The associated form of a variety over a field of prime characteristic p

by S. V. Keshava Hegde, Bangalore (India)

Introduction

Wei-Liang Chow and van der Waerden in a publication [1] have introduced the associated form of an irreducible variety V. If d is the dimension of V, the associated form $F(u)$ is defined as an irreducible form in $u_0, u_1, \ldots, u_n$, depending on d generic hyperplanes $u^{(1)}, \ldots, u^{(d)}$, such that $F(u)$ becomes zero as soon as the hyperplane u is specialised so as to contain one of the points of intersection of $u^{(1)}, \ldots, u^{(d)}$ with V. The form $F(u)$ is symmetric or antisymmetric in the $d + 1$ sets of variables $u, u^{(1)}, \ldots, u^{(d)}$.

André Weil in his "Foundations of Algebraic Geometry" [2] gave new definitions of the fundamental notions of algebraic geometry. In particular, he introduced the notions of algebraically disjoint and of linearly disjoint fields and he proved the theorem ([2], Th. 5, p. 18) : An extension $k(x)$ of a field k and the algebraic closure $\bar{k}$ of k are linearly disjoint if and only if k is algebraically closed in $k(x)$, and $k(x)$ separably generated over k.

W.-L. Chow used the characteristic form in his investigation of "Algebraic systems of positive cycles in an algebraic variety" [3]. In the introduction of his paper he mentioned, without prof, the following property of the characteristic form : If the variety is separably generated then the associated form has no multiple factors.

We shall investigate quite generally, how the characteristic form, which is irreducible in K, factorises in an extension field L of K, and how this factorisation is related to the splitting of V into varieties $V_1, V_2, \ldots$ irreducible over L. In particular Chow's assertion mentioned above will be proved.

1. Definitions and notations

Let us take an arbitrary field k as *ground field*. We shall assume k to be of characteristic p. *The universal extension field* Ω is obtained from k by adjunction of a countable number of indeterminates and algebraic closure. All coordinates of points and all coefficients of equations are always taken from Ω.

Let $K, L, \ldots$ stand for intermediate fields which contain k and are contained in Ω. These intermediate fields are always supposed to be generated by the adjunction of a finite number of elements to k.

An intermediate field L is said to be *separably generated* over K, if L is generated from K by adjunction of algebraically independent elements and separable algebraic functions of these elements.

A series of n coordinates $p_1, p_2, \ldots, p_n$ from Ω is called a *point of the affine space* R_n, and a *point of the projective space* S_n is a ray of the affine space R_{n+1} consisting of all points $(\omega p_0, \omega p_1, \ldots, \omega p_n)$, where $(p_0, \ldots, p_n) \neq (0, 0, \ldots, 0)$ is a fixed point of R_{n+1} and ω runs over all the elements of Ω.

A *variety* is the set of all points of R_n or S_n which satisfy a finite system of algebraic equations,

$$f_k(p_1, p_2, \ldots, p_n) = 0 \quad \text{or} \quad f_k(p_0, p_1, \ldots, p_n) = 0$$

where f_k shall be polynomials in the first case, forms in the second case with coefficients from Ω. We shall suppose that the set is non-empty.

If a variety can be represented as a union of two proper parts (subvarieties), it is said to be *divisible*. The variety is indivisible if such a representation is not possible.

If the equations that define the variety have their coefficients in K, the variety is called a *variety over* K. It is *irreducible over* K if it does not split into proper parts which are again varieties over K. By definition an indivisible variety remains irreducible over any extension field, i. e., it is *absolutely irreducible.*

A point P is said to be a *specialisation* of a point X with respect to a field K, if all equations $f(x_1, \ldots, x_n) = 0$ with coefficients from K, or in the projective case all homogenous equations $f(x_0, x_1, \ldots, x_n) = 0$, which are valid for the point X, remain valid if X is replaced by P.

An irreducible variety V over K has always a *generic point* X such that all points of V can be obtained by specialisation (with respect to K) of X. The generic point is uniquely determined by V except for isomorphisms. That is, in the affine case the coordinates $x_1, \ldots, x_n$ are uniquely determined except for a field isomorphism applied to all x_k, which leaves the elements of K unaltered. In the projective case the x_k are uniquely determined only up to a common factor ω. We may number the coordinates so that $x_0 \neq 0$ and then normalise ω so that $x_0 = 1$. The nonhomogeneous coordinates $x_1, \ldots, x_n$ of the point X are then uniquely determined but for an isomorphism. The number of the algebraically independent coordinates among the so normalised x_k is called the *dimension of* V.

The above terminology is in accordance with the suggestions of van der Waerden in one of his recent papers [4].

If $V = V_1 + V_2 + \cdots + V_r$, and all the imbedded V_i are left out and the rest have the same dimension then the variety is aid to be *unmixed* or *pure*.

We shall call with André Weil [2] an extension $K(X)$ of a field K *regular over* K or a *regular extension of* K if $\overline{K}$ (the algebraic closure of K) and $K(X)$ are linearly disjoint over K.

2. The associated form of a variety

Let V be an irreducible variety of dimension d over a field K in the projective space S_n.

Let $u^{(1)}, \ldots, u^{(d)}$ be hyperplanes with indeterminate coordinates $u_k^{(\nu)}$. The indeterminates $u_k^{(\nu)}$ shall be algebraically independent over K. The hyperplanes intersect V in a finite number of points $X^{(1)}, \ldots, X^{(g)}$, conjugate over K.

Now we take in addition a further series of indeterminates,

$$u_k (k = 0,1, \ldots, n) \ .$$

The product,

$$P = \prod_1^g (u_0 x_0^{(\nu)} + u_1 x_1^{(\nu)} + \cdots + u_n x_n^{(\nu)}) \tag{1}$$

is a symmetric function in $X^{(1)}, \ldots, X^{(g)}$.

In case of characteristic zero the product is rational in

$$K(u, u^{(1)}, \ldots, u^{(d)}):$$

In this case we write $P = Q(u, u^{(1)}, \ldots, u^{(d)})$.

In case of characteristic p a p^e th power of the product P is rational and we write, taking e to be the lowest possible exponent,

$$P^q = Q(u, u^{(1)}, \ldots, u^{(d)}), \quad (q = p^e) \ . \tag{2}$$

Q is integral in u and rational in $u^{(1)}, \ldots, u^{(d)}$. We can, therefore, write

$$Q = \frac{A}{B} F(u, u^{(1)}, \ldots, u^{(d)}) \tag{3}$$

where A and B depend only on $u^{(1)}, \ldots, u^{(d)}$, while F is integral in $u, u^{(1)}, \ldots, u^{(d)}$, and contains no more factors depending only on $u^{(1)}, \ldots, u^{(d)}$.

Q is irreducible in $K(u^{(1)}, \ldots, u^{(d)})[u]$ and hence F is irreducible in $K[u^{(1)}, \ldots, u^{(d)}, u]$.

For, if F is reducible in $K[u^{(1)}, \ldots, u^{(d)}, u]$, let $F = GH$, where G and H both contain u. Consequently, $Q = \frac{A}{B} GH = \left(\frac{A}{B} G\right) H$, contrary to hypothesis.

The irreducible form F is called the *associated form of* V.

We shall now show that a permutation of the variable series $u, u^{(1)}, u^{(2)}, \ldots, u^{(d)}$ leaves F unaltered up to a factor ± 1.

The condition,

$$F(v, v^{(1)}, \ldots, v^{(d)}) = 0$$

is necessary and sufficient in order that the hyperplanes $v, v^{(1)}, \ldots, v^{(d)}$ have a point in common with V ([5] § 36, p. 157).

In the same way the condition,

$$F(v^{(1)}, v, \ldots, v^{(d)}) = 0$$

(with v and $v^{(1)}$ interchanged) is necessary and sufficient in order that $v, v^{(1)}, \ldots, v^{(d)}$ have a point in common with V. The two conditions being equivalent, and both forms $F(u, u^{(1)}, \ldots, u^{(d)})$ and

$$F(u^{(1)}, u, u^{(2)}, \ldots, u^{(d)})$$

being irreducible, they must be proportional:

$$F(u^{(1)}, u, \ldots, u^{(d)}) = \gamma F(u, u^{(1)}, \ldots, u^{(d)})$$

where γ is a constant. The square of a transposition being identity, γ^2 must be equal to 1, so γ can only be $+1$ or -1. The same is true for all transpositions of two of the $d+1$ series $u, u^{(1)}, \ldots, u^{(d)}$.

Since every permutation is a product of two transpositions, it follows that every permutation leaves F invariant but for a factor ± 1.

In the following we shall be concerned only with the associated forms of varieties over a field K of characteristic p, where p is a prime number.

3. The behaviour of the associated form over an extended field

Let V be irreducible over a field K and d be the dimension of V. Then over any extension L of K, V is an unmixed variety of dimension d.

This theorem, which is proved by Hodge and Pedoe ([6], § 11, Th. 1,

p. 69) for the case of a field of characteristic zero, is also true for the case of a field of characteristic $p > 0$, since the conditions mentioned in the proof of the above theorem are independent of the characteristic of the field.

Let the field K be of characteristic p. The associated form F defined in § 1 is irreducible over K.

Let $L = K(t_1, \ldots, t_s)$ be a purely transcendental extension. That is, let $t_1, \ldots, t_s$ be algebraically independent over K. Now we shall prove

Theorem 1. *A purely transcendental extension $L = K(t_1, \ldots, t_s)$ leaves F and V irreducible.*

Proof: Suppose F could be factorised in $K(t)[u]$, e. g.

$$F(u) = g(t, u) \cdot h(t, u) \ .$$

By a well known theorem of Gauss ([7] I, § 23) this factorisation would imply a factorisation in $K[t, u] = K[t][u]$, say

$$F(u) = G(t, u) \cdot H(t, u)$$

where G and H are polynomials in t and u. Putting all $t_i = 0$, we would obtain a factorisation of $F(u)$ in K, which is impossible, i. e. $F(u)$ cannot be factorised in $K(t_1, \ldots, t_s) = L$.

If V were reducible, the points of intersection $X^{(\nu)}$ would split up into the generic points of V_1, generic points of V_2 and so on. This implies a factorisation of $F(u)$, as will be shown in the proof of theorem 4.

Theorem 2. *A transcendental extension L of K, in which the form F can be factorised into h factors,*

$$F(u) = G_1(u)\, G_2(u) \ldots G_h(u), \qquad (in \quad L[u])$$

always contains an algebraic extension A, in which $F(u)$ can be factorised in the same way:

$$F(u) = C F_1(u)\, F_2(u) \ldots F_h(u)\,, \qquad (in \quad A[u])$$

so that the factors F_j are not essentially different from G_j.

Proof: For the sake of convenience, the u_j and $u_j^{(i)}$ of our earlier notation will be replaced by $u_j^{(0)}$ and $u_j^{(i)}$. Let F be of order g and let k be any integer greater than g which we can choose once and for all. Let us fix $(d+1)(n+1)$ integers r_{ij} such that

$$0 \leqq r_{00} < r_{01} < \cdots < r_{0n} < r_{10} < \cdots < r_{1n} < \cdots < r_{d0} < \cdots < r_{dn} \ .$$

Let $\Phi(u_j^{(i)})$ be any polynomial in the $u_j^{(i)}$ such that no $u_j^{(i)}$ appears to a power greater than g and let $\varphi(t)$ be the polynomial in t obtained by replacing $u_j^{(i)}$ in $\Phi(u_j^{(i)})$ by t to the power $k^{r_{ij}}$ $(i = 0, \ldots, d\,;\ j = 0, \ldots, n)$. Consider now a term in $\Phi(u_j^{(i)})$ in which $u_j^{(i)}$ has exponent ϱ_{ij}. From this we get a term in $\varphi(t)$ with the exponent $\Sigma\,\varrho_{ij}\,k^{r_{ij}}$. Another term in $\Phi(u_j^{(i)})$ in which $u_j^{(i)}$ has exponent σ_{ij} leads to a term in t with exponent $\Sigma\,\sigma_{ij}\,k^{r_{ij}}$ and since $\varrho_{ij} \leqq g < k$, $\sigma_{ij} \leqq g < k$ we have $\Sigma\,\varrho_{ij}\,k^{r_{ij}} = \Sigma\,\sigma_{ij}\,k^{r_{ij}}$ if and only if $\sigma_{ij} = \varrho_{ij}$ for $i = 0, \ldots, d\,;\ j = 0, 1, \ldots, n$. Therefore, the set of coefficients of $\Phi(u_j^{(i)})$ must exactly be the same as the set of coefficients of $\varphi(t)$.

Now let L be any extension of K over which the associated form $F(u)$ becomes reducible,

$$F(u) = F(u^{(0)}, u^{(1)}, \ldots, u^{(d)}) = \prod_{j=1}^{h} G_j(u^{(0)}, u^{(1)}, \ldots, u^{(d)}) = \prod_{j=1}^{h} G_j(u) \ .$$

Let the corresponding polynomials in t be

$$f(t) = \prod_{j=1}^{h} g_j(t) \ .$$

If C_j is the leading coefficient of $g_j(t)$, i. e., the coefficient of the highest power of t, we may write $g_j(t) = C_j\,f_j(t)$, where $f_j(t)$ have leading coefficient 1. Hence $f(t) = \prod_{j=1}^{h} C_j\,f_j(t)$. The set of coefficients of $g_j(t)$ is the same as the set of coefficients of $G_j(u)$. Hence we can write $G_j(u) = C_j F_j(u)$ and $F(u) = \prod_{j=1}^{h} C_j F_j(u)$ corresponding to the above equation in t.

Now each coefficient of $f_j(t)$ is a symmetric function of the roots and hence lies in the root field B of the polynomial $f(t)$ over K. The coefficients of $f_j(t)$ also lie in L, because they are quotients of coefficients of $g_j(t)$. Hence they lie in the intersection field A of B and L. Thus the theorem is proved.

Theorem 3. *F can be split into absolutely irreducible factors $F = C F_1^q \cdot F_2^q \ldots F_h^q$ with coefficients in an algebraic extension field of K.*

Proof: If F can be factorised, let us write $F = F_1 \cdot F_2$. If F_1 or F_2 can be factorised we shall continue the factorisation until we arrive at absolutely irreducible factors : $F = G_1 G_2 \ldots G_h$.

By theorem 2, the G_j may be replaced by F_j with coefficients from an algebraic extension A. Thus we get :

$$F = C F_1\,F_2 \ldots F_h \ .$$

The F_j are absolutely irreducible, because they are proportional to the G_j.

Some of the factors may be repeated. In this case we shall write

$$F = CF_1^{q_1} \cdot F_2^{q_2} \dots F_h^{q_h} .$$

Later on we shall see that F can have repeated factors only if F is the q th power of a form F_0 without repeated factors, q being a power of the characteristic p. So the decomposition of F into absolutely irreducible factors must have the form,

$$F = CF_1^q F_2^q \dots F_h^q .$$

Theorem 4. *Let L be any extension of K. Let $V = V_1 + V_2 + \dots + V_h$ be the decomposition of V in L. Let $F_1, \dots, F_h$ be the associated forms of $V_1, \dots, V_h$. Then the decomposition of F in $L[u]$ is*

$$F = CF_1^{a_1} \cdot F_2^{a_2} \dots F_h^{a_h} .$$

Proof: We have, $V = V_1 + V_2 + \cdots + V_h$, where $V_1, V_2, \dots, V_h$ are irreducible over L and they are of the same dimension. The points of intersection $X^{(\nu)} (\nu = 1,2, \dots, g)$ are split up into generic points of V_1, generic points of V_2 and so on.

So if F_1 and F_2 are the associated forms of V_1 and V_2 the linear factors of F are partly contained in F_1 and partly in F_2 and so on.

Hence F can only be

$$F = CF_1^{a_1} \cdot F_2^{a_2} \dots F_h^{a_h} .$$

Corollary 1. *If V is absolutely irreducible then F is a power of a prime form.*

Proof: Suppose F can be expressed in some extension L of K as a product of different factors, say, $F = F_1 \cdot F_2$ having no prime factor in common. If F_1 is factorised into linear factors as in (1), it must contain with every factor all conjugate linear factors as well. Now all points of intersection of V with the hyperplanes $u^{(1)}, \dots, u^{(d)}$ are conjugate, because V is irreducible over L. Hence F_1 contains all prime factors of (1), each once at least. The same holds for F_2. Hence F_1 and F_2 have factors in common, against hypothesis. Thus, F can only be a power of a prime form in L.

In the special case when F has no multiple factors, $F = F_1 \cdot F_2 \dots F_h$. By Theorem 4, each of the prime factors $F_1, \dots, F_h$ defines a separate variety. These sub-varieties cannot be further subdivided, since the associated forms are irreducible.

Conversely, to every irreducible part of V corresponds a prime factor of F. For, if to an irreducible part of V corresponds a factor of F which is again factorisable into separate factors we arrive at a contradiction.

To each factor of F corresponds exactly one irreducible part of V. Hence the number of factors is the same. Therefore, we have:

Corollary 2. *If F has no repeated factors, the decomposition of F is $F = F_1 \cdot F_2 \ldots F_h$. In this case to every prime factor of F corresponds an irreducible part of V and conversely. The number of factors is equal to the number of irreducible parts.*

Corollary 3. *If V is absolutely irreducible and F has no repeated factors, F is absolutely irreducible.*

Corollary 4. *If F is absolutely irreducible or a power of an absolutely irreducible factor, then V is absolutely irreducible.*

Proof: Suppose V is reducible over some extension L of K, say into V_1 and V_2.

Let F_1, F_2 be the corresponding associated forms; then by Theorem 4,

$$F = F_1^{a_1} \cdot F_2^{a_2} \qquad \text{contrary to hypothesis.}$$

Theorem 5. *If $L = \Omega$ is chosen so that F factors into absolutely irreducible factors $F = F_1^{a_1} \ldots F_h^{a_h}$, then V decomposes into absolutely irreducible varieties in Ω.*

Proof: To each absolutely irreducible factor F_j or to a power of an absolutely irreducible factor F_j^q corresponds a part V_j of V according to Theorem 4.

Now, by corollary 4 these V_j are indivisible (i. e., absolutely irreducible) parts of V.

This concludes the proof of theorem 5.

4. The case of a purely inseparable extension field

Now we shall consider the case of a purely inseparable extension of a field K. A purely inseparable extension of K of characteristic p is defined as an extension L in which every element is a p^eth root of an element of K.

Theorem 6. *The variety V remains irreducible in a purely inseparable extension of K.*

Proof: Let p be the characteristic of K and let the algebraic extension

L be purely inseparable. Then L consists only of p^eth roots (which are unique) of elements of K.

If V were reducible over L, there would be a product of forms G and H with coefficients in L, such that GH contains V but neither G nor H contains V. Now $q = p^e$ can be so chosen as a power of p such that the qth powers of all coefficients of G and H are in L. By the well known rule, $(a + b + \ldots)^q = a^q + b^q + \ldots$ it follows that G^q and H^q are forms with coefficients in K. Now the form

$$(GH)^q = G^q H^q$$

contains V, but neither G^q nor H^q contains V. This is impossible since V is irreducible over K.

Now let $q = p^e$ have the same meaning as in formula (2), § 1. We shall prove

Theorem 7. *In a suitable, purely inseparable extension K_0 of K the form F becomes equal to F_0^q, where F_0 has no multiple factors any more.*

Proof: The formula (2) in § 2 implies that Q contains the indeterminates $u_0, \ldots, u_n$ only in the qth power.

The same holds good for F on account of (3) § 1. Now on account of the possibility of interchanging it follows, that F also contains the $u_k^{(\nu)}$ only in the qth power.

Therefore, F is a qth power of a form in u_k and $u_k^{(\nu)}$ with coefficients from a field K_0, which arises out of K by the adjunction of the qth roots of all coefficients of F. Thus we have

$$F = F_0^q \, . \tag{4}$$

Formula (3) now becomes

$$P^q = \frac{A}{B} F_0^q \, . \tag{5}$$

By (1), § 1, the product P has no multiple factors. Hence the left side of (5) and therefore, also the right side contains every factor exactly q times; it follows that F_0 contains every linear factor of P only once, i. e., F_0 does not contain multiple factors. This concludes the proof of Theorem 7.

Theorem 8. *If $q = 1$, the variety V is separably generated, i. e., all X are separable algebraic functions of d independent elements.*

In the proof 2 cases will be distinguished.

Case 1. We suppose K to be an infinite field. In the case of a field of characteristic p an irreducible polynomial $f(t)$ of one variable t is inseparable if and only if it may be written as a polynomial in t^p.

Suppose $e = 0$, i. e., $q = p^e = 1$. By (1) § 1 and (5), F_0 is a product of different linear factors :

$$u_0 x_0^{(\nu)} + u_1 x_1^{(\nu)} + \cdots + u_n x_n^{(\nu)} .$$

Now if we normalise $x_0 = 1$, we obtain

$$u_0 + u_1 x_1^{(\nu)} + u_2 x_2^{(\nu)} + \cdots + u_n x_n^{(\nu)} \quad \text{as factors.}$$

Now consider F_0 as a polynomial in one variable u_0. This polynomial is a product of linear factors

$$(u_0 - \vartheta)\,(u_0 - \vartheta')\ldots$$

all different. Consequently $\vartheta = -\,(u_1 x_1^{(\nu)} + u_2 x_2^{(\nu)} + \cdots + u_n x_n^{(\nu)})$ is separable with respect to the field, $K(u_1, \ldots, u_n;\ u^{(1)}, \ldots, u^{(d)})$.

Let V be defined over a field K. We shall enlarge the field K by the adjunction of n^2 indeterminates t_{ik}, where i and k take all values from 1 to n. Let the enlarged field $K(t_{ik})$ be denoted by K'. By Theorem 1, V is still irreducible with respect to K'. We shall first prove our theorem with respect to K'.

We have proved that

$$-\,\vartheta = u_1 x_1^{(\nu)} + u_2 x_2^{(\nu)} + \cdots + u_n x_n^{(\nu)}$$

is separable with respect to the field $K(u_1, \ldots, u_n;\ u^{(1)}, \ldots, u^{(d)})$. In this enunciation, the indeterminates u_k and $u_k^{(i)}$ may be replaced by any other set of indeterminates. Now replace,

u_k by $t_{ek}(k = 1, \ldots, n;\quad e = d + 1)$,
$u_k^{(i)}$ by $t_{ik}(k = 1, \ldots, n)$,
$u_0^{(i)}$ by new indeterminates $z_i(i = 1, \ldots, d)$.

It follows that,

$$-\,\vartheta_e = t_{e1} x_1 + t_{e2} x_2 + \cdots + t_{en} x_n \qquad (6)$$

is separable with respect to the field $K'(z_1, \ldots, z_d)$, where X is any one of the points of intersection of V with the hyperplanes

$$z_i + t_{i1} x_1 + t_{i2} x_2 + \cdots + t_{in} x_n = 0 . \qquad (7)$$

Now the problem may be simplified by a linear transformation of the coordinates $x_1, \ldots, x_n$:

$$y_i = \Sigma t_{ik} x_k ; \quad (i = 1, \ldots, n) . \tag{8}$$

Equations (6) and (7) now simplify to

$$z_i + y_i = 0 .$$

$$- \vartheta_e = y_e .$$

Hence $y_1, \ldots, y_d$ are equal to $- z_1, \ldots, - z_d$, and $y_{d+1} = y_e = - \vartheta_e$ is a separable function of the indeterminates $z_1, \ldots, z_d$.

The same holds, if $d + 1$ is replaced by any one of the numbers $d + 2, d + 3, \ldots, n$. Hence $y_{d+1}, \ldots, y_n$ are separable functions of $z_1, \ldots, z_d$. Also $y_1, \ldots, y_d$ are separable functions of $z_1, \ldots, z_d$, for they are equal to $- z_1, \ldots, - z_d$. So all y_i are separable functions of $z_1, \ldots, z_d$. Solving (8) with respect to the x_k, it is seen that also $x_1, \ldots, x_n$ are separable functions of the indeterminates $z_1, \ldots, z_d$.

Thus the theorem 8 is true provided K' [equal to $K(t_{ik})$] is taken as a field of constants instead of K. Now we have to pass from K' to K.

Let e be anyone of the numbers, $d + 1, \ldots, n$. We have an algebraic equation defining y_e as an algebraic function of $y_1, \ldots, y_d$:

$$f_e(y_1, \ldots, y_d, y_e) = 0 . \tag{9}$$

The coefficients of this equation are rational functions of the t_{ik}, but they may be made integral rational. To express this, we shall write

$$f_e(t_{ik}, y_1, \ldots, y_d, y_e) = 0 . \tag{10}$$

Now we can show that X is a generic point of V over $K(t_{ik})$:

$y_1, \ldots, y_d$ are algebraically dependent on $x_1, \ldots, x_n$ by (8); and $y_1, \ldots, y_n$ are algebraically dependent on $y_1, \ldots, y_d$ by (10). By solving (8) we see that $x_1, \ldots, x_n$ are dependent on $y_1, \ldots, y_n$. Hence $x_1, \ldots, x_n$ are algebraically dependent on $y_1, \ldots, y_d$. Therefore $x_1, x_2, \ldots, x_n$ are equivalent to $y_1, \ldots, y_d$.

That is, the degree of transcendency of X over $K(t_{ik})$ is d. Hence X is a generic point of V over $K(t_{ik})$.

The equations (8) and (9) or (10) may be interpreted in another way. We have considered $z_1, \ldots, z_d$ as indeterminates and $x_1, \ldots, x_n$ as algebraic functions of $z_1, \ldots, z_d$. We may also start with a generic point X of V, define $y_1, \ldots, y_n$ by (8) and define $z_1, \ldots, z_d$ by $z_i = -y_i$. The equations (9) remain valid in this interpretation, because all algebraic equations, valid for one generic point of V, remain valid for any other generic point. This means: if $y_1, \ldots, y_d$ and y_e are substituted from equation (8) into (10), we get an identity in the t_{ik}:

$$f_e(t_{ik}, \Sigma t_{ik} x_k) = 0 \ . \tag{11}$$

Such an identity remains valid, if the t_{ik} are specialised to t'_{ik}, and the y_i accordingly to $y'_i = \Sigma t'_{ik} x_k$.

Thus we get,

$$f_e(t'_{ik}, y'_1, \ldots, y'_d, y'_e) = 0 \ . \tag{12}$$

Let A_e be the coefficient of the highest power of y_e in (10) and D_e the discriminant of (10), considered as an equation for y_e. A_e does not vanish, nor does D_e, because the equation is separable. A_e and D_e are polynomials in t_{ik} and $y_1, \ldots, y_d$, and upon substitution of (8) they become polynomials in t_{ik} and $x_1, \ldots, x_n$. Further, let D be the determinant of the $t_{ik} (i = 1, \ldots, n; \ k = 1, \ldots, n)$.

Now specialise t_{ik} into t'_{ik} so that $D \prod_{d+1}^{n} A_e D_e$ remains $\neq 0$, where t'_{ik} are elements of K. Equation (12) now shows that all y'_e and hence all $x_1, \ldots, x_n$ are separable algebraic functions of $y'_1, \ldots, y'_d$. This completes the proof of theorem 8 for case 1.

Case 2. Now, let K be a finite field and hence perfect. In this case the theorem follows from the following[1])

Lemma: $x_1, \ldots, x_d$ can be numbered in such a way that $x_{d+1}, \ldots, x_n$ are separable algebraic functions of $x_1, \ldots, x_d$.

Theorem 9. *If V is separably generated then $q = p^e = 1$ (i. e., $e = 0$, where e is the exponent).*

Proof: By Kronecker's substitution, $F(u)$ is replaced by $f(t)$, where $f(t) = t^n + a_1 t^{n-1} + a_2 t^{n-2} + \cdots + a_n$.

Suppose it contains only t^q. Then we can write,

$$f(t) = t^{mq} + a_1 t^{(m-1)q} + \cdots + a_n = g(t^q) \ ;$$
$$g(v) = v^m + a_1 v^{(m-1)} + \cdots + a_n \ .$$

Now $g(v)$ is separable, otherwise it could be written as a polynomial in t^p.

Hence there is a separable extension L in which $g(v)$ is a product of different linear factors:

$$g(v) = (v - v_1) \ (v - v_2) \ldots (v - v_m) \ .$$

In L let the variety be $V = V_1 + V_2 + \cdots + V_h$ where $V_1, V_2, \ldots, V_h$

---

[1]) For a proof see [8], p. 620, § 1

are irreducible. Then,

$$F(u) = F_1 \cdot F_2 \dots F_h \ .$$

By Kronecker's substitution this is replaced by

$$f(t) = f_1(t) \cdot f_2(t) \dots f_h(t) \ .$$

$$\text{i. e.,} \qquad f(t) = g(t^q) = \prod_\nu (t^q - v_\nu) \ .$$

In L every $f_k(t)$ is a product of some factors $(t^q - v_\nu)$. Hence in $L^{1/q}$ every $f_k(t)$ is a product of some factors $(t - w_\nu)^q$ where $v_\nu = w_\nu^q$. That is, in $L^{1/q}$, we have $f_k(t) = \{f'_k(t)\}^q$, where $f'_k(t)$ is a product of different linear factors.

Now suppose V_k were reducible in a larger field L^*,

$$V_k = V_{k1}^* + V_{k2}^* \ .$$

Then, $F_k = F_{k1}^* \cdot F_{k2}^*$, where F_{k1}^* and F_{k2}^* have no factors in common. That is

$f_k = f_{k1}^* \cdot f_{k2}^*$, where f_{k1}^* and f_{k2}^* have no factors in common. We have then f_{k1}^* is a product of some factors $(t^q - v_\nu)$, where v_ν is in L and f_{k1}^* is in L. Similarly, f_{k2}^* is also in L contrary to hypothesis.

Hence $V_1, V_2, \dots, V_h$ are absolutely irreducible over L.

Now we shall prove the

Lemma: If V is absolutely irreducible and separably generated over L, then L is algebraically closed in $L(X)$.

Proof[2]*:* Suppose there were an element α in $L(X)$, algebraic over L and not in L. α being separable over L, the conjugate elements $\alpha, \alpha', \dots\dots$ are all different. That is $\alpha \neq \alpha'$ and

$$L(\alpha) \cong L(\alpha') \ . \qquad \text{(i)}$$

Now extend the isomorphism of $L(\alpha)$ to $L(X)$, so as to obtain an isomorphism $L(X) \cong L(X')$ as follows:

Let $x_1, \dots, x_d$ be algebraically independent and let $x_{d+1}, \dots, x_n$ be algebraic functions of $x_1, \dots, x_d$. Define the isomorphism as follows:

$$x_1 \longrightarrow x_1$$

$$\dots\dots\dots$$

$$x_d \longrightarrow x_d$$

$$L(\alpha, x_1, \dots, x_d) \cong L(\alpha', x_1, \dots, x_d) \ .$$

---

[2]) I owe the proof of this Lemma to Prof. B. L. van der Waerden.

$L(X)$ is algebraic over $L(\alpha, x_1, \ldots, x_d)$, hence this isomorphism can be extended to

$$L(X) \cong L(X') \text{ — (Proof in [7], I, § 35).} \qquad \text{(ii)}$$

X is a point of V and of degree of transcendency d. V remains irreducible over $L(\alpha)$. Hence X is a generic point of V with respect to $L(\alpha)$.

Because of the isomorphism (ii), X' too is a generic point of V. As before, we conclude: X' is a generic point with respect to $L(\alpha)$.

That is, X and X' are generic points of V with respect to $L(\alpha)$. Hence there is an isomorphism:

$$L(\alpha)(X) \longrightarrow L(\alpha)(X'). \qquad \text{(iii)}$$

The elements of $L(\alpha)$ remain fixed

$$\alpha \longrightarrow \alpha$$

and

$$X \longrightarrow X'$$

α is in $L(X)$. Hence $\alpha = f(X)$. Applying (ii) we get $\alpha' = f(X')$.

Applying (iii) we have,

$$\alpha = f(X')$$

Hence $\alpha = \alpha'$ contrary to hypothesis.

Now we can complete the proof of theorem 9 that was interrupted by this Lemma.

It is given that V is separably generated over K, i. e., the coordinates of X are separable algebraic functions of d independent elements. They are also independent over the algebraic closure $\overline{K}$ of K, and hence independent over L. It follows that V_1, the absolutely irreducible part of V is also separably generated over L.

Now by the theorem ([2], Th. 5, p. 18):

— An extension $L(X)$ of a field L is regular over L, if and only if L is algebraically closed in $L(X)$ and $L(X)$ is separably generated over L, — we have that $L(X) = L(x_0, \ldots, x_n)$ is regular over L, i. e., $L(X)$ and $\overline{L}$ are linearly disjoint over L. That is, every set of linearly independent elements in $L(X)$ over L is still linearly independent over $\overline{L}$. Hence also $L(t_{ik}, X)$ and $\overline{L}(t_{ik})$ are linearly disjoint over $L(t_{ik})$, where t_{ik} are defined as in the proof of theorem 8.

Now it can be proved that F_1 corresponding to V_1 is a product of different linear factors and hence q is equal to 1.

For, if not suppose,

$F_1 = F_0^p$. Then also, $f_1 = f_0^p$ and we should have,

$$f_0(y_1, \ldots, y_d, y_{d+1})^p = 0 \,, \quad \text{i. e.,} \quad f_0(y_1, \ldots, y_d, y_{d+1}) = 0 \ .$$

Putting $g' = g/p$, where g' = degree of f_0 and g = degree of f_1, this would mean a linear dependence between,

$$1, y_1, \ldots, y_{d+1}, y_1 y_2, \ldots, y_1^g, y_1^{g-1} y_2, \ldots, y_{d+1}^{g'}$$

with respect to $\overline{L}(t_{ik})$. Hence there is also a linear dependence with coefficients from $L(t_{ik})$. This means y_{d+1} has degree $g' (< g)$ at most with respect to $L(t_{ik}, y_1, \ldots, y_d)$, contrary to hypothesis.

Lastly, we shall show that $p^e = 1$ with respect to L leads to the result $p^e = 1$ with respect to K also. We have,

$$F = F_1 \cdot F_2 \ldots F_h \quad \text{in } L \quad (F \text{ irreducible in } K)$$

F_1 cannot be written as $f(u^p, \ldots)$; hence F_1 is a product of different linear factors:

$$F_1 = \Pi(u_0 x_0 + \cdots + u_n x_n)$$
$$F_2 = \Pi(- \ - \ -)$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$F_h = \Pi(- \ - \ -)$$

Hence F is a product of different linear factors. Hence $p^e = 1$ with respect to K.

I am deeply indebted to Prof. Dr. B. L. van der Waerden for his kind guidance and helpful advice throughout the course of this work.

REFERENCES

[1] *Wei-Liang Chow* and *B.L.van der Waerden.* Zur algebraischen Geometrie. IX. Über zugeordnete Formen und algebraische Systeme von algebraischen Mannigfaltigkeiten, Math. Ann., 113 (1937), pp. 692—704.

[2] *A.Weil,* Foundations of algebraic geometry, New York, 1946.

[3] *Wei-Liang Chow.* Algebraic systems of positive cycles in an algebraic variety. Amer. J. of Math., LXXII, No. 2 (1950), pp. 247—282.

[4] *B.L.van der Waerden.* Zur algebraischen Geometrie. XVI. Vielfältigkeiten von abstrakten Ketten, Math. Ann., 125 (1953), pp. 314—324.

[5] *B.L.van der Waerden.* Einführung in die Algebraische Geometrie, Berlin,1939.

[6] *W.V.D.Hodge* and *D.Pedoe.* Methods of algebraic geometry, Vol. II. Cambridge, 1952.

[7] *B.L.van der Waerden,* Modern Algebra, Vol.I (English translation), New York, 1949.

[8] *B.L.van der Waerden,* Zur algebraischen Geometrie. XIV, Math. Ann. 115 (1938), pp. 619—644.

(Received november 3, 1954)