse, which completes the proof of the lemma.

The remark below is due to A. L. Chistov and is not used here.

Remark. One can apply Lemma 2.5 to an arbitrary variety U (instead of W), given by a system of equations $g_1 = \cdots = g_s = 0$, under the condition that $U \cap \{Y_0 = \cdots = Y_{n-m-1} = 0\} = \emptyset$ and dim U = n − m − 1. Then the role of (1) is played by the system

$$g_1(Y_0, t_1Y_0, \ldots, t_{n-m-1}Y_0, Y_{n-m}, \ldots, Y_n) = \ldots = g_s(Y_0, t_1Y_0, \ldots, t_{n-m-1}Y_0, Y_{n-m}, \ldots, Y_n) = 0.$$

Here in point a) of Lemma 2.5 it is necessary to consider the set of all components W_u' of highest dimension n − m − 1. The proof is essentially unchanged since $S \cap I_u' \neq \emptyset$ for any prime ideal $I_u' \subset \Lambda_v'$, if $\deg tr_F(\Lambda_v' / I_u') < n-m-1$.

As a consequence (it is necessary to apply Lemma 2.5 to the case when $F_1 = F$), we get the required bijective correspondence between the components W_{w_1} of the variety W and the conjugacy classes over F' of roots of (1). Moreover, from the proof one can get a representation of a generic point of an arbitrary component W_{w_1} (let the polynomial $\Phi = \Phi_{w_1}$ correspond to W_{w_1} according to point c) of Lemma 2.5 and $\Phi_{w_1}(\theta'_{w_1})=0$). Namely, according to Lemma 2.5, to the component W_{w_1} corresponds a homomorphism $S^{-1}\Lambda_v \to \overline{F'}$ of F'-algebras with kernel $S^{-1} I_{w_1}$. This gives an imbedding of fields $S^{-1}\Lambda_v / S^{-1} I_{w_1} \hookrightarrow \overline{F'}$ which is the identity on F'. This imbedding can be extended uniquely to an imbedding of fields $\sigma : F^{q^{-\infty}}(W_{w_1}) \hookrightarrow \overline{F'}$. Then, as in the proof of Lemma 2.5, for the image under the action of σ of the subfield $F(Z_1,\ldots,Z_{n-m-1})[Z_{n-m}^{q^{\nu_{n-m}}},\ldots, Z_n^{q^{\nu_n}}] \subset S^{-1}\Lambda_v/S^{-1}I_{w_1} \subset F^{q^{-\infty}}(W_{w_1})$ one has the coincidence of fields $F'[\theta'_{w_1}] = F'[\sigma(Z_{n-m})^{q^{\nu_{n-m}}},\ldots,\sigma(Z_n)^{q^{\nu_n}}]$. And, finally, there is an isomorphism

$$F^{q^{-\infty}}(W_{w_1}) \supset F(Y_1/Y_0,\ldots,Y_{n-m-1}/Y_0,(Y_{n-m}/Y_0)^{q^{\nu_{n-m}}},\ldots,(Y_n/Y_0)^{q^{\nu_n}}) \simeq F'[\theta'_{w_1}], \qquad (2)$$

obtained from the preceding isomorphism, in which the imbedding σ participates. Under the isomorphism (2), the elements Y_j/Y_0 are considered as rational functions on W_{w_1}. This isomorphism also gives a generic point of the component W_{w_1}.

Now we make more precise to which components W_{w_1} of the variety W there correspond sons (we shall denote them by w_1) of the vertex v. For this it is necessary to verify whether $W_{w_1} \subset W_{v_1}$, for some leaf v_1 of level no greater than m of the first type (in this case to the component W_{w_1} there does not correspond any son of the vertex v). In order to verify this inclusion, the algorithm substitutes into the polynomials $(\psi_0^{(v_1)})^{q^{\nu'}},\ldots,(\psi_{N_2}^{(v_1)})^{q^{\nu'}}$ (here $q^{\nu'} \geqslant q^{\nu_i}$, $n-m \leqslant i \leqslant n$) the expressions for $(Y_i/Y_0)^{q^{\nu}}$, $0 \leqslant i \leqslant n$, from (2) (after replacement of the variables $X_0,\ldots,X_n$ by $Y_0,\ldots,Y_n$). The inclusion $W_{w_1} \subset W_{v_1}$ holds if and only if all $N_2 + 1$ elements of the field $F'[\theta'_{w_1}]$ obtained are equal to zero (see Lemma 2.7 below). If $W_w \not\subset W_{v_1}$ for all the v_1 mentioned, then the son w of the vertex v corresponds to W_w. If v has no sons, then v is a leaf of the second type. Thus, all the vertices w of level m + 1 are constructed; in Sec. 4 the algorithm constructs for each component W_w a system of equations defining it. Below by w we denote a son of the vertex v.

4. Construction of a System of Equations Defining a Component

One says that the component W_w is defined over the field $F^{q^{-\nu}}$ if the ideal $\mathcal{I}_w \subset \overline{F}[Z_1,\ldots,Z_n]$ of the affine variety $W_w \cap \{Y_0 \neq 0\}$ has a system of generators from the subring $F^{q^{-\nu}}[Z_1,\ldots,Z_n]$ (here it is essential that $W_w \not\subset \{Y_0 = 0\}$).

LEMMA 2.6. The component W_w is defined over the field $F^{q^{-\nu}}$, where $q^{\nu} = \max_{n-m \leqslant i \leqslant n} q^{\nu_i}$.

Proof. The assertion of the lemma is equivalent to the fact that the natural homomorphism $\bar{F}\otimes_{Fq^{-\nu}}(\mathcal{J}_w\cap F^{q^{-\nu}}[Z_1,\dots Z_n])\to\mathcal{J}_w$ is an isomorphism. There is an isomorphism $F^{q^{-\nu}}[Y_1/Y_0,\dots,Y_n/Y_0]\simeq F^{q^{-\nu}}[Z_1,\dots,Z_n]/(\mathcal{J}_w\cap F^{q^{-\nu}}[Z_1,\dots,Z_n])$. Consequently, the assertion of the lemma is equivalent to the fact that the composite homomorphism $\pi:\bar{F}\otimes_{Fq^{-\nu}}F^{q^{-\nu}}[Y_1/Y_0,\dots,Y_n/Y_0]\simeq\bar{F}[Z_1,\dots,Z_n]/(\bar{F}\otimes_{Fq^{-\nu}}(\mathcal{J}_w\cap F^{q^{-\nu}}[Z_1,\dots,Z_n]))\longrightarrow\bar{F}[Z_1,\dots,Z_n]/\mathcal{J}_w=\bar{F}[W_w\cap\{Y_0\neq 0\}]$ is an isomorphism. We consider the ring $(\bar{F}\otimes_{Fq^{-\nu}}F^{q^{-\nu}}(Y_1/Y_0,\dots,Y_n/Y_0))\simeq\bar{F}\otimes_F F((Y_1/Y_0)^{q^\nu},\dots,(Y_n/Y_0)^{q^\nu})\subset\bar{F}\otimes_F F((Y_1/Y_0),\dots,(Y_{n-m-1}/Y_0),(Y_{n-m}/Y_0)^{q^\nu},\dots,(Y_n/Y_0)^{q^\nu})\simeq\bar{F}\otimes_F F'[Z]/(\Phi_w)=\bar{F}(t_1,\dots,t_{n-m-1})[Z]/(\Phi_w)$. (the first isomorphism in the chain is induced by raising to the q^ν-th power). The last ring is the direct sum of fields, since the polynomial Φ_w is separable. Consequently, the ring $F\otimes_{Fq^{-\nu}}F^{q^{-\nu}}(Y_1/Y_0,\dots,Y_n/Y_0)$ has no nonzero nilpotents.

On the other hand, the nilradical $rad(\mathcal{J}_w)=rad(\bar{F}\otimes_{Fq^{-\nu}}(\mathcal{J}_w\cap F^{q^{-\nu}}[Z_1,\dots,Z_n]))$, since an arbitrary element $a\in\mathcal{J}_w$ can be represented in the form $a=\sum_i b_i a_i$, where $a_i\in F^{q^{-\infty}}[Z_1,\dots,Z_n]\cap\mathcal{J}_w$ is a finite system of generators of the ideal $\mathcal{J}_w$, the polynomials $b_i\in\bar{F}[Z_1,\dots,Z_n]$, and, consequently, $a^{q^s}\in\bar{F}\otimes_{Fq^{-\nu}}(\mathcal{J}_w\cap F^{q^{-\nu}}[Z_1,\dots,Z_n])$ for some s. From this it follows that $\operatorname{Ker}(\pi)\subset\mathfrak{R}(\bar{F}\otimes_{Fq^{-\nu}}F^{q^{-\nu}}[Y_1/Y_0,\dots,Y_n/Y_0])$, i.e., $\operatorname{Ker}(\pi)=0$. Obviously, the homomorphism π is surjective. The lemma is proved.

For the construction of polynomials $\psi_0^{(w)},\dots,\psi_N^{(w)}$, defining the component W$_w$ we formulate the following basic property of a generic point. Let $q^\nu=\max_{n-m\leqslant i\leqslant n}q^{\nu_i}$.

LEMMA 2.7. Let $\psi\in F^{q^{-\nu}}[Y_0,\dots,Y_n]$ be a homogeneous polynomial. Then ψ vanishes identically on the component W$_w$ if and only if $\psi^{q^\nu}(1,Y_1/Y_0,\dots,Y_n/Y_0)=0$ in the field $F(t_1,\dots,t_{n-m-1})[\theta'_w]$.

Proof. In fact, $\psi^{q^\nu}(1,Y_1/Y_0,\dots,Y_n/Y_0)=\tilde{\psi}(1,Y_1/Y_0,\dots,Y_{n-m-1}/Y_0,(Y_{n-m}/Y_0)^{q^\nu},\dots,(Y_n/Y_0)^{q^\nu})$ for a suitable polynomial $\tilde{\psi}\in F[Y_0,\dots,Y_n]$. Using the expressions from (2), one can find the value of $\psi^{q^\nu}(1,Y_1/Y_0,\dots,Y_n/Y_0)$ in the field $F'[\theta'_w]=F(t_1,\dots,t_{n-m-1})[\theta'_w]$. The polynomial ψ vanishes identically on the component W$_w$ if and only if $0=\psi(1,Y_1/Y_0,\dots,Y_n/Y_0)\in F^{q^{-\infty}}(W_w)$. The latter is equivalent to the fact that $0=\tilde{\psi}(1,Y_1/Y_0,\dots,Y_{n-m-1}/Y_0,(Y_{n-m}/Y_0)^{q^\nu},\dots,(Y_n/Y_0)^{q^\nu})\in F'[\theta'_w]$ according to the isomorphism (2). This completes the proof of the lemma.

The following assertion was actually proved, for example, in [14].

LEMMA 2.8. Let $\mathcal{U}\subset\mathbb{P}^n(\bar{K})$ be a variety of degree $\deg\mathcal{U}\leqslant d$, defined over some infinite or sufficiently large finite field K and $\mathcal{U}\subset W\subset\mathbb{P}^n$, where W is a projective variety. Then there exists a homogeneous polynomial $g\in K[X_0,\dots,X_n]$ such that $\deg(g)\leqslant d$ and g vanishes identically on U and, moreover, for any absolutely irreducible component W$_1$ of the variety W, which is not an absolutely irreducible component of the variety U, the dimension $\dim(W_1\cap\{g=0\})=\dim(W_1)-1$.

Proof. Let $\mathcal{U}=\bigcup_i\mathcal{U}_i$ be the decomposition into components which are defined and irreducible over K. We prove the assertion of the lemma respectively for each component U$_i$. As a result, we get polynomials g$_i$ and after this one can set $g=\prod_i g_i$, keeping in mind that

$deg(\mathcal{U}) = \sum_i deg(\mathcal{U}_i)$. Hence in what follows, without loss of generality, we shall assume that the variety U is defined and irreducible over K. Then all absolutely irreducible components of the variety U have the same dimension.

We choose in each component W_1, which is not a component of the variety U, one point $\alpha_{W_1} \in W_1 \setminus \mathcal{U}$. From considerations of "general position" (cf., e.g., [14]) it follows that there exists a (surjective) projection $\pi: \mathbb{P}^n \to \mathbb{P}^{(dim(\mathcal{U})+1)}$ with center in a suitable (n − dim U − r)-dimensional plane $L \subset \mathbb{P}^n$, defined over the field K, such that $dim\overline{\pi(\mathcal{U})} = dim(\mathcal{U})$ and $\pi(\alpha_{W_1}) \in \overline{\pi(\mathcal{U})}$ for all components W_1. For convenience of notation we shall assume that $\pi(X_0 : \ldots : X_n) = (X_0 : \ldots : X_{dim\mathcal{U}+1})$. Moreover, without loss of generality we shall assume that $\mathcal{U} \not\subset \{X_0 = 0\}$.

Since U is defined over K (cf. the proof of Lemma 2.6), the homomorphism $\overline{K} \otimes_K K[X_1/X_0, \ldots, X_n/X_0] \to \overline{K}[\mathcal{U} \cap \{X_0 \neq 0\}]$ is an isomorphism (here and later, X_i/X_0 are considered as rational functions either on U or on $\overline{\pi(\mathcal{U})}$). To the dominant morphism $\pi: \mathcal{U} \to \overline{\pi(\mathcal{U})}$ corresponds the dual imbedding of rings $\overline{K}[\overline{\pi(\mathcal{U})} \cap \{X_0 \neq 0\}] = \overline{K}[X_1/X_0, \ldots, X_{dim\mathcal{U}+1}/X_0] \hookrightarrow \overline{K}[\mathcal{U} \cap \{X_0 \neq 0\}]$. Our next goal is to show that the homomorphism $\tau: \overline{K} \otimes_K K[X_1/X_0, \ldots, X_{dim(\mathcal{U})+1}/X_0] \to \overline{K}[\overline{\pi(\mathcal{U})} \cap \{X_0 \neq 0\}]$ is an isomorphism. Obviously, τ is an epimorphism. On the other hand, the homomorphism $\overline{K} \otimes_K K[X_1/X_0, \ldots, X_{dim(\mathcal{U})+1}/X_0] \to \overline{K} \otimes_K K[X_1/X_0, \ldots, X_n/X_0]$ is a monomorphism due to the fact that the tensor product over a field preserves injectiveness [3]. It follows from this that τ is also injective and, consequently, $\overline{\pi(u)}$ is defined over K (see the proof of Lemma 2.6).

Further, $\overline{\pi(u)}$ is a hypersurface in $\mathbb{P}^{dim(\mathcal{U})+1}$ and let $g \in K[X_0, \ldots, X_{dim(\mathcal{U})+1}]$ define $\pi(u)$. Obviously, $deg(g) = deg(\overline{\pi(\mathcal{U})}) \leq deg(\mathcal{U}) \leq d$ [3]. It is straightforward to verify that the polynomial g is the one sought. This completes the proof of the lemma.

COROLLARY. Let $\mathcal{U} \subset \mathbb{A}^n(\overline{K})$ be a variety defined over the field K, all of whose components have the same dimension n − m. Let us assume that the linear forms $L_1, \ldots, L_{n-m+1} \in K[X_1, \ldots, X_n]$ have the property that the rational functions $L_1, \ldots, L_{n-m}$ form a transcendence basis for all components of the variety U. Then the ideal $I \subset K[Y_1, \ldots, Y_{n-m+1}]$ of relations on U between $L_1, \ldots, L_{n-m+1}$ is principal and has a generator $(\Phi) = I$, where $\Phi \in K[Y_1, \ldots, Y_{n-m+1}]$ is a polynomial of degree $deg\,\Phi \leq deg\,\mathcal{U}$. If U is irreducible over K, then Φ is also irreducible over K.

Proof. We consider the projection $\pi: \mathbb{A}^n \to \mathbb{A}^{n-m+1}$, defined by the formula $(X_1, \ldots, X_n) \to (L_1, \ldots, L_{n-m+1})$. It follows from Lemma 2.8 that the variety $\overline{\pi(u)}$ is defined over K. By the hypothesis of the corollary, any component of the variety $\overline{\pi(u)}$ has dimension (n − m), and, consequently, $\overline{\pi(u)}$ is a hypersurface in $\mathbb{A}^{n+m+1}$, defined by some polynomial $\Phi \in K[Y_1, \ldots, Y_{n-m+1}]$ of degree $deg(\Phi) = deg(\overline{\pi(\mathcal{U})}) \leq deg(\mathcal{U})$ (see the proof of Lemma 2.8). If U is irreducible, then $\pi(u)$ is also irreducible, and, consequently, Φ is irreducible, which completes the proof of the corollary.

We proceed now to the construction of the required family of polynomials $\psi_0^{(w)}, \ldots, \psi_N^{(w)}$, where $N \leq (3d^{(m+1)})^n$. The polynomials $\psi_0^{(w)}, \ldots, \psi_N^{(w)}$ form a basis for the linear space $\mathcal{J}$ over the field F of all homogeneous polynomials $g \in F[Y_0, \ldots, Y_n]$ of degree $q^\nu d^{(m+1)}$

(we recall that $q^{\nu} \deg W_w \leqslant q^{\nu} d^{m+1}$), such that $g(Y_0,\dots,Y_n)=\tilde{g}(Y_0^{q^{\nu}},\dots,Y_n^{q^{\nu}})$ for some polynomial $\tilde{g} \in F[Y_0,\dots,Y_n]$, $\deg \tilde{g} = d^{(m+1)}$ and such that $g(1, Y_1/Y_0,\dots,Y_n/Y_0)=0$ in the field $F'[\theta'_w]$ (the latter, according to Lemma 2.7, is equivalent to the vanishing of the polynomial g identically on the variety W_w). To construct $\psi_0^{(w)},\dots,\psi_N^{(w)}$ the algorithm solves a system of linear equations with coefficients from F, in which the unknowns are the coefficients of the polynomial $\tilde{g}$, using the expressions for $(Y_i/Y_0)^{q^{\nu}}$ from (2). The number N obviously does not exceed the dimension of the space of all homogeneous polynomials of degree $d^{(m+1)}$, i.e., is not greater than $\binom{d^{m+1}+n}{n} < (3d^{(m+1)})^n$.

According to Lemma 2.8 (we apply it to the different situations $K=F$, $\mathcal{U}=W_w$, $W=\mathcal{U} \cup \{\Omega\}$ for arbitrary points $\Omega \in \mathbb{P}^n(\bar{F}) \setminus \mathcal{U}$ of the variety $W_w=\{\psi_0^{(w)}=\dots=\psi_N^{(w)}=0\}$, in view of the fact that $\deg W_w \leqslant d^{(m+1)}$ by what was proved above. This completes the description of the inductive step of the algorithm for constructing the tree of components.

Now we proceed to get the upper bounds on the length of description of the coefficients of the system of equations constructed defining a component, a generic point, and the time in which the algorithm works, formulated in Sec. 3.

We need the following commutative diagram of rings:

$$\begin{tikzcd}
F[Z_1,\dots,\overset{\overset{\Lambda_2}{\parallel}}{Z_n}]/(\bar{h}_1,\dots,\bar{h}_{m+1}) \arrow[d, "\sigma_2"] & H[T_1,\dots,T_l,T,\overset{\overset{\Lambda_1}{\parallel}}{Z_1},\dots,Z_n]/(\varphi,\bar{\bar{h}}_1,\dots,\bar{\bar{h}}_{m+1}) \arrow[l] \arrow[d] \\
F[Y_1/Y_0,\dots,Y_n/Y_0] & H[T_1,\dots,T_l,h,Y_1/Y_0,\dots,Y_n/Y_0], \arrow[l, hook]
\end{tikzcd}$$

where $\bar{h}=h_i(1,Z_1,\dots,Z_n)$ and the polynomials $\bar{\bar{h}}_i$ are obtained from $\bar{h}_i$ by substituting T instead of h. The ratios Y_i/Y_0 are considered as rational functions on W_w. By the action of the epimorphisms σ_1, σ_2 the elements $Z_1,\dots,Z_n$ are mapped into $Y_1/Y_0,\dots,Y_n/Y_0$ respectively. We consider the multiplicatively closed set $S=H[T_1,\dots,T_l]\setminus(\varphi) \hookrightarrow \Lambda_1$. Then the rings in the left column of the diagram are the localizations of the corresponding rings from the right column with respect to S and $S^{-1}\operatorname{Ker}\sigma_1=\operatorname{Ker}\sigma_2$. Consequently, between the prime ideals which are contained in $\operatorname{Ker}\sigma_1$ and $\operatorname{Ker}\sigma_2$ there exists a bijective correspondence, preserving the inclusion relation (cf. [3]). Our next goal is to prove that $\operatorname{Ker}\sigma_1 \subset \Lambda_1$ is a minimal prime ideal. For this it suffices to show that $\operatorname{Ker}\sigma_2$ is a minimal prime ideal.

We consider another commutative diagram:

$$\begin{tikzcd}
\Lambda_3=F^{q^{-\infty}}[Z_1,\dots,Z_n]/(\bar{h}_1,\dots,\bar{h}_{m+1}) \arrow[d, "\sigma_3"] & F[Z_1,\dots,Z_n]/(\bar{h}_1,\dots,\bar{h}_{m+1}) \arrow[l, hook] \arrow[d, "\sigma_2"] \\
F^{q^{-\infty}}[W_w \cap \{Y_0 \neq 0\}] & F[Y_1/Y_0,\dots,Y_n/Y_0]. \arrow[l, hook]
\end{tikzcd}$$

Keeping in mind that the variety $W_w \cap \{Y_0 \neq 0\}$ is defined and irreducible over $F^{q^{-\infty}}$, and, consequently, $F^{q^{-\infty}}[W_w \cap \{Y_0 \neq 0\}]$ is an integral domain, we get that $\operatorname{Ker}\sigma_3$ is a prime ideal. Analogously, $\operatorname{Ker}\sigma_2$ and $\operatorname{Ker}\sigma_2$ are also prime ideals. Moreover, since $W_w \cap$

$\{Y_0 \neq 0\}$ is a component of the variety $\{\bar{h}_1=\ldots=\bar{h}_{m+1}=0\}$, one has $\operatorname{Ker}\sigma_3 \subset \Lambda_3$ is a minimal prime ideal. Since in the last diagram the horizontal arrows give integral purely inseparable extensions of rings, there exists a bijective correspondence between the prime ideals of the rings Λ_2 and Λ_3, and this correspondence preserves the inclusion relation (cf. [3]). Consequently, $\operatorname{Ker}\sigma_2 \subset \Lambda_2$ (it corresponds to $\operatorname{Ker}\sigma_3$) is also a minimal prime ideal, which completes the proof of the following lemma.

LEMMA 2.9. $\operatorname{Ker}\sigma_1$, $\operatorname{Ker}\sigma_2$, and $\operatorname{Ker}\sigma_3$ are minimal prime ideals.

This means that $\operatorname{Ker}\sigma_1$ is the ideal of some component U_W defined over the field H (the latter follows from the fact that the field H = H^q is perfect) and irreducible over H of the variety $\{\varphi=\bar{\bar{h}}_1=\ldots=\bar{\bar{h}}_{m+1}=0\}\subset \mathbb{A}^{n+\ell+1}(\bar{H})$. We recall that it follows from Theorem 2.3 of Sec. 2 that the primitive element constructed earlier, $\theta'_W=\sum_{n-m\leq j\leq n}\gamma'_j(Y_j/Y_0)^{q^\nu}$, where $\gamma'_i \in H$, consequently $\theta^{(1)}_W=(\theta'_W)^{q^{-\nu}}=\sum_{n-m\leq j\leq n}\gamma^{(1)}_j(Y_j/Y_0)$, where $\gamma^{(1)}_i=(\gamma'_i)^{q^{-\nu}}\in H$.

Now we apply the corollary to Lemma 2.8, setting $u=u_W$, K = H in it, and taking as the linear forms $L_1,\ldots,L_{\ell+n-m}$ respectively $T_1,\ldots,T_\ell,Y_1/Y_0,\ldots,Y_{n-m-1}/Y_0$ $\theta^{(1)}_W$. It follows from the corollary that $\Phi(T_1,\ldots,T_\ell,Y_1/Y_0,\ldots,Y_{n-m-1}/Y_0,\theta^{(1)}_W)=0$ on U_W, where $0\not\equiv\Phi\in H[Z_1,\ldots,Z_{\ell+n-m}]$ is a polynomial which is irreducible over H and $\deg\Phi\leq\deg U_W\leq\deg\varphi$. $\prod_{1\leq i\leq m+1}\deg_{T_1,\ldots,T_\ell,T,Z_1,\ldots,Z_n}(\bar{\bar{h}}_i)\leq d_1(d+d_1+d_2-1)^{m+1}$, according to Bezout's inequality (cf., e.g., [7]).

We recall (see Introduction) that the polynomial $\psi\in F(t_1,\ldots,t_{n-m+1})[Z]=F'[Z]$ can be represented in the form $\psi=\sum_i\sum_{0\leq j<\deg_T(\varphi)}\left(\frac{a_{ij}}{b}\right)h^jZ^i$, where $a_{ij},b\in H[T_1,\ldots,T_\ell,t_1,\ldots,t_{n-m-1}]$ for all i, j, and the degree deg (b) is as small as possible. The polynomials a_{ij}, b are uniquely defined up to factors from H*. The degrees $\deg_{T_1,\ldots,T_\ell t_1,\ldots,t_{n-m-1}}(\psi)=\max_{ij}\{\deg_{T_1,\ldots,T_\ell,t_1,\ldots,t_{n-m-1}}(a_{ij}),$ $\deg_{T_1,\ldots,T_\ell t_1,\ldots,t_{n-m-1}}(b)\}$. We consider the polynomial $\Phi^{(1)}(Z)=\Phi^q(T_1,\ldots,T_\ell,t_1,\ldots,t_{n-m-1},Z^{q^\nu})\in F'[Z]$. The degree with respect to the variables $T_1,\ldots,T_\ell\, t_1,\ldots,t_{n-m-1}$ of any factor $\Phi^{(1)}_1|\Phi^{(1)}$ which is irreducible over F and with leading coefficient $lc_Z(\Phi^{(1)}_1)=1$ can be bounded above by some polynomial in $q^\nu\cdot\deg\Phi$, d_1 according to Chapter I of [4]. Considering that $\Phi^{(1)}(\theta'_W)=0$, we get that $\Phi^{(2)}(\theta'_W)=0$ holds for a suitable divisor $\Phi_2\in F'[Z]$ of the polynomial $\Phi^{(1)}$ which is irreducible over F and with leading coefficient $lc_Z(\Phi^{(2)})=1$. The elements $t_1,\ldots,t_{n-m-1}$ are algebraically independent over the field F, so $\Phi^{(2)}$ coincides with the polynomial Φ_W (constructed previously in Sec. 3; cf. (2)) up to a factor from F*, and since $lc_Z(\Phi^{(2)})=lc_Z(\Phi_W)=1$ one has $\Phi^{(2)}=\Phi_W$.

Now for each $n-m\leq i\leq n$ we apply the corollary to Lemma 2.8, again setting U = U_W, K = H, and as the linear forms $L_1,\ldots,L_{\ell+n-m}$ we take $T_1,\ldots,T_\ell,Y_1/Y_0,\ldots,Y_{n-m-1}/Y_0,Y_i/Y_0$. It follows from the corollary that $\Phi_i(T_1,\ldots,T_\ell,Y_1/Y_0,\ldots,Y_{n-m-1}/Y_0,Y_i/Y_0=0$ on U_W for some polynomial $0\not\equiv\Phi_i\in H[Z_1,\ldots,Z_{\ell+n-m}]$ which is irreducible over H, such that $\deg\Phi_i\leq$ $\deg U_W\leq d_1(d+d_1+d_2-1)^{m+1}$. According to Theorem 2.3 and (2) one has $(Y_i/Y_0)^{q^{\nu_i}}\in F'[\theta'_W]$, where q^{ν_i} is as small as possible, so $(Z^{q^{\nu_i}}-(Y_i/Y_0)^{q^{\nu_i}})|\Phi_i(T_1,\ldots,t_\ell,t_1,\ldots,t_{n-m-1},Z)$ in the ring $F'[\theta'_W][Z]$ (analogously to the way this was done above, we represent the elements of the latter ring in the form

$$\sum_{j_1 j_2 j_3} \frac{a_{j_1 j_2 j_3}(T_1,\ldots,T_l, t_1,\ldots,t_{n-m-1})}{b(T_1,\ldots,T_l, t_1,\ldots,t_{n-m-1})} \eta^{j_2} (\theta'_w)^{j_3} Z^{j_1}$$

It follows from this that $q^{\nu_i} \leqslant \deg \Phi_i \leqslant d_1(d+d_1+d_2-1)^{m+1}$. Further, again according to Chapter I of [4], one can assert that $\deg_{T_1,\ldots,T_l t_1,\ldots,t_{n-m-1}}(Y_i/Y_0)^{q^{\nu_i}}$ can be bounded above by a polynomial in $\deg \Phi_i, d_1, \deg \Phi^{(2)}$, and hence by a polynomial in $(d+d_1+d_2)^{m+1}$, by virtue of what was proved above.

We turn now to the bounds for the length of description of the coefficients from H of all the rational functions constructed and the degree $\deg_{T_1,\ldots,T_l}(\psi_j^{(w)})$. According to the inductive hypothesis, $l(\psi_j^{(w)}), l(\Phi_\gamma), l((X_j/X_{j_0})^{q^{\nu_j}}) \leqslant (M_1+M_2+l)P((d+d_1+d_2)^{m^2 n})$ for a suitable polynomial P, independent of m. Then, applying Theorem 2.3 to the system (1), we get that $l(\Phi_w), l((Y_j/Y_0)^{q^{\nu_j}}$ can be bounded above by $M_3=((M_1+M_2+l)P((d+d_1+d_2)^{m^2 n})+(M_1 + (l+n)n^2 \log(d+d_1+d_2))P_1((d+d_1+d_2)^{2m+3}) \leqslant (M_1+M_2+l)P((d+d_1+d_2)^{(m+1)^2 n})$ for a suitable polynomial P_1. The application of Theorem 2.3 of Sec. 2 and the construction of Φ_w and $(Y_j/Y_0)^{q^{\nu_j}}$ in Sec. 3 are effected by the algorithm in time which is polynomial in $((d+d_1+d_2)^{m^2} d_1 (d+d_1+d_2)^{m(n-m)})^{(n-m+l)} M_1 M_2 (d+d_1+d_2)^{m^2 n}(l+n)(q+1)$ i.e., in time which is polynomial in $M_1 M_2 (d+d_1+d_2)^{mn(l+n)}(q+1)$.

We recall that then the algorithm in Sec. 4 constructs a basis $\psi_0^{(w)},\ldots,\psi_N^{(w)}$ of all solutions of some homogeneous linear system with coefficients from the field F (see above the description of the algorithm). The unknowns in this system are the coefficients of the polynomial $\tilde{g}$, so the number of unknowns is less than $(3d^{(m+1)})^{n+1}$. The equations are obtained as a result of substituting the expressions for $(Y_i/Y_0)^{q^{\nu_i}}$ in the polynomial g and setting the coefficients of $t_1,\ldots,t_{n-m-1}, \theta'_w$ in the expression obtained equal to zero. By what was proved above, the degree of the rational function $g(1, Y_1/Y_0,\ldots,Y_n/Y_0) \in F(t_1,\ldots, t_{n-m-1})[\theta'_w]$ with respect to $t_1,\ldots,t_{n-m-1}$ can be bounded above by a polynomial in $(d+d_1+d_2)^{m+1}$. Thus, the number of equations of the linear system considered can be bounded above by a polynomial in $(d+d_1+d_2)^{(m+1)(n-m)}$. The degrees with respect to $T_1,\ldots,T_l$ of the matrix of coefficients of this system are bounded above by a polynomial in $(d+d_1+d_2)^{m+1}$. The lengths of description of the coefficients from H of this system can be bounded, according to what was proved above, by $M_3 P_2((d+d_1+d_2)^{m+1} n-m)$ for a suitable polynomial P_2, independent of m.

From this, according to Cramer's rule, it follows that $\deg_{T_1,\ldots,T_l}(\psi_j^{(w)})$ is less than a polynomial in $(d+d_1+d_2)^{(m+1)(n-m)}$ for any $0 \leqslant j \leqslant N$. The lengths of description $l(\psi_j^{(w)}) \leqslant M_3 P_3((d+d_1+d_2)^{(m+1)(n-m)}) \leqslant (M_1+M_2+l)P((d+d_1+d_2)^{(m+1)^2 n})$ for a suitable polynomial P_3. The algorithm solves the system in time which is polynomial in $M_3(d+d_1+d_2)^{(m+1)nl}$ (cf. [21]).

At the end of its work the algorithm returns from the coordinates {Yi} introduced earlier to the original coordinates {Xi}. For this we need the following lemma.

LEMMA 2.10. Let W_w be a variety, irreducible over the field F, and let the isomorphism (2) define a generic point of it (cf. Sec. 3). Further, let $U_0,\ldots,U_{n-m}$ be linear forms in $X_0,\ldots,X_n$ with coefficients from F, where U_0 does not vanish identically on W_w. Then

a) if $\mathcal{U}_1/\mathcal{U}_0,\dots,\mathcal{U}_s/\mathcal{U}_0$ are algebraically dependent on W_w for some s, then there exists a homogeneous polynomial $0\not\equiv\chi\in F[Z_0,\dots,Z_s]$ such that $\deg\chi\leqslant q^\nu\deg W_w$ and $\chi(\mathcal{U}_0,\dots,\mathcal{U}_s)=0$ on W_w;

b) if $\{\mathcal{U}_1/\mathcal{U}_0,\dots,\mathcal{U}_{n-m-1}/\mathcal{U}_0\}$ is some transcendence basis for the variety W_w over $\bar{F}$, then the element $(\mathcal{U}_{n-m}/\mathcal{U}_0)^{q^\mu}$ is separable over the field $F(\mathcal{U}_1/\mathcal{U}_0,\dots,\mathcal{U}_{n-m-1}/\mathcal{U}_0)$, where $q^{\nu-1}\deg W_w < q^\mu\leqslant q^\nu\deg W_w$ when $q>0$ or $q^\mu=1$ if char (F) = 0.

Proof. a) We can assume without loss of generality that $\mathcal{U}_0,\dots,\mathcal{U}_s$ are linearly independent on W_w over F because, if not, a) is trivial. According to the proof of the corollary to Lemma 2.8, and according to Lemma 2.6, there exists a homogeneous polynomial $0\not\equiv\chi_1\in F^{q^{-\nu}}[Z_0,\dots,Z_s]$ such that $\deg(\chi_1)\leqslant\deg W_w$ and $\chi_1(\mathcal{U}_0,\dots,\mathcal{U}_s)=0$ on W_w. Then the polynomial $\chi=\chi_1^{q^\nu}$ satisfies the requirements of point a).

b) We consider a polynomial $0\not\equiv\chi\in F[Z_1,\dots,Z_{n-m}]$ such that $\chi(\mathcal{U}_1/\mathcal{U}_0,\dots,\mathcal{U}_{n-m}/\mathcal{U}_0)=0$ on W_w and $\deg\chi\leqslant q^\nu\deg W_w$, which exists according to point a). Then the exponents of the variable Z_{n-m} in this polynomial cannot be divisible by $q^{\mu+1}$ (when $q>0$), from which the assertion of point b) follows.

The algorithm, for each component W_w, finds some transcendence basis of it of the form $X_{j_1}/X_{j_0},\dots,X_{j_s}/X_{j_0}$. First of all, the algorithm chooses some X_{j_0} not vanishing identically on W_w. After this the algorithm constructs by induction on s a family of rational functions $\{X_{j_1}/X_{j_0},\dots,X_{j_s}/X_{j_0}\}$, algebraically independent of W_w over F. Let a family, consisting of s such functions, be constructed already. The algorithm considers $X_{j_s+1}/X_{j_0}, X_{j_s+2}/X_{j_0},\dots$ successively, and verifies, for each of these functions, its algebraic dependence with $\{X_{j_1}/X_{j_0},\dots,X_{j_s}/X_{j_0}\}$ on W_w. If $X_{j_1}/X_{j_0},\dots,X_{j_s}/X_{j_0}, X_{j_s+i}/X_{j_0}$ are algebraically dependent on W_w, then there exists a polynomial $0\not\equiv\chi\in F^{q^{-\nu}}[Z_1,\dots,Z_{s+1}]$, such that $\deg\chi\leqslant\deg W_w$ and $\chi^{q^\nu}(X_{j_1}/X_{j_0},\dots,X_{j_s}/X_{j_0},X_{j_s+i}/X_{j_0})$ is equal to zero on W_w, according to Lemma 2.10a). Consequently, the polynomial χ^{q^ν}, if it exists, can be found with the help of substituting in χ^{q^ν} the expressions for $(X_j/X_{j_0})^{q^\nu}$ from the generic point (2), setting the coefficients from H of the monomials in $T_1,\dots,T_\ell,h,t_1,\dots,t_{n-m-1},\theta'_w$ in the expressions obtained equal to zero, and then solving the system of homogeneous linear equations obtained over H. The unknowns in this system are the coefficients from H of the monomials in $T_1,\dots,T_\ell,h,Z_1,\dots,Z_{s+1}$ of the polynomial χ^{q^ν} (we use Lemma 2.7 here).

Now we renumber the indices so that $j_i\to i$, $0\leqslant i\leqslant n-m-1$. It follows from Lemma 2.10b) that there exists a primitive element θ_w, such that $F'[\theta_w]\simeq F(X_1/X_0,\dots,X_{n-m-1}/X_0, (X_{n-m}/X_0)^{q^\mu},\dots,(X_n/X_0)^{q^\mu})$. To get θ_w the algorithm constructs, analogously to Sec. 2, a sequence of elements $\theta_w^{(n-m)}=(X_{n-m}/X_0)^{q^\mu},\theta_w^{(n-m+1)},\dots$. If $\theta_w^{(i)}$ is already constructed, then we consider $d^{m+1}+1\geqslant\deg W_w+1$ of the elements of the form $\theta_w^{(i)}+\alpha_j(X_{i+1}/X_0)^{q^\nu}$ where $0\leqslant j\leqslant d^{m+1}$. and {dj} are pairwise different elements of the field H. For each of them the algorithm finds the minimal polynomial over the field $F(X_1/X_0,\dots,X_{n-m-1}/X_0)$, based on what was just said. As $\theta_w^{(i+1)}$ one can take any of the elements of the form $\theta_w^{(i)}+\alpha_j(X_{i+1}/X_0)^{q^\mu}$, whose minimal polynomial has highest degree. Finally, we set $\theta_w=\theta_w^{(n)}$.

Now we turn to getting an estimate for the procedure of returning to the coordinates {Xi} described. In order to estimate $\deg_{T_1,\dots,T_\ell}(\chi^{q^\nu})$, it is first necessary to solve a system of linear equations in which the unknowns are the coefficients from F of the monomials in $Z_1, \ldots, Z_{s+1}$ of the polynomial χ^{q^ν}. Then $\deg_{T_1,\ldots T_\ell}(\chi^{q^\nu})$ is bounded above by a polynomial in $(d+d_1+d_2)^{m(n-m+1)}$, analogously to the way the degree $\deg_{T_1,\ldots,T_\ell}(\psi_j^{(w)})$ was estimated above. The working time of the procedure described is bounded above by a polynomial in the sizes of the matrix of the linear system over H, which is solved in constructing χ^{q^ν} and of the minimal polynomials. The number of unknowns in these systems is less than a polynomial in $\deg_{Z_1,\ldots,Z_{s+1}}(\chi^{q^\nu})^{n-m}, \deg_{T_1,\ldots,T_\ell}(\chi^{q^\nu})^{\ell}$, i.e., a polynomial in $(d+d_1+d_2)^{m(n-m+1)(\ell+1)}$. The number of equations in these systems is not greater than a polynomial in

$$(\deg_{Z_1,\ldots,Z_{s+1}}(\chi^{q^\nu}))^{n-m}, (\deg_{T_1,\ldots,T_\ell}(\chi^{q^\nu}))^{\ell}, (\deg_{t_1,\ldots,t_{n-m-1}T_1,\ldots T_\ell}((X_j/X_{j_0})^{q^\nu}))^{\ell+n-m}, (\deg_{t_1,\ldots,t_{n-m-1}T_1,\ldots,T_\ell}(\Phi_w))^{n-m+1}.$$

Thus, the working time of the procedure described for returning from the coordinates $\{Y_i\}$ to the coordinates $\{X_i\}$ is bounded by a polynomial in $(d+d_1+d_2)^{m(n-m+1)(\ell+1)}$ and M_3.

In conclusion, at the very end of its work, the algorithm chooses all components which coincide, corresponding to leaves of the first type of the tree of components. For this, for each pair of components obtained, it substitutes the expressions from (2) for a generic point of one of these components into the system of equations constructed defining the other component, and conversely. By Lemma 2.7, the components coincide if and only if the results of all these substitutions are equal to zero.

Now we summarize the results of the recursive application of the algorithm described in the course of Secs. 3 and 4 in the following theorem, using the notation introduced at the beginning of Sec. 3.

THEOREM 2.4. An algorithm is constructed which finds all the components which are defined and irreducible over $F^{q^{-\infty}}$ of the variety $\{f(X_0,\ldots,X_n)=\ldots=f_{k-1}(X_0,\ldots,X_n)=0\} \subset \mathbb{P}^n(\bar{F})$ (we assume without loss of generality that $\mathrm{card}(H) \geq nd^n+2$). Namely, for any components W_ν of dimension $\dim W_\nu = n-m$ the algorithm gives a generic point of it, i.e., an isomorphism of fields

$$F(t_1,\ldots,t_{n-m})[\theta_\nu] \simeq F(X_{j_1}/X_{j_0},\ldots,X_{j_{n-m}}/X_{j_0},(X_0/X_{j_0})^{q^{\nu_0}},\ldots,(X_n/X_{j_0})^{q^{\nu_n}})$$

for suitable $0 \leq j_0 \leq n$, $0 \leq j_1 < \ldots < j_{n-m} \leq n$, where X_j/X_{j_0} are considered as rational functions on W_ν and $t_i \to X_{j_i}/X_{j_0}$, under this isomorphism (moreover $q^{\nu_j} \leq d_1(d+d_1+d_2)^m d^m$, when $q > 0$ and $q^{\nu_j}=1$, when char F = 0). The elements $t_1,\ldots,t_{n-m}$ are algebraically independent over F and $\Phi_\nu(\theta_\nu)=0$, where $\Phi_\nu \in F(t_1,\ldots,t_{n-m})[Z]$ is some separable polynomial which is irreducible over $F(t_1,\ldots,t_{n-m})$ with leading coefficient $lc_Z(\Phi_\nu)=1$ and $\deg_Z(\Phi_\nu) \leq \deg W_\nu \leq d^m$.

Moreover, the algorithm constructs a family of homogeneous polynomials $\psi_0^{(\nu)},\ldots \psi_N^{(\nu)} \in F[X_0,\ldots,X_n]$, $N \leq (3d^m)^n$, such that $W_\nu = \{\psi_0^{(\nu)}=\ldots=\psi_N^{(\nu)}=0\}$. The degrees $\deg_{T_1,\ldots T_\ell,t_1,\ldots t_{n-m}}(\Phi_\nu)$, $\deg_{T_1,\ldots T_\ell,t_1,\ldots,t_{n-m}}(X_j/X_{j_0})^{q^{\nu_j}}$ are bounded above by some polynomial in $(d+d_1+d_2)^m$; the degrees $\deg_{T_1,\ldots T_\ell}(\psi_j^{(\nu)})$ are bounded by a polynomial in $(d+d_1+d_2)^{m(n-m+1)}$ and $\deg_{X_0,\ldots X_n}(\psi_j^{(\nu)}) \leq (d+d_1+$

$d_2)^m d^m d_1$ for any i, j. The lengths of description $\ell(\Phi_v), \ell((X_j/X_{j_0})^{q_v j}), \ell(\psi_j^{(v)})$ of the coefficients from H of the corresponding elements do not exceed $(M_1+M_2+\ell)P((d+d_1+d_2)^{m^2 n})$ for a suitable polynomial P. Finally, the algorithm works (in finding W_V, under the condition that all components corresponding to vertices of level less than m have already been constructed) in time which is polynomial in $M_1 M_2 (d+d_1+d_2)^{mn(\ell+n)}(q+1)$. Thus, the total working time of the algorithm for finding all components can be bounded above by a polynomial in $M_1 M_2 (d+d_1+d_2)^{n^2(n+\ell)}(q+1)$.

LITERATURE CITED

1. B. L. Van Der Waerden, Modern Algebra [Russian translation], Parts 1 and 2, ONTI, Moscow–Leningrad (1937).
2. D. Yu. Grigor'ev, "Two reductions of graph isomorphisms to polynomial problems," J. Sov. Math., 20, No. 4 (1982).
3. O. Zariski and P. Samuel, Commutative Algebra [Russian translation], Vols. 1 and 2, IL, Moscow (1963).
4. A. L. Chistov, "Polynomial factoring algorithm for polynomials and finding components of varieties in subexponential time," J. Sov. Math., 34, No. 4 (1986).
5. D. Knuth, The Art of Computer Programming, Vol. 2, Addison-Wesley (1969).
6. S. A. Lang, Algebra, Addison-Wesley (1965).
7. I. R. Shafarevich, Fundamentals of Algebraic Geometry [in Russian], Nauka, Moscow (1972).
8. A. L. Chistov and D. Yu. Grigor'ev, "Polynomial-time factoring of the multivariable polynomials over a global field," LOMI Preprint E-5-82, Leningrad (1982).
9. A. L. Chistov and D. Yu. Grigor'ev, "Subexponential-time solving systems of algebraic equations. I." LOMI Preprint E-9-83, Leningrad (1983).
10. A. L. Chistov and D. Yu. Grigor'ev, "Subexponential-time solving systems of algebraic Equations. II," LOMI Preprint E-10-83, Leningrad (1983).
11. G. Collins, "Subresultants and reduced polynomial remainder sequences," J. Assoc. Comput. Mach., 14, No. 1, 128-142 (1967).
12. D. Yu. Grigor'ev, "Some new bounds on tensor rank," LOMI Prepring E-2-78, Leningrad (1978).
13. D. Yu. Grigor'ev, "Multiplicative complexity of a bilinear form over a commutative ring," Lect. Notes Comput. Sci., 118, 281-286 (1981).
14. J. Heintz, "Definability and fast quantifier elimination in algebraically closed field," Preprint Univ. Frankfurt, West Germany, December (1981).
15. E. Kaltofen, "A polynomial reduction from multivariate to bivariate integral polynomial factorization," in: Proc. 14th ACM Symp. Th. Comput., May, 1982, N.Y., pp. 261-266.
16. E. Kaltofen, "A polynomial-time reduction from bivariate to univariate integral polynomial factorization," in: Proc. 23rd Ann. Symp. Found. Comp. Sci., N.Y., Oct., 1982.
17. D. Lazard, "Algebre lineaire sur $k[X_1, \ldots, X_n]$ et elimination," Bull. Soc. Math. France, 105, 165-190 (1977).
18. D. Lazard, "Résolutions des systèmes d'équations algébriques," Theor. Comput. Sci., 15, 77-110 (1981).
19. D. Lazard, "Commutative algebra and computer algebra," Lect. Notes Comput. Sci., 144, 40-48 (1983).
20. A. K. Lenstra, H. W. Lenstra, and L. Lovasz, "Factoring polynomials with rational coefficients," Preprint Math. Centrum Amsterdam IW 195/82 (1982).
21. M. T. McClellan, "The exact solution of systems of linear equations with polynomial coefficients," JACM, 20, No. 4, 563-588 (1973).
22. A. Seidenberg, "Constructions in a polynomial ring over the ring of integers," Am. J. Math., 100, No. 4, 685-704 (1978).