1967

Valuation theoretic approach to ideal theory

Janet Mary Corcoran
Southern Illinois University Edwardsville

VALUATION THEORETIC APPROACH TO IDEAL THEORY

A Thesis

Submitted to the Graduate Faculty of
Southern Illinois University
Edwardsville, Illinois
in partial fulfillment of the
requirements for the degree of
Master of Science
in
The Department of Mathematics

by
Janet Mary Corcoran
B.A., Southern Illinois University
Edwardsville, Illinois, 1965

June, 1967

ACKNOWLEDGEMENT

The author wishes to express her sincere appreciation to Professor George V. Poynor for his guidance and interest in this thesis.

TABLE OF CONTENTS

INTRODUCTION

The theory of ideals in a commutative ring with identity forms a significant portion of the theory of such rings. Formally the theory of ideals is developed using the definitions and the properties of rings. A particularly elegant development of ideal theory uses the concept of valuations. In Chapter III, it is shown how the theory of ideals can be expressed in terms of valuation properties.

In order to consider this valuation approach to ideal theory, Chapter II is devoted to a brief development of the definitions and results of valuation theory which are used in Chapter III. The theory of valuations is developed using the concept of a place of a field. It is shown that there exists a 1-1 correspondence between places of a field and equivalent classes of valuations. Because of this, the terms "valuation" and "place" are sometimes substituted for each other, but the meaning remains clear from the context. Also it is shown that there is a correspondence between valuations and prime ideals. Hence these terms are also interchanged at times.

The material in Chapters II and III requires some knowledge of abstract algebra. To facilitate one's reading of Chapters II and III, Chapter I has been written so as to present the necessary algebraic definitions and basic results used in the later chapters. These results will not be proven. A complete discussion of all of these results can be found in any abstract algebra text.

The symbols used are standard notation. The relations of sets, elements of sets, etc., are all denoted by standard notation. All other notation will be defined as it appears.

CHAPTER I

ALGEBRAIC DEFINITIONS AND PROPERTIES

A semigroup is a set and an associative binary operation. A semigroup S has an identity e if for every $x \in S$, $ex = xe = x$.

A group G is a semigroup with an identity e such that for every $x \in G$, there exists $x^{-1} \in G$ such that $xx^{-1} = x^{-1}x = e$. If for every $a,b \in G$, $ab = ba$, G is said to be commutative.

A group G in which every element can be expressed as the power of some element is called cyclic. For $a \in G$, the smallest integer n such that $a^n = e$ is called the order of the element a.

The integers under addition form a group. The rationals $(\neq 0)$ under multiplication form a group.

A nonempty subset H of a group G is a group if H contains the identity and is closed under the operation. If H is a subgroup of G and a is an element of G, then the set $aH = \{ah \mid h \in H\}$ is called a right coset. The set $Ha = \{ha \mid h \in H\}$ is a left coset. If G is commutative, these sets are equivalent. A subgroup is invariant if and only if the right coset determined by any element coincides with the left coset determined by this element. Therefore there is only one coset decomposition of G for an invariant subgroup H.

If H is invariant, then $(xH)(yH) = xHyH = xyHH = xyH$. Hence the set of cosets is closed under the group operation. The collection of cosets, denoted G/H, and the group operation of G form a group. This set G/H is called the factor group of G relative to H.

A mapping of a group G into a group G' is called a homomorphism if the following property holds: for every $x,y \in G$,

$$f(xy) = f(x)f(y).$$

If f is a homomorphism of G onto G', then G' is called a homomorphic image of G. If f is 1-1 and onto, then f is an isomorphism of G onto G'.

The homomorphism of G onto its factor group G/H which maps $a \in G$ onto aH is called the natural homomorphism.

The set of all elements in G such that a homomorphism maps them onto the identity of G' is called the kernel of the homomorphism. The mapping is an isomorphism if and only if the kernel contains only the identity of G.

A ring R is a set and two binary operations called addition and multiplication such that

i) R under addition is a commutative group

ii) R under multiplication is a semigroup

iii) The distributive laws

$$a(b + c) = ab + ac$$

$$(b + c)a = ba + ca$$

hold.

A ring is said to be commutative if the multiplicative semigroup is commutative. R is said to have an identity if its multiplicative semigroup has an identity.

Examples of rings are the rational numbers and the real numbers.

A ring is called an integral domain if it contains no proper divisors of zero. A ring is a division ring if it contains more than one element and the nonzero elements form a group under multiplication.

A division ring in which the multiplicative group is commutative is a field.

Let F be a field. Suppose that 1 is the multiplicative identity, and 0 is the additive identity. Then the smallest natural number m such that m1 = 0 is called the characteristic of F. If no such integer exists, then F is said to have characteristic zero. All fields of characteristic zero contain the integers and hence the rational numbers. If the characteristic $m \neq 0$, them m is a prime.

Consider the set ofaall polynomials in an indeterminant x with coefficients from a field F. The set of such polynomials F[x] is a ring. An element which satisfies a polynomial in F[x] is said to be algebraic over F. If for some element, there does not exist a polynomial in F[x] which it satisfies, then this element is said to transcendental.

A homomorphism of a ring R into a ring R' is a mapping f of R into R' such that for every $a,b \in R$

$$f(a + b) = f(a) + f(b)$$

$$f(ab) = f(a)f(b).$$

If f is 1-1 and onto, it is called an isomorphism.

A ring R is said to be imbedded in a ring B if B contains a subring R' isomorphic to R. The ring R' is called an extension of R. Similarly a field K is an extension of a field k.

Let K be a given extension field of k, and let S be any set of elements in K. There are fields which include k and S. The intersection k(S) of all such fields is a field. k(S) is said to obtained from k by the adjunction of the set S. Extensions by the adjunction of a single element are called simple field extensions.

Let F be a field, and V a nonempty set on which there is defined an operation of addition. The elements of F and of V may be called scalars and vectors, respectively. Assume that there is defined on V a scalar multiplication by elements of F. The set V is then called a vector space over the field F if the following conditions are satisfied:

i) V is an abelian group with respect to addition

ii) $a(X + Y) = aX + aY$ for $a \varepsilon F$, $X,Y \varepsilon V$.

iii) $(a + b)X = aX + bY$ for $a,b \varepsilon F$, $X \varepsilon V$.

iv) $a(bX) = (ab)X$, for $a,b \varepsilon F$, $X \varepsilon V$.

v) $1X = X$ where 1 is the identity of F.

A set $x_1, x_2, . . ., x_n$ of vectors of a vector space V is said to be linearly dependent if there exist elements $a_1, a_2, . . ., a_n$ of F, not all zero, such that $a_1x_1 + a_2x_2 + . . . + a_nx_n = 0$. If the set is not linearly dependent, it is said to be linearly independent. A set of vectors of a vector space form a basis of the space if the vectors are linearly independent, and if every other vector of the space can be expressed as a linear combination of these elements. A vector space V is said to have dimension n if V has a vector basis consisting of n elements,

An extension field K of a field k is called a finite extension if the vector dimension of K over k is finite.

Let R be a ring. A nonempty set A of R is called a right ideal if

i) $a \varepsilon A$ and $b \varepsilon A$ implies $(a - b) \varepsilon A$ (module property)

ii) $a \varepsilon A$ implies $ar \varepsilon A$ for any $r \varepsilon R$.

Similarly a left ideal L is a nonempty subset of R with the module property and such that $a \varepsilon L$ implies $ra \varepsilon L$ for any $r \varepsilon R$. Finally a set A is a two-sided ideal, or an ideal, if A is both a left ideal and a right ideal. If R is commutative, then these types of ideals coincide. Since this thesis considers only commutative rings with identity, we will speak only of ideals.

In every ring R, the set consisting of only the zero forms an ideal, called the zero ideal. The ring R forms an ideal, and it is called the unit ideal.

If in an ideal, every element is of the form $ra + na$ where $r \varepsilon R$, n is an integer, and a is in the ideal, then the ideal is said to be generated by a. Such an ideal is called a principal ideal and will be denoted by (a) where a is the generator. Thus the zero ideal is a principal ideal.

An ideal A is a proper ideal of R if A is properly contained in R, and A is not contained properly in any other proper ideal. A is said to be maximal if A is not contained properly in any other proper ideal. In a ring with identity, every proper ideal is contained in a maximal ideal.

Given any two ideals A and B, their sum $A + B$ and their product AB are also ideals. The ideal B is said to divide the ideal A if and only if B contains A.

For principal ideals in commutative rings with identity, (a) divisible by (b) implies that $a = rb$ for some $r \varepsilon R$. Thus the concept of divisibility of principal ideals is identical to the ordinary concept.

An ideal P is called a prime ideal if and only if for every ab ε P where a $\not\varepsilon$ P, then b ε P. The unit ideal is always prime. The zero ideal is prime if and only if the ring is an integral domain. Any maximal proper ideal P in R is a prime ideal and R/P is a field. If R/P is a field, then P is a maximal ideal. An ideal is said to be primary if and only if for every ab ε P and a $\not\varepsilon$ P, then b^n ε P for some natural number n.

The ideal (A,B) generated by the union of two ideals A and B is the greatest common divisor (gcd) of A and B, since it is a common divisor which is divisible by every common divisor. It is also called the sum of A and B because it contains only elements which are sums of elements of A and B. The gcd of two prime ideals is the entire ring.

The intersection A $\cap$ B of two ideals A and B is called the least common multiple, and every other multiple is divisible by it.

Every ideal in a commutative ring with identity can be expressed as the intersection of a finite number of primary ideals, if every non-empty collection of ideals of the ring contains a maximal element.

CHAPTER II

VALUATIONS

The study of valuations is somewhat facilitated by considering first the subject of places of a field. Let R be a commutative ring with identity. A unit of R is an element of R whose inverse is also in R.

DEFINITION 2.1 A ring R is a local ring if and only if the non-units of R form an ideal in R.

THEOREM 2.1 A ring R is a local ring if and only if there exists exactly one maximal ideal in R.

Proof: Suppose R is a local ring. Then the non-units of R form an ideal A in R. A is maximal since any ideal containing A properly contains a unit and is the ring R.

Suppose A is the only maximal ideal in R. Let a be a non-unit of R. The element a generates a proper ideal since if for some x in R $ax = 1$, then a is a unit. Let (a) be the ideal generated by a. Then (a) is contained in A since every proper ideal is contained in a maximal ideal. Hence A contains the ideals generated by all non-units. A does not contain a unit since A is proper. Thus A contains only the non-units of R. Therefore R is a local ring.

<u>DEFINITION 2.2</u> Let R be a subring of a field k. R is a valuation ring in k if at least one of every pair of inverse elements of k is in R.

<u>THEOREM 2.2</u> A valuation ring R is a local ring.

Proof: Let R be a valuation ring in k. It must be shown that the set A of non-units of R forms an ideal. Choose a,b ε R such that (a + b) is a unit in R. Then (a + b) and $(a + b)^{-1}$ are in R. Suppose a,b $\neq$ 0. If one equals zero, the result is trivial. Suppose that a/b ε R. Then $(1 + \frac{a}{b})$ ε R implies $(\frac{a + b}{b})$ ε R implies $(\frac{1}{b})$ ε R. Thus b is a unit of R. If b/a ε R, then a similar argument shows that a is a unit. Thus if a and b are non-units of R, then (a $\pm$ b) is a non-unit.

Let a,b ε R and ab be a unit of R. Then $a^{-1}b^{-1}$ ε R, and $aa^{-1}b^{-1} = b^{-1}$. Hence b^{-1} ε R. Also, $a^{-1}b^{-1}b = a^{-1}$ and a^{-1} ε R. Thus if a is a non-unit, ab is a non-unit for every b ε R. Hence A is an ideal in R, and R is a local ring.

<u>DEFINITION 2.3</u> Let k be a field. A place of k is a homomorphic mapping ϕ of a subring R of k into a field Δ such that the following conditions are satisfied:

i) if x ε k, x $\notin$ R, then 1/x ε R and $\phi(1/x) = 0$;

ii) $\phi(x) \neq 0$ for some x in R.

<u>THEOREM 2.3</u> To every valuation ring R in k, there corresponds a place, and conversely, to every place ϕ of k, there corresponds a unique valuation ring.

Proof: Let R be a valuation ring in a field k. Let ϕ be a homomorphic mapping of R into the field $\Delta = R/A$ where A is the maximal ideal in R. Suppose $x \varepsilon k$ and $x \notin R$. Then $1/x \varepsilon R$ and $1/x$ is a non-unit of R. Therefore $\phi(1/x) = 0$. Surely, $1 \varepsilon R$, and $\phi(1) \neq 0$. Consequently ϕ defines a place of k.

Now let ϕ be a place of k, and R be its ring of definition. Then $x \varepsilon k$, $x \notin R$ implies $1/x \varepsilon R$. Therefore for every x, $1/x \varepsilon k$ at least one is in R. Consequently R is a valuation ring.

In the remainder of this paper, the valuation ring of a place ϕ will be denoted by R_ϕ .

If $a \varepsilon k$, and $a \notin R$, let$\phi(a) = \infty$. Then ϕ is a homomorphic mapping of R into $\Delta \cup \{\infty\}$. The following are immediate consequences of this change in definition:

i) If $\phi(x) = \infty$ and$\phi(y) \neq \infty$, then $\phi(x \pm y) = \infty$;

ii) If $\phi(x) = \infty$ and $\phi(y) \neq 0$, then $\phi(xy) = \infty$;

iii) If $x \neq 0$, then $\phi(x) = 0$ if and only if $\phi(1/x) = \infty$.

<u>THEOREM 2.4</u> The units of the valuation ring R_ϕ of field k corre - sponding to a place ϕ are fully characterized by $\phi(a) \neq 0$ and $\phi(a) \neq \infty$; the non-units, by $\phi(a) = 0$.

Proof: Suppose $\phi(a) \neq 0$ and $\phi(a) \neq \infty$. Then $\phi(a) \varepsilon \Delta$ and $a \varepsilon R$. If $a^{-1} \notin R$, then $\phi(a^{-1}) = \infty$ and $\phi(a) = 0$. But$\phi(a) \neq 0$. Thus $a^{-1} \varepsilon R$, and a is a unit of R.

Suppose a is a unit of R. Then a, $a^{-1} \varepsilon R$ implies $\phi(a) \neq \infty$ and $\phi(a^{-1}) \neq \infty$. Since ϕ is homomorphism $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(1) = 1$. Thus $\phi(a) \neq 0$, and $\phi(a^{-1}) \neq 0$.

Suppose two places are defined on a subring of a field k. These places are said to be <u>equivalent</u> if and only if their valuation rings coincide. Places which are isomorphisms of k are called <u>trivial</u> places of k.

The existence of places can be shown using the following lemma.

<u>LEMMA</u> Let R be a subring of a field k, containing an identity, and let B be a proper ideal in R. Then for any element x of k at least one of the extended ideals R[x]B, R[1/x]B is a proper ideal of R[x], R[1/x] respectively.

Proof: Suppose neither R[x]B nor R[1/x]B is a proper ideal. Then R[x]B = R[x] and R[1/x]B = R[1/x]. Since 1 ε R[x] and 1 ε R[1/x],

$$(1) \qquad 1 = \sum_{i=0}^{n} a_i x^i \qquad \text{where } a_i \in B,\ 0 \leq i \leq n$$

$$(2) \qquad 1 = \sum_{j=0}^{m} b_j x^{-j} \qquad \text{where } b_j \in B,\ 0 \leq j \leq m.$$

Suppose (1) and (2) are of least degree and m ≤ n.

Multiply (1) by $(1 - b_0)$ and (2) by $a_n x^n$;

$$1 - b_0 = (1 - b_0)\, a_0 + \cdot \cdot \cdot + (1 - b_0) a_n x^n$$

$$(1 - b_0) a_n x^n = a_n b_1 x^{n-1} + \ldots + a_n b_m x^{n-m} .$$

Thus $$1 - b_0 = (1-b_0)a_0 + \ldots + (1-b_0)a_{n-1}x^{n-1} + \ldots + a_n b_m x^{n-m}$$

or $$1 = \sum_{1=0}^{n-1} c_1 x^1 \qquad \text{where } c_1 \in B.$$

But (1) was assumed to be of least degree. Consequently at least one of the extended ideals is a proper ideal.

THEOREM 2.5 Let R be a subring of a field k, containing an identity, and let A be an ideal in R, different from R. Then there exists a place ϕ of k such that $R_\phi \subset R$ and $A_\phi \subset A$ where A_ϕ is the ideal of non-units of R_ϕ.

Proof: Let M denote the set of all subrings S of k such that $R \subset S$ and $SA \neq S$. M is non-empty since $R \in M$. Every totally ordered subset of M has an upper bound in M. Hence M has maximal elements.

Let L be a maximal element of M. Then L has the following properties:

i) $R \subset L$, $LA \neq L$;

ii) if L' is any subring of k such that $L \subset L'$, then $L'A = L'$.

Let R' be the union of the elements of any totally ordered subset of M. Consider the case where $R' = L$. Let P be a proper ideal in R such that $P = LA$. If $x \in k$, and if $L' = L[x]$, $L'' = L[1/x]$, then at least one of the following relations must hold: $L'P = L'$, $L''P \neq L''$. Since L is maximal, either $L = L'$ or $L = L''$; i.e. either $x \in L$ or $1/x \in L$. Hence L is a valuation ring to which there corresponds a place of k.

An important consequence of the existence theorem is the following theorem dealing with the extendability of a place of a field to an overfield.

EXTENSION THEOREM If k is a subfield of K, then any place of k can be extended to a place of K.

DEFINITION 2.4 Let k be a field, R be any subring containing the identity, and suppose α is an element of k. α is integral with respect to R if and only if α satisfies an equation of the form

$$\alpha^n + a_1\alpha^{n-1} + . . . + a_n = 0$$

where $a_i \in R$, $i = 1,2,. . .,n$.

Divide $\alpha^n + a_1\alpha^{n-1} + . . . + a_n = 0$ by α^{n-1}. Then

$$\alpha + a_1 + a_2\alpha^{-1} +. . . + a_n\alpha^{-(n-1)} = 0$$

$$\alpha = -a_1 - a_2\alpha^{-1} -. . . - a_n\alpha^{-(n-1)}.$$

Thus if α is integral with respect to R, $\alpha \in R[\alpha^{-1}]$; or, equivalently, α is a unit in $R[\alpha^{-1}]$.

THEOREM 2.6 α is integral with respect to R if and only if for every place ϕ of k for which the mapping ϕ restricted to R ($\phi|$ R) is finite, $\phi(\alpha)$ is also finite.

Proof: Let α be integral with respect to R, and let ϕ be a place of k for which $\phi|R$ is finite. Suppose $\phi(\alpha) = \infty$. Then$\phi(\alpha^{-1}) = 0$. Now $\alpha^n + a_1\alpha^{n-1} + . . . + a_n = 0$ and $1 + a_1\alpha^{-1} + . . . + a_n\alpha^{-n} = 0$.

$$\phi(1 + a_1\alpha^{-1} + . . .+ a\alpha_n^{-1}) = 1 + 0 + . . .+ 0 + 0 = \phi(0) = 0.$$

Hence $\phi(\alpha)$ is finite.

Suppose α is non-integral with respect to R. Let A be a maximal prime ideal of $R[\alpha^{-1}]$ containing α^{-1}. Let f be the natural homomorphism of $R]\alpha^{-1}]$ onto $R[\alpha^{-1}]/A$. This homomorphism is non-trivial. Thus it determines a place ϕ of $k[\alpha^{-1}]$. For every such place ϕ, ϕ restricted to R is finite, sinceϕ restricted to $R[\alpha^{-1}]$ is finite. Further $\phi(\alpha^{-1}) = f(\alpha^{-1}) \varepsilon f(A) = 0$. Hence $\phi(\alpha) = \infty$. Hence the theorem.

The kernel of ϕ in $R[\alpha^{-1}]$ is A. The kernel of ϕ in R is a prime ideal and is the intersection of R and A. This ideal is a maximal ideal in R.

<u>THEOREM 2.7</u> If 0 is the set of all elements of k integral with respect to R, then 0 is a ring. The integral closure of 0 is 0. 0 is the intersection of all valuation rings of k which contain the ring R.

Proof: Let α be in the integral closure I of 0. Then for every place ϕ of k,$\phi(\alpha)$ is finite when ϕ restricted to 0 is finite. But an element of 0 is integral with respect to R. For every ϕ of k for which ϕ restricted to R is finite, $\phi(x)$ is finite. Hence the places for which ϕ restricted to R is finite are those where ϕ restricted to 0 are finite. Thus for such ϕ , $\phi(\alpha)$ is finite. Hence α is integral with respect to R. Since I is contained in 0 and 0 is contained in I, I = 0.

Let I be the intersection of all valuation rings of k which contain the ring R. I is a ring. If x ε I, then x ε R_ϕ for every ϕ. Thus $\phi(x)$ is finite over R and $\phi(x)$ is finite for x ε R_ϕ . Therefore x ε 0. Then for every ϕ finite over R. $\phi(x)$ is finite. Consequently x ε R_ϕ for every ϕ. Hence the intersection of all the valuation rings of k is 0.

Again before considering valuations, consider the concept of an ordered group.

DEFINITION 2.5 The group G is an ordered group if it contains a semigroup S with the following properties:

i) $aSa^{-1} \subset S$ for all $a \varepsilon S$;

ii) $G = S \cup \{1\} \cup S^{-1}$ where $S^{-1} = \{s^{-1} \mid s \varepsilon S\}$.

DEFINITION 2.6 An ordered group is a completely ordered set by the order relation $a < b$ if and only if $ab^{-1} \varepsilon S$.

The definition is symmetric with respect to left and right multiplication, since

$$ab^{-1} \varepsilon S \text{ implies } b^{-1}a = b^{-1}(ab^{-1})b \varepsilon b^{-1}Sb \subset S,$$

and similarly

$$b^{-1}a \varepsilon S \text{ implies } ab^{-1} \varepsilon S.$$

Transitivity can be shown, since $a < b$, $b < c$ implies $ab^{-1} \varepsilon S$, $bc^{-1} \varepsilon S$ implies $ab^{-1}bc^{-1} = ac^{-1} \varepsilon S$ implies $a < c$.

Completeness follows directly from the defnition of ordered group since for any a,b either $ab^{-1} \varepsilon S$ or $ab^{-1} = 1$ or $ab^{-1} \varepsilon S^{-1}$ always holds, and hence either $a < b$, $a = b$, or $b < a$.

The complete ordering of an ordered group G has the following properties: For a,b,c,d,ε G

i) $a < b$ implies $ac < bc$, $ca < cb$;

ii) $a < b$, $c < d$ implies $ac < bd$;

iii) $a < b$ implies $b^{-1} < a^{-1}$;

iv) $a < 1$ if and only if $a \varepsilon S$.

Let $G = G' \cup \{\infty\}$ where G' is an additive ordered abelian group such that the following properties hold:

i) for every x in G', $x + \infty = \infty$

ii) for every x in G', $x < \infty$.

DEFINITION 2.7 Let k be a field. Let G be the set defined above. A valuation of k is a mapping v of k into G such that

i) $v(x) = \infty$ if and only if $x = 0$,

ii) $v(xy) = v(x) + v(y)$, for all x,y in k;

iii) $v(x + y) \geq \min \{v(x), v(y)\}$, for all x,y in K.

The multiplicative group of k is mapped into group G' and in most cases will be the only values considered. For any x in k, v(x) is called the value of x in the valuation v.

A valuation v is called non-trivial if $v(a) \neq 0$ for some a in k; otherwise, v is called trivial.

Let 0 be the zero of the group G'. Then the following are immediate consequences of the definition.

$v(1) = 0$ since v is a homomorphism.

$v(-1) = 0$, since $0 = v(1) = v(-1 \cdot -1) = v(-1) + v(-1)$ and G' is totally ordered.

$v(a) = v(-a)$, since $v(-a) = v(-1a) = v(-1) + v(a) = v(a)$.

$v(a^{-1}) = -v(a)$, since $v(1) = v(aa^{-1}) = v(a) + v(a^{-1}) = 0$ and hence $-v(a) = v(a^{-1})$.

$v(e) = 0$ if e is a root of unity. This implies that the only valuation of a finite field is the trivial valuation.

$v(x - y) \geq \min\{ v(x), v(y)\}$. For $v(x - y) \geq \min\{v(x), v(y)\}$

$v(x) < v(y)$ implies $v(x + y) = v(x)$.

Proof: $v(x + y) \geq \min\{ v(x), v(y)\} = v(x)$.

But $x = (x + y) - y$. So $v(x) \geq \min\{ v(x + y), v(y)\}$.

$v(x) \geq v(x + y)$ since by assumption $v(x) < v(y)$.

Thus $v(x) = v(x + y)$.

Let $k = Q$ be the field of rational numbers and let Q' denote the multiplicative group of Q. Let p be a fixed prime number. Every rational number a can be written $a = p^e b$ where e is an integer and b is a rational number prime to p.

Define a mapping v_p of Q' into Z, the additive group of integers, such that

$$v_p(x) = e, \text{ if } x = p^e b \text{ in } Q'.$$

Choose any x,y in Q', $x = p^e b$, $y = p^f c$. Then

$$v_p(xy) = v_p(p^{e+f}bc) = e + f = v_p(x) + v_p(y).$$

Thus v_p satisfies the second condition of the definition of a valuation.

Again consider x and y as given above. Assume $e < f$. Then

$$v_p(x + y) = v_p(p^e(b + p^{f-e}c)).$$

If $(b + p^{f-e}c)$ is prime to p, $v_p(x + y) = e$. If $(b + p^{f-e}c))= mp^r$ for some m and r, then $v_p(x + y) = e + r$. Hence $v(x + y) \geq \min\{v(x)v(y)\}$ Thus the third condition of the definition is satisfied.

Define $v_p(0) = \infty$.

The mapping v_p is a valuation of Q into $Z \cup \{\infty\}$.

Using multiplicative notation, a valuation may be defined as follows:

A valuation of a field k is a mapping v of k into an ordered group G with zero-element 0, such that the following properties hold:

i) $v(a) \geq 0$ for all $a \in k$, $v(a) = 0$ if and only if $a=0$;

ii) $v(ab) = v(a)v(b)$ for all $a,b \in k$;

iii) $v(a + b) \leq v(a) + v(b)$.

Using this notation, one may consider ordinary absolute value as a valuation of the real numbers into the non-negative real numbers.

Consider the set $R_v = \{x| \ x \in k, v(x)\} \geq 0$. The set R_v forms a ring. R_v is called the valuation ring of v. $R_v$is a valuation ring because for every $x \in k'$ (the multiplicative group of k), either $v(x)\geq 0$ or $v(1/x) \geq 0$ and hence either x or 1/x belongs to R_v. The relation $y|x$, defined by the condition that there exists a $z \in R_v$ such that $x = yz$, is equivalent to $v(x) \geq v(y)$.

DEFINITION 2.7 Two valuations are called equivalent valuations if and only if they have the same valuation ring.

The group of units of R_v is the set $\{x| \ x \in k, v(x) = 0\}$; the maximal ideal A of non-units of R_v is the set $A =\{ x| \ x \in k, v(x)>0\}$.

It has been shown that to every valuation ring there corresponds a place. For every valuation v, the set $R_v = \{x| \ x \in k, v(x) \geq 0\}$ is a valuation ring. To R_v, there corresponds a place. This place corresponds to a class of equivalent valuations which have R_v as their valuation ring.

Conversely for every ϕ of k, there corresponds a unique valuation ring R_ϕ. Let A be the maximal ideal in R_ϕ, and let U be the group of units of R_ϕ. Denote the quotient group by k/U and write the group operation additively. Let v be the natural homomorphism of k onto k/U. For every a,b ε k, $v(ab) = ab + U = (a + U) + (b + U) = v(a) + v(b)$. For ever a,b ε k, and if $v(a) \leq v(b)$, then

$$\begin{aligned} v(a + b) &= (a + b) + U = a(1 + \frac{b}{a}) + U \\ &= (a + U) + ((1 + \frac{b}{a}) + U) \\ &= v(1 + \frac{b}{a}) + v(a). \end{aligned}$$

But $v(a) \leq v(b)$ implies $b/a \; \varepsilon \; R_\phi$, and hence $(1 + \frac{b}{a}) \; \varepsilon \; R_\phi$. Therefore $v(1 + \frac{b}{a}) \geq 0$. Consequently $v(a + b) \geq v(a)$.

All that remains is to show that k/U is ordered. But $k/U = A/U \cup U/U \cup A^{-1}/U$ where $A^{-1} = \{a | \; a^{-1} \; \varepsilon \; A\}$ and A/U, U/U, and A^{-1}/U are pairwise disjoint. Let A/U be the required semi-group. Then for every a ε k/U, $a(A/U)a^{-1} \subset A/U$ since the product of a non-unit with any other element is a nonunit. Therefore k/U is ordered. v is a valuation of k with valuation ring R_ϕ. Thus for every place ϕ of k, there corresponds a class of equivalent valuations.

<u>DEFINITION 2.8</u> A valuation v is said to be a valuation of rank 1 if and only if the valuation group G' can be mapped order-isomorphically into a subgroup of the additive group of real numbers.

One may consider equivalence relationships for valuations of rank 1. Let v and u be valuations of a field. Let G be an additive group of a field F; and let R be the real numbers. Suppose

i) u is not a trivial valuation

ii) $u(a) < 0$ implies $v(a) < 0$.

Substituting $u(1/a)$ for $u(a)$ in (ii) yields $u(a) > 0$. Therefore $v(a)>0$.

Suppose $u(a) = 0$. By (i), there exists $b \in G$ such that $u(b) > 0$. But then $u(a^n b) > 0$ implies $v(a^n b) > 0$ implies $v(a) \geq \frac{-v(b)}{n}$ for any n. Letting $n \to \infty$, $v(a) \geq 0$.

Since a similar situation arises for $1/a$, $u(a) = 0$ implies $v(a)=0$.

Additional relationships derived from (i) and (ii) are the following:

$u(a) < u(b)$ implies $v(a) < v(b)$

$u(a) = u(b)$ implies $v(a) = v(b)$

$u(a) > u(b)$ implies $v(a) > v(b)$.

Since u is not trivial, there exists a fixed $c \in G$ such that $u(c) > 0$. For any given element $a \in G$, there exists a real number r such that $u(a) = ru(c)$. For any rational number $n/m > r$,

$$u(a) < \frac{n}{m} u(c) \text{ implies } u(a^m) < u(c^n) \text{ implies } v(a^m) < v(c^n).$$

Hence $v(a) < \frac{n}{m} v(c)$. Similarly if $r > n/m$, then $u(a) > \frac{n}{m} u(c)$ implies $v(a) > \frac{n}{m} v(c)$. Therefore $v(a) = rv(c)$.

Now $u(a) = ru(c)$ and $v(a) = rv(c)$ imply $v(a) = \alpha u(a)$ where $\alpha = \frac{v(c)}{u(c)}$. Since c was a fixed point in G, then $v(a) = \alpha u(a)$ holds for every $a \in G$. Thus v can be obtained by first applying u, then αu.

Applying these results to valuations of rank 1, identify G with k', the multiplicative group of k. Then two such valuations of k, in which the same inequalities arise between elements of the field, are multiples of each other. Thus one obtains the following definition.

Two valuations of rank 1, u and v, are called equivalent

if and only if $u = \alpha v$ for some $\alpha \epsilon R$.

A class of equivalent valuations consists of all multiples of some fixed valuation.

Thus far the field k has been any field. It was mentioned that the only valuation of a finite field was the trivial valuation. Further restrictions to the kinds of valuations permitted are consequences of the following definition,

DEFINITION 2.9 A valuation v is non-archimedean if and only if for some multiple m of 1, $v(m) = 0$. Otherwise, v is said to be archimedean.

Consider again the example of the rational numbers.

THEOREM 2.8 Any non-trivial, non-archimedean rank 1 valuation of Q is equivalent to a p-adic valuation for some prime p.

Proof: For every integer n, $v(n) \geq 0$. If.$v(n) = 0$ for every integer, then v is trivial. Thus there exists an integer $b \neq 0$ such that $v(b) > 0$. Let $B =\{ b| \ v(b) > 0\}$. B is an ideal in the ring of integers Z. Suppose $b,b' \epsilon B$. Then $v(b - b') \geq \min \{v(b), v(b')\}$ which implies $v(b - b') > 0$. Therefore $b - b' \epsilon B$. Also suppose $c \epsilon Z$, and $b \epsilon B$. Then $v(cb) = v(c) + v(b) > 0$. Consequently $cb \epsilon B$, and B is an ideal.

Let $a,c \in Z$ such that $a,c \notin B$. Then $v(a) = 0 = v(c)$ which implies that $0 = v(a) + v(c) = v(ac)$. Therefore $ac \notin B$. Thus B is also a prime ideal in Z. Hence $B = (p)$ where p is a prime.

Since $p \in B$, $v(p) > 0$. Therefore let $v(p) = s$. Let n be any integer. Then $n = n'p^k$ where $k \geq 0$ and $(n',p) = 1$. Thus $n' \notin B$ and $v(n') = 0$. $v(n) = v(n') + kv(p) = ks$. Hence v is a multiple of the p-adic valuation determined by p.

<u>THEOREM 2.9</u> Up to equivalence, the field Q of rational numbers has only one archimedean valuation, the usual absolute value.

Proof: Let $n, n' > 1$ be integers. Then $n' = a_0 + a_1 n + . . . a_k n^k$ where $0 \leq a_i < n$, $a_k \neq 0$.

$$v(n') \leq v(a_0) + v(a_1)\ v(n) + . . . + v(a_k)\ v(n)^k$$

where v is any archimedean valuation of Q. Since $0 \leq v(a_i) \leq v(_i < n$,

$$v(n') < n\surd[1 + v(n) + ... + v(n)^k] < n(k + 1)\max\{ 1, v(n)^k\} .$$

$n' \geq n^k$. Thus

$$k \leq \frac{\log n'}{\log n} \text{ implies } v(n') < n(\frac{\log n'}{\log n} + 1) \max \{1, v(n)^{\frac{\log n'}{\log n}} \}.$$

Now replace n' by $(n')^r$. Let $\log n'/\log n = t$. Thus

$$v(n')^r < n(rt + 1)\max \{1, v(n)^{rt}\} .$$

$$v(n') < [n(rt + 1)]^{1/r}\{\max\ 1, v(n)^t\} .$$

Consider the limit of the right member of the inequality as $r\to\infty$.

$$v(n') < \max \{1, v(n)^t\} .$$

Since v is archimedean, n' can be chosen so that $v(n') > 1$; hence

$$1 < v(n) \leq v(n)^t.$$

Thus $v(n) > 1$, so interchange n and n'. Then

$$v(n)^{\frac{1}{\cancel{\log} n}} = v(n')^{\frac{1}{\log n'}}$$

for any two positive n, n'. Then $\log v(n)/\log n$ is a positive real number s independent of n and $v(n) = n^s$. Hence $v(a) = |a|^s$ for every rational number a. Thus v is a power of the absolute value valuation.

Let $v_1, v_2, \ldots, v_n$ be a finite system of non-trivial inequivalent valuations of rank 1 of a field k. It will be shown that these n valuations are independent in the sense that none can be expressed in terms of the others.

LEMMA There exists an element $a \in k$ such that $v_1(a) > 0$ but $v_i(a) < 0$ for $i = 2,3,\ldots,n$.

Proof: The proof is by induction on n. If $n = 1$, the assertion is trivial. Suppose $n = 2$. Then since v_1 and v_2 are inequivalent, there exists $b \in k$ such that $v_1(b) < 0$ and $v_2(b) \geq 0$. Similarly there exists $c \in k$ such that $v_1(c) \geq 0$ and $v_2(c) < 0$.

Since k is a field, $c/b \in k$. Let $a = c/b$. Then

$$v_1(a) = v_1(c) - v_1(b) > 0 \quad ;$$

$$v_2(a) = v_2(c) - v_2(b) < 0 \quad .$$

Thus the element a has the required property.

Suppose the assertion is true for n - 1 of the n valuations. Then there exists b ε k and c ε k such that

$$v_1(b) > 0, \quad v_i(b) < 0 \qquad (i = 2,3,\ldots,n-1)$$

$$v_1(c) > 0, \quad v_n(c) < 0.$$

Let $a = b^r + c$ where r is a natural number. Consider two cases.

Case 1. $v_n(b) < 0$.

$$v_1(a) = v_1(b^r + c) \geq \min\{ v_1(b^r), v_1(c)\} \text{ implies}$$

$$v_1(a) > 0.$$

$$v_i(a) = v_i(b^r + c) \geq \min\{ v_i(b^r), v_i(c)\} .$$

For sufficiently large r,

$$v_i(b^r) = rv_i(b) < v_i(c) \text{ implies}$$

$$v_i(a) = v_i(b^r + c) = v_i(b^r) < 0.$$

Also $$v_n(a) = v_n(b^r + c) \geq \min \{v_n(b^r), v_n(c)\} .$$

For sufficiently large r

$$v_n(a) = v_n(b^r + c) = v_n(b^r) < 0.$$

Therefore a satisfies the assertion.

Case 2. $v_n(b) > 0$.

$$v_1(a) = v_1(b^r + c) \geq \min \{v_1(b^r), v_1(c)\} \text{ implies}$$

$$v_1(a) > 0.$$

$$v_i(a) = v_i(b^r + c) \geq \min \{v_i(b^r), v_i(c)\}$$

$$= v_i(b^r) < 0 \quad \text{for sufficiently large r..}$$

$$v_n(a) = v_n(b^r + c) \geq \min \{v_n(b^r), v_n(c)\} .$$

$$= v_n(c) < 0 \quad \text{since } v_n(c) < v_n(b^r),$$

Hence a satisfies the assertion.

LEMMA 2 There exists $b \varepsilon k$ such that $v_1(b) = 0$ and $v_i(b) > 0$ for $i = 2,3,\ldots,n$.

Proof: From the preceding lemma, there exists $a \varepsilon k$ such $v_1(a) > 0$ and $v_i(a) < 0$. Let $b = (a + 1)/(a^r + 1)$ where r is an integer. Then since $v_1(1) = 0$,

$$v_1(b) = v_1(\frac{a + 1}{a^r + 1}) = v_1(a + 1) - v_1(a^r + 1)$$

$$= v_1(1) - v_1(1) = 0.$$

Since $v_i(a) < v_i(1)$,

$$v_i(b) = v_i(a + 1) - v_i(a^r + 1)$$

$$= v_i(a) - rv_i(a) = -(r-1)v_i(a) > 0$$

for some r greater than 1.

<u>THEOREM 2.10 Approximation Theorem</u>. Let $\beta_1, \beta_2, \ldots, \beta_n$ be n elements of k. Then for every real $\varepsilon > 0$, there exists $a \varepsilon k$ such that

$$v_i(a - \beta_i) > \varepsilon, \; i = 1,2,\ldots,n.$$

Proof: From Lemma 2, there exists $b_1, b_2, \ldots, b_n$ such that $v_i(b_i) = 0$ and $v_j(b_i) > 0$. Consider $c_i = \dfrac{b_i}{b_1 + b_2 + \ldots + b_n}$.

$$v_i(c_i) = v_i(b_i) - v_i(b_1 + \ldots + b_n) = 0$$

and

$$v_j(c_i) = v_j(b_i) - v_j(b_1 + \ldots + b_n) = v_j(b_i) > 0.$$

Also $v_i(c_i - 1) > 0$.

Since the valuations are of rank 1, there exists an integer n such that both of the following inequalities are true:

$$n\, v_i(c_i - 1) + v_i(\beta_i) > \varepsilon$$

$$n\, v_j(c_i) + v_j(\beta_i) > \varepsilon \quad .$$

Now let $\alpha_i = 1 - (1 - c_i^n)^n$. Then

$$v_i(\alpha_i - 1) = n\, v_i(1 - c_i^n) \geq n\, v_i(1 - c_i).$$

Hence $\quad v_i(\alpha_i - 1) + v_i(\beta_i) > \varepsilon$ or $v_i(\beta_i(\alpha_i - 1)) > \varepsilon$.

$\alpha_i = 1 - (1 - c_i^n)^n = c_i^n\, f(c)$ where $f(c)$ is a polynomial with coefficients in k. Thus

$v_j(\alpha_i) = n\, v_j(c_i) + v_j(f(c_i))$ which implies

$$v_j(\alpha_i) \geq n\, v_j(c_i).$$

Therefore $v_j(\beta_i \alpha_i) > \varepsilon$.

Let $a = \beta_1\alpha_1 + \beta_2\alpha_2 + \ldots + \beta_n\alpha_n$.

$$v_i(a - \beta_i) = v_i(\beta_i(\alpha_i - 1) + \sum \beta_j\alpha_j) \qquad i \neq j$$

$$\geq \min \{v_i(\beta_i(\alpha_i - 1)), v_i(\beta_j\alpha_j)\}$$

$$> \varepsilon.$$

Corollary A relation of the form $\sum c_i v_i(a) = 0$ with real c_i can hold for all $a \varepsilon k$ only if all the c_i's = 0.

A valuation of rank 1 induces a topology, called the v-topology, on k defined by neighborhoods of zero: $\{a| \; |v(a)| < \varepsilon\}$ where $\varepsilon > 0$ is a real number. The n elements $\beta_1, \beta_2, \ldots, \beta_n$ of the field k can in their corresponding v_i-topology be approximated to any degree by a single element.

Valuations can be used to introduce the concept of completion for fields. The definitions and theorems involved follow closely those used in analysis.

DEFINITION 2.10 Let K be a field with a rank 1 valuation v. A sequence $\{a_k\}$, $k = 1,2, \ldots$ is said to converge in K (relative to v) if there exists an $a \varepsilon K$ such that for $\varepsilon > 0$, there exists an integer N depending only on ε such that $v(a - a_n) < \varepsilon$ for all $n > N$. Then a is unique and is called the limit of $\{a_k\}$. If $a = 0$, $\{a_k\}$ is called a null sequence. A sequence $\{a_k\}$is called a Cauchy sequence if for $\varepsilon > 0$ there exists an integer N depending only on ε such that for $m,n \geq N$

$$v(a_m - a_n) < \varepsilon.$$

DEFINITION 2.11 A field K is said to be complete with respect to a rank 1 valuation v if and only if every Cauchy sequence of elements of K is convergent with respect to v.

If K' is an extension field of K, and v is a rank 1 valuation of K, a valuation v' of K' such that $v(x) = v'(x)$ for all $x \varepsilon K$ is called an extension of v, or a valuation extensión of v.

The construction of a completion K' of any field K with respect to a rank 1 valuation v yields the following:

i) K' is an extension of K and v' is a valuation extension of v;

ii) K' is complete with respect to v';

iii) $K \subset K'$ and K' is dense in K, i.e. for every $a \varepsilon K'$, a is a limit of a Cauchy sequence of elements of K.

A brief outline of the proof of the above will be given here. The complete proof can be found in Appendix, 2.

If C is the set of Cauchy sequences, then C is a ring with respect to the operations $\{a_k\} + \{b_k\} = \{a_k + b_k\}$ and $\{a_k\}\{b_k\} = \{a_k b_k\}$. The sequence $\{a\}$where $a_k = a$ for all k is a constant sequence. In the ring $\{0\}$ is the additive identity, and $\{1\}$ is the multiplicative identity. C contains a subring of constant sequences which is isomorphic to K.

Let Z be the set of null sequences of C. Then Z is a maximal proper ideal in C. Thus C/Z is a field. Let K' = C/Z. Then K' contains a subfield isomorphic to K such that K' is the completion of K if K is identified with this isomorphic subfield.

The completion K' of any field K with respect to a rank 1 valuation is an extension of K and the valuation v' of K' is an extension of v. Consider now the extendability of a general valuation.

Consider first the extendability of non-archimedean valuations v of a field k. If v is the trivial valuation of k, then v can be extended to the trivial valuation in any overfield of k. Therefore assume that the non-archimedean valuations are also non-trivial.

THEOREM 2.11 Any non-archimedean valuation of a field k can be extended to a non-trivial valuation of any extension field of k.

Proof: Let v be any non-archimedean, non-trivial valuation of a field k, mapping k onto an ordered group G. Let K be any field extension of k.

By the extension theorem, a given place of k can be extended to a place of K. In particular if $\phi: k \to F \cup \{\infty\}$ is a non-trivial place of k with valuation ring R, then ϕ restricted to R maps R into F and this restriction is a non-trivial homomorphism of R. Since R is a subring of k, the extension theorem implies the existance of a place ϕ' of K with ϕ' restricted to R being equivalent to ϕ restricted to R ($\phi'|R = \phi|R$).

Also $a\varepsilon$ k, a $\notin$ R implies that $\phi(a) = \infty$ which implies $\phi(a^{-1}) = 0$. Hence $\phi'(a^{-1}) = 0$. Thus $\phi'(a) = \infty$. Therefore$\phi'|k = \phi|k$, and ϕ' extends the place ϕ onto K.

It now suffices to show the following: If ϕ is a place of k corresponding to the valuation v, and if ϕ' is a place of K which extends ϕ, then the valuation v', generated by ϕ' on K is, by suitable choice of the valuation group, an extension of the valuation v of k.

Let R' be the valuation ring corresponding to ϕ'. R' is given by:

$$R' = \{a \mid a \,\varepsilon\, K, \ \phi'(a) \text{ is finite}\}$$

$$= \{a \mid a \,\varepsilon\, K, \ v'(a) \geq 0 \}.$$

The valuation ring R of ϕ is given by:

$$R = \{a \mid a \,\varepsilon\, k, \ \phi(a) \text{ is finite}\}$$

$$= \{a \mid a \,\varepsilon\, k, \ v(a) \geq 0 \}.$$

Thus if ϕ' extends ϕ, then $R = R' \cap k$. If v' extends v, then $R = R' \cap k$.

Consider the converse of the two preceding statements.

Let R' and R be valuation rings of K and k respectively, where $R = R' \cap k$. Let P' and P be the respective prime ideals of R' and R; U' and U, the corresponding groups of units. Then $P'^{-1} = \{a^{-1} \mid a \,\varepsilon\, P'\}$ is the complement of R' in K, and $P^{-1} = \{a^{-1} \mid a \,\varepsilon\, P\}$ is the complement of R in k. Thus $R = R' \cap k$ implies $P^{-1} = P'^{-1} \cap k$ implies $P = P' \cap k$. Also $U = U' \cap k$. Thus U is a subgroup of U'.

I. As valuations corresponding to R' and R, define v' and v as follows:

In K: $v'(a) = aU'$, with the ordering relation $v'(a) > 0$ implying $a \,\varepsilon\, P'$.

In k: $v(a) = aU$, with the ordering relation $v(a) > 0$ implying $a \,\varepsilon\, P$.

The mapping $aU \rightarrow aU'$ is well-defined since $aU' = (aU)U'$, and is a homomorphism. It is also an isomorphism, since the kernel of the mapping consists only of the unity of U. Thus

$a \,\varepsilon\, k$, $aU' = U'$ if and only if $a \,\varepsilon\, k$, $a \,\varepsilon\, U'$
$a \,\varepsilon\, k$, $aU' = U'$ if and only if $a \,\varepsilon\, U' \cap k = U$

$a \,\varepsilon\, k$, $aU' = U'$ if and only if $aU = U$.

The ordering is also invariant under the isomorphism. If the aU are identified with their images aU', then v' is an extension of v.

II. As places ϕ' and ϕ, corresponding to R' and R, respectively, let them be defined as follows:

$$\text{In } K: \quad \phi'(a) = \begin{array}{ll} \infty & \text{if } a \notin R' \\ a + P' & \text{if } a \in R' \end{array}$$

$$\text{In } k: \quad \phi(a) = \begin{array}{ll} \infty & \text{if } a \notin R \\ a + P & \text{if } a \in R \end{array}$$

Map $\phi(k)$ into $\phi'(k)$ as follows:

$$\infty \to \infty$$

$$a + P \to a + P'$$

Since $a + P' = (a + P) + P'$, the mapping is well-defined and its restriction to R, $\phi(R) = R/P$ is an isomorphism. Hence the field R/P can be isomorphically mapped into R'/P'. Identify the inverse image with its isomorphic image. Then ϕ' is an extension in K of the place ϕ of k. Thus the extension of the valuation is equivalent to the extension of the corresponding place. Hence the theorem.

The question now arises as to whether an extension of a rank 1 valuation is again a rank 1 valuation. In general this is not the case. However, it is the case when the field extension is finite.

Consider first the case of a trivial valuation.

Let v be the trivial valuation of k. It will be shown that only the trivial valuation of K, an algebraic extension of k, extends the trivial valuation of k.

Suppose v' is a valuation of K, trivial on k. Suppose v' is non-trivial on K. Then there exists $\alpha \varepsilon K$ such that $v'(\alpha) \neq 0$. Let $v'(\alpha) < 0$. Since K is algebraic over k, $\alpha \varepsilon K$ satisfies a polynomial $x^n + a_1x^{n-1} + \ldots + a_n = 0$ where $a_i \varepsilon k$. Thus

$$\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0$$

$$\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha = -a_n$$

$$v'(\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha\ ) = v'(-a_n) = 0.$$

But $v'(\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha) \geq \min\{\ v'(\alpha^i)\}$

and for all $i = 1, 2, \ldots, n-1$, $n\ v'(\alpha) < (n - i)\ v'(\alpha)$. Thus

$$v'(\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha) = n\ v'(\alpha) < 0.$$

Consequently $v'(\alpha) \geq 0$. A similar computation shows that $v'(\alpha)$ can not be greater than zero. Therefore $v'(\alpha) = 0$ and v' must be the trivial valuation on K.

Let v' be a non-trivial non-archimedean valuation of K (not necessarily a rank 1 valuation); ϕ', the corresponding place; and k, some subfield of K. The restrictions of v' and ϕ' onto k yield respectively a valuation v of k and a place ϕ of k. The group of values G' for K contains the group of values G for k.

DEFINITION 2.12 The groups G' and G are the respective value groups. The index $e = (G':G)$ is called the ramification index.

The ramification index is a measure of how many new values are

int

introduced by the extension. The image field $\phi'(R')$ contains the image field $\phi(R)$ as a subfield where R' and R are the respective valuation rings.

DEFINITION 2.13 The degree $f = [\ \phi'(R') : \phi(R)]$ is called the residue class degree.

THEOREM 2.12 If K is a finite extension of k, then both e and f are finite and

$$ef \leq n = [K:k].$$

Proof: Let $\beta_1, \ldots, \beta_r$ be elements of K such that the cosets $v(\beta_1) + G, \ldots, v(\beta_r) + G$ are all different from each other, and let $w_1, \ldots, w_s$ be elements of R' so that $\phi'(w_1), \ldots, \phi'(w_s)$ are linearly independent over $\phi(R)$.

It will be shown that the rs elements $w_i\beta_j$ $(i=1,\ldots,s; j=1,\ldots,r)$ of K are linearly independent over k. This implies that $rs \leq n$.

Let $a_1, a_2, \ldots, a_s$ be elements of k, not all zero, and let $v(a_m) = \min_i \{ v(a_i)\}$. Then

$$v(a_1w_1 + \ldots + a_sw_s) = v(a_m) + v(x_1w_1 + \ldots + x_sw_s)$$

with $x_i = a_i/a_m$. But this implies $v(x_i) \geq 0$ and $v(x_m) = 0$. Hence

$$x_1w_1 + \ldots + x_sw_s \in R' \text{ and } v(x_1w_1 + \ldots + x_sw_s) \geq 0.$$

Since

$$\phi'(x_1w_1 + \ldots +x_sw_s) = \phi'(x_1)\phi'(w_1) + \ldots + \phi'(x_s)\phi'(w_s)$$

$$= \phi(x_1)\phi'(w_1) + \ldots + \phi(x_s)\phi'(w_s) \neq 0$$

and since $\phi(x_m) = \phi(1) = 1$ and the w_i's are linearly independent over $\phi(R)$, then $v(x_1w_1 + \ldots + x_sw_s) = 0.$

Hence $v(a_1w_1 + . . . + a_sw_s) = \min\limits_{i} \{v(a_i)\}$.

Define a relation

$$\sum (a_{1j}w_1 + a_{2j}w_2 + . . . + a_{sj}w_s) \; \beta_j = 0$$

where $a_{ij} \in k$, such that

$$v(a_{1j}w_1 + a_{2j} \, w_2 + . . . + a_{sj}w_s) = \min \{v(a_{ij})\} \, ,$$

if not all the a_{ij} are equal to zero.

The values of each of the summands are all different because they lie in distinct cosets. Hence

$$v(\sum a_{ij}w_i\beta_j) = v(0) = \infty$$

$$v(\sum a_{ij}w_i\beta_j) = \min \{v(a_{1j}w_1 + . . . + a_{sj}w_s) + v(\beta_j)\}.$$

Thus $\qquad v(a_{1j}w_1 + . . . a_{sj}w_s) = \infty \qquad$ which implies

$$\min \{v(a_{ij})\} = \infty \, .$$

Therefore $a_{ij} = 0$ for all i,j. The $w_i\beta_j$ are linearly independent over k.

THEOREM 2.13 If k is a field with a non-trivial, non-archimedean valuation v of rank 1 and K is a finite extension of k, with the non-equivalent valuations v_1, v_2, . . ., all of which are extensions of v, with respective ramifications e_1, e_2, . . . and residue class degrees f_1, f_2, . . . , then $\sum e_if_i \leq n = [K:k]$.

The proof of this theorem is a generalization of the proof of the previous theorem.

Using these two theorems, it can be shown that the extension of a rank 1 valuation to a finite overfield is a rank 1 valuation.

THEOREM 2.14 Let K be a finite extension of a field k; v', an extension of the valuation v of k where v is of rank 1. The group of values $v'(K')$ can be mapped order-isomorphically into a subgroup S of the additive group of reals so as to leave $v(k')$ fixed, where K' and k' are the multiplicative groups of K and k respectively.

Proof: Let $v'(K') = G$. Then $v(k') \subset G$ and $v(k') \subset S$. G is commutative and $(G: v(k')) = e$ is finite.

Let $eG = \{eg \mid g \in G\}$. Then $eG \subset v(k') \subset S$. Define a mapping $f: G \rightarrow S$ such that $f(a) = e^{-1}(ev'(a))$. f is a valuation. For $a \in k$, $f(a) = v(a)$. The valuations v' and f are equivalent since f is an isomorphism. Hence v' is a rank 1 valuation.

In the case where the field k is complete, let v be a rank 1 valuation of a field K, where K is a finite extension of k. k is complete with respect to v, and v is non-trivial on k. Under these conditions K is also complete.

THEOREM 2.15 A valuation v of rank 1 of a complete field k permits at most one extension onto a finite extension K of k.

Proof: See Appendix, 3.

Let the valuation v in the preceding theorem be non-archimedean. In this case there is always one and only one extension of the valuation.

In the case v is archimedean, the existence of an extension to an overfield has not been considered. In order to examine this, the following definition and results are necessary.

<u>DEFINITION 2.14</u> A field k containing R, the real numbers, is called normed if there exists a mapping a → $||a||$ of k into $R^+ \cup \{0\}$ such that

i) $||a|| = 0$ if and only if $a = 0$,

ii) $||ab|| \leq ||a|| \cdot ||b||$ for all a,b ε k,

iii) $||a + b|| \leq ||a|| + ||b||$ for all a,b ε k,

iv) $||ab|| = |a| \cdot ||b||$ for a ε R, b ε k.

<u>COROLLARY</u> a ε R implies $||a|| = ||a \cdot 1|| = |a| \cdot ||1||$; this implies the norm of elements of R, differ from their absolute value by some fixed real quantity. Hence the norm induces the same topology onto R as the absolute value.

<u>THEOREM 2.16 (Gelfand-Tornhein)</u> A normed field must either be equal to the field R of real numbers or be equal to the field C of complex numbers. (See Appendix 1 for proof).

Now let k be a field with archimedean valuation. Then k has characteristic zero. Thus k contains the field Q of rational numbers.

It has been shown that up to equivalence the absolute value is the only archimedean valuation of Q.

Let k' be the completion of k. The equivalence classes of k representably by Cauchy sequences of elements of Q form a subfield of k' isomorphic to R, the reals. The valuation of k' restricted to R, or Q', is the usual absolute value. Thus from the Gelfand-Tornhein theorem, k' must be either R or the field of complex numbers. The uniqueness theorem guarantees that the valuation is the usual absolute value. These results can be summarized into the following theorem.

THEOREM 2.17 A field with archimedean valuation is always isomorphic to a subfield of the field C of complex numbers, the valuation being the usual absolute valuation.

Let the field k have a non-archimedean valuation with group of values G.

DEFINITION 2.15 The valuation v of k is called discrete if and only if the group of values G is cyclic.

Since G is cyclic, one can assume that G is the group Z of integers.

Also from the definition, there exists $r \varepsilon k$ such that $v(r) = 1$. For this $r \varepsilon k$, $v(r)$ generates the group G. For each $a \varepsilon k$, $v(a) = n$ for some n. Hence $v(a/r^n) = 0$ which implies that a/r^n is a unit of the valuation ring. Thus for any element a in the valuation ring, there exists a unit c such that $a = r^n \cdot c$ $(n = 0,1,2,\ldots)$.

THEOREM 2.18 If K is a finite extension of k, then an extension of a discrete valuation of k onto K is a discrete valuation of K.

Proof: Suppose K is a finite extension of k. Then $(G'':G)$ is finite where G' and G are the groups of values of K and k respectively. Hence $G \subset G'$ and for some integer n, $nG' \subset G \subset Z$. The group nG' is an additive subgroup of Z which does not consist only of zero. Since any such subgroup is a principal ideal in Z, nG' is cyclic. Hence G' is cyclic.

G' may not be equal to Z. G' is at least an additive subgroup of Z. The value of an element $a \in k$ is therefore not uniquely determined. It depends on the field which is being considered. If $v(a)$ is the value of a in G, and $v'(a)$ is the value of a in G', then $v'(a) = n\,v(a)$ for any $a \in K$. Since G' is cyclic, there exists $s \in K$ such that $v'(s) = 1$. Thus $v'(r) = n$; and $r = cs^n$ where c is a unit of K, where $n = e = (G':G)$.

Example. Consider the rational numbers Q with a p-adic valuation where $p = 2$. Then in $Q(i)$ where $i^2 + 1 = 0$,

$$2 = (-i)(1 + i)^2.$$

Thus $(-i)$ is a unit. $(1 + i)$ is integral and prime. Since

$\sum_i e_i f_i \leq 2$, there exists only one extension of the valuation and that $e = 2$ and $f = 1$. Therefore if $Q(i) = K$,

$$v'(a) = 2v(a).$$

It has been shown that if the ramifiaation index e and the residue class degree f are finite, then $ef \leq n = [K:k]$. Now however, if k is complete by a discrete valuation, then $ef = n$.

THEOREM 2.19 Let k be a field complete by a discrete valuation. Let K be a finite extension of k, with ramification index e and residue class degree f. Then $ef = n = [K:k]$.

Proof: It suffices to show that $ef \geq n$. For every integer i, choose an element $r_i \in K$ such that

$$v(r_i) = v'(r_i) = i,$$

where v' is the valuation on K. Choose elements $w_1, w_2, \ldots, w_f$ from the valuation ring R' of K so that their images by the corresponding place are independent and form a basis of the residue class field of K over the residue class field of k. Any element of the residue class field of K is an image of a linear combination

$$A = a_1 w_1 + \ldots + a_f w_f$$

where $a_i \varepsilon$ R, the valuation ring of k; and conversely.

Let α be an element of K with $v(\alpha) \geq i$. α/r_i is integral since $v(\alpha/r_i) \geq 0$. Thus there exists a linear combination A whose image in the residue class field of K is the same as that of α/r_i, and $(\alpha/r_i)- A$ has image 0. Hence $v(\frac{\alpha}{r_i} - A) \geq 1$ which implies

$$v(\alpha - Ar_i) \geq i + 1.$$

Now let α be an integer in K and $v(\alpha) \geq 0$. By repeating the above process for each i, there exists a linear combination

$$A_0 \text{ with } \quad v(\alpha - A_0 r_0) \geq 1$$

$$A_1 \text{ with } \quad v(\alpha - A_0 r_0 - A_1 r_1) \geq 2$$

$$\vdots$$

$$A_i \ (i = 1,2,\ldots,n) \text{ with } \ v(\alpha - \sum A_i r_i) \geq n + 1.$$

Hence can be represented by a series $\sum A_i r_i$, where A_i's are combinations of the w_j's with coefficients in the valuation ring R. Hence

$$\alpha = \sum (a_{i1}w_1 + \ldots + a_{if}w_f)r_i \text{ with integral } a_{ij} \text{ in k.}$$

Choose r_i. Let $r_i = r^j s^t$, where $i = j + et$, $0 \leq j \leq e - 1$, $t \in Z$. Then

$$\alpha = \sum \sum (a_{i1}w_1 + \ldots + a_{if}w_f)\, s^t r^j$$

$$\alpha = \sum ((\sum a_{i1}s^t)w_1 + \ldots + (\sum a_{if}s^t)w_f)\, r^j .$$

Since k is complete the series $\sum a_{im}s^t$ converges to elements b_{jm} of k, which lie in the valuation ring R. Thus

$$\alpha = \sum (b_{j1}w_1 + b_{j2}w_2 + \ldots + b_{jf}w_f)\, r^j.$$

Therefore every integral element $\alpha \in$ K is a linear combination of the ef elements $w_i r^j$ with integral coeffieients in k.

In k, choose an element $a \neq 0$ with $v(a) > 0$. For any $\alpha \in K$ with $v(\alpha) < 0$, there exists an integer r such that $v(a^r) \geq 0$. Thus αa^r, and thus α is a linear combination of $w_i r^j$ with coefficients in k (which are no longer integral).

Consequently $n = [K:k] \geq ef$. Hence $n = ef$.

CHAPTER III

VALUATION THEORETIC APPROACH TO IDEAL THEORY

Let k be the quotient field of a ring R with identity. Let R be contained in the valuation ring of a discrete valuation of k. A valuation v is defined on the set of ideals of R by

$$v(A) = \min_{a \varepsilon A} \{v(a)\} \quad \text{for every ideal } A.$$

Such a minimum always exists since there exists $b \varepsilon k$, $b \neq 0$, such that bA is contained in R. Thus $v(ba) \geq 0$ and $v(a) \geq -v(b)$ for all $a \varepsilon A$. Since v is discrete, the values are integers. Hence a minimum exists.

THEOREM 3.1 For any ideal A and B in R

i) $v(A + B) = \min \{v(A), v(B)\}$;

ii) $v(AB) = v(A) + v(B)$;

iii) for any principal ideal (a),

$v((a)) = v(a).$

Proof: i) $$v(A + B) = \min_{\substack{a \varepsilon A \\ b \varepsilon B}} \{v(a + b), v(a), v(b)\}$$

$$= \min \{v(a), v(b)\}$$

$$= \min \{v(A), v(B)\}$$

ii) $$v(AB) = \min_{\substack{a \varepsilon A \\ b \varepsilon B}} \{v(ab)\} = \min \{v(a) + v(b)\}$$

$$= \min \{v(a)\} + \min\{v(b)\}$$

$$= v(A) + v(B).$$

iii) For every $x \varepsilon R$, $v(x) \geq 0$ and if $x = 1$, $v(x) = 0$.

Thus $v((a)) = \min \{v(ax)\} = \min\{v(a) + v(x)\} = v(a)$.

In order to fully characterize ideals by their value with respect to valuations, two axioms are required.

AXIOM 1 The field k has a set M of inequivalent discrete valuations such that for every $a \varepsilon k$ $v(a) \geq 0$ for all but a finite number of $v \varepsilon M$.

There are two immediate consequences of this axiom. First $v(a) = 0$ for almost all $v \varepsilon M$. Since $a \varepsilon k$, then $a^{-1} \varepsilon k$ and $v(a^{-1}) \geq 0$ for all but a finite number of $v \varepsilon M$. Hence $v(a) = 0$ for all but a finite number of $v \varepsilon M$.

Let R be contained in all the valuation rings corresponding to the $v \varepsilon M$ and let A be an ideal contained in R. Then $v(A) = 0$ for almost all $v \varepsilon M$ because of the following:

There exists an element $b \neq 0$ in k such that bA is contained in R, and hence $v(A) \geq -v(b)$ for all $v \varepsilon M$. Applying the axiom to b yields $v(A) \geq 0$ for almost all $v \varepsilon M$. But the value of A is less than the value of any nonzero element. Hence applying the axiom to some element of A yields $v(A) \leq 0$ for almost all $v \varepsilon M$. Thus $v(A) = 0$ for almost all $v \varepsilon M$.

DEFINITION 3.1 A divisor D of k is the product of the valuations $v \varepsilon M$; i.e., $D = \prod_{v \varepsilon M} v^{e_v}$ where e_v is an integer and equals zero for almost all $v \varepsilon M$.

The divisor is the product of all valuations $v \varepsilon M$. The divisor will be denoted by $\prod v^{e_v}$, and the index will not be written.

DEFINITION 3.2 The order of a divisor $D = \Pi v^{e_v}$ at a valuation $v \in M$ is $v(D) = e_v$.

DEFINITION 3.3 A divisor D is called integral if and only if

$v(D) \geq 0$ for all $v \in M$.

For two divisors $D = \Pi v^{e_v}$ and $D' = \Pi v^{f_v}$, their product is given by

$$DD' = \Pi v^{s_v} \quad \text{where } s_v = e_v + f_v;$$

and their sum is given by

$$D + D' = \Pi v^{m_v} \quad \text{where } m_v = \min\{e_v, f_v\} .$$

D is said to divide D' (denoted $D|D'$) if and only if $e_v \leq f_v$ for all $v \in M$.

Under multiplication, the set of divisors forms a group. The group axioms follow since the integers form a group under addition.

The set of ideals A of R can be mapped into the group of divisors by the mapping $A \rightarrow \Pi v^{e_v}$ where $e_v = v(A)$. Non-zero elements a of k can be mapped into the group of divisors by $a \rightarrow \Pi v^{e_v}$ where $e_v = v(a)$.

Since $v(A) = 0$ for almost all $v \in M$, Πv^{e_v} where $e_v = v(A)$ is a divisor. The principal ideal (a) is mapped onto the divisor Πv^{e_v} where $e_v = v((a))$ but $v((a)) = v(a)$. Thus the element a and the principal ideal (a) are mapped onto the same divisor.

For any two ideals A and B, $A \rightarrow \Pi v^{e_v}$ where $e_v = v(A)$ and $B \rightarrow \Pi v^{f_v}$ where $f_v = v(B)$.

$$(A + B) \rightarrow v^{h_v} \quad \text{where } h_v = v(A + B).$$

But $v(A + B) = \min\{v(A), V(B)\} = \min\{e_v, f_v\}$. Thus

$$(A + B) \rightarrow \Pi v^{\min\{e_v, f_v\}} = \Pi v^{e_v} + \Pi v^{f_v}.$$

Also $(AB) \rightarrow \Pi v^{h_v}$ where $h_v = v(AB)$. But $h_v = v(A\ ) + v(B)$.

Thus

$$(AB) \rightarrow \Pi v^{e_v + f_v} = (\Pi v^{e_v})(\Pi v^{f_v}).$$

Hence sums and products of ideals are mapped onto sums and products of divisors, respectively.

The mapping of ideals into divisors is a homomorphism of the multiplicative semigroup of ideals into the multiplicative group of divisors and the additive semigroup of ideals into the additive semigroup of divisors. In order that the homomorphism be an isomorphism, another axiom is needed.

AXIOM 2 Given a finite number of valuations $v_1, \ldots, v_r \in M$, a real number $\varepsilon > 0$, and any r elements $a_1, \ldots, a_r \in k$. There exists a $c \in k$ such that $v_i(c - a_i) \geq \varepsilon$ and $v(c) \geq 0$ for all other $v \in M$.

These axioms suffice to found ideal theory in valuation theory. To show that ideal theory does obey the axioms, diophantine equations will be used.

Let R be the intersection of the valuation rings R_ϕ for the places ϕ corresponding the the $v \in M$. Consider the problem of the solvability of diophantine equations locally at a place ϕ in R_ϕ and globally in R.

DEFINITION 3.4 Given a system of linear forms

$$\begin{aligned} y_1 &= a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n + b_1 \\ &\vdots \\ y_m &= a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n + b_m \end{aligned}$$

where $a_{ij} \varepsilon k$ and $b_i \varepsilon k$ for $i = 1,2,\ldots,m$ and $j = 1,2,\ldots,n$. A <u>local</u> <u>solution</u> is x_j ($j = 1,2,\ldots,n$) in some R_ϕ so that $y_i \varepsilon R_\phi$ for all i. The global solution consists of elements x_j in R such that $y_i \varepsilon R$ for all i.

<u>THEOREM 3.2</u> (Fundamental Theorem) The global solution exists if and only if, the local problem is solvable at every place corresponding to the $v \varepsilon M$.

Proof: Suppose the global problem is solvable. Then by the definition of R, the global solution is a local solution at every place.

Suppose the local problem is solvable for every place $v \varepsilon M$. Two cases may occur.

I If v is a valuation such that $v(a_{ij}) \geq 0$ and $v(b_i) \geq 1$ for all i and j, then all n-tuples $(x_1, x_2, \ldots, x_n)$ for which $v(x_j) \geq 0$ for all j are local solutions at v.

II. If $x_1, x_2, \ldots, x_n$ is a local solution for the place v, then every x_i' sufficiently close to x_i is also a local solution for that place.

Suppose there is a local solution $x_1, x_2, \ldots, x_n$ for every v. By Axiom 1, for almost all v, $v(a_{ij}) \geq 0$, $v(b_i) \geq 0$. Case I holds for almost all v. By axiom 2, there exists an $x_1' \varepsilon k$ such that

$$v_i(x_1' - x_1) \geq \varepsilon \qquad \text{for } i = 1,2,\ldots,r \text{ and}$$

$v(x_1') \geq 0$ for all other $v \varepsilon M$, where ε is chosen so as to make Case II applicable. Similarly there exist elements $x_2',\ldots,x_n' \varepsilon k$.

These elements $x_1', x_2', \ldots, x_n'$ are a local solution for all v. Hence they are a global solution.

DEFINITION 3.5 A first degree diophantine equation is a system

$$a_1x_1 + a_{12}x_2 + . . . + a_{1n}x_n = b_1$$

$$\vdots$$

$$a_mx_1 + a_{m2}x_2 + . . . + a_{mn}x_m = b_m$$

with a_{ij} , b_i ε k for i = 1, 2,...,m and j = 1,2,...,n and where x_j ε R for all j is a global solution and x_j in some R_ϕ is a local solution.

Applying the Fundamental Theorem to this system yields the following theorem.

THEOREM 3.3 The global solvability of a first degree diophantine equation is equivalent to local solvalitity at every v ε M.

THEOREM 3.4 Let a first degree diophantime equation consist of only one equation $a_1x_1 + a_2x_2 + . . . + a_nx_n = b$. Then a necessary and sufficient condition for the solution of the diophantine equation is $v(b) \geq \min\{ v(a_i)\}$.

Proof: Let $a_1x_1 + a_2x_2 + . . . + a_nx_n = b$ be a first degree diophantine dequation. Suppose the equation has a local solution at the place v. One may assume that at least one coefficient, say a_n, is not zero. Then

$$x_n = - \frac{a_1}{a_n}x_1 - \frac{a_2}{a_n}x_2 - . . . . - \frac{a_{n-1}}{a_n}x_{n-1} - \frac{b}{a_n} .$$

Consider the linear form $y = a_1x_1 + a_2x_2 + . . . + b$ where $x_1, x_2,. . . , y$ are integral at the place v.

Then $b = y - a_1x_1 - \cdot \cdot \cdot \cdot - a_nx_n$. Hence

$$v(b) \geq \min \{0, v(a_1), \ldots v(a_{n-1}) \} .$$

Suppose $v(b) \geq \min \{ 0, v(a_1), v(a_2), \ldots, v(a_{n-1})\}$.

Case I. Let the minimum be zero. Then $v(a_i) \geq 0$ for all i and $v(b) \geq 0$. Then every set $x_1, x_2, \ldots, x_n$ with $v(x_i) \geq 0$ is a local solution.

Case II. Let $v(a_1)$ be the minimum. Then $v(b) \geq v(a_1)$ and $v(b/a_1) \geq 0$. Let $x_1 = -b/a_1$, and let all other x_i's be zero. Then $y = 0$ and $x_1, x_2, \ldots, x_{n-1}$ is a local solution.

Consider the diophantine equation $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$, with $a_i \varepsilon k$, $b \varepsilon k$. Then using the inequality

$$v(b/a_n) \geq \min \{0, v(a_1/a_n), \ldots, v(a_{n-1}/a_n)\} ,$$

the theorem follows.

This condition coincides with the usual condition for solvability of diophantine equations in the ring of rational integers. Let $\beta = \Pi v^{v(b)}$ and $\alpha_i = \Pi v^{v(a_i)}$ be the divisors onto which the elements b and a_i are mapped. The condition becomes

$$\beta \text{ divisible by } \alpha_1 + \alpha_2 + \ldots + \alpha_n .$$

The definition of sums of divisors can be interpreted as the greatestt common divisor of $\alpha_1, \alpha_2, \ldots, \alpha_n$. Identifying the divisors with the corresponding principal ideals or the elements themselves, one obtains the usual condition for the solvability of diophantine equations.

To show that ideals do satisfy the axioms, it must been shown first that the field k is the quotient field of R.

Let $a \in k$ and $a \neq 0$. There exists $x \in k$ such that for some $\varepsilon > 0$,

$$v(x - \frac{1}{a}) > \varepsilon \qquad \text{if } v(a) < 0$$

$$v(x) \geq 0 \qquad \text{otherwise.}$$

Since $v(a) < 0$ implies $v(1/a) > 0$, for some $\varepsilon > 0$ $v(a) < 0$ implies $v(x) > 0$ and $x \neq 0$. Thus $x \in R$ and

$$v(ax - 1) > \varepsilon + v(a) \quad \text{if } v(a) < 0$$

$$v(ax) \geq 0 \quad \text{if } v(a) \geq 0.$$

Hence for some $\varepsilon > 0$, $ax \in R$. Thus $a = ax/x$ where x, $ax \in R$. Therefore every element of k can be expressed as the quotient of elements of R.

THEOREM 3.5 The mapping of the ideals of R into the group of divisors is one-to-one. That is, an ideal A of R can be characterized by its order v(A) for all $v \in M$.

Proof: Let A be an ideal of R and let the value of A be $V(A) = e_v$. Suppose a is any non-zero element in A. Then $v(a) \geq e_v$ for all $v \in M$. Let $v_1, v_2, \ldots, v_r$ be a subset of M such that for all other $v \in M$, $v(a) = e_v$. Such a finite set exists because both v(A) and v(a) are zero for almost all $v \in M$. For each $i = 1,2,\ldots,r$, choose $a_i \in R$ such that $v_i(a_i) = e_i$ where $e_i = e_{vi}$. Consider the diophantine equation

$$ax + a_1x_1 + \ldots + a_rx_r = b$$

where $b \in k$. By the choice of a and a_i, and by the condition of solvability of such equations, the equation is solvable if and only if

$$v(b) \geq e_v \quad \text{for all } v.$$

Every b satisfying this inequality can be expressed

$$b = ax + a_1x_1 + \ldots + a_rx_r$$

where x, $x_i \varepsilon R$. Since a and a_i are in A for all i, $b \varepsilon A$.

Thus A consists of all $b \varepsilon k$ such that $v(b) \geq e_v$ for all $v \varepsilon M$, and is therefore uniquely determined by the values e_v. Hence the mapping $A \rightarrow \Pi v^{e_v}$ where $e_v = v(A)$ is one-to-one. A is uniquely determined by its divisor.

THEOREM 3.6 The mapping of the ideals into the group of divisors is onto. That is, to any set of values for the orders of the valuations, there corresponds an ideal.

Proof: Suppose that for every v, a value e_v exists such that $e_v = 0$ for almost all $v \varepsilon M$. First it will be shown that to any given rational integers $e_1, e_2, \ldots, e_r$, there corresponds an element $a \varepsilon k$ such that

$$v_i(a) = e_i \qquad (i = 1,2,\ldots,r)$$

$$v(a) \geq 0 \qquad \text{for all other } v \varepsilon M.$$

For each i, choose $a_i \varepsilon k$ such that $v_i(a_i) = e_i$. Choose $a \varepsilon K$ such that

i) $v_i(a - a_i) \geq v_i(a_i) \quad (i = 1,2,\ldots,r)$

ii) $v(a) \geq 0$ for all other $v \varepsilon M$.

Since $v_i(a) = v_i(a_i + (a - a_i)) = v_i(a_i)$, a is the required element of k.

Choose $v_1, v_2, \ldots, v_r$ so that $e_v = 0$ for all other $v \varepsilon M$.

By axiom 2, there exists $a \in k$, $a \neq 0$, such that $v_i(a) \geq e_i$ for $i = 1,2,\ldots,r$ and $v(a) \geq 0$ otherwise. Thus $v(a) \geq e_v$ for all v. Choose $u_1, u_2, \ldots, u_s \in M$ such that $v(a) = 0$ for all v except u_j , v_i for all i and j. Then there exists $b \in k$ such that $v(b) = e_v$ where $v = v_i$, u_j for all i, j; and $v(b) \geq 0$, otherwise.

For the sum of divisors α and β , $v(\alpha + \beta) = \min\{ v(\alpha), v(\beta)\}$ for all v. But $\alpha + \beta$ is the image of the ideal $A = (a) + (b)$, which therefore has the given values. Thus the mapping is onto.

This last proof also illustrates that any ideal can be generated by two elements where one may be freely chosen.

One can now consider divisors instead of ideals. Since the divisors form a multiplicative group, the ideals form a group.

Integral ideals A, those contained in R, are the ideals for which $v(A) \geq 0$ for all v. Thus integral ideals correspond to integral divisors.

Prime ideals remain to be characterized. For two ideals A and B, B divides A $(B|A)$ if and only if B contains A. Then the values v(A) are contained in the valuation ring corresponding to the valuation of B. Thus $v(B) \leq v(A)$ for all $v \in M$. Consequently the divisor of B divides the divisor of A.

Let A,B,C be ideals with $B \neq R$, $C \neq R$, and $A = BC$. Thus $B|A$ and $C|A$. Then $A \subset B$ and $A \subset C$. Hence there exists $b \in B$ and $c \in C$ such that $b,c \neq A$ but $bc \in BC = A$. Hence A is not prime.

The only possible prime ideals other than (0) and R are those whose divisors have only one factor v. These are prime ideals.

Let β be a prime ideal and β' be its divisor. β is the set of all $a \in k$ with $v(a) \geq 1$ and $u(a) \geq 0$ for $u \neq v$. If $a,b \in \beta$, $a,b \in R$, then $v(ab) \geq 1$ and $u(ab) \geq 0$ for $u \neq v$. Either $v(a) \geq 1$ and $u(a) \geq 0$, or $v(b) \geq 1$ and $u(b) \geq 0$. Hence either $a \in \beta$ or $b \in \beta$.

Except for the zero ideal and R, the ideals corresponding to the valuations v are the only prime ideals of R. The isomorphism of ideals and divisors shows that every ideal is uniquely decomposable into the product of prime ideals.

The most important result of the axioms was that the ideals of R form a group. This property is sufficient to imply the validity of the axioms.

Let R be a ring with identity, with quotient field k, and whose ideals form a group.

THEOREM 3.7 In any integral domain D with quotient field k, any ideal A of D for which there exists an ideal B such that $AB = R$ is finitely generated.

Proof: Since $1 \in R$, there must exist a representation $1 = \sum a_i b_i$ where $a_i \in A$ and $b_i \in B$. The elements $a_1, a_2, \ldots, a_r$ generate A. If not, then there exists an ideal A' such that

$$A' = (a_1) + (a_2) + \ . \ . \ . + (a_r) \subset A.$$

Then $A'B \subset AB = R$. But $1 \in A'B$. Hence $A'B = R = AB$. Consequently $A' = A$ and A is finitely generated.

Since the ideals form a group, every ideal of R is finitely generated. But this is equivalent to the maximal property for ideals: Every set of ideals contains maximal ideals.

For every maximal proper ideal, define a valuation of k as follows:

Let $a \neq 0$ be an element of k. Let $(a) = \Pi\, p^{e_p}$ where p is a prime ideal. Define $v(a) = e_p$ and $v(0) = \infty$. Then the first property of the definition of valuations is satisfied. The second, property follows from the fact that $(ab) = (a)(b)$ implies $v(ab) = e_p + f_p$ where $(a) = \Pi p^{e_p}$, $(b) = \Pi\, p^{f_p}$ for $a,b \neq 0$. The third property, that $v(a + b) \geq \min\{ v(a), v(b)\}$, follows from $v(a + b) = v(\Pi\, p^{e_p} + \Pi p^{f_p}) = e_p$ if $e_p < f_p$. This valuation is discrete since the values are the integers (and ∞).

Different prime ideals, p and p', yield different valuations. The prime ideals are maximal. Hence for prime ideals A and B, $A + B = R$. Thus there exist $a \in A$ and $b \in B$ such that $a + b = 1$. Since $1 \notin A$ and $b \notin A$, $v_A(b) \leq 0$ and $v_B(b) > 0$. Thus these valuations differ.

THEOREM 3.8 The set of valuations with the above properties satisfies Axiom 1 and Axiom 2.

Proof: I. The first axiom is easily satisfied since the factorization of any ideal contains only a finite number of prime ideals p with nonzero exponents. Thus $v_p(a) = 0$ for almost all p.

II. An element $a \in k$ belongs to R if and only if $(a) \subset R$, i.e. $v_p(a) \geq 0$ for all p. Let R_p be the valuation ring of the valuation corresponding to p, then $R = \bigcap R_p$.

If $p_1, p_2, \ldots, p_s$ are any finite number of distinct prime ideals, then for any $n \geq 1$, $p_1^n + p_2^n p_3^n \cdots p_s^n = R$. The left member of the equation is the greatest common divisor of two prime ideals and must be R. Thus there exists $\alpha \in R$, $x \in R$ such that $\alpha + x = 1$, $p \mid (a)$ and $p \mid (x)$ for $i = 2,3,\ldots,s$. For some n

$$\text{i)} \quad v_{p_1}(x - 1) \text{ is large}$$

$$\text{ii)} \quad v_{p_i}(x) \text{ is large}$$

$$\text{iii)} \quad v\ (x) \geq 0 \text{ for all other } p.$$

Thus for $a \in k$ and r distinct prime ideals $p_1, p_2, \ldots, p_r$, there exists $x \in k$ such that $v_{p_1}(x - 1) \geq \varepsilon'$

$$v_{p_i}(x) \geq \varepsilon'$$

$$v_p(x) \geq \varepsilon' \qquad p \neq p, \text{ but } v_p(a) < 0$$

$$v_p(x) \geq 0 \qquad \text{otherwise.}$$

Let $y = ax$. Then

$$v_{p_1}(y - a) \geq \varepsilon' + v_{p_1}(a)$$

$$v_{p_i}(y) \geq \varepsilon' + v_{p_i}(a) \qquad i = 2,3,\ldots,r$$

$$v_p(y) \geq \varepsilon' + v_p(a) \qquad p \neq p_i,\ v_p(a) < 0$$

$$v_p(y) \geq v_p(a) \geq 0 \qquad \text{otherwise.}$$

Given $\varepsilon > 0$; r distinct prime ideals of R, $p_1, p_2, \ldots, p_r$; and r elements of k, $a_1, a_2, \ldots, a_r$. There exist $y_1, y_2, \ldots, y_r$ in k such that

$$v_{p_i}(y_i - a_i) \geq \varepsilon$$

$$v_{p_j}(y_i) \geq \varepsilon \qquad i \neq j$$

$$v_p\,(y_i) \geq \theta \qquad \text{otherwise}$$

for every $i = 1,2,..,r$. Let $z = y_1 + y_2 + \ .\ .\ . + y_r$. Then

$$v_{p_i}(z - a_i) \geq \varepsilon \quad (i = 1,2,...,r)$$

$$v_p\,(z) \geq 0 \qquad \text{otherwise.}$$

The element z satisfies the condition of Axiom 2. Therefore the set M of all valuations v_p satisfies Axiom 2.

Axioms 1 and 2 are equivalent to the statement that the ideals of a ring form a group.

<u>THEOREM 3.9</u> If the axioms are satisfied in a field k, and K is a finite field extension of k, then the axioms are satisfied in K.

Proof: Let R be the valuation ring corresponding to the valuations $p \varepsilon M$ of k, and let R be the intersection of these valuation rings. The ideals of R form a group.

Let the set M' of valuations of K be the set of all possible extensions P of valuations $p \varepsilon M$ of k. The valuations of M' are discrete. If P is an extension of p, the notation $P|p$ will be used to indicate that P divides p.

(1) p has only a finite number of divisors.

Let $\alpha \varepsilon K$ such that $\alpha^n + a_1\alpha^{n-1} + \ .\ .\ . + a_n = 0$ where $a_i \varepsilon k$. Since the axioms hold in k, $v_p(a_i) \geq 0$ for at most a finite number of $p \varepsilon M$. Since (1), $\mathrm{Min}_i\{\, v_p(a_i)\} \geq 0$ for almost all $P \varepsilon M'$. Thus $v_p(\alpha) \geq 0$ for almost all $P \varepsilon M'$. Therefore axiom 1 holds.

Let P_1, P_2, . . ., P_r be distinct valuations of M'. Let $w_1, w_2, . . ., w_n$ be a basis of K over k. Let $\alpha_1, \alpha_2, . . ., \alpha_r$ be elements of K, and let $\varepsilon > 0$ be a real number.

Choose valuations $P_{r+1}, . . ., P_s$ of M' such that $v_P(w_i) \geq 0$ for all i and for $P \neq P_1, . . ., P_r, P_{r+1}, . . ., P_s$. Let $p_1, ..., p_m$ be valuations of k such that each P_i is an extension of one of the p_j. Let $P_1, . . ., P_i$ be all possible extensions of the valuations p_j. The valuations $P_1, . . ., P_s$ are in this set. Let $\alpha_{r+1} = ... = \alpha_i = 0$ and assume $\varepsilon > 1$.

By the approximation theorem for rank 1 valuations, there exists K such that $v_{P_i}(\beta - \alpha_i) \geq \varepsilon \quad (i = 1,2,...,r)$.

Let $\beta = x_1 w_1 + . . . + x_n w_n$ with $x_i \in k$. Let

$b = y_1 w_1 + . . . + y_n w_n$ where y_i is chosen in k by axiom 2.

Then

$$v_p\,(y_j - x_j) \geq \varepsilon' \quad \text{for } i = 1,2,...,m; \quad \text{for some } \varepsilon'$$

$$v_p\,(yj) \geq 0 \quad \text{otherwise.}$$

Then for some '

$$v_P\,(b - \beta) \geq \varepsilon' + \min\{\, v_P\,(w_j)\} \geq \varepsilon \;(i = 1,2,...,r) \;.$$

Hence, for i = 1, 2,...,r

$$v_P\,(b - \alpha_i) = v\;\;((b - \beta) + (\beta - \alpha_i)) \geq \;\varepsilon$$

and $\qquad v_P\,(b) \geq 0 \qquad$ otherwise.

The element b satisfies the axiom.

Therefore axiom 2 holds in M'.

This development of ideal theory holds in the field of rational numbers using the ring of integers. It therefore holds in every algebraic number field, with the ring of algebraic integers. The set M of valuations consists of all possible valuations except the archimedean valuation.

APPENDIX

The following is a list of theorems and results that appear without proof. Given is the location of the proof, if the reader desires such proof. Since all books are listed in the bibliography only the name of the author and volume and page are given.

1. Artin, page 45.
2. Jacobson, Vol. III, page 217
3. Artin, page 65.

SELECTED BIBLIOGRAPHY

Artin, Emil. 1959. Theory of Algebraic Numbers, Gottingen, Germany, George Striker, distributor.

Jacobson, Nathan. 1961. Lectures in Abstract Algebra, Vol. I, Princeton, New Jersey, D.van Nostrand.

________ 1964. Lectures in Abstract Algebra, Vol. III, Princeton, New Jersey, D.van Nostrand.

van der Waerden, B.L. 1953. Modern Algebra, Vol. I, New York, Frederick Ungar Publishing Co.

________ 1950. Modern Algebra, Vol. II, New York, Frederick Ungar Publishing Co.

Zariski, O. and Samuel, Pierre. 1958. Commutative Algebra, Vol. I, Princeton, New Jersey, D.van Nostrand.

________ 1960. Commutative Algebra, Vol. II. Princeton, New Jersey, D.van Nostrand.