1962

Ideals varieties and valuations

Richard Joseph Konesky
The University of Montana

IDEALS, VARIETIES, AND VALUATIONS

by

RICHARD JOSEPH KONESKY

B.S. College of Great Falls, 1960

Presented in partial fulfillment of the requirements for the degree of

Master of Arts

MONTANA STATE UNIVERSITY

1962

Approved:

William R. Ballard
Chairman, Board of Examiners

Frank C. Abbott
Dean, Graduate School

AUG 1 4 1962
Date

ACKNOWLEDGEMENTS

I wish to express my appreciation to Professor William Ballard for his patience, valuable guidance, and encouragement given throughout the writing of this thesis. Also, I wish to thank Professor Arthur E. Livingston and Merle Manis for their critical reading of the thesis and Professor Hashisaki for his help and encouragement during the research period.

TABLE OF CONTENTS

INTRODUCTION

As the title implies, this thesis deals mainly with varieties and valuations, with some of the results applied to ideal theory. The reader should have a certain amount of familiarity with the basic concepts of modern algebra. Definitions of the standard notions not given in the thesis are presented here. The elements $x_1, \ldots x_n$ are <u>algebraically, independent</u> over a subring A of a ring R if and only if each x_k, $k = 1, 2, \ldots, n$ is transcendental over $A[x_1, x_2, \ldots, x_{k-1}]$. If K is an extension field of a field k and L is a subset of K, then the elements of L are said to be algebraically independent over k if each finite subset of L consists of elements which are algebraically independent over k. Such a set L is called a <u>transcendence set</u> over k. A transcendence set L in K is called a <u>transcendence basis</u> of K over k if it is maximal, i.e., if L is not a proper subset of another transcendence set. The common cardinal of the various transcendence bases of K over k is called the <u>degree of transcendency</u> of K over k. A field k is said to be <u>algebraically closed</u> if it possesses no proper algebraic extensions or also if every polynomial expression with coefficients in k has roots in k. If k is a subfield of a field K, then K is said to be an <u>algebraic closure</u> of k if (1) K is an algebraic extension of k and (2) K is an algebraically closed field. An irreducible polynomial f(X) in k[X] is <u>separable</u> or <u>inseparable</u> according as $f'(X) \neq 0$ or $f'(X) = 0$, where $f'(X)$ denotes the deriative of f(X). An arbitrary polynomial f(X) in k[X] is separable if all its irreducible factors are separable; otherwise f(X) is inseparable. Two elements x and y of one and the same extension field k of k are <u>conjugate</u> over k if they are algebraic over k and have the same minimal polynomial over k. Let K be a finite algebraic extension of the field k, of degree n, and let x be any element of K. Let $X^n+a_1X^{n-1}+\ldots+a_n$ be a monic irreducible polynominal over k satisfied by x. Then the <u>norm</u> of x relative to K over k, denoted by $N_{K/k}(x)$, is $(-1)^n a_n$. If $f(X) = \prod_{i=1}^{n} (X-x_i)$ then the norm of x is $\prod_{i=1}^{n} x_i$ and if x is separable over k, then $x_1, x_2, \ldots, x_n$ are distinct and the norm is equal to the product of the conjugates of x.

Chapter I introduces the concept of the variety and derives of its properties and also gives its relationship to prime ideals. The second chapter deals with valuations, valuation rings, and places with the main theorem being the extension theorem of a homomorphism to a place. This play a fundamental role in the development of algebraic geometry. The third chapter deals with a theorem of I. N. Herstein concerning three fields. In the development of this theorem, an existence lemma in valuation theory is used which is proved prior to the theorem.

CHAPTER I

BASIC CONCEPTS OF ALGEBRAIC GEOMETRY

SECTION I

INTRODUCTORY CONCEPTS OF ALGEBRAIC GEOMETRY

This chapter concerns the solutions $(x_1, \dots x_n)$ common to certain polynomial equations: $f_i(X_1, \dots, X_n) = o$ for $i = 1, 2, \dots, r$. In general the coefficients will belong to an arbitrary commutative field which will be denoted by k. In answer to the question, "In what domain do the solutions lie?", the components of the solutions are taken from the universal domain Ω, where Ω is an extension field of k such that:

1. The degree of transcendency of Ω/k is infinite and
2. Ω is algebraically closed.

The first theorem will show that any finitely generated extension field of k can be "taken care of" in Ω. Thus

Theorem 1.1 Let k be a field such that $k \subset E$ and let $E = k(a_1, \dots, a_r)$. Then there exists an isomorphism $\sigma : E \to \Omega$ which is the identity map on k.

Proof: Let $k_{r-1} = k(a_1, \dots a_{r-1})$ and let $k_o = k$. Then $E = k_r = k_{r-1}(a_r)$.

The proof is by induction. For $r = o$, the statement is trivial. Suppose it is true for extensions generated by fewer than r quantities. Then there exists an isomorphism $\sigma_{r-1}: k_{r-1} \to k'_{r-1} \subset \Omega$ which is the identity on k. There are two cases to consider: (1) a_r is transcendental over k_{r-1}, (2) a_r is algebraic over k_{r-1}. In the first case, select in Ω an element b_r which is transcendental over k_{r-1}. This can be done because of the infinite degree of transcendency of Ω over k. Now extend σ_{r-1} to E by mapping a_r onto b_r and this extension is an isomorphism leaving k fixed.

In the second case, let P be the monic irreducible polynomial over k_{r-1} having a_r as a root. Let P' be the image of P in $k'_{r-1}[X]$. Choose b_r in Ω as a root of P', which can be done since Ω is algebraically closed. Extend the isomorphism σ_{r-1} to an isomorphism of E into Ω leaving k fixed by mapping a_r onto b_r.

A zero of an ideal $A \subset k(X_1, \ldots, X_n)$ is an n-tuple $(\eta_1, \ldots, \eta_n) \in \Omega^n$ of elements in an extension field of k such that $f(\eta_1, \ldots, \eta_n) = 0$ whenever $f \equiv 0 \bmod (A)$. If A is an ideal of $k[X]$, then the set of zeros of A is called an <u>algebraic set</u> over k. It is also said that A defines an algebraic set over k. $A \to S$ will be used to designate that an ideal A defines an algebraic set S. Immediate consequences of this definition are: (1) S is the empty set when $A = k[X]$ ano (2) $S = \Omega^n$ (the n-fold Cartesian product of Ω), when $A = \{0\}$. It may also be the case that different ideals define the same algebraic set; for instance, A and A^2 always have the same algebraic set V.

<u>Lemma 1.2</u> If A and B are ideals then $A \subset B$ implies that $V \supset W$ where $A \to V$ and $B \to W$.

<u>Proof:</u> The proof is immediate from the previous discussion.

<u>Theorem 1.3</u> If A and B are ideals, and if $A \to V$ and $B \to W$ then $V \cup W$ and $V \cap W$ are algebraic sets such that $A + B \to V \cap W$, $A\,B \to V \cup W$, and $A \cap B \to V \cup W$.

<u>Proof:</u> That $A + B \to V \cap W$ is immediate. For the other part, let $A \cap B \to S$, and $AB \to R$. Since $A \cap B \subset A$ and $A \cap B \subset B$, $S \supset V$ and $S \supset W$, by Lemma is 1.2.

Thus $S \supset V \cup W$. To show that any zero of AB is in $V \cup W$, let $(x) = (x_1,\ldots,x_n)$ be a zero of AB and suppose (x) is not in V. By assumption, (x) is not a zero of A, so there exists an $f(X)$ in A such that $f(x) \neq 0$. Let $g(X)$ be any element of B; then $f(X)g(X)$ is in AB. Since $x \in S$, $f(x)g(x) = 0$, and this implies that $f(x) = 0$; i.e., (x) is in W. Finally, note that $AB \subset A \cap B$ so that $R \supset S$. Since any zero of AB is in $V \cup W$ and $S \supset V \cup W$, $V \cup W \supset R \supset S \supset V \cup W$, that is, $R = S = V \cup W$.

SECTION II

VARIETIES AND GENERIC POINTS

The set A is a <u>proper union</u> of the sets $A_1,\ldots,A_n$ in case $A = \bigcup_{i=1}^{n} A_i$ but $A \neq A_i$ for any i. In algebraic set V is called a <u>variety</u> if V is not a proper union of a finite number of algebraic sets.

<u>Theorem 1.4</u> Let S be any set Ω^n. With S, associate a subset A of $k[X]$ defined as: $A = \{f(X) \in k[X] \mid f(x) = 0 \text{ for all } x \in S\}$; then (1) is an ideal and (2) If S is an algebraic set defined by an ideal A_o in $k[X]$ then the ideal A of S is the maximal ideal defining S.

<u>Proof:</u> (1) A is certainly an ideal since the set is closed under subtraction and also under multiplication by elements of $k[X]$.

(2) $A_o \subset A$ since, for $A_o \longrightarrow S$, if $f \in A_o$, then $f(x) = 0$ for all $x \in S$, so that $f \in A$. Let $A \longrightarrow R$. Since $A_o \subset A$, $S \supset R$. But $R \supset S$ by the definition of A. Thus $R = S$, and A is the maximal ideal defining S.

The following discussion is restricted to maximal ideals, and the association between the algebraic set S and a maximal ideal A is denoted by $S \longrightarrow A$. The notation $f(V) = 0$ means if $x \in V$ the $f(x) = 0$.

Lemma 1.5 Let V, W be algebraic sets and let A, B be the maximal ideals defining V and W respectively. Then $V \supset W$ implies $A \subset B$.

Proof: If $f \in A$, then $f(V) = 0$ and $f(W) = 0$; consequently $f \in B$.

A ring R is said to satisfy the ascending chain conditions if each sequence of ideals $A_1, A_2, \ldots$ in R such that $A_1 \subset A_2 \subset \ldots$, has only a finite number of distinct terms. If a ring satisfies the ascending chain condition and is commutative then it is called Noetherian. Observe that since $k[X]$ is Noetherian, every descending chain of algebraic sets "breaks off" so that every non-empty collection of algebraic sets has a minimal element.

Theorem 1.6 Any non-empty algebraic set is the union of a finite number of varieties.

Proof: Consider the set Σ of all algebraic sets which do not satisfy the theorem. It will be shown that $\Sigma = \phi$. Assume Σ is not empty and let V be a minimal element of Σ, $V \neq \phi$. By definition V is not a variety. Thus $V = U \cup W$ where U, W are algebraic sets and $U \neq V$, $U \neq V$. From the choice of V it follows that $U \notin \Sigma$, $W \notin \Sigma$. Thus U is a finite union of varieties and similarly for W. Consequently, V is a finite union of varieties (since $V = U \cup W$); hence $V \notin \Sigma$, which is a contradiction so $\Sigma = \phi$.

Lemma 1.7 Let U be a variety and V be an algebraic set with the representation $V = W_1 \cup W_2 \cup \ldots \cup W_r$ If the $U \subset V$ then there exists an integer i such that $U \subset W_i$. (If the assumptions that $W_i \not\subset W_j$ for $i \neq j$ and that the W_j are varieties is added, then the representation $V = W_1 \cup W_2 \cup \ldots \cup W_r$ is unique.)

Proof: $U = U \cap V = \left[(U \cap W_1) \cup (U \cap W_2) \cup \ldots \cup (V \cap W_r)\right]$. Since the class of algebraic sets is closed under union and intersection, the representation yields: Variety U = union of at least two algebraic sets. The union cannot be proper, so that there exists an integer i such that $U = U \cap W_i$; thus $U \subset W_i$.

Suppose $V = U_1 \cup U_2 \cup \ldots \cup U_s$ where U_i is a variety and $U_i \not\subset U_j$; for $i \neq j$. Since $U_i \subset V$, from above there exists an integer j such that $U_i \subset W_j$ and similarly there exists an integer r such that $W_j \subset U_r$ so that $U_i \subset W_j \subset U_r$ and by assumption i = r so that $U_i = W_j$. Thus each U_i occurs among the W_j's and likewise each W_i occurs among the U_i's. This shows the uniqueness.

Theorem 1.8 If V is a variety, then $V \twoheadrightarrow P$, where P is a prime ideal.

Proof: Suppose P is not a prime ideal. Then there exist a, b in $k[X] = \mathcal{O}$ such that $ab \in P$ and $a \notin P$, $b \notin P$. Set $A = P + a\mathcal{O}$. Then $A \supset P$ properly since $A \not\subset P$ and $A \twoheadrightarrow U \subset V$ and the inclusion is proper, since P is the maximal ideal defining V. Similarly, set $B = P + b\mathcal{O}$. Then $B \supset P$ properly and $B \twoheadrightarrow W \subset V$ where again the inclusion is proper. Thus $U \cup W \subset V$. Now $AB = (P + a\mathcal{O})(P + b\mathcal{O}) = P^2 + aP + bP + ab\mathcal{O}$ so $AB \subset P$, but $AB \twoheadrightarrow U \cup W$ and thus $U \cup W \supset V$. Hence, $V = U \cup W$, where $U \subset V$ and $W \subset V$ properly, contradicting the assumption that V is a variety.

The next two results establish the fact that the varieties and prime ideals are in one-to-one correspondence.

Theroem 1.9 Any prime ideal P determines a variety which, in turn, determines the given ideal P.

Proof: Suppose that P is a given prime ideal defining an algebraic set V. If $P = k[X] = \mathcal{O}$ then the algebraic set is the variety ϕ. Assume $P \neq \mathcal{O}$.

Let α denote the natural map of $\mathcal{O}$ onto $\mathcal{O}/P$. Sine $\mathcal{O}/P$ is an integral domain, its quotient field $\bar{K}$ may be formed. Let β denote the identity isomorphism of $\mathcal{O}/P$ into $\bar{K}$. Now consider $\alpha | k$, the restriction of α to k. This gives a homomorphism of k, and is therefore either trivial or an isomorphism. Since $\mathcal{O} \neq P$, $1 \notin P$ and thus 1 does not map into 0 under α. Hence $\alpha | k$ is not trivial but is an isomorphism of k into $\mathcal{O} / P$. Let $\bar{k}$ denote the image of k under $\alpha | k$, so $\bar{k} \cong k$. Finally, let $X = (X_1, \ldots, X_n)$ go into $(\bar{x})$ where $(\bar{x}) = (\bar{x}_1, \ldots, \bar{x}_n)$ and where $X_i \alpha = x_i$ for each i. Then $\mathcal{O}/p = \bar{k} [\bar{x}]$, so $\bar{K} = \bar{k}(\bar{x})$. Now by the properties of the universal domain, there exists an $(x) \in \Omega$ such that the map γ: $\bar{k}(\bar{x}) \longrightarrow k(x)$ is an isomorphism. γ is called the realization in Ω. The sequence of maps $k[X] \xrightarrow{\alpha} \bar{k}[\bar{x}] \xrightarrow{\beta} \bar{k}(\bar{x}) \xrightarrow{\gamma} k(x)$ gives a homomorphism of $k[X]$ onto $k(x)$ whose kernel is P, so $(x) \in V$.

Now consider the set consisting of the one point (x). From above $(x) \rightarrow P$. Let $V \rightarrow A$. Since $(x) \in V$, $P \supset A$,; but A is the maximal ideal which can define V, so that $A \supset P$, whence $A = P$.

It is shown next that the algebraic set V is a variety. Suppose $V = U \cup W$ where U, W are algebraic sets such that $A \rightarrow U$ and $B \rightarrow W$. Then $AB \rightarrow U \cup W = V$ so $AB \subset P$ since P is the maximal ideal defining V. Now if $A \not\subset P$, then there exists an $a \in A$ such that $a \notin P$, but $ab \in P$ for any $b \in B$, implying $B \subset P$. Thus either $A \subset P$ or $B \subset P$. Hence either $U \supset V$ or $W \supset V$. Therefore either $U = V$ or $W = V$, so V is a variety.

This discussion and theorem 1.8 establish:

<u>Theorem 1.10</u> The varieties of Ω are in one to one correspondence with the prime ideals of $k[x]$.

Let V be a non-empty variety determined by the prime ideal P. Let $(x) \in V$. (x) is called a <u>generic point</u> of V if the ideal determined by the set consisting of just (x) is P, that is, $(x) \to P \to V$.

Some of the properties of the generic point are : (1) If (x) is a generic point of the variety V, then V is the smallest algebraic set containing (x). This is the case since if (x) is in a algebraic set W and $A \to W$, then (x) is a zero of the ideal A. This implies that $A \subset P$ and $W \supset V$. (2) Any point is a generic point of some variety. This is the case since if (x) is any point in Ω^2 and P is the ideal defined by the set consisting of one point, then $P \neq \mathcal{O}$ since 1 does not vanish for (x). Furthermore, P is a prime ideal; for suppose $f(X)\ g(X) \in P$. Then $f(x)$ $g(x) = 0$ so $g(x) \in P$. Thus P is a prime ideal not equal to $\mathcal{O}$, but P defines a variety, and (x) is a point of this variety. (x) satisfies the conditions of the definition so it is a generic point of the variety V.

Some examples to illustrate these concepts follow. Let $k = Q$, the field of rational numbers, and let Ω be the complex numbers. The varieties in Ω^2 will be determined for which the following points are generic points: (o,o), $(\sqrt{2},1)$, (e,e), $(e,e^{\sqrt{2}})$.

(1) (o,o). The prime ideal P consists of those polynomials of $\mathcal{O}$ with constant term zero, and (o,o) is the generic point of the variety consisting of the single point (o,o). If any point (r_1,r_2) of Q^2 had been considered, then the variety of this point is just the set $\{(r_1,r_2)\}$.

(2) $(\sqrt{2},1)$. The prime ideal $P = (x_1{}^2-z)\mathcal{O} + (x_2-1)\mathcal{O}$, so with the generic point $(\sqrt{2},1)$ is associated the variety $\{(\sqrt{2},1), (-\sqrt{2},1)\}$. Here $(-\sqrt{2},1)$ is also generic point of the variety.

(3) (e,e). Consider here those $f(x_1,x_2) \in \mathcal{O}$ for which $f(e,e) = 0$ The prime ideal is the principal ideal generated by $x_1 - x_2$ and the variety of which (e,e) is a generic point is $\{(x_1,x_2) \mid x_1 = x_2\}$.

(4) $(e, e^{\sqrt{2}})$. The elements e and $e^{\sqrt{2}}$ being independent transcendental elements (as is assumed here), the corresponding prime ideal P is $\{0\}$. It has been shown that $\{0\}$ defines the variety Ω^2. Here then $(e,e^{\sqrt{2}})$ is a generic point of Ω^2, and thus Ω^2 is the minimal algebraic set containing $(e,e^{\sqrt{2}})$.

These examples also illustrate what is meant by dimension. Let V be a variety and let (x) be a generic point. Then the <u>dimension</u> of V is: dim V = $[k(x):k]_t$, (degree of transcendency of k(x) over k); dim (x) is also written for dim V. In the above examples, the dimensions are 0,0,1, and 2, respectively.

Next a relation of the other points of a variety to a generic point is given. Let V be a variety and (x) a point of V. Consider the map $\eta : k[X] \to k(x)$ where η is identity on k and takes X into x. By theorem 1.9, η is a homomorphism with kernel P. Let $(z) \in \Omega^n$ and consider the map α: $k[x] \to k[x]$, i.e., $a\alpha = a$ for all a in k and $x\alpha = z$. If this map α is well-defined than it surely is a homomorphism. It must be the case if $g(x) = f(z)$ then $f(z) = g(z)$, or it will suffice to have $f(x) = 0$ implying $f(z) = 0$ If $f(x) = 0$ this means that $f(X) \in P$, so that α is well-defined if an only if $P[z] = 0$. The map α is then well-defined and is a homomorphism for all $(y) \in V$. Thus (x) is a generic point of the set of points of the variety for which the map α is well-defined and a homomorphism. This relation is called a <u>specialization</u>. (y) is a specialization of (x), written $(x) \to (y)$ in case the map α is well-defined and a homomorphism. Note also that $(x) \to (y)$ if and only if $f(x) = 0$ implies that $f(y) = 0$

Theorem 1.11 The relation $(x) \to (y)$ is transitive; i.e., $(x) \to (y)$ and $(y) \to (z)$ implies $(x) \to (z)$.

Proof: Let $f(x)$ be a polynomial such that x is a root. Since $(x) \to (y)$ y is also a root. Similarly, z is a root, and so $(x) \to (z)$.

Two points will be called equivalent if they are generic points of the same variety and each is a specialization of the other.

Theorem 1.12 dim V is independent of the choice of the generic point.

Proof: For any two generic points (x) and (y) of V, $(x) \to (y)$ and $(y) \to (x)$. Consequently, $k[x] \cong k[y]$ and $k(x) \cong k(y)$. If the degree of transcendency is then computed with (x) and with (y), the same result is obtained.

One also speaks of a subvariety W of the variety V. This means W is a variety itself and is a subset of V. The following connections between a variety and a subvariety hold.

Theorem 1.13 Any point of the variety V can be considered as a generic point of a subvariety.

Proof: Let (x) define V and let $(y) \in V$. The (y) defines W, a subvariety. For $(x) \to (y)$, and the specializations $(y) \to (z)$ define the points (z) of W; from theorem 1.11, these are points of V.

Theorem 1.14 Let V, W be varieties such that $W \subset V$. Then $\dim W \leq \dim V$, and if $\dim W = \dim V$, then $W = V$.

Proof: Let $(x) = (x_1, x_2, \ldots, x_n)$ be a generic point of V and let $(y) = (y_1, y_2, \ldots, y_n)$ be a generic point of W. Then the map $\varphi: k[x] \to k[y]$ defined as $a\varphi = a$ for all $a \in k$ and $x\varphi = y$ is well-defined. Suppose dim W = r. There is no loss in generality in assuming that $y_1, y_2, \ldots, y_r$ are algebraically independent elements over k. Then $x_1, x_2, \ldots x_r$ are algebraically independent. For if this is not the case, some polynomial $f(x_1, \ldots, x_n) = 0$. where f has some non-zero coefficients in k. Since φ is well-defined, $f(y_1, y_2, \ldots, y_r) = 0$, which is a contradiction; thus dim V $\geq$ r. Assume now that dim V = r. It is desired to show that φ is an isomorphism. Let $z \in k[x]$ and $z \neq 0$. Assume that z is in the kernel of φ. z is algebraically dependent on $x_1, x_2, \ldots, x_r$ since dim V = r. Thus $a_s(x_1 \ldots x_r)z^s + \ldots + a_o(x_1 \ldots x_r) = 0$ where each $a_i(x_1, x_2, \ldots x_r)$ is a polynomial with coefficients in k, and not all the a_i are zero. If it is assumed that s is the minimal degree for all such equations satisfied by z, than $a_o(x_1, x_2 \ldots x_r) \neq 0$. If φ is applied to the above equation $a_o(y_1, y_2, \ldots y_r) = 0$, since z is in the kernel of φ, which contradicts the assumption that $y_1, y_2, \ldots y_r$ are algebraically independent. Hence the kernel in 0, so both (x) and (y) are generic points of V; thus W = V.

Consider now the following:

(1) dim V = $\max_{(x) \in V}$ dim (x), where for any $(x) \in V$, dim (x) = $[k(x):k]_{t_r}$.

(2) Since $0 \leq$ dim V $\leq$ n, consider the following three cases:

(a) <u>dim V = n.</u> Let (x) be a generic point of V. Then $x_1, x_2, \ldots, x_r$ must be algebraically independent. Therefore any $(y) \in \Omega^n$ is a specialization of (x) since no polynomial relation can hold in $k[x]$ and in this case $V = \Omega^n$. Thus Ω^n has dimension n and any proper sub-variety will have dimension less than n.

(b) <u>dim V = 0.</u> Here (x) is algebraic, i. e., each x_i is algebraic over k. Let (y) be a specialization of (x). As previously, then, (y) is a generic point of a subvariety, say W, where $W \subset V$. Then $0 = \dim V \geqq \dim W$, so $\dim W = 0$ and, by theorem 1.14, $V = W$. Hence (y) and (x) are equivalent and every specialization is also. If $(x) \rightarrow (y)$, then $k[x] \cong k[y]$. However in this case $k(x) \cong k(y)$ because:

1. Let each x_i be algebraic over k. Suppose n_i is the degree of x_i over k. $k[x]$ is spanned by the totality of products of powers of $x_1, x_2, \ldots, x_n$, where the power of x_i is at most $n_i - 1$. Thus $k[x]$ is a finite dimensional vector space over k.

2. $k[x]$ is an integral domain since k is an integral domain.

3. A finite dimensional vector space over a field which is an integral domain is a field. For suppose R is a finite dimensional vector space over a field and R is an integral domain and $a \neq 0$, $a \in R$, and consider the map $x \rightarrow ax$ for all $x \in R$. This is an isomorphism of R into R which preserves dimension, so is onto. Thus the equation $ax = b$, where $a, b \in R$ always has a unique solution x in R.

Combining 1, 2, and 3 $k[x] = k(x)$ and the specializations of (x) are those $(y) \in \Omega$ such that $k(x) \cong k(y)$. When $\dim V = 0$, V has as many points as there are isomorphisms of $k(x)$ over k. If all x_i are separable, then the number of points equals the degree of $k(x)$ over k.

(3) <u>dim V = n-1</u>. First of all, the varieties of dimension n-1 are in one to one correspondence with certain prime ideals. Thus $V \leftrightarrow P$ where $P \neq \{0\}$ since $V \neq \Omega$. Let $f \in P$. Since $\mathcal{O} = k[x]$ is a unique factorization domain, f factors uniquely into a product of irreducible polynomials except for arrangement and units. If $f \in P$ then there exists an irreducible, non-constant polynomial $Q \in P$, since P is prime. Sine $\mathcal{O}$ is a unique

factorization domain, $Q\mathcal{O} = P_0$ is a prime ideal. Let $P_0 \longrightarrow V_0$. Since $P_0 \subset P$, $V_0 \supset V$, so that dim $V_0 \geq$ n-1. $P_0 \neq \{0\}$ so $V_0 \neq \Omega^n$ and dim $V_0 \leq$ n-1 and therefore dim V_0 = n-1, $V = V_0$ and $P = Q\mathcal{O}$. Thus any (n-1)-dimensional variety is defined by the zeros of a prime ideal generated by a non-constant, irreducible polynomial.

If Q is a non-constant irreducible polynomial, then $P = Q\mathcal{O}$ is a prime ideal. Let V be the variety determined by P. Since $V \neq \Omega^n$, dim $V \leq$ n-1. If one point of V is exhibited with dimension n-1 then dim V = n-1. Since Q is non-constant, it must depend on at least one variable, say x_n. Choose $x_1, x_2, \ldots, x_{n-1}$ in the universal domain, algebraically independent, and solve in Ω the equation $Q(x_1, x_2, \ldots, x_{n-1}, x_n) = 0$. Call this solution x_n. Thus $(x) = (x_1, x_2, \ldots, x_n)$ is a zero of Q, by construction, hence a zero of P, so that $(x) \in V$ and dim (x) = n-1 by construction. Thus the variety determined by a prime ideal generated by an irreducible polynomial is of dimension n-1. The prime ideal is unique and if $f_1\mathcal{O}$ and $f_2\mathcal{O}$ (f_1, f_2 irreducible) are representations for this prime ideal, then f_1 and f_2 differ by a constant factor.

As a matter of terminology one-dimensional varieties are called <u>curves</u>, two-dimensional varieties are called <u>surfaces</u>, and (n-1)-dimensional varieties are called <u>hypersurfaces</u>.

SECTION III

PRODUCTS OF ALGEBRAIC SETS

First the product of two algebraic sets is defined. Let $V \subset \Omega^n$ and $W \subset \Omega^m$ be algebraic sets. The subset V x W of Ω^{n+m} obtained by taking all points (x,y) where $(x) \in V$ and $(y) \in W$ is called the product of the algebraic sets V and W. This is the usual Cartesian product.

Theorem 1.15 $V \times W$ is an algebraic set.

Proof: Suppose $A \twoheadrightarrow V$ where A is an ideal of $k[X]$ and suppose $B \twoheadrightarrow W$ where B is an ideal of $k[Y]$. Set $\mathfrak{o} = k[X,Y]$ and let $D = A\mathfrak{o} + B\mathfrak{o}$. It will be shown that the ideal D of $\mathfrak{o}$ determines $V \times W$. Let (x,y) be a zero of A; then (x,y) must be a zero of $A\mathfrak{o}$. Thus (x) must be a zero of A since $A\mathfrak{o}$ does not depend on Y. Similarly, (y) is a zero of B, so that any zero of D is of the form (x,y) where $(x) \in V$ and $(y) \in W$. Hence the zeros of D belong to $V \times W$. On the other hand, if $(x,y) \in V \times W$ then (x,y) is a zero of D. Thus $V \times W$ is an algebraic set defined by D.

The following example shows that if V and W are varieties then $V \times W$ need not be a variety. Let $k = Q$, the rational numbers and let $\Omega = c$, the complex numbers. Consider the variety $V = \{(\sqrt{2}), (-\sqrt{2})\}$. Then $V \times V = \{(\sqrt{2},\sqrt{2}), (-\sqrt{2},\sqrt{2}), (-\sqrt{2},-\sqrt{2})\}$. This can be written as the union of two varieties: $V \times V = \{(\sqrt{2},\sqrt{2}), (-\sqrt{2},-\sqrt{2})\} \cup \{(\sqrt{2},-\sqrt{2}), (-\sqrt{2},\sqrt{2})\}$.

The dimension of an algebraic set is defined as the maximal dimension of its component varieties; equivalently, the dimension of the algebraic set V is $\max_{(x)\in V} \dim (x)$. From this we conclude that the dimension of a proper algebraic subset of the algebraic set V is not necessarily less than that of V.

Theorem 1.16 $\dim (V \times W) = \dim V + \dim W$.

Proof: Since $\dim (V \times W) = \max_{\substack{(x)\in V\\(y)\in W}} \dim(x,y)$, $\dim(V \times W) \leq \dim V + \dim W$.

Conversely, choose a point $(x) \varepsilon V$ with dim (x) = dim V, and a point $(y) \varepsilon W$ with dim (y) = dim W, such that the transcendence base of $k(y)$ is algebraically independent of that of $k(x)$. This can be done because of the properties of the universal domain. For these (x) and (y), dim (x,y) = dim V + dim W, so dim $(V \times W) \geq$ dim V + dim W. Thus dim $(V \times W)$ = dim V + dim W.

CHAPTER II

VALUATION RINGS, PLACES, AND VALUATION

SECTION I

INTRODUCTION

After laying the groundwork in Chapter I, the concepts of valuation rings, places, and valuations are now introduced. This builds up to the main theorem of this chapter, the extension theorem for places.

A subring $\mathcal{O}$ of a field K is called a valuation ring if for any $a \in K$, $a \notin \mathcal{O}$ implies that $a^{-1} \in \mathcal{O}$. An immediate consequence is $1 \in \mathcal{O}$, so a valuation ring is a ring with identity.

Consider first the set P of non-units of a valuation ring $\mathcal{O}$, i.e., $P = \{a \mid a \in \mathcal{O}, a^{-1} \notin \mathcal{O}\}$. Thus $a \in K$ and $a \notin P$ implies $a^{-1} \in \mathcal{O}$. Some of the properties of the set P are:

1. If $a+b \notin P$ then either $a \notin P$ or $b \notin P$. This is certainly true if either a or b is 0 so one may assume that $a \neq 0$, $b \neq 0$. Assume $a/b \in \mathcal{O}$ (if $\frac{a}{b} \notin \mathcal{O}$ then $\frac{b}{a} \in \mathcal{O}$ and the argument is analogous). Since $a+b \notin P$ and because $c \notin P$ implies $c^{-1} \in \mathcal{O}$, $(a+b)^{-1} \in \mathcal{O}$. Hence $b^{-1} = \left(1+\frac{a}{b}\right)(a+b)^{-1} \in \mathcal{O}$; that is, $b \notin P$.

2. If $a, b \in \mathcal{O}$ and $ab \notin P$ then neither a nor b belongs to P. For $ab \notin P$ implies $(ab)^{-1} \in \mathcal{O}$, and it follows that $a^{-1} = (ab)^{-1} b \in \mathcal{O}$. Thus $a \notin P$ and likewise $b \notin P$.

The contrapositives of these two results show that P is an ideal. The following theorem shows that it is a maximal ideal.

<u>Theorem 2.1</u> The non-units of a valuation ring $\mathcal{O}$ form a maximal ideal of P. Furthermore, $\mathcal{O}/P$ is a field and P is a prime ideal.

<u>Proof:</u> The above remarks show that P is an ideal. Also any proper ideal in $\mathcal{O}$ consists entirely of non-units, hence is contained in P; thus P is a maximal ideal. It follows at once that $\mathcal{O}/P$ is a field and P is a prime ideal.

If U denotes the set of units of $\mathcal{O}$ then clearly U is a multiplicative group. Consider then the decomposition of K as the disjoint union: $K = P \cup U \cup P^{(-1)}$, where $P^{(-1)}$ denotes the set of elements inverse to the non-zero elements of P. Since $P \cup U = \mathcal{O}$, it must be shown that $P^{(-1)}$ consists of the complement of $\mathcal{O}$ in K. This is the case, for if $a \notin \mathcal{O}$ then $a^{-1} \in \mathcal{O}$ but since $a^{-1} \notin U$, $a^{-1} \in P$ so that $a \in P^{(-1)}$. Now if $a \notin P^{(-1)}$ then $a^{-1} \in P$ and $a \in \mathcal{O}$. Thus $K = P \cup U \cup P^{(-1)}$, which shows that P determines the valuation ring $\mathcal{O}$. Since K may be written as this disjoint union, if $\mathcal{O}_1$ and $\mathcal{O}_2$ are two valuations rings of K with groups of units U_1 and U_2, and ideals of non- units P_1 and P_2, then $\mathcal{O}_1 \subset \mathcal{O}_2$ if and only if $P_1 \supset P_2$, which is the case and only if $U_1 \subset U_2$.

Let K and F be two arbitrary fields. Then a map $\varphi : K \to F \cup \{\infty\}$ is called a <u>place</u> if:

1. $\varphi^{-1}(F) = \mathcal{O}$ is a ring
2. $\varphi|\mathcal{O}$ is a non-trivial homomorphism, and
3. if $\varphi(a) = \infty$ $(a \notin \mathcal{O})$ then $\varphi(a^{-1}) = 0$,

where ∞ if a symbol adjoined to F.

Consider the following example of a place. Let F(x) be the field of rational functions in one variable over a field F. That is, each element of F(x) is a polynomial fraction in reduced form. If $a \in F$ is substituted for x, a map of $F(x)$ into $F \cup \{\infty\}$ is obtained. If, after the substitution, the denominator is zero, this element is mapped into ∞. Since the elements of $F(x)$ are in reduced form, the form $\frac{0}{0}$ does not occur. This map is well defined. It also satisfies the definition of a place since if $f, g \in F(x)$ have denominators not divisible by $x-a$ then the same is true for their sum and product so that condition 1. is satisfied. On $\mathcal{O}$ the map is a homomorphism, which is non-trivial since 1 does not go into 0, so condition 2 is satisfied. Condition 3 is certainly satisfied.

Consider now the valuation ring $\varphi^{-1}(F)$ associated with a place φ. Consider the non-units P of the valuation ring $\varphi^{-1}(F)$. Since $K = P \cup U \cup P^{(-1)}$, P consists of 0 and the inverses of elements not in $\mathcal{O}$. Thus $\varphi(P) = \{0\}$ so that P is in the kernel of φ. Suppose $\varphi(a) = 0$. If $a^{-1} \in \mathcal{O}$ then $\varphi(aa^{-1}) = \varphi(1) = \varphi(a)\varphi(a^{-1}) = 0$ so that $\varphi(1) = 0$ which implies that $\varphi(\mathcal{O}) = 0$, which contradicts condition 2 of the definition. Hence, $a^{-1} \notin \mathcal{O}$ so $\varphi(a^{-1}) = \infty$ or $a^{-1} \in P^{(-1)}$ and $a \in P$. Thus P is the kernel of φ on $\mathcal{O}$ and $\varphi(1) = 1$ from condition 2. Thus with a place is associated a valuation ring.

One can also start with a valuation ring $\mathcal{O}$ and associate with it a place φ. Let P be the ideal of non-units of $\mathcal{O}$ and define $\varphi(a) = \begin{cases} \infty & \text{if } a \notin \mathcal{O}. \\ a+P & \text{if } a \in \mathcal{O} \end{cases}$

That is, if $a \in \mathcal{O}$ we take the natural map so that $F = \mathcal{O}/P$. The claim is that this map φ is a place. By definition $\varphi^{-1}(F) = \mathcal{O}$, the given valuation ring, so that the first condition is satisfied. $\varphi/\mathcal{O}$ is a homomorphism and is non-trivial since $1 \notin P$. For condition 3, if $a \notin \mathcal{O}$ then $a^{-1} \in P$ since $K = P \cup U \cup P^{(-1)}$. Thus a given place determines a valuation ring, which in turn determines the given place φ, up to isomorphism of the field F.

Two places are said to be equivalent if they have the same valuation ring.

Before the introduction of the concept of a valuation, the definition of an ordered group is considered. A sub-semi-group S is called invariant if $a^{-1}Sa = S$ for every a in a group G. Let G be a multiplicative group. G is said to be ordered if it contains an invariant sub-semi-group S such that $G = S \cup \{1\} \cup S^{(-1)}$, where the union is disjoint. For a and b in an ordered group G, one defines $a < b$ to mean that $ab^{-1} \in S$. Thus $a < 1$ if and only if $a \in S$. Some of the properties of this relationship are:

1. $a < b$ if and only if $b^{-1}a \in S$. This is the case since $b^{-1}a = b^{-1}(ab^{-1})b$ so that if $ab^{-1} \in S$, then $b^{-1}a \in S$ because of the invariance of S; $ab^{-1} = b(b^{-1}a)b^{-1}$ gives the implication the other way.

2. From the decomposition of G, either (a) $ab^{-1} \in S$, (b) $ab^{-1} \in \{1\}$, or (c) $ab^{-1} \in S^{(-1)}$. That is, (a) $a < b$, (b) $a = b$, or (c) $b < a$ and the trichotomy law holds.

3. This relation is transitive, i.e., $a < b$ and $b < c$ implies $a < c$. If $ab^{-1} \in S$ and $bc^{-1} \in S$, by the semi-group property of S, $(ab^{-1})(bc^{-1}) = ac^{-1} \in S$, and $a < c$.

4. $a < b$ implies $ac < bc$. Here $ab^{-1} \in S$ so $acc^{-1}b^{-1} \in S$ and $ac < bc$. Similarly $ca < cb$ if $a < b$.

5. $a < b$ implies $b^{-1} < a^{-1}$. If $a < b$, applying property 4 twice gives $a^{-1}ab^{-1} < a^{-1}bb^{-1}$ and $b^{-1} < a^{-1}$

6. $a < b$ and $c < d$ implies $ac < bd$. Since $a < b$, $ac < bc$ by property 4. Similarly $bc < bd$ and $ac < bd$ by property 3.

There may or may not be an addition operation already defined in G. However, one may always define an operation + for an ordered group as $a+b = \max.(a,b)$. This definition gives a distributive law: $(a+b)c = ac+bc$. If $a \leq b$, then $ac \leq bc$ and $ac+bc = \max(ac,bc) = bc$ while $(a+b)c = [\max.(a,b)] \cdot c = bc$. If an element 0 is adjoined to G with the convention that $a \cdot 0 = 0$ and $0 < a$ for all $a \in G$, then $a+0 = a = 0+a$.

One can now define a valuation and relate it to valuation rings and places. A valuation of a field K is a map $|\cdot|: K \to G \cup \{0\}$ where G is an ordered group and $|\cdot|$ satisfies:

1. $|a| = 0$ if and only if $a = 0$,
2. $|ab| = |a| \cdot |b|$,
3. $|a+b| \leq |a| + |b|$

where $|\cdot|(a)$ is written $|a|$.

If addition in G is the maximum previously defined, then a valuation ring may be constructed from a valuation. Let $\mathcal{O} = \{a \mid a \in K, |a| \leq 1\}$ then $\mathcal{O}$ is a ring since if $|a| \leq 1$ and $|b| \leq 1$ then $|ab| = |a|\,|b| \leq 1$ and $|a+b| \leq \max.(|a|, |b|) \leq 1$. $\mathcal{O}$ is a valuation ring since if $a \notin \mathcal{O}$, then $|a| > 1$ so that $|a^{-1}| = |a|^{-1} < 1$ and $a^{-1} \in \mathcal{O}$. The non-units P of $\mathcal{O}$ are those $a \in \mathcal{O}$ such that $a^{-1} \notin \mathcal{O}$ so that $P = \{a \mid |a| < 1\}$ and the group of units is $U = \{a \mid |a| = 1\}$.

Next a valuation is obtained from a given valuation ring $\mathcal{O}$ in a field K, with maximal ideal P and group of units U. First, define for $a \in K$: $|a| = aU$. "$|\cdot|$" maps K onto $K^*/U \cup \{0\}$ where K^* is the multiplicative group $K - \{0\}$. If $G = K^*/U$ then G is an ordered group. In order to verify this, a sub-semi-group with the required properties must be exhibited. Define S as: $aU \in S$ if and only if all $aU \subset P$, i.e., if $a \in P$.

Now S is a semi-group and is invariant since K is a field. Since $K^* = (P-\{0\}) \cup U \cup (P-\{0\})^{(-1)}$ (disjoint), $G = K^*/U = S \cup \{1\} \cup S^{(-1)}$ (disjoint), so that G is an ordered group.

The map $|\cdot|$ is a valuation. It certainly satisfies the first two conditions. The third condition, $|a+b| \leq |a| + |b|$, is equivalent to $|a| \leq 1$ implying $|1+a| \leq 1+|a|$. For if $\left|\frac{a}{b}\right| \leq 1$ and this latter condition holds then $\left|1+\frac{a}{b}\right| \leq 1+ \left|\frac{a}{b}\right|$ and $|a+b| \leq |a| + |b|$; the implication the other way is obvious. If addition in G is the maximum addition, $|a| \leq 1$ implies $|1+a| \leq 1$. Suppose $aU = |a| \leq 1$; then $a \in \mathcal{O}$. In consequence $1+a \in \mathcal{O}$ so $|1+a| \leq 1$. Hence $|a| = aU$ is a valuation and its associated ring is the given one $\mathcal{O}$. Thus there is a one-to-one correspondence between valuations and valuation rings; previously a one-to-one correspondence between places and valuation rings was shown.

Consider next an example that illustrates the preceding discussion. Let $K = C(z)$ be the field of rational functions of a single complex variable. A place is obtained by substituting a complex number z_o for z. The valuation ring of this place is $\mathcal{O} = \left\{\frac{f(z)}{g(z)} \,\middle|\, g(z_o) \neq 0;\ f,\ g \in C(z)\right\}$. The maximal ideal of non-units is $P = \left\{\frac{f(z)}{g(z)} \,\middle|\, g(z_o) \neq 0,\ f(z_o) \neq 0,\right\}$ and the group of units $U = \left\{\frac{f(z)}{g(z)} \,\middle|\, g(z_o) \neq 0,\ f(z_o) \neq 0\right\}$. The valuation associated with this valuation ring is $|f(z)| = f(z)\,U$ where $f(z) \in C(z)$. Hence, $|f(z)| = (z-z_o)^n\,U$ for some integer n. Here n is called the order of the zero of f(z) at z_o where a negative n corresponds to a pole of order $-n$, and where $n = 0$ means that f(z) has no zero or pole at z_o. The ordered group G is simply a cyclic group generated by $(z-z_o)\,U$ and is isomorphic to Z, the additive group of integers. Also $|f(z)| < 1$ if and only if $(z-z_o)^n \in P$ which is the case if and only if $n > 0$; thus G has the reverse ordering of Z. Thus this place indicates whether a rational function approaches 0 or ∞ at z_0, while the valuation gives the order with which the function goes to 0 or ∞.

The position has now been reached to attack the fundamental extension theorem.

<u>Theorem 2.2</u> Let K be any field and $\mathcal{O}$ a subring of K. Let F be an algebraically closed field; suppose $\varphi : \mathcal{O} \to F$ is a non-trivial homomorphism. Then there exists a place φ^* of K such that $\varphi^* | \mathcal{O} = \varphi$. ($\varphi^*$ is not necessarily unique).

<u>Proof:</u> Two types of extensions will be considered. Let S consist of those elements $s \in \mathcal{O}$ such that $\varphi(s) \neq 0$. S forms a semi-group and $S \neq \phi$ since φ is non-trivial. Since $\mathcal{O}$ is a commutative ring and S a sub-semi-group which contains no divisors of zero, the quotient ring $\mathcal{O}' = \left\{\frac{a}{s} \middle| \ a \in \mathcal{O},\ s \in S\right\}$ is well defined. $\mathcal{O}'$ is a ring with identity.

Extend φ on $\mathcal{O}$ to φ' on $\mathcal{O}'$ by defining $\varphi'\left(\frac{a}{s}\right) = \varphi(a)/\varphi(s)$. φ' is well defined. If $\frac{a_1}{s_1} = \frac{a_2}{s_2}$ then $a_1s_2 = a_2s_1$ and, since φ is a homomorphism, $\varphi(a_1)\varphi(s_2) = \varphi(a_2)\varphi(s_1)$. $\varphi(s_1) \neq 0$, $\varphi(s_2) \neq 0$ since $s_1, s_2 \in S$ so, dividing, $\frac{\varphi(a_1)}{\varphi(s_1)} = \frac{\varphi(a_2)}{\varphi(s_2)}$ and φ' is well defined. φ' is a homomorphism because φ is. Now $\varphi' | \mathcal{O} = \varphi$ since each $a \in \mathcal{O}$ can be written as $\frac{as}{a}$ and $\varphi' \frac{as}{s} = \frac{\varphi(a)\varphi(s)}{\varphi(s)} = \varphi(a)$. Therefore φ' is an extension of φ and maps $\mathcal{O}'$ into F.

This may yield no extension at all if $\mathcal{O}$ is a subfield of K. Furthermore it is not an extension to K if K has a proper subfield containing $\mathcal{O}$. Thus it is necessary to show that if $\mathcal{O}$ is a subfield and $\alpha \in K$, then φ may be extended either to $\mathcal{O}[\alpha]$ or to $\mathcal{O}[\alpha^{-1}]$. This is the second type of extension. If $\mathcal{O}$ is a field and $\varphi(\mathcal{O}) = F_o < F$ then F_o is a field since φ is non-trivial. Let $\bar{a}$ denote the image of $a \in \mathcal{O}$ under φ. Extend φ to $\mathcal{O}[X]$, i.e., apply φ to the coefficients of each polynomial of $\mathcal{O}[X]$. The image of $P(X) \in \mathcal{O}[X]$ will be denoted by $\bar{P}(X)$. The image of $\mathcal{O}[X]$ is $F_o[X]$. Consider extending φ to ψ: $\mathcal{O}[\alpha] \longrightarrow F$ by defining $\psi(P(\alpha)) = \bar{P}(\beta)$ where β is any element of F. If ψ is well-defined it is a homomorphism, and is an extension of φ. Consider the question: Does $P(\alpha) = 0$ imply that $\bar{P}(\beta) = 0$? Let A be the set of all P(X) with $P(\alpha) = 0$. It is the kernel of the substitution may: $\mathcal{O}[X] \longrightarrow \mathcal{O}[\alpha]$. A is an ideal of $\mathcal{O}[X]$ so the question becomes: Is the image $\bar{A}$ in $F_o[X]$ of such a nature that $X = \beta$ is a zero of it? Since $\bar{A}$ is an ideal of $F_o[X]$, $\bar{A} = \bar{Q}(X) \cdot F_o[X]$ since $F_o[X]$ is a principal ideal domain. β must be selected as a zero of $\bar{Q}(X)$ and, since F is algebraically closed, such a β may be chosen, provided $\bar{Q}(X)$ is not a non-zero constant. In this case an extension to $\mathcal{O}[\alpha]$ is obtained. Consider next the possibility that $\bar{Q}(X)$ is a non-zero constant. Assume $\bar{Q}(X) = 1$. There is a $\bar{Q}(X) = 1+p_o+p_1X+\dots+p_rX^r$ where $\varphi(p_i) = 0$ for $i = 1,2,\dots,r$ and where $1+p_o+p_2\alpha+p_r\alpha^r = 0$. If α satisfies such an equation then the above construction does not work. It cannot, however, fail with both α and $\alpha^{-1} = \gamma$ as will be shown. Consequently, if the extension cannot be made to $\mathcal{O}(\alpha)$, it can be made to $\mathcal{O}(\gamma)$. To show this, suppose to the contrary that α, γ satisfy equations $1+p_o+p_1\alpha+p_r\alpha^r+\dots+p_r\alpha^r=0$; $1+p_o'+p_1'\gamma+\dots+p_s'\gamma^s = 0$ where $\bar{p}_i = \bar{p}_j' = 0$ for $i = 0,1,\dots,r$ and $j = 0,1,\dots,s$ and where r and s may be assumed to be minimal. Assume that $s \leq r$. Since $\gamma = \alpha^{-1}$

$$(1)\quad \alpha^s = -\frac{p_1'}{1+p_o}\alpha^{s-1} - \dots - \frac{p_s'}{1+p_o} \quad \text{or}$$

(2) $\alpha^{s} = p_0'' + p_1''\alpha + \ldots + p_{s-1}''\alpha^{s-1}$

where $p_i'' \in \mathcal{O}$ since $\bar{1} = \overline{p_i}' = \bar{1} \neq 0$ and where $\overline{p_i}'' = 0$ for $i=1,2,\ldots,s-1$. Since $s \leq r$, $\alpha^{r} = \alpha^{s}(\alpha^{r-s})$ and using (2), the degree of $1+p_0+p_1\alpha+\ldots+p_r\alpha^{r} = 0$ may be lowered. Thus $1+p_0+p_1 \quad +\ldots+p_r(\alpha^{r-s})\alpha^{s} = 0$ or $1+p_0+p_2\alpha+\ldots+p_r\alpha^{r-s}(p_0''+\ldots+p_{s-1}\alpha^{s-1}) = 0$ where the highest power of this is $r-1$, contradicting the minimality of r. Thus f may be extended to one of $\mathcal{O}[\alpha]$, $\mathcal{O}[\alpha^{-1}]$ in any case.

Now consider the set E of all extensions of φ to larger rings. If ψ_1, ψ_2 are two such extensions define $\psi_2 > \psi_1$ in case ψ_2 is an extension of ψ_1. This gives rise to a partial ordering. Thus if every totally ordered subset of E has an upper bound in E, Zorn's Lemma is applicable to E. Let $\{\psi_\alpha\}$ be a totally ordered subset of E, where the rings R_α on which the ψ_α are defined are totally ordered by inclusion. Consider the union of these rings and the map ψ defined on this union as: if δ is in the union, then δ is in some set A_α of the union and ψ would act on δ as the original ψ_α for that set did. The definition is consistent since all $\psi_\beta > \psi_\alpha$ are extensions of ψ_α, and ψ is a homomorphism.

Since if δ_1, δ_2 are in the union then δ_1, δ_2 are in some one set R_β of the union because the rings are totally ordered by inclusion and is also a homomorphism on R_β. ψ is an extension of any ψ_α and is thus an upper bound. By Zorn's Lemma, E has a maximal element. Let ψ be such an element where $\psi : O \to F$. Since ψ cannot be extended any further we have:

(3) O is its own quotient ring by elements with non-zero images, i.e., if $a \in O$ and $\psi(a) \neq 0$ then $a^{-1} \in O$.

(4) If $a \notin O$ then we cannot extend ψ to $O[a]$, since ψ is maximal; but this implies that we can extend ψ to $O[a^{-1}]$. Hence $a^{-1} \in O$ since ψ is maximal; so if $a \notin O$ then $a^{-1} \in O$, which means O is a valuation ring.

To complete the proof of the fundamental extension theorem, it is shown that the place φ^* belonging to this valuation ring is ψ up to isomorphism. This is the case from (3) since $\psi(a) \neq 0$ if and only if $a^{-1} \in O$ so the kernel P of ψ is the set of non-units of O. Extend ψ to K by mapping a into ∞ if $a \notin O$ and then $\psi = \varphi^*$ up to isomorphism.

Lemma 2.3 If a non-zero polynomial in several variables is given with coefficients in an infinite field then elements can be chosen from this field such that the polynomial remains non-zero upon substitution of these elements.

Proof: The proof is by induction on the number of variables. The choice is trivial for no variables. Assume that (n-1) variables can be chosen. Consider then a non-zero polynomial of n variables. Write it in terms of the n'th variable with coefficients which are polynomials in the other (n-1) variables. Not all the coefficients are zero since if they were the given polynomial would be zero. By assumption, n-1 values can be chosen in this field so that after substitution at least one of these coefficients is not zero. With this substitution a non-zero polynomial in one variable is obtained. This polynomial has at most as many roots in the field as its degree. A value such that the polynomial remains non-zero after substitution may be chosen, since the field is infinite. By induction, the choice of n values is possible.

The next theorem is a consequence of theorem 2.2.

<u>Theorem 2.4</u> Let $(x) \varepsilon \Omega^n$ and $f(X) \varepsilon k[X]$ and suppose $f(x) \neq 0$. Then there exists an algebraic specialization $(x) \rightarrow (x_o)$ (i.e., all components of (x_o) are algebraic) such that $f(x_o) \neq 0$.

<u>Proof:</u> If $(x) = (x_1, x_2, \ldots, x_n)$ is algebraic, set $(x_o) = (x)$ and the statement holds. Suppose then that $x_1, x_2, \ldots, x_r$ are algebraically independent over k while $x_{r+1}, \ldots, x_n$ are algebraic over $k(x_1, \ldots, x_r)$. Let α be one of the x_i's or $\frac{1}{f(x)}$; then α is algebraic over $k(x_1, \ldots, x_r)$. For each α there is an equation of the form

$$(1) \quad a_{o,\alpha}(x_1, \ldots, x_r)\alpha^{j_\alpha} + \ldots + a_{s,\alpha}(x_1, \ldots, x_r) = 0$$

with coefficients in $k[x_1, x_2, \ldots, x_r]$. Choose $x_1^o, \ldots, x_r^o$ from the algebraic closure of k in Ω in such a way that $a_{o,\alpha}(x_1^o, \ldots, x_r^o) \neq 0$ for all α considered. This is possible by lemma 2.3. Now let ψ be the map ψ: $k[x_1, \ldots, x_r] \rightarrow \Omega$ defined by mapping x_i to x_i^o for $i = 1, 2, \ldots, r$. Since $x_1, x_2, \ldots, x_r$ are algebraically independent, ψ is a homomorphism and is well-defined. Extend this homomorphism to a place φ : $k(x_1, \ldots x_n) \rightarrow \Omega \cup \{\infty\}$. φ is the identity on k and $\varphi(x_i) = x_i^o$ for $i = 1, 2, \ldots, r$, and if $\varphi(x_i) = x_i^o$ for $i = r+1, \ldots, n$ then $\varphi(x_i) = x_i^o$ for $i=1, 2, \ldots, n$. Now $\varphi(\alpha) \neq \infty$ for any α since if $\varphi(\alpha) = \infty$ then $\varphi\left(\frac{1}{\alpha}\right) = 0$. From (1),

$$a_{o,\alpha}(x_1, \ldots, x_r) + a_{1,\alpha}(x_1, \ldots, x_r)\frac{1}{\alpha} + \ldots + a_{s,\alpha}(x_1, \ldots, x_r)\left(\frac{1}{\alpha^{j}}\right) = 0$$

and, applying φ, $a_{o,\alpha}(x_1^o, \ldots, x_r^o) = 0$, a contradiction to the choice of $x_1^o, \ldots, x_r^o$. Therefore $\varphi(\alpha) \varepsilon \Omega$ for all α and applying φ to (1) it is seen that $\varphi(\alpha)$ is algebraic over $k(x_1^o, \ldots, x_r^o)$ and so $\varphi(\alpha)$ is algebraic over k. Thus $(x_o) = (x_1^o, \ldots, x_n^o)$ is algebraic and $(x) \rightarrow (x_o)$ is a specialization, since φ is a homomorphism on $\varphi^{-1}(\Omega)$. Finally, $\varphi(f(x)) = f(x_o)$ is finite and not zero since $\varphi(\alpha) \neq \infty$ for any α.

<u>Theorem 2.5</u> Let V be an algebraic set of Ω^n and V_o the subset of algebraic points of V. Let $f \in k[X]$ be such that $f(v_o) = 0$. The $f(V) = 0$.

<u>Proof</u>: Suppose $(x) \in V$ and $f(x) \neq 0$, then from theorem 2.4 there exists an algebraic specialization $(x) \to (x_o) \in V$ such that $f(x_o) = 0$ which is a contradiction.

SECTION II

HILBERT'S NULLSTELLENSATZ

Let $\mathcal{O}$ be any ring, not necessarily with identity, and let S be a multiplicative semi-group contained in $\mathcal{O}$. Suppose A is an ideal of $\mathcal{O}$ such that $A \cap S = \phi$. It will be shown that there exists a maximal ideal that contains A and has this property. Let E be the set of all ideals which contain A and do not intersect S. E is partially ordered by inclusion and for any totally ordered subset of E, the union is an ideal which does not intersect S. Thus, by Zorn's Lemma, E contains a maximal element, say P. Any ideal properly containing P will intersect S. P is a prime ideal, since if $a,b \notin P$, $ab \notin P$. Suppose $ab \in P$, let (a,P) and (b,P) be the ideals generated by a and P, and b and P respectively. Their intersections with the semi-group S contain elements s_1 and s_2 where $s_1 = p_1+m_1a+x_1a$; $s_2 = p_2+m_2b+x_2b$ for some $p_2, p_2 \in P$ where m_1, m_2 are integers and $x_1, x_2 \in \mathcal{O}$. Then $s_1s_2 = p_1s_2+(m_1a+x_1a)p_2+(m_1a+x_1a)(m_2b+x_2b)$. Thus if $ab \in P$, then $s_1s_2 \in P$ so P meets S, which is a contradiction.

If $\mathcal{O}$ is Noetherian, Zorn's Lemma need not be used for the existence of P, and if $\mathfrak{O}$ has identity the existence of maximal ideals for $\mathfrak{O}$ is obtained by taking $S = \{1\}$.

Let A be an ideal of $\mathfrak{O}$. Suppose $b \in \mathfrak{O}$ and has the property that $b^n \notin A$ for any positive integer n. Let $S = \{b^n$, where n is a positive integer$\}$. S us a multiplicative semi-group. Therefore there exists a prime ideal $P \supset A$ such that $b^n \notin P$ for any positive integer n. Let $\bar{A} = \bigcap_{P \supset a} P$ where the P's are the prime ideals which contain A. $\bar{A}$ is an ideal and $b \notin \bar{A}$ since there is a P such that $P \supset A$ and $b \notin P$. Thus an element $b \in \bar{A}$ implies $b^n \in A$ for some positive integer n. Conversely, if b has the property that some $b^n \in A$ and if P is any prime ideal with $P \supset A$, then $b^n \in P$, so $b \in P$; hence $b \in \bar{A}$. As a result of these considerations it is seen that $\bar{A} = \{b \mid b \in \mathfrak{O}\ ,\ b^n \in A$ for some $n\}$. $\bar{A}$ is called the <u>radical</u> of the ideal A.

Now if $A = \{0\}$ then its radical $\bar{A}$ consists of the nilpotent elements of $\mathfrak{O}$; in this case $\bar{A}$ is called the <u>radical of the ring</u>. It suffices in the definition of the radical $\bar{A}$ to consider only the minimal prime ideals containing A so that:

<u>Theorem 2.6</u> The radical of an ideal A in the ring $\mathfrak{O}$ is the intersection of all minimal prime ideals containing A.

<u>Proof</u>: In view of the preceding discussion, it remains only to show that there are minimal prime ideals containing A. Let F be the set of all prime ideals containing A. This set is partially ordered by reverse inclusion. Consider any totally ordered subset $\{P_\alpha\}$ of F. Let $P_0 = \bigcap_\alpha P_\alpha$ then P_0 is a prime ideal, for suppose $ab \in P_0$ and $a \notin P_0$. Then a is not in some P_α which implies $a \notin P_\beta \subset P_\alpha$, but ab is in every P_β, so $b \in P_\beta$ for

all $P_\beta \subset P_\alpha$. Thus $b \varepsilon P_o$ so P_o is a prime ideal, thus the totally ordered set $\{P_\alpha\}$ has an upper bound. Therefore, by Zorn's Lemma, there exists a minimal element in the set F, i.e., among the prime ideals containing A there are certain minimal ones, and all others contain one of these.

<u>Theorem 2.7</u> Let A be an ideal in $k[X]$ and V i s algebraic set. Then $\bar{A}$, the radical of A, is the ideal determined by V.

<u>Proof</u>: Let $V \to A'$ or $A' = \{f \mid f \varepsilon \mathcal{O}, f(V) = 0\}$. Let P be any prime ideal containing A; then $P \to W$, a variety, and $W \subset V$. But $W \subset V$ implies $P \supset A'$ so that $\bigcap_{A \subset P} P \supset A'$ or $\bar{A} \supset A$. If $f \varepsilon \bar{A}$, then $f^n \varepsilon A$ for some n, so that $f^n(V) = 0$; but then $f(V) = 0$ which implies $f \varepsilon A'$, so $\bar{A} \subset A'$. Hence $\bar{A} = A'$.

<u>Theorem 2.8</u> <u>Hilbert's</u> <u>Nullstellensatz</u> (strong form) Let A be an ideal of the ring $\mathcal{O} = k[X]$; suppose $A \to V$ and V_o is the subset of algebraic points of V. If $f \varepsilon \mathcal{O}$ is not identically zero and is such that $f(V_o) = 0$ then $f^n \varepsilon A$ for some positive integer n.

<u>Proof</u>: From theorem 2.4 $f(V_o) = 0$ implies $f(V) = 0$ which in turn implies, by theorem 2.6, that $f \varepsilon \bar{A}$, the radical of A, or $f^n \varepsilon A$ for some positive integer n.

Theorem 2.9 <u>Hilbert's</u> <u>Nullstellensatz</u> (weak form) let A be an ideal of the ring $\mathcal{O} = k[X]$; then A without zeros implies $A = \mathcal{O}$.

<u>Proof</u>: Suppose $V = \phi$; then $V_o = \phi$ so that all $f \varepsilon \mathcal{O}$ vanish on V_o. Hence, for all $f \varepsilon \mathcal{O}$, $f^n \varepsilon A$ for some n. In particular $1 \varepsilon A$ so $A = \mathcal{O}$.

SECTION III

INTEGRAL CLOSURE

Let $\mathcal{O}$ be a ring with identity and let $\mathcal{O}$ be a subring of the field K. An element $a \varepsilon K$ is said to be integral over $\mathcal{O}$ in case a satisfies an equation: $a^n+b_1a^{n-1}+\dots+b_n = 0$, where all $b_i \varepsilon \mathcal{O}$. The totality of elements of K, integral over $\mathcal{O}$, is called the integral closure of $\mathcal{O}$ in K. If $\mathcal{O}$ is the ring of integers and K the field of complex numbers, then an element a satisfying an equation $a^n+b_1{}^{n-1}+\dots+b_n=0$ is called an algebraic integer.

Theorem 2.10 Let S be the set of all places of K which are finite on $\mathcal{O}$ (All places of K whose valuation rings contain $\mathcal{O}$). If $a \in K$ is integral over $\mathcal{O}$, and if $\Phi \varepsilon S$, then $\Phi(a)$ is finite.

Proof: If $\Phi(a) = \infty$ then $\Phi\left(\frac{1}{a}\right) = 0$. Since a satisfies $a^n+b_1a^{n-1}+\dots+b_n = 0$, $b_i \varepsilon \mathcal{O}$, dividing by a^n yields $1+b_1\left(\frac{1}{a}\right)+\dots+b_n\left(\frac{1}{a^n}\right) = 0$. Applying Φ gives $1 = \Phi(1) = 0$, a contradiction. Thus any place of K which is finite on $\mathcal{O}$ is finite on any element of K integral over $\mathcal{O}$.

Corollary 2.11 If F is a subfield of K, and if K is algebraic over F, and if Φ is a place of K which is an isomorphism on F (i.e., a trivial place on F since the valuation ring of $\Phi | F$ is F), then Φ is an isomorphism on K (i.e., a trivial place of K.)

Proof: Consider F as a subring of K. Since K is algebraic over F, all elements of K are integral over F, so Φ is finite on all elements of K.

Consider now the converse of theorem 2.9. Here let $S_0 \subset S$ be the set of those places $\Phi \varepsilon S$ whose kernel in Δ is a maximal ideal of $\mathcal{O}$.

<u>Theorem 2.12</u> Let $a \in K$ and suppose $\mathcal{Q}(a) \neq \infty$ for any $\mathcal{Q} \in S_o$; then a is integral over $\mathcal{O}$, (and by theorem 2.9, $\mathcal{Q}(a) \neq \infty$ for any $\mathcal{Q} \in S$).

<u>Proof</u>: If $a = 0$, then $a \in \mathcal{O}$ and satisfies the equation $x = 0$. Thus assume $a \neq 0$. Consider the ring $\mathcal{O}_1 = \mathcal{O}\left[\frac{1}{a}\right]$. If $\frac{1}{a}$ is a unit of $\mathcal{O}_1$ then $a \in \mathcal{O}_1$ and $a = b_o + b_1\left(\frac{1}{a}\right) + \ldots + b_r\left(\frac{1}{a^r}\right)$ for $b_i \in \mathcal{O}$. Multiplying by a^r we have $a^{r+1} - b_o a^r - \ldots - b_r = 0$ so a is integral over $\mathcal{O}$. $\frac{1}{a}$ is a unit of $\mathcal{O}_1$ since if it were not, then the ideal $\frac{1}{a}\mathcal{O}_1 \neq \mathcal{O}_1$. There is a maximal ideal P of $\mathcal{O}_1$ such that $\frac{1}{a}\mathcal{O}_1 \subset P$. Consider the map $\mathcal{O}_1 \to \mathcal{O}_1/P$ Now $\mathcal{O}_1/P$ is a field and injecting this into its algebraic closure $\overline{\mathcal{O}_1/P}$ gives a homomorphism of the ring $\mathcal{O}_1$ into an algebraically closed field; this homomorphism is non-trivial since $P \neq \mathcal{O}_1$. Extend this homomorphism to a place $\mathcal{Q}$ of K. Since $\mathcal{Q}$ is finite on $\mathcal{O}_1$, it is finite on $\mathcal{O}$. $\frac{1}{a} \in P$, so that $\mathcal{Q}\left(\frac{1}{a}\right) = 0$ and $\mathcal{Q}(a) = \infty$, a contradiction already, if the set S is used in place of S_o in the statement of the theorem.

The set S_o does suffice. The kernel of $\mathcal{Q}$ in $\mathcal{O}_1$ is P, which is a maximal ideal. The kernel of $\mathcal{Q}$ in $\mathcal{O}$ is $\mathcal{O} \cap P = Q$. Q is maximal since if $c \in \mathcal{O}$, $c \notin Q$, then c has an inverse modulo Q, i.e., $\mathcal{O}/Q$ is a field. If $c \in \mathcal{O}$ and $c \notin Q$ then $c \in \mathcal{O}_1$ and $c \notin P$. Since P is a maximal ideal of $\mathcal{O}_1$, c has an inverse in $\mathcal{O}_1$ modulo P or $c\left(b_o + b_1\left(\frac{1}{a}\right) + \ldots + b_r\left(\frac{2}{a^r}\right)\right) \equiv 1 \bmod P$. But $\frac{1}{a} \equiv 0 \bmod P$ so this reduces to $cb_o \equiv 1 \bmod P$. Thus $cb_o - 1 \in P$ and $cb_o - 1 \in \mathcal{O}$ so $cb_o - 1 \in Q$ and $cb_o \equiv 1$ modulo Q.

From theorems 2.10 and 2.12 the integral closure of $\mathcal{O}$ in K consists of all those elements of K which are "finite on all places" of S. Therefore the integral closure O_ρ of $\mathcal{O}$ in K forms a ring.

The conclusion of this section will show that the terminology "integral closure" is justified, i.e., the integral closure of O in K is

O itself. Let S' denote the set of all places of K which are finite on O. If $\mathcal{Q} \varepsilon S$, then φ is finite on O and so is finite on $\mathcal{O}$ and $\mathcal{Q} \varepsilon S$. Conversely, if $\mathcal{Q} \varepsilon S$ then $\mathcal{Q}$ is finite on O since O is the integral closure of $\mathcal{O}$ in K, so $\mathcal{Q} \varepsilon S'$. Thus $S = S'$. Hence the integral closure of O in K is precisely O. The integral closure O of $\mathcal{O}$ in K can be written as $O = \bigcap \bar{\mathcal{O}}$ where the intersection is taken over all valuation rings $\bar{\mathcal{O}}$ of K such that $\bar{\mathcal{O}} \supset \mathcal{O}$.

CHAPTER III

THEOREMS CONCERNING MANY VALUATIONS

SECTION I

AN EXISTENCE LEMMA IN VALUATION THEORY

This chapter leads to the proof of a theorem concerning three fields as given by I. N. Herstein [3].* Some concepts are first introduced which are necessary in the proof of the theorem.

An exponential valuation on a field K is a map φ on K satisfying:

(1) For every $a \neq 0$, $\varphi(a)$ is a real number

(2) $\varphi(0) = \infty$, where ∞ is a symbol adjoined to the image field

(3) $\varphi(ab) = \varphi(a) + \varphi(b)$

(4) $\varphi(a+b) \geq \min.\ (\varphi(a), \varphi(b))$.

If $a \rightarrow |a|$ is a real valued valuation on K in the former sense, then $\varphi(a) = -\log|a|$ is an exponential valuation on K. In this chapter, "valuation" will mean "exponential valuation."

With an exponential valuation it is possible to obtain a metric which is a real valued distance function $\rho(a,b)$ defined such that $\rho(a,b) \geq 0$, $\rho(a,b) = 0$ if and only if $a=b$, $\rho(a,b) = \rho(b,a)$ and finally,

*The symbol [n] will refer to the n'th entry in the list of references.

$\rho(a,c) \leq \rho(a,b) + \rho(b,c)$ where a,b,c, are elements of K. Define for $x \in K$, a field, $|x| = e^{-\varphi(x)}$ if $x \neq 0$ and $|x| = 0$ if (and only if) $x = 0$. Then $|xy| = e^{-\varphi(xy)} = e^{-\varphi(x)-\varphi(y)} = |x||y|$, $|x+y| \leq$ max. $(|x|,|y|)$ since $|x+y| = e^{-\varphi(x+y)} \leq e^{-\min.(\varphi(x),\varphi(y))} \leq \max.\left(e^{-\varphi(x)}, e^{-\varphi(y)}\right)$. Let the metric ρ be given by $\rho(x,y) = |x-y|$. The properties of a metric are certainly satisfied and the inequality is stronger than the triangle axiom. The idea of this metric will be used but the development and results will be stated in terms of φ.

A sequence $\{a_n\}$ is a <u>fundamental sequence</u> in the valuation φ if for every $B > 0$ there exists N such that if $p,q > N$ then $\varphi(a_p - a_q) > B$. A field is <u>complete in the valuation</u> φ if and only if every fundamental sequence has a limit in K. An interesting consequence is the following:

<u>Theorem 3.1</u> A sequence $\{a_n\}$ in a field K with an exponential valuation φ is fundamental if and only if $\lim_{n \to \infty} \varphi(a_{n+1} - a_n) = \infty$.

<u>Proof:</u> The sequence $\{a_n\}$ is convergent exactly when $\lim_{n \to \infty} \varphi(a_{n+k} - a_n) = \infty$ uniformly in k. However, since $\varphi(a_{n+k} - a_n) \geq \min.\left(\varphi(a_{n+k} - a_{n+k-1}), \ldots, \varphi(a_{n+1} - a_n)\right)$, the condition $\lim_{n \to \infty} \varphi(a_{n+1} - a_n) = \infty$ is sufficient for convergence.

<u>Theorem 3.2</u> A field K with an exponential valuation φ may be extended to a field L with valuation φ^* such that $\varphi^* / K = \varphi$ and L is complete in the valuation φ^* (L is called the φ-completion of K).

<u>Proof:</u> The method of proof is exactly analogous to the Cantor method of defining real numbers by means of sequences of rationals. A sketch of the proof is given here. The steps in the proof are listed.

1. The set A of all fundamental sequences of a field K with an exponential valuation Φ is a commutative ring with an identity element.

The sum and product of fundamental sequences is first defined in the obvious way. That is, if $\alpha = \{a_n\}$, $\beta = \{b_n\}$ then define $\alpha + \beta = \{a_n + b_n\}$ and $\alpha\beta = \gamma = \{c_n\}$ where $c_n = a_n b_n$. Notice that any sequence $\delta = \{d_n\}$, $d = d_1 = d_2 = \ldots$ in K is a fundamental sequence all of whose elements are equal to d. Define $\delta\alpha = \{da_n\} = d\alpha$ which is fundamental for any d in K. In particular $-\alpha = \{-a_n\}$, $0 = \{0\}$ are fundamental and so is $\alpha - \beta$. Addition and multiplication are commutative and associative in K and also in A. The distributive law $\alpha(\beta + \gamma) = \{a_n(b_n + c_n)\} = \{a_n b_n + a_n c_n\} = \alpha\beta + \alpha\gamma$ holds and $1 = \{1\}$ is the identity element.

2. A fundamental sequence $\{a_n\}$ is called a <u>null sequence</u> if there exists for every $B > 0$ a N_B such that $\Phi(a_n) > B$ for $n > N_B$. The next step is then to reduce the sequences in A modulo the null sequences. Let η be the set of all null sequences of A. It is easy to show that η is an ideal in A and that the difference ring, $L = A - \eta$, is a field. The elements of $A - \eta$ are classes of equivalent fundamental sequences. The field K is isomorphic to the subfield of equivalence classes of constant sequences. The extension L is a field over K and all of its quantities not in K are equivalence classes, denoted by $[\alpha]$, where α is not equivalent to a constant sequence.

3. Φ^* is defined as follows: Let $[\alpha]$ be an element of L and $\alpha = \{a_n\}$, a member of the equivalence class $[\alpha]$. For every $B > 0$ there exists N such that $\Phi(a_p - a_q) > B$ for $p > N$, $q > N$. If $\{a_p\}$ is a fundamental

sequence and $\lim_{n\to\infty} a_p \neq 0$, then $\varphi(a_p)$ is ultimately constant as n increases. This is the case as $\varphi(a_p - a_{p+1})$ approaches ∞ as n increases, but a_p does not approach 0, i.e., $\varphi(a_p)$ does not approach ∞. Thus there exists a quantity M and an integer N such that for $p > N$, $\varphi(a_p) < M$ but $\varphi(a_p - a_{p+1}) > M$. $\varphi(a_p - a_{p+1}) = \min.\ \varphi(a_p),\ \varphi(a_{p+1}) < M$, unless $\varphi(a_p) = \varphi(a_{p+1})$. Hence for $p > N$, $(a_p) = (a_{p+1})$. From this $\Gamma = (a_p)$ is a constant fundamental sequence and $\varphi^*([\alpha]) = [\Gamma] = \lim_{n\to\infty}\varphi(a_n)$. This sequence is positive and consider $[\alpha]$, $[\beta]$ and the product $[\alpha\beta]$.
$\varphi^*([\alpha\beta]) = [\{\varphi(a_n b_n)\}] = [\{\varphi(a_n) + \varphi(b_n)\}] = [\{\varphi(a_n)\} + \{\varphi(b_n)\}] = \varphi^*[\alpha] + \varphi^*[\beta]$ and similarly the property $\varphi(a_n + b_n) \geq \min.\ \varphi(a_n, \varphi(b_n)$ implies that $\varphi^*([\alpha] + [\beta]) \geq \min.(\varphi^*[\alpha],\ \varphi^*[\beta])$. Also $\varphi^*(0) = \varphi(0) = \infty$ and φ^* is well defined. The valuation φ^* is a valuation on K to the reals with the symbol ∞ adjoined. If $a \in K$, $\varphi^*(a) = \varphi^*([\{a\}]) = \lim_{n\to\infty}\varphi(a) = \varphi(a)$.

4. L is complete in the vaulation φ^*. Let $\{c^{(p)}\}$ be a fundamental sequence in L where $c^{(p)} = [\alpha^{(p)}]$. Each $\alpha^{(p)} = \{a_n^{(p)}\}$ is a fundamental sequence in K. This implies that for every $B > 0$ there exists an N such that $\varphi(a_n^{(p)} - a_m^{(p)}) > B$ for n, $m > N$. Let $B = 2^{p-1}$, $m = N+1$ and define $a^{(p)} = a_m^{(p)}$. Replacing φ by φ^*, $\varphi^*(a_n^{(p)} - a^{(p)}) > 2^{p-1}$ for $n > N$. Let $\alpha^{(p)} = \{a_\mu^{(p)}\}$ and notice that $c^{(p)} - a_n^{(p)} = [\{a_\mu^{(p)} - a_n^{(p)}\}] > B$ for $\mu > N$, $n > N$, and for every n, $\varphi^*(c^{(p)} - a_n^{(p)}) = \lim_{\mu\to\infty}\varphi(a_\mu^{(p)} - a_n^{(p)})$. Fix $n > N$ and each $\varphi(a_\mu^{(p)} - a_n^{(p)}) > B$ so that certainly the limit $\varphi^*(c^{(p)} - a_n^{(p)}) > B$ for $n > N$. Again take $B = 2^{p-1}$ and have $c^{(p)} - a^{(p)} = c^{(p)} - a_n^{(p)} + a_n^{(p)} - a^{(p)}$, so that $\varphi^*(c^{(p)} - a^{(p)}) \geq \min.\ \varphi^*(c^{(p)} - a_n^{(p)})$, $\varphi^*(a_n^{(p)} - a^{(p)}) > 2^{p-1}$ for all values of p. For every $B > 0$ there exists

a p_b such that $2^{p-1} > B$ for $p > p_b$. Hence $\Phi^*(c^{(p)} - a^{(p)}) > B$ for $p > p_b$ and the sequence $\alpha_0 = \{a^p\}$, where $a^{(p)}$ is a constant sequence, is a fundamental sequence equivalent to $\{c^{(p)}\}$. The class $[\alpha_0]$ is the general quantity of L, where α_0 is a sequence in K and $[\alpha_0]$ is in L. Thus L is complete in the valuation Φ^*.

If K is a field with valuation Φ, the elements of the valuation ring O (the set of $x \varepsilon K$ such that $\Phi(x) \geq 0$) are said to be <u>integral</u>. A polynomial f(x) in K(x) with integral coefficients is <u>primitive</u> in case the greatest common divisor of its coefficients (considered as elements of O or of some other integral domain) is 1.

<u>Lemma 3.3</u> (Hensel) Let K be complete in the exponential valuation Φ. Let f(x) be a primitive polynomial with integral coefficients in K. Let $g_0(x)$ and $h_0(x)$ be two polynomials with integral coefficients in K which satisfy $f(x) \equiv g_0(x)h_0(x)$ modulo P, where P is the set of all elements in K with $\Phi(a) > 0$. Then there exist two polynomials $g(x), h(x)$ with integral coefficients in K for which:

$$f(x) = g(x)h(x)$$

$$f(x) = g_0(x) (\text{mod } P)$$

$$h(x) = h_0(x) (\text{mod } P)$$

provided $g_0(x)$ and $h_0(x)$ are relatively prime modulo P. It is, moreover, possible to determine g(x) and h(x) so that the degree of g(x) is equal to the degree of $g_0(x)$ modulo P.

<u>Proof:</u> Since, without changing hypothesis and conclusion, it is possible to omit in $g_0(x)$ and $h_0(x)$ coefficients contained in P, it may be assumed the $g_0(x)$ is a polynomial of degree r and that the leading coefficients of $g_0(x)$ and $h_0(x)$ are units. Assume $g_0(x) = x^r + \ldots$. If b is the leading

coefficient and s the degree of $h_0(x)$, then the leading coefficient of $g_0(x)h_0(x)$ is b are the degree $r+s\leq n$. The factors g(x) and h(x) shall be constructed so that g(x) is a polynomial of degree r and h(x) a polynomial of degree n-r.

By hypothesis, all the coefficients of the polynomial $f(x)-g_0(x)h_0(x)$ have positive values; let the smallest of them be $\delta_1>0$. If $\delta_1=\infty$ then $f(x)=g_0(x)h_0(x)$ so that nothing else need be proved. Since $g_0(x)$ and $h_0(x)$ are relatively prime modulo P there exist two polynomials l(x) and m(x) with integral coefficients in K for which

$$l(x)g_0(x)+m(x)h_0(x)\equiv 1 \pmod{P}$$

holds. Let the smallest of the values of the coefficients in the polynomial $l(x)g_0(x)+m(x)h_0(x)-1$ be $\delta_2>0$. Let ε be the smaller of δ_1 and δ_2 and let π be an element for which $\varphi(\pi)=\varepsilon$.

Then we have:

$$(1)\quad f(x)\equiv g_0(x)h_0(x) \pmod{(\pi)}$$

$$(2)\quad l(x)g_0(x)+m(x)h_0(x)\equiv 1 \pmod{(\pi)}$$

where by (π) is meant the principal ideal generated by π.

Now construct g(x) as the limit of a sequence of polynomials $g_n(x)$ of degree r, beginning with $g_0(x)$ and, similarly, construct h(x) as the limit of a sequence of polynomials $h_n(x)$ of degree less than or equal to n-r beginning with $h_0(x)$. Suppose $g_n(x)$ had $h_n(x)$ have already been determined so that:

$$(3)\quad f(x)\equiv g_n(x)h_n(x) \pmod{\pi^{n+1}}$$

$$(4)\quad g_n(x)\equiv g_0(x) \pmod{\pi}$$

$$(5)\quad h_n(x)\equiv h_0(x) \pmod{\pi}$$

and that $g_n(x) = x^r + \ldots$ has leading coefficient 1. For determining $g_{n+1}(x)$ and $h_{n+1}(x)$ put:

$$(6) \quad g_{n+1}(x) = g_n(x) + \pi^{n+1}u(x)$$

$$(7) \quad h_{n+1}(x) = h_n(x) + \pi^{n+1}v(x)$$

Then:

$$g_{n+1}(x)h_{n+1}(x) - f(x) = g_n(x)h_n(x) - f(x) + \pi^{n+1}\{g_n(x)v(x) + h_n(x)v(x)\} + \pi^{2n+2}u(x)v(x)$$

By (3), put $f(x) - g_n(x)h_n(x) = \pi^{n+1}p(x)$; then:

$$g_{n+1}(x)h_{n+1}(x) - f(x) \equiv \pi^{n+1}\{g_n(x)v(x) + h_n(x)u(x) - p(x)\} \bmod \pi^{n+2}.$$

For the left side to be divisible by π^{n+2}, it suffices that

$$(8) \quad g_n(x)v(x) + h_n(x)u(x) \equiv p(x) \bmod \pi$$

be satisfied. Thus multiply (2) by $p(x)$ and

$$(9) \quad p(x)l(x)g_o(x) + p(x)m(x)h_o(x) \equiv p(x) \pmod{\pi}.$$

Divide $p(x)m(x)$ by $g_o(x)$ so that the remainder $u(x)$ is of degree less than r and

$$(10) \quad p(x)m(x) = q(x)g_o(x) + u(x).$$

Substituting (10) into (9)

$$\{p(x)l(x) + q(x)h_o(x)\}\, g_o(x) + u(x)h_o(x) \equiv p(x) \bmod \pi.$$

Replace by zero all coefficients of the polynomial in braces which are divisible by π so that

$$(11) \quad v(x)g_o(x) + u(x)h_o(x) \equiv p(x) \bmod \pi.$$

From (11) follows the desired congruence (8) because of (4) and (5). Furthermore, $u(x)$ is of degree less than r and because of (6) $g_{n+1}(x)$ is of the same degree and has the same leading coefficient as $g_n(x)$. It remains to show that $v(x)$ is of degree less than or equal to $n-r$. If this were not the case, a highest term of degree greater than n would occur in the first term of (11) but not in the others. By (11), the coefficient of this term would have to be divisible by π, so that the leading coefficient of $\nu(x)$ would be divisible by π. But since all coefficients in $\nu(x)$ divisible by π have been omitted, $\nu(x)$ is of degree less than or equal to $n-r$, and the proof is complete.

A polynomial $f(x)$ of degree n is said to be <u>separable</u> over a field k if it has n distinct roots in some root field $K \geq k$; otherwise it is <u>inseparable</u>. A finite extension $K \supseteq k$ is called <u>separable</u> over a field F if every element in K satisfies a separable polynomial equation over k. An element x in K is <u>purely inseparable</u> over k if some p^e power of x belongs to k for $e \geqq 0$. K is a <u>purely inseparable extension</u> of k if every element of K is purely inseparable over k. If a field k is algebraic over its prime field then it is called <u>absolutely algebraic</u>. The set of all elements of K which are algebraic over k is called the <u>algebraic closure</u> of k in K. By the <u>discriminant</u> of a polynomial is meant the norm of the formal derivative of the polynomial. Let $h(x)$ be an irreducible polynomial and suppose $r(x)=h(x)^m\frac{a(x)}{b(x)}$ where $a(x)$ and $b(x)$ are relatively prime to $h(x)$. Then set $\mathcal{Q}(r(x)) = m$. If $m = 1$ then the valuation $\mathcal{Q}$ is said to be of the <u>first degree</u>.

<u>Lemma 3.5</u> Let K be a field which is either of characteristic 0 or not absolutely algebraic, and let L be its separable finite extension. Then there exist infinitely many valuations in L which are of first degree over K.

<u>Proof</u>: Let $L = K(\alpha)$ and let $F(x) = x^n+a_{n-1}x^{n-1}+\ldots+a_0$ be the minimal

polynomial over K with α as a root. Assume that $n > 1$ and let d be the discriminant of $F(x)$. It will be sufficient to get infinitely many pairs (w, φ), where $w \in K$ and φ is a valuation in L, with mutually pairwise distinct φ's such that for each pair (w, φ):

(1) $\varphi(d) = 0$

(2) $\varphi(a_i) \geq 0$ for $i=1,2,\ldots,n-1$

(3) $\varphi(\alpha - w) > 0$

for with such a pair and with $F(x+w) = x^n + b_{n-1}x^{n-1} + \ldots + b_o$ it follows that:

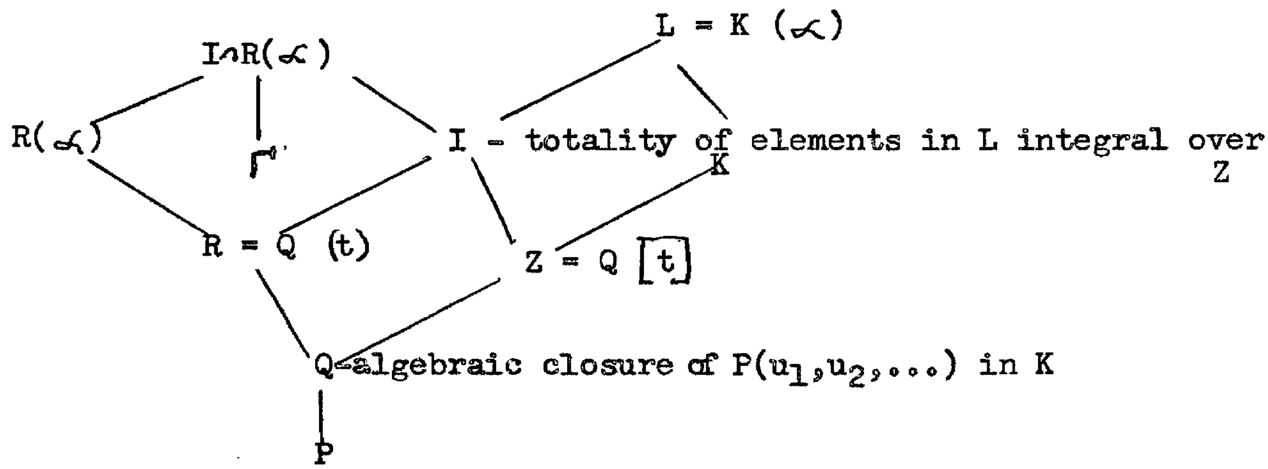
(4) $\varphi(\alpha) \geq 0$ because of theorem 2.9 since α is in the integral closure and $\varphi(w) \geq 0$ since $-w = (\alpha - w) - \alpha$ and $\varphi(\alpha - w) > 0$, $\varphi(\alpha) \geq 0$;

(5) $\varphi(b_o) = \varphi(F(w)) = \varphi(F(w) - F(\alpha)) > 0$ since $\alpha - w$ is a factor of $F(w) - F(\alpha)$ and $\varphi(\alpha - w) > 0$ by (3);

(6) $\varphi(b_1) = \varphi(F'(w)) = 0$ since $n\, F'(x)$ is the norm of $F'(x)$ and the norm of the derivative is zero, and $\varphi(b_i) \geq 0$ for $i=2,\ldots,n-1$ because the b_i's are polynomials in the a_i's and w with integer coefficients hence are in the valuation ring. The value of a constant times the b_i's or w's is greater than or equal to the minimum of their individual values which are all non-negative.

From lemma 3.3, $F(x+w)$ can be factored in the φ-completion of K into a product of the form $G(x) \cdot x$ with $G(x)$ prime to x and thus φ is of the first degree over K. Either the field K has an element t, transcendental over the prime field P, or is of characteristic 0. If it is the first, take a transcendence basis $(t, u, \ldots)$ of K over P, denote the algebraic closure of $P(u_1, u_2, \ldots)$ in K by Q and set $Z = Q[t]$, $R = Q(t)$.

In the second case set R = P and denote by Z the ring of rational integers which is considered as being contained in P. In either case let I be the totality of elements in L integral over Z. Let $c \neq 0$ be an element of Z such that $c\alpha \in I$. Take an element w_o in Z which is of sufficiently



high degree in t or of sufficiently large absolute value, according as $Z = Q[t]$ or the ring of rational integers. Then the norm, $N_{R(\alpha)/R}(c\alpha - W_o)$ is a non-unit in Z and there exists a prime ideal $\mathfrak{p}$ in $I \cap R(\alpha)$ containing $c\alpha - W_o$. In fact, $c\alpha - w_o$ is an irreducible polynomial and generates a prime ideal. Let φ be an extension to L of the valuation of $R(\alpha)$ defined by $\mathfrak{p}$. Then $\varphi(c\alpha - w_o) > 0$ and it is desired to obtain an infinity of w_o's such that the corresponding φ's are all distinct. It will be convenient, and possible, to choose w_o so that $(c\alpha, w_o) = 1$ in $I \cap R(\alpha)$. This implies that $c\alpha \in P$ and $w_o \notin P$ since $c\alpha - w_o \in P$. Consider now getting an infinity of these pairs (w, φ). Suppose $w_o^{(1)}, w_o^{(2)}, \ldots, w_o^{(m)}$ have been chosen and with them the corresponding $P^{(1)}, P^{(2)}, \ldots, P^{(m)}$ satisfying the above conditions, so that the $P^{(n)}$ are all distinct. Take $w_o^{(m+1)}$, satisfying the consitions above on w_o, from $P^{(1)} \cap P^{(2)} \cap \ldots P^m \cap Z$. The corresponding prime ideal is different from $P^{(1)}, P^{(2)}, \ldots, P^{(m)}$ since

$w_o^{(m+1)} \notin P^{(m+1)}$. In this manner an infinite sequence of distinct prime ideals is obtained and thus also an infinite sequence of distinct valuations in L. Now $\varphi^{(n)}(d) = 0$, $\varphi^{(n)}(a_i) \geq 0$ (here $\varphi^{(n)}(a_i) = 0$ wherever $a_i \neq 0$) and $\varphi^{(n)}(c) = 0$ for almost all n, since an element can only be in a finite number of the P's. For any of such n's, $\varphi(\alpha - w) > 0$ with $w = w_o c^{-1}$. Therefore an infinity of pairs (w, φ) has been obtained with distinct φ's satisfying (1),(2),and(3).

Lemma 3.6 Let L be a field and K be its proper subfield. Except either when L is of characteristic $p \neq 0$ and absolutely algebraic or when L is algebraic and purely inseparable over K there exists a pair of distinct (exponential) valuations in L which coincide on K.

Proof: There are two cases which arise. The first is when L is a transcendental extension of K. In this case the same procedure used in lemma 3.5 establishes the lemma if the roles of L and K are interchanged. The second case is when L is a separable algebraic extension of L. To establish this, the reader is referred to theorems 3 and 4 of chapter 4 in "The Theory of Valuations" by O. F. G. Schilling [7] .

SECTION II

A THEOREM CONCERNING THREE FIELDS

For the next two lemmas and Lüroth's theorem consider a field F, a transcendental x over F, and $y \in F(x)$, $y = g(x)/h(x)$ where g(x) and h(x) are relatively prime polynomials in F [x] . Let m be the maximum of the degrees of g(x) and h(x) in F [x] . Of course $F \subset F(y) \subset F(x)$.

Lemma 3.7 With the above assumptions, x is algebraic over F(y) of degree m and $g(t)-yh(t)=p(t)$ is the minimal polynomial for x over $F(y)$.

Proof: $p(x) = 0$ follows from the definition of $g(x)$ and $h(x)$. $p(t)$ is of degree m. It must be shown that $p(t)$ is irreducible. $p(t) \in F[t,y]$ is primitive in t and irreducible in $F(t)[y]$. It is therefore irreducible in $F[t,y]$, hence irreducible in $F(y)[t]$.

Before considering the second lemma, note that since $F(x)$ is algebraic over $F(y)$, $F(y)$ must be transcendental over F.

Lemma 3.8 If $\big(g(x),h(x)\big) = 1$ with maximum degree m, then $m(x,t) = g(x)h(t)-h(x)g(t)$ is primitive in t (also in x, by symmetry).

Proof: Let $g(x)=g_0+g_1x+\ldots+g_nx^n$, $h(x)=h_0+h_1x+\ldots+h_mx^m$. Then $m(x,t)= g_0h(t)-h_0g(t)+[g_1h(t)+h_1g(t)]x+\ldots+[g_ih(t)+h_ig(t)]x^i+\ldots$. If this is not primitive there exists $p(t)$ such that $p(t)$ divides $h_j/h_i[g_ih(t)-h_ig(t)] - [g_jh(t)-h_jg(t)] = [h_jg_i/h_i - g_j]\,h(t)$ for every choice of i and j. But this is just $h_j[g_i/h_i - g_j/h_j]h(t)$; now $p(t)$ does not divide $h(t)$ because of it did, it would have to divide $g(t)$ and these are relatively prime. The quantity in brackets is not always zero since if it were, the polynomials $g(x)$ and $h(x)$ would be proportional.

Theorem 3.9 (Lüroth) Any field L such that $F \subset L \subseteq F(x)$ has the $F(y)$ for some $y \in F(x)$. (L is isomorphic to a simple transcendental extension of F.)

Proof: Suppose the minimal equation of x over L is $p(t)=t^n+a_{n-1}t^{n-1}+\ldots+a_0=0$ $a_i \in L$. Not all the a_i's are in F. Suppose $a_r \notin F$ and take $y = a_r$, $y=\frac{g(x)}{h(x)}$, with m the greater of the degrees of g,h. $F \subset F(y) \subset L \subset F(x)$ where $[F(x):F(y)] = m$ and $[F(x):L] = n$. Now $F(y) \subseteq L$ and, by lemma 3,7, $m \geq n$. Write p in primitive form: $\bar{p}(x,t)=c_n(x)\,t^n+c_{n-1}(x)\,t^{n-1}+\ldots+c_0(x)$.

By lemma 3.7, $g(t)-yh(t)$ has $\bar{p}(x,t)$ as a factor in $F[x,t]$. Thus $h(x)g(t)-g(x)h(t)$ with degree m in x is equal to $\bar{p}(x,t)\bar{q}(x,t)$ of degree greater than or equal to m (since g,h were part of a coefficient). Therefore the degree of $\bar{p}(x,t)$ in x is m, $\bar{q}(x,t)$ is a polynomial in t alone; but by lemma 3.8 $h(x)g(t)-g(x)h(t)$ is primitive, whence q is a constant in F. Then the degree of x over L equals the degree of x over F(y) so n+m, and L=F(y), as was tp be shown.

Theorem 3.10 (Herstein) Suppose F,K, and L are three fields such that $F < K < L$ (proper inclusions). Suppose that for every x in L there exists a non-trivial polynomial $f_x(t)$ in t with coefficients in F (and which depend on x) such that the element $f_x(x)$ is in K. Then either:

(a) L is purely inseparable over K

or (b) L, and so K, is algebraic over F.

Proof: Suppose that L is not purely inseparable over K. Then there exists an element in L which is not in K and which is separable over K. The set of all elements in L, separable over K, forms a subfield L' of L. K is contained in L', because L is not purely inseparable over K, $L \neq K$. If this subfield L' were algebraic over F, then K would also be algebraic over F. This, combined with the fact that L is algebraic over K, would then lead to the desired conclusion that L is algebraic over F. Thus suppose, to the contrary, that there is some element $a \in L'$, $a \notin K$ which is transcendental over F. (Being in L', a is separable over K). The following shows this leads to a contradiction.

Let $\tilde{L} = F(z)$, the set of rational functions in a over the field F. Let $\tilde{K} = \tilde{L} \cap K$. Consider the three fields, $F, \tilde{K}, \tilde{L}$, here $F < \tilde{K} < \tilde{L}$. These inclusions are all proper since $a \in \tilde{L}$, $a \notin \tilde{K}$ and since a is algebraic over $\tilde{K}$ but not over F. If $x \in \tilde{L}$ then there is a polynomial $f_x(t)$ with coefficients in F so that $f_x(x) \in K$; since $f_x(x) \in \tilde{L}$, then $f_x(x) \in \tilde{K}$. Thus the conditions on the three fields, F,K,L carry over to $F, \tilde{K}, \tilde{L}$.

By theorem 3.6, K is a rational function field over F in some s, $\tilde{K} = F(s)$. $\tilde{L} = K(a)$ is of finite degree and separable over $\tilde{K}$. By lemma 3.3 there exist two distinct valuations φ_1, and φ_2 on $\tilde{L}$ which coincide on $\tilde{K}$. Such φ_1 and φ_2 exist which, in addition, are trivial on F. Thus for these two valuations the following properties hold:

1. There exists a $u \in \tilde{L}$, $u \notin \tilde{K}$ so that $\varphi_1(u) \neq \varphi_2(u)$
2. $\varphi_1(k) = \varphi_2(k)$ for all $k \in \tilde{K}$
3. $\varphi_1(\alpha) = \varphi_2(\alpha) = 0$ for all $\alpha \neq 0$ in F.

Without loss of generality it may be assumed that $\varphi_1(u) > 0$. By hypothesis, $k = u^n + \alpha_{n-1}u^{n-1} + \cdots + \alpha_r u^r \in \tilde{K}$ where $\alpha_r, \ldots, \alpha_{n-1} \in F$, $\alpha_r \neq 0$, $n \geq r \geq 1$. Thus $\varphi_1(k) = \varphi_2(k)$. Since $\varphi(\alpha_i) = 0$ for each i (consider only the non-zero coefficients that occur in the expression for k) and since $\alpha_r \neq 0$, $\varphi_1(\alpha_r u^r) = r\,\varphi_1(u) < \varphi_1(\alpha_m u^m) = m\,\varphi_1(u)$ for $m > r$ occurring in the expression for k with non-zero coefficient. Thus, since φ_1 is an exponential valuation, it follows that $\varphi_1(k) = r\,\varphi_1(u)$. Since $0 < \varphi_1(k) = \varphi_2(k)$ then $\varphi_2(k) > 0$. Thus the same argument used for φ_1 can be repeated and it follows that $\varphi_2(k) = r\,\varphi_2(u)$. But $\varphi_1(k) = \varphi_2(k)$ so that $r\,\varphi_1(u) = r\,\varphi_2(u)$ which, since $r = 0$, implies $\varphi_1(u) = \varphi_2(u)$. This is contrary to the assumption that $\varphi_1(u) \neq \varphi_2(u)$.

LIST OF REFERENCES

1. Albert, A. A., Modern Higher Algebra, The University of Chicago Press, Chicago, 1937.

2. Artin, E., Elements of Algebraic Geometry, New York University Institute of Mathematical Sciences, New York, 1955.

3. Herstein, I. N., A Theorem Concerning Three Fields, Canadian Journal of Mathematics, 7(1955), 202-203.

4. MacLane, S., Algebraic Functions, Lectures at Harvard University, Lithoprinted by Edwards Brothers, Inc., Ann Arbor, Michigan, 1947.

5. McCoy, N. H., Rings and Ideals, Carus Mathematical Monographs, The Mathematical Association of America, The Waverly Press, Baltimore, 1948.

6. Nagata, Nakayama, Tuzuku, On An Existence Lemma in Valuation Theory, Nagoya Mathematical Journal, 6(1953), 59-61.

7. Schilling, O. F. G., The Theory of Valuations, American Mathematical Society, New York, 1950.

8. van der Waerden, B. L., Modern Algebra, Revised English Edition, Frederick Ungar Publishing Co., 1953.