1956

Dedikind rings and valuations

Benjamin Myron Kramer
The University of Montana

DEDIKIND RINGS AND VALUATIONS

by

BENJAMIN M. KRAMER

B. A. Montana State University, 1954

Presented in partial fulfillment of the requirements

for the degree of

Master of Arts

MONTANA STATE UNIVERSITY

1956

Approved by:

Chairman, Board of Examiners

Dean, Graduate School

Date

DEDIKIND RINGS AND VALUATIONS

by

BENJAMIN M. KRAMER

B. A. Montana State University, 1954

Presented in partial fulfillment of the requirements

for the degree of

Master of Arts

MONTANA STATE UNIVERSITY

1956

Approved by:

Chairman, Board of Examiners

Dean, Graduate School

Aug 14 1956

Date

TABLE OF CONTENTS

CHAPTER PAGE

ACKNOWLEDGMENT ii

INTRODUCTION 1

I. VALUATIONS AND CLASSICAL IDEAL THEORY 2

II. OTHER AXIOMS FOR A DEDIKIND RING 11

III. PRINCIPALLY ORDERED SYSTEMS 29

IV. ALGEBRAIC EXTENSIONS 41

V. EXAMPLES 56

APPENDIX

I. BASIC SET CONCEPTS 63

II. BASIC IDEAS OF ALGEBRA 70

III. ALGEBRAIC EXTENSIONS 80

IV. COMPLETE FIELDS 89

BIBLIOGRAPHY 95

ACKNOWLEDGMENT

The author wishes to express his indebtedness and gratitude to Professor Donald G. Higman for suggesting the general pattern of this publication and also for instructing the author in certain areas of mathematics.

INTRODUCTION

This short survey consists of known results about the type of algebraic system known as a Dedikind ring. In this survey, the definition of a Dedikind ring is given first in terms of valuations, and the valuation approach is, for the most part, emphasized. Various different assumptions under which either the properties of valuations needed for Dedikind rings arise or under which only some of these properties arise are investigated. Two chapters discuss conditions equivalent with the valuation definition of a Dedikind ring. Another chapter relates the assumptions made in classical research papers on ideal theory (e.g., Van der Waerden's work) to the properties of valuation. The final results concern algebraic extensions viewed with regard to valuations.

CHAPTER I

VALUATIONS AND CLASSICAL IDEAL THEORY

Note in regard to references: In the first four chapters (I, II, III, and IV), the main statements proved are given Arabic numerals while useful preliminary results are assigned letters. Reference to a statement is made by enclosing in parentheses the appropriate symbols, e.g., "by (II.1c)" means "by the result (c) preceding the proof of statement (1) in Chapter II." The chapter and/or statement number is dropped in case of a reference pertaining to the same chapter and/or statement in which the reference occurs.

Results and definitions considered to be of an elementary or of a set theoretic nature appear in appendices. Reference to such material is made by using the abbreviation "app." followed by the appendix number (I, II, III, or IV) and the section number (1, 2, . . .), e.g., "by app. (II.3)." Occasionally the abbreviation "para." for "paragraph" is used. Also, terms and notations not defined in the course of the text are listed at the end of the first chapter in which they appear. Beside each listing is an appropriate reference to an appendix.

Publications referred to are indicated in the text by a bracketed number, followed by the chapter and section number. The bracketed number corresponds to the listing in the bibliography following the appendices.

Definition (*valuation*): Let $\bar{O}$ be an integral domain with identity. A discrete valuation of $\bar{O}$ is a mapping of the multiplicative semigroup $\bar{O}^*$ of $\bar{O}$ onto a set of non-negative rational integers such that:

(a) $v(ab) = v(a) + v(b)$

(b) $v(a+b) \geqq \min \{v(a), v(b)\}$

It is convenient to define $v(0) = \infty$ with the conventions $\infty > n$, $n + \infty = \infty + \infty = \infty + n = \infty$ where n is any rational integer.

Definition (Dedikind Ring): An integral domain with an identity element $\bar{o}$ is a Dedikind ring if there is defined on $\bar{o}$ a non-null set $\mathfrak{V}$ of discrete valuations which satisfy the following postulates:

(I) If the elements a,b of $\bar{o}$ are such that $v(a) \quad v(b)$ for all $v \in \mathfrak{V}$, then there exists c such that $a = bc$.

(II) For a $\bar{o}^*$, $v(a)$ is not equal to zero for at most finitely many $v \in \mathfrak{V}$.

(III) If $v_1, v_2 \in \mathfrak{V}$, $v_1 \neq v_2$, then there exists a $\bar{o}^*$ such that $v_1(a) = 0$, $v_2(a) > 0$.

(IV) The only ideal A of $\bar{o}$ with the property that $\min\{v(a)$, a in $A\} = 0$ for all v in $\mathfrak{V}$ is $\bar{o}$.

It will be shown in this chapter that the classical ideal theory holds in $\bar{o}$, that is, each proper ideal of $\bar{o}$ can be expressed in one and only one way as a product of powers of finitely many prime ideals; conversely, it will be shown on any integral domain in which the classical ideal theory holds, there can be defined a non-null set $\mathfrak{V}$ of valuations satisfying I through IV.

In the ensuing statements, (1) through (14) inclusive, it is assumed $\bar{o}$ is an integral domain and $\mathfrak{V}$ a set of discrete valuations satisfying postulates I, II, III, and IV.

(1) If $v \in \mathfrak{V}$, a and $b \in \bar{o}$, $v(a) \neq v(b)$, then $v(a + b) = \min\{v(a),$

$v(b)$.

Proof: it may be assumed $v(a) > v(b)$. Then if $v(a + b) > v(b)$, it follows $v(b) = v(a + b - a) \geq \min \{v(a + b), v(a)\} > \min \{v(a), v(b)\} = v(b)$.

(2) Let $v_1, v_2, v_3, \ldots\ldots v_n$ and v be distinct valuations in $\mathfrak{V}$. Then there exists:

(a) a in $\bar{O}$ such that $v(a) = 0$, $v_i(a) \quad 0$, $1 \leq i \leq n$;

(b) b in $\bar{O}$ such that $v(b) > 0$, $v_j(b) = 0$, $1 \leq i \leq n$.

Proof of (a): For each j, $1 \leq j \leq n$, there exists an element a_j such that $v(a_j) = 0$, $v_j(a_j) > 0$. Let $a = \prod_{i=1}^{m} a_j$. Then $v(a) = \sum_{i=1}^{m} v(a_j)$; $v(a_j) = 0$; $v_j(a) \geq v_j(a_j) > 0$.

Proof of (b): For each j, $1 \leq j \leq n$, there exists by (a) an element b_j such that $v(b_j) > 0$, $v_j(b_j) = 0$, and $v_k(b_j) > 0$, $k \neq j$, $1 \leq k \leq n$. Let $b = \sum_{j=1}^{m} b_j$. Then $v(b) \geq \min\limits_{1 \leq j \leq n} \{v(b_j)\} > 0$, and $v_k(b) = 0$ since $v_k(b_k) = 0$, $v_k(\sum_{\substack{j=1 \\ j \neq k}}^{m} b_j) > 0$.

(3) If $v, v_1, \ldots\ldots$ and v_n are distinct valuations in $\mathfrak{V}$, there exists in $\bar{O}$ an element p such that $v(p) = 1$, $v_j(p) = 0$ for $1 \leq j \leq n$.

Proof: There exists p in $\bar{O}$ such that $v(p') = 1$. By (2a) there exists for each k, $1 \leq k \leq n$, an element b_k such that $v_k(b_k) = 0$, $v(b_k) \quad 1$, $v_j(b_k) > 0$ when $j \neq k$, $1 \leq j \leq n$. Let $p = p' + \sum_{k=1}^{m} b_k$. p is the required element.

Definition (value of an ideal): If A is an ideal of $\bar{O}$ and if v is in $\mathfrak{V}$, define $v(A)$ as the $\min\limits_{a \text{ in } A} \{v(a)\}$. Note that since v is discrete, there actually exists in A such that $v(a) = v(A)$.

Definition (product of ideals): Let $A_1, A_2, \ldots\ldots A_n$ be ideals of $\bar{O}$. The product of the $[A_i]_{i=1}^{m}$, denoted by either $A_1A_2A_3\ldots A_n$ or by $\prod_{i=1}^{m} A_i$, is defined as the ideal

$\left\{ x \text{ in } \bar{O} \;\middle/\; \begin{array}{l}\text{for some positive integer } n \text{ there are elements} \\ a_{ij} \text{ in } A_i,\ 1 \leq i \leq n, \text{ such that } x = \sum_{j=1}^{m} a_{1_j} a_{2_j} a_{3_j} \ldots n_j \end{array} \right\}$

It is seen that $\prod_{i=1}^{m} A_i = \prod_{i=1}^{m} A_i \prod_{i=m+1}^{m} A_i$. Postulate IV states $v(A) = 0$ for all $v \varepsilon \mathfrak{V}$ only when the ideal A is $\bar{O}$ itself.

Let v be in $\mathfrak{V}$. Then

(4) $v(AB) = v(A) + v(B)$ for any pair of ideals, A and B of $\bar{O}$.

<u>Proof</u>: $v(AB) = \min\limits_{\substack{m<\infty \\ a_i \varepsilon A,\, b_i \varepsilon B}} v(\sum_{i=1}^{m} a_i b_1) \geq v(A) + v(B)$.

On the other hand, there is an element $\underline{a}$ in A and an element $\underline{b}$ in B such that $v(\underline{a}) = v(A)$ and $v(\underline{b}) = v(B)$. Since $\underline{ab}$ is in AB, $v(AB) \leq v(ab) = v(a) + v(b) = V(A) + v(B)$.

(5) For each ideal A, $v(A) = 0$ except for (at most) finitely many v in $\mathfrak{V}$.

<u>Proof</u>: Let $a \neq 0$ be an element of A. Then $v(a) \quad v(A) \quad 0$ for all v in $\mathfrak{V}$. Since $v(a) = 0$ for all but finitely many v in $\mathfrak{V}$, so also $v(A) = 0$ but for finitely many v in $\mathfrak{V}$.

(6) If $v_1, v_2, \ldots\ldots v_n$ are distinct valuations in $\mathfrak{V}$ and if A is an ideal, there exists $\underline{a}$ in A such that $v_i(a_1) = v_i(A)$, $1 \quad i \quad n$.

<u>Proof</u>: For each 1, $1 \leq i \leq n$, there exists a_i in A such that $v_i(A) = v_i(a_i)$. By (2a), there exists elements b_i such that $v_i(b_i) = 0$ and $v_j(b_i) > 0$ when $i \neq j$, $1 \leq i \leq n$. The element $a = \sum_{i=1}^{m} a_i b_i$ has the required property.

(7) If the set $\mathfrak{V}$ of valuations is finite, then $\bar{O}$ is a principle ideal ring.

<u>Proof</u>: Let A be an ideal. If $\mathfrak{V}$ is finite then by (6) there exists a in A such that $v(a) = v(A)$ for all v in $\mathfrak{V}$. If $\underline{b}$ is in A, then $v(b) \geq V(A) = v(a)$, for all v in $\mathfrak{V}$. By axiom I, $\underline{b}$ is a multiple of a;

A consists only of multiples of A.

(8) $v(A) \leq V(B)$ if and only if $B \subseteq A$.

<u>Proof</u>: Clearly if $B \subseteq A$, then $v(B) = \min_{b \in B} \{v(b)\} \geq \operatorname{Min}_{a \in A} \{v(a)\} = v(A)$.

To prove the converse, let $v_1, v_2, \ldots\ldots v_n$ be the set of all valuations v in $\mathfrak{D}$ such that $v(A) = 0$. This set is finite or null by (5). If $\mathfrak{D}$ consists of no other valuations, then $\bar{O}$ is a principle ideal ring by (7). Then $A = \bar{O}(a)$, $B = \bar{O}(b)$ for some elements a, b in A and B respectively. $V(A) = v(a)$, $v(B) = v(b)$ for all v in $\mathfrak{D}$. If $v(A) = V(B)$ for all v, then by axiom I <u>b</u> is a multiple of <u>a</u>. $B = \bar{O}b \subseteq A$ in this case.

Suppose now that there is a v_0 in $\mathfrak{D}$ distinct from either v_1, $v_2, \ldots\ldots$ or v_n. The set $C = \{ c \text{ in } \bar{O} / Bc \subseteq A \}$ is an ideal of $\bar{O}$. (Bc denotes the set of products of c by elements from B.) It will be shown for each v in $\mathfrak{D}$, there exists c in C such that $v(c) = 0$. Then by axiom IV, $C = \bar{O}$, and $B = B\bar{O} \subseteq A$ in this case.

By (6) there exists <u>a</u> in A such that $v_i(a) = v_i(A)$, $0 \leq i \leq n$. Let $v_0, v_1, \ldots\ldots v_n, v_{n+1}, \ldots\ldots v_{n+m}$ be a set of distinct valuations in $\mathfrak{D}$ containing all those which do not vanish on <u>a</u>. By (2b) there exists for each j, $1 \leq j \leq m$, an $\underline{a}_j$ such that $v_{mj}(a_j) > 0$ and $v_i(a_j) = 0$, $0 \leq i \leq n$. Let $c = \prod_{j=1}^{m} (a_j)^r$ with r so large that $v_k(c) \geq v_k(a)$, $n+1 \leq k \leq m$. Then $v_i(c) = 0$, $0 \leq i \leq n$, $W(c) \geq W(a)$ for all other w in $\mathfrak{D}$. Let <u>b</u> be any element of B. Then $v_i(b) \geq v_i(a)$, $0 \leq i \leq n$, and so $w(bc) = w(b) + w(c) \geq w(a)$ for all w in $\mathfrak{D}$.

Hence <u>bc</u> is a multiple of <u>a</u> by axiom I; therefore <u>bc</u> is is in <u>A</u> and <u>c</u> is in C. For $0 \leq i \leq n$, $0 \leq v_i(C) \leq v_i(c) = 0$ or $v_i(C) = 0$. Since V_0 can be any valuation in $\mathfrak{D}$ distinct from the $v_1, v_2, \ldots\ldots v_n$, the result follows.

Notation (*ideals* $\underline{P(v)}$): Let v be in $\mathbb{D}$. Denote by $\underline{P(v)}$ the totality of elements $\underline{a}$ on $\bar{O}$ such that $v(a)\ \ 0$. It is seen that $\underline{P(v)}$ is an ideal of $\mathbb{D}$.

(9) If v_1 and v_2 are distinct valuations in $\mathbb{D}$ then $\underline{P(V_1)} \not\subseteq \underline{P(v_2)}$.

Proof: By axiom II there is an $\underline{a}$ such that $v_1(a) > 0$ and $v_2(a) = 0$.

(10) If v_1 and v_2 are distinct valuations in $\mathbb{D}$, then $v_2(\underline{P(v_1)}) = 0$.

Proof: The statement follows at once from (9) and the definition of $v_1\ \underline{(Pv_2)}$.

(11) $\underline{Pv}$ is a maximal prime ideal of $\bar{O}$.

Proof: If $\underline{ab}$ is in $\underline{Pv}$, then $\mathbb{D}\ \ v(ab) = v(a) + v(b)$. Hence either $0 < v(a)$ or $0 < v(b)$: either $\underline{a}$ or $\underline{b}$ is in $\underline{Pv}$.

Suppose A is an ideal of $\bar{O}$ such that $Pv \subset A$. Then there is an element $\underline{a}$ in $\bar{O}$ for which $v(a) = 0$, and so $w(A) = 0$ for all w in $\mathbb{D}$. $A = \bar{O}$.

(12) Every prime ideal has the form $\underline{Pv}$ for some v in $\mathbb{D}$.

Proof: Let P be a prime ideal of $\bar{O}$. By axiom IV there is a v in $\mathbb{D}$ such that $vP > 0$. Then by (8) and (9), $P \leqq P(v)$. It is shown that $W(P) = w\ (P(v))$ for all w in $\mathbb{D}$, whence $P = P(v)$.

First it is shown $w(P) = 0$ for all w in $\mathbb{D}$ different from v; therefore, $w(P) = w(\underline{Pv})$ for $w \neq v$. There exists by (3) an element $\underline{p}$ such that $v(p) = 1$, $w(p) = 0$. There is an $\underline{a}$ in P such that $v(a) = v(P) = e > 0$. By (2a) there exists $\underline{b}$ in $\bar{O}$ such that $v(b) = 0$ and $v'(ab) \geq v'(p^e)$ for all v' in $\mathbb{D}$ different from v. By axiom I there is an element $\underline{c}$ in $\bar{O}$ such that $ab = op^e$; since $\underline{a}$ is in P, cp^e is in P and so either $\underline{c}$ or $\underline{p^e}$ is in P. But $v(c) = v(a) + v(b) - v(p^e) = 0$ and so $\underline{c}$ is not in P. Then $0 \leq W(P) \leq w(p^e) = e\big(w(p)\big) = 0$.

Finally it is shown that $v(P) = \underline{v(Pv)} = 1$. Suppose $e = V(P)$

$v(Pv) = 1$. The above argument shows that there are elements c and p in $\bar{O}$ such that $v(c) = 0$, $v(p) = 1$, and cp^e is in P. Then either cp or p^{e-1} must be in P, and in either case $v(P) < e$.

(13) The ideals of $\bar{O}$ form a semi-group under ideal multiplication; the mapping $\Psi: A \longrightarrow \{v(a)\}$, v in $\mathbb{D}$, is an isomorphism of this semi-group onto the restricted direct sum $\Gamma = \{\Gamma_v\}_{v \varepsilon \mathbb{D}}$ where Γ_v is the additive semi-group of non-negative integers. (Ideal multiplication is the operation "o" defined on pairs A,B of ideals in $\bar{O}$ such that $A^oB = AB$.)

Proof: By (4), (5) and (8), Ψ is an isomorphism into Γ. Now if $\{\Gamma_v\}_{v\varepsilon\mathbb{D}}$ is an element of Γ in which Γ_{v_1}, Γ_{v_2},...... Γ_{v_n} are the only non-zero Γ_v, then set $A = \prod_{i=1}^{m} P(V_i)^{\Gamma v_i}$. Then $v_i(A) = \Gamma_v k$, $1 \leq i \leq n$, and $v(A) = 0$ for all other v in $\mathbb{D}$ by (4) and (10). Hence $\Psi A = [\Gamma_v]_{v\varepsilon\mathbb{D}}$ and Ψ is an onto mapping.

Definition: Classical ideal theory (or prime power representation of ideals in $\bar{O}$). The classical ideal theory is said to hold in $\bar{O}$ if: for each proper ideal, A, of $\bar{O}$ there is a finite set of distinct prime ideals $[P_i]$, $1 \leq i \leq n$, and a positive integer, α_i, $1 \leq i \leq n$, corresponding to each prime, such that $A = \prod_{i=1}^{m} P_i^{\alpha_i}$; moreover, the set of prime ideals and the set of corresponding integers is uniquely determined by A.

(14) The classical ideal theory holds in $\bar{O}$.

Proof: If A is an ideal of $\bar{O}$ $(A \neq \bar{O})$, let $\Psi A = [\Gamma v]_{v\varepsilon\mathbb{D}}$ where Γv_1, Γv_2,...... Γv_n are not zero and all other Γ_v are zero. Then by (13), $A = F'(\Gamma A) = \Gamma^{-1}[\Gamma_v]_{v\in\mathbb{D}} = \prod_{i=1}^{m} P(v_i)^{\Gamma v_i}$. This representation of A as a product of powers of prime ideals is unique for by (12) every prime ideal is of the form P(v) for some v in $\mathbb{D}$, and any other product of pow-

st have a different image under the isomorphic mapping ψ. (See (13))

(15) If the classical ideal theory holds in the integral domain $\bar{O}$ with identity element, then $\bar{O}$ is a Dedikind ring.

Remark: It must tacitly be assumed that there is at least one prime ideal in $\bar{O}$.

Proof: Let $\mathbb{P}$ be the set of prime ideals of $\bar{O}$. Given P in $\mathbb{P}$, a valuation v_P is defined as follows: When a is in $\bar{O}^*$, the principle ideal $\bar{O}a$ can be written uniquely in the form P^xQ, where Q is a product of powers of prime ideals all distinct from P and where x is a non-negative rational integer. ($\bar{O}a = Q$ when $x = 0$.) Let $v_P(a) = x$. Let $v_P(0) = \infty$. The set of valuations $\{v_P\}_{P\in\mathbb{P}}$ is readily seen to satisfy II and IV.

Suppose $v_P(a) \geq V_P(b)$ for all P in $\mathbb{P}$. Then $\bar{O}a = \bar{O}b \circ A$ where A is a product of powers of finitely many prime ideals. Thus $a = b(ua')$ where u is in $\bar{O}$ and a' is in A. Axiom I thus holds.

$\bigcap_{i=1}^{\infty} A^i \circ A = \bigcap_{i=1}^{\infty} A^i$ for any ideal A. If $A \neq \bar{O}$, then $\bigcap_{i=1}^{\infty} A^i$ can consist only of the zero element. Thus if $\{0\} < B \subseteq A$, then $A^k \subseteq B$ for all sufficiently large K. Let P and Q be in $\mathbb{P}$, $P \neq Q$. Suppose $P \subset Q$. Let n be a positive integer such that $Q^n \subseteq P \subset Q^{n-1}$. There are elements a,b such that a is in Q, a is not in P, b is in Q^{n-1}, and b is not in P. Then ab is in Q^n, but ab is not in P, a contradiction. Thus there always is an element C in P and not in Q. $V_P(C) > 0$, but $V_Q(C) = 0$. Axiom III is valid.

Terms of Chapter I

Additive group	App. II.1
Element	App. I.1
Finite, finitely many	App. 1.4
Ideal	App. II.3
Identity element	App. II.2
Integral domain	App. II.2
Isomorphism	App. II.6
Mapping	App. I.3
Mapping onto	App. I.3
Maximal ideal	App. II.3
Multiple	App. II.3
Multiplicative semi-group	App. II.2
Null, non-null	App. I.1
Prime ideal	App. II.3
Principal ideal	App. II.3
Principal ideal ring	App. II.3
Proper ideal	App. II.3
Rational integers	App. I.2
Restricted direct sum	App. II.2
Ring	App. II.2
Semi-group	App. II.2
Set	App. I.1
Zero-element	App. II.1

Notation

$\subseteq, \supseteq, \not\subseteq, \subset, \varepsilon, \equiv, \neq$	App. I.1
$\{\ \}, [\ ]_{i=1}^{\alpha}, [\ ]_{i=1}^{n}$	App. I.4
$0, a + b, a - b, \sum_{i=1}^{m} a_i$	App. I.1
$1, a\ b, ab, a^n, \prod_{i=1}^{m} a_i$	App. II.2
$\overline{O}(a)$	App. II.3
$\cap$	App. I.1
$\overline{O^*}, \overline{R^*}, \overline{F^*}$	App. II.2
$\psi, \longrightarrow$	App. II.2
min.	App. I.3

CHAPTER II

OTHER AXIOMS FOR A DEDIKIND RING

Introduction: Throughout this chapter let $\bar{O}$ be an integral domain with identity element. Let *F* be the Quotient field of $\bar{O}$. (Refer to App. II. 7). A list, to be followed by proofs, will be given of conditions each necessary and sufficient in order that $\bar{O}$ be a Dedikind ring.

Definition (Valuation on a field; extension of valuation): Let *v* be a mapping of the multiplicative group of *F* (*F**) onto the rational integers. Let $v(0) = \infty$. Then *V* is termed a valuation on *F* if *V* satisfies the conditions: $V(a + b) \geq \min[V(a), v(b)]$; $v(ab) = v(a) + v(b)$.

Let *v* be a valuation of $\bar{O}$. Let *a* be in F*, with $a = x/y$, x, y in O*. For such *a* define $v(a) = v(x) - v(y)$; $v(0) = \infty$. It is observed that *v* will then be a valuation of *F*. Denote by *v'* the mapping into the integers determined by the restriction of *V* to $\bar{O}$. It is noted that the values of *V'* on $\bar{O}$ coincide with the values of the original valuation, *V*, on $\bar{O}$. Accordingly, *V* on *F* is referred to as an extension of *V* on $\bar{O}$.

Definition (valuation ring): Let *v* be a valuation on the field *F*. The valuation ring of *v*, denoted by $\bar{O}_V$, is the set $\{$ *x* in *F*/ $V(x) > 0 \}$. For all *a* in *F** either *a* or *1/a* is in $\bar{O}_v$.

Notation: Let A_1, A_2 -- An be subsets of F. By the product of the A_i, denoted by $\prod_{i=1}^{m} A_i$ or by A_1A_2 - - An is meant the set of all finite sums, $\sum_{i=1}^{m} a_{i_1}a_{i_2}\cdots a_{i_m}$ in which $a_{ij} \in A_j$, $1 \leq i \leq m$, $1 \leq j \leq m$.

Definition ($\bar{O}$-ideal): *A* is defined to be an $\bar{O}$-ideal of *F* providing the following conditions should hold:

A is an additive subgroup of F properly containing the set consisting only of the zero element; for all z in $\bar{O}$ and all a in A, za is in A; A has a multiplier p, that is to say,there is a p in F such that pA $\subseteq \bar{O}$.

Included amongst the $\bar{O}$ -ideals of F are the ideals in $\bar{O}$; these ideals are referred to as integral ideals. The term "prime ideal" refers to an integral ideal which is prime.

Notation: Unless specified otherwise, capital letters, e.g. A, B, C, ..., refer to $\bar{O}$ - ideals; underlined script letters, e. g. $\mathcal{P}$, $\mathcal{Q}$, $\mathcal{A}$, ..., refer to prime ideals.

Definition: (powers of an ideal): A^n is defined as $\prod_{k=1}^{n} A_k$, $A_k = A$, $1 \leq k \leq n$. A^{-1} is defined as follows: $A^{-1} = \{x \text{ in } F/\ xA \subseteq \bar{O}\}$ A^{-n}, n a positive integer, is defined as $(A^{-1})^n$. Since $AA^{-1} \subseteq \bar{O}$, A^{-1} has a multiplier, and therefore A^{-1} is an $\bar{O}$-ideal. The $\bar{O}$-ideals, $A^1 = A$, A^2, A^3, ...A^{-1}, A^{-2}, A^{-3}, ...are called the powers of A.

Definition (value of an $\bar{O}$-ideal) If V is a valuation defined on a field F, the V(A) is defined as $\min_{a \in A} \{V(a)\}$; it is observed that, since A has a multiplier, there actually is an a in A for which v(a) = v(A).

CONDITIONS FOR A DEDIKIND RING: A listing of conditions, each necessary and sufficient in order that $\bar{O}$ be a Dedikind ring, now follows:

(A): Valuations D on $\bar{O}$ satisfy axioms I-IV (See the beginning of Chapter I.)

(B): Prime power representation is valid in $\bar{O}$. (See I.15)

(C): Prime power representation is valid in F: For each $\bar{O}$- ideal A in F, A $\neq \bar{O}$, there is a finite set of distinct prime ideals, $[\mathcal{P}_1, \mathcal{P}_2 \ldots \mathcal{P}_n]$

and there is a set of non-zero integers $[\alpha_1, \alpha_2 --- \alpha_n]$ such that $\underline{A} = \prod_{i=1}^{n} \mathfrak{P}_i^{\alpha_i}$; moreover, the set of prime ideals and the corresponding integers α_i, $1 \leq i \leq n$, are uniquely determined by $\underline{A}$.

(D): There is a non-null set $\mathbb{D}$ of valuations on $\underline{F}$ such that:

I' - $\bar{O} = \bigcap_{v \in \mathbb{D}} \bar{O}_v$.

II' - If $\underline{a}$ is in $\underline{F}^*$ then $v(a) \neq 0$ for at most finitely many in $\mathbb{D}$.

III' - If $v_1 \neq v_2$, v_1 and v_2 in $\mathbb{D}$, then there is an $\underline{a}$ in $\underline{F}$ such that $v_1 (a)^- = 0$, $v_2(a) \neq 0$.

IV' - The only $\bar{O}$-ideal of $\underline{F}$ such that $v(A) = 0$ for all v in $\bar{O}$ is $\bar{O}$ itself.

(E): The $\bar{O}$ -ideals of $\underline{F}$ form a group. The group operation is ideal multiplication.

(G): There is a non-null set $\mathbb{D}$ of valuations on $\underline{F}$ such that:

(1) $\bar{O} = \bigcap_{v \in \mathbb{D}} \bar{O}_v$.

(2) If $\underline{a}$ is in $\underline{F}^*$ then $v(a) \neq 0$ for at most finitely many v in $\mathbb{D}$.

(3) Each Chinese Remainder system is solvable: Whenever a_1, a_2, ...a_n are in $\underline{F}$, v_1, v_2, ... v_n are distinct valuations of $\mathbb{D}$, and M is a positive integer, there then exists an element $\underline{x}$ in $\underline{F}$ such that $v_1 (x-a_1) > M$, $v_2 (x-a_2) > M$, ...$v_n (x-a_n) > M$, and $v(x) \geq 0$ for all other v in $\mathbb{D}$.

(F): Each of the following conditions hold:

(1) Each prime ideal is maximal. (Refer to app. II.3)

(2) The ascending chain condition is valid in $\bar{O}$. (Refer to app. II.5)

(3) $\bar{O}$ is integrally closed in its quotient field.

(Refer to app. III. 1)

In (14) and (15) of Chapter I it was shown conditions A and B are equivalent. The remainder of the chapter is concerned with proving that C, D, E, F and G are each equivalent to A and/or B.

<u>(1.) - A and B imply C:</u> Assume there are valuations $\mathbb{D}$ on $\bar{O}$ satisfying I-IV and that the classical ideal theory holds in $\bar{O}$. It then follows that in the quotient field <u>F</u> each $\bar{O}$ -ideal <u>A</u> ($A \neq \bar{O}$) is uniquely representable as a product of powers of finitely many prime ideals.

(a) $\mathfrak{p}\mathfrak{p}^{-1} = \bar{O}$.

<u>Lemma preceding (a):</u> For each v in $\mathbb{D}$ there is a <u>b</u> in <u>F</u> such that $v(b) = -1$ and v' (b) 0 for all other v' in $\mathbb{D}$.

<u>Proof of lemma</u>: There is an <u>r</u> in $\bar{O}$ such that $v(r) = 1$. By axiom I for the valuations $\mathbb{D}$ and result (I,2b), there is an <u>s</u> in $\bar{O}$ such that $v(s) = 0$ and $v'(s) \geq v'(r)$ for all other v' in $\mathbb{D}$. The element <u>s/r</u> has the required property.

<u>Proof of (a):</u> $\mathfrak{p} \leq \mathfrak{p}\mathfrak{p}^{-1} \leq \bar{O}$. Let v' be the valuation in $\mathbb{D}$ such that $\mathfrak{p} = P(v')$. It will be shown $V'(\mathfrak{p}\mathfrak{p}^{-1}) = 0$ whence $\mathfrak{p}\mathfrak{p}^{-1} = \bar{O}$ by (I,11) and (I, 8). By the lemma there exists <u>a</u> in <u>F</u> such that $v'(a) = -1$, $v(a) \geq 0$ for other v in $\mathbb{D}$. Thus, $a\mathfrak{p}^{-1} \leq \bar{O}$, <u>a</u> is in $\mathfrak{p}^{-1}$, and $0 \leq v'(\mathfrak{p}\mathfrak{p}^{-1})$ $v'(a\mathfrak{p}) = 0$.

<u>(b)</u> $\prod_{i=1}^{n} \mathfrak{p}_i^{\alpha_i} \cdot \prod_{i=1}^{n} \mathfrak{p}_i^{-\alpha_i} = \bar{O}$.

<u>Proof of (b):</u> This result follows by repeated application of (a), e. g., $(\mathfrak{p}\mathfrak{q})(\mathfrak{p}^{-1}\mathfrak{q}^{-1}) = (\mathfrak{p}\mathfrak{p}^{-1})(\mathfrak{q}\mathfrak{q}^{-1}) = \bar{O}\cdot\bar{O} = \bar{O}$.

<u>(c)</u> Let $\bar{O}a$ be a principle ideal in $\bar{O}$, and let $\bar{O}a = \prod_{i=1}^{n} \mathfrak{p}_i^{\alpha_i}$

Then $(\bar{O}a)\ -1 = \prod_{i=1}^{m} P_i^{-\alpha_i}$

<u>Proof of (c):</u> By result (d) below, $(\bar{O}a)^{-1}(\bar{O}a)(\prod_{i=1}^{m} P_i^{-\alpha_i}) = \prod_{i=1}^{m} P_i^{-\alpha_i}$ by (b), $(\bar{O}a)^{-1}(\bar{O}a)(\prod \underline{P}_i^{-\alpha_i}) = (Oa)^{-1}$

<u>(d)</u> For any <u>a</u> in <u>F*</u>, $(\bar{O}a)^{-1}\ \ (\bar{O}a) = \bar{O}$.

<u>Proof of (d):</u> This statement follows from the set equality $(Oa)^{-1} = \bar{O}(a^{-1})$.

$\bar{O}a^{-1} \subseteq (\bar{O}a)^{-1}$ for if <u>x</u> is in $\bar{O}a^{-1}$, then $x = b/a$ for some <u>b</u> in $\bar{O}$. $\bar{O}a(b/a) \subseteq \bar{O}$.

$(\bar{O}a)^{-1} \subseteq (Oa^{-1})$. If <u>x</u> is in $(\bar{O}a)^{-1}$, then <u>xa</u> is in $\bar{O}$ since <u>a</u> is in $\bar{O}a$; therefore, <u>x</u> is in $\bar{O}a^{-1}$.

<u>Proof of theorem:</u> Let <u>A</u> be an $\bar{O}$-ideal of F with multiplier <u>a</u>. Furthermore, let $\bar{O}a = \prod_{i=1}^{m} \underline{P}_i^{\alpha_i}$ and let $\underline{aA} = \prod_{j=1}^{m} \underline{q}_j$. Then, by (c) and (d), $\underline{A} = \bar{O}A = (\bar{O}a)^{-1}\ (\underline{aA}) = \prod_{i=1}^{m} P_i^{-\alpha_i} \prod_{i=1}^{m} q_j^{\beta_j}$. In this prime power representation of <u>A</u> it may be assumed that the $[\underline{P}_1 \ldots \underline{P}_n, \underline{q}_1 \ldots \underline{q}_m]$ are all distinct and that none of the $[\alpha_1, \ldots \alpha_n, \beta_1, \ldots \beta_m]$ are zero. Suppose that also $A = \prod_{k=1}^{p} \underline{R}_k^{\mu_k}$ where the $[\underline{R}_1, \ldots \underline{R}_p]$ are distinct prime ideals, and where the $[\mu_1, \ldots \mu_k]$ are non-zero integers. Then $A \circ \prod_{i=1}^{n} P_i^{\alpha_i} = \prod_{i=1}^{m} q_j^{\beta_j} = \prod_{i=1}^{n} P_i^{\alpha_i} \prod_{l=1}^{p} \underline{R}_k^{\mu_k}$ Thus $\prod_{k'=k \ni \mu_k > 0} \underline{R}_{k'}^{\mu_{k'}} \cdot \prod_{i=1}^{n} \underline{P}_i^{\alpha_i} = \prod_{j=1}^{m} \underline{q}_j^{\beta_j} \circ \prod_{k''=k \ni \mu_k < 0} \underline{R}_{k''}^{\mu_{k''}}$ The product on either side of the last "equals" sign is a representation of an integral ideal as a product of powers of finitely many distinct prime ideals. By the hypothesis, each of the $[R_k{}']$ is included amongst either the $[Q_j]$ or the $[R_k{}'']$; therefore, each $R_k{}'$ is included amongst the $[Q_j]$. Also, each of the $[Q_j]$ is included amongst the $[P_i]$ or amongst the $[R_k{}']$ and so each Q_j is included amongst the $[R_k{}']$. The $[R_k{}']$ and the $[Qj]$ thus coincide; by a similar argument, the $[R_k{}'']$ and the $[Pi]$ coincide. The exponents $[u_k{}']$ must then correspond to the exponents -

$[b_j]$ and the exponents $[u_k'']$ must then correspond to the exponents $[-a_i]$.

Corollary. The group condition is valid in F; the $\bar{O}$-ideals of F form a group under the operation ideal multiplication.

Proof of corollary: Clearly multiplication is an associative operation; the element $\bar{O}$ is an identity of the group; because of (b) and the conclusion of the theorem, each ideal has an inverse in the group.

Corollary. Condition D, axioms I'-IV' for a non-null set of valuations on the field F, is valid.

Proof of corollary: It was shown in (I.15) that the unique prime power representation of integral ideals implies axioms I-IV for valuations on $\bar{O}$; the proof of this corollary follows the same arguments.

Remark: Actually the axioms for the valuations Φ on F could be proved directly from the axioms for the valuations Φ on $\bar{O}$. If the non-null set Φ of valuations on $\bar{O}$ satisfy axioms I-IV, then the set Φ' of the extensions of these valuations satisfy I'-IV'.

In order to show that conditions A, B, C, and D are equivalent, a "sort of" converse to this last statement is proved. However, the axioms I'-IV' for valuations on the field F guarantee only that the axioms I-IV for some set Φ' of valuations on $\bar{O}$; the set Φ' is not necessarily the restriction to $\bar{O}$ of the valuations on F. (Example 1, Chapter V.)

(2) D implies A. Suppose the non-null Φ of valuations on F satisfies I'-IV' on F; then a non-null subset Φ of Φ' satisfies I-IV on $\bar{O}$.

Hypothesis for Φ on F *Conclusion for Φ on $\bar{O}$*

I'- $\bar{O} = \bigcap_{v \in \mathfrak{D}'} \bar{O}_v$

II'- For $v_1 \neq v_2$, v_1 and v_2 in $\mathbb{D}'$ there is an x in F such that $v_1(x) \neq \bar{O}$ and $v_2(x) > O$ O..

III'- For x in F*, $v(x) = 0$ except for at most finitely many v in $\mathbb{D}$.

IV'- $V(A) = 0$ for all v in $\mathbb{D}^*$ implies $A = \bar{O}$.

I. If a, b are in $\bar{O}$, v(a) v(b) for all v in $\mathbb{D}'$, the n a is a multiple of b.

II. For v_1, v_2 distinct members of $\mathbb{D}'$, there is an a in O such that $v_1(a) >$, $\bar{v}_2(a) = 0$.

III. For x in $\bar{O}^*$, $v(x) = 0$ except for at most finitely many v in $\mathbb{D}'$.

IV. $v(A) = 0$ for all v in $\mathbb{D}'$ implies $A = \bar{O}$.

Notation: The valuations in $\mathbb{D}$ and their respective restrictions to $\bar{O}$ will be denoted by the same symbols.

Proof of statement (2): The proof is by transfinite induction (refer to well-ordering axiom in appendix I.4 paragraph 3. Let the set $\mathbb{D}$ of valuations be indexed $[v_{1_\alpha}]_{i=1}^{i=\beta}$. Denote by $\{\bar{O}_\alpha\}$ the class of all subsets of F of the form $\bigcap_{j=1}^{\alpha} \bar{O}_{v_i}$ $(v_{i_j} \neq v_{i_k}$ for $j \neq k)$ where α is an index preceding or equal to β. Trivially all of the sets $\{\bar{O}_1\}$ or $\{\bar{O}_{vi}\}$, $1 \leq i \leq \beta$, are Dedikind rings. Suppose that for fixed α, all sets of the form $\{\bar{O}_{\alpha-1}\}$ are Dedikind rings. It will then be shown each of the sets $\{\bar{O}_\alpha\}$ are Dedikind rings. As a notational convenience, set $\bar{O}_\alpha = \bigcap_{i=1}^{\alpha} \bar{O}v_i$. It may be supposed that any set $\bigcap_{\substack{i=1 \\ i \neq k}}^{\alpha} \bar{O}v_i$ (where k is a fixed subscript, 1 k) properly contains $\bar{O}_\alpha$; if such is not the case, then $\bar{O}_\alpha$ is a Dedikind ring with valuations amongst the $[v_i]_{\substack{i=1 \\ i \neq k}}^{i=\alpha}$. In addition it can be inductively assumed that the valuations of the Dedikind rings $\bigcap_{\substack{i=1 \\ i \neq k}}^{i \leq \alpha} \bar{O}v_i$ $(1 \leq k \leq \alpha)$ are precisely the $\{V_i\}_{i=1}^{\alpha}$, $i \neq k$.

(a). The relation " < " (" > ") is defined as follows: $v_i < v_j$ $(v_j > v_1)$ if and only if there exists x in $\bar{O}_\alpha$ such that $v_1(x) = 0$

and $v_j\ (x) > 0$.

If v_i and v_j are distinct valuations, $1 \leq i,\ j \leq$, then it follows either $v_i < v_j$ or $v_i > v_j$

Proof of (a): Let m be a fixed subscript different from i and j. By the induction assumptions, there is an element x such that $v_j(x) > 0$, $v_i(x) = 0$, and $v_k(x) \geq 0$for $1 \leq k \leq \alpha$, $k \neq m$. It may be assumed that $v_m(x) < 0$. In the same way, there is an element y such that $v_m(y) > 0$, $v_j(y) = 0$, and $v_k\ (y) \geq 0$, $1 \leq k \leq \alpha$, $k \neq i$.

The possible cases are (i) $v_i(y) > 0$ (ii) $v_i(y) = 0$, and (iii) $v_i(y) < 0$.

Case (i) is trivial. In case (ii), $v_i(y^n x) = 0$, $v_j(y^n x) > 0$, and $y^n x$ is in $\bar{O}_\alpha$ for sufficiently large n. If case (iii) holds and if v_i is not $> v_j$, then there is a z in $\bar{O}$ such that vi (yz) =0, vj(yz)>0, and yz is in $\bar{O}_\alpha$.

(b). If $v_i < v_j$ for some subscript j, then $v_i < v_k$ for all $k \neq i$, $1 \leq k \leq \alpha$.

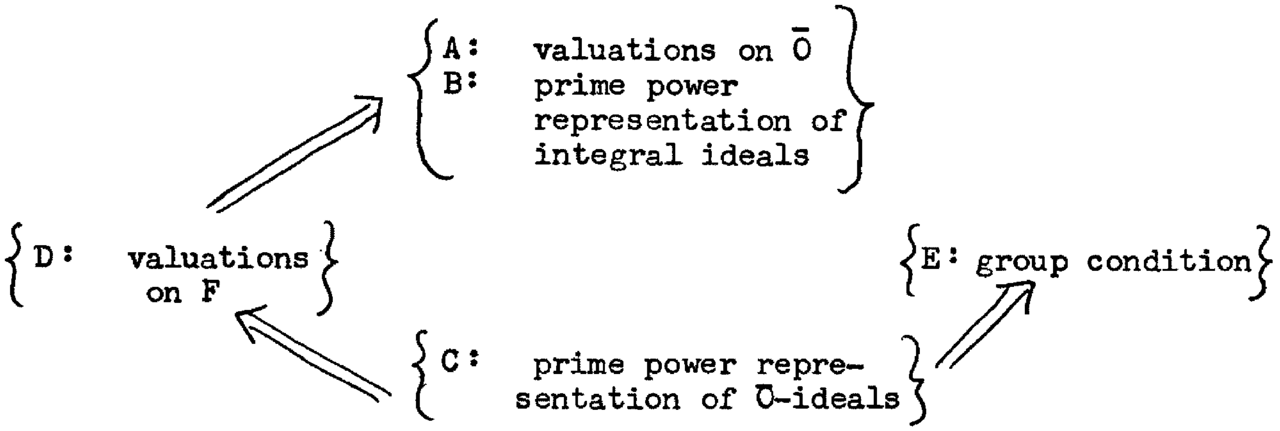
Proof of (b): There is a y in $\bar{O}$ such that $v_i(y) = 0, v_j(y) > 0$ $k \neq j$. There is a z in F such that $v_i(z) = 0$, $v_k(z) > 0$, and $v_h(z) \geq 0$, $1 \leq h \leq \alpha$, $h \neq j$. Then $v_i(y^m z) = 0$, $v_k(y^m z) > 0$, and $v_j\ (y^m z) \geq 0$ for m sufficiently large.

With these preliminary results, axiom II is shown to be valid in the ring $\bar{O}_\alpha$. Because of (a) it may be assumed $v_2 < v_1$. If it is also ttrue that $v_1 < v_2$, then by (b) , for all $i \neq j$ $1 \leq i,\ j \leq \alpha$, it is true that $v_i < v_j$.

Now let x be in $\bigcap_{i=1}^{\alpha} \bar{O}v_i$ and suppose $v_1\ (x) \nless 0$. There then exists y in $\bar{O}_\alpha$ such that $v_1(y) > 0$, $v_2(y) > 0$; there exists integers m and n such that $v_1(x_\alpha^m y^n) = 0$, $v_2(x^m y^n) > 0$, and $\underline{x^m y^n}$ is in $\bar{O}_\alpha$. Therefore, $v_1 < v_2$ unless $\bigcap_{i=2} \bar{O}v_i = \bar{O}_\alpha$.

$\bar{O}$ thus satisfies axiom II with valuations $\mathbb{D}_\alpha$, where $\mathbb{D}$ is either $[v_i]_{i=1}^{i=\alpha}$ or $[v_i]_{i=2}^{i=\alpha}$. Let $\underline{a}$ and $\underline{b}$ be elements in $\bar{Q}_\alpha$ such that $v(a) \geq v(b)$ for all v in $\mathbb{D}_\alpha$. Then a/b is in $\bigcap_{i=1}^{\alpha} \bar{O}v_i$, and so a= bc where c is in $\bar{O}_\alpha$. Axiom I thus holds for the $\mathbb{D}_\alpha$. Axioms III and IV readily follow from axioms III' and IV'.

Diagram of present results in this chapter:



{A: B: valuations on $\bar{O}$ prime power representation of integral ideals}

{D: valuations on F}

{E: group condition}

{C: prime power representation of $\bar{O}$-ideals}

Remark: As the diagram indicates, to show that A, B, C, D, and E are equivalent, it suffices to show that E implies B. Accordingly, in the ensuing statements (3, 4, and 5) it is assumed that the $\bar{O}$-ideals form a group under the operation of ideal multiplication; the conclusion will be that the classical ideal theory holds in $\bar{O}$.

(3A) $AA^{-1} = \bar{O}$.

Proof: Let A' be an $\bar{O}$-ideal of $\underline{F}$ such that $AA' = \bar{O}$. Then $A' \subseteq A^{-1}$. On the other hand, $AA^{-1} \subseteq \bar{\theta} = AA'$. Thus, $A^{-1} = A^{1} AA^{-1} \subseteq A' AA' = A'$.

(3b) Each $\bar{O}$-ideal of $\underline{F}$ is finitely generated over $\underline{O}$, and hence the ascending chain condition is valid for integral ideals.

Proof: Let A be an $\bar{O}$-ideal. By (3a), $1 = \sum_{i=1}^{m} x_i u_i$, where x_i is in A and u_i is in A^{-1}, $1 \leq i \leq n$. Then $A \circ \bar{O}(u_1, u_2, \ldots\ldots u_n) \subseteq \bar{O}$ since $Au_i \subseteq \bar{O}$, $1 \leq i \leq n$. Since $\underline{1}$ is in $\underline{\bar{O}}\ (x_1 \ldots\ldots . x_n)\bar{O}\ (u_1 \ldots . u_n)$, $\bar{O} \subseteq \bar{O}\ (x_1 \ldots x_n)\ \underline{\bar{O}}\ (u_1 \ldots u_n)$. It follows that $\underline{\bar{O}} \subseteq \underline{\bar{O}}(x_1 \ldots\ldots x_n)\ \bar{O}\ (u_1 \ldots . u_n) \subseteq A\bar{O}(u_1 \ldots u_n) \subseteq \bar{O}$. $\bar{O}(x_1 \ldots . x_n) = A$.

(3c) Each prime ideal is maximal amongst integral ideals: $\mathfrak{p} \subset A \subseteq \bar{O}$ implies $A = \bar{O}$.

Proof: The argument is exactly the same as that used in (I,15) with this slight change: If $A \neq \bar{O}$, then the group condition shows that $\bigcap_{i=1}^{\infty} A^i = A \cdot \bigcap_{i=1}^{\infty} A^i$ is possible if and only if $\bigcap_{i=1}^{\infty} A^i$ consists of only the zero element.

Notation: Let U and V be subsets of $\bar{O}$; by (U, V) is meant the ideal generated by U and V: $(U, V) =$

$$\left\{ x \text{ in } \bar{O} \;\middle|\; \begin{array}{l} \text{There are elmts. } a, b \text{ in } \bar{O}, \\ u \text{ in } U,\ v \text{ in } V \text{ such that} \\ x = au + bv. \end{array} \right\}$$

(4) If the ascending chain condition holds in $\bar{O}$, then each proper integral ideal A of $\bar{O}$ contains a finite product of prime ideals;: there are prime ideals $[\mathfrak{p}_i]_{i=1}^{i=n}$ such that $\prod_{i=1}^{m} \mathfrak{p}_i \leq A$. Furthermore, the $[\mathfrak{p}_i]_{1=1}^{i=n}$ may be chosen such that $\prod_{i=1}^{m} \mathfrak{p}_i \leq A \leq \mathfrak{p}_i$, $1 \leq i \leq n$.

Proof of (4): The required property is referred to as "P". Assume there is an ideal $A \subset \bar{O}$ for which "P" is not valid. Then A cannot be a prime ideal and there are elements $\underline{a}$,$\underline{b}$, in $\bar{O}$, $\underline{a}$ and $\underline{b}$ not in A, but $\underline{ab}$ is in A. Let $A_1 = (A, a)$ and $A_2 = (A, b)$. Then A_1 and A_2 are such that $A_1 A_2 \subseteq A$, $A \subset A_1$, $A \subset A_2$, and both A_1 and A_2 are proper ideals. (If, say, $A_1 = \bar{O}$, then $\bar{O}A_2 = A_2 \leq A$). Suppose "P" is valid for both A_1 and A_2; let $\prod_{i=1}^{m} \mathfrak{p}_i \leq A_1 \subseteq \mathfrak{p}_i$, $1 \leq i \leq n$ and $\prod_{i=1}^{m} \mathfrak{p}_{m+i} \subseteq A_2 \subseteq \mathfrak{p}_{m+i}$, $1 \leq i \leq m$. Then $\prod_{i=1}^{m+m} \mathfrak{p}_i \subseteq$

$A_1 A_2 \subseteq A \subseteq \mathfrak{p}_i$, $1 \leq i \leq n$ / m. Thus, "P" is not valid for either A_1 or A_2; suppose, then, "P" is not valid for A_1. As previously, there are proper ideals in $\bar{O}$, A_{21} and A_{22}, for which $A_{21}A_{22} \subset A_1 \subset A$ and $A_1 \subset A_{21}$, $A_1 \subset A_{22}$. Then $A \subset A_1 \subset A_{21}$, and $A \subset A_1 \subset A_{22}$. As before, "P" cannot be valid for both A_{21} and A_{22}. In this way arises a properly ascending chain of ideals, $A \subset A_1 \subset A_{21} \subset A_{31} \subset \cdots\cdots A_n 1 \subset A_{n/1}$ ......unless "P" is valid for the ideal A.

(5) Suppose that, in addition to the hypothesis of (4), it is true that all prime ideals of $\bar{O}$ are maximal. Then the prime ideals $[\mathfrak{p}_i]_{i=1}^{i=n}$ for which $\prod_{i=1}^{m} \mathfrak{p}_i \subseteq A \subseteq \mathfrak{p}_j$, j = 1, 2 .. and n, must be included amongst every set of prime ideals whose product is contained in A. In other words, if $\prod_{i=1}^{m} \mathfrak{q}_i \subseteq A$, then $[\mathfrak{q}_i]_{i=1}^{i=m} \subseteq [\mathfrak{p}_i]_{i-1}^{i=n}$.

<u>Proof of (5):</u> Let $\prod_{i=1}^{m} \mathfrak{q}_i \subseteq A \subseteq \mathfrak{p}$; now suppose that $\mathfrak{q}_j \not\subseteq \mathfrak{p}$ for j = 1, 2, , , ... or m. Then there are elements x_j in q_j, x_j not in $\mathfrak{p}$, $1 \leq j \leq m$; $\prod_{i=1}^{m} x_i$ is in $\prod_{i=1}^{m} \mathfrak{q}_i$, but not in $\mathfrak{p}$, a contradiction. Therefore, given a subscript i, $1 \leq i \leq n$, there is an i_j, $1 \leq i_j \leq m$, such that $\mathfrak{q}_{i_j} \subseteq \mathfrak{p}_i$.

(6) E implies B.

<u>Hypothesis:</u> The $\bar{O}$-ideals of <u>F</u> form a group under ideal multiplication.

<u>Conclusion</u>: Each integral ideal is uniquely representable as a product of powers of finitely many prime ideals.

<u>Remark:</u> If it is assumed that $\mathfrak{p}\mathfrak{p}^{-1} = \bar{O}$ for all $\mathfrak{p}$ and that the conclusions of (4) and (5) are valid, then the argument below is also applicable.

<u>Proof of (6)</u>: Let $A \subset \bar{O}$ and let $\prod_{i=1}^{m} \mathfrak{p}_i \subset A$. If $[\mathfrak{p}_i]_{i=1}^{i=n}$

consists of but one prime, $\mathfrak{p}$, then by (3c) $A = \mathfrak{p}$.

Assume for fixed m, but for all $A \subset \bar{O}$, that $\prod_{i=1}^{m} \mathfrak{p}_i \subseteq A$, implies A is equal to a finite product of prime ideals; $A = \prod_{j=1}^{m} \mathfrak{p}_{i_j}^{\alpha_j}$.

With this assumption on m consider $A \subset \bar{O}$ such that $\prod_{i=1}^{m+1} \mathfrak{p}_i \subseteq A$. By (4) there is a prime ideal $\mathfrak{p}$ which contains A; by (5), $\mathfrak{p}$ must be equal to $\mathfrak{p}_i$ for some i, $1 \leq i \leq n$, say $\mathfrak{p} = \mathfrak{p}_1$.

$\mathfrak{p}^{-1}(\mathfrak{p}_1 \mathfrak{p}_2 \cdots\cdots \mathfrak{p}_{m+1}) = \mathfrak{p}_2 \cdots\cdots \mathfrak{p}_{m+1} \subseteq \mathfrak{p}^{-1}A \subseteq \mathfrak{p}\mathfrak{p}^{-1} = \bar{O}$. The ideal $\mathfrak{p}^{-1}A$ is then integral, whence $\mathfrak{p}^{-1}A = \prod_{i=1}^{m} \mathfrak{p}_{i_j}^{\alpha_j}$, $2 \leq i_j \leq m \neq 1$. $\mathfrak{p}\mathfrak{p}^{-1}A = A = \mathfrak{p}\prod_{i=1}^{m} \mathfrak{p}_{i_j}^{\alpha_j}$.

Suppose $A = \prod_{i=1}^{m} \mathfrak{p}_i^{\alpha_i} = \prod_{j=1}^{m} \mathfrak{q}_j^{\beta_j}$. Then by (5) each $\mathfrak{q}_j$ is included amongst the $[\mathfrak{p}_i]_{1=1}^{i=n}$ and conversely, each $\mathfrak{p}_i$ is included amongst the $[\mathfrak{q}_j]_{i=1}^{j=m}$. $A = \prod_{i=1}^{m} \mathfrak{p}_i^{\alpha_i} = \prod_{i=1}^{m} \mathfrak{p}_i^{\beta_i}$:

$$\Bigl(\prod_{\substack{i=1 \\ i=i' \text{ such that } \alpha_i' \geq \beta_i'}}^{m} \mathfrak{p}_i^{\alpha_i' - \beta_i'}\Bigr) \circ \Bigl(\prod_{\substack{i=1 \\ i=i'' \text{ such that } \beta_i'' > \alpha_i''}}^{m} \mathfrak{p}_i^{\beta_i'' - \alpha_i''}\Bigr) = \bar{O}.$$

In this product, both of the bracketed ideals are integral, and so each of these ideals must be $\bar{O}$. Hence, $\alpha_i' = \beta_i'$ and $\alpha_i'' = \beta_i''$, $1 \leq i' \leq m$, $1 \leq i'' \leq n$. For each i, $\alpha_i = \beta_i$.

(7) A necessary and sufficient condition that $\bar{O}$ be a Dedikind ring is that each of the following conditions be valid: (a) $\bar{O}$ is integrally closed in F; (b) prime ideals are maximal and (c) the ascending chain condition hold.

Proof of necessity: Let $\mathfrak{D}$ be a set of valuations on $\bar{O}$ satisfying I-IV. If A is an ideal of $\bar{O}$, then A is a set of the form

$$\left\{ x \text{ in } \bar{O} \;\middle/\; \begin{array}{l} v_i(x) \geq a_i \text{ where the } a_1, a_2, \ldots\ldots a_n \text{ are positive integers;} \\ v_1, v_2 \ldots . v_n \text{ distinct members of } \mathfrak{D}, \end{array} \right\}$$

In view of (I.8) an ascending chain of ideals can consist of only finitely many distinct ideals. If $\mathfrak{p}$ is a prime ideal of $\bar{O}$ then by (I, 13)

$= P[v]$ for some valuation v; If the ideal A properly contains then $A = \bar{O}$. Thus (b) and (c) are proved; (a) follows in either of two ways, _____ as an immediate consequence of (IV.8), or as an immediate consequence of the fact that $\bar{O}$ is the intersection of a set of Gaussian rings, each of which has F as its quotient field.(Refer I.7, App. II.4 & III.1)

Proof of sufficiency: In view of previous results (see diagram p. 24) the classical ideal theory holds in $\bar{O}$ providing that $\underline{\mathfrak{p}}\underline{\mathfrak{p}}^{-1} = \bar{O}$ for all primes . In Van der Waerden [14, sect. 102, "Axiomatische Begrundung der Klassischen Idealtheorie".] appears a proof that $\underline{\mathfrak{p}}\underline{\mathfrak{p}}^{-1} = \bar{O}$.

Remarks: Actually the proofs of (1) and (2) of chapter III are applicable. These proofs show, assuming (a) and (c), that for certain prime ideals, $\underline{\mathfrak{p}}\underline{\mathfrak{p}}^{-1} = \bar{O}$. If in addition, it is assumed that all prime ideals are maximal (b), then it follows that for all prime ideals, $\underline{\mathfrak{p}}\underline{\mathfrak{p}}^{-1} = \bar{O}$.

In fact, the proof [12b, Van der Waerden, "Zur Productzerlegung der Ideale"; Sect. 485, pp. 298-9.] of (III.1) and (III.2) is essentially the proof in the above reference restated to include the possibility that a prime ideal is not maximal.

Remarks: The set of Chinese Remainder axioms (G) is, as previously mentioned, a necessary and a sufficient condition in order that $\bar{O}$ be a Dedikind ring. Result (80 proves the sufficiency of (G); result (9), the necessity.

The main results of this chapter, including (8) and (9) are diagrammed on p.. 24 bottom.

3b ascending chain cond. 4 proper integral ideal is contained in a prime ideal and contains a product of finitely many primes

(E) group condition 3c prime ideals max'l 5 the prime ideals may be chosen so as to appear in any product 6 unique prime power representation for integral ideals

3a $\underline{pp}^{-1} = \bar{O}$

G: Chinese Remainder axioms (9) A: Valuations on $\bar{O}$ B: Prime power representation for int. ideals (7) F: integral closure; chain cond.; prime ideals max'l

(8) (2) (1) 3,4,5,6

D: Valuations on $\underline{F}$. (1) C: Prime power representation for $\bar{O}$-ideals (1) E: Group condition

(8) Sufficiency of the Chinese Remainder axioms

Hypothesis: $\bar{O}$ is a Dedikind ring; the non-null set $\mathfrak{D}$ of valuations on $\bar{O}$ satisfy axioms I-IV. The valuations $\mathfrak{D}$ satisfy axioms I-IV' on the quotient field F. (See (1) and second corollary to (1)

Conclusion: The Chinese Remainder axioms are valid; in addition to axioms I' and II' being true, each Chinese Remainder equation is solvable. For each set $[a_i]_{i=1}^{i=n}$ of elements in F, each finite set of distinct valuations in $\mathfrak{D}$, and each positive integer M, there is an element x in F such that $v_i\ (x-a_i) > M$, $i \leq i \leq n$ and $v(x) \geq 0$ for all other v in $\mathfrak{D}$.

(a) If A and B are integral ideals such that v(A) and v(B) are never positive for the same v in $\mathfrak{D}$, then $(A,B) = \bar{O}$.

Proof of (a): Let v_1, v_2, ... v_n and v_{n+1}, . . .v_{m+m}, $v_i \neq v_j$ for $i \neq j$, include all positive values for A and B respectively. Let v_o be any valuation distinct from $[v_i]_{i=1}^{i=n+m}$. (The argument is still valid if there is no such v_o). There exists a in A such that $v_i(a) = v_i\ (A)$, $0 \leq i \leq n+m$; there exists b in B such that $v_i(b) = v_i(B)$, $0 \leq i \leq n+m$. There exists c in $\bar{O}$ such that $v_o(c) > 0$, $v_i(c) = 0$, $1 \leq i \leq n+m$. Then a + bc is in (A,B) and $v_i(a+bc) = 0$, $0 \leq i \leq n+m$. But v_o is arbitrary. $v(A,B) = 0$ for all v in $\mathfrak{D}$. $(A,B) = \bar{O}$.

(b) A Chinese Remainder equation in $\bar{O}$ has a solution:

If $v_i(x-a_i) > M$, $1 \leq i \leq n$, is a Chinese Remainder equation in which the $[a_i]_{i=1}^{i=n}$ are all elements in $\bar{O}$, then there is an x in $\bar{O}$ for which the equation is valid.

Proof of (b): Consider a possible solution of the form $x = a_1x_1 + a_2x_2 + a_3x_3 \ldots\ldots\ldots + a_nx_n$. The element x is then a solution providing that the $[x_i]_{i=1}^{i=n}$ are all in $\bar{O}$, $v_i(a_j$ M for

$i \neq j$ $(1 \leq i, j \leq m)$, and v_i $(a_i - 1) > M$ $(1 \leq i \leq n)$. If all these conditions hold then $v(x) \geq 0$ for $v \neq v_1, v_2, \ldots$ or v_n; $v_i(x - a_i) =$

v_i $\left[\sum_{j=1, j \neq i}^{m} A_j X_j + (x_{i-1}) a_i \right] \geq$
$\min \left[v_i(x_1 a_1), \ldots\ldots v_i(xj\text{-}1^a j\text{-}1), v_i(x_j + 1^a j + 1) \ldots\ldots\ldots \right.$
$\left. v_i(x_n a_n), v_i(x_i(a_{i_i}^{-1}) x_i) \right] > M.$

The $\left[x_i \right]_{i=1}^{i=n}$ may be chosen to satisfy the conditions mentioned in the last paragraph, because by (a) the ideals $A =$ $\{ \underline{x}$ in $\bar{O}$ / $vj(x)$ M, $1 \leq j \leq n$, $j \neq i \}$ and $B = \{ x$ in $\bar{O}$ / $v_i(x) > M \}$ are such that $(A,B) = \bar{O} \geq \{1\}$.

<u>Proof that each Chinese Remainder system is solvable:</u>

Let $\left[v_i \right]_{i=1}^{i=n}$ be distinct valuations in $\mathbb{D}$, $\left[a_i \right]_{i=1}^{i=n}$ be any elements of $\underline{F}$, and M any positive integer. Let $a_1 = c_1/d$, $a_2 = c_2/d$, $\ldots$ and $a_n = c_n/d$ where $\underline{d}$ is the product of the denominators of the $\left[a_i \right]_{i=1}^{i=n}$ when expressed as quotients of elements in $\bar{O}$. Then $c_1, c_2 \ldots\ldots c_n$ are in $\bar{O}$.

Now v_i $(x - a_i) > M$ $(1 \leq i \leq n)$ providing that v_i $\frac{(xd - c_i)}{d} > M$ $(1 \leq i \leq m)$. Let $v_1, v_2 \ldots v_n, v_{n+1} \ldots\ldots v_{n+m}$ include all valuations which do not vanish on $\underline{d}$, and let $N = \max_{v \text{ in } \mathbb{D}} \left[v(d) \right]$. By (b) there is an element $\underline{y}$ in $\underline{F}$ such that v_i $(y - c_i) > M + N$, $1 \leq i \leq n$; v_{n+i} $(y) > M + N$, $1 \leq i \leq m$; and $v(y) \geq 0$ for $v \neq v_1, \ldots\ldots$ or v_{n+m}; Let $x = y/d$. It follows v_i $\left(\frac{xd - c_i}{d} \right) > M$ for $v = v_1, \ldots$ or v_n and $v(x) \geq 0$ for all other v in $\mathbb{D}$.

<u>(9) G implies A</u>

<u>Hypothesis:</u> A set $\mathbb{D}$ of valuations on $\underline{F}$ is such that (i) $\bar{O} =$ $\bigcap_{v \in \mathbb{D}} \bar{O}_{v_i}$; (ii) $\underline{a}$ in $\underline{F}^*$ implies $v(a) \neq 0$ for a most finitely many v in $\mathbb{D}$; (iii) each Chinese Remainder system is solvable.

<u>Conclusion:</u> $\underline{\bar{O}}$ is a Dedikind ring with valuations $\mathbb{D}$ (or more

precisely, the restrictions of members of $\mathbb{D}$ to $\bar{O}$)

<u>Proof</u>: From hypothesis (i) and (ii) readily follow properties I and II for the valuations $\mathbb{D}$ on $\bar{O}$ (refer to the last paragraph of the proof of (2). Also if v_1, v_2 are distinct valuations in $\mathbb{D}$, then there is an element $\underline{x}$ in $\underline{F}$ such that $v_1(x) > 1$, $v_2\ (x-1) > 1$ and $v(x) \geq 0$ for all other v in $\mathbb{D}$. Thus $v_1(x) > 0$, $v_2(x) = 0$, and $\underline{x}$ is in $\bar{O}$. Axiom III is verified. The proof that $v(a) = 0$ for all valuations v implies that $A = \bar{\theta}$ follows:

<u>(a)</u> If $v_1, \ldots . v_n$ are distinct valuations in $\mathbb{D}$, there is an $\underline{a}$ in A such that $v_i(a) = 0$, $1 \leq i \leq n$.

<u>Proof of (a):</u> Assuming axioms I to IV for the valuations this statement is a special case of (I,6). It is observed that the proof of (I, 6) does not depend on axiom IV.

<u>(b)</u> A Chinese Remainder system is solvable in A: given elements $a_1, \ldots . a_n$ in $\bar{O}$ (they need not be in A), distinct valuations v_1, $\ldots .$and v_n, and a positive integer M, then it follows there exists $\underline{x}$ in A such that $v_i(x-a_i) > M$, $1 \leq i \leq n$.

<u>Proof of (b):</u> By (a) there is a $\underline{b}$ in A such that $v_i(b) = 0$, $1 \leq i \leq n$. Let $v_{n+1}, \ldots . v_{n+m}$ include all valuations that do not vanish for $\underline{b}$ (if there are no such v_{n+i}, $\underline{b}$ is a unit and $A = \bar{O}$). and let $N = \max\limits_{1 \leq i \leq m} \{ [v_{n+i}\ (b)], M \}$. Then, by (iii) there is a $\underline{y}$ in $\underline{F}$ such that $v_i\ (y-a_i) > N \geq M$ $(1 \leq i \leq n)$; $v_i(y) > N$ $(n+1 \leq i \leq n+m)$; $v(y) \geq \theta$ for all other v in $\mathbb{D}$. Then $v(y) \geq 0$ for all v in $\mathbb{D}$ and so $\underline{y}$ is in $\mathbb{D}$; since $v(y) \geq v(b)$ for all v in $\mathbb{D}$, $\underline{y}$ is a multiple of $\underline{b}$ and $\underline{y}$ is in A.

<u>Proof that $A = \bar{O}$:</u>

Let a be in $\bar{O}$. For a non-unit element $\underline{b}$ in A, by statement (b) there exists $\underline{x}$ in A such that $v_i(x-a) > M$ $(1 \leq i \leq n)$; the set $[v_1, \ldots . v_n]$ is presumed to include all the valuations positive for b and M is presumed to equal $\max_{1 \leq i \leq n} \{v_i(b)\}$. It then follows *x-a* is a multiple of *b*; *x-a* is in A. The element *a* is in A. A = $\bar{0}$.

Terms of Chapter II

Associative	App. II.2
Ascending chain condition	App. II.3
Finitely generated	App. II.5
Gaussian ring	App. II.4
Indexed set	App. I.4
Integrally closed	App. I.1
Multiplicative group	App. II.1
Operation	App. II.1
Power	App. II.1
Quotient field	App. II.7
Subset	App. I.1
Trans-finite induction	App. I.4

Notation

$\frac{b}{a}$, b/a, a^{-1}	App. II.7
max	App. I.3
$\bar{0}(x. - - x_n)$, $0(x)$, $\bar{0}x$	App. II.3
(A, B)	App. II.3

CHAPTER III

PRINCIPALLY ORDERED SYSTEMS

Introduction: A type of ring with somewhat less restrictive properties than a Dedikind ring is a principally ordered system. (Author's own translation of the German "Hauptordnung.") Briefly, a principally ordered system is an integral domain which is the intersection of valuation subrings of its quotient field. [6 Krull, Wolfgang, Sections 1 to 4] proves that an integral domain $\bar{O}$ is a principally ordered system if and only if it is integrally closed in its quotient field. Suppose, now, $\bar{O}$ is not only integrally closed in its quotient field, but also satisfies the ascending chain condition. The question then arises, just what sort of a principally ordered system is $\bar{O}$? In this chapter, results of Krull and Van der Waerden are derived and applied in order to answer this question.

Definition (*principally ordered system*): Let $\bar{O}$ be an integral domain with quotient field $\underline{F}$. If there exists a non-null set $\mathfrak{M}$ of valuations on $\underline{F}$ such that $\bar{O} = \bigcap_{v \in \mathfrak{M}} \bar{O}_v$, then $\bar{O}$ is called a principally ordered system. In this chapter a valuation on a field $\underline{F}$ is defined as a mapping of $\underline{F}^*$ onto a non-null, non-zero additive subgroup of a direct summand of real numbers (see "direct summand" in appendix on Basic Algebra) such that the conditions for v(ab) and v(a + b) hold as indicated in Chapter I.

The principally ordered system $\bar{O}$ is said to be discrete (rank one) if each of the valuations v in $\mathfrak{M}$ are discrete (rank one) valuations. In other words, if the system is discrete, each v in $\mathfrak{M}$ maps F* onto a set of rational integers.

The principally ordered system is said to be finite if for each $\underline{a}$ in F^+, $v(a) \neq 0$ for at most finitely many v in Φ.

The principally ordered system is said to have the separation property if for distinct v_1 and v_2 in Φ, there is an $\underline{a}$ in $\bar{\mathfrak{o}}$ such that $v_1(a) > 0$ and $v_2(a) = 0$.

Thus a finite, discrete principally ordered system with separation property satisfies axioms I-III for a Dedikind ring.

<u>Remark</u>: Since $\bar{\mathfrak{o}}$ is an intersection of valuation rings, the identity element of F, 1 is in $\bar{\mathfrak{o}}$.

Throughout most of this chapter (up to and including the proof of (8)) it is assumed that $\bar{\mathfrak{o}}$ is an integral domain, integrally closed in its quotient field, and satisfying the ascending chain condition.

The reader is advised especially to look up, amongst other references, the material in appendix II.5.

<u>Definitions</u> (<u>minimal prime ideals</u>; <u>higher ideals</u>): A prime ideal $\underline{p}$ in $\bar{\mathfrak{o}}$ is said to be a minimal prime ideal if $\mathfrak{q} \subseteq \mathfrak{p}$ ($\mathfrak{q}$ is a prime ideal) implies $\mathfrak{q} = \mathfrak{p}$. The primary ideal P is said to be an higher primary ideal if P is contained in one and only one prime ideal. The ideal A is said to be an higher ideal if A is the intersection of finitely many higher primary ideals.

<u>Definition</u> (<u>equivalence of ideals</u>): The ideals A and B of $\bar{\mathfrak{o}}$ are said to be equivalent, denoted by $A \sim B$, if there exist ideals C and D such that $\underline{AC} \leq \underline{B}$, $\underline{BD} \subseteq \underline{A}$, and such that C and D are the products of finitely many ideals that properly contain a minimal prime ideal.

<u>Remarks</u>: $A \sim B$ is an equivalence relation amongst ideals of $\bar{\mathfrak{o}}$. The class of all finite products of ideals which properly contain a minimal

prime ideal comprises the equivalence class of which $\bar{O}$ is a member (see Statement (1) below).

Let A, B, C, and D be ideals; if $A \sim B$, and $C \sim D$, then $AC \sim BD$.

(1) Let $[\mathfrak{p}_i]_{i=1}^{i=n}$ be a set of prime ideals of $\bar{O}$ and let $\mathfrak{p}$ be a minimal prime ideal. Then it is not possible that $\prod_{i=1}^{m} \mathfrak{p}_i \subseteq \mathfrak{p}$ unless either $\mathfrak{p} = \mathfrak{p}_1$, $\mathfrak{p} = \mathfrak{p}_2$, ... or $\mathfrak{p} = \mathfrak{p}_m$.

Proof: If $\mathfrak{p} \neq \mathfrak{p}_i$, $1 \leq i \leq n$, then there are elements x_1, $1 \leq i \leq n$, such that x_i is in $\mathfrak{p}_i$ and x_i is not in $\mathfrak{p}$. As in (II.5) this is not possible.

(2) If $\mathfrak{p}$ is a minimal prime ideal, then $\mathfrak{p}^{-1} \supset \bar{O}$.

Proof: Clearly $\mathfrak{p}^{-1} \supseteq \bar{O}$. Let $a \neq 0$, a in $\mathfrak{p}$. Then by (II.4) for some positive integer n there are prime ideals $\{\mathfrak{p}_i\}_{i=1}^{1=n}$ such that $\prod_{i=1}^{m} \mathfrak{p}_i \subseteq \bar{O}(a)$. (The primes, $\mathfrak{p}_i$, need not be distinct.) Let n be chosen to be minimal with respect to this property. Since a is in $\mathfrak{p}$, by (1) there is a subscript i, $1 \leq i \leq n$, such that $\mathfrak{p} = \mathfrak{p}_i$. Let $\mathfrak{p} = \mathfrak{p}_1$. Then $\mathfrak{p}_2 \cdot \mathfrak{p}_3 \cdots \mathfrak{p}_m \not\subseteq \bar{O}(a)$. Let b be an element in $\mathfrak{p}_2 \mathfrak{p}_3 \cdots \mathfrak{p}_m$, b not in $\bar{O}(a)$.

It follows $(b/a) \varepsilon' \bar{O}$, and b/a is in $\mathfrak{p}^{-1}$. (If x is an elemental such that $x(b/a)$ is not in $\bar{O}$, then xb is not in $\bar{O}(a)$). Since b is not in $\bar{O}(a)$, b/a is not in $\bar{O}$.

(3) If $\mathfrak{p}$ is a minimal prime ideal, then $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1}$, and so $\mathfrak{p}\mathfrak{p}^{-1} \sim \bar{O}$.

Proof: Suppose $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. Let $\mathfrak{p} = \bar{O}(a_1, ...a_n)$. Let x be in $\mathfrak{p}^{-1}$. Then $a_i x$ is in $\mathfrak{p}$, $1 \leq i \leq n$; there are elements of $\bar{O}$, $\{c_{ij}\}_{i,j=1}^{i,j=n}$ such that $a_i x = \sum_{k=1}^{m} c_{ik} a_k$, $1 \leq i \leq n$. The a_1, a_2, ...a_n then compose a non-trivial solution (app. II.8) to a linear homogeneous equation in F. Therefore,

$$\begin{vmatrix} c_{11}-x & c_{12} & c_{13} & \cdots & c_{1m} \\ c_{21} & c_{22}-x & c_{23} & \cdots & c_{2m} \\ c_{31} & c_{32} & c_{33}-x & \cdots & c_{3m} \\ \vdots & \vdots & \vdots & & \vdots \\ c_{m1} & c_{m2} & c_{m3} & \cdots & c_{mm}-x \end{vmatrix} = 0.$$

The element $\underline{x}$ is then a root of an equation of degree $\underline{n}$ in which the coefficient of $\underline{x}^n$ is +1 or −1 and all other coefficients are in $\bar{O}$.

Therefore, $\underline{x}$ must necessarily be in $\bar{O}$; this result contradicts (2).

(4) Each higher primary ideal is equivalent to a power of a minimal prime ideal.

<u>Proof</u>: Let $\underline{A}$ be a higher primary ideal, let $\underline{\mathfrak{p}}$ be the only minimal prime ideal containing A. Let $\bar{r}$ be the least positive integer for which $\underline{\mathfrak{p}}^n \subseteq$ A. (See app. II.5.) Let $\underline{G} = \underline{\mathfrak{p}}\underline{\mathfrak{p}}^{-1}$. Then $\underline{G} \sim \bar{O}$ and $\underline{G}^n \sim \bar{O}$. Because $\underline{G}^n = \underline{\mathfrak{p}}^{-n}\underline{\mathfrak{p}}^n \subseteq \mathfrak{p}^{-n}A$, $\underline{\mathfrak{p}}^{-n}A$ is not contained in $\underline{\mathfrak{p}}$ by (1). Let $\underline{s}$ be the least non-negative integer such that $\underline{\mathfrak{p}}^{-s}A \subseteq \underline{\mathfrak{p}}$ now. $\underline{\mathfrak{p}}^{-s-1}A$ = $\underline{\mathfrak{p}}^{-1}\underline{\mathfrak{p}}^{-s}A \subseteq \underline{\mathfrak{p}}\underline{\mathfrak{p}}^{-1} \subseteq \bar{O}$, and so $\underline{\mathfrak{p}}^{-s-1}A$ is then an integral ideal. Let $\underline{n}$ be any minimal prime ideal different from $\underline{\mathfrak{p}}$ and suppose that $\underline{\mathfrak{p}}^{-s-1}A \subseteq \underline{n}$. $\underline{G}^{s+1}A$ = $\underline{\mathfrak{p}}^{s+1}\underline{\mathfrak{p}}^{-s-1}A \subseteq \underline{n}\,\underline{\mathfrak{p}}^{s+1} \subseteq \underline{n}$. Since $\underline{G} \nsubseteq \underline{n}$, then as in (1) $A \subseteq \underline{n}$, but this is contrary to the hypothesis that $\underline{A}$ is a higher ideal. Thus $\underline{\mathfrak{p}}^{-s-1}A$ is not contained in any minimal prime ideal. By II.5 there are prime ideals $[\mathfrak{p}_i]_{i=1}^{m}$ such that $\prod_{i=1}^{m}\underline{\mathfrak{p}}_i \subseteq \mathfrak{p}^{-s-1}A \subseteq \mathfrak{p}_i$ 1≤ i ≤ n. Thus $\underline{D} \subseteq \underline{\mathfrak{p}}^{-s-1}A \subseteq \bar{O}$, where $\underline{D}$ is a product of finitely many non minimal prime ideals. $\underline{\mathfrak{p}}^{-s-1}A \sim \bar{O}$. $\underline{G}^{s+1}A \sim \underline{\mathfrak{p}}^{s+1}$. $A \sim \underline{\mathfrak{p}}^{s+1}$.

(5) Each higher ideal is uniquely equivalent to a finite product of powers of minimal prime ideals: if $\underline{A}$ is an higher ideal, then $A \sim \prod_{i=1}^{m}\underline{\mathfrak{p}}_i^{\alpha_i}$ where the $[\mathfrak{p}_i]_{i=1}^{i=n}$ are a set of distinct minimal prime ideals; the $[\underline{\mathfrak{p}}_i]_{i=1}^{i=n}$ and the corresponding exponents are uniquely determined by A.

(a) If the ideals A and B are such that $A \subseteq \underline{\mathfrak{p}}$, and $B \subseteq \underline{\mathfrak{q}}$ where $\underline{\mathfrak{p}}, \underline{\mathfrak{q}}$ are distinct minimal prime ideals, then $A \cap B \sim AB$.

<u>Proof</u>: (A ∩ B)° (A;B) ⊆ A°B since (A ∩ B)°(A,B) = [(A B)°A,

$(A\ B)^{o}B] \subseteq (B^{o}A, B^{o}A) = B^{o}A$. Then $(B \cap A) \circ N \subseteq B \circ A$ where $N = (\mathfrak{p}, \mathfrak{q})$. Since N properly contains the minimal prime, $\mathfrak{p}$, and since $BA \subseteq B \cap A$, $BA \sim B \cap A$.

(b) If $A_1, \ldots\ldots A_n$ are ideals of $\bar{O}$ such that $\underline{A_i} \subseteq \mathfrak{p}_i$, $1 \leq i \leq n$, where the $[\mathfrak{p}_i]_{i=1}^{i=n}$ are a set of distinct prime ideals, then $\bigcap_{i=1}^{m} A_i \sim \prod_{i=1}^{m} A_i$.

Proof follows by repeated application of (a).

Proof of (4): If A is an higher ideal, then $A = \bigcap_{i=1}^{m} Q_i$ where the Q_i, $1 \leq i \leq n$, are higher primary ideals, each contained in a distinct minimal prime ideal [2 Jacobson, N. H., section 8, chapter VI] (also see previous reference to appendix on algebra). Then by (b), $A \sim \prod_{i=1}^{m} Q_i$ and by (4) $A \sim \prod_{i=1}^{m} \mathfrak{p}_i^{\alpha_i}$, where the $[\mathfrak{p}_i]_{i=1}^{i=n}$ are minimal prime ideals. Now $A\mathfrak{p}_1^{-1} \sim \mathfrak{p}_1^{\alpha_1 - 1} \prod_{i=2}^{m} \mathfrak{p}_i^{\alpha_i}$ since otherwise $A \sim A\mathfrak{p}_1\mathfrak{p}_1^{-1}$ is not equivalent to $\prod_{i=1}^{m} \mathfrak{p}_i^{\alpha_i}$. The proof of uniqueness thus proceeds by induction on the sum of the exponents. If $B \sim \mathfrak{p}$ an $B \sim \mathfrak{q}$ where $\mathfrak{p}$ and $\mathfrak{q}$ are distinct minimal primes, then $G\mathfrak{p} \subseteq \mathfrak{q}$ where $G \sim O$. By (1) this is impossible.

Corollary: If $\underline{A}$ is an higher ideal, then A is contained in only finitely many prime ideals.

Proof: Let $A = \prod_{i=1}^{m} \mathfrak{p}_i^{\alpha_i}$ where the $[\mathfrak{p}_i]_{i=1}^{i=n}$ are minimal prime ideals. Thus $\underline{C}^{o} \prod_{i=1}^{m} \mathfrak{p}_i^{\alpha_i} \subseteq A$ where $\underline{C} \sim \bar{O}$. If $\mathfrak{p}$ is a minimal prime ideal containing $\underline{A}$, then as in (1), $\mathfrak{p}$ is included amongst the $[\mathfrak{p}_i]_{i=1}^{i=n}$.

(6) Hypothesis: $\bar{O}(a)$ is a principle ideal of $\bar{O}$ and $\bar{O}(a) \subset \bar{O}$.

Conclusion: $\bar{O}(a)$ is an higher ideal; by (5) $\bar{O}(a) \sim \prod_{i=1}^{m} \mathfrak{p}_i^{\alpha_i}$ where the $[\mathfrak{p}_i]_{i=1}^{i=n}$ are minimal prime ideals, $[\alpha_i]_{i=1}^{i=m}$ positive integers. Refer to app. (II.5) for results used in proof.

Remarks preceding proof: If Q is a non-higher primary ideal, then there are, as shown in Jacobson [2 Chapter 6, section 8], prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ such that $Q \subseteq \mathfrak{p} < \mathfrak{q}$ and such that $\mathfrak{p}$ equals the radical of Q.

It can be shown that an higher ideal is an irredundant short intersection of higher primary ideals: If A is an intersection of finitely many higher primary ideals, then A is also an irredundant intersection of finitely many higher ideals. If two distinct ideals, P and Q, of such an irredundant intersection have the same radical $\mathfrak{p}$, then $P \cap Q$ is a non-higher primary ideal only if either P or Q is non- higher. For, if $P \cap Q \subseteq \mathfrak{p} < \mathfrak{q}$, then $PQ \leq P \cap Q \subset \mathfrak{q}$ and by (1) either P or Q is contained in $\mathfrak{q}$. (See app. II.5.)

Proof: Let $\bar{O}(a)$ be an irredundant short intersection of primary ideals, $\bigcap_{i=1}^{n} Q_1$. If $\bar{O}(a)$ is not an higher ideal, then by the above remarks one of the Q_i, $1 \leq i \leq n$, is non-higher. Such a Q_1 is denoted by Q. Let $\mathfrak{p}$ be the radical of Q and let $\mathfrak{q}$ properly contain $\mathfrak{p}$. The set $\{b \varepsilon \bar{O} / b\mathfrak{p} \leq \bar{O}(a)\}$ is denoted by $\bar{O}(a): \mathfrak{p}$. Then $\bar{O}(a): \mathfrak{p} \geq \bar{O}(a)$ and, in fact, $\bar{O}(a): \mathfrak{p} \supset \bar{O}(a)$ as provided in Jacobson [Chapter XI, sections 7,8 (note theorem 6)]. Let b be an element of $\bar{O}(a): \mathfrak{p}$ not in $\bar{O}(a)$; then b/a is an element of $\mathfrak{p}^{-1}$ and also of $\mathfrak{q}^{-1}$ which is not in $\bar{O}$. Now by (II.1d), $\mathfrak{q}^{-1}\mathfrak{p} \leq \mathfrak{p}\bar{O}(a)^{-1} = \mathfrak{p}\,\bar{O}(a^{-1}) \subseteq \mathfrak{p}\ {}^{o}(\bar{O}(b/a)) \leq \bar{O}$; thus $\mathfrak{q}^{-1}\mathfrak{p}$ is an integral ideal containing $\mathfrak{p}$. By an argument similar to that employed in (3), $\mathfrak{q}^{-1}\mathfrak{p} > \mathfrak{p}$. Let c be an element of $\mathfrak{q}^{-1}\mathfrak{p}$ not in $\mathfrak{p}$. Then $c\mathfrak{q} \leq \mathfrak{p}\mathfrak{q}^{-1}\mathfrak{q} \leq \mathfrak{q}$ and so $\mathfrak{q} \leq \mathfrak{p}$. But this contradicts the choice of $\mathfrak{q}$.

Notation: Denote by $\mathfrak{M}$ the set of all minimal prime ideals of $\bar{O}$.

Corollary: If $\bar{O} \subsetneq F$ (F the quotient field), then $\mathfrak{M}$ is a non-null set.

Corollary: Let $\bar{O}(a)$ be a principal ideal properly contained in $\bar{O}$. Then $\bar{O}(a)$ is contained in only finitely many $\mathfrak{p}$ in $\mathfrak{M}$. (See the corollary to (4)).

(7) For each $\mathfrak{p} \varepsilon \mathfrak{M}$ let the set $\left\{ \underline{a} \text{ in } \underline{F} \,\middle/\, \begin{array}{l} \text{There exist u,v in } \bar{O} \text{ such} \\ \text{that a = u/v, v is not} \\ \text{in } \mathfrak{p}. \end{array} \right\}$ be denoted by $\bar{O}_{\mathfrak{p}}$. Then $\bar{O}_{\mathfrak{p}}$ is a ring, and is, in fact, an integral domain. Let the set $\left\{ \underline{a} \text{ in } \bar{O} \,\middle/\, \begin{array}{l} \text{There exist uh, such} \\ \text{that a = uh, where } \underline{h} \text{ is} \\ \text{in } \mathfrak{p} \text{ and u is a unit of} \\ \bar{O}\text{p}. \end{array} \right\}$ be denoted by $\underline{\mathfrak{p}}'$. It then follows $\mathfrak{p}'$ is a prime ideal of $\bar{O}$ and that each ideal $\underline{A}$ in $\bar{O}$ is equal to a uniquely determined power of $\mathfrak{p}'$. ($\bar{O}_{\mathfrak{p}}$ is referred to as $\underline{\mathfrak{p}}'^{o}$.) Thus $\bar{O}_{\mathfrak{p}}$ is a Dedikind ring.

Proof: Clearly $\bar{O}_{\mathfrak{p}}$ is an integral domain. The set, $U_{\mathfrak{p}}$, of units of $\bar{O}_{\mathfrak{p}}$ is composed of elements of the form a/b , where $\underline{a}$ and $\underline{b}$ are both in $\bar{O}$, but neither $\underline{a}$ nor $\underline{b}$ is in $\underline{\mathfrak{p}}$. Therefore, $\mathfrak{p}' \cup U_{\mathfrak{p}} = \bar{O}_{\mathfrak{p}}$, $\mathfrak{p}' \cap U_{\mathfrak{p}} = \emptyset$, and $\mathfrak{p}'$ is a maximal, prime ideal of $\bar{O}$. It is noted first that $\bar{O}_{\mathfrak{p}}$ comprises the set of all elements of the form $\underline{hu}$ such that $\underline{h}$ is in $\bar{O}$ and $\underline{u}$ is in $U_{\mathfrak{p}}'$; secondly, if $\underline{a}$ is in $\bar{O}$, but $\underline{a}$ is not in $\mathfrak{p}$, then $\underline{a}$ is in $U_{\mathfrak{p}}$.

Let $\bar{O}_{\mathfrak{p}}(\underline{au})$ be any principal ideal of $\bar{O}_{\mathfrak{p}}$ ($\underline{a}$ in $\bar{O}$, $\underline{u}$ in U .) It is claimed that $\bar{O}_{\mathfrak{p}}(au) = (\bar{O}\,(a))U_{\mathfrak{p}}$. First, $(\bar{O}a)\ U_{\mathfrak{p}} \subseteq \bar{O}_{\mathfrak{p}}(\underline{au})$. On the other hand, $\bar{O}_{\mathfrak{p}}(au) \subseteq \bar{O}(a)U_{\mathfrak{p}}$, for if $\underline{bv}$ is in $\bar{O}_{\mathfrak{p}}$ ($\underline{b}$ in $\bar{O}$, $\underline{v}$ in U), then $(\underline{bv})^{o}(\underline{au})$ is a member of $\underline{ba}U_{\mathfrak{p}}$ and $\underline{ba}U_{\mathfrak{p}}$ $\bar{O}(a)U_{\mathfrak{p}}$.

Let $\bar{O}(a) \sim \underline{\mathfrak{p}}^{\alpha} \cdot \prod_{i=1}^{m} \mathfrak{p}_i^{\alpha_i}$ where the $[\underline{\mathfrak{p}}, \mathfrak{p}_1, \mathfrak{p}_2, --- \mathfrak{p}_m]$ are distinct members of $\mathfrak{M}$. Then $C^{o} \prod_{i=1}^{m} \mathfrak{p}_i^{\alpha_i} \cdot \underline{\mathfrak{p}}^{\alpha} \subseteq \bar{O}(a)$ where $\underline{C} \sim \bar{O}$ and $\underline{*C} = \prod_{i=1}^{m} q_i^{\beta_i}$; the $[q_i]\,{}^{i=m}_{i=1}$ are, of course, a set of ideals in $\bar{O}$, each of which properly contains a member of $\mathfrak{M}$. Since in each of the ideals, $[\mathfrak{p}_1, \mathfrak{p}_2, ---- \mathfrak{p}_m, q_1 -- q_m]$ there is an element in the respective ideal that is not in $\mathfrak{p}$, it follows (see remark at the end of the first paragraph of the proof) $\underline{\mathfrak{p}}^{\alpha} U_{\mathfrak{p}} \subseteq \bar{O}(a)U_{\mathfrak{p}}$. Consequently, $\underline{\mathfrak{p}}'^{\alpha} \subseteq \bar{O}(au)$. Conversely, by setting $\underline{D}\ \bar{O}(a) \subseteq \prod_{i=1}^{m} \mathfrak{p}_i^{\alpha_i} \cdot \mathfrak{p}^{\alpha}$ where $\underline{D} \sim \bar{O}$, it follows $\bar{O}_{\mathfrak{p}}(au) \subseteq \mathfrak{p}'^{\alpha}$. Thus $\bar{O}_{\mathfrak{p}}(au) = \mathfrak{p}'^{\alpha}$.

Now let A be any ideal of $\bar{O}$. Let $m = \min\limits_{x \text{ in } A} \left\{ \begin{array}{l} \underline{n} \text{ such that} \\ \mathfrak{p}'^{m} = \bar{O}(x) \end{array} \right\}$.

It follows A $= \mathfrak{p}'^{m}$.

Clearly $\mathfrak{p}'^{m+1} \subseteq \mathfrak{p}'^{m}$, n = 1,2.... Suppose $\mathfrak{p}'^{m+1} = \mathfrak{p}'^{m}$ for some positive integer n. Then $\underline{\mathfrak{p}}^{m} U_{\mathfrak{p}} \subseteq \underline{\mathfrak{p}}^{m+1} U_{\mathfrak{p}}$ and so $\mathfrak{p}^{-m} \mathfrak{p}^{m} U_{\mathfrak{p}} \subseteq \underline{\mathfrak{p}}^{-m} \underline{\mathfrak{p}}^{m+1} U_{\mathfrak{p}} \subseteq \underline{\mathfrak{p}}^{-m} \mathfrak{p}^{m} [\underline{\mathfrak{p}} U_{\mathfrak{p}}]$ $= \bar{\mathfrak{p}}^{m} \mathfrak{p}^{m} \mathfrak{p}' \subseteq \bar{O}_{\mathfrak{p}} \mathfrak{p}' = \mathfrak{p}'$. Now by (1) and (3) $\underline{\mathfrak{p}}^{-m} \underline{\mathfrak{p}}^{m}$ contains an element of $\bar{O}$ not in $\underline{\mathfrak{p}}$, whence $\mathfrak{p}^{-m} \mathfrak{p}^{m} U_{\mathfrak{p}} = \bar{O}_{\mathfrak{p}}$. Therefore, $\bar{O}_{\mathfrak{p}} \subseteq \mathfrak{p}'$, an impossibility. $\underline{\mathfrak{p}}'^{m+1} \subset \mathfrak{p}'^{m}$, n = 0, 1, 2, etc. Q. E. D.

(8) Let $\bar{O}$ be an integral domain with ascending chain conditions such that $\bar{O}$ is a proper subset of and is integrally closed in its quotient field $\underline{F}$. Then $\bar{O}$ is a finite, discrete principally ordered system with separation property.

Proof: By the first corollary to (6), the set $\mathfrak{M}$ of minimal primes of $\bar{O}$ is non-null. Let $\underline{\mathfrak{p}}$ be a member of $\mathfrak{M}$. For each $\underline{b}$ in $\bar{O}$* , define v(b) = x where $\underline{x}$ is the non-negative integer such that $\bar{O}_{\mathfrak{p}}(b) = \underline{\mathfrak{p}}'^{x}$. If $v_{\mathfrak{p}}$ (0) is defined to be ∞ , and if $\underline{v}$ is extended to $\underline{F}$, then by (7) $\underline{v}$ is a discrete (rank one) valuation on $\underline{F}$ and $\bar{O}_{v_{\mathfrak{p}}} = \bar{O}_{\mathfrak{p}}$.

Clearly $\bigcap_{\mathfrak{p} \varepsilon \mathfrak{M}} \bar{O}_{\mathfrak{p}} \supseteq \bar{O}$, and it is claimed that $\bigcap_{\mathfrak{p} \varepsilon \mathfrak{M}} \bar{O}_{\mathfrak{p}} = \bar{O}$. Suppose $\underline{a}$ is in $\bar{O}$ but that there is an $\underline{\mathfrak{p}}$ in $\mathfrak{M}$ such that $\underline{a}$ is not in $\bar{O}_{\mathfrak{p}}$. Then 1/a is in $\underline{p}$ (see second definition in previous Chapter II) and indeed, 1/a is in $\bar{O}_{\mathfrak{p}}$. There are elements $\underline{h}$ in $\underline{\mathfrak{p}}$, $\underline{u}$ and $\underline{v}$ in $\bar{O}$, neither $\underline{U}$ nor $\underline{v}$ in $\underline{\mathfrak{p}}$, such that 1/a = h($\underline{u}$/v). It follows u = avh is a member of $\bar{O}\underline{\mathfrak{p}} = \mathfrak{p}$, a contradiction.

Suppose $\underline{a}$ is in $\underline{O}^*$, $\underline{\mathfrak{p}} \varepsilon \mathfrak{M}$, and $v_{\mathfrak{p}}$ (a) > 0. Then $\bar{O}(a) U_{\mathfrak{p}} \subseteq \mathfrak{p} U_{\mathfrak{p}}$, and by the argument employed in the above paragraph, $\underline{a}$ is in $\underline{\mathfrak{p}}$. Then $\bar{O}(a) \subseteq \underline{\mathfrak{p}}$. By the first corollary to (4), then $\underline{v}_{\mathfrak{p}}(a) > 0$ for at most finitely many $\mathfrak{p} \varepsilon \mathfrak{M}$. $\bar{O}$ is thus a discrete, finite principally ordered system; since $\mathfrak{M}$ consists of minimal-prime ideals, $\bar{O}$ has the separation

Remarks: (Finite, discrete, principally ordered systems, necessarily satisfy the separation property). Actually, the last step of the above proof is unnecessary. It is true that any finite, discrete principally ordered system has the separation* property for a subset of its valuations. In other words, if $\bar{O}$ is a finite, discrete principally ordered system with valuations Φ', then a subset Φ of these valuations will satisfy the separation property, and can be chosen such that $\bar{O} = \bigcap_{v \in \Phi} \bar{O}_{v_P}$. The subset Φ of Φ' will consist of valuations

$$\left\{ v \text{ in } \Phi' \;\Big/ \begin{array}{l}\text{the set of elements in } \bar{O} \\ \text{such that } v(x) > 0 \text{ is a minimal prime ideal}\end{array} \right\}.$$

[5Krull, section 37.]

However, the method of II.2 may easily be used to show that a finite, discrete principally ordered system has the separation property. It is recalled that II.2 proved that if axioms I through IV' are valid for a set of valuations on the quotient field of $\bar{O}$, then axioms I to IV are valid on $\bar{O}$ for a subset of these valuations. In this proof axiom II' is not needed while axiom IV' is used only to imply axiom IV.

An alternative proof of statements (8) and (9) is obtained in the following way: Van derWaerden [12a, Van.derWaerden, line 18, p. 307; 12b, line 11, p. 301, line 31, p. 302] proves that each principal ideal in $\bar{O}$, is uniquely expressible as a product of powers of finitely many minimal prime ideals. Proceeding as in (I.15) the properties for the non-null set of valuations are readily obtained.

The concept of equivalence, defined for ideals in $\bar{O}$, is readily extended to apply to all $\bar{O}$-ideals. The classes of equivalent $\bar{O}$-ideals form a group under ideal multiplication. If $\mathcal{Q}$ and $\mathcal{B}$ are each classes of equivalent $\bar{O}$-ideals, the product of the classes, $\mathcal{Q} \circ \mathcal{B}$, is the uniquely determined class $\left\{ \chi / \underset{\chi = AB}{\exists A \varepsilon \mathfrak{A}}, B \varepsilon \mathfrak{B} \ni \right\}$. Under this definition of class multiplication, the classes of ideals form a group. If the system $\bar{0}$ is such that each of the prime ideals $\{\mathfrak{P}(v_p\}_{p \varepsilon \mathfrak{M}}$ are maximal prime ideals, then the $\bar{0}$-ideals A and B are equivalent if and only if A = B. Therefore, the finite, discrete principally ordered system $\bar{0}$ with separation property is a Dedikind ring providing that each prime ideal is maximal; indeed, the system is a Dedikind ring if and only if prime ideals are maximal [11Schilling, Ch. IV, sec. 1,2,3] (see II.7). Statement (9) proves this result using arguments on valuations.

First, however, the question arises, is the converse to statement (8) valid? If the integral domain $\bar{0}$ is a finite, discrete principally ordered system, does the ascending chain condition hold in $\bar{0}$? Is $\bar{0}$ integrally closed in its quotient field, $\underline{F}$? As indicated, in the beginning of the chapter, $\bar{0}$ will be integrally closed in $\underline{F}$. However, $\bar{0}$ need not satisfy the ascending chain condition as (Chapter 5, sec.5) shows. If the ascending chain condition did necessarily hold in $\bar{0}$, the proof of (9) would, of course, be superfluous.

(9) Hypothesis: $\bar{0}$ is a finite, discrete principally ordered system in which the valuations satisfy the separation property. Each prime ideal in $\bar{0}$ is a maximal ideal.

Conclusion: $\bar{0}$ is a Dedikind ring with valuations $\mathfrak{M}$.

Proof: Axiom IV must be verified to show $\bar{0}$ is a Dedikind ring. It will be shown that if there is an ideal $\underline{A}$ in $\bar{0}$ such that $\underline{A} \subset \bar{0}$ and v(a) = 0 for all v in $\mathfrak{M}$, then there are prime ideals $\mathfrak{P}$, $\mathfrak{q}$ in $\bar{0}$ such that $\mathfrak{P} \subset \mathfrak{q}$.

Suppose $A \subset \bar{0}$ and $v(A) = \mathfrak{M}$ for all v in $\mathfrak{M}$. Then there is a maximal, prime ideal N such that $A \subseteq N \subset \overline{0}$. (Refer to "Hausdorf Maximality Principle," appendix I.4.) Then $0 = v(A) \geq v(N) \geq 0$ and so $v(N) = 0$ for all v in Φ. Let a̲ be a non-unit element of N̲ and let $v_1, v_2, \ldots\ldots\ldots v_n$ comprise the set of all valuations in Φ which do not vanish on a̲. Let $\mathfrak{p}_i = P(V_i)$, $1 \leq i \leq n$, let $v_i(a) = e_i > 0$, $1 \leq i \leq n$. Now $v(\overline{0}_a{}^{-1} 0 \prod \mathfrak{p}_i{}^{e_i}) =$ 0 for all v in Φ whence $\overline{0}a^{-1} 0 \prod_{i=1}^{m} \mathfrak{p}_i^{e_i} \subseteq \overline{0}$. By (II.2d), $\prod_{i=1}^{m} \mathfrak{p}_i{}^{e_i} = \overline{0}a^{0}(\overline{0}a^{-1}0 \prod_{i=1}^{m} \mathfrak{p}_i{}^{e_i}) \subseteq \overline{0}a \subset N$. Therefore, by (1), $\mathfrak{p}_i \subset N$ for $1 = 1, 2,$ or.....n.

Remark: Statements (8) and (9) offer a proof showing directly that the conditions (a) $\overline{0}$ is integrally closed in F̲; (b) ascending chain conditions hold in $\overline{0}$; and (c) maximality of prime ideals together guarantee that there are valuations Φ on $\overline{0}$ satisfying I-IV.

Terms of Chapter III

Coefficient . . . . App. III.1
Degree . . . . App. III.1
Direct summand . . . . App. II.2
Equation . . . . App. III.1
Equivalence classes . . . . App. I.5
Equivalence relation . . . . App. I.5
Hausdorf Maximality principle . . . . App. I.4
Non-trivial equation . . . . App. II.8
Radical . . . . App. II.5
Root . . . . App. III.1

Notations

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{vmatrix}$$ ______________________ App. II.8

$\emptyset$ ______________________ App. I.1

$\bigcup_{i\in I} A_i$ ______________________ App. I.1

CHAPTER IV

ALGEBRAIC EXTENSIONS

The reader is especially advised to refer to the appendices as well as to the other references that occur in this chapter. (IV.1, IV.2, and III.1 through III.7)

Question under consideration: Let $\bar{O}$ be a Dedikind ring with valuations $\mathbb{O}$. Let K be finite algebraic extension of F. Is K the quotient field of a Dedikind ring? If so, what is the nature of such a ring and what is the nature of the valuations on the ring?

Throughout this chapter, $\bar{O}$, F, K and $\mathbb{O}$ refer to the sets indicated above.

Notation: Let $G \leq H$ and let $\underline{v}$ be a valuation on the field H. The mapping of H onto the rational integers (with ∞ added) may be restricted to a mapping of G into the rational integers (with ∞ added). The restricted mapping is denoted by v/g; if a is in G, v/G(a) = v(a).

Definition: (prolongation of a valuation) Let u and v be valuations defined on K and F respectively. If u/F = v, then $\underline{u}$ is said to be a prolongation of $\underline{v}$ from F to K; if $\underline{u}$ is discrete (rank one), then $\underline{u}$ is said to be a discrete (rank one) prolongation.

(1) For each v in $\mathbb{O}$ there is at least one discrete (rank one) prolongation of $\underline{V}$ from F to K.

Preliminary remark: If w is a valuation on a field and w(a) >w(b), then w(a + b) = w(b). This statement, analogous to (I.1), is proved exactly the same argument.

Proof: First assume that K is a simple extension of F, say K = F [a]. Let Ω be the completion of F with respect to v (refer app.

IV.1). Let the defining equation for a over F be f(x) = 0 and let f(x) be represented as a product of monic, irreducible polynomials in $\Omega(x)$ as $\prod_{i=1}^{m} f_i(x)$ (refer to app. III.2, para. 4). Then a is a root of one of the monic, irreducible polynomials, $\left[f_i(x)\right]_{i=1}^{i=n}$ (otherwise $f(a) \neq 0$) and, indeed, suppose a is a root of $f_j(x)$. If $f_j(x) = \sum_{i=0}^{m-1} a_i x^i$, $[a_i]_{i=1}^{m} \in \Omega$, then the field $\Omega[a]$ is a finite algebraic extension of Ω with a basis of m elements. Each element of K (K = F[a]) is also an element of $\Omega[a]$. Let w be the restriction to K of the valuation N_Ω defined on the field $\Omega[a]$. Since N_Ω coincides with v on F (refer to app. (IV.1) and IV.2), w is a prolongation of V.

Since any algebraic extension K of F can be obtained as the result of finitely many successive simple extensions (app. II.2, last paragraph) a prolongation of the valuation v to K is obtained by successively prolonging v to simple extensions.

If K has a basis over F consisting of n elements, then each a in K is the root of an equation in F(x) of degree $m \leq n$. (Refer to app. II.2) Let $f(a) = a_0 a^m + a_1 a^{m-1} = \ldots \ldots a_{m-1} a + a_m = 0$. Then $w(a_i a^{m-1}) = w(a_j a^{m-j})$ for some $i \neq j$ since otherwise $w(f(a)) = \min_{1 \leq i \leq n} \{w(a_i a^{m-i})\} \neq \infty$. Let $w(a_s a^{m-a}) = w(a_r a^{m-r})$, $s > r$. Then $w(a^{s-r}) = w(a_s/a_r) = v(a_s/a_r) = b$ where b is a rational integer. Thus $w(a) = b/(s-r) = bc/N$ where c is a rational integer and $N = 1^\circ 2^\circ 3 \ldots\ldots {}^\circ N$. If v maps F^* onto the set of rational integers U, then w maps K^* onto a subset of the set $x = y/N$, y in U.

<u>Example</u>: Let v be a valuation of F which is a mapping onto the integers, ...$-3, -2, -1, 0, 1, 2,$...... . Let K be an algebraic extension with a basis of two elements over F. Then the extension w of v is a mapping of K^+ onto a subset of the rational numbers whose denomina-

tors are two: $\{\ldots .-5/2,-2,-3/2,-1,-1/2,0,+1/2,+1,\ldots \ldots\}$

(2) If K is a purely separable extension of F then each v in Φ has one and only one prolongation from F to K (see app. III.4).

<u>Proof</u>: By (1) the valuation v in Φ has at least one prolongation to K. Let v' be any prolongation of v from F to K. Each element <u>a</u> in K is the root of an equation $x^n - b = 0$ for an appropriate positive integer n and an appropriate element b in F (refer app. III.4). Thus $v'(a^n-b) =$ and so $v'(a^n) = v'(b) = v(b)$. Then v'(a) must be equal to v(b)/n.

<u>Definition</u>: <u>conjugate</u> <u>prolongation</u>. Let K' and M be respectively a least normal closure of K and a maximal separable subfield determined by K (app. III.6). Let w' be a prolongation of the valuation v from F to K'. Then for σ in $\mathcal{G}_F^M$ (app. III.5), and an a in M, $w'_\sigma(a)$ is defined as $w'(\sigma a)$. For a in K' but not in M $w'_\sigma(a)$ is set equal to the unique prolongation of the valuation w'_σ from M to K' (refer to statement 2 above). The prolongations w' and w of v are then said to be conjugate valuations on K'.

Finally, any pair of prolongations w and w_1 of v from F to K are defined to be conjugates if they are valuations w' and w_1' on K' such that $w'/K = w$, $w_1/K = w_1$, and such that w and w_1 are conjugate on K'. The notation W_σ is used to inducate a conjugate w_1 of w on K. The σ is here presumed to be the element in $\mathcal{G}_F^M$ such that $w_1(a) = w'(\sigma a)$ for all a in M where w' is the valuation on K' such that $w'/K = w$.

In case K is normal extension of F then valuations w_1 and w_2 are conjugate if and only if there is a σ in $\mathcal{G}_F^K$ such that $w_1(a) = w_2(\sigma a)$ for all a in K.

Actually any prolongation of the valuation v from F to K is, in a certain sense, equivalent to a member of a set of mutually conjugate prolongations. This is proved in (6).

Notation (for integral dependence): Let K be a field containing the ring with identity element R. The set of elements of K that are integrally dependent on R is denoted by $I[K]_R$

(3) Hypothesis: $v \varepsilon \mathbb{D}$. $[W_i]_{i=1}^{i=m}$ is a set of prolongations of v from F to K and w is in this set; moreover, any prolongation conjugate to w on K is in this set.

Conclusion: $I[K]_{\bar{O}_v} = \bigcap_{i=1}^{m} \bar{O}_{w_i} = \bigcap_{\sigma \varepsilon \mathcal{G}_F^M} \bar{O}_{w_\sigma}$.

Proof: Let K' and M be as indicated in the above definition. By the definition of conjugate prolongations on K, there is a set of valuations on K' which consists of respective prolongations of the w_i from K to K' and which includes for each σ in $\mathcal{G}_F^M$ (including $\sigma = I$, the identity of $\mathcal{G}_F^M$), the valuation w_σ on K'. As a notational convenience, this set of valuations on K' is also denoted by $[w_i]$.

$$\text{(a) } I[M]_{\bar{O}_v} = \bigcap_{i=1}^{m}(\bar{O}(w_i) \cap M) = \bigcap_{i=1}^{m}(\bar{O}(w_i) \cap M).$$

Proof of (a): Let b be in the $I[M]_{\bar{O}_v}$, and let b be a root of the monic polynomial (app. III.1) $x^m + a_1x^{m-1} + - - - - - - - + a_n$ in which the $[a_i]_{i-1}^{i=m}$ are elements in $\bar{O}$. Then $w_j(a_i) = v(a_i) \quad 0, 1 \leq i \leq m$, $1 \leq j \leq m$. Suppose $w_j(b) < 0$ for some subscript j. Then $w_j(b)^m <$ $w_j(a_i b^{m-i})$, $1 \leq i \leq m$ and so $w_j(b^m + a_1 b^{m-1} + \ldots\ldots a_n) = w_j(b^m) \neq \infty$. Therefore, $w_j(b) \geq 0$, $1 \leq j \leq n$. $I[M]_{\bar{O}_v} \leq \bigcap_{i=1}^{m}(\bar{O}(w_i) \cap M)$.

Let $\underline{c} \; \varepsilon \bigcap_{i=1}^{m}(\bar{O}_{w_i} \cap M)$. Then $\underline{c}$ is in M, and the defining equation for $\underline{c}$ is $f(c) = \prod_{i=1}^{m} (x - \sigma_{i_j} m) = 0$ where the $[\sigma_{i_j}]_{j=1}^{j=m}$ are a subset of the $[\sigma_i]_{i=1}^{i=n}$ (app. III.7). Let the coefficients of f(x) be denoted by $[a_i]_{i=1}^{i=k}$. Since $w(\sigma_{i_j} c) = w_{\sigma_{i_j}}(c) \geq 0$, $1 \leq i \leq m$, it follows $w(a_i) =$

$v(a_i) \geq 0$, $1 \leq i \leq k$, since the $\left[a_i\right]_{i=1}^{i=k}$ are the symmetric functions of the $\left[\sigma_j c\right]_{j=1}^{j=m}$. (App. III.7.) The element c is, therefore, in $I[M]_{\bar{O}_v}$. It follows $\bigcap_{i=1}^{m} (\bar{O}(w_i) \cap M) \subseteq \bigcap_{\sigma \varepsilon \mathcal{G}_F^M} (\bar{O}_{w_\sigma} \cap M) \subseteq I[M]_{\bar{O}_v} \subseteq \bigcap_{i=1}^{m} (\bar{O}_{w_i} \cap M)$, and (a) is proved. (Refer to App. III.5.)

(b) Let $a \epsilon K$ and $b \varepsilon M$, and suppose that a is an n^{th} root of b for some positive integer n. Then a is in $I[K]_{\bar{O}_v}$ if and only if b is in $I[K]_{\bar{O}_v}$.

Proof of (b): Assume b is in $I[K]_{\bar{O}_v}$ with a monic equation $f(b) = b^m + a_1 b^{m-1} + \ldots\ldots + a_n = 0$, in which $[a_1, a_2, \ldots . a_n]$ are members of $\bar{O}$. Let $g(x) = f(x^n)$. Then $g(a) = f(b) = 0$. All of the coefficients of $g(x)$ are in $\bar{O}_v$ and the coefficients of the leading term, x^{mn}, is one. Therefore, a is in $I[K]_{\bar{O}_v}$.

Suppose a is in $\mathbb{O}[K]_{\bar{O}_v}$.. Then $a^n = b$ is in the ring $I[K]_{\bar{O}_v}$. (Refer to app. III.1.)

Returning to the proof of (3), if a is in K' but a is not in M then a is the root of a polynomial $x^{p^n} - b = 0$ in which b M and p^n is a power of positive prime integer; if a is in K as well as in K', then b is in $M \cap K$. According to (2) the only prolongation, w_i', of the valuation $w_i / M \cap K$ from M K to K is such that $w_i'(a) = w_i(b)/p^n$. Thus, $w_i'(a) \geq 0$ if and only if $w_i(b) \geq 0$. Therefore, if $a \varepsilon K$, then a is in $\bigcap_{i=1}^{m} \bar{O}(w_i)$ if and only if b is in $\bigcap_{i=1}^{m} (\bar{O}w_i \cap M)$. Again, since the prolongation to K of the valuation $w_\sigma / M \cap K$, where $\sigma \varepsilon \mathcal{G}_F^M$, is unique, it follows that a is in $\bigcap_{\sigma \varepsilon \mathcal{G}_F^M} \bar{O}_{w_\sigma}$ if and only if b is in $\bigcap_{\sigma \varepsilon \mathcal{G}_F^M} (\bar{O}_{w_\sigma} \cap M)$. By (b) a is in $I[K]_{\bar{O}_v}$ if and only if b is in $I[M]_{\bar{O}_v}$. These three underlined statements, together with (a) above, complete the proof of (3).

Definition (equivalent, inequivalent prolongations): If w_1 and

w_2 are prolongations of a valuation from F to K, then w_1 and w_2 are said to be equivalent valuations (or prolongations) if $w_1(x) \geq 0$ implies that $w_2(x) \geq 0$ and $w_2(x) \geq 0$ implies that $w_1(x) \geq 0$ whenever x is in K. If this condition does not hold for all x in K then w_1 and w_2 are said to be inequivalent. The set $[w_i]_{i=1}^{i=n}$ of prolongations of v to K is said to be inequivalent if each distinct pair from the set are inequivalent.

(4) Let $[w_i\ {}_{i=1}^{i=n}$ be a set of prolongations of the valuation v form F to K such that any w_{j_σ}, $1 \leq j \leq n$, $\sigma \in \mathcal{G}_F^M$, is equivalent to at least one of the w_i, $1 \leq i \leq n$. Let $[W_i]_{i=1}^{i=m}$ be a set of prolongations of v which includes all of the $[w_i]_{i=1}^{i=n}$. It then follows $\bigcap_{i=1}^{n} \bar{O}_{w_i} = \bigcap_{i=1}^{m} \bar{O}_{w_i} = I[K]_{\bar{O}_v}$.

<u>Proof</u>: The proof follows by (3) and the definition of equivalent valuations.

(5) <u>Hypothesis</u>: $[w_i]_{i=1}^{i=n}$ are a set of inequivalent, discrete prolongations of the valuation <u>v</u> from F to K.

<u>Conclusion</u>: If $[a_i]_{i=1}^{i=n}$ is a set of elements of K, and if M is a positive integer, there then exists <u>z</u> in K such that $w_i(z-a_i) > M$, $1 \leq i \leq n$.

(a) Under the above hypothesis, for each pair of distinct w_i and w_j, $i \neq j$, there exists an element x in K such that $w_i(x) > 0$, and $w_j(x) < 0$; there exists y in <u>K</u> such that $w_1(y) > 0$ and $w_2(y) < 0$.

<u>Proof</u>: If w_i and w_j are inequivalent, then either there exists a in K such that $w_1(a) \geq 0$ and $w_2(a) < 0$ or there exists b in K such that $w_1(b) < 0$ and $w_2(b) \geq 0$. Suppose that the first possibility is true, and in fact, suppose that $w_1(a) = 0$. There exists c in F such that $v(c) > 0$. Then $w_1(c) = w_2(c) = v(c) > 0$. For sufficiently large n, $w_1(a^n c) > 0$, $w_2(a^n c) < 0$. The required elements are <u>$a^n c$</u> and <u>$1/a^n c$</u> respectively.

(b) Under the hypothesis of (5) there exists <u>x</u> in K such that

$w_1(x) < 0$, $w_2(x) > 0$, $w_3(x) > 0 \ldots\ldots w_{n-1}(x) > 0$, and $w_n(x) > 0$.

Proof: The following statement is logically equivalent to the statement to be proved: There exists y in K such that $w_1(y) > 0$, $w_2(y) < 0$, $w_3(y) < 0 \ldots\ldots w_{n-1}(y) < 0$, $w_n(y) < 0$. If z satisfies one of the conditions, then 1/z satisfies the other.

Statement (a) proves (b) for a case in which the $\left[w_i\right]_{i=1}^{i=n}$ consist of but two valuations. Inductively assume the equivalent statement is valid for any set of n-1 valuations. Let c be an element of K such that $w_1(c) > 0$, $w_2(c) < 0$, $w_3(c) < 0 \ldots\ldots w_{n-1}(c) < 0$. It may be assumed $w_n(c) \geq 0$. Let d be an element of K such that $w_1(d) > 0$, $w_n(d) < 0$, and let s be a positive integer such that abs.[1] $w_2(c^s) >$ abs. $w_i(d)$, $z \leq i \leq n$. Then w_1 $(c + d^s) > 0$ and $w_i(c + d^s) < 0$, $i = 2, 3, \ldots\ldots$ or m. (1. Abs. is a notation for absolute value.)

(c) Let M be a positive integer. Under the hypothesis of (5) there is an element z in K such that $w_1(y-1) > M$, $w_2(y) > M$, $w_3(y) > M \ldots\ldots$ $w_n(y) > M$.

Proof: By (b) there exists a in K such that $w_1(a) > 0$, $w_i(a) < 0$, $2 \leq i \leq n$. Let s be a positive integer. It follows $w_i(a^s/1 + a^s) = w_i$ $(1 + a^s) - w_i(1 + a^s) = w_i(a^s)$, $2 \leq i \leq n$. Also, $w_1(\frac{a^s}{1 + a^s} - 1) = w_1$ $(-1/1 + a^s) = -w_1(a^s)$. Hence $z = a^s/(1+a^s)$ is the required element for s sufficiently large.

Proof of (5): By (c) for each K, $1 \leq k \leq n$, there exists x_k in K such that $w_k(x_k - 1)$ M and $w_2(x_k) > M$, $1 \leq i \leq n$, $i \neq k$. As in (II.8) this result suffices to guarantee that each Chinese Remainder equation has a solution.

(6) Let $\left[w_1 \ldots\ldots w_n\right]$ be inequivalent discrete (rank one) prolongations of the valuation v from F to K. Let $\bar{O}_i$ designate the valuation ring

$\bar{O}_{w_i}$ and let $\bar{O}'$ designate the ring $\bigcap_{i=1}^{n} \bar{O}_i$. It follows there are exactly n prime ideals in $\bar{O}'$.

(a) Under the hypothesis (6) each ideal A of $\bar{O}'$ is equal to the set $\bigcap_{i=1}^{n} A_i$ in which A_i is an ideal of O_i and $A_i = O_iA$, $1 \le i \le n$; (b) conversely, each set $[A_i]_{i=1}^{i=n}$ in which A_i is an ideal of $\bar{O}_i$, $1 \le i \le n$, is such that $A = \bigcap_{i=1}^{n} A_i$ is an ideal of $\bar{O}'$ and $A_i = \bar{O}_iA$, $1 \le i \le n$.

Proof of a: Let A be an ideal of $\bar{O}'$. Clearly $\bar{O}_iA$ is an ideal of $\bar{O}_i$, $1 \le i \le n$, and $A \subseteq \bigcap_{i=1}^{n} \bar{O}_i{}^{o}A$. Suppose a is a member of $\bigcap_{i=1}^{n} \bar{O}i^{o}A$. For fixed i, $1 \le i \le n$, there exists a_i in A such that $w_i(a) = w_i(a_i)$ because of the following argument: Let $a = \sum_{j=1}^{m} a_j{}'b_j$ where $a_j{}'$ is in A, b_j is in $\bar{O}_j$, $1 \le j \le m$. Since it is impossible that $w_i(a_j{}') > w_i(a)$ for all j, $1 \le j \le m$, a subscript k may be chosen such that $w_i(a_k{}') \le w_i(a)$. Then $w_i(a_i{}''a_k{}') = w_i(a)$ and $a_i{}''a_k{}'$ is in A providing that $a_i{}''$ is chosen to be an element of $\bar{O}'$ such that $w_i(a_i{}'') = w_i(a) - w_i(a_k{}')$.

Let M equal $\max_{i=1,n}\{w_i(a)\}$. By (5c) there is a set of elements in K, $[c_i]_{i=1}^{i=n}$ such that $w_j(c_i) > M$ for $i \neq j$ and such that $w_i(c_i-1) > M$. Therefore, $w_i(c_i) = 0$ and $w_i(a_ic_i) = w_i(a)$; for $i \neq j$, $w_i(a_jc_j) \ge w_i(c_j) > M \ge w_i(a) \ge 0$. Let $d = \sum_{i=1}^{m} a_ic_i$. It follows d is in A and $w_i(d) = w_i(a)$, $1 \le i \le n$. Hence, d/a is an element of $\bar{O}'$, and a = (a/d) d is in A.

Proof of (b): Let $[A_i]_{i=1}^{i=n}$ be such that A_i is an ideal of $\bar{O}_i$, $1 \le i \le n$. Define $A' = \bigcap_{i=1}^{n} A_i$. Then A' is an ideal of $\bar{O}'$ and $\bar{O}_i{}^{o}A' \subseteq A_i$, $1 \le i \le n$. Consider any set of elements $[a_i]_{i=1}^{i=n}$ such that a_i is in A_i, $1 \le i \le n$. Define $M = \max_{1 \le i \le n}\{w_i(a_i)\}$. By (5) there is an element of K, a, such that $w_i(a-a_i) > M$, $1 \le i \le n$. It follows $w_i(a) = w_i(a_i)$ and so a is a multiple of a_i in the ring $\bar{O}_i$. Thus a is in $\bigcap_{i=1}^{n} A_i = A'$. Let k be a fixed subscript, $1 \le k \le n$. The element a_k is equal to (a_k/a) a, and therefore is in $A'\bar{O}_k$. $A'\bar{O}_k = A_k$, $1 \leq k \leq n$.

(c) Under the hypothesis of (6), for any rational number $\underline{r} > 0$, there exists a_k in $\bar{O}'$ such that $w_k(a_k) > r$ and $w_i(a_k) = 0$ for $1 \leq i \leq n$, $i \neq k$.

Proof: There is a set of elements in $\bar{O}$, $[b_i]_{i=1}^{i=n}$, such that $w_i(b_i) = 0$, $1 \leq i \leq n$, $i \neq k$, and $w_k(b_k) > r$. By (5) there exists a_k in K such that $w_i(a_k - b_i) > r$, $1 \leq i \leq n$. H follows $w_i(a_k) = 0$, $i \neq k$; $w_k(a_k) > r$. A_k is on $\bar{O}'$.

Proof of Theorem: Each of the valuation rings $\bar{O}_i$ has one and only one prime ideal, $\mathfrak{p}_i$. ($\mathfrak{p}_i$ consists of elements having non-zero value; see I.12) By statements (a) and (b) there is a one-to-one correspondence between ideals, A, in $\bar{O}'$ and sets $[A_i]_{i=1}^{i=n}$ of ideals in the respective $\bar{O}_i$, $1 \leq i \leq n$; the correspondence is such that whenever A and $[A_i]_{i=1}^{i=n}$ correspond, then $A = \bar{O}_i \circ A_i$. Denote by $[\mathfrak{q}_j]_{j=1}^{j=n}$ the ideals of $\bar{O}'$ such that $A_j\bar{O}_j = \mathfrak{p}_j$ for one subscript j and $A_i\bar{O}_i = \bar{O}_i$ for all the other n-1 subscripts, i. The $[\mathfrak{q}_j]_{j=1}^{j=n}$ are easily shown to be prime ideals; by (c) the $[\mathfrak{q}_j]_{j=1}^{j=n}$ must be distinct prime ideals. To complete the proof of (6) it must be shown that if the ideal A is not equal to $\mathfrak{q}_1$, $\mathfrak{q}_2$, ...or $\mathfrak{q}_n$, then A cannot be a prime ideal of $\bar{O}'$.

Suppose $A \subset \bar{O}$ and $A = \bigcap_{i=1}^{n} A_i\bar{O}_i$. Since $A \neq \mathfrak{q}_1$, $\mathfrak{q}_2$, ...or $\mathfrak{q}_n$ it follows then that either (i) $A_k\bar{O}'_k \subseteq \mathfrak{p}_k$ and $A_m\bar{O}_m \subseteq \mathfrak{p}_m$ for at least two distinct subscripts k and m or else (ii) $A_kO_k \subset \mathfrak{p}_k$ for some k and $A_i\bar{O}_i = \bar{O}_i$ for $i \neq k$. In case (i) by (c) there exists $\underline{a}$ in $\bar{O}'$ such that $w_i(a) = 0$ for $i \neq k$, $w_k(a) = w_k(A_k \circ \bar{O}_k)$; there exists $\underline{b}$ in $\bar{O}'$ such that $w_i(b) = 0$ for $i \neq m$, $w_m(b) = w_m(A_m \circ \bar{O}_m)$. It then follows that a is not in A and b is not in A but that $\underline{ab}$ is in A unless $A_iO_i \subseteq \mathfrak{p}_i$ for values of i distinct from k and m. In any case of type (i), however, repeated application of (c) yields a finite set of elements of $\bar{O}$; none of which is in A, but whose product is A. In case (i), the element $\underline{a}$ (above) is not in A, but a^n is in A for n sufficiently large.

(7) <u>Hypothesis</u>: v is in $\mathfrak{D}$, w is a prolongation of v from F to K.

<u>Conclusion</u>: Any prolongation of v from F to K is equivalent to a prolongation conjugate to w.

<u>Proof</u>: The relationship $w_1 \sim w_2$ (the prolongation w_1 of v is equivalent to the prolongation w_2) is an equivalence relation. (Refer: "Galois Group," app. III, Section 5; "Equivalence Rel.", app. I, Section 5.) Let m be an integer equal to the number of equivalence classes for the set . Let $\{w_1, \ldots\ldots w_m\}$ be a set consisting of one member from each of the m classes. Then $w_1, \ldots\ldots w_m$ is a set of inequivalent prolongations of the valuation v.

Suppose that there actually is a prolongation, w' of v from F to K such that $w' \sim w_\sigma$ is false for all $\sigma \in \mathcal{G}^M_F$. Then $w', w_1, \ldots\ldots w_n$ is a set of inequivalent prolongations of v. Since by (1) every prolongation of v is discrete (rank one), it follows by (6) that there are $\underline{m+1}$ and $\underline{m}$ prime ideals in the respective rings, $\left(\bigcap_{i=1}^{m} \bar{O}_{w_i}\right) \cap \bar{O}_{w'}$ and $\bigcap_{i=1}^{m} \bar{O}_{w_i}$. This is impossible, since by (4) $\bigcap_{i=1}^{m} (\bar{O}_{w_i}) \cap \bar{O}_{w'} = \bigcap_{i=1}^{m} (\bar{O}_{w_i})$.

The question proposed at the beginning of the chapter can now be answered. K is the quotient field of a Dedikind ring $\bar{O}_K$. $\bar{O}_K$ will coincide with the set $I[K]_{\bar{O}}$ of elements in K that are integrally dependent on $\bar{O}$. The valuations $\mathfrak{D}$ on K or on $\bar{O}_K$ arise in the following way:

For each v in $\mathfrak{D}$ let $w^v{}_1$ be the prolongation of v from F to K defined as in (1). In other words, if a is in K, then $w^v{}_1(a)$ is the norm of $\underline{a}$ with respect to the field $\Omega[a]$ over the field Ω. As in (7), a set of inequivalent prolongations is chosen from the equivalence classes which together comprise all prolongations conjugate to $w^v{}_1$. Let $\left[w^v{}_1, w^v{}_2, \ldots\ldots w^v{}_{n_v}\right]$ denote such a set; let Φ' denote the set $\left[w^v{}_i\right]^{i=n_v}_{\substack{i=1 \\ v \text{ in } \Phi}}$; and finally, let $\bar{O}_K$ denote the subset of K, $\bigcap_{w^v_i \in \Phi'} \bar{O}_{w^v_i}$.

(8) Conclusion: $\bar{O}_K$ is a Dedikind ring with valuations Φ'; $I[K]_{\bar{O}} = \bar{O}_K$; and K is the quotient field of $\bar{O}_K$.

(a) If a is in $\bar{O}_K$ then $w^v{}_1(a) \neq$ for at most finitely many $w^v{}_i$ in Φ.

Proof: If a is in $\bar{O}$, clearly $w^v{}_i(a) \neq 0$ for at most finitely many $w^v{}_i$ in Φ'; indeed, if a is in F, then $w^v{}_i(a) \neq 0$ for at most finitely many $w^v{}_i$ in Φ'.

Consider an element b in $\bar{O}_K$ which is not in $\bar{O}$. Let b be a root of $f(x) = 0$ where $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots\ldots + a_1 x + a_0$. (Refer: "Equations" in app. III, Sec. 2, paragraph 2.) It will be shown that $w^v_i(b)$ only i $w^v_i(a_j) \neq 0$ for some a_j, $1 \leq i \leq j$, whence $w^v{}_i\ (b) > 0$ is possible only for $w^v{}_i$ in the finite set $\bigcup_{j=1}^{j=m} \{ W^v_i \text{ is in } \Phi'; W^v_i(a_j) \neq 0 \}$

Suppose, then, to the contrary, that for some w in Φ' $w(b) > 0$ but $w(a_i) = 0$, $1 \leq i \leq m$. Then $w(f(^b)) = w(a_m b^m + a_{m-1}b^{m-1} + a_{m-2}b^{m-2} + \ldots\ldots a_0) = w(a_0) \neq \infty$, a contradiction.

(b) If w_1 and w_2 are distinct members of Φ', then there exists x in $\bar{O}_K$ such that $w_1(x) > 0$ and $w_2(x) = 0$.

Proof: The required element x is in $\bar{O}$ itself if w_1 and w_2 are prolongations of different members of Φ. Suppose, then, that w_1 and w_2 are respectively $w^v{}_i$ and $w^v{}_j$ for some v in Φ, $i \neq j$, where $\left[w^v{}_i, \ldots\ldots w^v{}_{n_v}\right]$ is the complete set of prolongations of v that are members of Φ'. By (5b) there exists b in K such that $w^v{}_i(b) < 0$, and such that $w^v{}_k(b) > 0$,

$1 \leq k \leq n_v$, $k \neq i$. Also, by (1), there exists c in $\bar{O}$ and there exists a positive integer m such that $w^v{}_i(b^m c) = 0$, and $w^v{}_k(b^m c) > 0$ for all $k \neq i$, $1 \leq k \leq n_v$, ______ in particular for $k = j$.

According to (a) let all negative values of $b^m c$ be included in the set $[W_1^{v_1}, W_2^{v_1}, \text{------} W_{n_1}^{v_1}, W_2^{v_2}, \text{------------} W_1^{v_n} \text{---} W_{n_n}^{v_n}]$. By (I,2b) there is an element d in $\bar{O}$ such that $v_i(d) > 0$, $1 \leq i \leq n$ and such that $v(d) = 0$. It follows $w_j{}^{vi}(b^m cd^n) \geq 0$ for sufficiently large n, $1 \leq i \leq r$, $1 \leq j \leq n_{v_i}$. Therefore, $w(b^m cd^n) \geq 0$ for all w in $\mathfrak{W}$; moreover, $w^v{}_i(b^m cd^n) = 0$ and $w^v{}_j(b^m cd^n) > 0$.

(c) In $\bar{O}_K$ each prime ideal is maximal.

Proof: Let $\mathfrak{p}$ be prime ideal of $\bar{O}_K$ and let A be an ideal of $\bar{O}_K$ that properly contains $\mathfrak{p}$. Then $\mathfrak{p} \cap \bar{O}$ must contain a non-zero element of $\bar{O}$. Let $a \in \mathfrak{p}$, $a \neq 0$, and let $f(a) = 0$ be the defining equation for a. If $f(x) = x^m + a_{n-1}x^{m-1} + \ldots\ldots + a_0$, then $a_0 \neq 0$. (Otherwise text, is reducible; see app. III.2.), and a_0 is in $\mathfrak{p} \cap \bar{O}$. Thus $\mathfrak{p} \cap \bar{O}$ is a prime ideal in $\bar{O}$, and $\mathfrak{p} \cap \bar{O} \subseteq A \cap \bar{O}$. If $\mathfrak{p} \cap \bar{O} \subset A \cap \bar{O}$, then by (I,8) and (I,12) $A \cap \bar{O} = \bar{O}$ whence A contains the identity element. In this case $A = \bar{O}_K$.

In the following way it is shown that $\mathfrak{p} \cap \bar{O} \subset A \cap \bar{O}$: Let $\underline{h}$ be an element of A not in $\mathfrak{p}$. Let $f(h) = 0$ be the defining equation for $\underline{h}$ and let $f(h) = b_m h^m + b_{m-1}h^{m-1} + \ldots\ldots + b_0$. Then b_0 is in $A \cap \bar{O}$; it may be assumed that b_0 is also in $\mathfrak{p} \cap \bar{O}$. Thus, $b_m h^m + b_{m-1}h^{m-1} + \ldots\ldots b_1 h$ is in $\mathfrak{p} \cap \bar{O}$, and since h is not in $\mathfrak{p} \cap \bar{O}$, $b_m h^{m-1} + b_{m-1}h^{m-2} + \ldots\ldots + b_1$ is a member of $\mathfrak{p} \cap \bar{O} \subseteq A \cap \bar{O}$. Then, b_1 is in $A \cap \bar{O}$, and, as previously, it may be assumed that b_1 is in $\mathfrak{p} \cap \bar{O}$. However, if this argument is successively repeated, after a certain number of steps m, $m \leq n$, it must follow that

in $\mathfrak{p} \cap \bar{O}$.

Proof of (8): (a) and (b) proved that the valuations $\mathfrak{D}'$ on $\bar{O}_K$ satisfy axioms II and III for a Dedikind ring; since by definition $\bar{O}_K = \bigcap_{w\in\Phi} \bar{O}_w$, axiom I is valid (see last para. of proof for II2). Because prime ideals in $\bar{O}_K$ are maximal by (c), $\bar{O}_K$ is a Dedikind ring with valuations $\mathfrak{D}'$.

Let x be an element of $I[K]_{\bar{O}}$. Then for each v in $\mathfrak{D}$, x is in $I[K]\bar{O}_v$ and so by (4), x is in $\bigcap_{i=1}^{m_v} \bar{O}_{wi}{}^{v}$ for each v in $\mathfrak{D}$; x is in $\bigcap_{w\in\Phi}\bar{O}_w$. $I[K]_{\bar{O}} \subseteq \bar{O}_k$. By simply reversing the steps of the preceding argument, the conclusion $\bar{O}_k \subseteq I[K]_{\bar{O}}$. is obtained. $I[K]_{\bar{O}} = \bar{O}_k$.

K is proved to be the quotient field of $\bar{O}_K$ in the following way: Let h be in K, f(h) = 0 where $f(x) = x^m + a_{m-1}x^{m-1} + \ldots\ldots a_0$. Let v_1, $v_2, \ldots\ldots v_n$ be a set of valuations in $\mathfrak{D}$ which includes valuations v (of $\mathfrak{D}$) for which $v(a_j) \neq 0$, j = 0, 1, 2,......or n-1. Set $M = \max\left\{-v_i(a_j)\right\}_{\substack{i=n\ j=m\\ i=1\ j=1}}$. There is an element a in $\bar{O}$ such that $v_i(a) \geq M$, $v_i(a) \geq 0$, $1 \leq i \leq m$. Let $g(x) = x^m + a_{m-1}a^{m-1} + a_{m-2}a^2x^{m-2} + \ldots\ldots a_0a^m$. Then g(x) is a monic polynomial with coefficients, $a_{m-1}a$, $a_{m-2}a^2, \ldots\ldots a_0a^m$, all in $\bar{O}$; also g(ax) = 0 if and only if f(x) = 0. Therefore <u>ah</u> is an element of $I[K]_{\bar{O}} = \bar{O}_K$ and <u>h</u> is the quotient of the elements <u>ah</u> and <u>h</u> from $\bar{O}_k$.

Remarks: applications of results to finite, discrete principally ordered systems with separation property: Suppose the hypothesis for the valuations $\mathfrak{D}$ on $\bar{O}$ are altered so that only axioms I-III are valid; in other words prime ideals are not necessarily maximal in $\bar{O}$. Can results similar to the above still be obtained for an appropriate subring of the algebraic extension K? It is observed that axiom IV is not used in this chapter except to prove that prime ideals are maximal in the ring O_K (9a). All other proofs are valid without axiom IV. Therefore, if O is a principally ordered system satisfying axioms I, II and III, just exactly as above valuations Φ' can be defined on a ring $\overline{O}_k$; the set of valuations Φ' can be constructed from Φ in precisely the same manner as in (1) and (7) and the ring $\overline{O}_k$ can again be defined as the intersection of the valuation rings. It will follow that axioms I, II and III are valid in O_k; K will be the quotient field of $\overline{O}_k$ and the ring of integrally dependent elements from K, $I[K]_{\overline{O}}$ will coincide with $\overline{O}_k$.

Terms of Chapter IV

Coefficient . . . . App. III.1 , para. 3

Completion of field with respect to valuation . . . . App. IV.1

Defining equation . . . . App. III.1, para. 3

Finite algebraic extension . . . . App. III.2

Galois group . . . . App. III.5

Integrally dependent . . . . App. III.1, last para.

Least normal closure . . . . App. III.6

Mapping into . . . . App. I.5

Maximal separable subfield . . . . App. III.6

Monic equation . . . . App. III.1, para. 3

Norm . . . . App. IV.2

Purely inseparable extension . . . . App. III.4

Quotient . . . . App. II.7

Simple extension App.III.2

Symmetric functions . . . . App. III.7

Notation

N_{Ω} ____ App. IV.2

CHAPTER V

EXAMPLES

Examples of rings which are Dedikind rings or which satisfy some of the properties of Dedikind rings are considered below. Each section of this chapter considers a certain specific example.

Example 1. Ring of integers: The ring of inters I is a Gaussian ring [Chapter IV., Sec. 3]. The only units of I are +1 and -1, and the only associates of an element are +a and -a. Therefore, the set $\mathbb{P}$ of those positive integers that are prime comprises a set of elements, no distinct two of which are associates; moreover, every prime integer is an associate of some member of $\mathbb{P}$. For each prime $\mathfrak{p}$ in $\mathbb{P}$, define $v_{\mathfrak{p}}(a)$ as the integer corresponding to the power of $\mathfrak{p}$ in the finite prime power representation of the non-zero element a. Define v (a) = 0 if the prime is not represented. Define $v_{\mathfrak{p}}(0) = \infty$ for all p in $\mathbb{P}$. For example, $12 = (2^2)\ (3)\ (-1)$; $v_2(-12) = 2$, $v_3(12) = 1$, $v_{\mathfrak{p}}(12) = 0$ for all other p in $\mathbb{P}$. Each v is a valuation on I and the set of valuations $\{v_p\}_{p\in\mathbb{P}}$ satisfies axioms I to III. Also, axiom IV is valid because I is a principle ideal ring.

Let R denote the rational numbers, the quotient field of I. As usual, each valuation v can be extended to the quotient field by defining $v(b/a) = v_p(b) - v_p(a)$. The set Φ' of the extended valuations then satisfies axioms I'-IV'. (Refer to statement of result (II.2).) For all a in I, define w(a) as follows: $w(a) = w_2(a) + v_3(a)$. w is then a valuation of I. Let w be extended to R. The set Φ of the extended valuations, $\{\Phi'\}\cup\{w\}$, then satisfies axioms I', III', and IV' on R.

Of course, distinct pairs of v_p satisfy axiom II'. If p is a member of $\mathbb{P}$ distinct from either 2 or 3, then $v_p(p) = 1$, $w(p) = 0$ and $v_p(2) = 0$, $w_p(2) = 1$. Also $v_2(2/3) = 1$, $w(2/3) = 0$, and $v_2(3) = 0$, $w(3) = 1$. Finally, $v_3(3/2) = 1$, $w(3/2) = 0$, and $v_3(2) = 0$, $w_3(2) = 1$. The set $\mathfrak{M}$ then satisfies axiom II'.

As pointed out in the proof of (II.2) and as now illustrated by this present example, the set of valuations satisfying axioms I'-IV' on the quotient field may well properly contain the set of valuations satisfying axioms I-IV on the ring.

Example 2. Algebraic extension of a Dedikind ring: Again denote by I, R, and $\mathbb{P}$ the integers, the rationals, and the set of prime (positive) integers respectively. Consider the polynomial $x^2 + 1$. As is customary, let i denote a root of this polynomial. Then i and -i are the roots of $x^2 + 1$. According to (III.7), R (i) will be then the quotient field of a Dedikind ring composed of the totality of elements (of R (i)) that are integrally dependent on I. If a + bi is in R(i), b ≠ 0, then the defining equations for a + bi is $x^2 - 2ax + (b^2 - a^2) = 0$. Thus a + bi is in the Dedikind ring if and only if 2a and $b^2 - a^2$ are integers. (See [16 Section 14.3].) This ring is the set $I(i) = \{a + bi$ in $R(i)/a$ and b integers$\}$. The valuations $\mathfrak{M}'$ on I(i) are composed of the following members: For each $\mathfrak{p}$ in $\mathbb{P}$ there is a valuation w_1 equal to the norm N over a completion of R (with respect to v); also, there are valuations conjugate to w_1. The question then arises, how many conjugate valuations are possible? Since R(i) is a normal extension of R with basis (1, i) over R, the only possible R-automorphisms of R(i) are the identity automorphism mapping each element onto itself and the automorphism σ defined by $\sigma(i) = -i$. Thus the only valuation conjugate to w_1, besides w_1 itself, is the valuation w_2 such that $w_2(a + bi) = w_2(a - bi)$.

For example, consider possible prolongations of the valuation v_3 from R to R(i). Consider the roots of the polynomial $x^2 + 1$ which are in the field . Is $x^2 + 1$ reducible in $\Omega_3(x)$? If so it has a root $\underline{r}$ in Ω_3.* As provided by appendix IV.5, set $r = \sum_{i=0}^{\infty} r_i 3i$, r_i in I, $0 \leq i \leq \infty$. (It is not possible that $r = \sum_{i=K}^{\infty} n_i 3^i, K<0, r_K \neq 0$; in this case $w_1^3(r) < 0$, but the roots of $x^2 + 1$ are members of I(i).) Then $r^2 = (r_0 + 3\sum_{i=0}^{\infty} r_{i+1} 3^i)^2 = -1$. Therefore, r_0^2 must be congruent to -1, mod 3. However, if $r_0 \equiv 0 \bmod 3$, $r_0^2 \equiv 0 \bmod 3$; if $r_0^2 \equiv 1 \bmod 3$, $r_0^2 \equiv -2 \bmod 3$; if $r_0 \equiv -1 \bmod 3$, $r_0^2 \equiv -2 \bmod 3$. Thus $x^2 + 1$ is irreducible over (x) and no root of this polynomial is in Ω_3. The valuations w_1^3 and w_2^3 each must be the restriction of the only possible valuation N_Ω to the field R(i). $w_1^3 = w_2^3$. In general, the prolongations w_1 and w_2 of v form R to R(i) are equal whenever $n^2 \equiv 1 \bmod p$ is valid for no positive integer n.

Suppose p is a member of $\mathbb{P}$ for which there exists an integer i, $i \equiv -1 \bmod$. As an example, consider $p = 5$. Then $2^2 \equiv -1 \bmod 5$, and $x^2 + 1 \equiv x^2 - 4 \equiv (x-2)(x+2) \bmod 5$ or mod $P\{v_5\}$. By Hensel's lemma (see app. IV.4), $x^2 + 1$ is then reducible in $\Omega_5(X)$. Let $x^2 + 1 = (x+r)(x-r)$ where $r = \sum_{i=0}^{\infty} r_i 5^i$ and where r is a root of $x^2 + 1$. (Refer IV.4 and IV.5.) The first term, r_0 of r must be either +2 or -2. It may be presumed to be +2.

$$r^2 + 1 = 0 = 0^\circ 5^0 + 0^\circ 5^1 + 0^\circ 5^2 + \ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$r = 2 + r_1 5^1 + r_2{}^\circ 5^2 + \ldots\ldots\ldots\ldots\ldots + r_n 5^n + \ldots\ldots\ldots\ldots$$

Then $2(2) + 1 + 2^\circ 2^\circ r_1{}^\circ 5^1 + h_2 = 0$. Here, h_2 consists of terms in the product r^2 which involve 5^n, $n \geq 2$. Therefore, [Section 19.2] 2(2) + 1

otes the completion of R with respect to v_p.

$+ 4r_1{}^\circ 5 \equiv 0 \bmod 5^2$ or $1 + 4r_1 \equiv 0 \bmod 5$.

$r_1 \equiv 1 \bmod 5$.

$r = 2 + 5^1 + r_2 5^2 + \dots\dots\dots r_n 5^n + \dots\dots\dots\dots\dots$

Therefore, $2^\circ 2 + 1 + 2^\circ 2^\circ 5^1 + 5^2 + 2^\circ 2^\circ r_2 5^2 + h_3 = 0$. Here h_3 consists of terms of the product r^2 involving 5^n, $n \geq 3$. Consequently, $2(2) + 1 + 4^\circ 5^1 + 5^2 + 4r_2 5^2 \equiv 0 \bmod 5^3$. $2 + 4r_2 \equiv 0 \bmod 5$. Therefore, $r_2 \equiv 2 \bmod 5$. The argument above then justifies the formula, valid for any positive integer n, $4r_n + \frac{Kn}{5^{n-1}} \equiv 0 \bmod 5$. Here Kn is the sum of all terms of either the expression r^2 or else of the expression $(r_i 5^i)^2 + 1$ which involves 5^j for some integer j, $0 \leq j \leq n$. In other words, k_n is $1 + \sum_{i,j} r_i r_j 5^{i+j}$ where the sum extends over all pairs i,j of non-negative integers such that $i+j \leq n$. It follows $a_3 \equiv 1 \bmod 5$, that $a_4 \equiv 4 \bmod 5$, etc.

Let a + bi be in I(i). Then w_1^5 (a + bi) is the value of a + 2b $+ \sum_{i=1}^{\infty} br_i 5^i$ with respect to v in the completion field (app. IV.1). As provided by app. IV.5, $w_1^5(a + bi)$ is then zero unless $a + bi \equiv 0 \bmod 5$. But if $a + 2b \equiv 0 \bmod 5$, then $w_1^5(a + bi)$ equals k where k is the first index for which the coefficient of 5^k in $\sum_{i=1}^{\infty} br_i 5^i$ is not zero. The conjugate prolongation $w_2^5(a + bi)$ is of course given by $w_2^5(a + bi) = w_1^5(a - bi)$. For example, $w_1^5(4 + 3i) = v(4 + 3^\circ 2 + 3^\circ 1^\circ 5^1 + 3^\circ 2^\circ 5^2 + 3^\circ 1^\circ 5^3 + \dots\dots)$ $= v(7^\circ 5^2 + 3^\circ 5^3 + \dots\dots)$. $w_1^5(4 + 3i) = 2$. $w_2^5(4 + 3i) = w_1^5(4 - 3i) = v(1 - 3^\circ 1 - 3^\circ 2^\circ 5^2 - 3^\circ 1^\circ 5^3 \dots\dots) = v(2 - 6^\circ 5^2 + \dots\dots)$. $w_2^5(4 + 3i) = 0$. Consideration of the element $\frac{1}{4 + 3i}$ shows that w_1^5 and w_2^5 are inequivalent. The prime ideals $P(w_1^5)$ and $P(w_2^5)$ corresponding to the two valuations will now be characterized. $P\, w_1^5 = \{x/x \text{ in } I(i),\ w_1^5(x) > 0\} = \{x/x = a + bi, \text{ a and b integers, } a + 2b \equiv 0 \bmod 5\}$. Likewise, $P\, w_2^5 = \{x/x = a + bi, \text{ a and b integers, } a - 2b \equiv 0 \bmod 5\}$. For the element a +

bi of I(i) to be in $P(w_1^5)$ one of the following situation must hold:

$a \equiv 0$, $b \equiv 0$; $a \equiv 1$, $b \equiv 2$; $a \equiv 2$, $b \equiv 3$; $a \equiv 3$, $b \equiv 1$; $a \equiv 4$, $b \equiv 3$ (congruences mod 5). In order that a + bi is in P w_2^5 the possible situations are:

$a \equiv 0$, $b \equiv 0$; $a \equiv 1$, $b \equiv 3$; $a \equiv 2$, $b \equiv 1$; $a \equiv 3$, $b \equiv 4$; $a \equiv 4$, $b \equiv 2$.

In conclusion it is interesting to note that I(i) is a Gaussian ring as well as a Dedikind ring. A mapping of I(i) into the positive integers is defined by the relation $(a + bi) = a^2 + b^2$. If m and n are in I(i), then $(mn) = (m)(n)$. Therefore, if u is a unit of I(i), $= 1$. If I(i) is not a Gaussian ring, there must be an integer n and two distinct sets of relatively prime* positive integers $\{x,y\}$ and $\{u,v\}$ such that $n = x^2 + y^2 = u^2 + v^2$. As arguments in Nagell [9 Section 54] and Wright [16 Section 14.3] indicate, this is not possible.

Other references to this section are [13 Sect. 76, Bewertung von Alg. Erweit], and [15 "Valuations of Alg. No. Fields"].

Example 3. A non-Gaussian Dedikind ring: In view of examples 1 and 2, it might be conjectured that every Dedikind ring is Gaussian. The example of the ring $I(\sqrt{-5})$ shows this conjecture is false. Here $\sqrt{-5}$ and $-\sqrt{-5}$ are roots of the equation $x^2 + 5 = 0$. $R(\sqrt{-5})$ is then a finite algebraic extension of the rationals R and is therefore the quotient field of a Dedikind ring. By the same type of argument used in example 2, this ring is simply the set of elements $I(\sqrt{-5}) = \{a + b\sqrt{-5}$ in $R(\sqrt{-5})/a$ and b in I(the set of integers)$\}$. $I(\sqrt{-5})$ is a standard well-known example of a non-Gaussian ring. A proof of this property of $I(\sqrt{-5})$ appears in Jacobson [8 example in Ch. IV, Sec. 2].

Example 4. A finite discrete principally ordered system with

*a and b are relatively prime if a and b have no common multiples except zero.

separation property that is not a Dedikind ring: Let G be a Gaussian domain (integral domain). Let G(x) denote the set of all polynomials in F(x) (where F is the quotient field of G) with coefficients in G, G(x) is also a Gaussian domain. [Ch. IV, Sec. 10, 11] Consider I(x) where I denotes the integers. The only units of I are +1 and -1. A polynomial, $\sum_{i=0}^{m} a_i x^i$, $a_n \neq 0$, is termed positive or negative accordingly as a_n is positive or negative. Let $\mathbb{P}$ be the set of positive prime elements of I(x). As in example 1, for each p in $\mathbb{P}$ define $v_p(a)$ to be the power of p that occurs in the essentially unique prime power representation of a given element a. Again, the set of valuations $\{V_p\}_{p\in\mathbb{P}}$ satisfies axioms I, II, and III. Consider the ideal $(x,2) = \{a$ in $I(x)/\ a = bx + c2$ for some elements b and c in $I(x)\}$. Then (x,2) consists of all the elements of I(x) excepting the odd integers, $\{-3,-1,1,3,\ldots\ldots.\}$. $v_p(x,2) = 0$ for all p in $\mathbb{P}$. Actually (x,2) is a maximal prime ideal that contains the prime ideal (x). (Reference [14 Section 63, "Einfache Transcendente Erweit."])

Example 5. A finite discrete principally ordered system in which the ascending chain condition is not valid: It is noted that if G is a Gaussian ring the polynomial ring G(x) can just as well be indicated by $G(x_n)$ where n is any index, $1 \leq n \leq \infty$ [Sec. 10, Ch. IV]. Let I_0 denote I, I_1 denote $I(x_1)$ or I(x). Inductively, let I_n denote $I_{n-1}(x_n)$. For n = 1,2......, I_n is a Gaussian domain. Finally, let I_∞ denote $\bigcup_{m=0}^{\infty} I_m$. I_∞ is then the set of all finite sums

$$\left\{\sum_{j=1}^{m} a_j X_{i_1}^{k_{i_1}} X_{i_2}^{k_{i_2}} \text{------} X_{i_m}^{k_{i_m}}\right\}.$$

Two such sums or members of I_∞ are equal if and only if the same collection of subscripts i_j and corresponding exponents k_{i_j} appear in each sum and also if the corresponding coefficients $[a_i]_{i=1}^{i=n}$ are equal. For a given element p of I let m equal the maximum of the subscripts $\{i_j\}$ in a finite sum that represents p. Then p is in I_m but p is not in I_n for $n > m$. Hence p is in no way representable as a finite product of elements, one of which is not in I_m. The unique prime power representation of p that occurs in I_m is also a unique representation in I_∞. I_∞ is Gaussian, and therefore, as in examples 1 and 4, a non-null set Φ of valuations can be defined on I_∞ satisfying axioms I, II, and III. The ascending chain condition is not valid in I . Consider the properly ascending chain in which the n^{th} ideal is generated by $(x_1, x_2 \ldots\ldots\ldots x_n)$: $(x_1), \subset (x_1, x_2) \subset (x_1, x_2, x_3) \ldots\ldots\ldots \subset (x_1, x_2, \ldots x_n) \subset \ldots$.(References: [14]Sec. 63, "Einfache Transcendente Erweit," and Sec. 64, "Der Transcendergrod.")

Appendix I

BASIC SET CONCEPTS

Section 1. Introduction. The meta-mathematical and/or logical notion of set and element is not defined. The statement "a is an element (or a member of) in B" is denoted symbollically by "a ε A." The set A is said to be contained in the set B if each element of A is also an element of B. In each case, A is said to be a subset of B and also B is said to contain A. The notation "A $\subseteq$ B" or "B $\supseteq$ A" means A is contained in B and B contains A. The negation of A $\subseteq$ B or of B $\supseteq$ A is indicated by A $\nsubseteq$ B or by B $\nsupseteq$ A. Thus, A $\nsubseteq$ B means that there is an element in the set A which is not in the set B. The sets A and B are said to be equal if A and B are composed of the same elements; set equality of A and B is indicated by A = B. It is observed that A = B if and only if A $\subseteq$ B and B $\supseteq$ A. The set A is said to be properly contained in the set B or B is said to properly contain A if A $\subseteq$ B but if A does not equal B. The notation A $\subset$ B or B $\supset$ A indicates such a relation. A null-set is a set which consists of not a single element. Such a set is denoted by $\emptyset$.

Class of sets; set operations: A class of sets is a collection of sets $\{A_i\}$ in which all members, A_i, of the collection are contained in some preassigned fundamental set or space. In this sense a class is a set composed of elements that are subsets of the space. Let $\{A_i\}$ be a class of sets. The union of the sets in the class is the set consisting of all elements of the space which are members of at least one set in the class. This union is denoted by $\bigcup_{A_i \varepsilon \{A_i\}} A_i$ or by $\bigcup_{i=1}^{\infty} A_i$ in case the class is well-ordered and indexed by the subscript i(see app. I.4). The intersection of sets in the class is the set consisting of all elements of the space which are members of each set in the class. This intersection is denoted by $\bigcap\limits_{A_i \in \{A_i\}} A_i$ or by $\bigcap\limits_{i=1}^{\alpha} A_i$ in case the class is well-ordered and indexed as above.

Other notation: " $\exists$ " is used to mean the phrase "there exists"; " $\ni$ " is used to mean "such that." Thus "$\exists$ A $\ni$ a ϵ B" means "there exists an element a in the set A such that a is also in the set B." The notation $\{x \in S/$ property "P" holds$\}$ denotes the subset of S which consists of all elements that have property "P". If A and B are elements of a set, the phrase "a equals b" or the notation "a = b" means that a and b are the same element. The negation of "a = b" is indicated by "a $\neq$ b."

For details of the above discussion refer to Kershner [4Ch. IV].

Section 2. Ordering Relation. Let A be a set. An ordered pair of A is an arrangement of subsets of two elements from A. Thus (a,b) where a and b are elements from A is an ordered pair of A. Two ordered pairs of A are considered to be equal if and only if the two pairs consist of the same arrangement of the same two elements; e.g., (a,b) is not equal to (b,a) unless a = b. A relation on A is a subset of the set of ordered pairs of A. Let R be a relation on A. The element a is then said to be related to the element b, denoted by a R b, if and only if (a,b) is in R. The relation R is termed an ordering (or an ordering relation) and A is said to be ordered by R (or A is said to be ordered) if R has the following properties: (i) for any pair of elements, a and b, from A either a R b or else b R a; (ii) if a R b and b R c, then a R c; (iii) if a R b and b R a, then a = b.

An ordering relation R is frequently denoted by "$\geq$." Thus a $\geq$ b means a R b. If "$\geq$ " is an ordering relation, then the converse relation

"$\leq$" is also an ordering relation. "$\leq$" is defined as follows: $a \leq b$ if and only if $b \geq a$. If a and b are elements of an ordered set, then a is said to succeed or be greater than b, denoted by $a > b$, if $a \geq b$ but $a \neq b$; a is said to precede or be less than b, denoted by $a < b$, if $a \leq b$ but $a \neq b$. For a detailed discussion refer to Kershner [4Sec. 4.8 and 15.4].

Example 1. Let I be the set of positive integers, $\{\ldots\ldots -2, -1, 0, 1, 2 - -\}$. Define $a \geq b$ where a and b are in I, as follows: $a \geq b$ if and only if either $a = b$ or else $a - b$ is a positive integer (refer to [4]Chapter VIII).

Example 2. Let R_n be a set of rational integers: $R_n = \{\ldots\ldots\ldots - {}^m/n, -m-1/n, \ldots\ldots\ldots -1/n, 0, 1/n/2/n, \ldots\ldots\ldots\}$ where n is an integer. Define "$\geq$" on R_n as follows: $b/n \geq a/n$ if and only if the integer b is greater than or equal to the integer a as provided in example 1.

Example 3. Let R_n be a set of rational integers as above. A set of extended rational integers, R_n', is a set comprised of the rational integers R_n together with two new elements, ∞ and $-\infty$. Elements in R_n are greater than or less than one another according to the same relation as before while $-\infty \leq a \leq \infty$ for all a in R_n.

<u>Section 3</u>. <u>Mappings</u>. Let S and S' be sets. Suppose that for each a in S there is a uniquely defined element $\varphi(a)$ in S'. This correspondence, φ, between elements of S and S' is termed a mapping of S into S' and is indicated by $\varphi : S \to S'$. The mapping $\varphi : S \to S'$ is said to be a mapping onto S' if for each b in S' there is an element a in S such that $\varphi(a) = b$. The mapping $\varphi : S \to S'$ is said to be single-valued if for each element a of S' the set $\{x \in S / \varphi(x) = a\}$ consists of at most one element. If the mapping $\varphi : S \to S'$ is single-valued and onto, then for each element a of S' the set mentioned above consists of exactly one

element. The single-valued onto mapping is often called a one-to-one correspondence or a correspondence between S and S'. Then $\varphi^{-1}: S' \to S$, defined by $\varphi^{-1}(a) = x$ where x is the element in S for which $\varphi(x) = a$, is a single-valued onto mapping. (Refer to {[2]Introduction, Sec. 2} and to [[4]Section 5.4.])

Consider the mapping, $\varphi : S \to R_n'$ where R_n' is a set of extended rational integers. The following definitions are made: $\min_{a \in S}\{\varphi(a)\} = p$ if p is a rational integer such that $\varphi(b) \geq p$ for all b in S and if $\varphi(c) = p$ for at least one element c in S; $\min_{a \in S}\{\varphi(a)\} = \infty$ means that $\varphi(b) = \infty$ for all b in S; $\min_{a \in S}\{\varphi(a)\} = -\infty$ means that for each rational integer p there is an element b in S for which $\varphi(b) \leq p$. $\max_{a \in S}\{\varphi(a)\}$ is defined analogously; more precisely, let $\max_{a \in S}\{\varphi(a)\}$ be defined as $\min_{a \in S}\{-\varphi(a)\}$ where $-(\infty) = -\infty$ and $-(-\infty) = \infty$. There always are extended rational extegers p and q such that $\min_{a \in S}\{\varphi(a)\} = p$ and such that $\max_{a \in S}\{\varphi(a)\} = q$. (Refer to Kershner, [4]15.4.)

Section 4. Well-ordering. Let A be an ordered set with ordering relation "$\leq$." A is then said to be a well-ordered set or to be well-ordered by "$\leq$" if each non-null subset $B \subseteq A$ has a so-called first element, an element b in B which precedes all other elements of b. Consider the possibility that an ordering relation ($\leq$) can be defined on every arbitrary set A in such a way that A is well-ordered. The axiom that states this possibility is in fact valid is called the well-ordering principle. This axiom is assumed to be true in many if not most current research papers. Accordingly, in the material at hand, the well-ordering principle is assumed.

Suppose that the set $\{1,2,3,........n,n+1,........\alpha-1,\alpha\}$ is well-ordered and that the positive integer n is the first element of each subset formed by deleting elements less than n. Then the set A is said to be indexed if there is a correspondence which is a single-valued onto mapping between A and the well-ordered set $\{1,2,3,\ldots\ldots n,n+1,\ldots\ldots \alpha 4,\alpha\}$. This correspondence between elements of a and the indices (the elements of the well-ordered set) is often indicated by affixing subscripts or occasionally by affixing superscripts, e.g., a_1 is the element corresponding to the index 1, a_2 is the element corresponding to 2, etc. In this publication square brackets will always designate indexed sets while curled brackets might refer to sets that are not indexed. Thus the indexed set A, mentioned above, can be denoted by $\left[a_i\right]_{i=1}^{i=\alpha}$. The notation "$\left[a_{i_j}\right]_{j=1}^{j=\beta}$" indicates a subset of the indexed set $\left[a_i\right]_{i=1}^{i=\alpha}$ such that a_i is in this subset if and only if the subscript i appears amongst $\left[i_1, i_2, \ldots\ldots i_\beta\right]$.

In referring to the indexed set A as $\left[a_i\right]_{i=1}^{i=\alpha}$, the "$\alpha$" is a symbol depending on the set A. If A has but finitely many n (where n is some positive integer) elements, then the appropriate symbol "α" for A is n. If the indices range over the complete set of integers, 1,2,3, ...n,n+1,........ but not over any larger set, then the appropriate "   " is∞.

Transfinite induction: Let $A = \left[a_i\right]_{i=1}^{i=\alpha}$ be an indexed set. For $1 \leq \beta \leq \alpha$ let $\{A_\beta\}$ denote any subset of the $\left[a_i\right]_{i=1}^{i=\alpha}$ of the form $\left[a_{i_j}\right]_{j=1}^{j=\alpha}$ where $i_j \neq i_k$ for $j \neq k$. For $1 \leq \beta \nleq \alpha$, let B + 1 denote the first index appearing in the set of indices in which the $i \leq B$ are deleted. Consider now a property $\mathbb{P}$ stated in terms of subsets of A. Suppose that the property $\mathbb{P}$ is valid for each subset of A of the form A_1; suppose further that it can be proved $\mathbb{P}$ is valid for each subset of the form A_{B+1} whenever $\mathbb{P}$ is valid for each subset of the form A_B, $1 \leq \beta < \alpha$. The principle of transfinite induction, which is a consequence of the well-ordering principle, then states that $\mathbb{P}$ is then valid for the set A_α or A. In case A = $[a_i]_{i=1}^{i=\infty}$ then the induction principle is nothing more than the usual induction employed in the most elementary algebra.

Hausdorf Maximality Principle: As a consequence of the well-ordering principle follows the Hausdorf maximality principle. Suppose $\mathcal{S}$ is a non-null set of subsets of a space S. ($\mathcal{S}$ is a non-null class of sets.) A chain of $\mathcal{S}$ in a non-null subset of $\mathcal{S}$ such that for every distinct pairof sets A,B in the chain, either A $\subset$ B or B $\subset$ A. The maximality principle states that each chain of $\mathcal{S}$ is contained in a maximal chain $\mathfrak{M}$: $\mathfrak{M}$ is a chain and is not properly contained in any chain of $\mathcal{S}$. A detailed discussion of this section appears in Kelley [3Ch. 0]; see especially under heading "Hausdorf Maximality Principle."

The proof of the following result, needed in the main body of results, illustrates the principle:

Hypothesis: A is a proper ideal of a ring with identity element.

Conclusion: A is contained in a maximal ideal.

Proof: Let $\mathcal{S}$ be the set of proper ideals of the ring containing A. Let $\mathfrak{M}$ be a maximal chain of $\mathcal{S}$ containing the trivial chain consisting only of the set A. Let $M = \bigcup_{B \in \mathfrak{M}} B$. M is then an ideal of S, indeed a proper ideal since none of the sets of $\mathcal{S}$ contain unit elements. Therefore, M is in $\mathfrak{M}$ and M must be a maximal ideal.

Section 5. Equivalence relation. Let $\sim$ denote a relation on the non-null set A with the following properties: a $\sim$ a for all a in A;

$a \sim b$ implies $b \sim a$ for any a and b in A; $a \sim b$, $b \sim c$ implies $a \sim c$ for any triplet a,b and c in A. " $\sim$ " is said to be an equivalence relation if " $\sim$ " satisfies these properties.

An equivalence relation on A partitions A into disjoint sets of mutually equivalent elements. In other words, there are certain non-null subsets of A, called equivalence classes, and denoted by $\{A_i\}_{i=1}^{\alpha}$ such that: $A = \bigcup_{i=1}^{\alpha} A_i$; $A_i \cap A_j = \emptyset$ for any distinct A_i, A_j; if x and y are elements of A, then x and y are members of the same set A_i if and only if $x \sim y$. For further discussion see Kershner [4Sec. 15.2 and 15.3].

Appendix II

BASIC IDEAS OF ALGEBRA

Section I Groups; operations: Let $\mathscr{G}$ be a non-null set. An operation on $\mathscr{G}$ (sometimes called a binary operation) is a singled-valued mapping $\mathscr{G}$ from the set of ordered pairs of $\mathscr{G}$ into the set $\mathscr{G}$. In other words, corresponding to each ordered pair (a,b) is a uniquely corresponding element of $\mathscr{G}$, $\mathscr{G}(a,b)$. A more usual notation for an operation, is, however "o". Thus "$a^\circ b$" refers to $\mathscr{G}(a,b)$. The set $\mathscr{G}$ and the operation "o" is denoted by $(\mathscr{G},^\circ)$ or simply by $\mathscr{G}$ if no ambiguity is possible.

4, Chapter VII .

Let "o" be an operation on $\mathscr{G}$. Parenthesis are used to indicate the order of successive "o" operations, e.g. $(a^\circ b)c$ means $d^\circ c$ where d is $a^\circ b$. $(\mathscr{G},o)$ is said to be associative or $\mathscr{G}$ is said to be associate under "o" if $(a^\circ b)^\circ c = a^\circ\,(b^\circ c)$ for all a,b, and c in $\mathscr{G}$. An identity element for "o" is an element e in $\mathscr{G}$ such that $e^\circ a = a = a^\circ e$ for all a in $\mathscr{G}$. Suppose there is an identity element e for "o". If a is in $\mathscr{G}$, an inverse element of a, denoted by a^{-1} is an element such that $a^\circ a^{-1} = a^{-1\circ} a = e$.

The non-null set on which the operation "o" is defined is said to be a group under "o" (or is said to be a group) if all of the conditions below hold. Alternative terminology is to refer to $(\mathscr{G},^\circ)$ as a group.

(i) "o" is associative on $\mathscr{G}$.

(ii) There is an identity element in $\mathscr{G}$ for the operation "o".

(iii) Each element of $\mathscr{G}$ has an inverse under "o".

(iv) If the elements a, b and c in $\mathscr{G}$ are such that $(b^\circ a) = (c^\circ a)$ then $b=c$; if the elements are such that $a^\circ b = a^\circ c$ then $b=c$.

Actually condition (iv) follows if (i), (ii) and (iii) hold. If conditions (i) and (iv) are valid then $\mathscr{G}$ is termed a semi-group under "o" or simply a semi-group. $(\mathscr{G},o)$ is termed a semi-group.

If (G,o) is a group(semi-group), if the restriction of the operation "o" to elements in $\mathcal{H}$, $\mathcal{H} \leq \mathcal{G}$, is a group (semi-group) operation, then $\mathcal{H}$ is termed a subgroup (subsemi-group) of G.

The operation "o" on is called commutative operation if aob= b^{o}a for all a, b in $\mathcal{G}$. If ($\mathcal{G}$, o) is a commutative group (group in which "o" is commutative) then often (G, o) is termed an addative group, the operation is termed addition and is denoted by $+$. If ($\mathcal{G}$, o) is a commutative semi-group ("o" is commutative) then often "o" is referred to as multiplication or occasionally as addition and ($\mathcal{G}$, o) is termed a multiplicative or an a ddative semi-group respectively.

For an addative group the following notation is adopted: $\sum_{i=1}^{m} a_i$ denotes the successive addition operations $a_1 + a_2 + a_3 \ldots . + a_n$. Because " $+$" is associative it does not matter in what order the n-1 "$+$" operations are performed. Indeed, because " $+$" is commutative, it does not matter if the order of the $[a_i]_{i=1}^{m}$ are interchanged. "-b" denotes the inverse of b and a-b denotes.a.$+$.(-b) . "O" denotes the identity or zero element of $\mathcal{G}$. "na", where n is positive integer denotes $\sum_{i=1}^{m}$ a_i, a_i =a, $1 \leq i \leq n$.; "na", where n is zero, denotes 0; "na", where n is negative denotes -n(-a). For all integers n and m (n $+$m) a = na $+$ ma.

The concept of a linearly ordered group is defined as follows: Let $\mathcal{G}$ be an additive group that contains a non-zero element; suppose that there is an ordering relation, $\geq$, defined on $\mathcal{G}$ with the properties a $+$ b $\geq$ c $+$ d whenever a $\geq$ b and c $\geq$ d. Then $\mathcal{G}$ is termed a linearly ordered group. (See Krull, [6, Section 1].)

A restricted direct sum is defined as follows: Let $[\mathcal{G}_i, o_i]_{i=1}^{i=\alpha}$ be an indexed set of additive groups (or of semigroups). Define $\mathcal{G} = \{x\}$ where x is any set $[x_i]_{i=1}^{i=\alpha}$ such that x_i is in $\mathcal{G}_i$, $1 \leq i \leq \alpha$, and such that x_i is an identity of $\mathcal{G}_i$ for at most finitely many i. Then $\mathcal{G}$ is an additive group (or a semigroup) with operation $\circ$ defined as follows:

$[x_i]_{i=1}^{i=\alpha} \; [y_i]_{i=1}^{i=\alpha} = [x_i \, o_i \, y_i]_{i=1}^{i=\alpha}$. Then $(\mathcal{G}, \circ)$ is called the restricted direct summand of the $[\mathcal{G}_i, o_i]_{i=1}^{i=\alpha}$ Jacobson [2, Chap. V, Sect. 14] discusses the direct summand under the name "direct product".

Examples: The set of integers $\{. . .-n, -n + 1, . . .-2, -1, 0, 1, 2, 3, ...n-1, n . . . . .\}$ forms a commutative group under the usual addition operation; the set of positive integers $\{- -1, 2, 3 . . . n, . . .\}$ forms a commutative semi-group under the usual addition.

The previous paragraphs of this section are discussed in detail in: Jacobson [2, Introduction, Sect. 4] and Kershner [4, Chapters VIII and XII].

Section 2. Rings and Integral domains. Let R be a non-null set on which two binary operations, addition (denoted by $+$) and multiplication (denoted by $\circ$) are defined. Then R or $(R, +, \circ)$ is termed an integral domain or more precisely an integral domain under $(+, \circ)$ if the following conditions are valid:

(i) $(R, +)$ is an additive group.

(ii) $(R, \circ)$ is a multiplicative semi-group. In other words, " ." is both associative and commutative; $a \circ b = a \circ c$ implies that $a = c$.

(iii) The distributive law holds: $a \circ (b + c) = (a \circ b) + (a \circ c)$

for all a, b, and c in R. (Once again, parenthesis are used to indicate the order of a series of operations.)

If $(R, +, \circ)$ satisfies (i) and (iii) but if only the associative and commutive part of condition (ii) is necessarily valid then R is termed a commutative ring (under $+$ and $\circ$). If conditions (i), (iii), the associativity part of condition (ii), and a so-called "right" distributive law are valid, then $(R, +, \circ)$ is termed a ring (under $+$ and $\circ$). By the right distributive law is that that $(b + c) \circ a = (b \circ a) + (c \circ a)$ for all a, b, and c in R.

An identity element of a ring $(R, +, \circ)$ is an element of R that is an identity in $(R, \circ)$. A ring need not have an identity element. If however the ring R does have an identity, then an element is called a unit if the element has an inverse for the multiplication operation.

In cases where no ambiguity is possible, the multiplication operation on a ring, $a \circ b$, is frequently indicated by ab. $\prod_{i=1}^{n} a_i$ denotes the element $a_1 a_2 a_3 \; . \; . \; . \; . \; . a_n$; because " o " is associative in a ring, this definition does not depend on the order in which the operations are performed. It follows $\prod_{i=1}^{n} a_i = \prod_{i=1}^{m} a_i \circ \prod_{i=m+1}^{n} a_i$ Also in a commutative ring, $\prod_{i=1}^{m} a_i$ remains unchanged if the order of the $[a_i]$ is changed. If $a = \prod_{i=1}^{n} a_i$, then a is called the product of the $[a_i]_{i=1}^{i=n}$. a^n is defined as $\prod_{i=1}^{n} a_i$, $a_i = a$, $1 \leq i \leq n$. The set $[a^n]_{n=1}^{\infty}$ is called the powers of a. Examples: The set of integers . . . . . $\{-3, -2, 1, 0, 1, 2, 3 \; . \; . \; . \; . \; .\}$ is an integral domain under the usual addition and multiplication operations. "1" is an identity for this ring. The set of even integers $\{. \; . \; . \; . \; . -6, -4, -2, 0, 2, 4, 6 \; . \; . \; . \; . \; . \; .\}$ is a ring and a integral domain without identity.

Unless parenthesis indicate otherwise, whenever there is a succession of addition and multiplication operations in a ring, the addition operation is understood to come first, e. g. $2 \circ 1 \not- 2 = 2 \circ 3 = 6$ in the ring of integers, but $(2 \circ 1) \not- 2 = 2 \not- 2 = 4$.

The set of non-zero elements of any integral domain is frequently indicated by affixing a superscript $*$ to the symbol for the integral domain, e.g. if I denotes the non-negative integers then I^* denotes the positive integers.

The material in this section is discussed in detail in Jacobson [2, Chap. II, Sect. 1 and 2].

<u>3. Ideals in Commutative rings</u>. The subset A of the commutative ring$(R, \not-, \circ)$ is called an ideal of R if the following conditions are valid:

A is a group under the addition operation of R restricted to elements in A; If a is in A and r is in R, then ar is in A; A properly contains the zero element.

In regard to the last condition, the standard definition of ideal requires only that A may be non-null set. Under this definition the set consisting only of the zero element is an ideal. The departure from this convention is made because in the material at hand it is desired to separate the zero "ideal" from other ideals. (Refer to Jacobson, [2, section 7, chapter II.]

R itself is always an ideal of R. The term proper ideal refers to ideals properly contained in R. A prime ideal is a proper ideal such that if a product of elements of R, ab, is in R then either a or b must be in R .

In the text prime ideals are invariably designated by underlined script letters.

A maximal ideal is an ideal M such that if $M \leq N \subset R$ and if N is an ideal, then N must equal M. A maximal ideal is always a prime ideal, but a prime ideal need not be maximal. For further discussion see Van der Waerden. [13, section 16, "Ideale, Restklassenringe."] .

Let $[x_i]_{i = 1}^{1 = n}$ be a finite set of elements in the commutative ring R with identity element. By the ideal generated by $[x_i]_{i = 1}^{i = n}$, denoted by $R(x_1, x_2, \ldots . . x_n)$, is meant the ideal $\{ a \text{ in } R / \exists$ elements $[a_i]_{i=1}^{i=n}$ in R such that $a = \sum_{i=1}^{n} a_i x_i \}$.

The ideal A in R is said to be finitely generated if there is a set $[x_i]_{i = 1}^{i = n}$ of elements of R such that $A = R(x_1, x_2 \ldots . . x_n)$.

Acommuatative ring (integral domain) is termed a principle ideal ring (principle ideal domain) if each ideal of the ring (integral domain) can be generated by a set consisting of only one element.

If A and B are ideals of the commutative ring R, then by (A,B) is meant the ideal generated by A and B: $(A, B) =$ r in R a in A, b in B such that $r = a \neq b$

<u>Section 4. Prime elements; Gaussian rings.</u> Let a and b be elements of an integral domain R. Then a is said to be a multiple of b if there is an element c in R such that $a = bc$. If a and b are multiples of one another, then a and b are called associates; in this case $a = bu$ and $b = av$ for appropriate unit elements u and v. A non-unit, non-zero element of R is called a prime element (or a prime) if p is a multiple of no element of R excepting units and associates of p.

An integral domain R is said to be a Gaussian ring if ezch non-unit of R* is essentially uniquely representable as a product of powers of finitely many prime elements: If a is a non-unit of R*, then there is a set of distinct primes $\left[p_i \right]_{i=1}^{i=n}$ and a set of positive integers $\left[k_i \right]_{i=1}^{i=n}$ such that $a = \prod_{i=1}^{m} (p_i^{k_i}) u$ where u is a unit. Moreover, if $a = \prod_{j=1}^{m'} q_j^{l_j} v$ where $\left[q_j \right]_{j=1}^{j=n'}$ is a set of distinct primes, $\left[l_j \right]_{j=1}^{j=n'}$ is a set of positive integers and v is a unit then there is a singled-valued, onto mapping, $\varphi : [p_i]_{i=1}^{m} \to [q_j]_{j=1}^{m'}$ such that $\varphi(p_i)$ is an associate of p_i, $1 \leq i \leq n$, and such that the integer k_i equals the integer l_j corresponding to $\varphi(p_i)$, $1 \leq i \leq n$. A more detailed discussion of this section appears in Jacobson [2, Chapter IV, sections 1, 2, 3 and 4].

5. <u>Rings with Ascending Chain Condition:</u> Let R be a commutative ring. A set of ideals of R, $\left[A_i \right]_{i=1}^{i=\infty}$ is said to be an ascending chain of ideals if $A_1 \subseteq A_2 \subseteq A_3 \subseteq A_4$ . . . . .or in other words if $A_k \subseteq A_{k \neq 1}$ for k = 1, 2, 3, etc. the ascending chain condition is said to be valid in R if each ascending chain of ideals terminates: for each chain $\left[A_i \right]_{i=1}^{i=\infty}$ there is an integer n such that $A_n = A_{n \neq 1} = A_{n \neq 2} = A_{n \neq 3} = \ldots . A_{n \neq k} = \ldots$, k = 1, 2, 3, etc.

The ascending chain condition is valid in R if and only if every ideal is finitely generated. For the proof, refer to Jacobson, [2, sections 4, 5, and 6, chapter VI].

Let A be a proper ideal in the integral domain R with identity element and satisfying the ascending chain condition. The set of elements $\left\{ z \text{ in } R \,/\, \exists \text{positive integer } n \text{ (depending on } z) \ni z^n \text{ is in } A \right\}$ is called the radical of A and is denoted by R(A). Because of the chain condition there is an integer m such that $R^m(A) \subseteq A$. The proper ideal A is said to be a primary ideal if whenever a product of two elements of R, ab, is in A, then either one of the elements a is in A or else the other element b is in R(A). If A is a primary ideal, then R(A) is a minimal prime ideal as McCoy shows [8, theorem 59].

Let A be any proper ideal in this integral domain R. Then there is a set $[\, Q_i \,]_{i=1}^{i=n}$ of primary ideals such that A $= \bigcap_{i=1}^{n} Q_i$. The intersection, $\bigcap_{i=1}^{n} Q_i$, is said to be irredundant if for each integer k, $1 \leq k \leq n$, it is true that $\bigcap_{i \neq k}^{n} Q_i \supset \bigcap_{i=1}^{n} Q_i$. Now if C and D are primary ideals with the same radical $\mathfrak{P}$, then $C \cap D$ is a primary ideal with radical $\mathfrak{P}$. It then follows that each proper ideal of R is equal to an irredundant short intersection of finitely many higher primary ideals: the term "short intersection" means that the radicals of the respective primary ideals are distinct. Details of the discussion in the last two paragraphs appear in Jacobson, [2, Chapter VI, sections 4-8] and in McCoy [8, Sect. 43-45].

<u>Section 6, Isomorphism, embedding</u>: Let R and R' be rings with addition and multiplication operations ($+$, $\circ$) and ($+'$, $\circ'$) respectively. A singled-valued mapping φ of R onto R' is termed a ring ismorphism or simply an ismorphism if for each pair of elements in R, a and b, $\varphi(a + b) = \varphi(a) +' \varphi(b)$ and $\varphi(a \circ b) = \varphi(a) \circ' \varphi(b)$. In such a case R' is said to be ismorphic to R. The concept of isomorphism (-phic, mapping) is also defined $^{-1}$ for groups (semi-groups). If φ is a singled-valued mapping of $\mathcal{G}$ onto $\mathcal{G}'$ where $(\mathcal{G}, \circ)$, $(\mathcal{G}', \circ')$ are both groups (semi-groups) then φ is said to be an isomorphism if $\varphi(a \circ b) = \varphi(a) \circ' \varphi(b)$ for all a, b in $\mathcal{G}$.

Let R and S be rings. Suppose there is an ismorphism of R $(\not- , \circ)$ onto a (not necessarily proper) subset R' of S $(\not- ' , \circ ')$. Then R is said to be embedded in S. Although R $(\not- , \circ)$ and R' $(\not- ' , \circ ')$ are not necessarily composed of the same set of elements and the same operations, because of the ismorphic mapping the elements of and the operations on R are frequently desingated by the same symbols as are the elements and operations of R'. For details refer to Jacobson /[2, section 9, Chapter II]

Section 7. Field, Quotient Field A field is a ring F in which the non-zero elements, F*, form a commutative group under multiplication. Am equivalent defihition of a field is: an integral domain with identity in which each non-zero element is a unit.

Suppose R is an integral domain. Then R can always be embedded in some field F. F may be chosen to be a "smallest" such field in the sense that if F' is any field in which R is embedded, then F can be embedded in F'. Such a smallest field F has the property that each element of F is equal to the quotient of an element in R by an element in R*. (In a field the element ab^{-1} often denoted by a/b or by $\frac{a}{b}$ is termed the quotient of a by b.**) In other words, $F = \{ x \text{ in } F / \exists\, a, b \text{ in } R' \ni x = a/b \}$ where R' is the subset of F ismorphic to R.

These "smallest" fields in which the integral domain can be embedded are ismorphic to one another. Any of the "smallest" fields is termed "the" quotient field of R.

Example: Let R be the ring of rational numbers (where p and q are integers) with the usual addition and multiplication operations. R is then the quotient field of the integral domain of integers. A more complete discussion of this example and of this whole section appears in

Jacobson $\lceil 2$, sections 1, 2, and 3, chapter III $\rfloor$

** (a^{-n} denotes $(a^{-1})^n$.)

Section 8. Determinents and homogeneous linear equations

Let $\{c_{ij}\}$, $1 \leq i \leq n$, $1 \leq j \leq n$ (n a positive integer) be a set of n^2 elements from a field F. Suppose that the c_{ij} are arranged in a square array of n rows and n columns such that c_{ij} appears in the i_{th} row and the j_{th} column. The determinent of this array, (c_{ij}) is defined as follows:

Let $\mathcal{S}$ be the set of all possible products of the form $c_{1j_1}c_{2j_2} \cdot \cdot \cdot \cdot \cdot c_{nj_n}$ in which the $\lceil j_k \rfloor_{k=1}^{k=n}$ are all different and $1 \leq j_k \leq n$. In other words, $\mathcal{S}$ consists of all those products (up to order) of n elements in which each row and each column is represented exactly once. Let t be in $\mathcal{S}$. For $1 \leq i \leq n$, define $P_i(t)$ to be the numbers of subscripts $\lceil j_k \rfloor_{k=i}^{k=n}$ that are greater than j_i. Define n(t) as $\sum_{i=1}^{n-1} P_i(t)$. The determinent of (c_{ij}) is defined as t $\sum_{t \in S} t(-1)^{n(t)}$. The sign $\sum_{t \in S}$ indicates successive addition operations on a set of elements in which $t(-1)^{n(t)}$ is represented exactly once for each t in $\mathcal{S}$.

The determinent is denoted by $\det(c_{ij})$, or by

$$\begin{vmatrix} C_{11} & C_{12} & C_{13} & \text{-----} & C_{1n} \\ C_{21} & C_{22} & C_{23} & \text{-----} & C_{2n} \\ C_{31} & \text{-----} & & & C_{3n} \\ - & - & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \\ C_{n1} & C_{n2} & C_{n3} & \text{-----} & C_{nn} \end{vmatrix}$$

Consider the equations: (j = 1, 2, ...or n) $\sum_{j=1} c_{ij} u_j = 0$.

One solution of this set of equations is obtained by letting the u_j, $1 \leq j \leq n$, all equal zero. A set $\lceil u_i \rfloor_{i=1}^{i=n}$ of elements of the field F is called a non-trivial solution to this set of equations if $\sum_{i=1}^{n} c_{ij}u_j = 0$, $1 \leq i \leq n$, and if also at least one of the u_i, $1 \leq i \leq n$ is not zero. A necessary and sufficient condition that the indicated set of equations have a non-trivial solution is that $\det(c_{ij}) \neq 0$. In MacDuffie, $\lceil 7$, section 4, pp. 8 $\rfloor$ appears a detailed discussion of this section.

Appendix III

ALGEBRAIC EXTENSIONS

Section 1. Polynomial domain, algebraic extensions

Suppose F(+,°) is a field. Let x be an arbitary symbol. There then exists a Gaussian integral domain, F(x), (operations + and °) that consists of elements that for some non-negative integer n are represented either as $a_nx^n + a_{n-1}x^{n-1}\ a_{n-2}x^n + \ldots\ldots + a_1x + a_0$ or as $\sum_{i=0}^{m} a_ix^i$. The $\left[a_i\right]_{i=0}^{i=n}$ are presumed to be elements of F. Here x^0 is defined to be 1, the identity of F and x^nx^m is defined as x^{n+m}. The elements $\sum_{i=0}^{m} a_ix^i$ and $\sum_{i=0}^{m} b_ix^i$ are considered to be equal if and only if $a_i=b_i$ for all i, $0 \leq i \leq \max(n,m)$ (max (n,m) means of course the greater of n and m). It is supposed that $a_i=0$ for $\max(m,n) \geq i \geq m$, and that $b_i=0$ for max $(m,n) \geq i \geq n$. The integral domain F(x) is called a polynomial domain over F. Elements of F(x) are called polynomials in x or, if no ambiguity is possible, polynomials. For further discussion, refer to Jacobson, [2, chapter III, section 4].

If K and F are fields, then K is termed an extension of F if $K \supseteq F$. The element a in K is a root of the polynomial $f(x) = \sum_{i=0}^{m} a_ix^i$ a_ix^i if $f(a) = 0$; in other words, if $\sum_{i=0}^{m} a_ia^i = 0$ where the operations are carried out in the field K. The field K is called an algebraic extension of F if K is an extension of F and if for each element a of K, there is a polynomial which has <u>a</u> as a root.

Let $f(x) = \sum_{i=0}^{m} a_ix^i$ be a polynomial. Then a_i, $0 \leq i \leq n$, is called the coefficient x^i and $\left[a_i\right]_{i=0}^{m}$ are the coefficients of f(x). The degree of polynomial is the maximum value of i for which the coefficient of x^i is not zero. A monic polynomial is a polynomial in which the coefficient of x^n, where n if the degree, is 1.

If a is a root of a polynomial of degree n, then a is a root of a monic polynomial of degree n. Suppose a is an algebraic extension of F. The defining equation of A over F is an equation f(x)=0 (sometimes written f(a) = 0) where f(x) is a monic polynomial that has as a root and where the degree of f(x) = minimum {degree of g(x)/g(x) in F(x), g(a) = 0.}

The polynomial k(x) is said to be reducible in F(x) if there are polynomials g(x) and h(x) such that k(x)=g(x)h(x) and such that 0 < degree of g(x)< degree of k(x). If no such g(x) and h(x) exist, then k(x) is said to be irreducible in F(x). The irreducible polynomials then comprise the set of prime elements of the Gaussian ring F(x) while elements of F*comprise the units. Also, it follows that the polynomial corresponding to the defining equation of an element (e.g. the f(x) mentioned above) is irreducible in F(x). For further discussion refer to Jacobson, [2, section 5, chapter III] and to Van der Waerden, [13, section 35, "Alg. Korperweitungen"] .

Let R be a subring (subset that is a ring) of the field F and let K be an algebraic extension of F. An element a of K is said to be intergrally dependent on R if a is a root of a monic polynomial all of whose coefficients are in R. The set of elements of K integrally dependent on R is a ring as provided by Jacobson [2, section 9, chapter VI] . If R is a Gaussian ring, then an element of K is integrally dependent on R if and only if the polynomial corresponding to the defining equation (Recall such a polynomial is monic) has all its coefficients in R. A ring is integrally closed in the field F if the set of elements in F integrally dependent on the ring coincides with the ring. A Gaussian ring is always integrally closed in its quotient field (see theorem 11 of above

Section 2. Basis, vector space, finite extension.

Let F($+$,o) be a field. An addative group, (Λ, $+'$) is then said to be a vector space over F if there is a mapping Ψ : $\Lambda \times F \to \Lambda$ with properties listed below. Here Λ x F denotes the set of all pairs of elements $\{\alpha, a\}$ where α is in Λ and a is in F.

$$\left.\begin{array}{l} \Psi\{\alpha +' \beta, a\} = (\Psi\{\alpha, a\}) +' \\ \qquad\qquad (\Psi\{\beta, a\}) \\ \Psi\{\alpha, a+b\} = (\Psi\{\alpha,a\}) +' (\Psi\{\alpha, a\}) \\ \Psi\{\Psi\{\beta,a\}, b\} = \Psi\{\beta, ab\} \\ \Psi\{0, a\} = 0 \end{array}\right\}$$

Here α and β are arbitrary elements of Λ,
a, b, " " " F;
O the zero element of Λ

Let $[\alpha_i]_{i=1}^{i=n}$ be elements of Λ. Denote by F($\alpha_1, \alpha_2, \ldots \alpha_m$) the set

$$\left\{ y \in \Lambda \middle/ \begin{array}{l} \exists \text{ elements } [a_i]_{i=1}^{i=n} \in F \text{ such} \\ \text{that } y = \sum_{i=1}^{m} \Psi\{\alpha_i, a_i\} \end{array} \right\}.$$

The elements $_{i=1}^{i=n}$ of are said to be linearly independent over F if $\sum_{i=1}^{m} \Psi\{\alpha_i, a_i\} = 0$ is possible only if the $[a_i]_{i=1}^{i=n}$ are all zero. If F($\alpha_1, \alpha_2, \ldots \alpha_m$) $= \Lambda$ and if the $[\alpha_i]_{i=1}^{i=n}$ are linearly independent over F then $[\alpha_i]_{i=1}^{i=n}$ is said to be a basis, or more precisely a finite basis, of Λ over F. For details refer to Van der Waerden, [14, section 33, "Linear Abnag. Grozen" and Section 34, "linear Fleichungen."]

Suppose K is an extension of the field F. Then K is a vector space over F as follows: for each in K and each a in F define to be the field operation in K, α a. If there is a finite basis for (the vector space) K over F then K is termed a finite extension of F and $K \geq H \geq F$ (H a field) then H is also a finite extension of F. (See section 34 of above reference) If K is a finite extension of F with a basis (over F) of n elements, then each element a of K is a root of a polynomial in F(x) of degree not greater than n. Accordingly, a finite extension is often termed a finite algebraic extension. For detailed discussion of this paragraph, refer to Van der Waerden, [13, section 35, Alg. Korperweitungen].

If the elements $\left[a_i\right]_{i=1}^{i=n}$ are in some finite extension K of F, then the notation $F\left[a_1, a_2, \ldots\ldots a_m\right]$ is used to indicate the subfield of K (subset which is a field), $F(1, a_1, a^2, a_1^{\,3}, \ldots\ldots a_1^{\,n1-1}, a_2, a_2^{\,2}, \ldots\ldots a_2^{\,n_2-1}, a_3 \ldots\ldots)$ where the $\left[n_i\right]_{i=1}^{i=k}$ are the degrees of the polynomials corresponding to the defining equations of the $\left[a_i\right]$.

The finite algebraic extension K of F is said to be a simple extension if for some a in K, $K=F\left[a\right]$. Any finite algebraic extension K of F is the last member of some finite chain of fields beginning with F such that each member of the chain is a simple extension of the previous member. Indeed, if a is a basis element of K over F not in F, the first member of such a chain can be $F\left[a\right]$; if b is a basis element of K over F not in $F\left[a\right]$, the next member of the chain can be $F\left[a\right]\left[b\right]$, etc.

Section 3. Decomposition fields.

According to Van der Waerden [13, section 35, "Alg. Korpeweitungen"] it is possible to construct a finite algebraic extension of a field without making use of any preassigned "larger" field. Let f(x) be a monic polynomial in F(x). There is then a field K satisfying the conditions:

(i) K is a finite algebraic extension of F.

(ii) f(x) factors linearly in K(x): $f(x) = \prod_{i=1}^{n}(x-\alpha_i)$ where the $[\alpha_i]_{i=1}^{i=n}$ are elements of K.

(iii) If K' is any field satisfying (i) and (ii) then K can be embedded in K'.

Such a field K is called a decomposition field of f(x) over F.

If F H K, if a is in K and not in H, if H and K are fields, if the defining equations of a in H(x) is g(x) = 0, and if the defining equations of a in F(x) is f(x) = 0, there then exists a polynomial h(x) in H(x) such that f(x) = g(x)h(x). Proof appears in the course of Van der Waerden's discussion [13, Section 35, "Alg. Korperweitungen"].

Section 4. Seperable and inseperable.

Let K be an algebraic extension of F and let a be an element of K. If the polynomial f(x), where f(x) corresponds to the defining equation of a over F, is a seperable polynomial (has only distinct roots in a decomposition field) then a is said to be seperable over F. In other words, a is seperable over F if $f(x) = (x-a) \prod_{i=1}^{n} (x-a_i)$ where $a, a_1, a_2 \ldots a_n$ are all distinct members of a decomposition field. If the element a is in an algebraic extension of F, but is not seperable over F, then a is said to be inseperable over F. (Refer to Van der Waerden, [13 ,section 38, "Seperable und Insep. Erweiterungen"]).

K is said to be a seperable extension of F if each element of K is seperable over F. If K is both a seperable and a finite extension of F, then as Van der Waerden's proof shows [13, section 40, Einfachkeit von Alg. Erweiterungen"] K is a simple extension of F.

If K is a finite extension of F, the set of elements in K seperable over F is a field (Refer to Van der Waerden [13, fine print at the end of section 39,"Vollkommene und Unvdl. Korper"]); therefore this set of seperable elements is a finite extension of F (possibly equal to F) or indeed, is a simple extension of F.

K is said to be a purely inseperable extension of F if K is composed entirely of elements in F and of a non-null set of elements inseperable over F. In this case the defining equations of each element in K (not in F) is of the form $x^{p^n} - b = 0$ where b is in F and p^n is a power of a prime integer p which is the characteristic of F. (If n is a least positive integer such that na $=$ 0 for all a in F, then n is termed the characteristic of F) (Refer: Van der Waerder [13 , section 38, "Seperable und. Insep. Erweiterungen"])

Section 5. Group of automorphisms: normal extension

Again let K be a finite algebraic extension of the field F. An automorphism of K is defined to be a (ring) isomorphism of K onto itself. The automorphism, σ , of K is termed an F-automorphism if $\sigma(a) = a$ for all a in F. The set of all distinct automorphisms of K are elements of a group. Denote this set by $\mathcal{G}$. If σ , ρ are in $\mathcal{G}$ then the group operation $\sigma \circ \rho$ is defined as follows: for all a in K, $(\sigma \circ \rho)(a) = (\sigma\, \rho(a)\ )$. Denote by F' the set $\{ a \text{ in } K / \sigma(a) = a \text{ for all } \sigma \in \mathcal{G} \}$. Then F' is a field containing F. In case F' $=$ F, then K is termed a normal extension of F, the group $\mathcal{G}$ of automorphisms is called the Galois group K over F and is denoted by $\mathcal{G}_F^K$. K is a normal extension of F if and only if K is the decomposition field of a seperable polynomial f(x) in F(x). For details,(refer to : [1], Sections IIF and IIH)

Section 6. Least normal closure:

Let K and F be as above. Denote by S the complete set of elements in K that are seperable over F. As provided by section 4 of this appendix (3rd para.) let S = F [a] where a is in S, and let f(x)=) be the defining equation of a over F. Set M equal to a decomposition field of f(x) over S. Then M is also a decomposition field of f(x) over F and is, consequently, a normal extension of F.

Let K' denote the field $M[\alpha_1, \alpha_2 - \cdots \alpha_m]$ where $[\alpha_i]_{i=1}^{i=n}$ is a basis of K over F. K' is termed the least normal closure of k while M is termed the maximal seperable subfield of K' (or also the maximal seperable subfield determined by K). It follows that unless K' = M, K' is a purely inseperable extension of M. Proof below:

K' $\not\leq$ M only if K $\not\leq$ S. If K$\not\leq$ S, then K' may be represented as $M[\alpha_1', \alpha_2', \cdots \alpha_m']$ where the $[\alpha_j']_{j=1}^{j=m}$ are in K but not in S. The $[\alpha_j']_{j=1}^{j=m}$ are inseperable over F and therefore have defining equations over F of the form $x^{p^n} - a = 0$ where p is the characteristic of F (See section 3 of app.). As provided in the discussion under the subheading "Wurzel Korper" (Van der Waerden, [13 , section 39, " Seperable und Insep. Erweiterungen"]) K' may be obtained as the result of successively adjoining a set of pth roots. In other words, there is a finite chain of fields, $M=K_0 \leq K_1 \leq K_2 \leq K_3 \ldots\ldots\ldots K_{n-1} \leq K_n = K$ such that $k_i = K_{i-1}[u_i]$ where u_i is not in K_{i-1} but is a root of a polynomial in $K_{i-1}(x)$ of the form $x^p - a = 0$, $1 \leq i \leq n$. As indicated in the course of the proof of Van der Waerden's statement II [13, section 39, "Seperable und Insep. Erweiterungen." (Also see above reference in regard to pth roots being unique)], this polynomial of fomx^p - a = 0 is irreducible in $K_{i-1}(x)$.

The defining equation of u is therefore of the form $x^p - a = 0$. If a is in K_i and not in K_{i-1} than a $=\sum_{i=0}^{p-1} b_i u^i$ ($b_i \neq 0$ for some $i > 0$; $\left[b_i\right]_{i=o}^{i=p-1}$ in k_{i-1}). By algebraic manipulations it follows $u_i = \sum_{i=0}^{p-1} c_i a^i$ ($\left[c_i\right]_{i=1}^{i=p-1}$ in K_{i-1}). Therefore a cannot be seperable over K_{i-1} (See App. III, para.3). The defining equations over K_{i-1} for the element a is of the form $x^{p^r} + c_1 x^{pr-1} + c_2 x^{p^{r-2}} + \ldots\ldots\ldots c_r =$). (Refer to Van der Waerden, [13, first italicized statement of section 39, "Seperable un Insep. Erweiterungen."].) In view of app. II.3, last para., the defining equation over M of the element a is of the form $x^{p^s} + d_1 x^{p^{s-1}} + d_1 x^{p^{s-2}} + \ldots\ldots + d_{r'} = 0$. Thus each element a of K' not in M is inseperable over M (See above reference.).

Additional remarks: The least normal closure K' of K can be obtained as a decomposition field of a polynomial f(x) in F(x). The polynomial f(x) must be chosen so that its roots include all elements not in F of a basis of K over F; f(x) must be chosen to have the least degree for which the first condition is possible.

Section 7. Defining equation in a normal extension

Let f(x) be a monic, irreducible polynomial in F(x). Let $u_i \, {}_{i=1}^{i=n}$ be the complete set of roots of f(x) in a decomposition field. Then the coefficients of $f(x) = x^n + a_1 x^{n-1} + a_n x^{n-2} + \ldots\ldots + a_n$ are the so-called symmetric functions of the $u_i \, {}_{i=1}^{i=n}$. Fo $1 \leq k \leq n$, the coefficient a_k equals the result of adding together all the products $u_{i_1} u_{i_2} \ldots\ldots u_{i_k}$ involving k different U's: for each set of K distinct u_i's, $1 \leq i \leq n$, there is exactly one term equal to the product of the set of U_i's.

For example, $a_n = \prod_{i=1}^{m} u_i$; $a_{n-1} = \sum_{i=1}^{m} \left(\prod_{\substack{k=1 \\ k \neq i}}^{m} u_k\right)$; $a_1 = u_1 + u_2 + \dots\dots\dots + u_n$.

Let K be a finite and normal extension of F, and let u be in K, but not in F. The defining equation for u over F is then $f(x) = 0$ as follows: $f(x) = \prod_{i=1}^{m} (x - \sigma_{ij} u)$ where the $\left[\sigma_{i_j}\right]_{j=1}^{j=m}$ are chosen in such a way that the greatest possible number of $\left[\sigma_{i_j}\right]$ appear subject to the restriction that $\sigma_{i_j} u \neq \sigma_{i_k} u$ for $i \neq k$. [1, lemma following theorem 15, section H.]

Appendix IV

COMPLETE FIELDS

Section 1. Completion of a field with respect to a valuation

Let F be a field on which is defined a valuation v. Let a be an element of F. The absolute value of a with respect to v, denoted by $/a/_v$ is defined to be 0 if a = 0 and to be $\frac{1}{2^{v\ (a)}}$ _ for a in $F+$. ($\frac{1}{a}$ means a^{-1}.) It follows that $/a+b/_v = \frac{1}{2^{v(a+b)}} \leq \frac{1}{2^{\min \{v(a),\ v(b)\}}} = \max \left\{ \frac{1}{2^{v(a)}},\ \frac{1}{2^{v\ (b)}} \right\} \overset{\max}{=} \{/a/_v,\ /b/_v\}$. Thus the absolute value, / /, is a norm function (refer: Newmann, [10, p. 19]) on F just as does the usual absolute value defined on the rationals. The statement that $/\ /_v$ a norm function means that $/\ /_v$ is a mapping of F into the rationals (or more generally, into an ordered set containing the rationals) such that:

(i) $/a/_v \geq 0$ for all a in F; $/a/_v =$) if and only a = 0.

(ii) $/a+b/_v \leq \max\ /a/_v,\ /b/_v\ \leq\ /a/_v + /b/_v$

(iii) $/ab/_v = /a/_v\ /b/_v$

A sequence or set of elements of F, $\{a_i\}_{i=1}^{i=\infty}$ is said to be a fundamental sequence with respect to $/\ /_v$ if for every $\varepsilon > 0$ (ε is presumed to be a rational number) there is an index N such that $/a_m - a_n/_v < \varepsilon$ whenever both m and n exceed N. The sequence $\{a_i\}_{i=1}^{i=\infty}$ is said to converge with respect to to the element a in F if for every $\varepsilon > 0$ there is an index N such that $/a-a_n/ < \varepsilon$ for every $n > N$.

In the case of / / defined on the rationals it is not true that for every fundamental sequence (with respect to / /) there is a rational number to which the sequence converges (with respect to / /). However the rationals may be embedded in a "larger" field, the field of real numbers, and a mapping with the properties (i), (ii) and (iii) may be so defined that every fundamental sequence of real numbers converges to some real number.

In the case at hand, if the valuation v is discrete, rank one then again there is a field in which F is embedded and such that that a norm function can be defined on in a manner so taht each fundamental sequence converges to an element of Ω. Specifically there is a field with the following properties:

(i) F can be embeded in Ω.

(ii) There is a mapping, $/\ /_v$ from into the rationals which has the above properties of a norm function. Furthermore, Ω, is complete with respect to $/\ /_{\bar{v}}$: Every fundamental sequence (with respect to $/\ /_{\bar{v}}$) converges to an element of Ω.

(iii) $/\ /_{\bar{v}}$ coincides with $/\ /_v$ on F. In other words if φ is the mapping of F onto an isomorphic subset of Ω, then for all a in F, $/a\ /_v = /\varphi\,(a)/_{\bar{v}}$

(iv) $\left\{x \in \Omega \,\middle/\, \begin{array}{l}\text{there exists a sequence } \left[a_i\right]_{i=1}^{i=\infty} \text{ in F that} \\ \text{converges to x with respect to } /\ /_v\end{array}\right\}$ equals Ω.

(v) If the sequence of F, $\left[a_i\right]_{i=1}^{i=\infty}$ converges to a (with respect to $/\ /_{\bar{v}}$) then the $/\ a/_{\bar{v}}$ equals limit $\left\{/a_i/_v\right\}_{i=1}^{i=\infty}$. Here "limit" means the usual limit of a sequence of rational numbers, in this case the sequence of absolute values of the $\left[a_i\right]_{i=1}^{i=\infty}$

The field Ω is termed a completion of F with respect to v. In view of the isomorphism of F with a subset of Ω (i) and the equality of $/\ /_{\bar{v}}$ and $/\ /_v$ on correspcnding members (iii), the absolute value mapping on Ω will be indicated simply by $/\ /_v$.

Property (iv) guarantees that "the" completion will be a "smallest" field satisfying (i), (ii), (iii) and (v). In other words, if there is mapping $/ \; /_v'$ of a field Ω' into the rationals and if all the conditions excepting (iv) are satisfied by $/ \; /_v'$ on Ω' then Ω can be embedded in Ω' in such a way that $/ \; /_{\bar{v}}$ and $/ \; /_v'$ are equal for corresponding elements.

The significance of conditions (v) lies in the fact that it enables the valuation v to be extended to the field Ω. If $\left[a_i\right]_{i=1}^{i=\infty}$ converges to a (with respect $/ \; /_v$) then $/a/_v$ is the limit of the rational numbers $\left[\frac{1}{2^{\,v(a_i)}}\right]_{i=1}^{i=\infty}$. Then $/a/_v$ is either $\frac{1}{2^n}$ for some integer n or is zero. Then v(a) is defined as n or as ∞ respectively. In view of (ii), v defined on Ω in this way has the properties of a discrete (rank one) valuation. In view of (iii) this "new" valuation v is indeed an extention of the valuation on F.

Details of this section of the appendix are discussed in Wan der Waerden. [13, sect. 67, "Reelen Zahlen", and sect. 74, "Perfeckte Erweiterungen"].

Section 2. Norm with Respect to a Completion

Suppose Ω is complete with respect to $/ \; /_v$ where v is a valuation on Ω. Let Ψ be a finite algebraic extention of Ω with basis $(w_1 \ldots\ldots w_n)$ over Ω. Suppose a is in Ψ. Let $w_i a = \sum_{j=1}^{m} c_{ij} w_j$, $1 \le i \le n$, c_{ij} in Ω, $1 \le i \le n$, $1 \le j \le n$. Define $N'^{\Psi}_{\Omega}(a) = /\det(c_{ij})/_v$. Then $N'^{\Psi}_{\Omega}(a)$ is in fact defined independently of the choice of basis for Ψ over Ω. Indeed, if $x^m + b_1 x^{m-1} \ldots\ldots + b_{m-1} x + b_m = 0$ is the defining equation for a, then $N'^{\Psi}_{\Omega}(a) = \sqrt[m]{/b_m/_v}$. If a and b are in Ψ, it can be shown $N'^{\Psi}_{\Omega}(ab) = N'^{\Psi}_{\Omega}(a)\, N'^{\Psi}_{\Omega}(b)$. Define $N_{\Omega}(a)$ as $v(b_m)/m$. Then the norm with respect to Ω, N_{Ω}, is related to N'^{Ψ}_{Ω} by: $N_{\Omega}(a) = N'^{\Psi}_{\Omega}(a)$.

It follows that for a and b in Ψ, $N_{\Omega}(ab) = N(a) + N(b)$; also as a corallary to Hensel's lemma $N(a+b) \leq \min\{N_{\Omega}(a), N_{\Omega}(b)\}$. Trivially $N_{\Omega}(a) = v(a)$ for all a in Ω. Thus N indeed defines a prolongation of v from Ω to Ψ and indeed N is the only possible prolongation of v to Ψ.

For a detailed discussion of N'^{Ψ}_{Ω} refer to Wan der Waerden, [13, section 71, "Normen und Spuren"]; for discussion of rest of section refer to [13, section 76, "Bewerttung von Alg. Erweit."].

Section 3. Congruenence, relatively prime

Let A be an ideal of a ring R and let a be an element of R. Then b is said to be congruent to c mod A, written $b \equiv c \bmod A$, if b-c is in the ideal A; b is said to be congruent to c mod a, $b \equiv c \bmod a$, if b-c is in the principle ideal $R(a)$.

Let the ring R be a subset of the field F and let f(x) and g(x) be polynimials in R(x), that is polynomials of F(x) whose coefficients are in R. Then $f(x) \equiv g(x) \bmod A$ means that the coefficient of x^i in f(x) is congruent mod A to the coefficient of x^i in g(x) mod A for each i, $1 \leq i \leq \max\{\text{degree of } f(x), \text{degree of } g(x)\}$.

Let v be a valuation on the field F. A polynomial is said to be primitive (or primitive with respect to v if there are other valuations on F) if the polynomial is in $\bar{O}_v(x)$ where $\bar{O}_v$ is the valuation ring but at least one of the coefficients is not in the prime ideal $P(v)$.

The polynomials g(x) and h(x) in $\bar{O}_v(x)$ are said to be relatively prime mod $P(v)$ if: whenever both g(x) and h(x) are multiples of a polynomial k(x) in $\bar{O}_v(x)$, then k(x) is congruent to a unit of $\bar{O}_v(x)$ mod $P(v)$. The polynomials g(x) and h(x) are relatively prime mod $P(v)$ if and only if there are polynomials m(x) and n(x) in $\bar{O}_v(x)$ such that $m(x)g(x) +$

$n(x)h(x) \equiv 1 \bmod P(v)$. For the proof of this last statement, see Van der Waerden [13, section 18, "Euclidische Ringe" and section 23, "Factorzelegung" (refer to main theorem following section heading; recall statement I.7)].

The degree of a polynomial in $\bar{O}_v(x) \bmod P(v)$ is the maximal index i such that the coefficient of x^i is not congruent to zero mod $P(v)$.

Section 4. Statement of Hensel's Lemma

Hypothesis: The valuation v is defined on the field Ω; Ω is complete with respect to v, has valuation ring $\bar{O}_v$ with prime ideal $\mathfrak{p}_v$. f(x) is a primitive polynomial in $\bar{O}_v(x)$. G(x) and H(x) are polynomials in $\bar{O}_v(x)$ such that G(x) and H(x) are relatively prime mod $\mathfrak{p}_v$ and such that $f(x) \equiv G(x)\, H(x) \bmod \mathfrak{p}_v$.

Conclusion: There are polynomial g(x) and h(x) in $\Theta_v(x)$ such that $f(x) = g(x)\, h(x)$, $g(x) \equiv G(x) \bmod \mathfrak{p}_v$, $h(x) \equiv H(x) \bmod \mathfrak{p}_v$, and the degrees of g(x) and h(x) equal the degrees mod $\mathfrak{p}_v$ of G(x) and H(x) respectively.

This result, known as Hensel's lemma, is proved in Van der Waerden [14, section 76, "Bewertung von Alg. Erweit."].

The significance of the lemma is that it provides a condition under which a polynomial is irreducible in $\Omega(x)$: if f(x) is equal mod $\mathfrak{p}_v$ to the product of two polynomials (relatively prime mod $\mathfrak{p}_v$) and if each of these polynomials has degree mod $\mathfrak{p}_v$ less then the degree of f(x), then f(x) is reducible in $\Omega(x)$.

Section 5. Properties of p-adic completions

Let v be a valuation on the rationals R corresponding to some prime integer p (refer example 1, chapter V) and let Ω_v be the completion of R with respect to v. According to Van derWaerden [13 section 34, "Perfeckta Erweiterungen"], each element of Ω may be represented in a power series $\sum_{i=m}^{\infty} a_i p^i$ in which each a_i is either zero or else has value zero, and in which m is an integer, possibly a negative integer. The sum of series, $\sum_{i=m}^{\infty} a_i p^i + \sum_{i=n}^{\infty} b_i p^i$ is defined as the series $\sum_{i=M}^{\infty} (a_i + b_i) p^i$ (a_i or b_i are presumed to be zero for $M \leq I \leq m$ or $M \leq I \leq M$) and the product is defined to be the series $\sum_{i=m}^{\infty} a_i p^i \circ \sum b_i p^i = \sum c_i p^i$ where each c_i is the result of adding together all of the $(a_j + b_k)$ such that $j + k = i$. Any two series $\sum_{i=m}^{\infty} a_i p^i$ and $\sum_{i=M}^{\infty} b_i p^i$ are considered equal if and only if $\sum_{i=m}^{\infty} (a_i - b_i) p^i = 0$; a series is considered equal to zero if and only if it consists of (at most) finitely many non-zero terms that together add (addition operation in R) to zero.

Let k be the first index of terms in the series corresponding a, $\sum_{i=m}^{\infty} a_i p^i$, such that $a_i \neq 0$. Then $v(a) = v\left((a_k) + \sum_{i=k+1}^{\infty} a_i p^i\right)$. Now since $v(a_i p^i) = i$ or ∞ for all i, then $\sum_{i=k+1}^{\infty} a_i p^i$ converges in Ω (refer to paragraphs 2 and 3 of above reference): by property (v) of the completion (refer app., section 1), $v(\sum_{i=k+1}^{\infty} a_i p^i) > k$. Therefore, $v(a) = v(a_k p^k) = K$ and the valuation ring of Ω is the set of power series $\sum_{i=0}^{\infty} a_i p^i$.

BIBLIOGRAPHY

1. Artin, Emil. Lectures in Galois Theory, Notre Dame Mathematical Lectures No. 2., copyright 1942, 1944, University of Notre Dame, Notre Dame, Indiana. Ann Arbor: Edwards Brothers, Inc., 1950.

2. Jacobson, N. H. Lectures in Abstract Algebra. Vol. I, The University Series in Higher Mathematics, M. H. Stone, chairman of editorial board; New Haven. D. Van Nostrand Company, 1951.

3. Kelley, J. L. General Topology. University Series in Higher Mathematics, M. H. Stone, chairman of editorial board; Berkeley. D. Van Nostrand Company, 1955.

4. Kershner, R. B., and Wilcox, L. R. The Anatomy of Mathematics. New York: The Ronald Press Company, 1950.

5. Krull, Wolfgang. Idealtheorie, copyright 1935, Berlin. New York: Chelsea Publishing Company, 1950.

6. Krull, Wolfgang. "Allgemeine Bewertungtheorie," Journal fur die Reine und Angewandte Mathematik, 167:160-96, 1932. Kurt Hensel, editor. Berlin: Walter de Gruyter and Company, W 10.

7. MacDuffie, C. C. "Vectors and Matrices," Carus Mathematical Monographs, No. 7.; Mathematical Association of America. Menesha, Wisconsin: George Banta Publishing Company, 1949.

8. McCoy, N. H. "Rings and Ideals," Carus Mathematical Monographs, No. 8; Mathematical Association of America. Baltimore: The Waverly Press, 1948.

9. Nagell, T. Introduction to Number Theory. New York: John R. Wiley and Sons, Inc., 1951.

10. Newmann, M. H. A. Elements of the Topology of Plane Sets of Points. Cambridge, England: University Press, 1951.

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

12. Stewart, B. M. Theory of Numbers. New York: The Macmillan Company, 1952.

12a. Van derWaerden, B. L. "Zur Productzurlegung der Ideale in ganz-abgeschlossenen Ringen," Mathematische Annalen, 101:293-308. Berlin: Verlag von Julius Springer. ("Gegenwartig herausgegeben von David Hilbert")

12b. Van derWaerden, B. L. "Zur Idealtheorie der gans-Abgeschlossenen Ringe," Mathematische Annalen, 101:309-311. Berlin: Verlag von Julius Springer.

13. Van derWaerden, B. L. Moderne Algebra. Vol. I. New York: Frederick Ungar Publishing Company, 1940.

14. Van derWaerden, B. L. _Moderne Algebra_. Vol. II. New York: Frederick Ungar Publishing Company, 1940.

15. Van derWaerden, B. L. _Modern Algebra_, Vol. I, English Edition. 1949.

16. Wright, E. M., and Hardy, G. H. _An Introduction to the Theory of Numbers_. Oxford: Oxford University Press, n.d.