VI. Rudiments of Algebraic Geometry. The Number of Points in Varieties over Finite Fields.

General References: Artin (1955), Lang (1958), Shafarevich (1974), Mumford ( ) .

§1. Varieties.

THEOREM 1A. Let k be a field. Let $X_1, \ldots, X_n$ be variables.

(i) In the ring $k[X_1, X_2, \ldots, X_n]$ every ideal has a finite basis.

(ii) In this ring the ascending chain condition holds, i.e., if $\mathfrak{A}_1 \subseteq \mathfrak{A}_2 \subseteq \ldots$ is an ascending sequence of ideals, then for some m, $\mathfrak{A}_m = \mathfrak{A}_{m+1} = \ldots$.

(iii) Every non-empty set of ideals in this ring which is partially ordered by set inclusion, has at least one maximal element.

Statement (i) is the Hilbert Basis Theorem (Hilbert 1888). It is well known that the three conditions (i), (ii), (iii) for a ring R are equivalent. A ring satisfying these conditions is called Noetherian. A proof of this Theorem may be found in books on algebra, e.g. Van der Waerden (1955), Kap. 12 or Zariski-Samuel (1958), Ch. IV, and will not be given here.

If k, K are fields such that $k \subseteq K$, the transcendence degree of K over k, written tr. deg. K/k, is the maximum number of elements in K which are algebraically independent over k.

In what follows, k, Ω will be fields such that $k \subseteq \Omega$, the tr. deg $\Omega/k = \infty$, and Ω is algebraically closed. We call k the ground field, and Ω the universal domain. For example, we may take

$k = \mathbb{Q}$ (the rationals), $\Omega = \mathbb{C}$ (the complex numbers). Or $k = F_q$, the finite field of a q elements, $\Omega = \overline{F_q(X_1, X_2, \ldots)}$, i.e. the algebraic closure of $F_q(X_1, X_2, \ldots)$.

Consider Ω^n, the space of n-tuples of elements in Ω. Suppose $\mathfrak{J}$ is an ideal in $k[X_1, \ldots, X_n] = k[\underline{X}]$. Let $A(\mathfrak{J})$ be the set of $\underline{x} = (x_1, \ldots, x_n) \in \Omega^n$ having $f(\underline{x}) = 0$ for every $f(\underline{X}) \in \mathfrak{J}$. Every set $A(\mathfrak{J})$ so obtained is called an <u>algebraic set</u>. More precisely, it is a k-algebraic set. If we have such an ideal $\mathfrak{J}$, then by Theorem 1A, there exists a basis of $\mathfrak{J}$ consisting of a finite number of polynomials, say $f_1(\underline{X}), \ldots, f_m(\underline{X})$. Therefore $A(\mathfrak{J})$ can also be characterized as the set of $\underline{x} \in \Omega^n$ with $f_1(\underline{x}) = \ldots = f_m(\underline{x}) = 0$. Note that if $\mathfrak{J}_1 \subseteq \mathfrak{J}_2$, then $A(\mathfrak{J}_1) \supseteq A(\mathfrak{J}_2)$.

<u>Examples</u>: (1) Let $k = \mathbb{Q}$, $\Omega = \mathbb{C}$, $n = 2$, and $\mathfrak{J}$ the ideal generated by $f(X_1, X_2) = X_1^2 + X_2^2 - 1$. Then $A(\mathfrak{J})$ is the unit circle.

(2) Again let $k = \mathbb{Q}$, $\Omega = \mathbb{C}$, $n = 2$, and take $\mathfrak{J}$ to be the ideal generated by $f(X_1, X_2) = X_1^2 - X_2^2$. Then $A(\mathfrak{J})$ consists of the two intersecting lines $x_2 = x_1$, $x_2 = -x_1$.

<u>THEOREM 1B</u>. (i) <u>The empty set $\emptyset$ and Ω^n are algebraic sets.</u>

(ii) <u>A finite union of algebraic sets is an algebraic set.</u>

(iii) <u>An intersection of an arbitrary number of algebraic sets is an algebraic set.</u>

<u>Proof</u>: (i) If $\mathfrak{J} = k[X_1, \ldots, X_n]$, then $A(\mathfrak{J}) = \emptyset$. If $\mathfrak{J} = (0)$, i.e. the principal ideal generated by the zero polynomial, then $A(\mathfrak{J}) = \Omega^n$.

(ii) It is sufficient to show that the union of two algebraic sets is again an algebraic set. Suppose A is the algebraic set given by the equations $f_1(\underline{\underline{x}}) = \dots = f_\ell(\underline{\underline{x}}) = 0$, B is the algebraic set given by the equations $g_1(\underline{\underline{x}}) = \dots = g_m(\underline{\underline{x}}) = 0$. Then $A \cup B$ is the set of $\underline{\underline{x}} \in \Omega^n$ with $f_1(\underline{\underline{x}})\, g_1(\underline{\underline{x}}) = f_1(\underline{\underline{x}})\, g_2(\underline{\underline{x}}) = \dots = f_\ell(\underline{\underline{x}})\, g_m(\underline{\underline{x}}) = 0$.

(iii) Let A_α , $\alpha \in I$, where I is any indexing set, be a collection of algebraic sets. Suppose that $A_\alpha = A(\mathfrak{J}_\alpha)$, where $\mathfrak{J}_\alpha$ is an ideal in $k[\underline{\underline{X}}]$. We claim that

(1.1) $$\bigcap_{\alpha \in I} A(\mathfrak{J}_\alpha) = A\left(\sum_{\alpha \in I} \mathfrak{J}_\alpha \right),$$

where $\sum_{\alpha \in I} \mathfrak{J}_\alpha$ is the ideal consisting of sums $f_1(\underline{\underline{X}}) + \dots + f_\ell(\underline{\underline{X}})$ with each $f_i(\underline{\underline{X}})$ in $\mathfrak{J}_\alpha$ for some $\alpha \in I$. To prove (1.1) , suppose that $\underline{\underline{x}} \in \bigcap_{\alpha \in I} A(\mathfrak{J}_\alpha)$. Then for each $\alpha \in I$, $\underline{\underline{x}} \in A(\mathfrak{J}_\alpha)$, whence $f(\underline{\underline{x}}) = 0$ if $f \in \mathfrak{J}_\alpha$. Therefore $f(\underline{\underline{x}}) = 0$ if $f \in \sum_{\alpha \in I} \mathfrak{J}_\alpha$. Hence $\underline{\underline{x}} \in A\left(\sum_{\alpha \in I} \mathfrak{J}_\alpha \right)$. Conversely, if $\underline{\underline{x}} \in A\left(\sum_{\alpha \in I} \mathfrak{J}_\alpha \right)$, then $f(\underline{\underline{x}}) = 0$ if $f \in \sum_{\alpha \in I} \mathfrak{J}_\alpha$. So for any $\alpha \in I$, if $f \in \mathfrak{J}_\alpha$, then $f(\underline{\underline{x}}) = 0$. Thus, $\underline{\underline{x}} \in A(\mathfrak{J}_\alpha)$ for all α , or $\underline{\underline{x}} \in \bigcap_{\alpha \in I} A(\mathfrak{J}_\alpha)$. This proves (1.1) . It follows that $\bigcap A_\alpha = \bigcap A(\mathfrak{J}_\alpha)$ is an algebraic set.

In Ω^n we can now introduce a topology by defining the <u>closed sets</u> as the algebraic sets. This topology is called the <u>Zariski Topology</u>. As usual, the <u>closure</u> of a set M is the intersection of the closed sets containing M . It is the smallest closed set containing M and is denoted by $\overline{M}$.

Let M be a subset of Ω^n . We write $\mathfrak{J}(M)$ for the ideal of all polynomials $f(\underline{\underline{X}})$ which vanish on M, i.e., all polynomials $f(\underline{\underline{X}})$

such that $f(\underline{\underline{x}}) = 0$ for every $\underline{\underline{x}} \in M$. It is clear that if $M_1 \subseteq M_2$, then $\mathfrak{I}(M_1) \supseteq \mathfrak{I}(M_2)$.

THEOREM 1C. $\overline{M} = A\mathfrak{I}(M))$.

Proof: Clearly $A(\mathfrak{I}(M))$ is a closed set containing M. Therefore it is sufficient to show that $A(\mathfrak{I}(M))$ is the smallest closed set containing M. Let T be a closed set containing M; say $T = A(\mathfrak{J})$. Since $T \supseteq M$, it follows that $\mathfrak{J} \subseteq \mathfrak{I}(T) \subseteq \mathfrak{I}(M)$, so that

$$T = A(\mathfrak{J}) \supseteq A\mathfrak{I}(M)).$$

Remark: If S is an algebraic set, then it follows from Theorem 1C that $S = A\mathfrak{I}(S))$.

If $\mathfrak{A}$ is an ideal, define the radical of $\mathfrak{A}$, written $\sqrt{\mathfrak{A}}$, to consist of all $f(\underline{\underline{X}})$ such that for some positive integer m, $f^m(\underline{\underline{X}}) \in \mathfrak{A}$. The radical of $\mathfrak{A}$ is again an ideal. For if $f(\underline{\underline{X}}), g(\underline{\underline{X}}) \in \sqrt{\mathfrak{A}}$, then there exist positive integer m, ℓ such that $f^m(\underline{\underline{X}}), g^{\ell}(\underline{\underline{X}}) \in \mathfrak{A}$. Thus by the Binomial Theorem, $(f(\underline{\underline{X}}) \pm g(\underline{\underline{X}}))^{m+\ell} \in \mathfrak{A}$, so that $f(\underline{\underline{X}}) \pm g(\underline{\underline{X}}) \in \sqrt{\mathfrak{A}}$. Also, for any $h(\underline{\underline{X}})$ in $k[\underline{\underline{X}}]$, $(h(\underline{\underline{X}})\ f(\underline{\underline{X}}))^m \in \mathfrak{A}$, so that $h(\underline{\underline{X}})f(\underline{\underline{X}}) \in \sqrt{\mathfrak{A}}$.

If $\mathfrak{P}$ is a prime ideal, then $\sqrt{\mathfrak{P}} = \mathfrak{P}$, since if $f(\underline{\underline{X}}) \in \sqrt{\mathfrak{P}}$, then $f^m(\underline{\underline{X}}) \in \mathfrak{P}$, which implies that $f(\underline{\underline{X}}) \in \mathfrak{P}$.

THEOREM 1D. Let $\mathfrak{A}$ be an ideal in $k[\underline{\underline{X}}]$. Then

$$\mathfrak{I}(A(\mathfrak{A})) = \sqrt{\mathfrak{A}}.$$

Example: Let $k = \mathbb{Q}$, $\Omega = \mathbb{C}$, $n = 2$, and $\mathfrak{A}$ the principal ideal generated by $f(X_1, X_2) = (X_1^2 + X_2^2 - 1)^3$. Then $A(\mathfrak{A})$ is the unit circle, and $\mathfrak{I}(A(\mathfrak{A})) = (X_1^2 + X_2^2 - 1)$. Thus $\sqrt{\mathfrak{A}} = (X_1^2 + X_2^2 - 1)$, the ideal generated by $X_1^2+X_2^2-1$.

Before proving Theorem 1D we need two lemmas.

LEMMA 1E. Given a prime ideal $\mathfrak{P} \neq k[\underline{\underline{X}}]$, there exists an $\underline{\underline{x}} \in \Omega^n$ with $\mathfrak{I}(\underline{\underline{x}}) = \mathfrak{P}$.

Proof. Form the natural homomorphism from $k[\underline{X}]$ to the quotient ring $k[\underline{X}]/\mathfrak{P}$. Since $\mathfrak{P} \cap k = \{0\}$, the natural homomorphism is an isomorphism on k. Thus we may consider $k[\underline{X}]/\mathfrak{P}$ as an extension of k, and the natural homomorphism restricted to k becomes the identity map. Thus our homomorphism is a k-homomorphism. Let the image of X_i be $\xi_i (i = 1,\ldots,n)$. The natural homomorphism is then a homomorphism from $k[X_1,\ldots,X_n]$ onto $k[\xi_1,\ldots,\xi_n]$ with kernel $\mathfrak{P}$. Since $\mathfrak{P}$ was a prime ideal, $k[\xi_1,\ldots,\xi_n]$ is an integral domain.

Try to replace ξ_i by $x_i \in \Omega$. If, say, $\xi_1,\ldots,\xi_d$ are algebraically independent over k with $\xi_{d+1},\ldots,\xi_n$ algebraically dependent on them, choose $x_1,\ldots,x_d \in \Omega$ algebraically independent over k. Then $k(\xi_1,\ldots,\xi_d)$ is k-isomorphic to $k(x_1,\ldots,x_d)$. Also, ξ_{d+1} is algebraic over $k(\xi_1,\ldots,\xi_d)$, and so satisfies a certain irreducible equation with coefficients in $k(\xi_1,\ldots,\xi_d)$. Choose x_{d+1} in Ω such that it satisfies the corresponding equation as ξ_{d+1} but with coefficients in $k(x_1,\ldots,x_d)$. Then $k(\xi_1,\ldots,\xi_{d+1})$ is k-isomorphic to $k(x_1,\ldots,x_{d+1})$. There is a k-isomorphism with $\xi_i \to x_i$ $(i = 1,\ldots,d+1)$.

Continuing in this manner, we can find $x_1,\ldots,x_n \in \Omega$ such that $k(\xi_1,\ldots,\xi_n)$ is k-isomorphic to $k(x_1,\ldots,x_n)$. There is an isomorphism α with $\alpha(\xi_i) = x_i$ $(i = 1,\ldots,n)$.

Composing the natural homomorphism with the isomorphism α we obtain a homomorphism

$$\varphi\colon k[X_1,\ldots,X_n] \to k[x_1,\ldots,x_n]$$

with kernel $\mathfrak{P}$. Write $\underline{x} = (x_1,\ldots,x_n)$.

Now $\mathfrak{J}(\underline{x}) = \mathfrak{P}$, for $f(\underline{x}) = 0$ precisely if $\varphi(f(\underline{X})) = 0$, which is true if $f(\underline{X}) \in \mathfrak{P}$.

<u>LEMMA 1F. Let $\mathfrak{S}$ be a non-empty subset of $k[\underline{X}]$ which is closed under multiplication and doesn't contain zero. Let $\mathfrak{P}$ be an ideal</u>

which is maximal with respect to the property that $\mathfrak{P} \cap \mathfrak{S} = \emptyset$. *Then* $\mathfrak{P}$ *is a prime ideal.*

Proof: Suppose $f(\underline{X})g(\underline{X}) \in \mathfrak{P}$ but that $f(\underline{X})$ and $g(\underline{X})$ are not in $\mathfrak{P}$. Let $\mathfrak{A} = (\mathfrak{P}, f(\underline{X}))^{*}$, so that $\mathfrak{A}$ properly contains $\mathfrak{P}$. Since $\mathfrak{P}$ is maximal with respect to the property that $\mathfrak{P} \cap \mathfrak{S} = \emptyset$, it follows that $\mathfrak{A} \cap \mathfrak{S} \neq \emptyset$. So there exists a $c(\underline{X}) = p(\underline{X}) + h(\underline{X})\, f(\underline{X})$, where $c(\underline{X}) \in \mathfrak{S}$, $p(\underline{X}) \in \mathfrak{P}$, $h(\underline{X}) \in k[\underline{X}]$. Similarly, there exists a $c'(\underline{X}) = p'(\underline{X}) + h'(\underline{X})\, g(\underline{X})$, where $c'(X) \in \mathfrak{S}$, $p'(\underline{X}) \in \mathfrak{P}$, $h'(\underline{X}) \in k[\underline{X}]$. Then

$$c'(\underline{X})\, c(\underline{X}) = (p'(\underline{X}) + h'(\underline{X})\, g(\underline{X}))(p(\underline{X}) + h(\underline{X})\, f(\underline{X})) \in \mathfrak{P} .$$

However, since $\mathfrak{S}$ is closed under multiplication, $c'(\underline{X})\, c(\underline{X}) \in \mathfrak{S}$, contradicting the hypothesis that $\mathfrak{P} \cap \mathfrak{S} = \emptyset$.

Proof of Theorem 1D: Suppose $f \in \sqrt{\mathfrak{A}}$, so that there exists a positive integer m with $f^m \in \mathfrak{A}$. Thus for every $\underline{x} \in A(\mathfrak{A})$, $f^m(\underline{x}) = 0$. Hence $f(\underline{x}) = 0$ for every $\underline{x} \in A(\mathfrak{A})$. Therefore $f(\underline{X}) \in \mathfrak{J}(A(\mathfrak{A}))$, and $\sqrt{\mathfrak{A}} \subseteq \mathfrak{J}(A(\mathfrak{A}))$.

Suppose $f \notin \sqrt{\mathfrak{A}}$. If $\mathfrak{S}$ is the set of all positive integer powers of f , then $\mathfrak{S} \cap \mathfrak{A} = \emptyset$; also $\mathfrak{S}$ does not contain zero. Let $\mathfrak{P}$ be an ideal containing $\mathfrak{A}$ which is maximal[†] with respect to the property that $\mathfrak{S} \cap \mathfrak{P} = \emptyset$. By Lemma 1F, $\mathfrak{P}$ is a prime ideal. By Lemma 1E, there exists a point $\underline{x} \in \Omega^n$ such that $\mathfrak{P} = \mathfrak{J}(\underline{x})$. Since $f \notin \mathfrak{P}$, $f(\underline{x}) \neq 0$. Also, $(\overline{\underline{x}}) = A(\mathfrak{J}(\underline{x})) = A(\mathfrak{P}) \subseteq A(\mathfrak{A})$, so that $\underline{x} \in A(\mathfrak{A})$. It follows that $f \notin \mathfrak{J}(A(\mathfrak{A}))$. Thus $\mathfrak{J}(A(\mathfrak{A})) \subseteq \sqrt{\mathfrak{A}}$.

---

†) The existence of such an ideal is guaranteed by Theorem 1A.

* the ideal generated by $\mathfrak{P}$ and $f(\underline{X})$.

Suppose S is an algebraic set. We call S reducible if $S = S_1 \cup S_2$, where S_1, S_2 are algebraic sets, and $S \neq S_1, S_2$. Otherwise, we call S irreducible.

Example: Let $k = \mathbb{Q}$, $K = \mathbb{C}$, $n = 2$, and let $\mathfrak{J}$ be the ideal generated in $k[X_1, X_2]$ by the polynomial $f(X_1, X_2) = X_1^2 - X_2^2$. Then $S = A(\mathfrak{J})$ is the set of all $\underline{\underline{x}} \in \mathbb{C}^2$ such that $x_1^2 - x_2^2 = 0$. If S_1 is the set of all $\underline{\underline{x}} \in \mathbb{C}^2$ with $x_1 + x_2 = 0$, and S_2 is the set of all $\underline{\underline{x}} \in \mathbb{C}^2$ with $x_1 - x_2 = 0$, then $S = S_1 \cup S_2$, and $S_1 \neq S \neq S_2$. Hence S is reducible.

THEOREM 1G. Let S be a non-empty algebraic set. The following four conditions are equivalent:

(i) $S = \overline{(\underline{\underline{x}})}$, i.e. S is the closure of a single point $\underline{\underline{x}}$,

(ii) S is irreducible,

(iii) $\mathfrak{J}(S)$ is a prime ideal in $k[\underline{\underline{X}}]$,

(iv) $S = A(\mathfrak{P})$, where $\mathfrak{P}$ is a prime ideal in $k[\underline{\underline{X}}]$.

Proof: (i) $\Rightarrow$ (ii). Suppose $S = A \cup B$, where A and B are algebraic sets, and $A \neq S \neq B$. We have $\underline{\underline{x}} \in S = A \cup B$. We may suppose that, say, $\underline{\underline{x}} \in A$. Then $S = \overline{(\underline{\underline{x}})} \subseteq \overline{A} = A$, whence $S = A$, which is a contradiction.

(ii) $\Rightarrow$ (iii). Suppose that $\mathfrak{J}(S)$ is not prime. Then we would have $f(\underline{\underline{X}})\, g(\underline{\underline{X}}) \in \mathfrak{J}(S)$ with neither $f(\underline{\underline{X}})$ nor $g(\underline{\underline{X}})$ in $\mathfrak{J}(S)$. Let $\mathfrak{A} = (\mathfrak{J}(S), f(\underline{\underline{X}}))$ (i.e. the ideal generated by $\mathfrak{J}(S)$ and $f(\underline{\underline{X}})$). Let $\mathfrak{B} = (\mathfrak{J}(S), g(\underline{\underline{X}}))$. Let $A = A(\mathfrak{A})$, $B = A(\mathfrak{B})$. In view of $S = A(\mathfrak{J}(S))$ and $\mathfrak{A} \supseteq \mathfrak{J}(S)$, we have $A \subseteq S$. But $A \neq S$ since $f \in \mathfrak{J}(A)$ and

$f \notin \mathfrak{J}(S)$. Thus $A \subsetneq S$. Similarly, $B \subsetneq S$. But we claim that $S = A \cup B$. Clearly $A \cup B \subseteq S$. On the other hand, if $\underline{\underline{x}} \in S$, then $f(\underline{\underline{x}})\, g(\underline{\underline{x}}) = 0$. Without loss of generality, let us assume that $f(\underline{\underline{x}}) = 0$. Then $\underline{\underline{x}}$ is a zero of every polynomial of $\mathfrak{A}$, so that $\underline{\underline{x}} \in A$. Therefore $S \subseteq A \cup B$. Thus $S = A \cup B$, with $A \neq S \neq B$. This contradicts the irreducibility of S .

(iii) ⇒ (iv). Set $\mathfrak{P} = \mathfrak{J}(S)$. Then $S = A(\mathfrak{J}(S)) = A(\mathfrak{P})$.

(iv) ⇒ (i). Choose $\underline{\underline{x}}$ according to Lemma 1E with $\mathfrak{J}(\underline{\underline{x}}) = \mathfrak{P}$. Then $S = A(\mathfrak{P}) = A(\mathfrak{J}(\underline{\underline{x}})) = (\overline{\underline{\underline{x}}})$. The proof of Theorem 1G is complete.

A set S satisfying any one of the four equivalent properties of Theorem 1G is called a <u>variety</u>. (More precisely, it is a k-<u>variety</u>.) If V is a variety, $\underline{\underline{x}} \in V$ is called a <u>generic point</u> of V if $V = (\overline{\underline{\underline{x}}})$.

<u>COROLLARY 1H</u>. <u>There is a one to one correspondence between the collection of all k-varieties V in Ω^n and the collection of all prime ideals $\mathfrak{P} \neq k[\underline{X}]$ in $k[\underline{X}]$, given by</u>

$$V \overset{\alpha}{\rightarrow} \mathfrak{P} = \mathfrak{J}(V) \quad \underline{\text{and}} \quad \mathfrak{P} \overset{\beta}{\rightarrow} V = A(\mathfrak{P}) .$$

<u>Proof</u>: Let V be a variety in Ω^n ; then $V \overset{\alpha}{\rightarrow} \mathfrak{J}(V) \overset{\beta}{\rightarrow} A(\mathfrak{J}(V)) = V$. Also, if $\mathfrak{P}$ is a prime ideal in $k[\underline{X}]$, then $\mathfrak{P} \overset{\beta}{\rightarrow} A(\mathfrak{P}) \overset{\alpha}{\rightarrow} \mathfrak{J}(A(\mathfrak{P})) = \sqrt{\mathfrak{P}} = \mathfrak{P}$

<u>Examples</u>: (1) Let $S = \Omega^n$. Now $\mathfrak{J}(\Omega^n) = (0)$, a prime ideal. Suppose $\underline{\underline{x}} = (x_1,\ldots,x_n)$ is of transcendence degree n , i.e. the n

coordinates are algebraically independent over k. Then $\mathfrak{J}(\underline{\underline{x}}) = (0)$, so $(\overline{\underline{\underline{x}}}) = A(\mathfrak{J}(\underline{\underline{x}})) = A((0)) = \Omega^n$. So any point of Ω^n of transcendence degree n over k is a generic point of Ω^n.

(2) Let $k = \mathbb{Q}$, $\Omega = \mathbb{C}$, $n = 2$. Let $\mathfrak{P}$ be the principal ideal generated by $f(X_1,X_2) = X_1^2 + X_2^2 - 1$. $\mathfrak{P}$ is a prime ideal since f is irreducible. Thus $A(\mathfrak{P})$, i.e. the unit circle, is a variety. Choose $x_1 \in \Omega$ and transcendental over $\mathbb{Q}$. Pick $x_2 \in \Omega$ with $x_2^2 = 1 - x_1^2$. Then the point $\underline{\underline{x}} = (x_1,x_2)$ belongs to $A(\mathfrak{P})$. In fact, $\underline{\underline{x}}$ is a generic point of $A(\mathfrak{P})$:

To see this, it will suffice to show that $\mathfrak{J}(\underline{\underline{x}}) = (X_1^2 + X_2^2 - 1)$, i.e. the principal ideal generated by $X_1^2 + X_2^2 - 1$. If $g(X_1,X_2) \in \mathfrak{J}(\underline{\underline{x}})$, that is, if $g(x_1,x_2) = 0$, then $g(x_1,X_2)$ is a multiple of $X_2^2 - 1 + x_1^2$, since x_2 is a root of $X_2^2 - 1 + x_1^2$, which is irreducible over $\mathbb{Q}(x_1)$. More precisely,

$$g(x_1,X_2) = (X_2^2 - 1 + x_1^2)\ h(x_1,X_2)\ ,$$

where $h(X_1,X_2)$ is a polynomial in X_2 and is rational in X_1. Since x_1 was transcendental, we get

$$g(X_1,X_2) = (X_1^2 + X_2^2 - 1)\ h(X_1,X_2)\ .$$

In view of the unique factorization in $\mathbb{Q}[X_1]$, it follows that $h(X_1,X_2)$ is in fact a polynomial in X_1,X_2. Thus $\mathfrak{J}(\underline{\underline{x}}) = (X_1^2 + X_2^2 - 1)$.

(3) Let $k = \mathbb{Q}$, $\Omega = \mathbb{C}$, $n = 2$. Let $\mathfrak{P}$ be the principal ideal generated by $f(X_1,X_2) = X_1^2 - X_2$. Then $A(\mathfrak{P})$ is irreducible and is a parabola. Choose $x_1 \in \Omega$ and transcendental over Q, and put $x_2 = x_1^2$. Then $\underline{\underline{x}} = (x_1,x_2)$ lies in $A(\mathfrak{P})$. An argument similar to

the one given in (2) shows that $\underline{\underline{x}}$ is a generic point of $A(\mathfrak{P})$. For example, Lindemann's Theorem says that e is transcental over $\mathbb{Q}$, and therefore (e,e^2) is a generic point of $A(\mathfrak{P})$.

(4) Let $k = \mathbb{Q}$, $\Omega = \mathbb{C}$. Let $\mathfrak{A}$ be the principal ideal $\mathfrak{A} = (X_1^2 - X_2^2)$. Then as we have seen above, $A(\mathfrak{A})$ is reducible and is therefore not a variety.

(5) Consider a linear manifold M^d given by a parameter representation

$$x_i = b_i + a_{i1} t_1 + \dots + a_{id} t_d \qquad (1 \leqq i \leqq n) .$$

Here the b_i and the a_{ij} as given elements of k, with the $(d \times n)$ - matrix (a_{ij}) of rank d . As $t_1, \dots, t_d$ run through Ω , $\underline{\underline{x}} = (x_1, \dots, x_n)$ runs through M^d . It follows from linear algebra that M^d is an algebraic set. (It is a "d-dimensional linear manifold". See also §2 about the notion of dimension). In fact M^d is a variety:

Choose $\eta_1, \dots, \eta_d$ algebraically independent over k . Put

$$\xi_i = b_i + a_{i1} \eta_1 + \dots + a_{id} \eta_d \qquad (1 \leq i \leq n)$$

and $\underline{\underline{\xi}} = (\xi_1, \xi_2, \dots, \xi_n) \in \Omega^n$. Now $\underline{\underline{\xi}} \in M^d$, so $(\overline{\underline{\underline{\xi}}}) \subseteq M^d$. Conversely, if $f(\underline{\underline{\xi}}) = 0$, then

$$f(b_1 + a_{11}T_1 + \dots + a_{1d}T_d ,$$
$$b_2 + a_{21}T_1 + \dots + a_{2d}T_d, \dots, b_n + a_{n1}T_1 + \dots + a_{nd}T_d) = 0 ,$$

where $T_1, \dots, T_d$ are variables. Thus if $\underline{\underline{x}} \in M^d$, then $f(\underline{\underline{x}}) = 0$. So every $\underline{\underline{x}} \in M^d$ lies in $A(\mathfrak{J}(\underline{\underline{\xi}})) = (\overline{\underline{\underline{\xi}}})$. Therefore we have shown that $M^d = (\overline{\underline{\underline{\xi}}})$, or that M^d is a variety.

(6) Take $k = \mathbb{Q}$, $\Omega = \mathbb{C}$, $n = 2$, and $\mathfrak{A}$ the principal ideal generated by $f(X_1,X_2) = X_1^2 - 2X_2^2$. Over $k = \mathbb{Q}$, this polynomial is irreducible. Thus $\mathfrak{A}$ is a prime ideal, and $A(\mathfrak{A})$ is a variety. However, if we take $k' = \mathbb{Q}(\sqrt{2})$, then $f(X_1,X_2)$ is no longer irreducible over k' , so that $\mathfrak{A}$ is no longer a prime ideal in $k'[X_1,X_2]$, and $A(\mathfrak{A})$ is no longer a variety.

This prompts the definition: A variety is called an <u>absolute variety</u> if it remains a variety over every algebraic extension of k .

<u>THEOREM 1I. Every non-empty algebraic set is a finite union of varieties.</u>

<u>Proof</u>: We first show that every non-empty collection $\mathfrak{S}$ of algebraic sets has a minimal element. For if we form all ideals $\mathfrak{J}(S)$, where $S \in \mathfrak{S}$, there is by Theorem 1A a maximal element of this non-empty collection of ideals. Say $\mathfrak{J}(S_0)$ is maximal. We claim that $S_0 \in \mathfrak{S}$ is minimal. For if $S_1 \subseteq S_0$ where $S_1 \in \mathfrak{S}$, then $\mathfrak{J}(S_1) \supseteq \mathfrak{J}(S_0)$; but since $\mathfrak{J}(S_0)$ is maximal, $\mathfrak{J}(S_1) = \mathfrak{J}(S_0)$. Thus $S_1 = A(\mathfrak{J}(S_1))$ $= A(\mathfrak{J}(S_0)) = S_0$.

Suppose that Theorem 1I is false. Let $\mathfrak{S}$ be the collection of algebraic sets for which Theorem 1I is false. There is a minimal element S_0 of $\mathfrak{S}$. If S_0 were a variety, then the theorem would be true for S_0 . Hence S_0 is reducible. Let $S_0 = A \cup B$, where A,B are algebraic sets, with $A \neq S_0 \neq B$. Since S_0 is minimal and $A \subsetneqq S_0$, $B \subsetneqq S_0$, the theorem is true for A,B . Hence, we can write $A = V_1 \cup \ldots \cup V_m$, and $B = W_1 \cup \ldots \cup W_\ell$, where $V_i\ (1 \le i \le m)$ and $W_j\ (1 \le j \le \ell)$ are varieties. Thus

$$S_0 = A \cup B = V_1 \cup \ldots \cup V_m \cup W_1 \cup \ldots \cup W_\ell ,$$

contradicting our hypothesis that $S_0 \in \mathfrak{S}$.

It is clear that there exists a representation of S as $S = V_1 \cup \ldots \cup V_t$ where $V_i \not\subseteq V_j$ if $i \neq j$.

THEOREM 1J. *Let S be a non-empty algebraic set. The representation of S as*

$$S = V_1 \cup \ldots \cup V_t ,$$

where $V_1,\ldots,V_t$ are varieties with $V_i \not\subseteq V_j$ if $i \neq j$, is unique.

Proof: Exercise.

The V_i in the unique representation of S given in Theorem 1J are called the *components* of S .

Example: Let $k = \mathbb{Q}$, $\Omega = \mathbb{C}$, $n = 2$, and $S = A((X_1^2 - X_2^2))$. Let $V_1 = A((X_1 - X_2))$ and $V_2 = A((X_1 + X_2))$; then $S = V_1 \cup V_2$. Here V_1, V_2 are two intersecting lines.

Finally we introduce the following terminology and notation. We say $\underline{\underline{y}}$ is a *specialization* of $\underline{\underline{x}}$ and write

$$\underline{\underline{x}} \to \underline{\underline{y}} ,$$

if $\underline{\underline{y}} \in \overline{(\underline{\underline{x}})}$. This holds precisely if $f(\underline{\underline{y}}) = 0$ for every $f(\underline{\underline{X}}) \in k[\underline{\underline{X}}]$ with $f(\underline{\underline{x}}) = 0$. It is immediately seen that $\to$ is transitive, i.e. that

$$\underline{\underline{x}} \to \underline{\underline{y}} \text{ and } \underline{\underline{y}} \to \underline{\underline{z}} \text{ implies that } \underline{\underline{x}} \to \underline{\underline{z}} .$$

If both $\underline{\underline{x}} \to \underline{\underline{y}}$ and $\underline{\underline{y}} \to \underline{\underline{x}}$, then we write $\underline{\underline{x}} \leftrightarrow \underline{\underline{y}}$. This is equivalent with the equation $(\bar{\underline{x}}) = (\bar{\underline{y}})$.

Example: Let $\underline{x} = (e, e^2)$ and $\underline{y} = (1,1)$. Then $\underline{x} \to \underline{y}$. For as we saw in example (3) below Theorem 1G , the point $\underline{x}$ is a generic point of the parabola $x_2 - x_1^2 = 0$, and $\underline{y}$ lies on this parabola.

§2. Dimension.

Let $\underline{x} \in \Omega^n$. The transcendence degree of $\underline{x}$ over k is the maximum number of algebraically independent components of $\underline{x}$ over k . This clearly is equal to the transcendence degree of $k(\underline{x})$ over k . We have

$$0 \le \text{tr. deg. } \underline{x} \le n .$$

THEOREM 2A. Suppose $\underline{x} \to \underline{y}$. Then

(i) tr. deg. $\underline{y} \le$ tr. deg. $\underline{x}$.

(ii) Equality hold in (i) if and only if $\underline{x} \leftrightarrow \underline{y}$.

Proof: (i) Induction on n . If n = 1 , and if trans. deg. $\underline{x} = 1$, then tr. deg. $\underline{y} \le n = 1 =$ trans. deg $\underline{x}$; if tr. deg. $\underline{x} = 0$, then $\underline{x}$ is algebraic over k . In this case, since $\underline{x} \to \underline{y}$, the components of $\underline{y}$ satisfy the algebraic equations satisfied by the components of $\underline{x}$, and tr. deg. $\underline{y} = 0$.

To show the induction step, let d be the transcendence degree of $\underline{x}$. We may assume that $d < n$. We may also assume that tr. deg. $\underline{y} \ge d$. Without loss of generality, we assume that $y_1, \ldots, y_d$ are algebraically independent over k . Since $\underline{x} = (x_1, \ldots, x_n) \to (y_1, \ldots, y_n) = \underline{y}$, it follows that $(x_1, \ldots, x_d) \to (y_1, \ldots, y_d)$. By induction, and since

$d < n$, the elements $x_1,\ldots,x_d$ are also algebraically independent over k . Let $d < i \le n$. Then x_i is algebraically dependent on $x_1,\ldots,x_d$. So x_i satisfies some non-trivial equation

$$x_i^a\, g_a(x_1,\ldots,x_d) + x_i^{a-1}\, g_{a-1}(x_1,\ldots,x_d) + \ldots + g_0(x_1,\ldots,x_d) = 0$$

Since $\underline{\underline{x}} \rightarrow \underline{\underline{y}}$, it follows that

$$y_i^a\, g_a(y_1,\ldots,y_d) + y_i^{a-1}\, g_a(y_1,\ldots,y_d) + \ldots + g_0(y_1,\ldots,y_d) = 0 .$$

Thus y_i is algebraically dependent on $y_1,\ldots,y_d$. This is true for any i in $d < i \le n$. So tr. deg. $\underline{\underline{y}} \le d$.

(ii) If $\underline{\underline{x}} \leftrightarrow \underline{\underline{y}}$, then it follows from part (i) that tr. deg. $\underline{\underline{x}}$ = tr. deg. $\underline{\underline{y}}$.

Suppose $\underline{\underline{x}} \rightarrow \underline{\underline{y}}$ and tr. deg. $\underline{\underline{x}}$ = tr. deg. $\underline{\underline{y}}$. Let the common transcendence degree be d . We may assume without loss of generality that the first d coordinates $y_1,\ldots,y_d$ are algebraically independent over k . Then by part (i) and by $(x_1,\ldots,x_d) \rightarrow (y_1,\ldots,y_d)$, also $x_1,\ldots,x_d$ are algebraically independent over k . We have to show that $\underline{\underline{y}} \rightarrow \underline{\underline{x}}$, i.e. that if $f(\underline{\underline{y}}) = 0$ for $f \in k[\underline{\underline{X}}]$, then $f(\underline{\underline{x}}) = 0$. Put differently, we have to show that if $f(\underline{\underline{x}}) \neq 0$, then $f(\underline{\underline{y}}) \neq 0$. So let $f(\underline{\underline{x}}) \neq 0$. Then $f(\underline{\underline{x}})$ is a non-zero element of $k(\underline{\underline{x}})$ and $1/f(\underline{\underline{x}}) \in k(\underline{\underline{x}})$. Now since $x_{d+1},\ldots,x_n$ are algebraic over $k(x_1,\ldots,x_d)$, it is well known that

$$k(\underline{\underline{x}}) = k(x_1,\ldots,x_d)[x_{d+1},\ldots,x_n] ,$$

i.e. $k(\underline{\underline{x}})$ is obtained from $k(x_1,\ldots,x_d)$ by forming the polynomial ring in $x_{d+1},\ldots,x_n$.

Thus

$$1/f(\underline{\underline{x}}) = v(x_1,\ldots,x_n)/u(x_1,\ldots,x_d) ,$$

where $v(X_1,\ldots,X_n)$ and $u(X_1,\ldots,X_d)$ are polynomials. We have

$$u(x_1,\ldots,x_d) = f(\underline{\underline{x}})\ v(\underline{\underline{x}}) ,$$

which implies that

$$u(y_1,\ldots,y_d) = f(\underline{\underline{y}})\ v(\underline{\underline{y}}) ,$$

in view of $\underline{\underline{x}} \to \underline{\underline{y}}$. Now $y_1,\ldots,y_d$ are independent over k , whence $u(y_1,\ldots,y_d) \neq 0$, whence $f(\underline{\underline{y}}) \neq 0$. Our proof is complete.

The _dimension_ of a variety V is defined as the transcendence degree of any of its generic points. In view of Theorem 2A , there is no ambiguity. A variety of dimension 1 is called a _curve_, one of dimension $n - 1$ is called a _hypersurface_.

Example: Let us consider again the example of the linear manifold M^d . We constructed a generic point $(\xi_1,\ldots,\xi_n)$ with $k(\eta_1,\ldots,\eta_d) = k(\xi_1,\ldots,\xi_n)$, where $\eta_1,\ldots,\eta_d$ were algebraically independent. Thus tr. deg. $k(\xi_1,\ldots,\xi_n) = d$. Hence in the sense of our definition, M^d has dimension d . This agrees with the dimension d assigned to M^d in linear algebra.

THEOREM 2B. (i) _Let_ V _be a variety and let_ $\underline{\underline{x}} \in V$ _with tr. deg._ $\underline{\underline{x}} = \dim V$. _Then_ $\underline{\underline{x}}$ _is a generic point of_ V .

(ii) _If_ $W \subseteq V$ _are two varieties, and if_ $\dim W = \dim V$, _then_ $W = V$.

Proof: (i) Let $\underline{y}$ be a generic point of V. Then $\underline{y} \to \underline{x}$ and tr. deg. $\underline{x}$ = tr. deg. y. By Theorem 2A, $\underline{x} \leftrightarrow \underline{y}$, so that $\overline{(\underline{x})} = \overline{(\underline{y})} = V$.

(ii) Let $\underline{x}$ be a generic point of W. Now $\underline{x} \in V$, and tr. deg. $\underline{x} = \dim V$, so that by part (i), $\underline{x}$ is a generic point of V. Thus $\overline{(\underline{x})} = W = V$.

THEOREM 2C. (i) *If $f(\underline{X}) \in k[\underline{X}]$ is a non-constant irreducible polynomial, then the set of zeros of $f(\underline{X})$ is a hypersurface; that is, a variety of dimension $n-1$.*

(ii) *If S is a hypersurface, then $\mathfrak{J}(S)$ is a principal ideal (f), generated by some non-constant irreducible polynomial $f(\underline{X}) \in k[\underline{X}]$.*

Proof: (i) The principal ideal (f) is a prime ideal in $k[\underline{X}]$, so $A((f))$ is a variety. Without loss of generality, suppose X_n occurs in $f(\underline{X})$, say $f(\underline{X}) = X_n^a g_a(X_1,\ldots,X_{n-1}) + \ldots + g_0(X_1,\ldots,X_{n-1})$. Choose $x_1,\ldots,x_{n-1} \in \Omega$ algebraically independent over k. Choose $x_n \in \Omega$ with $f(x_1,\ldots,x_n) = 0$. Then $\underline{x} = (x_1,\ldots,x_n) \in A((f))$. Also, tr. deg. $\underline{x} = n-1$. Thus $\dim A((f)) \geq n-1$. On the other hand, $\dim A((f)) \neq n$, by Theorem 2B and since $A((f)) \neq \Omega^n$. Hence $\dim A((f)) = n-1$. In other words, $A((f))$ is a hypersurface.

(ii) If S is a hypersurface, then $\mathfrak{J}(S)$ is a prime ideal. Let $g(\underline{X}) \in \mathfrak{J}(S)$, $g \neq 0$. Since $\mathfrak{J}(S)$ is prime, there exists some irreducible factor f of g such that $f(\underline{X}) \in \mathfrak{J}(S)$. So $(f) \subseteq \mathfrak{J}(S)$, whence $A((f)) \supseteq A(\mathfrak{J}(S)) = S$. But $\dim A((f)) = n-1$ by part (i), and $\dim S = n-1$. Therefore by Theorem 2B, $A(f) = S$. Hence

$$\mathfrak{J}(S) = \mathfrak{J}(A(f)) = \sqrt{(f)} = (f),$$

since (f) is prime.

Examples: (1) Let $k = \mathbb{Q}$, $\Omega = \mathbb{C}$, $n = 2$ and $f(X,Y) = Y - X^2$. Now f is irreducible. So by Theorem 2C , the set of zeros of f is a hypersurface of dimension 1 . Since $n - 1 = 1$, it is also a curve. The point (e, e^2) has transcendence degree 1 and lies on our curve. Hence we see again that it is a generic point of our curve.

(2) Same as above, but with $f(X,Y) = X^2 + Y^2 - 1$. Again the set of zeros of f (namely the unit circle) is a hypersurface and also a curve.

Let t be transcendental and consider the point

$$\underline{\underline{x}} = (x_1, x_2) = \left(\frac{2t}{t^2+1} , \frac{t^2-1}{t^2+1}\right) .$$

Here $t = \frac{x_1}{1-x_2}$, whence $k(\underline{\underline{x}}) = k(t)$, so that $\underline{\underline{x}}$ has transcendence degree 1 . Since $\underline{\underline{x}}$ lies on our curve, it follows that $\underline{\underline{x}}$ is a generic point of the unit circle. In particular,

$$\left(\frac{2e}{e^2+1} , \frac{e^2-1}{e^2+1}\right)$$

is a generic point of the unit circle.

THEOREM 2D. *Let* $n = 1 + t$, *let* $f_1(X, Y_1)$, $f_2(X, Y_1, Y_2), \ldots, f_t(X, Y_1, Y_2, \ldots, Y_t)$ *be polynomials of the type*

$$f_i(X, Y_1, \ldots, Y_i) = Y_i^{d_i} - g_i(X, Y_1, \ldots, Y_i) ,$$

where $d_i > 0$ *and* g_i *is of degree* $< d_i$ *in* Y_i . *Let* $\mathfrak{Y}_1, \ldots, \mathfrak{Y}_t$ *be algebraic functions with* $f_1(X, \mathfrak{Y}_1) = \ldots = f_t(X, \mathfrak{Y}_1, \ldots, \mathfrak{Y}_t) = 0$, *and suppose that*

$$[k(X,\mathfrak{Y}_1,\dots,\mathfrak{Y}_t): k(X)] = d_1 d_2 \dots d_t .$$

<u>Then the equations</u>

$$f_1 = f_2 = \dots = f_t = 0$$

<u>define a curve; that is, a variety of dimension</u> 1 .

<u>Examples</u>: (1) Let k be a field whose characteristic does not equal 2 or 3 . Take $t = 2$, so that $n = 3$. Consider $f_1(X,Y_1) = Y_1^2 + X^2 - 1$, $f_2(X,Y_1Y_2) = Y_2^2 + X^2 - 4$. Then $\mathfrak{Y}_1^2 = 1 - X^2$, and $\mathfrak{Y}_2^2 = 4 - X^2$, or $\mathfrak{Y}_1 = \sqrt{1 - X^2}$ and $\mathfrak{Y}_2 = \sqrt{4 - X^2}$. Also,

(2.1) $$[k(X,\sqrt{1 - X^2}, \sqrt{4 - X^2}): k(X)] = 4 .^{\dagger)}$$

By Theorem 2D , the equations $f_1 = f_2 = 0$ define a curve. This curve is the intersection of two circular cylinders with radii 1,2 , whose axes intersect at right angles.

(2) Same as above, but with $f_2(X,Y_1,Y_2) = Y_2^2 + X^2 - 1$. In this case $[k(X,\mathfrak{Y}_1,\mathfrak{Y}_2): k(X)] = 2$. So Theorem 2D does not apply. In fact,

---

†) The proof of (2.1) is as follows. Since the characteristic is not 2 or 3 , the four polynomials $1 - X$, $1 + X$, $2 - X$, $2 + X$ are distinct and are irreducible. Hence none of $1 - X^2$, $4 - X^2$ and $(1 - X^2)/(4 - X^2)$ is a square in $k(X)$, and each of $\sqrt{1 - X^2}$, $\sqrt{4 - X^2}$, $\sqrt{(1 - X^2)/(4 - X^2)}$ is of degree 2 over $k(X)$. It will suffice to show that $\sqrt{4 - X^2} \notin k(X,\sqrt{1 - X^2})$. Suppose to the contrary that

$$\sqrt{4 - X^2} = r(X) + s(X)\sqrt{1 - X^2}$$

with rational functions $r(X)$, $s(X)$. We now square and observe that the factor in front of $\sqrt{1 - X^2}$ must be zero. Thus $2r(X)s(X) = 0$. If $r(X) = 0$, then $(1 - X^2)/(1 - X^4)$ would be a square in $k(X)$, which was ruled out. If $s(X) = 0$, then $4 - X^2$ would be a square, which was also ruled out.

The situation is similar to the one in Corollary 5B of Chapter II, §5, and the exercise below it.

$$A((f_1,f_2)) = V_1 \cup V_2 ,$$

where $V_1 = A((f_1, Y_1 - Y_2))$, $V_2 = A(f_1, Y_1 + Y_2))$.
Thus we do not obtain a variety. This algebraic set is the intersection of two circular cylinders of radius 1 whose axes intersect at right angles. Both V_1 and V_2 are the intersection of a plane with a circular cylinder; they are ellipses.

(3) Let $k = F_q$, the finite field of q elements. Take $t = 2$, $n = 3$ and $f_1(X,Y_1) = Y_1^d - f(X)$ where $d|(q-1)$, and $f_2(X,Y_2) = Y_2^q - Y_2 - g(X)$. Suppose f_1, f_2 to be irreducible. Then $\mathfrak{Y}_1, \mathfrak{Y}_2$ with $\mathfrak{Y}_1^d = f(X)$, $\mathfrak{Y}_2^q - \mathfrak{Y}_2 = g(X)$ have

$$[k(X,\mathfrak{Y}_1) : k(X)] = d \quad , \quad [k(X,\mathfrak{Y}_2) : k(X)] = q \quad .$$

Since $(d,q) = 1$, we have $[k(X,\mathfrak{Y}_1,\mathfrak{Y}_2) : k(X)] = dq$. Thus $f_1 = f_2 = 0$ defines a curve. In the same way one sees that if f_1, f_2 both are absolutely irreducible, then $f_1 = f_2 = 0$ is an absolute curve, i.e., a curve which is an <u>absolute</u> variety.

<u>Proof of Theorem 2D</u>: Pick $\underline{\underline{x}} = (x, y_1, \ldots, y_t) \in \Omega^n$, such that the mapping $X \to x$, $\mathfrak{Y}_i \to y_i$ $(1 \le i \le t)$ yields an isomorphism of $k(X,\mathfrak{Y}_1,\ldots,\mathfrak{Y}_t)$ to $k(x,y_1,\ldots,y_t)$. We claim that the set of zeros of $f_1 = f_2 = \cdots = f_t = 0$ is the variety $(\overline{\underline{\underline{x}}})$. It suffices to show that $\mathfrak{J}(\underline{\underline{x}}) = (f_1,\ldots,f_t)$; for then $(\overline{\underline{\underline{x}}}) = A(\mathfrak{J}(\underline{\underline{x}})) = A((f_1,\ldots,f_t))$. Clearly, every $f \in (f_1,\ldots,f_t)$ vanishes on $\underline{\underline{x}}$; so $(f_1,\ldots,f_t) \subseteq \mathfrak{J}(\underline{\underline{x}})$. Conversely, we are going to show that

(2.2) <u>if</u> $f(\underline{\underline{x}}) = 0$, <u>then</u> $f \in (f_1, \ldots, f_t)$.

We'll show (2.2) by induction on s, for functions $f = f(X,Y_1,\dots,Y_s)$ where $0 \leqq s \leqq t$. If $s = 0$, then $f(\underline{\underline{x}}) = 0$; but x is transcendental over k, so $f(X) = 0$, whence $f \in (f_1,\dots,f_t)$. Next, we show that if (2.2) is true for $s-1$, it is true for s. In $f(X,Y_1,\dots,Y_s)$, if $Y_s^{d_s}$ occurs, replace it by $g_s(X,Y_1,\dots,Y_s)$. Do this repeatedly, until you get a polynomial $\hat{f}(X,Y_1,\dots,Y_s)$ of degree $< d_s$ in Y_s. We observe that $f - \hat{f} \in (f_s)$, and that $\hat{f}(\underline{\underline{x}}) = 0$. Suppose

(2.3) $$\hat{f} = Y_s^{d_s-1} h_{d_s-1}(X,Y_1,\dots,Y_{s-1}) + \dots + h_0(X,Y_1,\dots,Y_{s-1}).$$

Our hypothesis implies that $[k(x,y_1,\dots,y_t): k(x)] = d_1 d_2 \dots d_t$, and we have

$$k(x) \subseteq k(x,y_1) \subseteq k(x,y_1,y_2) \subseteq \dots \subseteq k(x,y_1,\dots,y_t),$$

where for each i in $1 \le i \le t$, the field $k(x,y_1,\dots,y_i)$ is an extension of degree $\le d_i$ over $k(x,y_1,\dots,y_{i-1})$. Hence it is actually an extension of degree d_i. In particular, $[k(x,y_1,\dots,y_s): k(x,y_1,\dots,y_{s-1})] = d_s$. Since $\hat{f}(\underline{\underline{x}}) = 0$, we see from (2.3) that each $h_j(\underline{\underline{x}}) = 0$. So by induction, each $h_j \in (f_1,\dots,f_t)$, hence also $\hat{f} \in (f_1,\dots,f_t)$, and $f \in (f_1,\dots,f_t)$. The proof of (2.2) and therefore the proof of the theorem is complete.

§3. Rational Maps.

A <u>rational function</u> φ <u>on</u> Ω^n is an element of $k(X_1,\dots,X_n)$, i.e. of the form $\varphi = a(X_1,\dots,X_n)/b(X_1,\dots,X_n)$, where $a(X_1,\dots,X_n)$, $b(X_1,\dots,X_n)$ are polynomials over k. We may assume that a,b have no common factor.

We say a rational function φ is <u>defined</u> (or <u>regular</u>) at a point $\mathbf{x} \in \Omega^n$ if $b(\mathbf{x}) \neq 0$. If φ is defined at $\mathbf{x}$, put $\varphi(\mathbf{x}) = a(\mathbf{x})/b(\mathbf{x})$.

The rational functions φ which are defined at $\mathbf{x} \in \Omega^n$ form a ring consisting of all $a(\mathbf{X})/b(\mathbf{X})$ with $b(\mathbf{x}) \neq 0$. This ring is denoted as $\mathfrak{O}_{\mathbf{x}}$ and is called the <u>local ring</u> of $\mathbf{x}$. Let $\mathfrak{J}_{\mathbf{x}}$ consist of all $\varphi \in \mathfrak{O}_{\mathbf{x}}$ with $\varphi(\mathbf{x}) = 0$. (Thus $\mathfrak{J}_{\mathbf{x}}$ consists of all $a(\mathbf{X})/b(\mathbf{X})$ with $b(\mathbf{x}) \neq 0$, $a(\mathbf{x}) = 0$.) Then $\mathfrak{J}_{\mathbf{x}}$ is an ideal in $\mathfrak{O}_{\mathbf{x}}$.

<u>LEMMA 3A</u>. (i) <u>If</u> $\mathbf{x} \to \mathbf{y}$, <u>then</u> $\mathfrak{O}_{\mathbf{y}} \subseteq \mathfrak{O}_{\mathbf{x}}$.

(ii) <u>If</u> $\mathbf{x} \leftrightarrow \mathbf{y}$, <u>then</u> $\mathfrak{O}_{\mathbf{x}} = \mathfrak{O}_{\mathbf{y}}$ <u>and</u> $\mathfrak{J}_{\mathbf{x}} = \mathfrak{J}_{\mathbf{y}}$.

<u>Proof</u>: Obvious.

<u>THEOREM 3B</u>. (i) $\mathfrak{J}_{\mathbf{x}}$ <u>is a maximal ideal in</u> $\mathfrak{O}_{\mathbf{x}}$, <u>hence</u> $\mathfrak{O}_{\mathbf{x}}/\mathfrak{J}_{\mathbf{x}}$ <u>is a field (called the function field of</u> $\mathbf{x}$).

(ii) $\mathfrak{O}_{\mathbf{x}}/\mathfrak{J}_{\mathbf{x}}$ <u>is</u> k-<u>isomorphic to</u> $k(\mathbf{x})$.

<u>Proof</u>: (i) Let $\varphi \in \mathfrak{O}_{\mathbf{x}}$, $\varphi \notin \mathfrak{J}_{\mathbf{x}}$. Then $\varphi = a(\mathbf{X})/b(\mathbf{X})$, where $b(\mathbf{x}) \neq 0$ and $a(\mathbf{x}) \neq 0$, and therefore $\frac{1}{\varphi} = b(\mathbf{X})/a(\mathbf{X})$ lies in $\mathfrak{O}_{\mathbf{x}}$. Thus every $\varphi \in \mathfrak{O}_{\mathbf{x}}$ which does not lie in $\mathfrak{J}_{\mathbf{x}}$ is a unit. It follows that $\mathfrak{J}_{\mathbf{x}}$ is a maximal ideal.

(ii) The map $\omega\colon \mathfrak{O}_{\mathbf{x}} \to k(\mathbf{x})$ given by

$$\omega(a(\mathbf{X})/b(\mathbf{X})) = a(\mathbf{x})/b(\mathbf{x})$$

has image $k(\mathbf{x})$ and kernel $\mathfrak{J}_{\mathbf{x}}$. Therefore $k(\mathbf{x}) \cong \mathfrak{O}_{\mathbf{x}}/\mathfrak{J}_{\mathbf{x}}$.

We now come to the definition of a rational function defined on a variety V. The simplest definition to try would be that a rational function on V is the restriction to V of a rational function $\varphi(\underline{\underline{X}})$ on Ω^n. However, we want this rational function to be defined for at least some point of V. Hence by Lemma 3A it must be defined for every generic point $\underline{\underline{x}}$ of V, i.e. it must lie in $\mathfrak{O}_{\underline{\underline{x}}}$. Moreover, given two functions $a(\underline{\underline{X}})/b(\underline{\underline{X}})$ and $c(\underline{\underline{X}})/d(\underline{\underline{X}})$ in $\mathfrak{O}_{\underline{\underline{x}}}$, we should regard them as equal functions on V if their restrictions to V are equal. Clearly this is true precisely if their difference lies in $\mathfrak{J}_{\underline{\underline{x}}}$.

Thus we come to define a rational function on V as an element of $\mathfrak{O}_{\underline{\underline{x}}}/\mathfrak{J}_{\underline{\underline{x}}}$, where $\underline{\underline{x}}$ is a generic point. Clearly this is independent of the choice of the generic point. $\mathfrak{O}_{\underline{\underline{x}}} = \mathfrak{O}_V$ (say) consists of $a(\underline{\underline{X}})/b(\underline{\underline{X}})$ with $b(\underline{\underline{X}}) \notin \mathfrak{J}(V) = \mathfrak{J}(\underline{\underline{x}})$, and $\mathfrak{J}_{\underline{\underline{x}}} = \mathfrak{J}_V$ (say) consists of $a(\underline{\underline{X}})/b(\underline{\underline{X}})$ with $a(\underline{\underline{X}}) \in \mathfrak{J}(V)$, $b(\underline{\underline{X}}) \notin \mathfrak{J}(V)$. We say a function $r(\underline{\underline{X}}) \in k(\underline{\underline{X}})$ represents a rational function φ of V if $r(\underline{\underline{X}}) \in \mathfrak{O}_V$ and if $r(\underline{\underline{X}})$ lies in the class φ of $\mathfrak{O}_V/\mathfrak{J}_V$.

Example: Let $n = 2$, $k = \mathbb{Q}$, $\Omega = \mathbb{C}$, and V the circle $x_1^2 + x_2^2 - 1 = 0$. Let φ be the rational function represented by X_1/X_2. Then φ is also represented by $(X_1 + X_1^2 + X_2^2 - 1)/X_2$ and by $X_1/(X_2 + X_1^2 + X_2^2 - 1)$, for example.

The rational functions defined on V form a field, called the function field of V. This field is denoted $k(V)$. In view of Theorem 3B, the function field is k-isomorphic to $k(\underline{\underline{x}})$ where $\underline{\underline{x}}$ is any generic point of V.

Let $\psi_1^V, \ldots, \psi_n^V$ be the elements of $k(V)$ represented, respectively, by the polynomials $X_1, \ldots, X_n$. Then it is clear that

$$k(V) = k(\psi_1^V, \ldots, \psi_n^V) \quad .$$

It is easily seen that a polynomial $f(X_1,\ldots,X_n)$ has $f(\overset{V}{\psi}_1,\ldots,\overset{V}{\psi}_n) = 0$ if and only if $f \in \mathfrak{J}(V)$. Hence if $\underline{\underline{x}} = (x_1,\ldots,x_n)$ is a generic point, then there is a k-isomorphism $k(\underline{\underline{x}}) \to k(V)$ with $x_i \to \overset{V}{\psi}_i$ $(i = 1,\ldots,n)$.

<u>Example</u>: Let $n = 2$, $k = \mathbb{Q}$, $\Omega = \mathbb{C}$, and V the circle $x_1^2 + x_2^2 - 1 = 0$. We have seen in previous examples that if η is trancendental over $\mathbb{Q}$, then the point $\left(2\eta/(\eta^2+1), (\eta^2-1)/(\eta^2+1)\right)$ is a generic point for V . Clearly $k(\underline{\underline{x}}) = k(\eta) \cong k(X)$. Thus the function field of the circle is isomorphic to $k(X)$.

A curve is called <u>rational</u> if its function field is $\cong k(X)$. Thus the circle is a rational curve. It can be shown that $x_1^n + x_2^n - 1 = 0$ is not a rational curve if $n > 2$ and is not divisible by the characteristic. See Shafarevich (1969), p. 8 .

Let φ be a rational function on a variety $V = \overline{(\underline{\underline{x}})}$ and let $\underline{\underline{y}}$ be a point of V . We say that φ <u>is defined</u> at $\underline{\underline{y}}$ if there exists a representative $r(\underline{\underline{X}}) = a(\underline{\underline{X}})/b(\underline{\underline{X}})$ with $b(\underline{\underline{y}}) \neq 0$. If this is the case, set

$$\varphi(\underline{\underline{y}}) = a(\underline{\underline{y}})/b(\underline{\underline{y}}) .$$

We have to show that this independent of the representative. Suppose that φ is represented by both $a(\underline{\underline{X}})/b(\underline{\underline{X}})$ and by $\hat{a}(\underline{\underline{X}})/\hat{b}(\underline{\underline{X}})$, and that $b(\underline{\underline{y}}) \neq 0$, $\hat{b}(\underline{\underline{y}}) \neq 0$. The difference $(a\hat{b} - \hat{a}b)/(b\hat{b})$ represents the zero rational function on V . Hence $a(\underline{\underline{x}})\hat{b}(\underline{\underline{x}}) - \hat{a}(\underline{\underline{x}})b(\underline{\underline{x}}) = 0$, and since $\underline{\underline{x}} \to \underline{\underline{y}}$, we have $a(\underline{\underline{y}})\hat{b}(\underline{\underline{y}}) - \hat{a}(\underline{\underline{y}})b(\underline{\underline{y}}) = 0$. We conclude that $a(\underline{\underline{y}})/b(\underline{\underline{y}}) = \hat{a}(\underline{\underline{y}})/\hat{b}(\underline{\underline{y}})$.

Examples: (1) Let $n = 3$, $k = \mathbb{Q}$, $\Omega = \mathbb{C}$, and V the sphere $x_1^2 + x_2^2 + x_3^2 - 1 = 0$. Let φ be the rational function represented by $1 = 1/1$. Put $\underline{y} = (1,0,0)$. Now φ is defined at $\underline{y}$ and $\varphi(\underline{y}) = 1$. Now φ is also represented by $1/(X_1^2 + X_2^2 + X_3^2)$. Again the denominator does not vanish at $\underline{y}$. If we use this representation, we again find, as expected, that $\varphi(\underline{y}) = 1$. Finally φ is also represented by $(X_1 - X_1^2 - X_2^2 - X_3^2)/(X_1 - 1)$. This representative cannot be used to compute $\varphi(\underline{y})$, since its denominator vanishes at $\underline{y}$.

(2) Let n, k, Ω and V be as above. Let φ be the rational function represented by $1/X_3$. This function φ is certainly defined if $\underline{y} \in V$ and $y_3 \neq 0$. We ask if there is representative of φ which allows us to define $\varphi(\underline{y})$ for some $\underline{y}$ with $y_3 = 0$. Let $a(\underline{X})/b(\underline{X})$ be a representative. Then

$$\frac{1}{X_3} - \frac{a(\underline{X})}{b(\underline{X})} = \frac{b(\underline{X}) - X_3 a(\underline{X})}{X_3 b(\underline{X})}$$

vanishes on V. Thus $b(\underline{X}) - a(\underline{X})\,X_3 \in (X_1^2 + X_2^2 + X_3^2 - 1)$. So $b(\underline{X}) \in (X_3, X_1^2 + X_2^2 + X_3^2 - 1)$, and therefore $b(\underline{y}) = 0$, if $\underline{y} \in V$ and $y_3 = 0$. It follows that φ is defined precisely for those points $\underline{y}$ on the sphere which are not on the circle $y_3 = 0$, $y_1^2 + y_2^2 - 1 = 0$.

THEOREM 3C. *Let φ be a rational function on a variety V. The set of points $\underline{y} \in V$ for which φ is not defined is a proper* algebraic subset of V .

Proof: The set of points where φ is not defined is

$$S = V \cap \bigcap_{b(\underline{\underline{X}})} A((b(\underline{\underline{X}}))\quad ,$$

where the intersection is taken over all $b(\underline{\underline{X}})$ which occur as a denominator of a representative of φ . Since the intersection of an arbitrary number of algebraic sets is an algebraic set, S is an algebraic set. In addition, S is a proper subset of V , since a generic point of V is not in S .

Let φ be a rational function of a variety V , and let W be a subvariety of V . We say φ is defined on W if φ is defined at a generic point of W .

A rational map $\underline{\underline{\varphi}}$ from a variety V to Ω^m is defined simply as an m - tuple of rational functions $(\varphi_1,\ldots,\varphi_m)$. We say $\underline{\underline{\varphi}}$ is defined at $\underline{\underline{y}} \in V$, if each $\varphi_i(\underline{\underline{y}})$ is defined at $\underline{\underline{y}}$. If this is the case, put $\underline{\underline{\varphi}}(\underline{\underline{y}}) = (\varphi_1(\underline{\underline{y}}),\ldots,\varphi_n(\underline{\underline{y}}))$. The set of points $\underline{\underline{y}} \in V$ for which $\underline{\underline{\varphi}}$ is not defined is the union of the sets of points for which φ_i is not defined $(i = 1,\ldots,m)$. In view of Theorem 3C , and since a finite union of proper algebraic subsets of a variety is still a proper algebraic subset, the points where $\underline{\underline{\varphi}}$ is not defined are a proper algebraic subset of V .

The image of $\underline{\underline{\varphi}}$ is defined as the closure of the set of points $\underline{\underline{\varphi}}(\underline{\underline{y}})$, $\underline{\underline{y}} \in V_A$ for which $\underline{\underline{\varphi}}$ is defined.

THEOREM 3D. The image of $\underline{\underline{\varphi}}$ is a variety W . If $\underline{\underline{x}}$ is a generic point of V , then $\underline{\underline{\varphi}}(\underline{\underline{x}})$ is a generic point of W .

Proof: Let $V = (\underline{\underline{x}})$. If $\underline{\underline{x}} \to \underline{\underline{y}}$ and if $\underline{\underline{\varphi}}(\underline{\underline{y}})$ is defined, we have to show that $\underline{\underline{\varphi}}(\underline{\underline{x}}) \to \underline{\underline{\varphi}}(\underline{\underline{y}})$. Let $\underline{\underline{\varphi}} = (\varphi_1,\ldots,\varphi_m)$, and suppose that φ_i is represented by $a_i(\underline{\underline{X}})/b_i(\underline{\underline{X}})$ with $b_i(\underline{\underline{y}}) \neq 0$. Let $f(\underline{\underline{\varphi}}(\underline{\underline{x}})) = 0$, and suppose that $f(\underline{\underline{U}}) = f(U_1,\ldots,U_m)$ is of degree d_i in U_i . Put

$$g(U_1,\ldots,U_m, V_1,\ldots,V_m) = V_1^{d_1} \ldots V_m^{d_m} f\left(\frac{U_1}{V_1},\ldots,\frac{U_m}{V_m}\right) .$$

Since $f(a_1(\underline{\underline{x}})/b_1(\underline{\underline{x}}),\ldots,a_m(\underline{\underline{x}})/b_m(\underline{\underline{x}})) = 0$, it follows that $g(a_1(\underline{\underline{x}}),\ldots,a_m(\underline{\underline{x}}),b_1(\underline{\underline{x}}),\ldots,b_m(\underline{\underline{x}})) = 0$. But $\underline{\underline{x}} \to \underline{\underline{y}}$, so $g(a_1(\underline{\underline{y}}),\ldots,a_m(\underline{\underline{y}}),b_1(\underline{\underline{y}}),\ldots,b_m(\underline{\underline{y}})) = 0$, and

$$b_1(\underline{\underline{y}})^{d_1} \ldots b_m(\underline{\underline{y}})^{d_m} f\left(\frac{a_1(\underline{\underline{y}})}{b_1(\underline{\underline{y}})},\ldots,\frac{a_m(\underline{\underline{y}})}{b_m(\underline{\underline{y}})}\right) = 0 .$$

Since $b_1(\underline{\underline{y}})^{d_1} \ldots b_m(\underline{\underline{y}})^{d_m} \neq 0$, it follows that

$$f(\underline{\underline{\varphi}}(\underline{\underline{y}})) = f\left(\frac{a_1(\underline{\underline{y}})}{b_1(\underline{\underline{y}})},\ldots,\frac{a_m(\underline{\underline{y}})}{b_m(\underline{\underline{y}})}\right) = 0 .$$

So every polynomial f vanishing on $\underline{\underline{\varphi}}(\underline{\underline{x}})$ also vanishes on $\underline{\underline{\varphi}}(\underline{\underline{y}})$, and $\underline{\underline{\varphi}}(\underline{\underline{x}}) \to \underline{\underline{\varphi}}(\underline{\underline{y}})$.

Example: Let V be the sphere $x_1^2 + x_2^2 + x_3^2 = 1$, and let $\underline{\underline{\varphi}}: V \to \Omega^2$ have a representation as $\underline{\underline{\varphi}} = ((X_1^2 + X_2^2)/X_3^2 , -1/X_3^2)$. Let $\underline{\underline{\xi}} = (\xi_1,\xi_2,\xi_3)$ be a generic point of V . We have

$$\underline{\underline{\varphi}}(\underline{\underline{\xi}}) = \left(\frac{\xi_1^2 + \xi_2^2}{\xi_3^2} , -\frac{1}{\xi_3^2}\right) = \left(\frac{1}{\xi_3^2} - 1 , -\frac{1}{\xi_3^2}\right).$$

Thus $\varphi(\xi) = (\zeta_1, \zeta_2)$ satisfies $\zeta_1 + \zeta_2 + 1 = 0$. Since $\varphi(\xi)$ has transcendence degree 1, it is in fact a generic point of the line $z_1 + z_2 + 1 = 0$. Thus this line is the image of φ. But not every point on this line is of the type $\varphi(y)$. If (z_1, z_2) is on the line and is $\neq (-1,0)$, then if we pick y_1, y_2, y_3 in Ω with $y_3 = 1/\sqrt{z_2}$, $y_1^2 + y_2^2 + y_3^2 - 1 = 0$, we obtain $\varphi(y) = (z_1, z_2)$. But $(z_1, z_2) = (-1,0)$ is not of the type $\varphi(y)$. For if $y_3 \neq 0$, then $\varphi(y) \neq (-1,0)$, and if $y_3 = 0$, then $\varphi(y)$ is not defined.

THEOREM 3E. *Let φ be a rational map from V with image W. Let T be a proper algebraic subset of W. Then the set $L \subseteq V$ consisting of points y where either φ is not defined or where $\varphi(y) \in T$, is a proper algebraic subset of V.*

Proof: Suppose W and T lie in Ω^m. Suppose T is defined by equations $g_1(y) = \dots = g_t(y) = 0$, where $y = (y_1, \dots, y_m)$. Let $g_i(Y_1, \dots, Y_m)$ have degree d_{ij} in Y_j $(1 \leqq i \leqq t, 1 \leqq j \leqq m)$. Put

$$h_i(Y_1, \dots, Y_m, Z_1, \dots, Z_m) = Z^{d_{i1}} \dots Z^{d_{im}} g_i\left(\frac{Y_1}{Z_1}, \dots, \frac{Y_m}{Z_m}\right).$$

Let

$$r = r(X) = (a_1(X)/b_1(X), \dots, a_m(X)/b_m(X))$$

represent φ and put

$$\ell_i^{r}(X) = b_1(X) \dots b_m(X)\ h_i(a_1(X), \dots, a_m(X), b_1(X), \dots, b_m(X)) \quad (1 \leqq i \leqq t).$$

Let L_r consist of points y of V with

$$\ell_1^{r}(y) = \dots = \ell_t^{r}(y) = 0.$$

We claim that

$$(3.1) \qquad L = \cap L_{\underline{\underline{r}}} ,$$

with the intersection taken over all representations $\underline{\underline{r}}$ of $\underline{\underline{\varphi}}$. In fact if $\underline{\underline{y}} \notin L_{\underline{\underline{r}}}$ for some $\underline{\underline{r}}$, then some $\ell_i^{\underline{\underline{r}}}(\underline{\underline{y}}) \neq 0$, and hence $b_1(\underline{\underline{y}}_m) \ldots b_m(\underline{\underline{y}}) \neq 0$ and $g_i(a_1(\underline{\underline{y}})/b_1(\underline{\underline{y}}), \ldots, a_m(\underline{\underline{y}})/b_m(\underline{\underline{y}})) \neq 0$. So $\underline{\underline{\varphi}}(\underline{\underline{y}})$ is defined and $g_i(\underline{\underline{\varphi}}(\underline{\underline{y}})) \neq 0$, so that $\underline{\underline{\varphi}}(\underline{\underline{y}}) \notin T$ and $\underline{\underline{y}} \notin L$. On the other hand if $\underline{\underline{y}} \notin L$, then $\underline{\underline{\varphi}}(\underline{\underline{y}})$ is defined, and for some representation $\underline{\underline{r}}$ we have $b_1(\underline{\underline{y}}) \ldots b_m(\underline{\underline{y}}) \neq 0$. Moreover, $\underline{\underline{\varphi}}(\underline{\underline{y}}) \notin T$, whence some $g_i(\underline{\underline{\varphi}}(\underline{\underline{y}})) \neq 0$, and $\ell_i^{\underline{\underline{r}}}(\underline{\underline{y}}) \neq 0$. Thus $\underline{\underline{y}} \notin L_{\underline{\underline{r}}}$, and (3.1) is established.

In view of (3.1), L is an algebraic subset of V. Since a generic point of V lies outside each $L_{\underline{\underline{r}}}$, the set L is a proper algebraic subset.

<u>Example</u>. Let $V \subseteq \Omega^3$ be the sphere $x_1^2 + x_2^2 + x_3^2 - 1 = 0$ and let $W \subseteq \Omega^2$ be the line $z_1 + z_2 + 1 = 0$. We have seen above that the map $\underline{\underline{\varphi}}$ represented by $((X_1^2 + X_2^2)/X_3^2 , -1/X_3^2)$ has image W. Let $T \subseteq W$ consist of the single point $(0,-1)$. It is easily seen that the set L of points $\underline{\underline{y}}$ where $\underline{\underline{\varphi}}(\underline{\underline{y}})$ is not defined or where $\underline{\underline{\varphi}}(\underline{\underline{y}}) \in T$ consists of $\underline{\underline{y}} \in V$ with $y_3(y_3^2 - 1) = 0$.

4. Birational Maps.

We define a rational map from a variety V to a variety W as a rational map $\underline{\varphi}$ of V whose image is contained in W. We express this in symbols by $\underline{\varphi}$: $V \to W$.

Let $\underline{\varphi}: V \to W$ and $\underline{\psi}: W \to U$ be rational maps such that $\underline{\psi}$ is defined on the image of V under $\underline{\varphi}$. Thus if $\underline{x}$ is a generic point of V, then $\underline{\psi}$ is defined on $\underline{\varphi}(\underline{x})$. Suppose $V \subseteq \Omega^v$, $W \subseteq \Omega^w$, $U \subseteq \Omega^u$, and suppose $\underline{\varphi}$ is represented by

$$(4.1) \qquad (a_1(\underline{X})/b_1(\underline{X}), \ldots, a_w(\underline{X})/b_w(\underline{X})) ,$$

and $\underline{\psi}$ is represented by

$$(4.2) \qquad (c_1(\underline{Y})/d_1(\underline{Y}), \ldots, c_u(\underline{Y})/d_u(\underline{Y})) ,$$

where $d_1, \ldots, d_u$ are non-zero at $\underline{\varphi}(\underline{x})$. Let $\underline{\psi}\,\underline{\varphi}$ be the rational map $V \to U$ represented by

$$(4.3) \qquad (c_1(a_1(\underline{X})/b_1(\underline{X}), \ldots)/d_1(a_1(\underline{X})/b_1(\underline{X}), \ldots)), \ldots, c_u(\ldots)/d_u(\ldots)) .$$

Since $d_1, \ldots, d_u$ are not zero at $\underline{\varphi}(\underline{x})$, each of the u components in (4.3) lies in $\mathcal{O}_{\underline{x}}$, and $\underline{\psi}\,\underline{\varphi}(\underline{x})$ is defined and equals $\underline{\psi}(\underline{\varphi}(\underline{x}))$. It is clear that $\underline{\psi}\,\underline{\varphi}$ is independent of the special representations (4.1), (4.2) of $\underline{\varphi}$, $\underline{\psi}$, respectively. We call $\underline{\psi}\,\underline{\varphi}$ the composite of $\underline{\psi}$ and $\underline{\varphi}$. If $\underline{v}$ is a point of V such that $\underline{\varphi}$ is defined at $\underline{v}$ and $\underline{\psi}$ is defined at $\underline{\varphi}(\underline{v})$, then $\underline{\psi}\,\underline{\varphi}$ is defined at $\underline{v}$ and

$$\underline{\psi}\,\underline{\varphi}(\underline{v}) = \underline{\psi}(\underline{\varphi}(\underline{v})) .$$

But $\underline{\psi}\underline{\varphi}(\underline{v})$ may be defined although perhaps either $\underline{\varphi}(\underline{v})$ is not defined, or $\underline{\underline{\varphi}}(\underline{\underline{v}})$ is defined and $\underline{\underline{\psi}}(\underline{\underline{\varphi}}(\underline{\underline{v}}))$ is not defined.

Examples. (1) Let $V = \Omega^1$, $W = \Omega^2$, $U = V = \Omega^1$. Further let $\underline{\underline{\varphi}}: V \to W$ be represented by (X^2, X), and let $\underline{\underline{\psi}}: W \to V$ be represented by X_1/X_2. Then $\underline{\underline{\psi}}\,\underline{\underline{\varphi}}$ is the identity map on V. Thus $\underline{\underline{\psi}}\,\underline{\underline{\varphi}}$ is defined on 0 and $\underline{\underline{\psi}}\,\underline{\underline{\varphi}}(0) = 0$. However $\underline{\underline{\varphi}}(0) = (0,0)$, and $\underline{\underline{\psi}}$ is not defined at $(0,0)$.

(2) Let $k = \mathbb{Q}$ and $\Omega = \mathbb{C}$. Let $V = \Omega^1$, W the unit circle $x_1^2 + x_2^2 - 1 = 0$, and $U = V = \Omega^1$. Further let $\underline{\underline{\varphi}}: V \to W$ be represented by $(2X/(X^2+1), (X^2-1)/(X^2+1))$, and let $\underline{\underline{\psi}}: W \to V$ be represented by $X_1/(1-X_2)$. Then $\underline{\underline{\psi}}\,\underline{\underline{\varphi}}$ is the identity map on V and $\underline{\underline{\varphi}}\,\underline{\underline{\psi}}$ is the identity map on W. In particular, $\underline{\underline{\psi}}\,\underline{\underline{\varphi}}$ is defined at i and $\underline{\underline{\psi}}\,\underline{\underline{\varphi}}(i) = i$, but $\underline{\underline{\varphi}}$ is not defined at i.

Exercise. Show that in Example (2), $\underline{\underline{\varphi}}$ is defined for every point of V except for i, $-i$, and that $\underline{\underline{\psi}}$ is defined for every point of W except for $(0,1)$. Further show that every point of V with the exception of $i, -i$ is of the type $\underline{\underline{\psi}}(\underline{\underline{y}})$ with $\underline{\underline{y}} \in W$, and every point of W with the exception of $(0,1)$ is of the type $\underline{\underline{\varphi}}(\underline{\underline{x}})$ with $\underline{\underline{x}} \in V$. Hence if V' is obtained from V by deleting i, $-i$ and W' is obtained from W by deleting $(0,1)$, then $\underline{\underline{\varphi}}$ and $\underline{\underline{\psi}}$ provide a 1-1 correspondence between points of V' and of W'.

A rational map $\underline{\underline{\varphi}}: V \to W$ is called a bi-rational map (or a bi-rational correspondence) if there exists a rational map $\underline{\underline{\psi}}: W \to V$ such that $\underline{\underline{\psi}}\,\underline{\underline{\varphi}}$ is the identity on V and $\underline{\underline{\varphi}}\,\underline{\underline{\psi}}$ is the identity on W. Two varieties are bi-rationally equivalent if there exists a bi-rational correspondence between them. We denote this by $V \cong W$. This is an equivalence relation of varieties. (Note that this relation is defined in terms of the ground field k).

THEOREM 4A. Let φ be a bi-rational map from V to W with inverse ψ. Then there exist proper algebraic subsets L of V and M of W, such that on the set theoretic differences $V \sim L$ and $W \sim M$, the maps φ and ψ are defined everywhere and are inverses of each other.

Proof: Let S be the subset of V where φ is not defined. Let T be the subset of W where ψ is not defined. Let L be the subset of V where either φ is not defined or where $\varphi(x) \in T$. Similarly, let M be the subset of W where either ψ is not defined or where $\psi(x) \in S$. In view of Theorem 3E, the sets L, M are proper algebraic subsets of V, W, respectively. Now φ is defined on $V \sim L$. Clearly, if $x \in V \sim L$, then $\varphi(x) \notin T$. So $\psi(\varphi(x))$ is defined; but then $\psi(\varphi(x)) = x$. From this it follows that $\varphi(x) \in W \sim M$, since $x \notin S$. So the restriction of φ to $V \sim L$ maps $V \sim L$ into $W \sim M$. The restriction of ψ to $W \sim M$ maps $W \sim M$ into $V \sim L$. These maps are inverses of each other.

THEOREM 4B. Let V and W be varieties. Then $V \cong W$ if and only if their function fields are k-isomorphic.

Proof: If x is a generic point of V and y is a generic point of W, then the function fields are isomorphic to $k(x)$ and $k(y)$, respectively. So we need to show that $V \cong W$ if and only if $k(x)$ is isomorphic to $k(y)$.

Suppose that $V \cong W$. Let $\underline{\underline{\varphi}}: V \to W$ and $\underline{\underline{\psi}}: W \to V$ be bi-rational maps, such that $\underline{\underline{\varphi}}\underline{\underline{\psi}}$ and $\underline{\underline{\psi}}\underline{\underline{\varphi}}$ are the identity maps on W and V , respectively.

It is clear from Theorem 4A that the "image" of V under $\underline{\underline{\varphi}}$ is W . Thus if $\underline{\underline{x}}$ is a generic point of V , then by Theorem 3D the point $\underline{\underline{y}} = \underline{\underline{\varphi}}(\underline{\underline{x}})$ is a generic point of W . We have $\underline{\underline{y}} = \underline{\underline{\varphi}}(\underline{\underline{x}})$ and $\underline{\underline{x}} = \underline{\underline{\psi}}(\underline{\underline{y}})$, whence $k(\underline{\underline{y}}) \subseteq k(\underline{\underline{y}})$ and $k(\underline{\underline{x}}) \subseteq k(\underline{\underline{y}})$, whence $k(\underline{\underline{x}}) = k(\underline{\underline{y}})$. Thus the function fields are certainly k - isomorphic.

Conversely, let $k(\underline{\underline{x}})$ be isomorphic to $k(\underline{\underline{y}})$, where $\underline{\underline{x}} = (x_1 \dots, x_n), \underline{\underline{y}} = (y_1, \dots, y_m)$ are generic points of V , W respectively. Let α be a k - isomorphism from $k(\underline{\underline{x}})$ to $k(\underline{\underline{y}})$. Let $\alpha(x_i) = x_i'$ $(i = 1, \dots, n)$ and put $\underline{\underline{x}}' = (x_1', \dots, x_n')$. Then $k(\underline{\underline{x}}') = k(\underline{\underline{y}})$ and $\underline{\underline{x}}'$ is again a generic point of V . Thus we may suppose that $k(\underline{\underline{x}}) = k(\underline{\underline{y}})$. Suppose that

$$y_i = r_i(\underline{\underline{x}}) \qquad (i = 1, \dots, m)$$

and

$$x_j = s_j(\underline{\underline{y}}) \qquad (j = 1, \dots, n)$$

for certain rational functions $r_1, \dots, r_m$ and $s_1, \dots, s_n$. Then $\underline{\underline{\varphi}}: V \to W$ represented by $(r_1(\underline{\underline{X}}), \dots, r_m(\underline{\underline{X}}))$ and $\underline{\underline{\psi}}: W \to V$ represented by $(s_1(\underline{\underline{Y}}), \dots, s_n(\underline{\underline{Y}}))$ are rational maps which are inverses of each other.

In §3 we defined a rational curve as one whose function field is isomorphic to $k(X)$. In view of Theorem 4B , we may also define a rational curve as a curve which is birationally equivalent to Ω^1 .

LEMMA 4C. The following two conditions on a field k are equivalent.

(i). Either char $k = 0$, or char $k = p > 0$ and for every $a \in k$ there is a $b \in k$ with $b^p = a$.

(ii). <u>Every algebraic extension of</u> k <u>is separable.</u>

<u>Proof.</u> We clearly may suppose that char $k = p > 0$.

(i) → (ii). A polynomial of $k[X]$ of the type

$$a_0 + a_1X^p + \dots + a_tX^{tp} \tag{4.4}$$

equals $(b_0 + b_1X + \dots + b_tX^t)^p$ where $b_i^p = a_i$ $(i = 0, \dots, t)$. Thus an irreducible polynomial over k is not of the type (4.4), hence is separable.

(ii) → (i). Suppose there is an $a \in k$ not of the type $a = b^p$ with $b \in k$. Then there is a b which is not in k but in an algebraic extension of k, with $a = b^p$. Since p is a prime, it is easily seen that $i = p$ is the smallest positive exponent with $b^i \in k$. The polynomial $X^p - a = (X - b)^p$ has proper factors $(X - b)^i$ with $1 \leqq i \leqq p - 1$, but none of these factors lies in $k[X]$ since $b^i \notin k$. Thus $X^p - a$ is irreducible over k , and b is inseparable over k .

A field with the properties of the lemma is called <u>perfect.</u> A Galois field is perfect. For if a lies in the finite field F_q with $q = p^\nu$ elements, then $a = a^q = \left(a^{p^{\nu-1}}\right)^p$.

<u>THEOREM 4D.</u> <u>Suppose</u> V <u>is a variety defined over a perfect ground field</u> k . <u>Then</u> V <u>is birationally equivalent to a hypersurface.</u>

<u>Proof.</u> Suppose $\dim V = d$ and $\underline{x} = (x_1, \dots, x_n)$ is a generic point of V . Then $n \geqq d$. In view of Theorem 4B it will suffice to show that there is a $\underline{y} = (y_1, \dots, y_{d+1})$ with

(4.5) $$k(\underline{\underline{x}}) = k(\underline{\underline{y}}) .$$

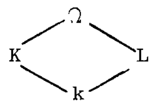
We shall show this by induction on $n-d$. If $n-d = 0$, set $y_1 = x_1, \ldots, y_d = x_d$, $y_{d+1} = 0$. If $n-d = 1$, set $\underline{\underline{y}} = \underline{\underline{x}}$. Suppose now that $n-d > 1$ and that our claim is true for smaller values of $n-d$. We may suppose without loss of generality that $x_1, \ldots, x_{d+1}$ have transcendence degree d over k. Then $(x_1, \ldots, x_{d+1})$ is the generic point of a hypersurface in Ω^{d+1}. This hypersurface is defined by an equation $f(z_1, \ldots, z_{d+1}) = 0$ where $f(Z_1, \ldots, Z_{d+1})$ is irreducible over k. Since k is perfect, it is clear that f is not a polynomial in $Z_1^p, \ldots, Z_{d+1}^p$ if char $k = p > 0$. We may then suppose without loss of generality that f is not a polynomial in $Z_1, \ldots, Z_d, Z_{d+1}^p$. Thus f is separable in the variable Z_{d+1}, and x_{d+1} is separable algebraic over $k(x_1, \ldots, x_d)$. By the theorem of the primitive element (see Van der Waerden, §43), there is an x' with

$$k(x_1, \ldots, x_d, x_{d+1}, x_{d+2}) = k(x_1, \ldots, x_d, x').$$

Thus $\underline{\underline{x}}' = (x_1, \ldots, x_d, x', x_{d+3}, \ldots, x_n)$ has $k(\underline{\underline{x}}') = k(\underline{\underline{x}})$. By induction hypothesis there is a $\underline{\underline{y}} \in \Omega^{d+1}$ with $k(\underline{\underline{x}}') = k(\underline{\underline{y}})$, hence with (4.5).

5. Linear Disjointness of Fields

LEMMA 5A: *Suppose that* Ω , K , L , k *are fields with* $k \subseteq K \subseteq \Omega$, $k \subseteq L \subseteq \Omega$:



The following two properties are equivalent:

(i) *If elements* $x_1,\dots,x_m$ *of* K *are linearly independent over* k , *then they are also linearly independent over* L .

(ii) *If elements* $y_1,\dots,y_n$ *of* L *are linearly independent over* k , *then they are also linearly independent over* K .

Proof: By symmetry it is sufficient to show that (i) implies (ii). Let $y_1,\dots,y_n$ of L be linearly independent over k . Let $x_1,\dots,x_n$ of K be not all zero. We want to show that

(5.1) $$x_1y_1 + \dots + x_ny_n \neq 0 .$$

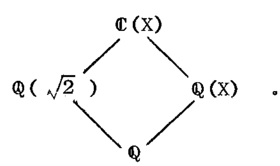
Let d be the maximum number of $x_1,\dots,x_n$ which are linearly independent over k . Without loss of generality, we may assume that $x_1,\dots,x_d$ are linearly independent over k . Thus for $d < i \leqq n$ we have $x_i = \sum_{j=1}^{d} c_{ij} x_j$, where $c_{ij} \in k$. We obtain

$$x_1y_1 + \dots + x_ny_n = \left(y_1 + \sum_{i=d+1}^{n} c_{i1}\, y_i\right) x_1 + \dots + \left(y_d + \sum_{i=d+1}^{n} c_{id}\, y_i\right) x_d .$$

Here $x_1, \ldots, x_d \in K$ are linearly independent over k , whence linearly independent over K . Their coefficients are not zero since $y_1, \ldots, y_n$ are linearly independent over k . Thus (5.1) follows.

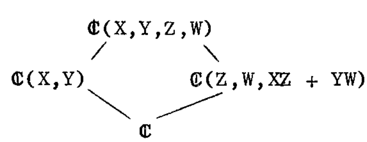
We say that field extensions K , L of k are *linearly disjoint over* $\underline{k}$, if properties (i) and (ii) hold.

Examples: (i) Consider the fields



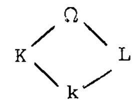
Here $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(X)$ are linearly disjoint over $\mathbb{Q}$. For if $(a + b\sqrt{2})$ and $c + d\sqrt{2})$ are linearly independent over $\mathbb{Q}$, then clearly they are linearly independent over $\mathbb{Q}(X)$.

(ii) Let X,Y,Z,W be variables, and consider the fields



In this case $\mathbb{C}(X,Y)$ and $\mathbb{C}(Z,W,XZ + YW)$ are not linearly disjoint over $\mathbb{C}$. For $Z, W, XZ + YW$ are linearly dependent over $\mathbb{C}(X,Y)$, but are linearly independent over $\mathbb{C}$.

LEMMA 5B: Let us consider fields

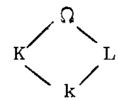


,

where L *is the quotient field of a ring* R . *For linear disjointness it is sufficient to show that if* $z_1,\ldots,z_n \in R$ *are linearly independent over* k , *then they are also linearly independent over* K .

Proof: Let $y_1,\ldots,y_n \in L$ be linearly independent over k . We can find a $z \neq 0$, $z \in R$, such that $zy_1,\ldots,zy_n \in R$. Now $zy_1,\ldots,zy_n$ are linearly independent over k, hence also linearly independent over K . Therefore $y_1,\ldots,y_n$ are linearly independent over K .

LEMMA 5C: Suppose we have fields



,

where K *is algebraic over* k . *Let* KL *be the set of expressions* $x_1 y_1 + \ldots + x_n y_n$ *with* $x_i \in K$, $y_i \in L$ *for* $1 \leq i \leq n$, *and with* n *arbitrary*.

(i) *The set* KL *is a field, it contains* K *and* L , *and is the smallest such field.*

(ii) *Suppose that* $[K : k]$ *is finite. Then* $[KL : L] \leqq [K : k]$, *with equality precisely if* K , L *are linearly disjoint over* k .

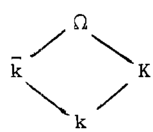
(iii) *Now suppose that* K , L *are linearly disjoint over* k . *Let* α *be a* k-*isomorphism from* K *to a field* H *containing* k . *Let* β *be a* k-*isomorphism from* L *to* H . *Then*

$$x_1 y_1 + \ldots + x_n y_n \to \alpha(x_1)\beta(y_1) + \ldots + \alpha(x_n)\beta(y_n)$$

is a well-defined map from KL *to* H . *It is a* k-*isomorphism into* H .

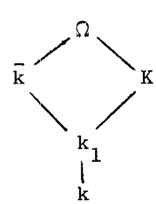
Proof: Exercise.

LEMMA 5D. *Suppose we have a diagram of fields and subfields*



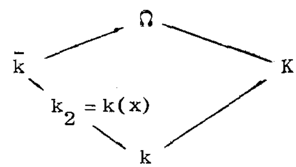
where k *is perfect and* $\bar{k}$ *is the algebraic closure of* k . *Then* K , $\bar{k}$ *are linearly disjoint over* k *if and only if* k *is algebraically closed in* K.

Proof: If k is not algebraically closed in K , then there exists a proper algebraic extension k_1 of k with $k_1 \subseteq K$;



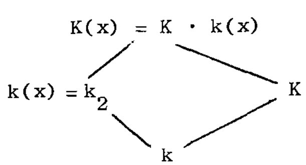
It is now clear that $\bar{k}$ and K cannot be linearly disjoint over k .

Conversely, suppose that k is algebraically closed in K. It suffices to show that k_2, K are linearly disjoint over k, where k_2 is any finite algebraic extension of k. Since k is perfect, $k_2 = k(x)$, and we have the following diagram of fields:



If $f(X)$ is the defining polynomial of x over k, then it remains irreducible over K, since every proper factor of $f(X)$ has coefficients which are algebraic over k, with some coefficients not in k, and hence not in K.

So for the fields



we have $[K\cdot k(x) : K] = [k(x) : k]$; hence $k(x), K$ are linearly disjoint over k by Lemma 5C.

6. Constant Field Extensions

Consider fields k, K, Ω, such that $k \subseteq K \subseteq \Omega$, and Ω is algebraically closed and has infinite transcendence degree over K. If $\underline{x} \in \Omega^n$, then $\mathfrak{J}_k(\underline{x})$† is the ideal of all polynomials $f(\underline{X}) \in k[\underline{X}]$ with $f(\underline{x}) = 0$. We have seen in §1 that $\mathfrak{J}_k(\underline{x}) = \mathfrak{p}$ is a

† Given a subset $M \subseteq \Omega^n$, we write $\mathfrak{J}_k(M)$ or $\mathfrak{J}_K(M)$ for the set of polynomials $f(\underline{X})$ in $k[\underline{X}]$ or $K[\underline{X}]$, respectively, which vanish on M.

prime ideal in $k[\underline{\underline{X}}]$. Similarly, $\mathfrak{I}_K(\underline{\underline{X}}) = \mathfrak{P}$ is a prime ideal in $K[\underline{\underline{X}}]$. Let $\mathfrak{g}K[\underline{\underline{X}}]$ be the ideal in $K[\underline{\underline{X}}]$ generated by $\mathfrak{g}$. The ideal $\mathfrak{g}K[\underline{\underline{X}}]$ consists of all linear combinations $c_1 f_1 + \dots + c_m f_m$, where $c_i \in K$, $f_i \in \mathfrak{g}$ $(i = 1,\dots,m)$. Clearly $\mathfrak{g}K[\underline{\underline{X}}] \subseteq \mathfrak{P}$. Denote the closure of a point $\underline{\underline{x}}$ with respect to k, K by $(\overline{\underline{\underline{x}}})^k$, $(\overline{\underline{\underline{x}}})^K$, respectively. We have $(\overline{\underline{\underline{x}}})^k = A(\mathfrak{g}) = A(\mathfrak{g}K[\underline{\underline{X}}]) \supseteq A(\mathfrak{P}) = (\overline{\underline{\underline{x}}})^K$. So

$$(\overline{\underline{\underline{x}}})^K \subseteq (\overline{\underline{\underline{x}}})^k .$$

<u>Example</u>: Let $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$, $\Omega = \mathbb{C}$, and $n = 2$. Consider the point $(e\sqrt{2}, e) = \underline{\underline{x}}$. Then $(\overline{\underline{\underline{x}}})^k$ is the set of zeros of the polynomial $X^2 - 2Y^2$. But $(\overline{\underline{\underline{x}}})^K$ is the set of zeros of $X - \sqrt{2}\,Y$.

THEOREM 6A. <u>Let $k \subseteq K \subseteq \Omega$ be fields, where Ω is algebraically closed and has infinite transcendence degree over K. Let $\underline{\underline{x}} \in \Omega^n$, $\mathfrak{I}_k(\underline{\underline{x}}) = \mathfrak{g}$, $\mathfrak{I}_K(\underline{\underline{x}}) = \mathfrak{P}$. Consider the following four properties:</u>

(i) <u>The fields K, $k(\underline{\underline{x}})$ are linearly disjoint extensions of k</u>,

(ii) $\mathfrak{P} = \mathfrak{g}K[\underline{\underline{X}}]$,

(iii) $(\overline{\underline{\underline{x}}})^k = (\overline{\underline{\underline{x}}})^K$,

(iv) $\mathfrak{P} = \sqrt{\mathfrak{g}K[\underline{\underline{X}}]}$.

<u>The properties (i), (ii) are equivalent. Property (ii) implies property (iii), which in turn implies property (iv).</u>

<u>Proof</u>: To show that (i) implies (ii), let $f(\underline{\underline{X}}) \in \mathfrak{P}$. Write $f(\underline{\underline{X}}) = \sum_{i=1}^{n} a_i f_i(\underline{\underline{X}})$, where $a_i \in K$, $f_i(\underline{\underline{X}}) \in k[\underline{\underline{X}}]$, and $a_1,\dots,a_n$ are linearly independent over k. Now $f(\underline{\underline{x}}) = 0$, so $\sum_{i=1}^{n} a_i f_i(\underline{\underline{x}}) = 0$.

By the linear disjointness of K and $k(\underline{\underline{x}})$, the a_i's are linearly independent over $k(\underline{\underline{x}})$. It follows that each $f_i(\underline{\underline{x}}) = 0$, and each $f_i(\underline{\underline{X}}) \in \mathcal{Y}$. Thus $f(\underline{\underline{X}}) \in \mathcal{Y}K[\underline{\underline{X}}]$.

To show that (ii) implies (i), let $u_1(\underline{\underline{X}}),\ldots,u_\ell(\underline{\underline{X}})$ be elements of $k[\underline{\underline{X}}]$, such that $u_1(\underline{\underline{x}}),\ldots,u_\ell(\underline{\underline{x}})$ are linearly independent over k. By Lemma 5B, it will suffice to show that $u_1(\underline{\underline{x}}),\ldots,u_\ell(\underline{\underline{x}})$ remain linearly independent over K. Suppose $a_1u_1(\underline{\underline{x}}) + \ldots + a_\ell u_\ell(\underline{\underline{x}}) = 0$, with $a_i \in K$. Let $f(\underline{\underline{X}}) = a_1u_1(\underline{\underline{X}}) + \ldots + a_\ell u_\ell(\underline{\underline{X}})$. Since $f(\underline{\underline{x}}) = 0$, the polynomial $f(\underline{\underline{X}})$ lies in $\mathfrak{N} = \mathcal{Y}K[\underline{\underline{X}}]$. We have a relation

$$a_1u_1(\underline{\underline{X}}) + \ldots + a_\ell u_\ell(\underline{\underline{X}}) = b_1f_1(\underline{\underline{X}}) + \ldots + b_mf_m(\underline{\underline{X}}) , \tag{6.1}$$

where $b_i \in K$, $f_i(\underline{\underline{X}}) \in \mathcal{Y}$ $(i = 1,\ldots,m)$. We may assume that $f_1,\ldots,f_m$ are linearly independent over k. We claim that $u_1(\underline{\underline{X}}),\ldots,u_\ell(\underline{\underline{X}})$, $f_1(\underline{\underline{X}}),\ldots,f_m(\underline{\underline{X}})$ are linearly independent over k. Suppose that

$$\sum_{i=1}^{\ell} c_iu_i(\underline{\underline{X}}) + \sum_{j=1}^{m} d_jf_j(\underline{\underline{X}}) = 0 , \tag{6.2}$$

where c_i, $d_j \in k$. Substituting $\underline{\underline{x}}$ for $\underline{\underline{X}}$, we obtain $\sum_{i=1}^{\ell} c_iu_i(\underline{\underline{x}}) = 0$. However, the $u_i(\underline{\underline{x}})$ are linearly independent over k, so that $c_1,\ldots,c_\ell$ are all zero. Thus (6.2) reduces to $\sum_{j=1}^{m} d_jf_j(\underline{\underline{X}}) = 0$. But the $f_j(\underline{\underline{X}})$ are linearly independent over k, and hence $d_1 = \ldots = d_m = 0$. We have established the linear independence of $u_1(\underline{\underline{X}}),\ldots,u_\ell(\underline{\underline{X}})$, $f_1(\underline{\underline{X}}),\ldots,f_m(\underline{\underline{X}})$ over k. These $\ell + m$ polynomials have coefficients in k and are linearly independent over k, and hence they are also linearly independent over

K^t . Hence in (6.1), all the coefficients are zero, and in particular $a_1 = \dots = a_\ell = 0$.

We next want to show that (ii) implies (iii). Let $\underline{\underline{y}} \in \overline{(\underline{\underline{x}})}^k$. Then $f(\underline{\underline{y}}) = 0$ if $f(\underline{\underline{X}}) \in \mathfrak{g}$. Since $\mathfrak{P} = \mathfrak{g}\, k[\underline{\underline{X}}]$, we have $g(\underline{\underline{y}}) = 0$ for every $g(\underline{\underline{X}}) \in \mathfrak{P}$. Thus $\underline{\underline{y}} \in A(\mathfrak{P}) = \overline{(\underline{\underline{x}})}^K$. Hence $\overline{(\underline{\underline{x}})}^k \subseteq \overline{(\underline{\underline{x}})}^K$, and since the reversed relation is always true, we obtain (iii).

Finally, we are going to show that (iii) implies (iv). Suppose $f(\underline{\underline{X}}) \in \mathfrak{N}$. Then f vanishes on $\overline{(\underline{\underline{x}})}^K = \overline{(\underline{\underline{x}})}^k$, and $f \in \mathfrak{J}_K(\underline{\underline{x}}) = \mathfrak{J}_K(\overline{(\underline{\underline{x}})}^k) = \mathfrak{J}_K(A(\mathfrak{g}K[\underline{\underline{X}}])) = \sqrt{\mathfrak{g}\, K[\underline{\underline{X}}]}$. So $\mathfrak{N} \subseteq \sqrt{\mathfrak{g}\, K[X]}$. Conversely, we have $\mathfrak{g}\, K[\underline{\underline{X}}] \subseteq \mathfrak{P}$, whence $\sqrt{\mathfrak{g}\, K[\underline{\underline{X}}]} \subseteq \sqrt{\mathfrak{N}} = \mathfrak{N}$.

<u>Example</u>: We give an example where $\overline{(\underline{\underline{x}})}^K = \overline{(\underline{\underline{x}})}^k$, but $\mathfrak{P} \neq \mathfrak{g}\, K[\underline{\underline{X}}]$. Thus (iii) does not imply (ii). Let k_0 be a field of characteristic p , and let $k = k_0(z)$, where z is transcendental over k_0 . Put $\underline{\underline{x}} = (t, t\sqrt[p]{z})$, where t is transcendental over k . Then $\mathfrak{g} = \mathfrak{J}_k(\underline{\underline{x}}) = (zX_1^p - X_2^p)$, since $zX_1^p - X_2^p$ is an irreducible polynomial over k . Now take $K = k(\sqrt[p]{z})$. Then $\mathfrak{N} = \mathfrak{J}_K(\underline{\underline{x}}) = (\sqrt[p]{z}\, X_1 - X_2)$, and $\mathfrak{N} \neq \mathfrak{g}\, K[\underline{\underline{X}}]$. We have $\overline{(\underline{\underline{x}})}^k = A((zX_1^p - X_2^p))$ and $\overline{(\underline{\underline{x}})}^K = A((\sqrt[p]{z}\, X_1 - X_2))$. We observe that $\overline{(\underline{\underline{x}})}^k = \overline{(\underline{\underline{x}})}^K$, since if $(u,v) \in A((zX_1^p - X_2^p))$, then $zu^p - v^p = (\sqrt[p]{z}\, u - v)^p = 0$, so that $(u,v) \in A((\sqrt[p]{z}\, X_1 - X_2))$.

<u>THEOREM 6B. Let</u> k , K , $\underline{\underline{x}}$, $\mathfrak{g}$, $\mathfrak{N}$ <u>be as in Theorem 6A. Suppose, moreover, that</u> K <u>is a separable algebraic extension of</u> k . <u>Then</u> $\sqrt{\mathfrak{g}\, K[\underline{\underline{X}}]} = \mathfrak{g}\, K[\underline{\underline{X}}]$.

---

† Linearly independent vectors in a vector space k^t over k remain linearly independent in the vector space K^t , where K is an over-field of k .

<u>Proof</u>: Let $f \in \sqrt{\mathfrak{y}\, K[\underline{X}]}$. There is a field K_0 with $k \subseteq K_0 \subseteq K$ which is finitely generated over k , such that $f \in K_0[\underline{X}]$ and $f \in \sqrt{\mathfrak{y}\, K_0[\underline{X}]}$. Let $f = \sum_{i=1}^{n} c_i f_i$, where $f_i(\underline{X}) \in k[\underline{X}]$, $c_i \in K_0$, and $c_1, \ldots, c_n$ are linearly independent over k . In fact, by allowing some f_i to be zero, we may suppose that $c_1, \ldots, c_n$ are a basis for K_0 over k , where $n = [K_0 : k]$. There are n distinct k-isomorphisms σ of K_0 into Ω ; write c^σ for the image of c under σ . We put

$$f^\sigma(\underline{X}) = \sum_{i=1}^{n} c_i^{\sigma} f_i(\underline{X}) .$$

Here the (n×n)-determinant $|c_i^\sigma|$ is not zero, and hence there are $d_i^{(\sigma)}$ such that

$$f_i(\underline{X}) = \sum_{\sigma} d_i^{(\sigma)} f^\sigma(\underline{X}) \qquad (i = 1, \ldots, n).$$

Now for some m , $f^m \in \mathfrak{y}\, K_0[\underline{X}]$, whence $(f^\sigma)^m \in \mathfrak{y}\, K_0^\sigma[X]$, whence $(f^\sigma)^m(\underline{x}) = 0$, and therefore $f^\sigma(\underline{x}) = 0$ for each σ . Thus each $f_i(\underline{x}) = 0$, and $f_i \in \mathfrak{y}$. We have shown that $f \in \mathfrak{y}\, K_0[\underline{X}] \subseteq \mathfrak{y}\, K[\underline{X}]$.

It follows from Theorems 6A, 6B, that the four properties listed in Theorem 6A are equivalent if K is a separable algebraic extension of k . Now if k is perfect, then every algebraic extension K of k is separable. Thus we obtain

<u>COROLLARY 6C</u>. <u>If</u> k <u>is perfect and if</u> V <u>is a variety over</u> k <u>with generic point</u> $\underline{x}$, <u>then</u> V <u>is an absolute variety if and only</u>

if $k(\underline{x})$ *and* k *are linearly disjoint over* k *. This is the case if and only if* k *is algebraically closed in* $k(\underline{x})$.*)

THEOREM 6D. Let k *be a perfect ground field.*

(i) *If* $f(\underline{X}) \in k[\underline{X}]$ *is not constant and is absolutely irreducible, then the set of zeros of* f *is an absolute hypersurface.*

(ii) *If* S *is an absolute hypersurface, then* $\mathfrak{J}_k(S) = (f)_k$†, *where* f *is absolutely irreducible and nonconstant.*

Proof: (i) This follows directly from Theorem 2C, and the fact that f is absolutely irreducible.

(ii) From Theorem 2C it follows that $\mathfrak{J}_k(S) = (f)_k$, where f is nonconstant and irreducible over k . Let K be an algebraic extension of k . Then $\mathfrak{J}_K(S) = \mathfrak{P} = \mathfrak{p}K[\underline{X}] = (f)_k K[\underline{X}] = (f)_K$. Thus the principal ideal generated by f in $K[\underline{X}]$ is a prime ideal, and f is irreducible over K .

REMARKS (1). Let k be perfect and let V be a variety over k . In Theorem 4D we constructed a hypersurface S which was birationally equivalent to V . In fact, the construction was such that $k(\underline{x}) = k(\underline{y})$, where $\underline{x}$, $\underline{y}$ were certain generic points of V , S , respectively. Now if V is an absolute variety, then k is algebraically

† We write $(f)_k$ resp. $(f)_K$ for the principal ideal generated by f in $k[\underline{X}]$ and in $K[\underline{X}]$.

*) Compare with Theorem 3A of Ch. V.

closed in $k(\underline{\underline{x}}) = k(\underline{\underline{y}})$, and S is *also an absolute variety*.

(2) Another approach to Corollary 6C is this: It may be shown directly that if two k-varieties are k-birationally equivalent, and if one is absolute, then so is the other. Thus the proof may be reduced to the case of a hypersurface. But this case is essentially Theorem 3A of Ch. V.

7. Counting Points in Varieties Over Finite Fields

The goal of this section is a proof of

THEOREM 7A. *Let* V *be an absolute variety of dimension* d *defined over* $k = F_q$. *Let* $N_\nu = N_\nu(V)$ *be the number of points* $\underline{\underline{y}} = (y_1, \ldots, y_n)$ *in* V *with each coordinate in* F_{q^ν} . *Then as* $\nu \to \infty$,

$$N_\nu = q^{\nu d} + O\left(q^{\nu(d - 1/2)}\right) . \tag{7.1}$$

The proof will depend on a result we derived in Chapter V. Namely, if $f(X_1, \ldots, X_n) \in F_q[X_1, \ldots, X_n]$ is nonconstant and absolutely irreducible and if N is the number of zeros of f in F_q , then

$$|N - q^{n-1}| \le cq^{n - 3/2} , \tag{7.2}$$

where c is a constant which depends on n and the total degree of f . For $n = 2$, this result is Theorem 1A of Chapter III, and for general n it is Theorem 5A of Chapter V. Only the case $n = 2$ is needed if V is a curve.

LEMMA 7B: Theorem 7A is true for hypersurfaces.

Proof: Let S be an absolute hypersurface of dimension d. By Theorem 6D, S is given by $f(\underline{\underline{x}}) = 0$, where $f(\underline{\underline{X}})$ is not constant and is absolutely irreducible. Thus by (7.2),

$$|N - q^d| = |N - q^{n-1}| \leq cq^{n-(3/2)} = cq^{d - 1/2} .$$

Now applying this result to F_{q^ν} instead of F_q, we see that $|N_\nu - q^{\nu d}| \leq cq^{\nu(d - 1/2)}$.

Theorem 7A for the general variety is done by induction on d. If $d = 0$ and $V = (\overline{\underline{\underline{x}}})$, then every $z \in F_q(\underline{\underline{x}})$ is algebraic over F_q, and so satisfies an equation $1 \cdot z - \alpha \cdot 1 = 0$ where $\alpha \in \overline{F}_q$. Thus z, 1 are linearly dependent over $\overline{F}_q$. Since $F_q(\underline{\underline{x}})$ and $\overline{F}_q$ are linearly disjoint over F_q, it follows that z, 1 are linearly dependent over F_q. So $z \in F_q$, and $F_q(\underline{\underline{x}}) = F_q$. Thus $\underline{\underline{x}}$ has coordinates in F_q, and $V = (\overline{\underline{\underline{x}}}) = \underline{\underline{x}}$. It follows that $N_\nu = 1$ for every ν.

In order to do the induction step from $d - 1$ to d, we shall need

LEMMA 7C. Suppose Theorem 7A is true for absolute varieties of dimension $< d$. Let W be a variety of dimension $< d$, not necessarily an absolute variety. Then as $\nu \to \infty$,

$$N_\nu(W) = O\left(q^{\nu(d-1)}\right) .$$

Proof: It is clear that W is still an algebraic set over $K = \overline{F}_q$, but not necessarily a K-variety. So W is a finite union $W = W_1 \cup \ldots \cup W_t$, where the W_i are K-varieties. Each W_i is defined by finitely many equations. The coefficients of all these equations for $W_1,\dots,W_t$ generate a finite extension F_{q^μ} of F_q. So each W_i is a F_{q^μ}-variety and is as such an absolute variety, and $d_i = \dim W_i \le d - 1$. Let $N_{\lambda\mu}(W_i)$ be the number of points in W_i with coordinates in $F_{q^{\lambda\mu}}$. By our induction hypothesis, applied to F_{q^μ} instead of F_q, we see that as the integer λ tends to ∞, we have

$$N_{\lambda\mu}(W_i) = q^{\lambda\mu(d_i-1)} + O\left(q^{\lambda\mu(d_i - 3/2)}\right)$$

$$= O\left(q^{\lambda\mu(d-1)}\right) .$$

Thus $N_{\lambda\mu}(W) = O\left(q^{\lambda\mu(d-1)}\right)$ as $\lambda \to \infty$. Given ν, pick an integer λ with $(\lambda - 1)\mu < \nu \le \lambda\mu$. Then as $\nu \to \infty$,

$$N_\nu(W) \le N_{\lambda\mu}(W) = O\left(q^{\lambda\mu(d-1)}\right)$$

$$= O\left(q^{\nu(d-1) + \mu(d-1)}\right)$$

$$= O\left(q^{\nu(d-1)}\right) .$$

The proof of Theorem 7A is now completed as follows. According to Theorem 4D, the variety V is birationally equivalent to a hypersurface S, and this hypersurface is an absolute variety by the remark at the end of §6. By Theorem 4A, there exist proper algebraic subsets $L \subseteq V$, $M \subseteq S$, such that the birational correspondence $\underline{\underline{\omega}}$ between V and S becomes a $1 - 1$ correspondence between points of $V \sim L$ and of $S \sim M$. Now $\underline{\underline{\omega}}$ as well as its inverse is defined over $k = F_q$, i.e. is defined in terms of rational functions with coefficients in F_q. Thus in this correspondence, points with components in F_q correspond to points with components in F_q.

More generally, points with components in F_{q^ν} correspond to points with components in F_{q^ν}. Hence

(7.3) $$|N_\nu(V) - N_\nu(S)| \leq N_\nu(L) + N_\nu(M) .$$

However, L and M are composed of varieties of dimension $< d$. So by Lemma 7C, $N_\nu(L) + N_\nu(M) = O\left(q^{\nu(d-1)}\right)$. On the other hand, by Lemma 7B, $N_\nu(S) = q^{\nu d} + O\left(q^{\nu(d - 1/2)}\right)$. These relations in conjunction with (7.3) yield (7.1).

REMARKS. (i) Theorem 7A together with Theorem 2D shows that the number N_ν of solutions $(x, y_1,\ldots,y_t) \in F_{q^\nu}^{t+1}$ of certain systems of equations

$$y_1^{d_1} = g_1(x) , \quad y_2^{d_2} = g_2(x,y_1) ,\ldots, \quad y_t^{d_t} = g_t(x, y_1,\ldots, y_t)$$

satisfies $N_\nu = q^\nu + O(q^{\nu/2})$ as $\nu \to \infty$. In particular this holds for certain systems of equations

$$y_1^{d_1} = g_1(x),\ldots, y_t^{d_t} = g_t(x) .$$

But a better result for such systems was already derived in Theorem 5A of Chapter II. Under suitable conditions on $g_1(X),\ldots,g_t(X)$ it was shown that $|N_\nu - q^\nu| \leqq cq^{\nu/2}$, where c was a constant explicitly determined in terms of t and the degrees of the polynomials $g_1,\ldots,g_t$.

(ii) More generally, if V is an absolute variety defined over F_q determined by equations $f_1(\underline{\underline{x}}) = \cdots = f_\ell(\underline{\underline{x}}) = 0$, then our Theorem 7A could be strengthened to

$$|N_\nu - q^{\nu d}| \leqq cq^{\nu(d - 1/2)} ,$$

where c is a constant depending only on the number n of variables, on ℓ, and on the total degrees of the polynomials $f_1,\dots,f_t$.

(iii) Corollary 2B of Chapter V can be generalized as follows. Suppose V is an absolute variety of dimension d over $\mathbb{Q}$ defined by equations $f_1(\underline{\underline{x}}) = \dots = f_\ell(\underline{\underline{x}}) = 0$, where $f_1(\underline{\underline{X}}),\dots,f_\ell(\underline{\underline{X}})$ have rational integer coefficients. Let $\overline{f}_i(\underline{\underline{X}})$ be obtained from $f_i(\underline{\underline{X}})$ by reduction modulo p and let V_p be the algebraic set defined over F_p by $\overline{f}_1(\underline{\underline{x}}) = \dots = \overline{f}_\ell(\underline{\underline{x}}) = 0$. Then if $p > p_0$, the set V_p is an absolute variety of dimension d. Here p_0 depends only on n, ℓ and the degrees of the polynomials $f_1,\dots,f_\ell$. Hence if $p > p_0$, then the number $N(p)$ of solutions of the system of congruences

$$f_1(\underline{\underline{x}}) \equiv \dots \equiv f_\ell(\underline{\underline{x}}) \equiv 0 \pmod{p}$$

satisfies $|N(p) - p^d| \leqq cp^{d - 1/2}$.

(iv) The Weil (1949) conjectures (see also Ch. IV, §6) imply much better estimates than Theorem 7A if V is a "non-singular" variety of dimension $d > 1$. These conjectures were recently proved by Deligne

+) But see the remark in the Preface.