TOPICS IN ALGEBRAIC GEOMETRY

by

T. P. M. Taylor

A dissertation submitted to the University of Glasgow in fulfilment of the requirements for the Degree of Master of Science.

SUMMARY

The dissertation begins in Chapter I with the basic properties of an algebraic variety. The Hilbert Nullstellensatz and its important consequences are then given; the proofs of the results on dimension are greatly simplified by appealing to a result of the next chapter.

In Chapter II, the length of a primary ideal is first discussed, preparatory to the ideas of height and depth of prime ideals. The fundamental equivalence between height and depth, and rank and dimension in a finite integral domain, is the last main theorem of this chapter.

The simple point on a variety is discussed in Chapter III from a local - algebraic point of view. It is shown that simplicity corresponds to regularity of the local ring, as defined by W. Krull. Finally the Jacobian criterion for a simple point of a variety is established, and we mention the extension to algebraic subvarieties.

PREFACE

The first chapter of this dissertation lays the foundations of algebraic geometry, with emphasis on the Hilbert Nullstellensatz. Making use of a chain condition established in Chapter II, we then give new proofs of some consequences for algebraic varieties.

In the second chapter we discuss the dimension theory of ideals and finite integral domains. A simplified proof of Property 2 of §3 is given.

By following O. Zariski in "The concept of a simple point on an abstract algebraic variety" ([4] see references), we close the third chapter with the classical criterion for simplicity in the seperable case.

My thanks are due to Dr. A. Geddes of the department, who supervised the work.

T. P. M. TAYLOR, 1965.

CONTENTS

CHAPTER I

ALGEBRAIC VARIETIES

§1. Notation.

We work with a fixed field k, called the ground field and a given integer n. If we denote by S^k the algebraic closure of k, then the set of ordered n-tuples of elements in S^k form a vector space over k (with usual componentwise addition and scalar multiplication). A vector $\alpha = (\alpha_1, \ldots, \alpha_n): \alpha_i \in S^k$ is called a point of the space S_n^k (S_n for short).

The polynomial ring in n variables $X_1, \ldots, X_n$ over the field k will be written $k[X_1, \ldots, X_n]$ or $k[\underline{X}]$; 'polynomials' will belong to this ring unless otherwise stated. By the Hilbert Basis Theorem, any ideal in $k[\underline{X}]$ has a finite basis.

§2. The Algebraic Variety.

Let $\{f_\lambda : \lambda \in \Lambda\}$ be a set of polynomials in $k[\underline{X}]$. The points in S_n which are zeros of f_λ for all $\lambda \in \Lambda$ constitute the <u>variety</u> defined by $\{f_\lambda\}$.

The polynomials f_λ generate an ideal A in $k[\underline{X}]$ and it is clear that the variety defined by $\{f : f \in A\}$ is the same as that defined by $\{f_\lambda\}$. Now the ideal A has a finite basis $(f_1, \ldots, f_r)$ and so the variety $V(A)$ is just the set of points which are simultaneous zeros of $f_1, \ldots, f_r$. We have shown that a given variety is the variety of an ideal, and as such is definable by a <u>finite</u> number of polynomials.

Suppose M is a variety, then we write $I(M)$ for the set of all polynomials vanishing at every point of M:

$$I(M) = \{f : f \in k[\underline{X}] : f(M) = 0\}$$

It is easy to check that $I(M)$ is an ideal containing A, where $M = V(A)$. If we now consider the variety $V(I(M))$ defined by this ideal then we get

THEOREM 2.1. $\quad V(I(M)) = M = V(A)$

<u>Proof</u>. Let $x \in$ L.H.S. then x is a zero of all polynomials which vanish on all zeros of A; in particular x is a zero of A. Thus $x \in$ R.H.S.

Let $x \in$ R.H.S. then x is a zero of A so x is a zero of all polynomials which vanish on all zeros (e.g. x) of A. Thus $x \in$ L.H.S.

However the parallel result $I(V(A)) = A$ is not always valid:

in the next section we shall see when this holds. Before doing this we introduce the idea of irreducibility.

DEFINITION. A variety V is <u>irreducible</u> if it is not the proper union of two smaller varieties V_1 and V_2.

THEOREM 2.2. <u>A variety V is irreducible if and only if the ideal $I(V)$ is prime.</u>

<u>Proof.</u> Let V be reducible i.e. $V = V_1 \cup V_2$, $V_1 \neq V$, $V_2 \neq V$. Then $V_1 \subset V$ implies that $I(V) \subset I(V_1)$ for if $I(V) = I(V_1)$ then $V(I(V)) = V(I(V_1))$ i.e. $V = V$ by Theorem 2.1, contradiction. Choose $f_1 \in I(V_1)$ but $\notin I(V)$; similarly there exists $f_2 \in I(V_2) - I(V)$. Now $f_1 f_2 \in I(V)$ showing that $I(V)$ is not prime.

Conversely let $I(V)$ be not prime; we show $V = V(A)$ is reducible. There are f_1 and f_2 such that $f_1 f_2 \in I(V)$, $f_1 \notin I(V)$, $f_2 \notin I(V)$. Put $V_1 = V(A + (f_1))$ and $V_2 = V(A + (f_2))$. Then we have $V_1 \subset V$ and $V_2 \subset V$; for suppose, for example, that $V_1 = V$, then $I(V_1) = I(V)$ but $f_1 \in I(V_1)$; contradiction.

If $x \in V_1 \cup V_2$ i.e. $x \in V_1$ say, then $x \in V$. On the other hand $x \in V$ implies $f_1(x) f_2(x) = 0$ so that either $f_1(x) = 0$ or $f_2(x) = 0$; hence $x \in V_1 \cup V_2$. Therefore $V = V_1 \cup V_2$ and is not irreducible.

THEOREM 2.3. <u>Every variety V can be expressed as a finite union of irreducible varieties.</u>

<u>Proof.</u> We suppose the contrary, that at least one variety exists which does not admit the above representation. The set T of all these varieties is non-empty, and the corresponding set $\sum$ of ideals given by $\sum = \left\{ I(V) : V \in T \right\}$ has a maximal ideal $I(V^*)$ by the noetherian property of $k[\underline{X}]$, see [5] I. p199. By Theorem 2.1 the variety V^* must be minimal in T.

Now V^* is reducible ($V^* \in T$) so let $V^* = V_1 \cup V_2$ where $V_1 \subset V^*$ and $V_2 \subset V^*$. As neither V_1 nor V_2 is in T, it follows that V_1 and V_2 both are finite unions of irreducible varieties; hence $V^* = V_1 \cup V_2$ is too - a contradiction.

COROLLARY. <u>The representation is unique</u> (provided no member of the union contains another).

<u>Proof.</u> Let $V = V_1 \cup \dots \cup V_s = V_1^* \cup \dots \cup V_t^*$ be two representations, so that V_i and V_j^* are irreducible.

We have $V_1 = \bigcup\limits_{j=1}^{t} (V_j^* \cap V_1)$, thus $V_1 = V_j^* \cap V_1$ for some j, i.e. $V_1 \subseteq V_j^*$. Similarly $V_j^* \subseteq V_i$ for some $i \in (1, \dots, s)$. But then $V_1 \subseteq V_j^* \subseteq V_i$ and so in fact $V_1 = V_j^* = V_i$. Hence the representations are unique to within ordering of the components.

§3. The Hilbert Nullstellensatz.

The question arises when does an ideal have an algebraic zero? We give the answer in the following theorem called the weak form of the Hilbert Nullstellensatz.

THEOREM 3.1. *The variety $V(A)$ is non-empty if and only if the ideal A is not the whole ring $k[\underline{X}]$.*

Proof. 1. Suppose $V(A)$ is non-empty, then $\alpha \in V(A)$ is a zero of every polynomial in A, so $1 \notin A$.

2. Let A be an ideal different from $k[\underline{X}]$ then $A \subseteq P$, a maximal ideal. The residue class ring $k[X]/P = k[\xi_1, \ldots, \xi_n]$, where $\xi_i = X_i + P$, is therefore a field, which we denote by F.

We require to show $\xi_1, \ldots, \xi_n$ are algebraic over k. For $n = 1$ the result is obvious. Now $F = k[\xi_1, \ldots, \xi_n] = k(\xi_1)[\xi_2, \ldots, \xi_n]$ and if we make the induction assumption for $n - 1$, then $\xi_2, \ldots, \xi_n$ are algebraic over $k(\xi_1)$. It remains to prove ξ_1 algebraic over k.

Now there exists a polynomial $p(X_1)$ with $p(\xi_1) \neq 0$ such that $p(\xi_1)\xi_i$ is integral over $k[\xi_1]$, for $2 \leq i \leq n$. It follows that for any element $f(\xi_1, \ldots, \xi_n)$ of F, $[p(\xi_1)]^\rho f(\xi_1, \ldots, \xi_n)$ is integral over $k[\xi_1]$ (ρ a positive integer). In particular, any element of $k(\xi_1)$ has this property. If we had ξ_1 transcendental over k, then $k[\xi_1]$ would be integrally closed in $k(\xi_1)$, which gives us that any element of $k(\xi_1)$ can be expressed as a quotient $\dfrac{g(\xi_1)}{[p(\xi_1)]^\rho}$, a contradiction. The proof is now complete.

By using a device due to Rabinowitsch (see [5] Vol II, pages 164-165), or alternatively see [2] p 33), we can deduce

THEOREM 3.2. <u>The Hilbert Nullstellensatz.</u>

<u>Let</u> $f \in k[\underline{X}]$ <u>vanish at all common zeros of</u> $f_1, \ldots, f_s$. <u>Then there exists an integer</u> r <u>such that</u> $f^r \in (f_1, \ldots, f_s)$.

COROLLARY 1. $I(V(A)) = \text{rad } A$.

<u>Proof.</u> Let $f \in \text{rad } A$, then $f^r \in A$ i.e. f^r and hence f vanish on $V(A)$, as $k[\underline{X}]$ is an integral domain; i.e. $f \in I(V(A))$.

On the other hand, $f \in I(V(A))$ i.e. f vanishes on all zeros of A implies, by the theorem, that $f^r \in A$, or $f \in \text{rad } A$.

COROLLARY 2. $I(V(A)) = A$ <u>if and only if</u> $A = \text{rad } A$.

COROLLARY 3. $V(A) = V(\text{rad } A)$.

COROLLARY 4. $V(A) = V(B)$ <u>if and only if</u> $\text{rad } A = \text{rad } B$.

COROLLARY 5. <u>The correspondence</u> $V \leftrightarrow I(V)$ <u>is a one-one mapping between proper irreducible varieties and proper prime ideals.</u>

§4. Dimension of an Irreducible Variety.

Let V be an irreducible variety, then $P = I(V)$ is a prime ideal and the integral domain $k[X]/P$ we call the coordinate ring $R[V]$ of V. As we saw this is equal to $k[\xi_1, \dots, \xi_n]$ where ξ_i is the P-residue of X_i. The degree of transcendence of $R[V]$ (strictly speaking of the quotient field of $R[V]$) over k is therefore an integer r: $0 \leq r \leq n$ which we define to be the dimension of V: we put $\dim V = r$.

The n-tuple $(\xi_1, \dots, \xi_n)$ may be considered as a point of K^n, where K is the universal extension field of k. $\xi = (\xi_1, \dots, \xi_n)$ is then called a generic point of V, and has the property: $f \in I(V) \Leftrightarrow f(\xi) = 0$.

The following theorems can be proved directly from the definition of dimension, but we shall make use of a result to be proved in the next chapter.

PROPOSITION. *V has dimension r if and only if there exists a maximal chain*

$$V_0 \subset \dots \subset V_r = V$$

of irreducible varieties, and no such chain is longer.

Proof. This follows from Corollary 5 to the Hilbert Nullstellensatz, and Chapter II Theorem 3.2.

THEOREM 4.2. *Let V_1 and V_2 be (irreducible) varieties such that $V_1 \subseteq V_2$, then $V_1 = V_2$ if and only if $\dim V_1 = \dim V_2$.*

Proof. Obvious from the proposition.

THEOREM 4.3. *A variety has dimension n if and only if it is the whole space S_n.*

Proof. $S_n = V((0))$ and $I(S_n) = \mathrm{rad}(0) = (0)$ as (0) is prime.

The domain $k[\underline{X}]/(0)$ has degree of transcendence n; this is $\dim S_n$ by definition.

Conversely no proper subvariety of S_n can have dimension n, by the proposition.

THEOREM 4.4. <u>An irreducible variety has dimension $n-1$ if and only if it is the variety of a principal ideal generated by an irreducible polynomial.</u>

<u>Proof.</u> $\dim V = n - 1$

$\Leftrightarrow$ V is a maximal proper variety (Theorems 4.2 and 4.3)

$\Leftrightarrow$ $I(V)$ is a minimal proper prime ideal (Corollary 5)

$\Leftrightarrow$ $I(V)$ is generated by a single irreducible polynomial. (since $k[\underline{X}]$ is a unique factorisation domain, and see [5] Vol I page 149, example 2).

THEOREM 4.5. <u>A variety of dimension 0 has only a finite number of points.</u>

<u>Proof.</u> Let V have dimension 0. Choose a fixed point α in V. Then there are only a finite number of points $\beta, \gamma, \ldots$ in S_n such that $f(\alpha) = 0 \Leftrightarrow f(\beta) = 0$ for any $f \in k[\underline{X}]$. [This can be shown by induction: in the case $n = 1$, the points $\alpha, \beta, \ldots$ are just conjugates]. Now these points belong to V, for let $g \in A$ where $V = V(A)$. Then $g(\beta) = 0$ since $g(\alpha) = 0$; i.e. $\beta \in V$. Also these points form the variety V_α defined by $V\{f : f \in k[\underline{X}] : f(\alpha) = 0\}$. V_α is a finite irreducible subvariety of V, and so must equal V by the proposition, since $\dim V = 0$.

CHAPTER II

DIMENSION

§1. The Length of a Primary Ideal.

Let Q be a P-primary ideal (in a ring R) and Q_i a sequence of primary ideals satisfying

$$Q = Q_1 \subset Q_2 \subset \dots \subset Q_{n-1} \subset Q_n = P. \tag{1a}$$

Such a sequence is called a (primary) chain from Q to P. A chain $Q'_1, \dots, Q'_m$ is said to be a refinement of the given chain $Q_1, \dots, Q_n$ if every Q_i appears among the Q'_j. Moreover, the refinement is proper if $m > n$. When a chain from Q to P has no proper refinements we call it a composition series for Q.

Our aim in this section is to show that any chain from Q to P may be refined to a composition series, the length l of this series depending only on Q. Having established this result we can then make the following definition:

The length of a primary ideal Q is the number of terms in any composition series for Q.

As we make use only of the case R an integral domain, we assume below that R_s is the usual local ring associated with a prime ideal: if R is not an integral domain then the generalised ring of quotients can be used instead.

There is a one-one correspondence between P-primary ideals Q_i such that $Q \subseteq Q_i \subseteq P$ and P'-primary ideals Q'_i in the local ring R_s, where $s = R - P$, such that $Q' \subseteq Q'_i \subseteq P'$. Thus to any primary chain $Q'_1, \dots, Q'_n$ corresponds a primary chain $Q_1, \dots, Q_n$

and a composition series for Q' likewise corresponds to a composition series for Q. Now in the ring R_S the ideal P' is maximal, so our problem is reduced to the case in which the chain terminates in a <u>maximal</u> prime ideal.

Assuming then that P is maximal in R, any ideal A between Q and P will be P-primary, for $P^r \subseteq Q \subseteq A \subseteq P$. Thus a composition series for Q is now a maximal chain of ideals from Q to P.

A further simplification can be made by passing over to the residue ring R/Q, where a chain of ideals from (0) to P/Q corresponds to a chain from Q to P in R. Since P is maximal and a minimal prime ideal of Q, P/Q is the <u>only</u> proper prime ideal in R/Q. A noetherian ring having unique proper prime ideal is called a <u>primary</u> ring.

THEOREM 1. <u>There exists a maximal chain (of length l, say) from (0) to P in a primary ring R. No chain from (0) to P has length greater than l.</u>

Proof. (i) Suppose $P^{n+1} = A_1 \subset \dots \subset A_r = P^n$ is a chain from P^{n+1} to P^n. We find a bound for the length of this chain by noticing that the residue ring P^n/P^{n+1} may be regarded as a vector space over R/P if we put

$$r + P \cdot v + P^{n+1} = rv + P^{n+1}. \quad (r \in R,\ v \in P^n)$$

This vector space has finite dimension (d, say) since P^n is finitely generated. Now the ideal residues A_i/P^{n+1} form a sequence of subspaces of increasing dimension; hence $r \leq d + 1$.

To construct a maximal chain of ideals from P^{n+1} to P^n, take vector subspaces of all dimensions 0, 1, ..., d and the corresponding ideals will do.

There being no other proper prime ideal than P (in R), the ideal (0) is P-primary and so $P^k = (0)$ for some integer k. The join of the maximal chains from P^k to P^{k-1}, from P^{k-1} to P^{k-2}, ..., and from P^2 to P clearly gives a maximal chain from (0) to P.

(ii) Let $(0) = A_0 \subset \ldots \subset A_l = P$ be a maximal chain. If $(0) = B_0 \subset \ldots \subset B_r = P$ then we prove $r \leq l$.

For some integer t $(1 \leq t \leq r-1)$, $A_1 \subseteq B_{t+1}$ but $A_1 \nsubseteq B_t$ and we deduce

$$A_1 + B_0 \subset A_1 + B_1 \subset \ldots \subset A_1 + B_t.$$

[An element $x \in B_{i+1}$: $x \notin B_i \Rightarrow x \notin A_1 + B_i$. For $x = a_1 + b_i$ $\Rightarrow a_1 = x - b_i \in A_1 \cap B_{i+1} = 0$ since A_1 minimal]

The sequence (0), $A_1 + B_0$, $A_1 + B_1$, ..., $A_1 + B_r$ must therefore contain a chain of length $r+1$, equality only being possible at $A_1 + B_t$, $A_1 + B_{t+1}$.

Consider now the sequence (0), A_2/A_1, ..., A_l/A_1 which is a maximal chain in R/A_1. Applying the above argument to this primary ring, we see that there exists a chain of length at least r from (0) to A_l/A_1 beginning (0), A_2/A_1, ... It follows that there is a chain (0), A_1, A_2, ..., P in R of length at least $r+1$. By considering the rings R/A_2, R/A_3 etc. we get a chain (0), A_1, ..., A_l; ..., P in R of length at least $r+1$; this can only be the maximal chain $(0) \subset A_1 \subset \ldots \subset A_l$ and thus $r \leq l$.

COROLLARY 1. <u>Any two maximal chains have the same length.</u>

For neither can be longer than the other.

COROLLARY 2. *Any chain from (0) to P may be refined to a maximal chain, which has fixed bounded length.*

In terms of primary chains in a noetherian ring R these corollaries show

THEOREM 1'. *There is a composition series for Q, and all composition series have the same length. Any chain from Q to P may be refined to a composition series for Q.*

§2. Height and Depth of a Prime Ideal.

Definition. A proper prime ideal P in an integral domain R is said to have height h if there exists a chain

$$(0) \subset P_1 \subset \ldots \subset P_h = P$$

of prime ideals, but no such longer chain. Similarily P has depth d if

$$R \supset P_o \supset \ldots \supset P_d = P$$

and no prime chain from R to P is longer.

THEOREM 2.1. Let P^* be a minimal prime ideal of a principal ideal (a), $a \neq 0$, in a noetherian domain R. Then P^* has height unity.

Proof. Use will be made of the n-th symbolic powers $P^{(s)}$ of a prime ideal P; these are defined $P^{(s)} = \{x : x \in R:\ rx \in P^n$ for some $r \notin P\}$ and are P-primary ideals. If for some integer i, $P^{(i)} = P^{(i+1)}$ then it is easy to check that $P^{(i+1)} = P^{(i+2)} = P^{(i+3)}$ etc. (1) . Also, given a P-primary ideal Q, then some symbolic power $P^{(n)}$ is contained in Q. For R noetherian $\Rightarrow P^v \subseteq Q$ (some integer v), then $x \in P^{(v)} \Rightarrow rx \in P^v\ (r \notin P) \Rightarrow rx \in Q \Rightarrow x \in Q$.

The problem can be reduced by consideration of the local ring R_{P^*}, in which (a) and P^* correspond to an M-primary ideal and a unique maximal ideal M. To simplify notation suppose these properties hold for (a) and P^* in R. Then any ideal between (a) and P^* is P^*-primary; in particular $(a) + P^{(i)}$ for any proper prime ideal $P \subset P^*$.

In view of Theorem 1' the chain

$$(a) + P^{(1)} \supseteq (a) + P^{(2)} \supseteq (a) + P^{(3)} \supseteq \ldots$$

is bounded by the length of (a). Therefore $(a) + P^{(s)} = (a) + P^{(s+1)}$ for some integer $s \geq 1$. If now $x \in P^{(s)}$, then $x = za + y$ $(z \in R,\ y \in P^{(s+1)})$ so that $za = x - y \in P^{(s)}$ and hence $z \in P^{(s)}$, as $a \notin P$ since P^* is a minimal prime ideal of (a) and $P \subset P^*$. Consequently $P \subseteq aP^{(s)} + P^{(s+1)}$ and the reverse inclusion is obvious. In other words, $P^{(s)} = (a)P^{(s)} \pmod{P^{(s+1)}}$. By the lemma which usually precedes Krull's Intersection Theorem [5] Vol I. p215 there exists $r \in R$ such that $(1 - ra)P^{(s)} = 0 \pmod{P^{(s+1)}}$; but $ra \in P^*$, $1 - ra$ has an inverse and so $P^{(s)} = P^{(s+1)}$ (2).

On the other hand $P \subseteq P^* \Rightarrow P^{(s)} \subseteq P^{*(s)}$. Now for a <u>maximal</u> prime ideal, the symbolic prime powers are just the powers of the ideal, and we know $\bigcap_{i=1}^{\infty} P^{*i} = 0$. Hence $\bigcap_{i=1}^{\infty} P^{(i)} = 0$, which together with (1) and (2) shows that $P^{(s)} = (0)$. But $P^{(s)}$ is P-primary and so $P = (0)$, a contradiction. Thus there is no proper prime ideal P strictly between (0) and P^*.

Before generalising the result we require the

<u>LEMMA</u>. <u>Let $M_1, \ldots, M_m$ be a family of prime ideals none of which contains P. If $(0) \subset P_1 \subset \ldots \subset P_r = P$ is a chain of prime ideals from (0) to P, then there is a similar chain $(0) \subset P_1' \subset \ldots \subset P_r' = P$ with no P_j' contained in any M_i.</u>

Proof. Firstly consider $P_{r-2} \subset P_{r-1} \subset P_r = P$. We can choose $a \in P$: $a \notin M_i$ $(1 \leq i \leq m)$. Taking P_{r-1}' to be a minimal prime ideal of $P_{r-2} + (a)$ so that $P_{r-1}' \subseteq P$, we can replace P_{r-1} by P_{r-1}' if $P_{r-1}' \not\subseteq P$. Suppose then $P_{r-1}' = P$. By Theorem 2.1 this implies that P/P_{r-2} (a minimal prime ideal of $P_{r-2} + (a)/P_{r-2}$)

has height one, contradicting the chain $(0) \subset P_{r-1}/P_{r-2} \subset P_r/P_{r-2}$.

To produce the required chain each of the P_i is replaced step by step, from right to left.

THEOREM 2.2. <u>Let</u> P <u>be a minimal prime ideal of the ideal</u> $A = (a_1, \dots, a_r)$ <u>in a noetherian domain</u> R. <u>Then the height of</u> P <u>cannot exceed</u> r.

<u>Proof</u>. Noting that the case $r = 1$ is the previous theorem, we make the induction hypothesis that the result holds for ideals generated by $r-1$ elements: in particular the minimal prime ideals $P_1', \dots, P_k'$ of $(a_2, \dots, a_r)$ have height not greater than $r-1$. If $P \subseteq P_i'$ for some $i \in (1, \dots, k)$ then trivially P has height less than r; so assume $P \nsubseteq P_i'$ $(1 \le i \le k)$. Then by the lemma any chain $(0) \subset P_1 \subset \dots \subset P_s = P$ may be supposed to have $P_1 \nsubseteq P_i'$ $(1 \le i \le k)$. Let $b \in P_1$; $b \notin P_i'$ $(1 \le i \le k)$, then we choose P^* from the minimal prime ideals of $(b, a_2, \dots, a_r)$ to be contained in P. For some $i \in (1, \dots, k)$, $P_i' \subseteq P^*$ $((a_2, \dots, a_r) \subseteq P^*)$, but by choice of b, $P_i' \neq P^*$ and thus $P_i' \subset P^*$. If we had $P \supset P^* \supset P_i'$ then $P/(a_2, \dots, a_r)$ would have height at least two in $R/(a_2, \dots, a_r)$, contradicting the minimality of $P/(a_2, \dots, a_r)$ as a prime ideal belonging to the <u>principal</u> ideal $(a_1, \dots, a_r)/(a_2, \dots, a_r)$.

Necessarily then $P = P^*$, which means P must be a minimal prime ideal of $(b, a_2, \dots, a_r)$, and therefore $P/(b)$ is a minimal prime ideal of $(b, a_2, \dots, a_r)/(b) = (a_2, \dots, a_r)/(b)$, an ideal generated by $r-1$ elements.

By induction hypothesis the residue chain

$$0 \le P_1/(b) \subset \dots \subset P_s/(b)$$

cannot have more than r terms, whence the height of P is at most r.

The converse of this theorem is also true:

THEOREM 2.3. *Given P a prime ideal of height h, then h elements can be found to generate an ideal with P as a minimal prime.*

Proof. $P = (0)$ is trivial.

Assume $P \neq (0)$ and take $a_1 \in P$, $a_1 \neq 0$. Then (Theorem 2.1) every minimal prime ideal of (a_1) has height one. Assume, for induction purposes, that elements $a_1, \ldots, a_s$ of P $(s < h)$ have been found such that every minimal prime ideal P_i of $(a_1, \ldots, a_s)$ has height s.

Now clearly no P_i can contain P, and so there is an element $a_{s+1} \in P$: $a_{s+1} \notin P_i$ for all minimal primes of $(a_1, \ldots, a_s)$. Then any minimal prime ideal P'_j of $(a_1, \ldots, a_{s+1})$ contains strictly one of the P_i and so has height not less than $s + 1$. That this height is exactly $s + 1$ follows from the last theorem.

By induction, there exist elements $a_1, \ldots, a_h$ of P such that every minimal prime ideal P_i^* of $(a_1, \ldots, a_h)$ has height h. Among these minimal primes P_i^* occurs P, for P contains some P_i^*, but having same height h must in fact equal this P_i^*.

For later use we state the

COROLLARY. *From a given basis $(u_1, \ldots, u_s)$ of the unique maximal ideal $\mathfrak{M}$ in a local ring Q we may select $u_1, \ldots, u_h$ to generate an $\mathfrak{M}$-primary ideal, where h is the height of $\mathfrak{M}$.*

Proof. It is easily seen in the above proof that the a_i can be taken from a given basis of P. In accord with the theorem let $(u_1, \ldots, u_s)$ have $\mathfrak{M}$ as a minimal prime ideal: $\mathfrak{M}$ is maximal and so $(u_1, \ldots, u_h)$ is $\mathfrak{M}$-primary.

As a special case of Theorem 2.2 we note that every prime ideal in a noetherian ring R has finite height. On the other hand a prime ideal may well have infinite depth, and there is no relation between the two in the general case. Our aim in the next section is to show that for finite integral domains height and depth are determined one by the other, and that rank and dimension are the equivalents of height and depth respectively.

§3. Rank and Dimension in a Finite Integral Domain.

Let $R = k[\xi_1, \ldots, \xi_n]$, a finite integral domain, have degree of transcendence r over k, and let $\xi_1, \ldots, \xi_r$ constitute a transcendence base for $k(\xi_1, \ldots, \xi_n)$ over k.

If P is a prime ideal strictly contained in R then R/P is an integral domain with k as a subfield. We define the <u>dimension</u> of P - $\dim P$ - to be the transcendence degree of this domain over k; the complement $(r - \dim P)$ we call the <u>rank</u> of P.

Consequences of the definition are:-

1. <u>A prime ideal of dimension 0 is maximal.</u>

For R/P is a field in this case.

2. <u>If $P \subset P'$ then $\dim P' < \dim P$.</u>

<u>Proof.</u> Consider the k-homomorphism ϕ of R/P onto R/P' given by $\phi(r + P) = r + P'$. If we let $\eta_1 + P, \ldots, \eta_t + P$ be a transcendence base for R/P over k; then any non-zero element of R/P, in particular $y + P$, where $y \in P'$, $y \notin P$, satisfies a relation $g(\eta_1, \ldots, \eta_t, y) \in P$ (g has coefficients in k and $g \not\equiv 0$). It may happen that every term in g contains some power of y; if so write $g = g' y^m$ (m is the minimum of these powers), then g' has at least one term not involving y (^{1}). Also $y \notin P$, P prime implies that $g' \in P$.

We have $g'(\eta_1, \ldots, \eta_t, y) \in P$, i.e. $g' + P = 0$, hence $\phi(g' + P) = 0$, i.e. $g^* \in P'$ where $g^*(\eta_1, \ldots, \eta_t) = g'(\eta_1, \ldots, \eta_t, y)_{y=}$ and g^* is non-zero by (^{1}).

Clearly $\eta_1 + P, \ldots, \eta_t + P$ is a transcendence set for R/P' and we have shown that it is not an algebraically independent set. Q.E.D.

3. <u>Every proper prime ideal has dimension less than</u> $r = \underline{\dim}(0)$.

4. <u>A prime ideal of dimension</u> $r - 1$ <u>is **minimal**</u> (that is, there is no prime ideal strictly smaller except (0)).

These last two follow from <u>2</u>.

The converse of Property <u>4</u> is given in

THEOREM 3.1. <u>If</u> P <u>is a minimal prime ideal in</u> $R = k[\xi_1, \ldots, \xi_n]$ <u>**then dim**</u> $P = r - 1$. $(r = \text{transc}_k R)$

<u>Proof</u>. The general proof depends upon the normalisation theorem [5] I.p.26 and we treat only the case $r = n$, i.e. $k[\xi_1, \ldots, \xi_n] = k[X_1, \ldots, X_n]$

Thus R is a unique factorisation domain, in which a minimal prime ideal P is easily seen to be generated by a single irreducible element $f(X_1, \ldots, X_n)$ say.

Let X_1 occur in f $(f \neq 0)$ then every polynomial in P contains X_1. Therefore $X_2, \ldots, X_n$ are algebraically independent mod P (over k), which shows that $\dim P \geqslant n - 1$ and the result follows by Property <u>3</u>.

At this juncture we recall that $P \subset P' \Rightarrow \dim P > \dim P'$; $h(P) < h(P')$; $d(P) > d(P')$. From Theorem 3.1 we can now prove the main theorem of dimension theory in finite integral domains.

THEOREM 3.2. <u>If</u> $P \subset R$ <u>is a prime ideal of dimension</u> s <u>in a finite integral domain</u> R <u>of transcendence</u> r , <u>then the height</u> $h(P)$ <u>and the depth</u> $d(P)$ <u>of</u> P <u>satisfy:</u>

(i) $h(P) = \underline{\text{rank}}$ of $P = r - s$.

(ii) $d(P) = \underline{\dim}\ P = s$.

<u>Proof</u>. (i). In the case $s = r$ $(P = (0)$) the result is trivial.

We assume the theorem for ideals of dimension $s + 1$ and deduce its validity for dimension s.

Let $(0) = P_0 \subset P_1 \subset \dots \subset P_h = P$ be a chain of length $h(P) = h$. By our remarks above $s = \dim P < \dim P_{h-1} < \dots < \dim P_0 = r$ and hence $h \leq r - s$ (1).

Since h has an upper bound (R being noetherian), there exists a prime ideal P' such that $P' \subset P$ and no prime ideals lie strictly between P' and P. Thus P/P' is minimal prime in R/P' and has (Theorem 3.1) dimension = transc $R/P' - 1$. But $\dim P/P'$ = transc $R/P'/P/P'$ = transc $R/P = \dim P$, and transc $R/P' = \dim P'$ by definition; therefore $\dim P' = s + 1$. From our induction hypothesis $h(P') = r - (s + 1) \Rightarrow h(P) \geq r - s$, which together with (1) is the required result.

(ii) We use induction on s. Here $s = 0$, which by Property 1 implies that P is maximal and so $d(P) = 0$, is the trivial case.

If $R \supset P_0 \supset \dots \supset P_d = P$ then $0 \leq \dim P_0 < \dim P_1 < \dots < \dim P_d = s$, which shows $d(P) \leq s$ (2).

Let $P' \supset P$ such that P'/P is minimal prime in R/P; then by Theorem 3.1 $\dim P'/P = s - 1$. Now $\dim P'/P = \dim P'$ and making the induction hypothesis for $s - 1$, $\dim P' = s - 1 = d(P')$. Then clearly $d(P) \geq s$ which along with (2) completes the proof.

COROLLARY 1. *Let P P' and s, s' be their respective dimensions. Then there is a chain*

$$P \subset P_1 \subset \dots \subset P_{s-s'-1} \subset P'$$

and no such chain is longer.

Proof. In R/P, P'/P has dimension s' and therefore height $s - s'$.

COROLLARY 2. <u>A finite integral domain</u> R <u>of transcendence degree</u> r <u>has prime ideals of all dimensions</u> 0, 1, ..., r - 1.

<u>Proof.</u> $P = (0)$ in the theorem implies $d(P) = r$, and a chain of length $r + 1$ descending to P will contain ideals of the above dimensions.

COROLLARY 3. Theorem 3.1. of Chapter I.

<u>Proof.</u> Let $P \neq (1)$ then $R = k[\xi_1, \ldots, \xi_n] = k[\underline{X}]/P$ contains the field k. By Corollary 2, R has a prime ideal of dimension 0, say P'/P. Wherefore $k[\underline{X}]/P' = k[\eta_1, \ldots, \eta_n]$ has transcendence degree 0, i.e. $\eta_1, \ldots, \eta_n$ are algebraic over k. Also $f(\underline{X}) \in P \Rightarrow f(\underline{X}) \in P' \Rightarrow f(\eta_1, \ldots, \eta_n) = 0$ so η lies in V(P). Q.E.D.

The theorems on height in the previous section can be expressed in terms of dimension in view of the identities proved in Theorem 3.2.

THEOREM 3.3. <u>In a finite integral domain</u> R <u>of transcendence degree</u> r <u>every minimal prime ideal of a proper principal ideal</u> (a) <u>has dimension</u> r - 1. (cf Theorem 2.1).

THEOREM 3.4. <u>Every minimal prime ideal of</u> $A = (a_1, \ldots, a_s)$ <u>in the finite integral domain</u> R <u>of transcendence degree</u> r <u>has dimension at least</u> r - s. (cf Theorem 2.2).

CHAPTER III

THE SIMPLE POINT ON A VARIETY

§1. Notation.

Throughout this chapter W will be a ρ -dimensional irreducible subvariety of the r-dimensional irreducible variety V, these having $\eta = (\eta_1, \ldots, \eta_n)$ and $\xi = (\xi_1, \ldots, \xi_n)$ as generic points respectively.

In the co-ordinate ring $R[V]$ we have $I(V) \subset I(W)$ and $I(W)/I(V)$ is a prime ideal which we write $\mathfrak{p}(W/V)$.

The quotient ring $R[V]_{\mathfrak{p}(W/V)} = \left\{ \frac{f(\xi)}{g(\xi)} : g(\eta) \neq 0 \right\}$

(f and g will always be polynomials with coefficients in the ground field k) is a local ring [1] , which we shall denote by $Q(W/V)$, with unique maximal ideal $\mathfrak{m}(W/V) = \left\{ \frac{f(\xi)}{g(\xi)} : f(\eta) = 0, g(\eta) \neq 0 \right\}$.

§2. The Local Vector Space.

2.1. Let us write $\overline{u}$ for the $\mathfrak{M}^2$ - residue of $u \in \mathfrak{M}$, and $\tilde{d}$ for the $\mathfrak{M}$ -residue of $d \in Q = Q(W/V)$. Then $\tilde{d}$ is an element of the field $Q/\mathfrak{M}$ which may be identified with the field $\mathcal{F}(W)$ consisting of all quotients $\frac{f(\eta)}{g(\eta)}$: $g(\eta) \neq 0$, i.e. the field $k(\eta_1, \ldots, \eta_n)$.

If we now define the product $\tilde{d}\overline{u}$ to be the $\mathfrak{M}^2$ -residue of $d.u$, then $\mathfrak{M}/\mathfrak{M}^2$ becomes a vector space over $\mathcal{F}(W)$. That $\tilde{d}\overline{u}$ is well-defined follows from noting that if $d \equiv d' \pmod{\mathfrak{M}}$ and $u \equiv u' \pmod{\mathfrak{M}^2}$ then

$$du - d'u' = (d-d')u - d'(u'-u) \in \mathfrak{M}^2 ,$$

so that $\overline{d.u} = \overline{d'.u'}$.

We denote this vector space by $M(W/V)$ and call it <u>the local vector space of V at W</u>.

The elements $u_1, \ldots, u_p$ form a basis for $\mathfrak{M}$ if and only if their $\mathfrak{M}^2$ -residues $\overline{u}_1, \ldots, \overline{u}_p$ span the space. For suppose that $u_1, \ldots, u_p$ form a basis and let $\overline{u} \in \mathfrak{M}/\mathfrak{M}^2$; then if u has $\mathfrak{M}^2$-residue $\overline{u}$, we have

$$u = \sum_{i=1}^{p} \lambda_i u_i \qquad (\lambda_i \in Q)$$

which implies

$$\overline{u} = \sum_{i=1}^{p} \tilde{\lambda}_i \overline{u}_i$$

On the other hand, suppose that $\overline{u}_1, \ldots, \overline{u}_p$ span $M(W/V)$, and consider the ideal $\mathfrak{U}$ generated in $Q(W/V)$ by $u_1, \ldots, u_p$. Now $\mathfrak{M}/\mathfrak{M}^2 = \mathfrak{U}/\mathfrak{M}^2$ i.e. $\mathfrak{M} = \mathfrak{U} + \mathfrak{M}^2$; hence $\mathfrak{M}^2 = \mathfrak{U}\mathfrak{M} + \mathfrak{M}^3 \subseteq \mathfrak{U} + \mathfrak{M}^3$ and so $\mathfrak{M} = \mathfrak{U} + \mathfrak{M}^3$. In fact we find that $\mathfrak{M} = \mathfrak{U} + \mathfrak{M}^i$ for any positive integer i. But $\bigcap_{i=1}^{\infty} (\mathfrak{U} + \mathfrak{M}^i) = \mathfrak{U}$ (see [3] p 65) so that $\mathfrak{M} = \mathfrak{U}$, which shows that $u_1, \ldots, u_p$ form a basis of $\mathfrak{M}$.

Let us call a basis $(u_1, \ldots, u_s)$ of $\mathfrak{M}$ minimal if no proper subset of these elements constitutes a basis. It follows from the above that $(u_1, \ldots, u_s)$ will be a minimal basis if and only if $\bar{u}_1, \ldots, \bar{u}_s$ form a basis of the vector space $M(W/V)$.

All minimal bases of $\mathfrak{M}$ have therefore the same number of elements, namely the dimension of $M(W/V)$; this number is finite by the Hilbert Basis Theorem.

When $(u_1, \ldots, u_s)$ is a basis of $\mathfrak{M}$ we can assume that $u_i \in R[V]$, for if $u_i = \dfrac{f_i(\xi)}{g_i(\xi)}$ then $f_i(\xi)$ also form a basis.

Clearly $\mathfrak{p}(W/V)$ is a minimal prime ideal of $R[V]$. $(u_1, \ldots, u_s)$ and so by Theorem 3.4 of Chapter II the dimension of $\mathfrak{p}(W/V)$ is at least $r - s$. But $\mathfrak{p}(W/V)$ has dimension ρ, and we deduce

$$\dim M(W/V) \geqslant \dim V - \dim W \tag{2a}$$

or in the case in which $W = \alpha = (\alpha_1, \ldots, \alpha_n)$, a point of V,

$$\dim M(\alpha/V) \geqslant \dim V. \tag{2a'}$$

The following two lemmas are used later in the chapter.

2.2. Reduction to dimension zero.

REMARK. If the k-homomorphism

$$k[\xi_1, \ldots, \xi_\nu] \to k[\eta_1, \ldots, \eta_\nu], \quad \xi_i \to \eta_i$$

is an isomorphism then we may write $\xi_i = \eta_i$ $(i = 1, \ldots, \nu)$.

LEMMA 1. Let V and W be varieties such that their generic points ξ and η have $\xi_i = \eta_i$ $(i = 1, \dots, \nu)$. Then if V^* and W^* are the varieties over $k^* = k(\xi_1, \dots, \xi_\nu)$ with generic points $(\xi_{\nu+1}, \dots, \xi_n)$ and $(\eta_{\nu+1}, \dots, \eta_n)$ we have

$$Q(W^*/V^*) = Q(W/V).$$

Proof. Let $f(\xi_1, \dots, \xi_\nu) \in k[\xi_1, \dots, \xi_\nu] \cap \mathfrak{p}(W/V)$ i.e. $f(\eta_1, \dots, \eta_\nu) = 0 \Rightarrow f(\xi_1, \dots, \xi_\nu) = 0$ as $\xi_i = \eta_i (i = 1, \dots, \nu)$. This shows that $k^* \subseteq Q(W/V)$. Also $R[V^*] = k^*. R[V]$ and $\mathfrak{p}(W^*/V^*) = k^*. \mathfrak{p}(W/V)$; so if $f^*(\xi_{\nu+1}, \dots, \xi_n)$ lies in $R[V^*]$ but not in $\mathfrak{p}(W^*/V^*)$ (i.e. $f^*(\xi_{\nu+1}, \dots, \xi_n) \neq 0$) then $f^*(\xi_{\nu+1}, \dots, \xi_n)$ has an inverse in $Q(W/V)$. Thus

$$Q(W^*/V^*) = \frac{R[V^*]}{R[V^*] - \mathfrak{p}(W^*/V^*)} \subseteq Q(W/V).$$

$$\text{Conversely } x \in Q(W/V) \Rightarrow x = \frac{f(\xi)}{g(\xi)} = \frac{f^*(\xi_{\nu+1}, \dots, \xi_n)}{g^*(\xi_{\nu+1}, \dots, \xi_n)} \in Q(W^*/V^*)$$

if $g^*(\eta_{\nu+1}, \dots, \eta_n) \neq 0$ which is the case otherwise $g(\eta) = 0$ contradiction.

APPLICATION. As W has dimension ρ we may assume that $\eta_1, \dots, \eta_\rho$ are algebraically independent over k. So also are $\xi_1, \dots, \xi_\rho$, for $W \subset V$ means $f(\xi) = 0$ implies $f(\eta) = 0$. The mapping

$f(\xi_1, \dots, \xi_\rho) \to f(\eta_1, \dots, \eta_\rho)$ is a k-isomorphism of $k[\xi_1, \dots, \xi_\rho]$ onto $k[\eta_1, \dots, \eta_\rho]$ and by our remark we may write $\xi_i = \eta_i$ $(i = 1, \dots, \rho)$. Then applying the lemma to V^* which has dimension $r - \rho$, and to W^* which is now a point α^*

(because $\eta_{\rho+1}, \ldots, \eta_n$ are algebraic over $k^* = k(\eta_1, \ldots, \eta_\rho)$), we see that

$$Q(W/V) = Q(\alpha^*/V^*).$$

2.3. Insertion of a third variety

Let V' be an irreducible variety between W and V. Then $M(W/V')$ and $M(W/V)$ have the same field of scalars viz. $\mathcal{J}(W)$.

Since $V' \subset V$, there is a k-homomorphism ϕ of $R[V]$ onto $R[V']$ taking ξ_i to ξ_i' (where $\xi' = (\xi_1', \ldots, \xi_n')$ is the generic point of V'). Noting that $f(\xi) \notin p(W/V)$ implies $\phi f(\xi) \notin p(W/V')$ we can extend ϕ to a homomorphism ψ of $Q(W/V)$ onto $Q(W/V')$ by defining

$$\psi\left\{\frac{f(\xi)}{g(\xi)}\right\} = \frac{f(\xi')}{g(\xi')}.$$

Under this mapping $\mathfrak{M} \to \mathfrak{M}'$ and $\mathfrak{M}$ is the full inverse image of $\mathfrak{M}'$.

If now we denote by τ the mapping

$$u \to \bar{u} \quad (u \in \mathfrak{M} \ ; \ \bar{u} = u + \mathfrak{M}^2)$$

and similarily

$$\tau' : \ u' \to \overline{u'} \quad (u' \in \mathfrak{M}' ; \ \overline{u'} = u' + \mathfrak{M}'^2)$$

then the composition $\tau' \psi \tau^{-1}$ is a mapping from $M(W/V)$ to $M(W/V')$. To check that it is single-valued, let $\bar{u}_1 = \bar{u}_2 (u_1 - u_2 \in \mathfrak{M}^2)$; then $\psi(u_1 - u_2) \in \mathfrak{M}'^2$ which implies that $\tau' \psi (u_1 - u_2) = 0$; whence result.

LEMMA 2. The mapping $\tau' \psi \tau^{-1}$ is a linear transformation of $M(W/V)$ onto $M(W/V')$. The nullspace is the subspace of $M(W/V)$ spanned by the vectors belonging to $\tau(Q(W/V).\, p(V'/V))$.

Proof. We prove only the second part of the lemma, the proof of the first part being similar.

In $R[V]$ the ideal $\mathfrak{p}(V'/V) = \{ f(\xi) : f(\xi') = 0 \}$ is the kernel of the homomorphism ϕ. Its extension $Q(W/V).\mathfrak{p}(V'/V)$ to $Q(W/V)$ is clearly the kernel of ψ.

Suppose now that $\bar{u} \in$ Nullspace $(\tau'\psi\tau^{-1})$, i.e. that $\tau'\psi\tau^{-1}(u) = 0$. Then $\tau'\psi(u) = 0$, that is $\psi(u) \in \mathfrak{m}'^2$, which shows that $u \in \operatorname{Ker}\psi + \mathfrak{m}^2$. Finally $\bar{u} \in \tau(\operatorname{Ker}\psi) = \tau(Q(W/V).\mathfrak{p}(V'/V))$.
Q.E.D.

§3. Simple points and subvarieties.

In view of (2a) and (2a') we make the following definitions:-
A point α is <u>simple</u> (for V) if

$$\dim M(\alpha/V) = \dim V.$$

A subvariety W is <u>simple</u> (for V) if

$$\dim M(W/V) = \dim V - \dim W.$$

With the help of the lemmas we can derive some consequences of these definitions.

PROPOSITION 1. <u>Any point α is simple for S_n.</u>

<u>Proof.</u> In Lemma 2 take $W = \alpha$, V' = the variety having $(\alpha_1, X_2, \ldots, X_n)$ as generic point, and $V = S_n$. Here $(V'/V) = \left\{ f(\underline{X}) : f(\alpha_1, X_2, \ldots, X_n) = 0 \right\} = (h(X_1))$, h being the irreducible polynomial in $k(X_2, \ldots, X_n)\left[X_1\right]$ such that $h(\alpha_1) = 0$. The $\mathfrak{M}^2$- residue of this polynomial clearly generates the nullspace of $\tau' \psi \tau^{-1}$, which cannot therefore have dimension greater than one. Hence $\dim M(\alpha/S_n) \leq 1 + \dim M(\alpha/V')$. Now by Lemma 1, $\dim M(\alpha/S_n) = \dim M(\alpha^*/S^{k^*}_{n-1})$; $\alpha^* = (\alpha_2, \ldots, \alpha_n)$ and $k^* = k(\alpha_1)$. If we make the induction assumption that the proposition is true for $n - 1$, it follows that $\dim M(\alpha/S_n) \leq 1 + (n-1) = n$; but certainly $\dim M(\alpha/S_n) \geq \dim S_n - \dim \alpha = n$, so in fact $\dim M(\alpha/S_n) = n$. The case $n = 1$ is trivially true and the proposition is proved.

COROLLARY. <u>W is simple for S_n.</u>

<u>Proof.</u> We know $M(W/S_n)_{k^*} = M(\alpha^*/S^{k^*}_{n-\rho})$ where $k^* = k(\eta_1, \ldots, \eta_\rho)$ and α^* is a point of $S^{k^*}_{n-\rho}$. The above proposition shows that

$M(\alpha^* / S^{k^*}_{n-\rho})$ has dimension $n - \rho$, thus so also has $M(W/S_n)$.

PROPOSITION 2. α <u>is simple for</u> V <u>if and only if the ideal</u> $p(V/S_n)$ <u>contains</u> $n - r$ <u>elements</u> $u_1, \ldots, u_{n-r}$ <u>such that</u> $\tau u_1, \ldots, \tau u_{n-r}$ <u>are linearly independent in</u> $M(\alpha/S_n)$.

<u>Proof</u>. $\alpha \subset V \subset S_n$ and $\dim M(\alpha/S_n) = n$. Considering the transformation of Lemma 2,

$$n = \dim \tau(\, p(V/S_n)\,) + \dim M(\alpha/V).$$

Now α is simple for V if and only if $\dim M(\alpha/V) = r$, i.e. if and only if $\dim \tau(\, p(V/S_n)) = n - r$.

§4. Regular Rings.

A local ring Q is said to be *regular* if, for $(u_1, \ldots, u_s)$ a minimal basis of $\mathfrak{M}$, a homogeneous relation

$$\phi_\nu(u_1, \ldots, u_s) = 0 \qquad (4a)$$

with coefficients in Q is possible only if the coefficients are in $\mathfrak{M}$.

This type of local ring was introduced and studied by Krull [1].

An equivalent condition for regularity is: Let ϕ_ν be a form of degree ν, with coefficients in Q; then

$$\phi_\nu(u_1, \ldots, u_s) \in \mathfrak{M}^{\nu+1} \qquad (4b)$$

implies that all coefficients of ϕ_ν are in $\mathfrak{M}$.

Proof. That (4b) implies (4a) is trivial.

Assume that (4a) holds. Let $\phi_\nu(u_1, \ldots, u_s) \in \mathfrak{M}^{\nu+1}$; then is a homogeneous polynomial of degree $\nu + 1$, say $\psi_{\nu+1}$. Take the typical term of ϕ_ν,

$$r u_1^{\alpha_1} u_2^{\alpha_2} \cdots u_s^{\alpha_s}, \; \alpha_1 + \alpha_2 + \cdots + \alpha_s = \nu, \; r \in Q$$

and in $\psi_{\nu+1}$ choose the term

$$s u_1^{\alpha_1+1} u_2^{\alpha_2} \cdots u_s^{\alpha_s}, \quad s \in Q$$

then the term in $u_1^{\alpha_1} \cdots u_s^{\alpha_s}$ of $\phi_\nu - \psi_{\nu+1}$ has coefficient $r - s u_1$, which by (4a) belongs to $\mathfrak{M}$. But $s u_1 \in \mathfrak{M}$; hence $r \in \mathfrak{M}$ and we have (4b).

The concepts of simple point and regular local ring are related in

THEOREM 4.1. The point α is simple for V if and only if $Q(\alpha/V)$ is regular.

Proof. Recall that α is simple if and only if $r = \dim V = \dim M(\alpha/V) = s$.

Let $s > r$; we show that Q is not regular, thereby establishing the 'if' part of the theorem.

From the corollary to Theorem 2.3, and Theorem 3.2 of Chapter II, we can choose $u_1, \ldots, u_r$ from a minimal basis of $\mathfrak{m}$ so that they generate in Q an $\mathfrak{m}$-primary ideal $\mathfrak{a}$, say, of dimension 0.

Consider the element $u_s \notin \mathfrak{a}$. Now since $\mathfrak{a}$ is $\mathfrak{m}$-primary $u_s^h \in \mathfrak{a}$ for some power h.

Also there exists a positive integer ν such that $u_s^h \in \mathfrak{a}\mathfrak{m}^\nu$ but $u_s^h \notin \mathfrak{a}\mathfrak{m}^{\nu+1}$, otherwise $u_s^h \in \mathfrak{a}\mathfrak{m}^\nu$ i.e. $u_s^h \in \mathfrak{m}^\nu$ for all ν, i.e. $u_s^h \in \bigcap_{i=1}^{\infty} \mathfrak{m}^i = 0$, i.e. $u_s = 0$ contradicting $u_s \notin \mathfrak{a}$.

The general element of $\mathfrak{a}\mathfrak{m}^\nu$ is

$\sum \phi_1(u_1, \ldots, u_r)\, \psi_\nu(u_1, \ldots, u_s)$, where ϕ_1 is linear in $u_1, \ldots, u_r$ and ψ_ν is homogeneous of degree ν in $u_1, \ldots, u_s$; in particular u_s^h can be represented in this way. We have

$$u_s^h - \sum \phi_1(u_1, \ldots, u_r)\, \psi_\nu(u_1, \ldots, u_s) = 0 \qquad \text{(i)}$$

Case 1. $h \leq \nu + 1$ means $u_s^h \in \mathfrak{a}\mathfrak{m}^\nu \subseteq \mathfrak{m}^\nu \subseteq \mathfrak{m}^{h+1}$ which by (4b) shows that Q is not regular.

Case 2. $h = \nu + 1$ then (i) is a form of degree h in $u_1, \ldots, u_s$. Now clearly the products $\phi_1 \psi_\nu$ do not contain a term in u_s alone (ϕ_1 is linear in $u_1, \ldots, u_r$); accordingly the coefficient of u_s^h in (i) is unity. Hence Q cannot be regular for $1 \notin \mathfrak{m}$.

Case 3. $h > \nu + 1$. From $u_s^h \notin \mathfrak{a}\mathfrak{m}^{\nu+1}$, the coefficients of ϕ_1

and ψ_ν cannot all belong to $\mathfrak{M}$. However $\sum \phi_1\psi_\nu = u_s^h \in \mathfrak{M}^h \subseteq \mathfrak{M}^{\nu+2}$ and $\sum \phi_1\psi_\nu$ is homogeneous of degree $\nu+1$. Thus condition (4b) is not satisfied.

We now prove the 'only if' part of the theorem.

CASE 1. Let $\mathcal{J}(\alpha) = k(\alpha)$ be infinite.

Corresponding to a given form $p_\nu(x_1, \ldots, x_s)$ of degree ν with coefficients in Q, write $\widetilde{p}_\nu(x_1, \ldots, x_s)$ when these coefficients are replaced by their $\mathfrak{M}$-residues. To establish the regularity of Q we show that $p_\nu(u_1, \ldots, u_s) = 0$ implies $\widetilde{p}(x_1, \ldots, x_s) = 0$.

Suppose now $\widetilde{p}(x_1, \ldots, x_s) \neq 0$; then in $\mathcal{J}(\alpha)$ we may select a non-singular homogeneous transformation

$$x_i' = \sum_{j=1}^{s} \widetilde{a}_{ij}x_j \qquad (\widetilde{a}_{ij} \in \mathcal{J}(\alpha))$$

to make the coefficient of $x_s'^{\nu}$ in the resulting form $\widetilde{\pi}(x_1', \ldots, x_s')$ non-zero.

If we put

$$u_i' = \sum_{j=1}^{s} a_{ij}u_j \qquad (a_{ij} \in Q)$$

then assuming $p(u_1, \ldots, u_s) = 0$ we get $\pi(u_1', \ldots, u_s') = 0$ and the coefficient of $u_s'^{\nu}$ is not in $\mathfrak{M}$. The nonsingularity of the transform guarantees that $(u_1', \ldots, u_s')$ is a new minimal basis for $\mathfrak{M}$. By a suitable division $u_s'^{\nu} \in Q.(u_1', \ldots, u_{s-1}')$ and therefore $\mathfrak{M}^\nu \subseteq Q(u_1', \ldots, u_{s-1}')$, giving that the ideal $Q.(u_1', \ldots, u_{s-1}')$ has dimension 0. This contradicts the fact that all minimal prime ideals of $Q.(u_1', \ldots, u_{s-1}')$ have dimension $r-(s-1) = r-(r-1) = 1$ (see Chapter II, Theorem 3.4).

CASE 2. If $k(\alpha)$ is finite take a new ground field $k^* = k(z)$ where z is an indeterminate. Let V^* be the variety over k^* having the same generic point as V and let α^* have the same coordinates as α.

Clearly $\dim V^* = \dim V = r$. Also

$$\mathfrak{M}^* = Q^* \cdot \mathfrak{M} \qquad \text{(a)}$$

$$\mathfrak{M} = \mathfrak{M}^* \cap Q \qquad \text{(b)}$$

where $Q^* = Q(\alpha^*/V^*)$ and $\mathfrak{M}^* = \mathfrak{M}(\alpha^*/V^*)$.

The basis $(u_1, \ldots, u_s)$ of $\mathfrak{M}$ is by (a) also a basis of $\mathfrak{M}^*$ and necessarily minimal as

$$\dim V^* = r = s.$$

Now $\mathcal{J}(\alpha^*)$ is infinite and by CASE 1 we have Q^* regular. Thus $\phi_\nu(u_1, \ldots, u_s) = 0$ with coefficients in $Q \subseteq Q^*$ implies the coefficients belong to $\mathfrak{M}^*$ and so to $\mathfrak{M}$ by (b).

The proof is now complete.

COROLLARY. <u>W is simple for V if and only if Q(W/V) is regular.</u>

<u>Proof.</u> By reduction to dimension zero (q.v.) this follows from the theorem.

§5. The Space of Local Differentials.

Let $u \in \mathfrak{M}(W/S_n)$, then $u = \dfrac{f(X)}{g(X)}$: $f(\eta) = 0$, $g(\eta) \neq 0$ and the partial derivatives $\dfrac{\partial u}{\partial X_i}$ belong to $Q(W/S_n)$ since $g^2(\eta) \neq 0$. The $\mathfrak{M}$-residues $\left.\dfrac{\partial u}{\partial X_i}\right|_{X=\eta}$ lie in the field $\mathcal{F}(W) = k(\eta)$.

The ordered n-tuple of these residues

$$\left(\frac{\partial u}{\partial X_1}, \ldots, \frac{\partial u}{\partial X_n}\right)_{X=\eta}$$

we call the local W-differential of u, and write $d_W u$, or du for short.

It is easily verified that $du + dv = d(u + v)$, u and $v \in \mathfrak{M}$. Moreover if $\tilde{\lambda} \in \mathcal{F}(W)$ then $\tilde{\lambda}(du) = d(\lambda u)$ as $u \in \mathfrak{M}$ implies $\tilde{u} d\lambda = 0$. Consequently these ordered n-tuples form a vector space (over $\mathcal{F}(W)$) which we denote by D(W).

Given $u \in \mathfrak{M}(W/S_n)$ we can associate with τu, its $\mathfrak{M}^2$-residue in $M(W/S_n)$ the local W-differential of u viz.

$$\tau u \to du \tag{5a}$$

This mapping is well-defined, for if $\tau u = \tau u'$ i.e. $u - u' \in \mathfrak{M}^2$ then $du - du' = d(u - u') = d(\sum pq) = \sum d(pq) = \sum p.dq + \sum dp.q = 0$ $(p, q \in \mathfrak{M})$. Also this mapping is a linear transformation of $M(W/S_n)$ onto D(W) and so

LEMMA 3. The dimension of D(W) is at most $n - \rho$, and equals $n - \rho$ only if (5a) is non-singular.

Proof. In the corollary to Proposition 1 we saw that $\dim M(W/S_n) = n - \rho$.

§6. The Jacobian criterion for simple points in the separable case.

As a preliminary we establish

LEMMA 4. The zero manifold $I(\alpha)$ of the point α can be generated by n polynomials $f_1, \ldots, f_n$ such that f_i contains only $X_1, \ldots, X_i$.

Proof. For $n = 1$ the result is trivial.

Let $f_1(X_1)$ be the irreducible polynomial in $k[X_1]$ such that $f_1(\alpha_1) = 0$. The residue class ring $k[X_1, \ldots, X_n]/f_1(X_1)$ is just the polynomial ring $k^*[X_2, \ldots, X_n]$ where $k^* = k(\alpha_1)$, and $I(\alpha)/f_1(X_1)$ is the zero manifold of $(\alpha_2, \ldots, \alpha_n)$ over k^*.

Assuming the result true for $n - 1$, $I(\alpha_2, \ldots, \alpha_n)$ can be generated by $f_2^*, \ldots, f_n^*$ such that f_i^* involves only $X_2, \ldots, X_i$. Therefore $I(\alpha)$ is generated by $f_1(X_1), f_2(X_1, X_2), \ldots, f_n(\underline{X})$ if f_i has f_1 - residue f_i^*.

Using this particular basis we can now prove

THEOREM 6.1. The space $D(\alpha)$ of local α-differentials has dimension n if and only if $\alpha_1, \ldots, \alpha_n$ are all seperable over k.

Proof. The polynomials $f_1, \ldots, f_n$ of Lemma 4 form a minimal basis of $\mathfrak{M}(\alpha/S_n)$ (any basis must have at least n elements) and so $\tau f_1, \ldots, \tau f_n$ are independent vectors in $M(\alpha/S_n)$. Thus by Lemma 3 dim $D(\alpha) = n$ if and only if $df_1, \ldots, df_n$ are independent, which is the case if and only if the Jacobian determinant $\left|\partial(f_1, \ldots, f_n)/\partial(X_1, \ldots, X_n)\right|_{X=\alpha}$ is non-zero.

Now by the choice of f_i this determinant is $\prod_{i=1}^{n}\left(\frac{\partial f_i}{\partial X_i}\right)_{X=\alpha}$.

Since $f_1(\alpha_1) = 0$ the first factor $\frac{\partial f_1}{\partial X_1} : X_1 = \alpha_1$ is non-zero if and only if α_1 is seperable over k. Similarly the second factor is non-zero if and only if α_2 is seperable over $k(\alpha_1)$. Both factors are thus non-zero if and only if α_1 and α_2 are seperable over k. Continuing in this way we find the necessary and sufficient condition as stated.

We now come to the classical criterion for simple points (in the seperable case)

THEOREM 6.2. <u>Let $I(V)$ have a basis of polynomials g_i. The point α is simple for V if and only if</u> $\left[\dfrac{\partial g_i}{\partial X_j}\right]_{X=\alpha}$ <u>has rank</u> $n - r$. $(r = \dim V)$

<u>Proof</u>. By Proposition 2, α is simple for V if and only if $n - r$ of the vectors τg_i are independent.

Theorem 6.1 and Lemma 3 show this holds if and only if $n - r$ of the local α -differentials dg_i are linearily independent in $D(\alpha)$, which is the condition on rank given above.

COROLLARY. <u>When k has characteristic 0, or is a perfect field, the classical criterion and the condition</u> $\dim M(\alpha/V) = r$ <u>coincide</u>.

For any field k, and whether or not $\alpha_1, \dots, \alpha_n$ are seperable, we have that rank $\left[\dfrac{\partial g_i}{\partial X_j}\right]_{X=\alpha} = n - r$ implies that α is a simple point of V. To see this we need only remark that if $n - r$ of the dg_i are independent then the corresponding $n - r$ vectors τg_i are independent.

These results may be extended to simple subvarieties e.g. the Jacobian criterion becomes: Provided $k(\eta_1, \dots, \eta_n)$ is seperably generated over k, W is simple for V if and only if the matrix $\left[\dfrac{\partial g_i}{\partial X_j}\right]$ has rank $n - r$ at η.

REFERENCES

[1] W. Krull - Dimensionstheorie in Stellenring, J.Reine Angew., Math.vol.179 (1938),pp.204-226.

[2] S. Lang - Introduction to Algebraic Geometry, Interscience Publishers Inc., lemma on p.33.

[3] D. G. Northcott - Ideal Theory, Cambridge No.41 (1953), Corollary 1 on p.65.

[4] O. Zariski - The concept of a simple point on an abstract algebraic variety, Trans.Amer.Math.Soc.vol.62 (1947).

[5] O. Zariski & P. Samuel - Commutative Algebra, D. Van Nostrand, Volumes I & II.