V. Absolutely Irreducible Equations $f(x_1,\dots,x_n) = 0$.

References: Ostrowski (1919), Noether (1922), Lang & Weil (1954), Nisnevich (1954).

§1. Elimination theory.

Our goal is to derive an estimate for the number of zeros of an absolutely irreducible polynomial in n variables. This will be achieved in §5 . But in order to reach this goal we need "Bertini's Theorem", and for that in turn we need elimination theory. For more information on elimination theory see Van der Waerden (1955) , Chapter 11 . Elimination theory is now considered old fashioned, since most of its applications can be derived in a more elegant way from algebraic geometry. On the other hand, in these lectures we do not presume any knowledge of algebraic geometry. Moreover, elimination theory is constructive and easily permits one to estimate the degrees and the size of the coefficients of the constructed polynomials.

The reader will recall that given two polynomials over a field K ,

$$f(X) = c_0X^a + c_1X^{a-1} + \dots + c_a ,$$

$$g(X) = d_0X^b + d_1X^{b-1} + \dots + d_b ,$$

the resultant $R = R(c_0,c_1,\dots,c_a,d_0,d_1,\dots,d_b)$ of $f(X)$ and $g(X)$ is a certain polynomial in the coefficients of f and g . The polynomial R vanishes precisely if either f and g have a common root or if both leading coefficients are zero $(c_0 = d_0 = 0)$. If $c_0 \neq 0$ and $d_0 \neq 0$, then

$$R = c_0^b d_0^a \prod_{i=1}^{a} \prod_{j=1}^{b} (y_i - z_j) ,$$

where $y_1,\dots,y_a$ and $z_1,\dots,z_b$ are the roots of f and of g , respectively. R is homogeneous of degree b in $c_0,\dots,c_a$, and homogeneous of degree a in $d_0,\ldots,d_b$, and each term $c_0^{i_0} c_1^{i_1} \ldots c_a^{i_a} d_0^{j_0} d_1^{j_1} \ldots d_b^{j_b}$ has

$$(i_1 + 2i_2 + \ldots + ai_a) + (j_1 + 2j_2 + \ldots + bj_b) = ab \ .$$

Let

$$f^*(X_0,X_1) = c_0X_1^a + c_1X_0X_1^{a-1} + \ldots + c_aX_0^a$$

and

$$g^*(X_0,X_1) = d_0X_1^b + d_1X_0X_1^{b-1} + \ldots + d_bX_0^b$$

be the two forms associated with $f(X)$ and $g(X)$. We say that a pair (x_0,x_1) is a <u>common zero</u> of f^* and g^* if $(x_0,x_1) \neq (0,0)$ and $f^*(x_0,x_1) = g^*(x_0,x_1) = 0$, and if $x_0,x_1 \in \bar{K}$.

<u>Claim</u>: $f^*(X_0,X_1)$ <u>and</u> $g^*(X_0,X_1)$ <u>have a common zero if and only if</u> $R = 0$.

<u>Proof</u>: First suppose that f^* and g^* have the common zero (x_0,x_1) . If $x_0 \neq 0$ then they have a common zero of the form $(1,z)$. Here z is a common root of f and g , and therefore $R = 0$. If $x_0 = 0$, then $c_0x_1^a = 0$ and $d_0x_1^b = 0$. Since x_1 cannot also be zero, it follows that $c_0 = d_0 = 0$, and $R = 0$.

Now suppose $R = 0$. Either f and g have a common root z , in which case f^* and g^* have the common root $(1,z)$. Or $c_0 = d_0 = 0$, in which case $(1,0)$ is a common root of f^* and g^* . This verifies the claim. It follows that the vanishing of the resultant has a more elegant interpretation in terms of f^* and g^* than of f and g .

Let $f_1(X_0,X_1,\ldots,X_k)$, ... , $f_r(X_0,X_1,\ldots,X_k)$ be forms with coefficients in a field K . A *common zero* of $f_1,\ldots,f_r$ is an $(n+1)$-tuple $(x_0,x_1,\ldots,x_k) \neq \underline{0}$ with components in $\bar{K}$ such that $f_i(\underline{x}) = 0$ for $i = 1,2,\ldots,r$. Suppose each of these forms is of degree d , and that for $j = 1,2,\ldots,r$,

$$(1.1)\quad f_j(X_0,X_1,\ldots,X_k) = \sum_{i_0+i_1+\ldots+i_k=d} a^{(j)}_{i_0 i_1\ldots i_k} X_0^{i_0} X_1^{i_1} \ldots X_k^{i_k} .$$

We extend the concept of a resultant of two polynomials to a resultant system for r forms in $k+1$ variables by giving the following

Definition: A *resultant system* for the forms (1.1) is a finite set of forms $g_1,\ldots,g_s$ in variables

$$A^{(j)}_{i_0 i_1\ldots i_k} \qquad (1 \le j \le r \ ; \ i_0 + i_1 + \ldots + i_k = d) \ ,$$

with the property that $g_i\left(a^{(j)}_{i_0 i_1\ldots i_k}\right) = 0$ for each $i = 1,\ldots,s$ if and only if the forms $f_1,\ldots,f_r$ have a common zero.

Example 1: Take $k = 1$ and $r = 2$. The resultant system for the forms $f_1(X_0,X_1)$, $f_2(X_0,X_1)$ consists of just one form $(s = 1)$ - the resultant of the two polynomials $f_1(1,X_1)$ and $f_2(1,X_1)$.

Example 2: Take

$$\begin{aligned} f_1(X_1,\ldots,X_n) &= a_{11}X_1 + \ldots + a_{1n}X_n \ , \\ &\vdots \\ f_n(X_1,\ldots,X_n) &= a_{n1}X_1 + \ldots + a_{nn}X_n \ , \end{aligned}$$

i.e. a set of n linear forms in n variables. Again there is a resultant system for these forms consisting of a single form g, namely the determinant

$$g = \begin{vmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ \vdots & \vdots & & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{vmatrix} .$$

More generally, we can describe a resultant system for the forms

$$\begin{aligned} f_1(X_1,\dots,X_n) &= a_{11}X_1 + \dots + a_{1n}X_n \\ &\vdots \\ f_m(X_1,\dots,X_n) &= a_{m1}X_1 + \dots + a_{mn}X_n . \end{aligned}$$

If $m < n$, a resultant system for the forms $f_1,\dots,f_m$ is the identically zero form, since $f_1,\dots,f_m$ always have a common zero. If $m \geq n$, a resultant system is the set of all $(n \times n)$- subdeterminants of the associated $m \times n$ matrix.

THEOREM 1A: *Let* $f_1(X_0,X_1,\dots,X_k)$, ... , $f_r(X_0,X_1,\dots,X_k)$ *be forms of degree* d *as in* (1.1) . *There exists a resultant system* $g_1,\dots,g_s$, *where each* g_i *is a form in the variables* $A^{(j)}_{i_0i_1\dots i_k}$ *of degree*

$$2^k d^{2^k-1} .$$

LEMMA 1B: *Let* $\hat{g}(X_1,\dots,X_m)$ *be a form of degree* e , *and let* $h_1(Y_1,\dots,Y_\ell),\dots,h_m(Y_1,\dots,Y_\ell)$ *be forms of degree* e' . *Then the polynomial*

$$g(Y_1,\ldots,Y_\ell) = \hat{g}(h_1(Y_1,\ldots,Y_\ell),\ldots,h_m(Y_1,\ldots,Y_\ell))$$

is a form of degree ee'.

Proof: Obvious.

We begin the

Proof of Theorem 1A: Let the forms $f_1(X_0,\ldots,X_k),\ldots,f_r(X_0,\ldots,X_k)$ be given by (1.1) . The proof is by induction on k . If $k = 0$, then (1.1) becomes

$$f_j(X_0) = a_d^{(j)} X_0^d \quad , \qquad 1 \le j \le r . \tag{1.2}$$

Clearly the forms

$$g_j(A_d^{(1)},\ldots,A_d^{(r)}) = A_d^{(j)} \quad , \qquad 1 \le j \le r ,$$

form a resultant system for (1.2) . Moreover, $\deg g_j(A_d^{(1)},\ldots,A_d^{(r)}) = 1$ for $1 \le j \le r$, which agrees with Theorem 1A .

Suppose that the theorem holds for forms in k variables $X_0,X_1,\ldots,X_{k-1}$. We introduce new variables $U_1,\ldots,U_r$, $V_1,\ldots,V_r$, and form two polynomials

$$\bar{f} = U_1 f_1(X_0,\ldots,X_k) + \ldots + U_r f_r(X_0,\ldots,X_k) ,$$

$$\bar{g} = V_1 f_1(X_0,\ldots,X_k) + \ldots + V_r f_r(X_0,\ldots,X_k) ,$$

where

$$f_j(X_0,\ldots,X_k) = \sum_{i_0+\ldots+i_k=d} A^{(j)}_{i_0\ldots i_k} X_0^{i_0}\ldots X_k^{i_k} .$$

If we view $\bar{f}$ and $\bar{g}$ as polynomials in the variable X_k, they have a resultant

$$R = R(X_0,\dots,X_{k-1},U_1,\dots,U_r,V_1,\dots,V_r,\text{all } A's^{\dagger)}) .$$

If we write

$$\bar{f} = \bar{a}_0 X_k^d + \dots + \bar{a}_d$$

and

$$\bar{g} = \bar{b}_0 X_k^d + \dots + \bar{b}_d ,$$

then each $\bar{a}_i$ and each $\bar{b}_i$ is a form of degree i in $X_0,\dots,X_{k-1}$, is linear in the variables $U_1,\dots,U_r,V_1,\dots,V_r$, and linear in the $A's$.

In the resultant, a term $\bar{a}_0^{j_0}\dots\bar{a}_d^{j_d}\bar{b}^{\ell_0}\dots\bar{b}_d^{\ell_d}$ has

$$j_1 + 2j_2 + \dots + dj_d + \ell_1 + 2\ell_2 + \dots + d\ell_d = d^2 .$$

The resultant is of degree d in $\bar{a}_0,\dots,\bar{a}_d$, and also of degree d in $\bar{b}_0,\dots,\bar{b}_d$. Therefore

(i) R is a form of degree d^2 in $X_0,\dots,X_{k-1}$;

(ii) R is a form of degree $2d$ in the $A's$;

(iii) R is a form of degree $2d$ in $U_1,\dots,U_r$, $V_1,\dots,V_r$ together.

Collecting terms involving like powers in the $U's$ and $V's$, we may certainly write

$$R = \sum_{u_1,\dots,u_r} \sum_{v_1,\dots,v_r} R_{u_1,\dots,u_r,v_1,\dots,v_r}(X_0,\dots,X_{k-1},A's)U_1^{u_1}\dots U_r^{u_r} V_1^{v_1}\dots V_r^{v_r}$$

$\dagger)$ That is, all variables A.

Abbreviating the above coefficients by $R_{\underline{\underline{u}},\underline{\underline{v}}}$, we observe that

(i) $R_{\underline{\underline{u}},\underline{\underline{v}}}$ is a form of degree d^2 in $X_0,\dots,X_{k-1}$;

(ii) $R_{\underline{\underline{u}},\underline{\underline{v}}}$ is a form of degree $2d$ in the $A's$.

LEMMA 1C: *Suppose the variables* $A^{(j)}_{i_0,\dots i_k}$ *are replaced by coefficients* $a^{(j)}_{i_0\dots i_k}$ *in the field* K . *Then* $f_1,\dots,f_r$ *have a common zero if and only if all of the polynomials* $R_{\underline{\underline{u}},\underline{\underline{v}}}(X_0,\dots,X_{k-1},a's)$ *have a common zero.*

Proof: Suppose $f_1,\dots,f_r$ have a common zero $(x_0,x_1,\dots,x_k)$. If $(x_0,x_1,\dots,x_{k-1}) \neq (0,0,\dots,0)$ and the values $x_0,x_1,\dots,x_{k-1}$ are substituted in $\bar{f}$ and $\bar{g}$, then x_k is a common zero of $\bar{f}$ and $\bar{g}$, whence $R = 0$. But since

$$0 = R = \sum_{\underline{\underline{u}}}\sum_{\underline{\underline{v}}} R_{\underline{\underline{u}},\underline{\underline{v}}}(x_0,\dots,x_{k-1},a's)U_1^{u_1}\dots U_r^{u_r}V_1^{v_1}\dots V_r^{v_r} ,$$

the polynomials $R_{\underline{\underline{u}},\underline{\underline{v}}}(X_0,\dots,X_{k-1},a's)$ must have $(x_0,\dots,x_{k-1})$ as a common zero. If, on the other hand, $(x_0,\dots,x_{k-1}) = (0,\dots,0)$, then $f_1,\dots,f_r$ have the common zero $(0,\dots,0,1)$. It follows that the coefficient of X_k^d is zero for each f_i , hence also for $\bar{f}$ and $\bar{g}$. Again $R = R(X_0,\dots,X_{k-1},U's,V's,a's) = 0$, so all of the forms $R_{\underline{\underline{u}},\underline{\underline{v}}}(X_0,\dots,X_{k-1},a's)$ are identically zero, and therefore have a non-trivial common zero.

Conversely, suppose that $(x_0,x_1,\dots,x_{k-1})$ is a common zero of the forms $R_{\underline{\underline{u}},\underline{\underline{v}}}(X_0,\ldots,X_{k-1},a's)$. In particular, $x_0,\ldots,x_{k-1}$ lie in $\bar{K}$. Then

$$R(x_0,x_1,\ldots,x_{k-1},U's,V's,a's) = 0 ,$$

so that either $\bar{a}_0 = \bar{b}_0 = 0$ or $\bar{f}$ and $\bar{g}$ have a common zero x_k. If $\bar{a}_0 = \bar{b}_0 = 0$, then $f_1,\ldots,f_r$ clearly have the common zero $(0,0,\ldots,0,1)$. If $\bar{f}$ and $\bar{g}$ have the common root x_k, then x_k as a root of $\bar{f}$ is algebraic over $K(U_1,\ldots,U_r)$, and as a root of $\bar{g}$ is algebraic over $K(V_1,\ldots,V_r)$. It follows that x_k is algebraic over K. But since

$$\bar{f} = U_1f_1(x_0,\ldots,x_k) + \ldots + U_rf_r(x_0,\ldots,x_k) = 0 ,$$

and since each $f_j(x_0,\ldots,x_k)\in\bar{K}$, we conclude that

$$f_j(x_0,\ldots,x_k) = 0 \qquad (1 \le j \le r) .$$

We now return to the proof of Theorem 1A. By the inductive hypothesis, there is a resultant system $\hat{g}_1,\ldots,\hat{g}_s$ for the forms $R_{\underline{\underline{u}},\underline{\underline{v}}}(X_0,\ldots,X_{k-1})$, with

$$\deg \hat{g}_i = 2^{k-1}(d^2)^{2^{k-1}-1} = 2^{k-1}d^{2^k-2} \qquad (1 \le i \le s) .$$

Each coefficient of $R_{\underline{\underline{u}},\underline{\underline{v}}}$ was a form of degree $2d$ in the A's. Let $g_1,\ldots,g_s$ be obtained from $\hat{g}_1,\ldots,\hat{g}_s$ by substituting for each coefficient of $R_{\underline{\underline{u}},\underline{\underline{v}}}$ its expression in terms of the A's. By Lemma 1C, it is obvious that $g_1,\ldots,g_s$ form a resultant system for $f_1,\ldots,f_r$. Finally, by Lemma 1B, each g_i is a form in the A's of degree

$$2d \,.\, 2^{k-1}d^{2^k-2} = 2^k d^{2^k-1} \;.$$

This concludes the proof of Theorem 1A . We remark that the forms $g_1,\ldots,g_s$ have rational integer coefficients and are independent of the field K if char $K = 0$. In a field of characteristic p , the coefficients of the forms $g_1,\ldots,g_s$ are replaced by the residue classes modulo p of the corresponding coefficients in characteristic zero.

If a is a polynomial with rational integer coefficients in any number of variables, we define $\|a\|$ as the sum of the absolute values of the coefficients. For

Example: If $a(X,Y) = (X-Y)^n$, then $\|a\| = 2^n$.

Theorem 1 D: *In a field of characteristic zero, the forms $g_1,\ldots,g_s$ of Theorem 1A have rational integer coefficients and satisfy*

$$\|g_i\| \leq 2^{2^{4k}} . d^{2^k} \qquad (1 \leq i \leq s) \;.$$

For the remainder of this section, all polynomials are assumed to have rational integer coefficients. We first prove an analog to Lemma 1B .

LEMMA 1E: *Let $\hat{g}(X_1,\ldots,X_m)$ be a polynomial of total degree e . Let $b_1(Y_1,\ldots,Y_t),\ldots,b_m(Y_1,\ldots,Y_t)$ be polynomials with $\|b_i\| \leq \psi$ $(1 \leq i \leq m)$. Then*

$$g(Y_1,\ldots,Y_t) = \hat{g}(b_1(Y_1,\ldots,Y_t),\ldots,b_m(Y_1,\ldots,Y_t))$$

has the property that

$$\|g\| \leq \|\hat{g}\| \, \psi^{e} \ .$$

Proof: For any two polynomials a and b in any number of variables, observe that

$$\|ab\| \leq \|a\| \, . \, \|b\| \ .$$

For if a', b' and $(ab)'$ are obtained from a , b and ab , respectively, by replacing each coefficient by its absolute value, then

$$\|ab\| = \|(ab)'\| \leq \|a'b'\| = \|a'\| \, \|b'\| = \|a\| \, \|b\| \ .$$

Now a typical term in the polynomial g is $b_1^{i_1} \ldots b_m^{i_m}$ where

$$i_1 + i_2 + \ldots + i_m \leq e \ ,$$

so that

$$\|b_1^{i_1} \ldots b_m^{i_m}\| \leq \psi^{e} \ .$$

The lemma follows.

In order to prove Theorem 1D , we examine more closely the polynomials introduced in the proof of Theorem 1A .

LEMMA 1F:

$$\|R_{\underline{\underline{u}},\underline{\underline{v}}}(X_0, \ldots, X_{k-1}, A\text{'s})\| \leq (2d)^{6dk} \ .$$

Proof: We saw that $R(X_0, \ldots, X_{k-1}, U_1, \ldots, U_r, V_1, \ldots, V_r, A\text{'s})$ had total degree $2d$ in $U_1, \ldots, U_r, V_1, \ldots, V_r$. Therefore in each monomial $U_1^{u_1} \ldots U_r^{u_r} V_1^{v_1} \ldots V_r^{v_r}$,

$$u_1 + \ldots + u_r + v_1 + \ldots + v_r \le 2d \ .$$

Hence for any $R_{\underline{\underline{u}},\underline{\underline{v}}}$ which is not identically zero, at most $2d$ of the numbers $u_1,\ldots,u_r,v_1,\ldots,v_r$ can be non-zero. Let $c = \min\{2d,r\}$. Suppose, without loss of generality, that $u_i = v_i = 0$ if $i > c$. Let $R^*(X_0,\ldots,X_{k-1},U_1,\ldots,U_c,V_1,\ldots,V_c,A' s)$ be obtained from R by omitting all terms where some U_i or V_i with $i > c$ occurs. Then

$$\|R_{\underline{\underline{u}},\underline{\underline{v}}}(X_0,\ldots,X_{k-1},A' s)\| \le \|R^*\| \ .$$

R^* is clearly the resultant of the two polynomials

$$\bar{f}^* = U_1 f_1(X_0,\ldots,X_k) + \ldots + U_c f_c(X_0,\ldots,X_k)$$

$$= \bar{a}_0^* X_k^d + \ldots + \bar{a}_d^* \ ,$$

$$\bar{g}^* = V_1 f_1(X_0,\ldots,X_k) + \ldots + V_c f_c(X_0,\ldots,X_k)$$

$$= \bar{b}_0^* X_k^d + \ldots + \bar{b}_d^* \ ,$$

when considered as polynomials in X_k . If we write, for $1 \le j \le r$,

$$f_j(X_0,\ldots,X_k) = \sum_{i_0+\ldots+i_k=d} A^{(j)}_{i_0\ldots i_k} X_0^{i_0}\ldots X_k^{i_k} \ ,$$

the number of summands in f_j is not more than $(d+1)^k$. So the number of summands in $\bar{f}^*$ or $\bar{g}^*$ is bounded by

$$(d+1)^k c \le 2d(d+1)^k \le (2d)^{k+1} \ .$$

Therefore the number of summands in each $\bar{a}_i^*$ or $\bar{b}_i^*$ is also bounded by $(2d)^{k+1}$. But each coefficient in $\bar{a}_i^*$ or $\bar{b}_i^*$ is either 0 or 1, so that

$$\|\bar{a}_i^*\| \le (2d)^{k+1} \quad , \quad \|\bar{b}_i^*\| \le (2d)^{k+1} \qquad (i = 0,\dots,d) .$$

The resultant of $\bar{f}^*$ and $\bar{g}^*$ is of degree $2d$ in $\bar{a}_0^*,\dots,\bar{a}_d^*,\bar{b}_0^*,\dots,\bar{b}_d^*$. This resultant is a $(2d \times 2d)$ - determinant, so the resultant r satisfies $\|r\| \le (2d)!$. By Lemma 1E, $R^* = r(a_0^*,\dots,a_d^*, b_0^*,\dots,b_d^*)$ has

$$\|R^*\| \le (2d)! \ ((2d)^{k+1})^{2d} .$$

Hence

$$\begin{aligned}\|R_{\underline{\underline{u}},\underline{\underline{v}}}(X_0,\dots,X_{k-1},A-s)\| &\le \|R^*\| \\ &\le (2d)^{2d}(2d)^{2dk+2d} \\ &= (2d)^{2dk+4d} \\ &\le (2d)^{6dk} .\end{aligned}$$

<u>Proof of Theorem 1D</u>: We proceed by induction on k. If $k = 0$, then $\|g_i\| = 1$ and the theorem holds trivially. Suppose it has been established that for $k-1$ one obtains the estimate

$$\|g_i\| \le c_{k-1} = c_{k-1}(d) = 2^{2^{4(k-1)}} . d^{2^{k-1}} .$$

Let $\hat{g}_1,\dots,\hat{g}_s$ be a resultant system for the $R_{\underline{\underline{u}},\underline{\underline{v}}}$'s. By induction, $\|\hat{g}_i\| \le c_{k-1}(d^2)$, since each $R_{\underline{\underline{u}},\underline{\underline{v}}}$ is of degree d^2 in $X_0,\dots,X_{k-1}$.

On the other hand, g_i is obtained from $\hat{g}_i$ by substituting for the coefficients of each $R_{\underline{\underline{u}},\underline{\underline{v}}}$ their expressions in terms of the A's . By applying Lemmas 1E , 1F and observing that $\hat{g}_i$ has degree

$$2^{k-1}(d^2)^{2^{k-1}-1} = 2^{k-1} d^{2^k-2} ,$$

we obtain

$$\|g_i\| \le c_{k-1}(d^2) \left|(2d)^{6kd}\right|^{2^{k-1} d^{2^k-2}} .$$

But by the inductive hypothesis,

$$c_{k-1}(d^2) = 2^{2^{4k-4} d^{2^k}} .$$

Hence

$$\begin{aligned}\|g_i\| &\le 2^{2^{4k-4} d^{2^k}} \,.\, 2^{2d \,.\, 6kd \,.\, 2^{k-1} \,.\, d^{2^k-2}} \\ &= 2^{2^{4k-4} d^{2^k}} \,.\, 2^{6k\, 2^k d^{2^k}} \\ &= 2^{(2^{4k-4} + 6k2^k) d^{2^k}} \\ &< 2^{2^{4k} d^{2^k}} .\end{aligned}$$

§2. The absolute irreducibility of polynomials (I) .

Given a polynomial $f(X_1,\dots,X_n)$ in n variables with coefficients in a field K , we wish to investigate the absolute irreducibility of f ; i.e., the irreducibility of f over $\bar{K}$. Suppose f has total degree at most $d > 0$ and is given by

$$(2.1)\qquad f(X_1,\dots,X_n) = \sum_{i_1+\dots+i_n \le d} a_{i_1\dots i_n} X_1^{i_1}\dots X_n^{i_n} .$$

THEOREM 2 A: (E. Noether (1922)) *There exist forms* $g_1,\dots,g_s$ *in variables* $A_{i_1\dots i_n}$ $(i_1 + \dots + i_n \le d)$ *such that the above polynomial* $f(X_1,\dots,X_n)$ *is reducible over* $\bar{K}$ *or of degree* $< d$ *if and only if*

$$g_j\{a_{i_1\dots i_n}\} = 0 \qquad (1 \le j \le s) .$$

Moreover, if $k = \binom{n+d-1}{n}$, *then*

(i) $\deg g_j \le k^{2^k}$ $(1 \le j \le s)$.

These forms depend only on n *and* d , *and are independent of the field* K *in the sense that if* $\operatorname{char} K = 0$, *they are fixed forms with rational integer coefficients; while if* $\operatorname{char} K = p\,(\ne 0)$, *they are obtained by reducing the integral coefficients modulo* p . *In the case when* $\operatorname{char} K = 0$,

(ii) $\|g_j\| \le 4^{k^{2^k}}$ $(1 \le j \le s)$.

Proof: We first dispose of the trivial cases. If $d = 1$, the forms may be taken to be just the variables corresponding to the coefficients of f . If $d \geq 2$ and $n = 1$, then f is always reducible over $\bar{K}$, so we may take $s = 1$ and g_1 identically zero. We may therefore assume that both $d \geq 2$ and $n \geq 2$, from which it follows that $k \geq 2$.

Observe that f is reducible or $\deg f < d$ if and only if $f = gh$ with $\deg g < d$, $\deg h < d$. Now suppose $f = gh$ where

$$g(X_1, \dots, X_n) = \sum_{j_1+\dots+j_n \leq d-1} b_{j_1 \dots j_n} X_1^{j_1} \dots X_n^{j_n} ,$$

$$h(X_1 \dots, X_n) = \sum_{k_1+\dots+k_n \leq d-1} c_{k_1 \dots k_n} X_1^{k_1} \dots X_n^{k_n} .$$

Then the coefficients of f must have the form

$$a_{i_1 \dots i_n} = \sum_{j_1+k_1=i_1} \dots \sum_{j_n+k_n=i_n} b_{j_1 \dots j_n} c_{k_1 \dots k_n}$$

for any $i_1, \dots, i_n$ with $i_1+\dots+i_n \leq 2d-2$ [†]. Let g be fixed, not identically zero, and consider the system of linear equations

$$(2.2) \quad c \cdot a_{i_1 \dots i_n} = \sum_{j_1+k_1=i_1} \dots \sum_{j_n+k_n=i_n} b_{j_1 \dots j_n} c_{k_1 \dots k_n} \qquad (i_1+\dots+i_n \leq 2d-2)$$

in c and the elements $c_{k_1 \dots k_n}$. If g divides f , then (2.2) has a solution with $c = 1$, hence has a non-trivial solution. Conversely, if (2.2) has a non-trivial solution, then if $c = 0$, we would obtain the contradictory result that $gh = 0$ while both $g \neq 0$ and $h \neq 0$. So in fact $c \neq 0$, and there is a solution of (2.2) with $c = 1$,

[†] We set $a_{i_1 \dots i_n} = 0$ for $i_1 + \dots + i_n > d$.

and hence g divides f.

We have shown that g divides f if and only if (2.2) has a non-trivial solution in the variables $c, \{c_{k_1 \dots k_n}\}$. The number of variables is $k + 1$ with $k = \binom{n+d-1}{n}$. Therefore the condition that g divide f is that all the $(k + 1) \times (k + 1)$ determinants, say $\Delta_1, \dots, \Delta_r$, of the system of linear equations (2.2) vanish. But each Δ_i is a form in the coefficients $b_{j_1 \dots j_n}$ of degree k, and the number of these coefficients is also k. We know from elimination theory, specifically Theorem 1A, that there exist forms $h_1, \dots h_s$ in the coefficients of $\Delta_1, \dots, \Delta_r$, such that the equations $\Delta_1 = \dots = \Delta_r = 0$ have a non-trivial solution (in the $b_{j_1 \dots j_n}$'s) if and only if $h_1 = \dots = h_s = 0$. Also by Theorem 1A,

$$(2.3) \qquad \deg h_i = 2^{k-1} k^{2^{k-1}-1} \le k^{2^k} \qquad (1 \le i \le s).$$

If $\operatorname{char} K = 0$, it follows from Theorem 1D that

$$(2.4) \qquad \|h_i\| \le 2^{2^{4k-4} k^{2^{k-1}}} \le 2^{k^{2^k}} \qquad (1 \le i \le s).$$

Now let g_i be obtained from h_i by substituting for the coefficients of the forms $\Delta_1, \dots, \Delta_r$ their expressions in terms of the original coefficients $a_{i_1 \dots i_n}$ of f. Each such coefficient is linear in the $a_{i_1 \dots i_n}$ with norm at most $k!$ Combining (2.3), (2.4) with Lemmas 1B, 1E, we obtain

$$\deg g_i \leqq \deg h_i \leqq k^{2^k} \qquad (1 \leqq i \leqq s)$$

and

$$
\begin{aligned}
\|g_i\| &\le \|h_i\| (k!)^{2^{k-1}} k^{2^{k-1}-1} \\
&\le 2^{k^{2^k}} 2^{k^2 2^{k-1}} k^{2^{k-1}-1} \\
&\le 2^{k^{2^k}} 2^{k^{2^{k-1}+k}} \\
&\le 2^{k^{2^k}} 2^{k^{2^k}} \\
&= 4^{k^{2^k}} \quad .
\end{aligned}
$$

<u>COROLLARY 2B:</u> (Ostrowski (1919)) *Let* $f(X_1,\ldots,X_n)$ *be a polynomial of degree* $d > 0$ *with rational integral coefficients. Suppose* f *is absolutely irreducible* (i.e. *irreducible over* $\bar{\mathbb{Q}}$) . *Let* p *be a prime with*

$$p > (4\|f\|)^{k^{2^k}} \quad ,$$

where $k = \binom{n+d-1}{n}$. *Then the reduced polynomial modulo* p *is again of degree* d *and absolutely irreducible* (i.e. *irreducible over* $\bar{\mathbb{F}}_p$).

Proof: Let f be given by (2.1) , where the coefficients $\{a_{i_1\ldots i_n}\}$ are now integers. Since f is of degree d and absolutely irreducible, in the notation of Theorem 2A , not all the numbers $g_i(\{a_{i_1\ldots i_n}\})$ are zero. Let us say $g_1(\{a_{i_1\ldots i_n}\}) \neq 0$. We have the estimate

$$0 < |g_1(\{a_{i_1\ldots i_n}\})| \le \|g_1\| . \|f\|^{k^{2^k}} \le (4\|f\|)^{k^{2^k}} \quad .$$

So if $p > (4\|f\|)^{k^{2^k}}$, then the number $g_1(\{a_{i_1\ldots i_n}\})$ is still non-zero modulo p. It follows, again by Theorem 2A, that the reduced polynomial modulo p is of degree d and absolutely irreducible.

COROLLARY 2C: *Let* $f(X,Y)$ *be a polynomial with rational integer coefficients which is absolutely irreducible. If* $N(p)$ *denotes the number of solutions of the congruence*

$$f(x,y) \equiv 0 \pmod{p} ,$$

then for large primes p,

$$N(p) = p + O(p^{1/2}) .$$

Proof: Combine Corollary 2B with Theorem 1A of Chapter III.

§3. *The absolute irreducibility of polynomials* (II).

Let K and L be two fields with $K \subseteq L$. The *algebraic closure of* K *in* L, denoted by K^o, is defined as the set of elements of L which are algebraic over K. Clearly K^o is a field and $K \subseteq K^o \subseteq L$.

THEOREM 3 A: *Suppose* $f(X_1,\ldots,X_m,Y)$ *is a polynomial with coefficients in a field* K, *irreducible over* K, *and of degree* $d > 0$ *in* Y. *Further suppose that* f *is not a polynomial in only* $X_1^p,\ldots,X_m^p,Y^p$ *if* K *has characteristic* $p \neq 0$. *Let* $\mathfrak{Y}$ *be a quantity satisfying* $f(X_1,\ldots,X_m,\mathfrak{Y}) = 0$, *and let* $L = K(X_1,\ldots,X_m,\mathfrak{Y})$. *Let* K^o *be the algebraic closure of* K *in* L. *Then* $[K^o : K]$ *is a divisor of* d *and* K^o *is separable over* K. *Moreover, the polynomial* $f(X_1,\ldots,X_m,Y)$ *is absolutely irreducible if and only if* $K^o = K$.

Theorems of this type are well known to algebraic geometers. See, e.g., Zariski (194[illegible]) . See also Corollary 6C in Ch. VI.

Example: Consider the polynomial $f(X,Y) = 2X^2 - Y^4$ over the field $K = \mathbb{Q}$ of rational numbers. Clearly $f(X,Y)$ is irreducible over $\mathbb{Q}$. Choose $\mathfrak{Y}$ so that $\mathfrak{Y}^4 = 2X^2$ and let $L = \mathbb{Q}(X,\mathfrak{Y})$. If we put $\alpha = \mathfrak{Y}^2/X$, then $\alpha^2 = 2$, so $\sqrt{2} \in \mathbb{Q}^o$. This means that $\mathbb{Q}$ is not algebraically closed in L , or $\mathbb{Q}^o \neq \mathbb{Q}$. By Theorem 3 A , $f(X,Y)$ is not absolutely irreducible; in fact, we see directly that

$$f(X,Y) = (\sqrt{2}\, X - Y^2)(\sqrt{2}\, X + Y^2)$$

is a factorization of $f(X,Y)$ over $\mathbb{Q}(\sqrt{2})$.

Proof of Theorem 3 A. We begin with the following remark: If K^o is algebraic over K of degree d , then $K^o(X_1,\dots,X_m)$ is algebraic over $K(X_1,\dots,X_m)$ of degree d , and vice versa. If K^o is separable (or inseparable) over K , then $K^o(X_1,\dots,X_m)$ is separable (or inseparable) over $K(X_1,\dots,X_m)$, and conversely. This follows from the argument used in Lemma 2A of Chapter III .

Now observe that

$$(3.1)\quad K(X_1,\dots,X_m) \subseteq K^o(X_1,\dots,X_m) \subseteq K^o(X_1,\dots,X_m,\mathfrak{Y}) = K(X_1,\dots,X_m,\mathfrak{Y}) .$$

Since $K(X_1,\dots,X_m,\mathfrak{Y})$ is an extension of $K(X_1,\dots,X_m)$ of degree d , it follows that $[K^o(X_1,\dots,X_m) : K(X_1,\dots,X_m)]$ divides d , whence $[K^o : K]$ divides d by the above remark.

If f is absolutely irreducible, then f is irreducible over K^o . Hence $\mathfrak{Y}$ is algebraic of degree d over $K^o(X_1,\dots,X_m)$; that is ,

$$[K^o(X_1,\dots,X_m,\mathfrak{Y}) : K^o(X_1,\dots,X_m)] = d .$$

From (3.1) it follows that $K(X_1,\dots,X_m) = K^o(X_1,\dots,X_m)$, so that $K = K^o$.

For the remainder of the proof, we shall tacitly assume that char $K = p \neq 0$. Actually the case when char $K = 0$ is simpler, and several steps may be omitted.

Let $f_1(X_1,\dots,X_m,Y)$ be an irreducible factor of $f(X_1,\dots,X_m,Y)$ over $\bar{K}$ such that

$$(3.2) \qquad f_1(X_1,\dots,X_m,\mathfrak{Y}) = 0 .$$

We normalize f_1 by requiring that the leading coefficient (in some lexicographic ordering of the monomials) is 1. Then every power of f_1 also has this property. Let K_1 be the field obtained from K by adjoining the coefficients of f_1. Let a be the smallest positive integer such that every coefficient of f_1^a is separable over K. If b is a positive integer such that f_1^b has coefficients which are separable over K, then $a \mid b$: For if $b = at + r$ with $0 \leqq r < a$, then f_1^r has separable coefficients, and by the minimal choice of a, we have $r = 0$. Now $f_1^{p^\ell}$ has separable coefficients for some ℓ, hence $a \mid p^\ell$, and a itself must be a power of p. We have

$$K \subseteq K_1^s \subseteq K_1 ,$$

where K_1^s is the separable extension of K obtained from K by adjoining the coefficients of f_1^a.

The polynomial $g = f_1^a$ has coefficients in K_1^s and is irreducible over K_1^s, since its proper divisors (which would necessarily be powers of f_1) have coefficients which are not all separable over K, hence do not all lie in K_1^s . Now $g = f_1^a$ divides f^a , and since g is irreducible, g divides f . Write $\delta = [K_1^s : K]$ and let $g^{(1)}, g^{(2)}, \ldots, g^{(\delta)}$ be the distinct conjugates of g . Each $g^{(i)}$ divides f , so the product

$$g^{(1)} g^{(2)} \ldots g^{(\delta)} \mid f .$$

But this product has coefficients which are separable over K , and which are invariant under conjugation. Hence this product has coefficients in K . Since f is irreducible over K , there exists a constant $c \in K$ such that

$$f = c\, g^{(1)} g^{(2)} \ldots g^{(\delta)} .$$

If a were a positive power of p , then g would be a polynomial in $X_1^p, \ldots, X_m^p, Y^p$, hence each conjugate would be such a polynomial, and therefore f would be a polynomial in $X_1^p, \ldots, X_m^p, Y^p$. But this is impossible by hypothesis. Hence $a = 1$. It follows immediately that $K_1^s = K_1$, whence that K_1 is a separable extension of K .

Now $f = c\, f_1^{(1)} \ldots f_1^{(\delta)}$ has degree d in Y , so each factor $f_1^{(i)}$ has degree d/δ in Y . Hence by (3.2) , $\mathfrak{Y}$ has degree d/δ over $K_1(X_1, \ldots, X_m)$. Since $[K_1 : K] = \delta$, it follows that $[K_1(X_1, \ldots, X_m, \mathfrak{Y}) : K(X_1, \ldots, X_m)] = d$. Since $K \subseteq K_1$, and since also $[K(X_1, \ldots, X_m, \mathfrak{Y}) : K(X_1, \ldots, X_m)] = d$, we have

$$K_1(X_1, \ldots, X_m, \mathfrak{Y}) = K(X_1, \ldots, X_m, \mathfrak{Y}) = L .$$

Thus K_1 is contained in L and is algebraic over K , whence $K_1 \subseteq K^o$.

Now f_1 was irreducible over K_1, in fact absolutely irreducible. By the part of the theorem already proved, $(K_1)^o = K_1$. But $(K_1)^o = K^o$, so $K_1 = K^o$, and K^o is separable over K. Finally, if $K^o = K$, then $K_1 = K$ and f is absolutely irreducible. This completes the proof.

We are now able to finish the

Proof of Lemma 2B of Chapter III: In the notation of that lemma, we need to show that if

$$[K(X,Z,\mathfrak{Y},\mathfrak{U}):\ (K(X,Z)] = d^2 ,$$

then $f(X,Y)$ is absolutely irreducible. Suppose $f(X,Y)$ is not absolutely irreducible. By Theorem 3A, $K^o \neq K$. Let $[K^o(X):\ K(X)] = u > 1$ and let $[K(X,\mathfrak{Y}):\ K^o(X)] = v$, so that $uv = d$. In the chain $K(X,Z) \subseteqq K^o(X,Z) \subseteqq K^o(X,Z,\mathfrak{Y}) \subseteqq K^o(X,Z,\mathfrak{Y},\mathfrak{U}) = K(X,Z,\mathfrak{Y},\mathfrak{U})$, the field extensions are of respective degrees u,v,v, so that

$$[K(X,Z,\mathfrak{Y},\mathfrak{U}):\ K(X,Z)] = uv^2 < (uv)^2 = d^2 ,$$

which completes the proof.

In §2 of Chapter IV we introduced an equivalence relation for quadratic forms. We make a slight adjustment of that definition to define an equivalence for polynomials in n variables over a field K. We say that $f(\underline{\underline{X}}) \sim g(\underline{\underline{X}})$ if there is a non-singular $(n \times n)$ matrix T and a vector $\underline{\underline{t}}$, both having components in K, such that

$$f(\underline{\underline{X}}) = g(T\underline{\underline{X}} + \underline{\underline{t}}) .$$

This is clearly an equivalence relation.

LEMMA 3B: *Suppose* $f(\underline{\underline{X}}) \sim g(\underline{\underline{X}})$. *If* f *is irreducible over* K *(or absolutely irreducible), then so is* g . *Moreover, the total degrees of* $f(\underline{\underline{X}})$ *and* $g(\underline{\underline{X}})$ *are equal.*

Proof: Exercise. Notice that the first part of the lemma is a generalization of Lemma 2B of Chapter I .

Let $f(X_1,\dots,X_n)$ be a polynomial over K . For $1 \le \ell \le n$, we will write

$$f(\widehat{X_1,\dots,X_\ell}\, , X_{\ell+1},\dots,X_n)$$

when the polynomial is to be interpreted as a polynomial in the variables $X_{\ell+1},\dots,X_n$, with coefficients in the field $K(X_1,\dots,X_\ell)$.

LEMMA 9C: *If* $f(X_1,\dots,X_n)$ *is irreducible (over* K) , *then* $f(\widehat{X_1,\dots,X_\ell}\, , X_{\ell+1},\dots,X_n)$ *is irreducible (over* $K(X_1,\dots,X_\ell)$) .

Proof: This follows from the unique factorization in $K[X_1,\dots,X_\ell]$. The details are left as an exercise.

We remark that if $f(X_1,\dots,X_n)$ is absolutely irreducible (i.e. irreducible over $\overline{K}$) , it does not follow that $f(\widehat{X_1,\dots,X_\ell}\, , X_{\ell+1},\dots,X_n)$ is absolutely irreducible (i.e. irreducible over $\overline{K(X_1,\dots,X_\ell)}$). In fact, if $\ell = n - 1$, the new polynomial is a polynomial in one variable, which cannot be absolutely irreducible unless its degree is one. As another example, the polynomial

$$f(X_1,X_2,X_3) = X_2^2 - X_1X_3^2$$

is absolutely irreducible, while $f(\widehat{X_1},X_2,X_3)$ has the factorization

$$f(\widehat{X_1},X_2,X_3) = (X_2 - \sqrt{X_1}\,X_3)(X_2 + \sqrt{X_1}\,X_3)$$

over $\overline{K(X_1)}$.

THEOREM 3D: *Suppose* $f(X_1,\ldots,X_n)$ *is a polynomial over an infinite field* K . *Suppose* f *is absolutely irreducible and of degree* $d > 0$. *Let* $1 \le \ell \le n-2$. *Then there is a polynomial* $g \sim f$ *such that*

$$g(\widehat{X_1,\ldots,X_\ell}, X_{\ell+1},\ldots,X_n)$$

is absolutely irreducible and of degree d *(in* $X_{\ell+1},\ldots,X_n$) .

We shall need

LEMMA 3E: *Let* $J \subseteq L$ *be fields such that* L *is a finite separable algebraic extension of* J . *Then there are only finitely many fields* J' *with*

$$J \subseteq J' \subseteq L .$$

Proof: Let N be a finite separable algebraic normal extension of J with $L \subseteq N$. Let G be the Galois group of N over J , and let H be the Galois group of N over L . Then $H \subseteq G$. From Galois theory, we know that there is a one-one correspondence between fields J' with $J \subseteq J' \subseteq L$ and groups H' with $H \subseteq H' \subseteq G$. The number of such groups H' is finite, so the number of fields J' is finite.

Remark: Separability is essential in Lemma 3E. For let F be an algebraically closed (hence infinite) field of characteristic p . Take

$$J = F(X,Y) \subseteq L = J(X^{1/p}, Y^{1/p}) ,$$

and if $c \in F$, let

$$J'_c = J\left((X + cY)^{1/p} \right) = J(X^{1/p} + c^{1/p}Y^{1/p}) .$$

Clearly $J \subseteq J'_c \subseteq L$, but for different choices of $c \in F$ we get different fields J'_c , so that the collection of intermediate fields is infinite.

We begin the

<u>Proof of Theorem 3D</u>: We shall tacitly assume that $\text{char } K = p \neq 0$, the proof for the case $\text{char } K = 0$ being easier. First observe that $f(X_1,\ldots,X_n)$ is not a polynomial in $X_1^p,\ldots,X_n^p$, for if it were then

$$f(X_1,\ldots,X_n) = \sum_{i_1,\ldots,i_n} a_{i_1\ldots i_n} X_1^{pi_1} \ldots X_n^{pi_n}$$

$$= \left(\sum_{i_1,\ldots,i_n} a_{i_1\ldots i_n}^{1/p} X_1^{i_1} \ldots X_n^{i_n} \right)^p ,$$

contradicting the assumption that $f(X_1,\ldots,X_n)$ is absolutely irreducible. We change notation and write

$$f = f(X_1,\ldots,X_m,Y)$$

where $m = n - 1$. After a linear transformation of variables $(X'_i = X_i + c_iY \ ; \ i = 1,2,\ldots,m)$ we may suppose that f is of degree d in Y and separable in Y . Let $\mathfrak{Y}$ be a quantity satisfying

$$f(X_1,\ldots,X_m,\mathfrak{Y}) = 0 ,$$

and let $L = K(X_1,\ldots,X_m,\mathfrak{Y})$. For $c \in K$, put $X_1^{(c)} = X_1 + cX_m$. Construct the fields $K(X_1^{(c)})$ and $\left(K(X_1^{(c)})\right)^o$, the latter being the algebraic closure of $K(X_1^{(c)})$ in L .

LEMMA 3 F: For some $c \in K$,

$$\left(K(X_1^{(c)})\right)^o = K(X_1^{(c)}) .$$

Proof: For every $c \in K$ we have

$$K(X_1,\ldots,X_m) \subseteq \left(K(X_1^{(c)})\right)^o (X_2,\ldots,X_m) \subseteq L .$$

Note that L is a separable extension of $K(X_1,\ldots,X_m)$ of degree d . By Lemma 3E , there are only finitely many subfields of L containing $K(X_1,\ldots,X_m)$. Hence there exist two distinct elements $c,c' \in K$ such that

$$\left(K(X_1^{(c)})\right)^o (X_2,\ldots,X_m) = \left(K(X_1^{(c')})\right)^o (X_2,\ldots,X_m) ,$$

or

$$\left(K(X_1^{(c)})\right)^o (X_m)(X_2,\ldots,X_{m-1}) = \left(K(X_1^{(c')})\right)^o (X_m)(X_2,\ldots,X_{m-1}) .$$

But since $X_2,\ldots,X_{m-1}$ are algebraically independent over $K(X_1,X_m)$, it follows that

$$\left(K(X_1^{(c)})\right)^o (X_m) = \left(K(X_1^{(c')})\right)^o (X_m) .$$

For brevity we shall write $X = X_1^{(c)}$ and $Z = X_1^{(c')}$. By Theorem 3A ,

$K(X_1^{(c)})^o$ is a finite separable extension of $K(X_1^{(c)})$, and hence there exists an element $\mathfrak{X}$ such that

$$\left(K(X_1^{(c)})\right)^o = \left(K(X)\right)^o = K(X,\mathfrak{X}) .$$

Similarly, there is a $\mathfrak{Z}$ with

$$\left(K(X_1^{(c')})\right)^o = \left(K(Z)\right)^o = K(Z,\mathfrak{Z}) .$$

Let $\mathfrak{X}$ have the defining equation $h_1(X,\mathfrak{X}) = 0$, where h_1 is irreducible over K ; let $\mathfrak{Z}$ have the defining equation $h_2(Z,\mathfrak{Z}) = 0$, where h_2 is irreducible over K. Now by Theorem 3A and the absolute irreducibility of f, $K = K^o$, so that K is algebraically closed in L. It follows that K is algebraically closed in $K(X,\mathfrak{X})$ and in $K(Z,\mathfrak{Z})$. Then by Theorem 3A again, h_1 and h_2 are absolutely irreducible. Hence if $\mathfrak{X}$ is of degree d_1 over $K(X)$ and if $\mathfrak{Z}$ is of degree d_2 over $K(Z)$, then

$$[K(X,Z,\mathfrak{X},\mathfrak{Z}) : K(X,Z)] = d_1 d_2$$

by Lemma 2A of Chapter III . But we have

$$K(X,Z,\mathfrak{X}) = \left(K(X_1^{(c)})\right)^o (X_m) = \left(K(X_1^{(c')})\right)^o (X_m) = K(X,Z,\mathfrak{Z}) ,$$

so that

$$K(X,Z,\mathfrak{X}) = K(X,Z,\mathfrak{Z}) = K(X,Z,\mathfrak{X},\mathfrak{Z}) .$$

These three fields are extension of $K(X,Z)$ of respective degrees d_1, d_2 and $d_1 d_2$, so that $d_1 = d_2 = d_1 d_2$, and therefore $d_1 = d_2 = 1$. Hence $\left(K(X_1^{(c)})\right)^o = K(X_1^{(c)})$ and $\left(K(X_1^{(c')})\right)^o = K(X_1^{(c')})$, which proves the lemma.

We now conclude the proof of Theorem 3D . We may write

$$f(X_1,\dots,X_m Y) = g(X_1^{(c)}, X_2,\dots,X_m,Y)$$

where $c \in K$ is obtained from Lemma 3F and where

$$g(X,X_2,\dots,X_m,Y) = f(X - cX_m,X_2,\dots,X_m,Y) .$$

Clearly $g(X_1^{(c)},X_2,\dots,X_m,\mathfrak{Y}) = 0$ and g is irreducible. But $g(\widehat{X_1^{(c)}},X_2,\dots,X_m,Y)$ is absolutely irreducible (i.e., irreducible over $\overline{K(X_1^{(c)})}$) because $\left(K(X_1^{(c)})\right)^o = K(X_1^{(c)})$. By a change of notation, $g(\widehat{X_1},X_2,\dots,X_m,Y)$ is absolutely irreducible. This new polynomial is clearly equivalent to f and is of degree d in Y . This process must now be repeated by setting $X_2^{(c)} = X_2 + cX_m$ with $c \in K$, etc., to obtain the result. Note that in the last step $X_\ell^{(c)} = X_\ell + cX_m$, hence that we certainly do need the condition $\ell \leqq m - 1 = n - 2$.

§ 4. The absolute irreducibility of polynomials (III) .

Let K be a field. We have denoted by K^n the n-dimensional vector space over K consisting of n-tuples $(x_1,\dots,x_n)$ with components in K . Suppose M is an m-dimensional linear manifold in K , where $1 \leq m \leq n$. Then M has a parameter representation

$$\underline{\underline{X}} = y_0 + U_1\,\underline{\underline{y}}_1 + \dots + U_m\,\underline{\underline{y}}_m ,$$

where $\underline{\underline{y}}_0$, $\underline{\underline{y}}_1$,..., $\underline{\underline{y}}_m \in K^n$, with $\underline{\underline{y}}_1,\dots\underline{\underline{y}}_m$ linearly independent, and where $U_1,\dots,U_n$ are parameters. We write $\underline{\underline{X}} = L(\underline{\underline{U}})$. Suppose M has another parameter representation

$$\underline{\underline{X}} = L'(\underline{\underline{U}}') = \underline{\underline{y}}'_0 + U'_1\,\underline{\underline{y}}'_1 + \ldots + U'_m\,\underline{\underline{y}}'_m \; .$$

Then $\underline{\underline{U}} = T\underline{\underline{U}}' + \underline{\underline{t}}$, where T is a non-singular $(m \times m)$-matrix over K and $\underline{\underline{t}} \in K^n$, hence $L(T\underline{\underline{U}}' + \underline{\underline{t}}) = L'(\underline{\underline{U}}')$. If $f(X_1,\ldots,X_n)$ is a polynomial with coefficients in K and M is a linear manifold with parameter representation $L(\underline{\underline{U}})$, put

$$f_L(\underline{\underline{U}}) = f(L(\underline{\underline{U}}))\,.$$

If L' is another parameter representation of M , then

$$f_{L'}(\underline{\underline{U}}') = f(L'(\underline{\underline{U}}')) = f(L(T\underline{\underline{U}}' + \underline{\underline{t}})) = f_L(T\underline{\underline{U}}' + \underline{\underline{t}}) \; .$$

Hence the polynomial f_L is determined by M up to equivalence in the sense of §3 . One can therefore speak of the "degree of f on M" and of the irreducibility or absolute irreducibility of f on M .

LEMMA 4A: *Suppose* $f(X_1,\ldots,X_n)$ *has coefficients in an infinite field* K , *is of degree* $d > 0$ *and is absolutely irreducible. Let* $n \geq 3$ *and suppose that* m *is such that* $2 \leq m < n$. *Then there exists a linear manifold* M *of dimension* m *such that* f *is of degree* d *and absolutely irreducible on* M .

Proof: We may replace f by an equivalent polynomial. We may therefore assume by Theorem 3D that

$$f(\overgroup{X_1,\ldots,X_{n-m}},X_{n-m+1},\ldots,X_n)$$

is of degree d (in $X_{n-m+1},\ldots,X_n$) and is absolutely irreducible. By Theorem 2A , for polynomials in m variables of degree at most

d , there is a system of forms $g_1,\ldots,g_s$ in the coefficients so that the polynomial is reducible or of degree $< d$ precisely if $g_1 = \ldots = g_s = 0$. In our case, the coefficients are polynomials in $X_1,\ldots,X_{n-m}$, so that we may write

$$g_i = g_i(X_1,\ldots,X_{n-m}) \qquad (1 \leq i \leq s) \; .$$

Since $f(\widehat{X_1,\ldots,X_{n-m}},X_{n-m+1},\ldots,X_n)$ is of degree d and is absolutely irreducible, we must have some $g_i(X_1,\ldots,X_{n-m}) \neq 0$, say for simplicity $g_1(X_1,\ldots,X_{n-m}) \neq 0$. Since K is infinite there exist elements $t_1,\ldots,t_{n-m} \in K$ such that $g_1(t_1,\ldots,t_{n-m}) \neq 0$. Then the polynomial

$$f(t_1,\ldots,t_{n-m},X_{n-m+1},\ldots,X_n)$$

in variables $X_{n-m+1},\ldots,X_n$ is of degree d and absolutely irreducible. This means simply that the polynomial f on the manifold M given by

$$x_1 = t_1,\ldots,x_{n-m} = t_{n-m}$$

is of degree d and absolutely irreducible, which proves the lemma.

Let M be a linear manifold of dimension $m \geqq 2$ with parameter representation

$$(4.1) \qquad \underline{\underline{X}} = L(\underline{\underline{U}}) = \underline{\underline{y}}_0 + U_1\,\underline{\underline{y}}_1 + \ldots + U_m\,\underline{\underline{y}}_m \; .$$

The polynomial f_L is absolutely irreducible and of degree d precisely if not all of certain froms $g_1,\ldots,g_s$ in the coefficients of f_L vanish. We have $g_i = g_i(\underline{\underline{y}}_0,\ldots,\underline{\underline{y}}_m)$, where $g_i(\underline{\underline{Y}}_0,\ldots,\underline{\underline{Y}}_m)$ are polynomials in $n(m+1)$ variables. Since there exists a manifold M on which f is of degree d and absolutely irreducible, not all these polynomials $g_i(\underline{\underline{Y}}_0, \underline{\underline{Y}}_1, \ldots, \underline{\underline{Y}}_n)$ are identically zero.

Let F be a subfield of K. We shall say that a linear manifold M in K^n is *generic* if it has[†] a parameter representation (4.1) where the $n(m+1)$ components of $\underline{\underline{y}}_0, \underline{\underline{y}}_1, \ldots, \underline{\underline{y}}_n$ are algebraically independent over F. (That is, they satisfy no non-trivial polynomial equation in $n(m+1)$ variables with coefficients in F). More precisely, one should say that M is generic over F. Suppose $f(X_1, \ldots, X_n)$ has coefficients in F and is absolutely irreducible. Then some $g_i(\underline{\underline{Y}}_0, \ldots, \underline{\underline{Y}}_n) \neq 0$, whence $g_i(\underline{\underline{y}}_0, \ldots, \underline{\underline{y}}_n) \neq 0$ if the components of $\underline{\underline{y}}_0, \underline{\underline{y}}_1, \ldots, \underline{\underline{y}}_n$ are algebraically independent over F. Thus f is absolutely irreducible on M. We thus have

THEOREM 4B: *Let* $f(\underline{\underline{X}}) \in F[\underline{\underline{X}}]$ *be absolutely irreducible and of degree* d. *Then on a generic linear manifold* M *of dimension* m $(2 \leq m \leq n)$, *the restriction of* f *is again absolutely irreducible and of degree* d.

This theorem, or rather a generalization of it, is sometimes called Bertini's Theorem. It is connected with work of the Italian geometer Bertini (1892).

Example: Take $n = 3$ and $m = 2$. The polynomial

$$f(X_1, X_2, X_3) = X_1^2 + X_2^2 - X_3^2 - 1$$

defines a hyperboloid of one shell in 3-space. The intersection of this hypersurface with a plane (a 2-dimensional linear manifold) can[*] be an ellipse, a hyperbola, a parabola, or if the plane is tangent

[*] this includes the case when the plane is "tangent to a point at infinity".

[†] Note that the parameter representation is not unique.

to the surface, two lines. The restriction of f to a plane is reducible precisely if the intersection consists of two lines; that is, precisely if the plane is tangent to the surface. It can be shown that the tangent planes are the planes

$$a_1x_1 + a_2x_2 + a_3x_3 + a_0 = 0$$

with $a_1^2 + a_2^2 - a_3^2 - a_0^2 = 0$. The planes with $a_0 = 0$ are tangent to an infinite point of the hyperboloid, and the intersection of the hyperboloid with such a plane consists of two parallel lines (i.e., two lines which intersect at an infinite point). The other tangent planes have an intersection with the hyperboloid which consists of two intersecting lines (i.e., lines whose intersection is a finite point).

THEOREM 4C: *Let* $f(X_1,\ldots,X_n)$ *be a polynomial over* F_q *of degree* $d > 0$ *which is absolutely irreducible. Let* $n \geq 3$ *and let* A *be the number of* 2-*dimensional linear manifolds* $M^{(2)}$. *Let* B *denote the number of manifolds* $M^{(2)}$ *on which* f *is not of degree* d *or is not absolutely irreducible. Let* $\Psi = 2dk^{2^k}$ *where* $k = \binom{d+1}{2}$.

Then

$$B/A \leq \Psi/q \ .$$

Proof: Every linear manifold $M^{(2)}$ has a parameter representation

$$\underline{\underline{X}} = \underline{\underline{y}}_0 + U_1\,\underline{\underline{y}}_1 + U_2\,\underline{\underline{y}}_2 \ ,$$

where $\underline{\underline{y}}_0, \underline{\underline{y}}_1, \underline{\underline{y}}_2 \in F_q^n$, and $\underline{\underline{y}}_1$ and $\underline{\underline{y}}_2$ are linearly independent.

If A' is the number of such parameter representations, then

$$A' = q^n(q^n - 1)(q^n - q) \geq \frac{1}{2}\,q^{3n} \ .$$

But each linear manifold $M^{(2)}$ has

$$D = q^2(q^2 - 1)(q^2 - q)$$

different parameter representations, whence $A = A'/D$. Now on a manifold $M^{(2)}$,

$$f_L(\underline{\underline{X}}) = f(\underline{\underline{y}}_0 + U_1 \underline{\underline{y}}_1 + U_2 \underline{\underline{y}}_2)$$

is a polynomial in U_1, U_2 . By Theorem 2A , there are forms $g_1, \ldots, g_s$ in the coefficients of this polynomial such that $g_1 = \ldots g_s = 0$ is equivalent to the polynomial being of degree $< d$ or irreducible. The degree of each g_i was at most

$$k^{2^k} = \Psi' ,$$

say, where $k = \binom{d+1}{2}$. (Note that f_L is a polynomial in 2 variables). The coefficients of $f(\underline{\underline{y}}_0 + U_1 \underline{\underline{y}}_1 + U_2 \underline{\underline{y}}_2)$ are polynomials in the coordinates of $\underline{\underline{y}}_0, \underline{\underline{y}}_1, \underline{\underline{y}}_2$ of degree at most d . Substituting these coefficients into $g_1, \ldots, g_s$, we obtain polynomials $h_1, \ldots h_s$ in the coordinates of $\underline{\underline{y}}_0, \underline{\underline{y}}_1, \underline{\underline{y}}_2$, each of degree at most $d\Psi'$, and having the property that $f(\underline{\underline{y}}_0 + U_1 \underline{\underline{y}}_1 + U_2 \underline{\underline{y}}_2)$ is of degree $< d$ or reducible if and only if $h_i(\underline{\underline{y}}_0, \underline{\underline{y}}_1, \underline{\underline{y}}_2) = 0$ for $i = 1, \ldots, s$. Since the restriction of f to a generic manifold $M^{(2)}$ is absolutely irreducible, some $h_i = h_i(\underline{\underline{Y}}_0, \underline{\underline{Y}}_1, \underline{\underline{Y}}_2)$, say h_1, is not identically zero. By Lemma 3A of Chapter IV, the number of $\underline{\underline{y}}_0, \underline{\underline{y}}_1, \underline{\underline{y}}_2$ with $h_1(\underline{\underline{y}}_0, \underline{\underline{y}}_1, \underline{\underline{y}}_2) = 0$ is at most $d\,\Psi' q^{3n-1}$. But since each $M^{(2)}$ has D representations,

$$B \le d\,\Psi'\, q^{3n-1}/D .$$

Hence

$$B/A \le d\,\Psi'\, q^{3n-1}/A' \le 2d\,\Psi'/q = \Psi/q .$$

§ 5. The number of zeros of absolutely irreducible polynomials in n variables.

In this section we shall allow the symbols $\omega(q,d)$ and $\chi(d)$ to take on either one of the following interpretations:

$$\text{(i)} \quad \omega(q,d) = \sqrt{2}\, d^{5/2} q^{1/2}, \quad \chi(d) = 250\, d^5,$$

$$\text{(ii)} \quad \omega(q,d) = (d-1)(d-2)q^{1/2} + d^2, \quad \chi(d) = 1.$$

So if $f(X,Y)$ is a polynomial with coefficients in F_q, absolutely irreducible and of degree $d > 0$, then

$$|N - q| < \omega(q,d) \tag{5.1}$$

whenever $q > \chi(d)$, where N is the number of zeros of $f(X,Y)$. With interpretation (i), this statement has been proved as Theorem 1A of Chapter III. However the statement also holds under interpretation (ii), as follows from the study of the zeta function of the curve $f(x,y)$ (Weil (1948a), Bombieri (1973)), and as may be known to a more sophisticated reader.

THEOREM 5A; Suppose $f(X_1,\ldots,X_n)$ is a polynomial over F_q of total degree $d > 0$ and absolutely irreducible. Let N be the number of zeros of f in F_q^n. Then

$$|N - q^{n-1}| \le q^{n-2}(\omega(q,d) + 2d\Psi), \tag{5.2}$$

where Ψ was defined in Theorem 4C.

If interpretation (i) is used, we obtain

$$|N - q^{n-1}| \le q^{n-2}(\sqrt{2}\, d^{5/2} q^{1/2} + 2d\Psi).$$

If we use interpretation (ii) , then

$$|N - q^{n-1}| \le q^{n-2}\left((d-1)(d-2)q^{1/2} + d^2 + 2d\,\Psi\right)$$

$$\le (d-1)(d-2)q^{n-(3/2)} + 3d\,\Psi\, q^{n-2} .$$

This theorem is due to Lang and Weil (1954) , and also Nisnevich (1954) . However, no value of the constant $2d\,\Psi$ was given . We now begin the

Proof: For a 2-dimensional linear manifold $M^{(2)}$ in F_q^n , let $N(M^{(2)})$ be the number of zeros of f on $M^{(2)}$. Every point of F_q^n lies on exactly

$$E = \frac{(q^n - 1)(q^n - q)}{(q^2 - 1)(q^2 - q)}$$

manifolds $M^{(2)}$. Thus

$$N = \frac{1}{E} \sum_{M^{(2)}} N(M^{(2)}) . \tag{5.3}$$

Observe that by the property of $\omega(q,d)$ discussed above and by Lemma 3A of Chapter IV, we have for $q > \chi(d)$,

$$|N(M^{(2)}) - q| \le \begin{cases} \omega(q,d) & \text{if } f \text{ is absol. irred. on } M^{(2)} , \\ dq & \text{if } f \text{ is not identically zero on } M^{(2)} , \\ q^2 & \text{if } f = 0 \text{ identically on } M^{(2)} . \end{cases} \tag{5.4}$$

LEMMA 5B: *Let* $f(X_1,\dots,X_n)$ *be a polynomial over* F_q , *of degree* $d > 0$ *and irreducible. Suppose* f *is not equivalent to a polynomial* $g(X_1,\dots,X_{n-2})$, *where only* $n - 2$ *variables appear. As in Theorem 4C ,* *let* A *be the number of 2-dimensional linear manifolds* $M^{(2)}$. Let C

be the number of manifolds $M^{(2)}$ *where* f *is identically zero. Then*

$$C/A \le d^3/q^2 \ .$$

Proof: Consider the planes $M^{(2)}$ parallel to the plane $x_1 = \dots = x_{n-2} = 0$; these number $A^* = q^{n-2}$. Let C^* be the number of those parallel planes on which f is identically zero. A typical plane of this type is

$$M^{(2)} : x_1 = c_1 , \dots , x_{n-2} = c_{n-2} \ .$$

The polynomial f can, of course, be written as

$$f(X_1,\dots,X_n) = \sum_{i,j} p_{ij}(X_1,\dots,X_{n-2})X_{n-1}^i X_n^j \ .$$

If f is identically zero on $M^{(2)}$, then

$$p_{ij}(c_1,\dots,c_{n-2}) = 0$$

for all i and j . If these polynomials p_{ij} have a common factor $g(X_1,\dots,X_{n-2})$ of positive degree, then g divides f and, since f is irreducible , $f = cg$. But by hypothesis f is not a polynomial in only $n - 2$ variables, hence the p_{ij} have no proper common factor. By Lemma 3D of Chapter IV, the number of common zeros $(c_1,\dots,c_{n-2})$ of the polynomials p_{ij} is at most $d^3 q^{n-4}$. It follows that $C^* \le d^3 q^{n-4}$ and

$$C^*/A^* \le d^3/q^2 \ .$$

The same argument holds for planes parallel to any given plane, and the result follows.

We now continue the

Proof of Theorem 5A: The proof is by induction on n. The case $n = 1$ is completely trivial, and the case $n = 2$ holds by what we said above. If $f \sim g$ where g is a polynomial in $n - 2$ variables, then the number of zeros of f is q^2 times the number N' of zeros of g in F_q^{n-2}. So by induction

$$|N' - q^{n-3}| \le q^{n-4}\left(\omega(q,d) + 2d\,\Psi\right),$$

whence (5.2). We may therefore suppose that f is not equivalent to a polynomial in $n - 2$ variables. Assume at first that $q > \chi(d)$. From (5.3) and (5.4) we find that

$$\left|N - \frac{1}{E}\sum_{M^{(2)}} q\right| \le \frac{1}{E}\left(\omega(q,d)\sum_{M^{(2)}} 1 + dq \sum_{\substack{M^{(2)} \\ f \text{ not absol.} \\ \text{irred.}}} 1 + q^2 \sum_{\substack{M^{(2)} \\ f \equiv 0 \text{ on } M^{(2)}}} 1\right).$$

In our established notation, it follows that

$$\begin{aligned}
|N - q^{n-1}| &\le \frac{1}{E}\left(\omega(q,d)A + dqB + q^2C\right) \\
&= (A/E)\left(\omega(q,d) + dq(B/A) + q^2(C/A)\right) \\
&\le q^{n-2}\left(\omega(q,d) + d\,\Psi + d^3\right) \\
&\le q^{n-2}\left(\omega(q,d) + 2d\,\Psi\right).
\end{aligned}$$

On the other hand if $q < \chi(d)$, then $q^2 < 2d\,\Psi$, whence

$$|N - q^{n-1}| < q^n < q^{n-2}\left(\omega(q,d) + 2d\,\Psi\right).$$

COROLLARY 5C: *Suppose* $f(X_1, \ldots, X_n)$ *is a polynomial with rational integer coefficients which is of degree* d *and absolutely irreducible. For primes* p, *let* $N(p)$ *be the number of solutions of the congruence*

$$f(x_1,\ldots,x_n) \equiv 0 \pmod{p} .$$

Then as $p \to \infty$,

$$N(p) = p^{n-1} + O\left(p^{n-(3/2)}\right).$$

Proof: The proof is a combination of Theorem 5A and Corollary 2B .

The error terms of Theorem 5A in the two possible interpretations are

$$\sqrt{2}\ d^{5/2} q^{n-(3/2)} + O\left(q^{n-2}\right)$$

and

$$(5.5) \qquad (d - 1)(d - 2)q^{n-(3/2)} + O\left(q^{n-2}\right) .$$

It may be shown (Weil (1948a)) that when $n = 2$, the exponent $\frac{1}{2}$ in the error term $(d - 1)(d - 2)q^{\frac{1}{2}} + O(1)$ is best possible. Also the constant $(d - 1)(d - 2)$ is best possible. If $g(X,Y)$ is a polynomial in 2 variables with N' zeros , then the polynomial $f(X_1,\ldots,X_n) = g(X_1,X_2)$ in n variables has $N = N'q^{n-2}$ zeros. Hence the exponent $n - (3/2)$ and the constant $(d - 1)(d - 2)$ in (5.5) are best possible for every n .

On the other hand the constant $2d\Psi$ in (5.2) is certainly too large. This is especially bad if one wants to estimate how large q must be in order that $N > 0$. With (5.2) one needs that q is certainly larger than $2d\Psi$, hence that q is very large as a function of d .

Schmidt (1973) applied the method of Stepanov directly to equations in n variables and obtained

$$N > q^{n-1} - 3d^3 q^{n-(3/2)} \quad \text{provided} \quad q > c_0 n^3 d^6 \quad ,$$

if (5.1) is used with $\omega(q,d)$ given by (i), and

$$N > q^{n-1} - (d-1)(d-2)q^{n-(3/2)} - 6d^2 q^{n-2} \quad \text{provided}$$
$$q > c_0(\varepsilon) n^3 d^{5+\varepsilon}$$

if (5.1) is used with $\omega(q,d)$ given by (ii) .

Much more is true for "non-singular" hypersurfaces by the deep work of Deligne (1973).[+)]

[+)] But see the remark in the Preface.