A STUDY OF VALUATIONS

OF GENERAL RANK

By

EDWARD NEWTON MOSLEY

Bachelor of Arts
Arkansas College
Batesville, Arkansas
1960

Master of Science
University of Arkansas
Fayetteville, Arkansas
1962

Submitted to the Faculty of the Graduate College
of the Oklahoma State University
in partial fulfillment of the requirements
for the Degree of
DOCTOR OF EDUCATION
May, 1970

A STUDY OF VALUATIONS

OF GENERAL RANK

Thesis Approved:

Gerald K. Goff
Thesis Adviser

John Jewett

Robert P. Alciatore

D. Durham
Dean of the Graduate College

ACKNOWLEDGMENTS

I wish to express my appreciation to all who have helped me in the preparation and writing of this dissertation. Particular gratitude is due to Dr. Gerald K. Goff, my dissertation adviser, who not only made valuable suggestions concerning this paper, but also encouraged me in my work and served as a much needed morale builder. Special thanks also go to Dr. John Jewett, my committee chairman; to Dr. Robert Alciatore, a member of my advisory committee; and to Dr. Jeanne Agnew, who is responsible for my interest in this topic; for their cooperation during my study at Oklahoma State University.

Finally, I express my appreciation to my wife, Mary, for her patience and understanding and to my parents for their assistance and encouragement throughout my graduate work.

TABLE OF CONTENTS

Chapter		Page
I.	INTRODUCTION	1
II.	VALUATIONS OF GENERAL RANK	4
	Ordered Groups	4
	Valuations	6
	Valuation Rings and Places	9
	Rank	16
III.	RANK ONE VALUATIONS	22
	Rank One Ordered Groups	22
	Non-Archimedian Valuations	33
	Convergence and Completeness	43
	Equivalent Valuations	46
IV.	EXTENSIONS	51
	Mappings and Places	51
	Valuations	60
	Normed Linear Spaces and Uniqueness	64
V.	SUMMARY	75
BIBLIOGRAPHY		77

CHAPTER I

INTRODUCTION

A valuation is a generalization of the absolute value function of the real numbers. This notion was probably first sparked by Kurt Hensel in 1908 in his book Theorie der Algebraischen Zahlen. Hensel introduced a new number field called the field of p-adic numbers. His treatment was somewhat informal and intuitive (cf. MacDuffee [12], p. 501). Later in 1913, J. Kurschak was interested in the formulation of an absolute value type function on an arbitrary field. He wanted the function to have the same basic properties as the absolute value functions on the real and complex numbers. The problem was solved by merely postulating such a function. That is, if given a field F then let $|\ |:F\to R$ be a real valued function such that $|x|\geq 0$, $|x|=0$ if, and only if $x=0$, $|xy|=|x||y|$ and $|x+y|\leq|x|+|y|$. It is now popular to treat Hensel's p-adic numbers as the completion of the rational numbers with respect to a special kind of absolute value (valuation) of the rationals. This completion process is similar to the development of real numbers by Cauchy sequences (cf. MacDuffee [12], p. 501).

However, many of Kurschak's conservative contemporaries were disgusted with his newly concocted absolute value or valuation. They considered it as a disreputable trick because he postulated what he wanted to get. It almost seemed that Kurschak with a divine wave of the hand had said, "Let there be absolute values," and there were absolute values (cf. Bell [4], p. 160). But, it can be shown that every field has at least one valuation, and also the ideas of Hensel and Kurschak have generated a rich theory of valuations. Valuations have played an important role in the development of algebraic number theory and algebraic geometry (cf. Bachman [2], p. v). Some of the mathematicians that have since contributed to the development of valuation theory include Chevalley, Krull, Ostrowski, Cohen, and Zariski (cf. Schilling [16], p. iv).

In Chapter II of this paper many of the basic ideas concerning valuations of rank n are introduced. Ordered groups of rank n, places, valuation rings, and non-archimedian valuations are some of the topics included. Many examples of these structures and mappings are given. It is shown that there is a one-to-one correspondence between places and non-archimedian valuations up to an isomorphism. The framework for the study of valuations is constructed in this chapter.

Much work has been done on the subject of rank one valuations, and in particular on rank one non-archimedian valuations. In fact many writers require a valuation to be a rank one non-archimedian valuation or at least require it to be rank one (cf. McCarthy [14], Borevich and Shafarevich [5] and Cassels and Fröhlich [7]). Chapter III is concerned with rank one valuations. In this chapter it is shown that a rank one ordered group is isomorphic to a subgroup of the multiplicative group of positive real numbers, and from this it is shown how a definition of a rank one valuation such as Kurschak's is a specialization of the definition of a rank n valuation. Also, a rank one valuation is characterized when the non-archimedian property is assumed, and a non-archimedian valuation is characterized when rank one is assumed. The notions of convergence of sequences and completeness of a field with respect to a rank one valuation are presented. Finally the chapter concludes with a discussion of equivalent valuations.

Chapter IV deals with some of the standard extension problems concerning mappings that resemble valuations, places and valuations. The chapter ends with a uniqueness theorem concerning the extension of a rank one non-archimedian valuation.

The main sources of information that are used in the paper are the works by Artin [1], Bachman [2], and Schilling [16].

CHAPTER II

VALUATIONS OF GENERAL RANK

Ordered Groups

Before formulating a general definition of a valuation, the concept of an ordered group will be considered.

Definition 2.1. Let G be a multiplicative group. G is an ordered group if, and only if there exists a normal subsemigroup S of G such that $G = S \cup \{1\} \cup S^{-1}$ where $S^{-1} = \{a^{-1} \in G \mid a \in S\}$ and S, $\{1\}$ and S^{-1} are mutually disjoint.

An example of an ordered group is the group G of all positive real numbers under the operation of multiplication. This can be shown by letting $S = \{a \in G \mid a < 1\}$. Then it follows that $G = S \cup \{1\} \cup S^{-1}$ where S, $\{1\}$ and S^{-1} are mutually disjoint.

An order relation $\succ$ can be defined on an ordered group G. Let a, b $\in$ G. Define $a \succ b$ if, and only if $a\,b^{-1} \in S$, where $a \succeq b$ means $a \succ b$ or $a = b$.

Theorem 2.2. Let G be an ordered group. Then

(a) a, b $\in$ G imply $a \succ b$ or $a = b$ or $b \succ a$

(b) a, b, $\in$ G, $a \succ b$ and $b \succ c$ imply $a \succ c$

(c) a, b $\in$ G and $a \succ b$ imply $b^{-1} \succ a^{-1}$

(d) a, b, c, d $\in$ G, $a \succ b$ and $c \succeq d$ imply $ac \succ bd$ and $ca \succ db$.

Proof:

(a) a, b $\in$ G implies $ab^{-1} \in G = S \cup \{1\} \cup S^{-1}$ since G is a group. Therefore, ab^{-1} is in S or is equal to 1 or is in S^{-1}. If ab^{-1} is in S then $a \prec b$. If $ab^{-1} = 1$ then $a = b$. If ab^{-1} is in S^{-1} then $(ab^{-1})^{-1} = ba^{-1}$ is in S which implies $b \prec a$.

(b) $a \prec b$ and $b \prec c$ imply $ab^{-1} \in S$ and $bc^{-1} \in S$ which imply $ac^{-1} = (ab^{-1})(bc^{-1}) \in S$ since S is a semigroup. This implies $a \prec c$.

(c) $a \prec b$ implies $ab^{-1} \in S$ which implies $b^{-1}a = b^{-1}(ab^{-1})b$ since S is normal; hence $b^{-1} \prec a^{-1}$.

(d) $a \prec b$ and $c = d$ imply $ab^{-1} \in S$ which implies $c(ab^{-1})c^{-1} \in S$ since S is normal. Therefore, $(ca)(cb)^{-1} \in S$, and so $ca \prec cb$ which implies $ca \prec db$. Also, $a(cc^{-1})b^{-1} = (ac)(bc)^{-1} \in S$; thus $ac \prec bc$ and $ac \prec bd$. If $c \prec d$ then $ac \prec bc$ and $bc \prec bd$. Then $ac \prec bd$ by part (b). Similarly it can be shown that $ca \prec db$.

In the ordered group G of all positive real numbers the order relationship $\prec$ is the same as the natural ordering $<$. This is true because $a < b$ if, and only if $ab^{-1} \in S$ if, and only if $ab^{-1} < 1$ if, and only if $a < b$.

<u>Theorem 2.3</u>. Every non-trivial ordered group is infinite.

Proof: Let G be a non-trivial ordered group. Let $a \in G$. Suppose $1 \prec a$. It can be shown by induction that $1 \prec a^n$ for any positive integer n. The statement is certainly true for n = 1. Assume true for some $n \geq 1$. This implies $1 \prec a^n$. Therefore, $1 \prec a \prec a^{n+1}$ by Theorem 2.1 (d) and (b). In a similar way it can be shown that $a^n \prec 1$ for any negative integer n. Now, suppose $a \prec 1$. Again by induction it follows that $a^n \prec 1$ for any positive integer n, and

$1 \ngtr a^n$ for any negative integer n. Therefore, if $a \neq 1$ then $a^n \neq 1$ for any non-zero integer n.

Consider the sequence $\{a^n\}$ where $a \in G$ and $a \neq 1$. Suppose there exists two positive integers n and m such that $n \neq m$ but $a^n = a^m$. Then $a^{n-m} = 1$. This contradicts the above result that $a^n \neq 1$ for any non-zero integer n. This implies that G contains a sequence of distinct terms and is therefore infinite.

The following corollary is a result of the proof of this theorem.

Corollary 2.4. The only element of an ordered group that has finite order is the group identity.

Valuations

Now a general definition of a valuation can be constructed. The notion of an ordered group is important in the discussion because a valuation is a mapping from an arbitrary field onto an ordered group and an additional element. The definition is stated formally as follows:

Definition 2.5. Let K be a field and G an ordered group with an additional operation defined on it which is denoted by +. Let z be an additional element for G such that for all $a \in G$, $z \ngtr a$, $az = za = z$ and $a + z = z + a = a$. A valuation is a mapping $v:K \to G\cup\{z\}$ such that $v(K) = G\cup\{z\}$ and

(a) $v(a) = z$ if, and only if $a = 0$

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

(c) $v(a+b) \ngeq v(a) + v(b)$.

The group G is sometimes called the value group of v.

It should be pointed out that an extra operation can always be introduced on an ordered group, for let $a + b = \max(a,b)$. This is well defined because exactly one of the following will be true: $a \succ b$, $a = b$, or $b \succ a$. Also, $c \max(a,b) = \max(ca, cb)$ and $\max(a,b)c = \max(ac,bc)$. This implies $c(a+b) = ca + cb$ and $(a+b)c = ac + bc$. If this max operation is used then (c) in Definition 2.5 becomes $v(a+b) \succeq \max\big(v(a), v(b)\big)$. This property is given a special name.

<u>Definition 2.6</u>. If a valuation v has the property $v(a+b) \succeq \max\big(v(a), v(b)\big)$ then v is said to be a non-archimedian valuation.

Consider the absolute value function $|\,|:R \to G \cup \{0\}$ where R is the field of real numbers and G is the ordered multiplicative group of positive real numbers. It is easily verified that $|\,|$ is a valuation. Also, the function $t:K \to \{1\} \cup \{z\}$ where K is a field and t is defined as $t(a) = 1$ if $a \neq 0$ and $t(0) = z$ is a valuation known as the trivial valuation. The valuation t is also non-archimedian. Let $a, b \in R$. If $a \neq 0$ or $b \neq 0$ then $t(a) = 1$ or $t(b) = 1$. This implies $t(a+b) \succeq 1 = \max\big(t(a), t(b)\big)$. If $a = b = 0$ then $t(a+b) = t(o) = z = \max\big(t(a), t(b)\big)$. The next three theorems are modifications of some theorems and problems in Bachman [2].

<u>Theorem 2.7</u>. Let $v:K \to G \cup \{z\}$ be a valuation. Then

(a) $v(1) = v(-1) = 1$ and $v(-a) = v(a)$

(b) $v(a/b) = v(a)/v(b)$ if $b \neq 0$.

Proof:

(a) First of all, $v(1) = v(1 \cdot 1) = v(1)v(1)$ which implies $v(1) = 1$. Secondly, $1 = v\big((-1)^2\big) = v^2(-1)$ which implies $v(-1) = 1$ by

Corollary 2.4. Also, $v(-a) = v(-1 \cdot a) = v(-1)v(a) = v(a)$.

(b) Let $b \in K$ such that $b \neq 0$. Then $v(b^{-1}b) = v(1) = 1$. This implies $v(b^{-1})v(b) = 1$ which implies $v(b^{-1}) = 1/v(b)$. Therefore, $v(a/b) = v(ab^{-1}) = v(a) \cdot v(b^{-1}) = v(a)\left(1/v(b)\right) = v(a)/v(b)$.

<u>Theorem 2.8</u>. The only valuation of a finite field is the trivial valuation.

Proof: Let $v: K \to G \cup \{z\}$ be a valuation defined on a finite field $K = \{a_1, \ldots, a_n, a_{n+1}\}$. Let $a \in K$ such that $a \neq 0$. Then $a^n = 1$ which implies that $v^n(a) = v(a^n) = v(1) = 1$ by Theorem 2.7. This implies $v(a) = 1$ by Corollary 2.4. Therefore, v is the trivial valuation.

<u>Theorem 2.9</u>. If $v: K \to G \cup \{z\}$ is a non-archimedean valuation then $v(a_1 + \ldots + a_n) \preceq \max\left(v(a_1), \ldots, v(a_n)\right)$. If $v(a_j) \prec v(a_1)$ for $j = 2, \ldots, n$ then $v(a_1 + \ldots + a_n) = v(a_1)$.

Proof: Let $\{a_i\}$ be a sequence of elements of K. Then $v(a_1 + \ldots + a_n) \preceq \max\left(v(a_1), \ldots, v(a_n)\right)$ for $n = 2$ since v is non-archimedean. Assume true for some $n \geq 2$. Now, $v(a_1 + \ldots + a_n + a_{n+1}) \preceq \max\left(v(a_1 + \ldots + a_n), v(a_{n+1})\right) \preceq \max\left(\max\left(v(a_1), \ldots, v(a_n)\right), v(a_{n+1})\right) = \max\left(v(a_1), \ldots, v(a_n), v(a_{n+1})\right)$. Therefore, it has been shown by induction that the first part of the theorem is true.

Now, let $a_1, \ldots, a_n \in K$ such that $v(a_j) \prec v(a_1)$ for $j = 2, \ldots, n$. Then $v(a_1) = v\left((a_1 + \ldots + a_n) - (a_2 + \ldots + a_n)\right) \preceq \max\left(v(a_1 + \ldots + a_n), v(a_2 + \ldots + a_n)\right)$. If $v(a_1 + \ldots + a_n) \prec v(a_2 + \ldots + a_n)$ then $v(a_1) \preceq v(a_2 + \ldots + a_n) \preceq \max\left(v(a_2), \ldots, v(a_n)\right)$. This contradicts the fact that $v(a_j) \prec v(a_1)$ for $j \leq 2$. Therefore, $v(a_1) \preceq v(a_1 + \ldots + a_n) \preceq$

max $\left(v(a_1), v(a_2), \ldots, v(a_n)\right) = v(a_1)$. Hence, $v(a_1) = v(a_1 + \ldots + a_n)$.

Valuation Rings and Places

Valuation rings and places play an important role in the development of the theory of valuations. It will be shown that there is more or less a one-to-one correspondence between valuation rings and places, and later it will be shown that there is a similar relationship between valuation rings and non-archimedian valuations. Most of the theorems in this section can be found in Artin [1] and Bachman [2].

Definition 2.10. A subring V of a field K is called a valuation ring if, and only if $a \in K - V$ implies $a^{-1} \in V$. Let $P = \{a \in V \mid a^{-1} \notin V\}$ and let $U = V - P$. P is called the set of non-units of V, and U is called the set of units of V.

A trivial example of a valuation ring of a field K would be the ring $V = K$. The following example which can be found in Artin [1] is much more interesting.

Example 2.11. Let Q be the field of rational numbers. Let p be a fixed prime integer. Assume that every element of a/b of Q is in reduced form. Let $V = \{a/b \in Q \mid p \nmid b\}$. If $a/b, c/d \in V$ then $p \nmid bd$ since $p \nmid b$ and $p \nmid d$; hence $a/b - c/d = (ad - bc)/bd \in V$ and $(a/b)(c/d) = (ac)/(bd) \in V$. Therefore, V is a subring of Q.

Now, suppose $a/b \in Q - V$. This implies that $p \mid b$, and so $p \nmid a$ since $(a,b) = 1$. Thus, $(a/b)^{-1} = b/a \in V$ which makes V a valuation ring. Also, $P = \{a/b \in V \mid b/a \notin V\} = \{a/b \in V \mid p \mid a\}$, and $U = V - P = \{a/b \in V \mid p \nmid a\}$.

Theorem 2.12. Let V be a valuation ring in a field K. Then

(a) The set of non-units P of V is a unique maximal ideal of V.

(b) The set of units U of V is a multiplicative group.

(c) The field K is equal to $P \cup U \cup (P-\{0\})^{-1}$ and P,U and $(P - \{0\})^{-1}$ are mutually disjoint.

Proof:

(a) The ring V contains the field unity element, otherwise $1 \in K - V$ which implies $1 = (1)^{-1} \in V$, a contradiction. Let $a,b \in P$. This implies $a^{-1}, b^{-1} \notin V$ and $a-b \in V$. Suppose $a/b \in V$. Then $a/b-1 \in V$. Now, $(a-b)^{-1} \notin V$, otherwise $b^{-1} = (a-b)^{-1}(a/b-1) \in V$, which is a contradiction. Therefore, $a-b \in P$. Suppose $a/b \notin V$. Then $b/a \in V$, and by a similar argument it can again be shown that $a-b \in P$.

Let $a \in V$ and $b \in P$. This means that $ab \in V$, but $b^{-1} \notin V$. Also, $(ab)^{-1} \notin V$, otherwise $b^{-1} = a(a^{-1}b^{-1}) = a(ab)^{-1} \in V$. Therefore, $ab \in P$, and P is an ideal of V.

The ideal P is not equal to V since $1 \notin P$. Let I be an ideal of V such that $P \subset I$. Let $a \in I - P$. Then $a^{-1} \in V$ and $a^{-1}a \in I$ since I is an ideal. Therefore, $1 \in I$ and $I = V$. Thus P is a maximal ideal of V.

Let I be another maximal ideal of V. Suppose there exists $a \in I - P$. Then $a^{-1} \in V$, and $1 = a^{-1}a \in I$. Therefore, $I = V$ which contradicts the fact that I is a maximal ideal of V. Hence, $I - P = \varphi$ or $I \subseteq P$. But, this implies $I = P$ since $P \neq V$ and I is maximal. Thus, P is a unique maximal ideal of V.

(b) Let $a,b \in U$. Then $a, b, a^{-1}, b^{-1} \in V$. Therefore, $ab^{-1}, a^{-1}b \in V$. Thus, $ab^{-1}, (ab^{-1})^{-1} \in V$ which implies that $ab^{-1} \in U$. Hence U is a multiplicative subgroup of the field K.

(c) By Definition 2.10, $V = P \cup U$ with P and U disjoint. Therefore, to prove (c) it only remains to show that $K - V = (P - \{0\})^{-1}$. Let $x \in K - V$. Then $x^{-1} \in V$ by definition of V. But, $(x^{-1})^{-1} = x \notin V$, so $x^{-1} \in P$. Thus, $x \in (P - \{0\})^{-1}$ and $K - V \subseteq (P - \{0\})^{-1}$. If $x \in (P - \{0\})^{-1}$ then $x^{-1} \in P$ which implies $x^{-1} \in V$, but $x = (x^{-1})^{-1} \notin V$. Therefore, $x \in K - V$ and $(P - \{0\})^{-1} \subseteq K - V$. Hence, $K - V = (P - \{0\})^{-1}$.

This theorem implies that P is a prime ideal in V because a maximal ideal of a commutative ring with unity is also a prime ideal (cf. Barnes [3], p. 125).

Definition 2.13. Let K and F be fields. A map $\varphi : K \to F \cup \{\infty\}$ is called a place if, and only if

(a) $\varphi^{-1}(F) = V$ is a ring

(b) $\varphi \mid_V$ is a non-trivial homomorphism

(c) If $\varphi(a) = \infty$ then $\varphi(a^{-1}) = 0$.

Let p be prime in Z, the ring of integers. It is known that Z is a principal ideal domain (cf. Barnes [3], p. 112). Therefore, (p), the ideal generated by p, is a maximal ideal in Z. This implies Z/(p) is a field (cf. Barnes [3], p. 126). Let V be the ring defined in Example 2.11. Define a mapping $\varphi : Q \to Z/(p) \cup \{\infty\}$ in the following way. Let $\bar{a}$ denote the coset which contains a. Let $\varphi(a/b) = \bar{a}/\bar{b}$ if $a/b \in V$. If $a/b \notin V$ then let $\varphi(a/b) = \infty$. Now, certainly $\varphi^{-1}\big(Z/(p)\big)$ is a ring, namely V. Let $a/b, c/d \in V$. Then $\varphi(a/b + c/d) = \overline{(ad + bc)} / \overline{(bd)} = \overline{ad} / \overline{bd} + \overline{bc} / \overline{bd} = \varphi(a/b) + \varphi(c/d)$. Also, $\varphi(a/b \cdot c/d) = \overline{ac} / \overline{bd} = (\bar{a}/\bar{b})(\bar{c}/\bar{d}) = \varphi(a/b)\,\varphi(c/d)$. Therefore, $\varphi \mid_V$ is a homomorphism.

It is non-trivial since $\varphi(1) = \overline{1} \neq \overline{0}$. If $\varphi(a/b) = \infty$ then $a/b \notin V$. This implies $p \mid b$, $b/a = (a/b)^{-1} \in V$ and $\varphi(b/a) = \overline{b}/\overline{a} = \overline{0}$. Thus, φ is an example of a place.

Theorem 2.14. For every place there exists an associated valuation ring, and for every valuation ring there is an associated place.

Proof: Let $\varphi : K \to F \cup \{\infty\}$ be a place. Let $V = \varphi^{-1}(F)$. V is a subring of F by definition. If $a \in K$, but $a \notin V$ then $\varphi(a) = \infty$. Hence, $\varphi(a^{-1}) = 0 \in F$. Therefore, $a^{-1} \in \varphi^{-1}(F) = V$, and V is a valuation ring.

Let V be a valuation ring in a field K. Let P be the unique maximal ideal of V. Let the field V / P be denoted by F. Define a mapping $\varphi : K \to F \cup \{\infty\}$ in the following way. Let $\varphi(a) = \overline{a}$, the coset which contains a, if $a \in V$, and $\varphi(a) = \infty$ if $a \notin V$. It can readily be verified that φ is a place, for $\varphi^{-1}(F) = V$, a ring, $\varphi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \varphi(a) + \varphi(b)$ if $a,b \in V$, $\varphi(ab) = \overline{ab} = \overline{a}\,\overline{b} = \varphi(a)\varphi(b)$ if $a,b \in V$, and if $\varphi(a) = \infty$ then $a \in K - V$ which implies $a^{-1} \in P$; thus $\varphi(a^{-1}) = \overline{a^{-1}} = \overline{0}$.

Theorem 2.15. Let V be a valuation ring in the fields K_1 and K_2. Let $\varphi_1 : K_1 \to F_1 \cup \{\infty\}$ and $\varphi_2 : K_2 \to F_2 \cup \{\infty\}$ be two places such that $\varphi_1^{-1}(F_1) = \varphi_2^{-1}(F_2) = V$. Then there exists an isomorphism i, between $\varphi_1(V)$ and $\varphi_2(V)$ such that $i(\varphi_1(a)) = \varphi_2(a)$.

Proof: Let $a \in P$, the unique maximal ideal of V. Thus, $a^{-1} \in K_1 - V$ and $\varphi_1(a^{-1}) = \infty$. Therefore, $\varphi_1(a) = 0$ since φ_1 is a place. This means that $\varphi_1(P) = 0$. Similarly, $\varphi_2(P) = 0$. Now, let $a \in V$ such that $\varphi_1(a) = 0$. Now, if $a \notin P$ then $a^{-1} \in V$ and $\varphi_1(1) = \varphi(a\, a^{-1}) =$

$\varphi(a)\varphi(a^{-1}) = 0$. This means that $\varphi_1 \mid_V$ is a trivial homomorphism, a contradiction since φ_1 is a place. Thus, $a \in P$, and the kernal of $\varphi_1 \mid_V$ is P. Likewise it can be shown that the kernal of $\varphi_2 \mid_V$ is P.

Define $i:\varphi_1(V) \to \varphi_2(V)$ as $i(\varphi_1(a)) = \varphi_2(a)$ for all $\varphi_1(a) \in \varphi_1(V)$. Let $\varphi_1(a), \varphi_1(b) \in \varphi_1(V)$. Then $i(\varphi_1(a) + \varphi_1(b)) = i(\varphi_1(a+b)) = \varphi_2(a+b) = \varphi_2(a) + \varphi_2(b) = i(\varphi_1(a)) + i(\varphi_1(b))$. Also, $i(\varphi_1(a)\varphi_1(b)) = i(\varphi_1(ab)) = \varphi_2(ab) = \varphi_2(a)\varphi_2(b) = i(\varphi_1(a))(i\ \varphi_2(b))$. If $\varphi_1(a) = \varphi_1(b)$ then $\varphi_1(a-b) = 0$ which implies $a-b \in P$; hence $\varphi_2(a-b) = 0$ which implies $i(\varphi_1(a)) = \varphi_2(a) = \varphi_2(b) = i(\varphi_1(b))$. Thus, i is well defined. If $\varphi_1(a) = 0$ then $a \in P$ which implies $\varphi_2(a) = 0$. The function i is clearly onto; hence i is an isomorphism.

<u>Theorem 2.16</u>. For every non-archimedian valuation there exists an associated valuation ring, and for every valuation ring there exists an associated non-archimedian valuation.

Proof: Let $v:K \to G \cup \{z\}$ be a non-archimedian valuation. Let $V = \{a \in K \mid v(a) \ngeq 1\}$. Let $a,b \in V$. Then $v(a-b) \ngeq \max(v(a),v(b)) \ngeq 1$, and $v(ab) = v(a)v(b) \ngeq 1 \cdot 1 = 1$. Therefore, $a-b$, $ab \in V$, and V is a subring of K. Now, let $a \in K - V$. This implies $1 \ngeq v(a)$. Hence, Theorems 2.7 and 2.2 imply $v(a^{-1}) = 1/v(a) \ngtr 1$. Therefore, $a^{-1} \in V$, and V is a valuation ring. Also, it should be pointed out that $P = \{a \in V \mid v(a) \ngtr 1\}$ is the set of non-units of V. This is true because if $a \in P$ then $1 \ngtr v(a^{-1})$ which implies $a^{-1} \notin V$ and because if $a \in V$ and $a^{-1} \notin V$ then $1 \ngtr v(a^{-1})$ which implies $v(a) \ngtr 1$. It follows that the group of non-units is $U = V - P = \{a \in V \mid v(a) = 1\}$.

Now, let V be a valuation ring in a field K. Let P and U be the non-units and units of V respectively. It will now be established that the multiplicative quotient group $G = (K - \{0\})/U$ is an ordered group. Let $S = \left\{\bar{a} \in G \mid a \in (P - \{0\})\right\}$. If $\bar{a},\bar{b} \in S$ then $a,b \in (P - \{0\})$; whence $v(a)$, $v(b) \not> 1$. This implies $v(ab) = v(a)v(b) \not> 1$. Therefore, $\overline{ab} \in S$, and S is a subsemigroup of G. S is normal since G is abelian. It is clear that $S \cup \{1\} \cup S^{-1} \subseteq G$. Theorem 2.12 implies $K - \{0\} = (P - \{0\} \cup U \cup (P - \{0\})^{-1}$. Therefore, if $\bar{a} \in G$ then $a \in K - \{0\}$ which implies $a \in (P - \{0\})$ or $a \in U$ or $a \in (P - \{0\})^{-1}$. Thus $\bar{a} \in S$ or $\bar{a} = \bar{1}$ or $a^{-1} \in (P - \{0\})$. If $a^{-1} \in (P - \{0\})$ then $1/\bar{a} = \overline{a^{-1}} \in S$, and so $\bar{a} \in S^{-1}$. Hence, $\bar{a} \in S \cup \{\bar{1}\} \cup S^{-1}$ and $G = S \cup \{\bar{1}\} \cup S^{-1}$. Also, S, $\{\bar{1}\}$ and S^{-1} are mutually disjoint since $(K - \{0\})$ is the union of $(P - \{0\}$, U and $(P - \{0\})^{-1}$ which are mutually disjoint. Therefore, G is an ordered group.

Let z be an additional element such that $z \not> a$ and $az = za = z$ for all $a \in G$. Let $v: K \to G \cup \{z\}$ be a mapping defined as follows: $v(a) = \bar{a}$ if $a \neq 0$, and $v(0) = z$. Now, it will be shown that v is a non-archimedian valuation. It is clear that $v(a) = z$ if, and only if $a = 0$. Also, $v(ab) = \overline{ab} = \bar{a}\,\bar{b} = v(a)v(b)$. It now remains to show that $v(a+b) \not\geq \max\left(v(a), v(b)\right)$. Let $a,b \in (K - \{0\})$ and suppose $v(a) \not> v(b)$. This implies $\bar{a} \not> \bar{b}$, and so $\overline{ab^{-1}} \in S$ by definition of $\not>$. Thus, $ab^{-1} \in (P - \{0\} \subseteq V$, and $1 + ab^{-1} \in V$. Hence, $1 + ab^{-1} = 0$ or $1 + ab^{-1} \in (P - \{0\}$ or $1 + ab^{-1} \in U$. Therefore, $v(1+ab^{-1}) = z$ or $v(1+ab^{-1}) \in S$ or $v(1+ab^{-1}) = \bar{1}$. Hence, $v(1+ab^{-1}) \not\geq \bar{1}$. Then $v(b)v(1+ab^{-1}) \not> v(b)$ which implies $v(a+b) \not> v(b) = \max\left(v(a),v(b)\right)$. If $v(b) \not> v(a)$ then the argument is similar. If $v(a) = v(b)$ then $\bar{a} = \bar{b}$, and $\overline{ab^{-1}} = \bar{1}$. Therefore, $ab^{-1} \in U \subseteq V$, and again the argument is similar. If $a = 0$ then $v(a+b) = v(b) = \max\left(z,v(b)\right) = \max\left(v(a),v(b)\right)$. If $b = 0$ the argument is similar. Therefore, V is a non-archimedian valuation.

Theorem 2.17. Let $v_1:K_1 \rightarrow G_1 \cup \{z_1\}$ and $v_2:K_2 \rightarrow G_2 \cup \{z_2\}$ be two non-archimedian valuations such that v_1 and v_2 have the same associated valuation ring V. Then there exists an isomorphism $i:v_1(K_1 - \{0\}) \rightarrow v_2(K_2 - \{0\})$ such that $i(v_1(a)) = v_2(a)$.

Proof: Let $V = \{a \in K_1 \mid v_1(a) \not\geq 1\} = \{a \in K_2 \mid v_2(a) \not\geq 1\}$ be the common valuation ring of v_1 and v_2. Let P and U be the non-units and units of V. The set U is the kernal of v_1 and v_2. That is, $U = \{a \in K_1 \mid v_1(a) = 1\} = \{a \in K_2 \mid v_2(a) = 1\}$. Also, $v_1(K_1 - \{0\})$ and $v_2(K_2 - \{0\})$ are multiplicative subgroups of G_1 and G_2 since v_1 and v_2 are group homomorphisms on the multiplicative groups $(K_1 - \{0\})$ and $(K_2 - \{0\})$.

Now, define a mapping $i:v_1(K_1 - \{0\}) \rightarrow v_2(K_2 - \{0\})$ as follows: $i(v_1(a)) = v_2(a)$. If $v_1(a) = v_1(b)$ then $v_1(a/b) = v_1(a)/v_2(b) = 1$. This implies $a/b \in U$ which implies $v_2(a)/v_2(b) = v_2(a/b) = 1$. Therefore, $v_2(a) = v_2(b)$ which implies that i is well defined. Clearly i is onto, and $i(v_1(a)v_1(b)) = i(v_1(ab)) = v_2(ab) = v_2(a)v_2(b) = i(v_1(a))\,i(v_1(b))$. If $i(v_1(a)) = 1$ then $v_2(a) = 1$, and so $a \in U$. Therefore, $v_1(a) = 1$; hence i is an isomorphism.

The last four theorems which can be found in Artin [1] and Bachman [2] state that each valuation ring determines a place (non-archimedian valuation), unique up to an isomorphism, and each place (non-archimedian valuation) determines a valuation ring. This implies that there is a type of one-to-one correspondence between valuation rings and non-archimedian valuations. It follows that each place determines a non-archimedian valuation, and vice versa. The places and valuations are paired by finding their common valuation ring. This discussion motivates the following definition.

Definition 2.18. Two places (or non-archimedian valuations) are said to be equivalent if, and only if they determine the same valuation rings.

Clearly equivalence of places (or non-archimedian valuations) is an equivalence relation.

Rank

In this section the notion of rank will be introduced. The rank of an ordered group will be defined which will be related to the definition of the rank of a valuation. In order to establish these definitions, isolated subgroups will be considered.

Definition 2.19. A subgroup H of an ordered group G is called an isolated subgroup if, and only if $a \in G$, $b \in H$ and $b^{-1} \preceq a \preceq b$ imply $a \in H$.

In every ordered group G the subgroups G and $\{1\}$ are isolated.

Definition 2.20. Let G be an ordered group. The number of isolated subgroups of G different from G is called the rank of G.

Let G be the multiplicative group of positive reals. Let $\prec \, = \, <$ be the natural ordering on G. Suppose H is a non-trivial isolated subgroup of G. Let $b \in G$ such that $1 < b$. Let $x \in (H - \{1\})$. If $x > 1$ then $x^{-1} < 1$. Therefore, there exists an element $a \in H$ such that $a < 1$. Thus, $a < b$ and $1 < a^{-1}$. The Archimedian Principle implies that there exists an integer n such that $b < a^{-n}$. However, $a^{n} < a < 1$ which implies $a^{n} < b < a^{-n}$, and so $b \in H$. If $b > 1$ it can again be shown that $b \in H$ by similar reasoning. If $b = 1$ then $b \in H$ since H is a subgroup. Therefore, $G = H$, and G is an example of a rank one ordered group.

<u>Theorem 2.21</u>. Let G be an ordered group. Let H_1 and H_2 be isolated subgroups of G. Then $H_1 \subset H_2$ or $H_2 \subset H_1$.

Proof: Suppose H_1 is not a subset of H_2. Then there exists $x \in H_1 - H_2$. This implies that $x^{-1} \in H_1 - H_2$. Either $1 \succ x$ or $1 \succ x^{-1}$ by Theorem 2.2. Let $y \in H_2$ such that $1 \succeq y$. If $1 \succ x$ then $y \succ x$, otherwise $x \succeq y$ which implies $y^{-1} \succeq 1 \succeq x \succeq y$, and so $x \in H_2$ since H_2 is isolated, which is a contradiction. Therefore, $x^{-1} \succ 1 \succeq y \succ x$ which implies $y \in H_1$ since H_1 is isolated. Let $y \in H_2$ such that $y \succ 1$. Then $1 \succ y^{-1}$, and $y^{-1} \in H_1$ by the above argument. It now follows that $y \in H_1$ since H_1 is a group. Thus, it has been shown that $H_2 \subset H_1$ if, $1 \succ x$. Similarly it can be shown that $H_2 \subset H_1$ if $1 \succ x^{-1}$. Therefore, $H_1 \subset H_1$.

The above theorem was taken from Artin [1]. The next example was motivated by an example in Schilling [16], p. 7.

<u>Example 2.22</u>. Let Z be the integers. Let $G_3 = \{(a,b,c) \mid a,b,c \in Z\}$. G_3 is a group under the additive operation defined as $(a,b,c) + (d,e,f) = (a+d,\ b+e,\ c+f)$. The group G_3 can be ordered by the so called lexicographic ordering in the following way. Let $S_3 = \{(a,b,c) \in G \mid a < 0\} \cup \{(0,b,c) \in G \mid b < 0\} \cup \{(0,0,c) \mid c < 0\}$. It is clear that S_3 is a normal subsemigroup of G_3. Let

$(-S_3) = \{s \in G_3\} \mid -s \in S_3\}$. If $(a,b,c) \in G$ and $(a,b,c) \notin S_3 \cup \{(0,0,0)\}$ then $a > 0$ or $a = 0$ and $b > 0$ or $a = b = 0$ and $c > 0$. If $a > 0$ then $-a < 0$ which implies $-(a, b, c) = (-a, -b, -c) \in S_3$. If $a = 0$ and $b > 0$ then $-b < 0$ and $-(a,b,c) = (0,-b,-c) \in S_3$. If $a = b = 0$ and $c > 0$ then $-c < 0$ and $-(a,b,c) = (0,0,-c) \in S_3$. Therefore, $G_3 = S_3 \cup \{(0,0,0)\} \cup (-S_3)$ which implies G_3 is ordered. As usual the ordering is defined as $(a,b,c) \prec (d,e,f)$ if, and only if $(a,b,c) - (d,e,f) = (a-d, b-e, c-f) \in S_3$. Hence, $(a,b,c) \prec (d,e,f)$ if, and only if $a < d$ or $b < e$ when $a = d$ or $c < f$ when $a = d$ and $b = e$.

Next it will be shown that the subgroups $H_1 = \{(o,b,c) \mid b,c \in Z\}$, $H_2 = \{(0,0,c) \mid c \in Z\}$ and $H_3 = \{(0,0,0)\}$ are isolated subgroups of G_3. Let $(x,y,z) \in G$ such that there exists $(0,b,c) \in H_1$ where $-(0,b,c) \preceq (x,y,z) \preceq (0,b,c)$. This implies that $0 \leq x \leq 0$, and so $x = 0$ which implies $(x,y,z) \in H_1$. If there exists $(0,0,c) \in H_2$ where $-(0,0,c) \preceq (x,y,z) \preceq (0,0,c)$ then $0 \leq x \leq 0$, and so $x = 0$ which implies $0 \leq y \leq 0$. Therefore, $x = y = 0$ and $(x,y,z) \in H_2$. If $-(0,0,0) \preceq (x,y,z) \preceq (0,0,0)$ then $(x,y,z) = (0,0,0)$ by Theorem 2.2. Hence, H_1, H_2 and H_3 are isolated.

Now it will be established that H_1, H_2 and H_3 are the only isolated subgroups of G_3 different from G_3 itself. Assume there exists an isolated subgroup K of G_3 such that $K \neq H_1, H_2, H_3$. If $K \subset H_2$ then there exists $(0,0,c) \in H_2 - K$. Also, $-(0,0,c) = (0,0,-c) \in H_2 - K$. Either $c > 0$ or $-c > 0$. Let $(0,0,z) \in K$ such that $z > 0$. If $c > 0$ then there exists $n \in Z$ such that $nz > c$. It now follows that $-(0,0,nz) \prec (0,0,c) \prec (0,0,nz)$. Thus, $(0,0,c) \in K$ since K is isolated, but this is a contradiction. By an analogous argument a contradiction would be reached if $-c > 0$. Therefore, K is not a subset of H_2.

Using this fact and the same type of reasoning it can be shown that K is not a subset of H_1. Hence, Theorem 2.21 implies $H_3 \subset H_2 \subset H_1 \subset K$. Let $(x,y,z) \in G_3$. If $x = 0$ then $(x,y,z) \in H_1 \subset K$. If $x > 0$ then let $(a,b,c) \in K$ such that $a > 0$. Then there exists $n \in Z$ such that $na > x$. This implies that $-(na,nb,nc) \not\geq (x,y,z) \not\geq (na,nb,nc)$, and so $(x,y,z) \in K$. If $x < 0$ then a similar argument would again show that $(x,y,z) \in K$. Therefore, $G_3 = K$.

It has been shown that G_3 is an ordered group with exactly three isolated subgroups distinct from G_3, that is, G_3 has rank three. This notion can be generalized, and a group of rank n, where n is a positive integer can be exhibited. Let $G_n = \{(a_1,\ldots,a_n) \mid a_i \in Z\}$. Let $S_n = \{(a_1,\ldots,a_n) \in G_n \mid a_1 < 0\} \cup \{(0,a_2,\ldots,a_n) \in G_n \mid a_2 < 0\} \cup \ldots \cup \{(0,0,\ldots,a_i,\ldots,a_n) \in G_n \mid a_i < 0\} \cup \ldots \cup \{(0,0,\ldots,0,a_n) \in G_n \mid a_n < 0\}$. It can be shown that $G_n = S_n \cup \{(0,0,\ldots,0)\} \cup (-S_n)$ where the union is disjoint. Thus, G_n is ordered lexicographically. Likewise it can be shown that G_n has exactly the following isolated subgroups. They are $H_1 = \{(0,a_2,\ldots,a_n) \mid a_i \in Z\}$, $H_2 = \{(0,0,a_3,\ldots,a_n) \mid a_i \in Z\}$, ..., $H_{n-1} = \{(0,0,\ldots,0,a_n) \mid a_n \in Z\}$, $H_n = \{(0,0,\ldots,0)\}$ and G_n itself. Therefore, G_n is an ordered group of rank n.

It has been shown that an ordered group of rank n exists where n is an arbitrary positive integer. The next example illustrates an ordered group of infinite rank.

Example 2.23. Let G_∞ be the set of all sequences of real numbers. Define addition in G_∞ in the following way. Let $\{a_n\} + \{b_n\} = \{a_n + b_n\}$. It can readily be shown that G_∞ is an additive group.

Let $S = \{\{a_n\} \in G\infty \mid a_1 < 0\} \cup \{\{a_n\} \in G\infty \mid a_1 = 0, a_2 < 0\} \cup \ldots$ $\cup \{\{a_n\} \in G\infty \mid a_1 = a_2 = \ldots = a_{i-1} = 0,\ a_i < 0\} \cup \ldots$. Let $\{a_n\} \in G$ such that $\{a_n\} \notin S \cup \{e\}$ where e is the sequence with each term equal to zero. If a_j is the first non-zero term of $\{a_n\}$ than $a_j > 0$. This implies $-a_j < 0$, and $-\{a_n\} = \{-a_n\} \in S$. Hence, $\{a_n\} \in (-S) = \{\{a_n\} \in G \mid -\{a_n\} \in S\}$. It follows that G∞ is the disjoint union of S, $\{e\}$ and (-S). Therefore, G∞ is an ordered group where $\{a_n\} \ngtr \{b_n\}$ if, and only if $\{a_n - b_n\} \in S$ if, and only if $a_i < b_i$ where i is the first integer such that $a_i \neq b_i$.

Let i be a positive integer. Define $H_i = \{\{a_n\} \in G \mid a_1 = a_2 = \ldots = a_i = 0\}$. Clearly H_i is a subgroup of G∞. Let $\{a_n\} \in H_i$ and $\{b_n\} \in G$ such that $-\{a_n\} \lneq \{b_n\} \lneq \{a_n\}$. Therefore, $0 = -a_1 \leq b_1 \leq a_1 = 0$ implies $0 = -a_2 \leq b_2 \leq a_2 = 0$ implies ... implies $0 = -a_i \leq b_i \leq a_i = 0$. This implies $\{b_n\} \in H_i$, and so H_i is isolated. Also, if j is a positive integer such that $i \neq j$ then it can be shown that $H_i \neq H_j$. Suppose $i < j$. Then the sequence $\{a_n\}$, where $a_n = 0$ for all $n \neq j$ and $a_j = 1$, is an element of H_i, but $\{a_n\} \notin H_j$. Therefore, G∞ has infinitely many isolated subgroups. Hence, G∞ has infinite rank.

<u>Definition 2.24</u>. Let $v: F \rightarrow G \cup \{z\}$ be a valuation on the field F. Let n be a positive integer. Then v is said to have rank n if, and only if the ordered group G has rank n.

<u>Example 2.25</u>. Let G_3 be the ordered group of three-tuples of integers discussed in Example 2.22. Let F = R(x,y,z). That is, F is the field

of rational functions in the three variables x, y and z. Let $f \in F$. Then f can be written as $f = x^{\alpha} y^{\beta} z^{\gamma} a(x,y,z) / b(x,y,z)$ where $a(x,y,z)$ and $b(x,y,z)$ are polynomials, but $x,y,z \nmid a(x,y,z)$ and $x,y,z \nmid b(x,y,z)$, and α, β, and γ are integers either positive, negative or zero. Define $v: F \to G_3 \cup \{z\}$ as follows: $v(f) = (\alpha, \beta, \gamma)$ if $f \neq 0$ and $v(0) = z$. It will now be shown that v is a valuation. Let $g = x^a y^b z^c p(x,y,z) / q(x,y,z)$ where p and q are polynomials, but $x,y,z \nmid p$ and $x,y,z \nmid q$. Then $v(fg) = v(x^{\alpha + a} y^{\beta+b} z^{\gamma+c} ap / bq) = (\alpha+a, \beta+b, \gamma+c) = v(f) + v(g)$. This satisfies condition (b) of Definition 2.5 since G is an additive group. Also, $v(f+g) =$ $v([x^{\alpha} y^{\beta} z^{\gamma} aq + x^a y^b z^c bp] / bq) = (\min(\alpha, a), \min(\beta,b), \min(\gamma,c))$. Now suppose $(\alpha,\beta,\gamma) \ngtr (a,b,c)$. Then $\alpha < a$ or $\alpha = a$ and $\beta < b$ or $\alpha = a$, $\beta = b$ and $\gamma < c$. If $\alpha < a$ then $v(f+g) = (\alpha, \min(\beta,b), \min(\gamma,c)) \ngtr (a,b,c)$. If $\alpha = a$ and $\beta < b$ then $v(f+g) = (a,\beta, \min(\gamma,c)) \ngtr (a,b,c)$. If $\alpha = a$, $\beta = b$ and $\gamma < c$ then $v(f+g) = (a,b,\gamma) \ngtr (a,b,c)$. Therefore, $v(f+g) \ngeq \max(v(f), v(g))$. The argument is similar if $(a,b,c) \ngtr (\alpha,\beta,\gamma)$. The function v is onto since $v(x^{\alpha} y^{\beta} z^{\gamma}) = (\alpha,\beta,\gamma)$ for all $(\alpha,\beta,\gamma) \in G_3$. Hence, v is a non-archimedian rank three valuation.

In a similar manner a non-archimedian rank n valuation could be constructed on $F = R(x_1, x_2, \ldots, x_n)$, the field of rational functions in n variables, onto $G_n = \{(a_1, \ldots, a_n) \mid a_i \in Z\}$.

It seems, however, that the most interesting valuations are of rank one and are non-archimedian. The trivial valuation is non-archimedian. The absolute value function on the reals is of rank one, but it is archimedian. These and other rank one valuations will be discussed in the next chapter.

CHAPTER III

RANK ONE VALUATIONS

Rank One Ordered Groups

In the last chapter the concept of an ordered group of general rank was introduced. The aim of this section is to consider some of the properties of rank one ordered groups, and in particular to show that every rank one ordered group is isomorphic to a subgroup of the additive real numbers. First, an archimedian ordered group will be defined.

<u>Definition 3.1</u>. Let G be an ordered group. If for every $a, b \in G$ with $1 \succ a$ there exists an integer n such that $b \succ a^n$ then G is said to be archimedian.

<u>Theorem 3.2</u>. If G is an archimedian ordered group then for any $a, b \in G$ with $1 \succ a$ there exists an integer $n > 1$ such that $b \succ a^n$.

Proof: If $b \succeq 1$ then $b \succ a^2$ since $1 \succ a \succ a^2$. In this case let $n = 2$. If $1 \succ b$ then there exists k such that $b \succ a^k$ since G is archimedian. The integer k is greater than zero, otherwise $k \leq 0$ which implies $a^k \succeq 1 \succ b$. However, this contradicts the fact that $b \succ a^k$. Therefore, $k + 1 > 1$, so let $n = k + 1$.

The proof of the next theorem is a modification of one found in Schilling [16].

<u>Theorem 3.3</u>. Let G be an ordered group. G is archimedian if, and only if G is of rank one.

Proof: Suppose G is archimedian. Let H be an isolated subgroup of G such that $H \neq \{1\}$. Let $a \in G$. Let $b \in H$ such that $1 \succ b$. If $1 \succ a$ then there exists an n such that $a \succ b^n$ since G is archimedian. Thus, $b^{-n} \succ a \succ b^n$. Therefore, $a \in H$ since H is isolated. If $a \succ 1$ then $1 \succ a^{-1}$, and there exists k such that $b^{-k} \succ a^{-1} \succ b^k$. Hence, $a^{-1} \in H$ which implies $a \in H$. If $a = 1$ then $a \in H$ since H is a group. It now follows that $G \subseteq H$ or that $G = H$. Therefore, G is of rank one.

Now suppose G is of rank one, but not archimedian. Then there exists $a,b \in G$ such that $1 \succ a \succ b$ but $a^n \succeq b$ for every integer n. Let $S = \{x \in G \mid 1 \succ x \text{ and } x \succ a^n \text{ for some integer } n\}$. If $x,y \in S$ then there exist integers n and m such that $1 \succ x \succ a^n$ and $1 \succ y \succ a^m$. This implies that $1 \succ xy \succ a^{n+m}$, and so $xy \in S$. Therefore, S is a semigroup.

Let H be the subgroup generated by S. Then H is the set of all finite products of powers of elements in S (i.e. $x \in H$ if, and only if

$x = \prod_{i \in I} x_i^{p_i}$ where $x_i \in S$ for all $i \in I$, p_i is an integer for all $i \in I$

and I is a finite index set). It follows that for any $x \in H$, x can

also be represented as a finite product, $\prod_{i \in I} x_i^{p_i}$, where $p_i = \pm 1$ and

$x_i \in S$ for all $i \in I$, since S is a semigroup.

It will now be shown that H is a proper isolated subgroup of G. This will contradict the statement that G is of rank one and will complete the proof of the theorem. The subgroup $H \neq \{1\}$ since $a \in S \subset H$. Now assume $b \in H$. This implies $b = \prod_{i \in I} b_i^{p_i}$ where I is finite, $b_i \in S$ and $p_i = \pm 1$. If $p_i = -1$ then $b_i^{pi} \succ 1$. If $p_i = 1$ then $b_i^{pi} = b_i$, and so there exists an integer n_i such that $b_i^{pi} \succ a^{ni}$. Thus, $b \succ \prod_{i \in J} a^{ni}$ where $J = \{i \in I \mid p_i = 1\}$. Hence, $b \succ a^n$ where $n = \sum_{i \in J} n_i$, a contradiction. Therefore, H is a proper subgroup of G.

Let $x \in G$ and $y \in H$ such that $y^{-1} \succeq x \succeq y$. Thus, there exists a positive integer n, elements $y_i \in S$ for i = 1, 2, ..., n and integers $p_i = \pm 1$ for i = 1, 2, ..., n such that $y_n^{-pn} \ldots y_2^{-p2} y_1^{-p1} \succeq x \succeq y_1^{p1} y_2^{p2} \ldots y_n^{pn}$. However, it can be shown, by using an argument similar to the one above, that there exists an integer k such that $x \succ a^k$. If $1 \succ x$ then $x \in S \subset H$. If $x \succ 1$ then $1 \succ x^{-1} \succeq y_1^{p1} y_2^{p2} \ldots y_n^{pn}$, and so again there exists an integer k such that $x \succ a^k$. This implies that $x^{-1} \in S \subset H$ and $x \in H$. If x = 1 then $x \in H$ since H is a group. Hence, H is isolated, and the theorem is proved.

Theorem 3.4. Let G be an ordered group. Let $a \in G$ such that $1 \succ a$ then

(a) $a^n \succ a^m$ if, and only if $n < m$.

(b) If G is archimedian and $b \in G$ then there exists a smallest integer m such that $b \succ a^m$ and $a^{m-1} \succeq b \succ a^m$.

Proof:

(a) If $1 \succ a$ and k is an integer such that $k > 0$ then $1 \succ a \succ a^2 \succ \ldots \succ a^k$ by Theorem 2.2. Suppose $m \leq n$; thus $0 \leq n - m$. This implies $1 \succeq a^{n-m}$ which implies $a^m \succeq a^n$. Therefore, if $a^n \succ a^m$ then $n < m$. If $n < m$ then $0 < m-n$ which implies $1 \succ a^{m-n}$. Thus, $a^n \succ a^m$.

(b) There exists an integer ℓ such that $b^{-1} \succ a^{\ell}$. Hence, $a^{-\ell} \succ b$. Let n be an integer such that $b \succ a^{n}$. Then $-\ell < n$, otherwise $n \leq -\ell$ and $a^{n} \succeq a^{-\ell}$ by (a). However, $a^{n} \succ b$, a contradiction. Therefore, $-\ell$ is a lower bound of the set $S = \{n \mid n \text{ is an integer and } b \succ a^{n}\}$. Hence, S has a greatest lower bound m. Therefore, m is the smallest integer such that $b \succ a^{m}$. Also, $a^{m-1} \succeq b$ by definition of greatest lower bound.

The next two theorems are taken from a single theorem in Bachman [2].

<u>Theorem 3.5</u>. Let G be an ordered group of rank one. If there exists a smallest element $c \in G$ such that $1 \succ c$ then G is the infinite cyclic group generated by c.

Proof: Let $a \in G$. If $1 \succ a$ then $c \succeq a$. Also, there exists an integer n such that $c^{n} \succeq a \succ c^{n+1}$ by Theorems 3.3 and 3.4. This implies $1 \succeq ac^{-n} \succ c$ which means $ac^{-n} = 1$ by definition of c. Therefore, $a = c^{n}$.

Now, if $a \succ 1$ then $1 \succ a^{-1}$, and so there exists an integer n such that $a^{-1} = c^{n}$ by the above argument. Thus, $a = c^{-n}$. If $a = 1$ then $a = c^{o}$. Therefore, G is cyclic and is generated by c.

<u>Theorem 3.6</u>. If G is an ordered group of rank one than G is abelian.

Proof: If G has a smallest element c such that $1 \succ c$ then G is cyclic by Theorem 3.5. Thus, G is abelian.

Suppose G has no smallest element c such that $1 \succ c$. Let $x \in G$ such that $1 \succ x$. It will now be shown that there exists an element $y \in G$ such that $1 \succ y \succ x$ and $y^{2} \succeq x$. There exists a q such that

$1 \succ q \succ x$ since G has no smallest element c such that $1 \succ c$. If $q^2 \succeq x$ then the assertion is proved. If $x \succ q^2$ then it can be shown that xq^{-1} has the desired properties. This is true because $x \succ q^2$ implies $xq^{-1} \succ q$ which means $q^{-1}x\, q^{-1} \succ 1$ which in turn implies $xq^{-1}\, xq^{-1} = (xq^{-1})^2 \succ x$ and since $x \succ q^2$ this implies $xq^{-2} \succ x$. Therefore, the desired element y is either q or xq^{-1}.

Now, let $a,b \in G$ such that $1 \succ a,b$. It will be demonstrated that $ab = ba$ by assuming the contrary and finding a contradiction. Thus, suppose $ab \neq ba$. This implies $(ab)(ba)^{-1} \neq 1$. Let $x = (ab)(ba)^{-1}$, and assume $1 \succ x$. By the preceding paragraph there exists an element $y \in G$ such that $1 \succ y \succ \min(a,b,x)$ and $y^2 \succeq \min(a,b,x)$. Therefore, $1 \succ y \succ x$, $y^2 \succeq x$, $y \succ b$. Theorem 3.3 implies G is archimedian, and this fact together with Theorem 3.4 imply that there exist integers m and n such that $y^m \succeq a \succ y^{m+1}$ and $y^n \succeq b \succ y^{n+1}$. This implies that $y^{n+m} \succeq ab \succ y^{m+n+2}$ and $y^{m+n} \succeq ba \succ y^{m+n+2}$. Therefore, $y^{m+n} \succeq ab \succ y^{m+n+2}$ and $y^{-m-n-2} \succ (ba)^{-1} \succeq y^{-m-n}$. These two statements yield $y^{-2} \succ (ab)(ba)^{-1} \succ y^2$. It now follows that $x \succ y^2 \succeq x$. This is a contradiction. It was assumed that $1 \succ x$, but if $x \succ 1$ then $1 \succ x^{-1} = (ba)(ab)^{-1}$, and a similar argument will likewise produce a contradiction.

If $1 \succ a$ and $b \succ 1$ then $1 \succ a$ and $1 \succ b^{-1}$. Thus, the fact that was proved above implies $ab^{-1} = b^{-1}a$. Therefore, $a = b^{-1}ab$ which implies $ba = ab$. If $a \succ 1$ and $1 \succ b$ then by a similar method it can be shown that $ab = ba$. If either a or b are equal to 1 then $ab = a = ba$ or $ab = b = ba$. Hence, G is abelian.

<u>Example 3.7</u>. An example of an ordered group that is not abelian is the group G of all ordered pairs of real numbers with the group operation defined as $(a_1, a_2) + (b_1, b_2) = (a_1 + a_2, a_2\, e^b + b_2)$. First the

group postulates will be verified. Let (x_1, x_2), (y_1, y_2), (z_1, z_2) $\in G$. Then

(a) $\big((x_1,x_2) + (y_1,y_2)\big) + (z_1,z_2) = (x_1 + y_1,\ x_2\ e^{y_1} + y_2) + (z_1,z_2) =$

$\big((x_1 + x_2) + z_1,\ (x_2\ e^{y_1} + y_2)\ e^{z_1} + z_2\big) = \big(x_1 + (y_1 + z_1),$

$x_2\ e^{y_1+z_1} + y_2\ e^{z_1} + z_2\big) = (x_1,\ x_2) + (y_1 + z_1,\ y_2\ e^{z_1} + z_2) =$

$(x_1,\ x_2) + \big((y_1,\ y_2) + (z_1,\ z_2)\big)$

(b) $(x_1,\ x_2) + (0,0) = (x_1 + 0,\ x_2\ e^{0} + 0) = (x_1,\ x_2) =$

$(0 + x_1,\ 0\ e^{x_1} + x_2) = (0,0) + (x_1,\ x_2)$

(c) $(x_1,\ x_2) + (-x_1,\ - x_2\ e^{-x_1}) = (x_1 - x_1,\ x_2\ e^{-x_1} - x_2\ e^{-x_1}) =$

$(0,0), (-x_1,\ -x_2\ e^{-x_1}) + (x_1,\ x_2) = (-x_1 + x_1,\ - x_2\ e^{-x_1}\ e^{x_1} + x_2) =$

$(0,0)$.

Therefore, G is a group. Now it will be shown that G is an ordered group. Let $S = \{(x,y) \mid x < 0\} \cup \{(0,y) \mid y < 0\}$. It is easy to see that S is closed under addition and is therefore a subsemigroup of G. Let $(x,y) \in S$ and $(a,b) \in G$. Then $(a,b) + (x,y) + (-a,\ -b\ e^{-a}) =$

$(a+x,\ b\ e^{x} + y) + (-a,\ -b\ e^{-a}) = \big(x,\ (b\ e^{x} + y)\ e^{-a} - b\ e^{-a}\big)$ which

is an element of S if $x < 0$. If $x = 0$ then $y < 0$ and

$\big(x,\ (b\ e^{x} + y)\ e^{-a} - b\ e^{-a}\big) = (0,\ y\ e^{-a}) \in S$. Thus, S is a normal subsemigroup. Let $(a,b) \in G$ such that $(a,b) \neq 0$. If $a < 0$ or $a = 0$ and $b < 0$ then $(a,b) \in S$. If $a = 0$ and $b > 0$ then $(a,b) \in (-S)$ since $(a,b) = (0,b) = (-0,\ b\ e^{0}) = -(0,-b)$ and since $-b < 0$. If $a > 0$ then $(a,b) \in (-S)$ since $(a,b) = (a,\ b\ e^{-a}\ e^{a}) = -(-a,\ -b\ e^{-a})$ and since $-a < 0$. Therefore, $G = (-S) \cup (0,0) \cup S$. The element $(0,0) \notin S$ since

$(x,y) \in S$ implies $x < 0$ or $y < 0$. Also, $(0,0) \notin (-S)$. Otherwise $-(0,0) = (0,0) \in S$, a contradiction. If $(a,b) \in (-S) \cap (S)$ then $(a,b) \in S$ and $-(a,b) \in S$ which implies $(0,0) = (a,b) - (a,b) \in S$. But, again, this is a contradiction. Thus, $G = (-S) \cup (0,0) \cup S$ and the union is disjoint, and so G is an ordered group.

It can readily be shown that G is not abelian by the following computations.

$$(0, 1) + (1, 0) = (0 + 1, 1 \cdot e^1 + 0) = (1, e)$$

$$(1, 0) + (0, 1) = (1 + 0, 0 \cdot e^0 + 1) = (1, 1)$$

This example can be found in Schilling [16], p. 7.

It is now advantageous to define a Dedekind out. The following definition is very closely related to the one devised by Burrill [6]. In the definition Q will denote the rationals and R the reals.

<u>Definition 3.8</u>. Let $d = (L, U)$ be an ordered pair of two disjoint subsets of Q such that

(a) $L \neq Q$, $U \neq \varphi$

(b) $Q = L \cup U$

(c) $r_1 \in U$, $r_2 \in Q$ and $r_1 \leq r_2$ imply $r_2 \in U$.

(d) U does not contain a smallest element.

Then d is called a Dedekind cut in R, and L and U are called the lower and upper classes of d, respectively.

<u>Theorem 3.9</u>. If $d = (L, U)$ is a Dedekind cut in R then there exists a number $\bar{d} \in R$ such that $U = \{x \in Q \mid \bar{d} < x\}$ and $L = Q - U = \{x \in Q \mid x \leq \bar{d}\}$.

Proof: Let $a \in L$. The set U is bounded below by a, otherwise there exists $b \in U$ such that $b < a$. However, this implies $a \in U$ which is impossible since $L \cap U = \varphi$. Therefore, U has a greatest lower bound $\bar{d}$. Let $x \in Q$ such that $x > \bar{d}$. It follows that there exists $y \in U$ such that $\bar{d} < y < x$ which implies $x \in U$ by (c) in Definition 3.8. This together with (d) in the definition and the fact $\bar{d}$ is the greatest lower bound of U imply $U = \{x \in Q \mid \bar{d} < x\}$. Therefore, $L = Q - U = \{x \in Q \mid x \leq \bar{d}\}$ since Q is the disjoint union of L and U.

Definition 3.10. Let $d = (L, U)$ be a Dedekind cut in R. Let $\bar{d} \in R$ such that $U = \{x \in Q \mid \bar{d} < x\}$. If $\bar{d} \in Q$ then d is called a rational cut.

The next theorem shows that a particular ordered pair of subsets of Q derived in a certain manner from an element of a rank one ordered group is a Dedekind cut. It is adapted from a theorem in Bachman [2].

Theorem 3.11. Let G be a rank one ordered group. Let $a,b \in G$ such that $1 \not> a$. Let $L(b) = \{m/n \in Q \mid n > 0,\ a^m \not\geq b^n\}$ and $U(b) = \{m/n \in Q \mid n > 0,\ b^n \not> a^m\}$. Then $d(b) = \big(L(b), U(b)\big)$ is a Dedekind cut in R.

Proof: Let $m/n \in L(b) \cap U(b)$. This implies that $a^m \not\geq b^n \not> a^m$ which is impossible. Hence, $L(b) \cap U(b) = \varphi$.

(a) If $b = 1$ then $a^{-1} \not> 1 = b$ and $b = 1 \not> a$ which implies $-1 \in L(b)$ and $1 \in U(b)$. If $1 \not> b$ then there exists $n > 0$ such that $a \not> b^n$ since G is archimedian and by Theorem 3.2. Also, there exists an m such that $b^n \not> a^m$. Thus, $1/n \in L(b)$ and $m/n \in U(b)$. If $b \not> 1$ then $b \not> a$ which implies $1 \in U(b)$. Also, $1 \not> b^{-1}$ which implies that there exists an $n > 0$ such that $a \not> b^{-n}$. However, there exists an m such that $b^{-n} \not> a^m$. This implies $a^{-m} \not> b^n$, and so

$-m/n \in L(b)$. Hence, $L(b) \neq \varphi$ and $U(b) \neq \varphi$.

(b) Let $r \in Q$. Then there exists integers m and n such that $n > 0$ and $r = m/n$. By the trichotomy law in an ordered group $a^m \succeq b^n$ or $b^n \succ a^m$. Hence, $r \in L(b) \cup U(b)$ which implies $Q \subseteq L(b) \cup U(b)$. Therefore, $Q = L(b) \cup U(b)$ since $L(b) \cup U(b) \subseteq Q$.

(c) Let $r_1 = m_1/n_1 \in U(b)$ and $r_2 = m_2/n_2 \in Q$ such that $r_1 \leq r_2$ and $n_1, n_2 > 0$. It follows that $m_1n_2 \leq m_2n_1$ and $b^{n_1} \succ a^{m_1}$, and so $b^{n_1n_2} \succ a^{m_1n_2} \succeq a^{m_2n_1}$ by (b) of Theorem 2.2 and (a) of Theorem 3.4. Therefore, $b^{n_2} \succ a^{m_2}$. Otherwise $a^{m_2} \succeq b^{n_2}$ which implies $a^{m_2n_1} \succeq b^{n_1n_2}$ by Theorem 2.2; hence $r_2 = m_2/n_2 \in U(b)$.

(d) Let $m/n \in U(b)$. This implies $n > 0$ and $b^n \succ a^m$. Thus, $1 \succ a^m b^{-n}$, and so there exists integers $p_1, p_2, p_3 > 1$ such that $b \succ (a^m b^{-n})^{p_1}$, $b^{-1} \succ (a^m b^{-n})^{p_2}$ and $a \succ (a^m b^{-n})^{p_3}$ by Theorem 3.2. It follows that $b \succ a^{mp_1} b^{-np_1}$, $b^{-1} \succ a^{mp_2} b^{-np_2}$ and $a \succ a^{mp_2} b^{-np_3}$ since G is abelian by Theorem 3.6. Hence, $b^{np_1 + 1} \succ a^{mp_1}$, $b^{np_2-1} \succ a^{mp_2}$ and $b^{np_3} \succ a^{mp_2-1}$ which implies $mp_1/(np_1 + 1)$, $mp_2/(np_2-1)$ and $(mp_2-1)/np_3 \in U(b)$. If $m > 0$ then $mp_1/(np_1 + 1) < mp_1/np_1 = m/n$. If $m < 0$ then $mp_2/(np_2-1) < mp_2/np_2 = m/n$. If $m = 0$ then $(mp_2-1)/np_3 = -1/np_3 < 0 = m/n$. Therefore, U(b) has no smallest element.

Now, as promised, the isomorphism theorem concerning rank one ordered groups will be proved. This is a classical theorem and can be found in Artin [1] and Bachman [2].

Theorem 3.12. Let G be an ordered group of rank one. Then there exists an order preserving isomorphism between G and an additive subgroup of the real numbers.

Proof: Let $f: G \rightarrow R$ be a mapping defined in the following manner. Let a be a fixed element of G such that $1 \prec a$. Now, if $b \in G$ then there exists a Dedekind cut $d(b) = \big(L(b), U(b)\big)$ in R where $L(b) = \{m/n \in Q \mid n > 0, a^m \preceq b^n\}$ and $U(b) = \{m/n \in Q \mid n > 0, b^n \prec a^m\}$. This was shown in Theorem 3.11. Now, let $f(b) = \overline{d(b)}$ where $\overline{d(b)}$ is the real number such that $U(b) = \{x \in Q \mid \overline{d(b)} < x\}$ and $L(b) = \{x \in Q \mid x \leq \overline{d(b)}\}$. Theorem 3.9 states that such a number exists.

Let $b, c \in G$ such that $c \prec b$. This implies that $1 \prec bc^{-1}$ which in turn implies there exists an $n > 0$ such that $a \prec (bc^{-1})^n$; hence $ac^n \prec b^n$ since G is abelian. By (b) of Theorem 3.4 there exists a smallest integer m such that $c^n \prec a^m$. If $b^n \prec a^m$ then $ac^n \prec a^m$ which implies $c^n \prec a^{m-1}$. But this is impossible since m is the smallest such integer. Thus, $c_n \prec a^m \preceq b^n$ which implies $m/n \in U(c) \cap L(b)$. This implies that $\overline{d(c)} < m/n \leq \overline{d(b)}$ because of Theorem 3.9. Therefore, $f(c) < f(b)$ which implies f is an order preserving map. Suppose $b, c \in G$ such that $f(b) = f(c)$. Then $b = c$, otherwise $b \prec c$ which implies $f(b) < f(c)$ or $c < b$ which implies $f(c) < f(b)$, a contradiction in either case. Therefore, f is one-to-one.

Let $b, c \in G$, and let the set $\{r_1 + r_2 \mid r_1 \in U(b), r_2 \in U(c)\}$ be denoted by $U(b) + U(c)$. Let $x \in U(b) + U(c)$. This implies $x = m_1/n_1 + m_2/n_2$ where $m_1/n_1 \in U(b)$, $m_2/n_2 \in U(c)$. Let $q = n_1n_2$, $p_1 = m_1n_2$ and $p_2 = m_2n_1$. Then $m_1/n_1 = p_1/q$ and $m_2/n_2 = p_2/q$; hence $b^q \not> a^{p_1}$ and $c^q \not> a^{p_2}$ which imply $(bc)^q \not> a^{p_1+p_2}$. Thus, $x = m_1/n_1 + m_2/n_2 = p_1/q + p_2/q = (P_1+p_2)/q \in U(bc)$. Therefore, $U(b) + U(c) \subseteq U(bc)$. In a similar manner it can be shown that $L(b) + L(c) \subseteq L(bc)$. Let $r_1 \in U(b)$ and $r_2 \in U(c)$. Then $r_1 + r_2 \in U(bc)$ which implies $\overline{d(bc)} < r_1 + r_2$ by Theorem 3.9. Therefore, $\overline{d(bc)}$ is a lower bound for $U(b) + U(c)$. Also, Theorem 3.9 implies that $\overline{d(b)} = \inf U(b)$ and $\overline{d(c)} = \inf U(c)$. Let $\epsilon > 0$. Then there exists $x \in U(b)$ and $y \in U(c)$ such that $\overline{d(b)} \le x < \overline{d(b)} + \epsilon/2$ and $\overline{d(c)} \le y < \overline{d(c)} + \epsilon/2$, and so $\overline{d(b)} + \overline{d(c)} \le x + y < \overline{d(b)} + \overline{d(c)} + \epsilon$. Also, if $r_1 \in U(b)$ and $r_2 \in U(c)$ then $\overline{d(b)} < r_1$ and $\overline{d(c)} < r_2$ which implies $\overline{d(b)} + \overline{d(c)} < r_1 + r_2$. Therefore, $\overline{d(b)} + \overline{d(c)} = \inf \big(U(b) + U(c)\big)$. This together with the fact that $\overline{d(bc)}$ is a lower bound of $U(b) + U(c)$ imply $\overline{d(bc)} \le \overline{d(b)} + \overline{d(c)}$. Since $L(b) + L(c) \subseteq L(bc)$, it can be shown by an analogous argument that $\overline{d(b)} + \overline{d(c)} \le \overline{d(bc)}$. Therefore, $f(b) + f(c) = \overline{d(b)} + \overline{d(c)} = \overline{d(bc)} = f(bc)$. Hence, f is an isomorphism, and the theorem is proved.

Corollary 3.13. Let G be a rank one ordered group. Then G is order isomorphic to a subgroup of the multiplicative group of all positive real numbers.

Proof: The ordered group G is isomorphic to a subgroup H of the additive group of all real numbers by Theorem 3.12. Let $f: H \to R$ be defined as $f(x) = 2^x$. The following statements show that f is an order preserving isomorphism.

$$f(x+y) = 2^{x+y} = 2^x 2^y = f(x)f(y)$$

$$f(x) = f(y) \text{ implies } 2^x = 2^y \text{ implies } x = y$$

$$x < y \text{ implies } 2^x < 2^y \text{ implies } f(x) < f(y)$$

Therefore, G is an order isomorphic to f(H).

Non-Archimedian Valuations

The last corollary shows that the value group of a rank one valuation is always isomorphic to a subgroup of the multiplicative group of real numbers. Three of the main purposes of this section are to characterize a rank one valuation when the non-archimedian property is assumed to show how one of the standard definitions of a rank one valuation is motivated and to characterize a non-archimedian valuation when rank one is assumed.

Definition 3.14. Let H be a subset of an ordered group G. The set $\{a \in H \mid a \ngtr 1\}$ will be denoted by H^-. H will be called a lower class in G if $a \in G$, $b \in H$ and $a \ngtr b$ imply $a \in H$.

Theorem 3.15. Let G be a non-trivial ordered group. Let H be an isolated subgroup of G. Let $W = B^- - H^-$. Then W is a lower class of G.

Proof: Let $a \in G$ and $b \in W$ such that $a \succeq b$. Then $a \succ 1$ since $b \succ 1$; hence $a \in G^-$. Suppose $a \in H^-$. This implies that $a, a^{-1} \in H$. Also, $a \succeq b \succ 1 \succ a^{-1}$. Thus, $b \in H$ since H is isolated. However, this is impossible since $b \in W = G^- - H^-$. Therefore, $a \notin H^-$ which implies that $a \in W$, and so W is a lower class of G.

<u>Lemma 3.16</u>. Let $v{:}F \to G \cup \{z\}$ be a non-archimedian valuation of rank greater than one. Let $P = \{a \in F \mid v(a) \succ 1\}$. Let H be an isolated subgroup of G such that $H \neq \{1\}$ and $H \neq G$. Let $W = G^- - H^-$ and $P' = \left\{a \in F \mid v(a) \in W \cup \{z\}\right\}$. Then P′ is a prime ideal of the valuation ring $O = \{a \in F \mid v(a) \succeq 1\}$ and P′ is a proper subset of P.

Proof: Let $a,b \in P'$. Then $v(a), v(b) \in W \cup \{z\}$ which implies $v(a), v(b) \succ 1$. If $v(a) = z$ or $v(b) = z$ then $v(ab) = v(a)v(b) = z \in W \cup \{z\}$ which implies $ab \in P'$. If $v(a) \neq z$ and $v(b) \neq z$, then $v(ab) = v(a)v(b) \succ v(a)\cdot 1 = v(a)$; hence $v(ab) \in W$ since $v(a) \in W$ and W is a lower class. Thus, $ab \in P'$.

By the non-archimedian property $v(a-b) \succeq \max\big(v(a),v(b)\big) = \max\big(v(a),v(b)\big) \in W \cup \{z\}$. If $v(a-b) \neq z$ then $v(a) \neq z$ or $v(b) \neq z$; hence $v(a-b) \in W$ since W is a lower class, and so $a-b \in P'$. If $v(a-b) = z$ then $v(a-b) \in W \cup \{z\}$ which implies $a-b \in P'$. Therefore, P′ is a ring.

If $a \in P'$ then $v(a) = z$ or $v(a) \in G^-$. In either case, $v(a) \succ 1$ which implies that $a \in P$. Thus, $P' \subseteq P \subset O$. Let $a \in F$ such that $v(a) \in H^-$. This implies $v(a) \notin W$ and $v(a) \succ 1$. Therefore, $a \in P - P'$ which implies that P′ is a proper subset of P.

Let $a \in P'$ and $b \in O$. If $a = 0$ or $b = 0$ than $ab = 0 \in P'$. If $a \neq 0$ and $b \neq 0$ then $v(ab) = v(a)v(b) \succeq v(a)\cdot 1 = v(a) \in W$. Therefore,

$v(ab) \in W$, and so $ab \in P'$. This proves that P' is an ideal of O.

Let $a, b \in O$ such that $ab \in P'$. This implies $v(ab) = z$ or $v(ab) \in W$. If $v(ab) = z$ then $ab = 0$ which implies $a = 0$ or $b = 0$ which implies $v(a) = z$ or $v(b) = z$. Thus, $a \in P'$ or $b \in P'$. If $v(ab) \in W = G^- - H^-$ then $v(a)v(b) \in G^-$. It follows that $v(a) \in G^-$ and $v(b) \in G^-$ otherwise $v(a) = z$ or $v(b) = z$ which implies that $v(ab) = v(a)v(b) = z \notin W$. Suppose $v(a), v(b) \in H^-$. Then $v(a), v(b) \in H$ and $v(a), v(b) \not\succ 1$; hence $v(ab) = v(a)v(b) \not\succ 1$ and $v(ab) \in H$ which implies that $v(ab) \in H^-$, a contradiction. Therefore, $v(a) \notin H^-$ or $v(b) \notin H^-$ which implies $v(a) \in W$ or $v(b) \in W$. Thus $a \in P'$ or $b \in P'$. This proves that P' is a prime ideal of O.

<u>Lemma 3.17</u>. Let O be a subring of a field F. Let P' be a prime ideal of O such that $O \neq P'$. Let $T = \{a/b \in F \mid a \in O, b \in O - P'\}$. Then T is a subring of F. If $1 \in O$ then $O \subseteq T \subsetneq F$.

Proof: Let $x, y \in T$. Then there exist $a, c \in T$ and $b, d \in O - P'$ such that $x = a/b$ and $y = c/d$. Thus, $x-y = (ad - bc)/bd$. The element $bd \notin P'$, otherwise $b \in P'$ or $d \in P'$ since P' is prime; hence $bd \in O-P'$. Also, $ad - bc \in O$ since $a,b,c,d \in O$. Therefore, $x-y \in O$. In a similar manner it can be shown that $xy \in T$. This shows that T is a subring of F.

The unity element 1 is not in P', otherwise $P' = O$. If $1 \in O$ then $1 \in O - P'$ which implies that for all $x \in O$, $x = x/1 \in T$, and so $O \subseteq T$. Let $a \in P'$ and $b \in O - P'$ such that $a \neq 0$. Then $b/a \notin T$, otherwise there exist $c \in O$ and $d \in O - P'$ such that $b/a = c/d$, and so $bd = ac \in P'$ which implies that $b \in P'$ or $d \in P'$ since P' is prime in O. However, this contradicts the choice of b and d. Therefore, $T \subsetneq F$.

The next theorem is one of the characterizations mentioned earlier. It is taken from Schilling [16].

<u>Theorem 3.18</u>. Let $v:F \to G \cup \{z\}$ be a non-archimedian non-trivial valuation. Then v is of rank one if, and only if its valuation ring O is a maximal subring of F, that is, $O \subset O' \subseteq F$ for a ring O' implies $O' = F$.

Proof: Suppose v has rank one. Let O' be a ring such that $O \subset O' \subseteq F$. Let $O[x]$ be the ring of all polynomials with coefficients in O. Let $a \in O' - O$. Let $O[a] = \{p(a) \mid p(x) \in O[x]\}$. If $p(a) \in O[a]$ then $p(a) = a_0 + a_1 a + \ldots + a_n a^n$ where $a_i \in O$. Thus, $p(a) \in O'$, and so $O[a] \subseteq O'$. Let $b \in F - O$. Then there exists an integer $n > 0$ such that $v(b) \not> v^n(a)$ since $1 \not> v(a)$ and G is archimedian. Therefore, $v(b/a^n) = v(b)/v^n(a) \not> 1$ which implies that $b/a^n = c \in O$; hence $b = ca^n$. This implies $b \in O[a]$. Thus, $F \subseteq O[a]$ since $O \subseteq O[a]$ and $F = (F - O) \cup O$. Therefore, $F \subseteq O'$ which implies $F = O'$.

Now, suppose O is a maximal subring of F. Also, assume v is not of rank one. Then there exists an isolated subgroup H of G such that $H \neq \{1\}$ and $H \neq G$. Lemma 3.16 implies that $P' = \{a \in F \mid v(a) \in W \cup \{z\}\}$ where $W = G^- - H^-$ is a prime ideal of O and is properly contained in the ideal $P = \{a \in F \mid v(a) \not> 1\}$. Let $T = \{a/b \in F \mid a \in O, b \in O - P'\}$. Then Lemma 3.17 implies $O \subseteq T \subset F$. Thus $O = T$ since O is maximal. Now, let $a \in P - P'$. This implies that $1/a \in T = O$. Then $1 = (a)(1/a) \in P$ since P is an ideal of O. Thus, $v(1) \not> 1$, a contradiction. Therefore, v is of rank one.

Ths following discussion will perhaps point out why many writers prefer one of the classical definitions of a rank one valuation.

Let $v:F \to G \cup \{z\}$ be a non-archimedian rank one valuation. The ordered group G is order isomorphic to a subgroup of the multiplicative group of positive reals by Corollary 3.13. Let H be such a subgroup, and let $i:G \to H$ be the isomorphism. Let $\bar{i}:G \cup \{z\} \to H \cup \{0\}$ be a mapping defined as $\bar{i}(x) = i(x)$ for any $x \in G$, but $\bar{i}(z) = 0$ where 0 is the real number zero. Let $t:F \to H \cup \{0\}$ be the composition of the two functions v and $\bar{i}$. That is, $t(x) = \bar{i}\big(v(x)\big)$.

Suppose $t(F - \{0\}) = \{1\}$. This implies $\bar{i}\big(v(F - \{0\})\big) = i(G) = \{1\}$, and so $G = \{1\}$ since i is an isomorphism. However, this is a contradiction because G is of rank one. Therefore, $t(F - \{0\}) \neq \{1\}$.

Now, $t(0) = \bar{i}\big(v(0)\big) = \bar{i}(z) = 0$, and if $t(a) = 0$ then $\bar{i}\big(v(a)\big) = 0$ which implies $v(a) = z$ which implies $a = 0$. Hence, $t(a) = 0$ if, and only if $a = 0$.

Let $a,b \in F$. Then $t(ab) = \bar{i}\big(v(ab)\big) = \bar{i}\big(v(a)v(b)\big) =$
$\bar{i}\big(v(a)\big)\ \bar{i}\big(v(b)\big) = t(a)\ t(b)$.

Let $x,y \in G \cup \{z\}$ such that $x \ngeq y$. Let $<$ be the usual "less than" order relation in the reals. If $x \neq z$ and $y \neq z$ then $\bar{i}(x) = i(x) \leq i(y) = \bar{i}(y)$ since i is an order preserving isomorphism. If $x = z$ then $\bar{i}(x) = 0 \leq \bar{i}(y)$ since $0 \leq a$ for all $a \in H \cup \{0\}$. If $y = z$ then $x = z$ by definition of z as found in Definition 2.5. Then $\bar{i}(x) = 0 = \bar{i}(y)$. Therefore, $x \ngeq y$ implies $\bar{i}(x) \leq \bar{i}(y)$.

Let $x,y \in G \cup \{z\}$. If $x \ngeq y$ then $y = \max(x,y)$ and $\bar{i}(x) \leq \bar{i}(y)$; hence $\bar{i}\big(\max(x,y)\big) = \bar{i}(y) = \max\big(\bar{i}(x), \bar{i}(y)\big)$. If $y \ngeq x$ then a similar argument would again show that $\bar{i}\big(\max(x,y)\big) = \max\big(\bar{i}(x), \bar{i}(y)\big)$.

Let a,b $\in$ F. Then $v(a+b) \not> \max\big(v(a),\ v(b)\big)$. This implies $\bar{i}\big(v(a+b)\big) \not> \bar{i}\Big(\big(\max v(a),\ v(b)\big)\Big) = \max\Big(\bar{i}\big(v(a)\big),\ \bar{i}\big(v(b)\big)\Big)$; hence $t(a+b) \le \max\big(t(a),\ t(b)\big)$.

Thus, it has been shown that v induces a mapping $t{:}F \to R$ such that $t(F - \{0\}) \neq \{1\}$ with the following four properties

(a) $t(a) \ge 0$ for any $a \in F$

(b) $t(a) = 0$ if, and only if $a = 0$

(c) $t(ab) = t(a)\ t(b)$

(d) $t(a+b) \le \max\big(t(a),\ t(b)\big)$

Now, suppose $t{:}F \to R$ is a mapping with the above properties such that $t(F - \{0\}) \neq \{1\}$. It will be shown that t is a non-archimedian rank one valuation.

First of all, $H = t(F - \{0\})$ is a non-trivial multiplicative subgroup of the positive real numbers since t is a non-trivial homomorphism from $(F - \{0\})$ into the positive reals. Let $S = \{a \in H \mid a < 1\}$. Therefore, if $a,b \in H$ then $a < b$ if, and only if $ab^{-1} \in S$. Also, S is a normal subsemigroup since H is abelian and since $0 < a < 1$, $0 < b < 1$ imply $o < ab < 1$. Let $S^{-1} = \{a \in H \mid a^{-1} \in S\}$. Then $S^{-1} = \{a \in H \mid 1 < a\}$. Hence, $H = S \cup \{1\} \cup (S^{-1})$ where S, $\{1\}$ and S^{-1} are mutually disjoint. Thus, H is an ordered group. Let $a,b \in H$ such that $1 < a$. This implies that there exists an integer n such that $b < a^n$ since R has the archimedian property. Thus, H is archimedian, and so H is of rank one by Theorem 3.3. Therefore, t is a non-archimedian rank one valuation.

In the above remarks it has been shown that any non-archimedian rank one valuation induces a mapping t with properties (a), (b), (c) and (d), and conversely if a mapping has these properties then it is a non-archimedian rank one valuation. It should be pointed out that property (d) implies $t(a+b) \le t(a) + t(b)$ since $\max(t(a), t(b)) = t(a)$ or $t(b)$ and $t(a), t(b) \le t(a) + t(b)$. These facts could be the motivation for the following popular definition.

<u>Definition 3.19</u>. Let F be a field and $t: F \to R$ be a mapping such that $t(F - \{0\}) \ne \{1\}$ and satisfies the following conditions:

(a) $t(a) \ge 0$ for all $a \in F$

(b) $t(a) = 0$ if, and only if $a = 0$

(c) $t(ab) = t(a)\, t(b)$

(d) $t(a+b) \le \max(t(a), t(b))$

Then t is called a non-archimedian rank one valuation. If condition (d) is relaxed and replaced by

(d)′ $t(a+b) \le t(a) + t(b)$

then t is simply called a rank one valuation.

Henceforth, in this paper a rank one valuation or a non-archimedian rank one valuation will always be defined as a mapping with the properties as described in Definition 3.19.

An example of a rank one valuation will now be considered. Let $a \in R$ such that $0 < a \le 1$. Let Q be the rationals and $| \ | : Q \to R$ be the usual absolute value function. It can be shown that $| \ |^a$ is a rank one valuation. First of all it is clear that (a), (b) and (c) of Definition 3.19 are satisfied. Next, suppose that $x, y \in Q$ such that $|x| \le |y|$ and $y \ne 0$. Then

$$\begin{aligned} |x+y|^a &\le (|x| + |y|)^a \\ &= |y|^a \, (|x|/|y| + 1)^a \\ &\le |y|^a \, (|x|^a/|y|^a + 1) \ (\text{since } |x|/|y| \le 1,\ a \le 1) \\ &= |x|^a + |y|^a \end{aligned}$$

If $y = 0$ then $x = 0$ and $|x+y|^a = 0 = |x|^a + |y|^a$. If $|y| < |x|$ the argument would be similar. Therefore, (d)′ of Definition 3.19 is satisfied and $|\ |^a$ is a rank one valuation.

Another valuation on Q which is important and interesting is the p-adic valuation. It is described in the following example.

Example 3.20. Let p be a fixed prime integer, and let c be a real number such that $0 < c < 1$. Let $|\ |_p : Q \to R$ be a mapping such that $|0|_p = 0$ and $|x|_p = c^n$ for $x \neq 0$ and $x = p^n(a/b)$ where $p \nmid ab$.

Now, it will be shown that v is a non-archimedian rank one valuation. Parts (a) and (b) of Definition 3.19 are clearly satisfied. Now, if $x = p^n(a/b) \in Q$ and $y = p^m(c/d) \in Q$ such that $p \nmid ab$, $p \nmid cd$ and $x,y \neq 0$ then $|xy|_p = |p^{n+m}(ac/(bd))|_p$ and $p \nmid (ac)(bd)$; hence $|xy|_p = c^{n+m} = c^n c^m = |x|_p |y|_p$. If $x = 0$ or $y = 0$ then $|xy|_p = |0|_p = 0 = |x|_p |y|_p$. Thus, (c) of Definition 3.19 is verified. Suppose, $x \in Q$ such that $x \neq 0$ and $|x|_p \leq 1$. This implies that $x = p^n(a/b)$, $p \nmid ab$ and $n \geq 0$. Therefore, $p^n a$ is an integer and $1 + x = (b + p^n a)/b$. Now, if $(b + p^n a)/b$ is written as $p^m(c/d)$ where $p \nmid (cd)$ then $m \geq 0$, otherwise $p \mid b$ which is impossible. Therefore, $|1+x| = c^m \leq 1$. If $|x|_p \leq 1$ and $x = 0$ then $|1+x|_p = |1|_p = 1$. Thus, it has been shown that $|x|_p \leq 1$ implies $|1+x|_p \leq 1$ which implies $|x+y|_p \leq \max(|x|_p, |y|_p)$ by Theorem 3.23. Therefore, $|\ |_p$ is a non-archimedian rank one valuation.

It should be mentioned that the valuation ring of $|\ |_p$, $V = \{x \in Q \mid |x|_p \leq 1\} = \{a/b \in Q \mid p \nmid b\}$, is the ring of Example 2.11.

Definition 3.21. Let F be a field, n an arbitrary positive integer and 1 the unity element of F. The symbol n will also denote

$n \cdot 1 = 1 + 1 + \ldots + 1$ (n addends). Then n is called a natural number of F if, and only if $n \in F$.

The next theorem is taken from a problem in Borevich and Shafarevich [5].

Theorem 3.22. Let $t: F \to R$ be a rank one valuation where F is a field of characteristic $p \neq 0$. Then t is non-archimedean.

Proof: Let M be the set of all natural numbers of the field F. This implies $M = \{0, 1, 2, \ldots, p-1\}$ since F has characteristic $p \neq 0$. Let $d = \max\big(t(0), t(1), \ldots, t(p-1)\big)$. Let ℓ, m and n be positive integers such that $n = \ell + m$. Suppose $a, b \in F$ and $t(a) \le t(b)$. Then, $t^{\ell}(a)t^{m}(b) \le t^{n}(b) = \Big(\max\big(t(a), t(b)\big)\Big)^{n}$. If $t(b) < t(a)$ then again it could be shown that $t^{\ell}(a)t^{m}(b) \le \Big(\max\big(t(a), t(b)\big)\Big)^{n}$.

Now, let $a, b \in F$, and let n be a positive integer. Then,

$$t^{n}(a+b) = t\big((a+b)^{n}\big) = t\left(a^{n} + \binom{n}{1} a^{n-1}b + \ldots + \binom{n}{n-1} a\, b^{n-1} + b^{n}\right) \le$$

$$t(a^{n}) + t\binom{n}{1} t(a^{n-1})\, t(b) + \ldots + t\binom{n}{n-1} t(a)\, t(b^{n-1}) + t(b^{n}) =$$

$$t^{n}(a) + t\binom{n}{1} t^{n-1}(a)\, t(b) + \ldots + t\binom{n}{n-1} t(a)\, t^{n-1}(b) + t^{n}(b) \le$$

$$d\big(t^{n}(a) + t^{n-1}(a)\, t(b) + \ldots + t(a)\, t^{n-1}(b) + t^{n}(b)\big) \le$$

$$d\Big(\{\max\big(t(a), t(b)\big)\}^{n} + \{\max\big(t(a), t(b)\big)\}^{n} + \ldots + \{\max\big(t(a), t(b)\big)\}^{n} =$$

$$d(n+1)\, \{\max\big(t(a), t(b)\big)\}^{n}.$$

Therefore, $t(a+b) \le \big(d(n+1)\big)^{1/n} \max\big(t(a), t(b)\big)$. This implies

$$t(a+b) = \lim_{n\to\infty} t(a+b) \le \lim_{n\to\infty}\big(d(n+1)\big)^{1/n} \max\big(t(a), t(b)\big) = \max\big(t(a), t(b)\big)$$

since $\lim_{n\to\infty} \big(d(n+1)\big)^{1/n} = e^{\lim \frac{\ln(d(n+1))}{n}} = e^{0} = 1$. Thus, t is non-archimedean.

The next theorem is a statement of two characterizations of a non-archimedian valuation provided the valuation is rank one.

Theorem 3.23. Let $t:F \to R$ be a rank one valuation. The following three statements are logically equivalent.

(a) t is non-archimedian.

(b) $t(n) \leq 1$ for all natural numbers of F.

(c) $t(a) \leq 1$ implies $t(1+a) \leq 1$.

Proof:

(a) implies (b)

Let n be a natural number of F. Then $t(n) = t\,(1 + 1 + \ldots + 1) \leq \max\big(t(1), t(1), \ldots, t(1)\big) = \max\,(1, 1, \ldots, 1) = 1$

(b) implies (c)

Let m be a positive integer. Then $t^m(1+a) = t\big((1+a)^m\big) = t\big(1 + \binom{m}{1}a + \binom{m}{2}a^2 + \ldots + a^m\big) \leq t(1) + t\binom{m}{1}\, t(a) + t\binom{m}{2}\, t(a^2) + \ldots + t(a^m) \leq 1 + t(a) + t^2(a) + \ldots + t^m(a)$. Now, if $t(a) \leq 1$ then $t^k(a) \leq 1$ where k is a positive integer. Therefore, $t^m(1+a) \leq m + 1$ which implies $t(1 + a) \leq (m + 1)^{1/m}$, and so $t(1 + a) = \lim_{n\to\infty} t(1 + a) \leq \lim_{n\to\infty} (m + 1)^{1/m} = 1$

(c) implies (a)

Let $a,b \in F$ such that $a,b \neq 0$. Suppose $t(a) \leq t(b)$. Then $t(a/b) \leq t(a)/t(b) \leq 1$. This implies that $t(1 + a/b) \leq 1$; hence $t(b)\; t(1 + a/b) \leq t(b)$ which implies $t(a + b) = t\big(b(1 + a/b)\big) \leq \max\big(t(a), t(b)\big)$. If $t(b) < t(a)$ then the argument would be similar.

If $a = 0$ then $t(a + b) = t(b) = \max\big(t(a),\ t(b)\big)$. If $b = 0$ then $t(a + b) = t(a) = \max\big(t(a),\ t(b)\big)$.

Thus, the proof of this theorem which is stated as a problem in Borevich and Shafarevich [5] is complete.

Convergence and Completeness

In this section the notion of convergence of sequences, null sequences, Cauchy sequences and completeness will be defined. An interesting theorem concerning convergence of series will be proved, and the concept of p-adic numbers will be mentioned.

Definition 3.24. Let F be a field with a rank one valuation t. Let $\{a_n\}$ be a sequence of elements of F. The sequence $\{a_n\}$ is said to converge with respect to t to the element $a \in F$ if, and only if for any $\epsilon > 0$ there exists an integer N such that $t(a_n - a) < \epsilon$ for all $n > N$. In this case a is said to be the limit of $\{a_n\}$ and this is denoted by $\lim_t a_n = a$.

Definition 3.25. Let F be a field with a rank one valuation t. Let $\{a_n\}$ be a sequence of elements of F.

(a) $\{a_n\}$ is said to be a null sequence with respect to t if $\lim_t a_n = 0$.

(b) $\{a_n\}$ is said to be a Cauchy sequence with respect to t if for every $\epsilon > 0$ there exists an integer N such that $t(a_n - a_m) < \epsilon$ for all $n, m > N$.

(c) The infinite series $\sum_{n=1}^{\infty} a_n$ is said to converge with respect to t if the sequence $\{S_n\}$, where $S_n = a_1 + a_2 + \dots + a_n$, converges with respect to t to an element of F.

Definition 3.26. Let F be a field with a rank one valuation t. The field F is complete with respect to t if every Cauchy sequence with respect to t in F converges with respect to t to an element of F.

The next theorem states a necessary and sufficient condition for the convergence of a series in a field which is complete with respect to a non-archimedian valuation t. If the series $\sum_{n=1}^{\infty} a_n$ converges then it would be expected that $\lim_t a_n = 0$. However, the interesting part of this theorem is that the converse is true. The second part of the proof can be found in Bachman [2].

Theorem 3.27. Let F be a field which is complete with respect to a non-archimedian rank one valuation t. Let $\{a_n\}$ be a sequence of elements in F. Then $\sum_{n=1}^{\infty} a_n$ converges with respect to t if, and only if $\lim_t a_n = 0$.

Proof: Suppose $\sum_{n=1}^{\infty} a_n$ converges. This implies that there exists $s \in F$ such that $\lim_t S_n = s$ where $S_n = a_1 + \ldots + a_n$. Let $\epsilon > 0$. Then there exists an integer N such that $t(S_n - s) < \epsilon/2$ for $n > N$. Let $n > N + 1$. Then $t(a_n) = t(S_n - S_{n-1}) = t(S_n - s + s - S_{n-1}) \leq t(S_n - s) + t(s - S_{n-1}) < \epsilon/2 + \epsilon/2 = \epsilon$. Thus, $\lim_t a_n = 0$.

Now, assume $\lim_t a_n = 0$. Then there exists an N such that $t(a_n) < \epsilon$ if $n > N$. Let $n > m > N$, $S_n = a_1 + \ldots + a_n$ and $S_m = a_1 + \ldots + a_m$. This implies that $t(S_n - S_m) = t(a_{m+1} + a_{m+2} + \ldots + a_n) \leq \max\big(t(a_{m+1}), \ldots, t(a_n)\big) < \epsilon$; hence $\{S_n\}$ is a Cauchy sequence with respect to t. Therefore, $\{S_n\}$ converges to an element in F since F is complete with respect to t. Thus $\sum_{n=1}^{\infty}$ converges with respect to t.

The usual limit theorems still hold. For example, if F is a field with a valuation t and $\{a_n\}$ is a sequence in F that converges with respect to t then the limit is unique. Also, statements such as

$$\lim_t (a_n \pm b_n) = \lim_t a_n + \lim_t b_n$$

$$\lim_t a_n b_n = \lim_t a_n \lim_t b_n$$

$$\lim_t (a_n/b_n) = \lim_t a_n \,/\, \lim_t b_n \quad (\text{if } \lim_t b_n \neq 0)$$

are true provided $\lim_t a_n$ and $\lim_t b_n$ exist. These theorems can be proved by using the same techniques that are used in the proofs of the corresponding theorems in real analysis.

An interesting structure can be developed by completing the rational field with respect to the p-adic valuation of Example 3.20. The rationals can be completed with respect to the absolute value function by constructing the real numbers as a set of equivalence classes of Cauchy sequences (cf. Cohen and Ehrlich [9]). In a similar manner the rationals can be completed with respect to $|\ |_p$. This new structure is called the field of p-adic numbers. It has some interesting properties, but this paper will not probe into the rich theory of p-adic numbers.

Equivalent Valuations

In Chapter II, the concept of "equivalence" of non-archimedian valuations was defined (cf. Definition 2.18). Two non-archimedian valuations were said to be equivalent if they had the same associated valuation rings. However, a general rank one valuation may not determine a valuation ring in the usual manner. For example let $| \ |: Q \to R$ be the absolute value function. The set $V = \{x \in Q \mid |x| \leq 1\}$ is not even a ring much less a valuation ring. The pitfall is the fact that $| \ |$ does not have the non-archimedian property. Therefore, a more general definition of equivalence must be devised if all rank one valuations are to be included.

<u>Definition 3.28</u>. Let t_1 and t_2 be rank one valuations of the field F. Then t_1 and t_2 are called equivalent if, and only if $t_1(a) < 1$ implies $t_2(a) < 1$. This is denoted by $t_1 \sim t_2$.

<u>Theorem 3.29</u>. If $t_1 \sim t_2$ and $t_1(a) = 1$ then $t_2(a) = 1$.

Proof: Let F be the field over which t_1 and t_2 are defined. Let $b \in F$ such that $b \neq 0$ and $t_1(b) \neq 1$. Suppose $t_1(b) < 1$. Let n be a positive integer. Then $t_1(a^n b) = t_1^n(a)\, t_1(b) < 1$. Therefore, $t_2(a^n b) < 1$ since $t_1 \sim t_2$. This implies that $t_2(a) < \left(1/t_2(b)\right)^{1/n}$. Therefore, $t_2(a) = \lim_{n\to\infty} t_2(a) \leq \lim_{n\to\infty}\left(1/t_2(b)\right)^{1/n} = 1$. In a similar manner it can be shown that $t_2(1/a) \leq 1$; hence $1/t_2(a) \leq 1$ or $1 \leq t_2(a)$.

Thus, $t_2(a) = 1$. If $t_1(b) > 1$ then $t_1(1/b) < 1$ and the same type of argument would again prove $t_2(a) = 1$.

Theorem 3.30. $\sim$ is an equivalence relation.

Proof:

(a) Reflexive: If $t_1(a) < 1$ then $t_1(a) < 1$. Therefore, $t_1 \sim t_2$.

(b) Symmetric: Suppose $t_1 \sim t_2$. Let $a \in F$ such that $t_2(a) < 1$. If $t_1(a) > 1$ then $t_1(1/a) = 1/t(a_1) < 1$; hence $t_2(1/a) < 1$ which implies $1/t_2(a) < 1$ or $t_2(a) > 1$, a contradiction. If $t_1(a) = 1$ then $t_2(a) = 1$ by Theorem 3.29. This is also impossible. Therefore, $t_1(a) < 1$ which implies $t_2 \sim t_1$.

(c) Transitive: Suppose $t_1 \sim t_2$ and $t_2 \sim t_3$. Let $a \in F$ such that $t_1(a) < 1$. Then $t_2(a) < 1$ since $t_1 \sim t_2$. This implies $t_3(a) < 1$ since $t_2 \sim t_3$. Thus, $t_1 \sim t_3$.

The last two theorems were adapted from the book by Bachman [2]. The next theorem shows the new definition of equivalence is a generalization of the old one.

Theorem 3.31. Let $t_1, t_2 : F \to R$ be non-archimedian rank one valuations. Then $t_1 \sim t_2$ if, and only if t_1 and t_2 have the same associated valuation rings.

Proof: Assume $t_1 \sim t_2$. Let $V_1 = \{x \in F \mid t_1(x) \le 1\}$ and $V_2 = \{x \in F \mid t_2(x) \le 1\}$ be the valuation rings of t_1 and t_2 respectively. If $x \in V_1$ then $t_1(x) \le 1$ which implies $t_2(x) \le 1$ since $t_1 \sim t_2$ and by Theorem 3.29; hence $a \in V_2$ which implies $V_1 \subseteq V_2$. By using the fact that $t_2 \sim t_1$ and Theorem 3.29 it can also be shown that $V_2 \subseteq V_1$. Therefore, $V_1 = V_2$.

Assume $V_1 = V_2$. Let $a \in K$ such that $t_1(a) < 1$. This implies $a \in V_1$ which implies $a \in V_2$. Thus, $t_2(a) < 1$ and $t_1 \sim t_2$.

The next two theorems are adapted from a theorem and a problem in Bachman [2]. The first theorem shows that if two valuations are equivalent then one can be written as a power of the other. The second theorem is another characterization of equivalence.

Theorem 3.32. Let t_1, t_2:$F \to R$ be two rank one valuations such that $t_1 \sim t_2$. Then there exists a real number c such $c > 0$ and $t_2 = t_1^c$.

Proof: Let b be a fixed element of F such that $t_1(b) > 1$. Let $a \in F$ such that $a \neq 0$. Let $d = \ln t_1(a)/\ln t_1(b)$. Then $d \ln t_1(b) = \ln t_1(a)$ which implies $\ln t_1^d(b) = \ln t_1(a)$; hence $t_1(a) = t_1^d(b)$.

Now, suppose n and m are integers such that $n/m > d$. Then $t_1(a) < \left(t_1(b)\right)^{n/m}$ which implies $t_1{}^m(a) < t_1{}^n(b)$ and $t_1(a^m/b^n) < 1$. Therefore, $t_2(a^m/b^n) < 1$ since $t_1 \sim t_2$; hence $t_2(a) < \left(t_2(b)\right)^{n/m}$. Suppose $n/m < d$. Then in a similar manner it can be shown that $t_2(a) > \left(t_2(b)\right)^{n/m}$. These two facts imply $t_2(a) = t_2^d(b)$ for suppose not. Then $t_2(a) < \left(t_2(b)\right)^d$ or $t_2(a) > t_2^d(b)$. If $t_2(a) < t_2^d(b)$ then there exists a real number $e < d$ such that $t_2(a) = t_2^e(b)$ because the exponential function $y = t_2^x(b)$ is increasing and its range contains every positive real number, and in particular its range contains the positive number $t_2(a)$.

Now, there exists a rational number n/m such that $e < n/m < d$ since the rationals are dense in the reals. This implies $t_2(a) = t_2^e(b) < (t_2(b))^{n/m}$ since $y = t_2^x(b)$ is increasing. However, this is a contradiction since $t_2(a) > (t_2(b))^{n/m}$ if $n/m < d$. If $t_1(a) > t_2^d(b)$ then in a similar fashion another contradiction will be obtained. Thus, $t_2(a) = t_2^d(b)$.

Now, $\ell n\, t_2(a) = d\, \ell n\, t_2(b)$ which implies that $d = \ell n\, t_2(a)/\ell n\, t_2(b)$; hence

$$\ell n\, t_2(a)/\ell n\, t_2(b) = \ell n\, t_1(a)/\ell n\, t_1(b).$$

This implies that

$$\begin{aligned}\ell n\, t_2(a) &= \left(\ell n\, t_1(a)/\ell n\, t_1(b)\right) \ell n\, t_2(b) \\ &= \left(\ell n\, t_2(b)/\ell n\, t_1(b)\right) \ell n\, t_1(a)\end{aligned}$$

Now, let $c = \ell n\, t_2(b)/\ell n\, t_1(b)$. Then, $\ell n\, t_2(a) = c\, \ell n\, t_1(a)$ which implies $\ell n\, t_2(a) = \ell n\, t_1^c(a)$, so $t_2(a) = t_1^c(a)$.

If $a = 0$ then $t_2(a) = 0 = 0^c = (t_1(a))^c$.

Definition 3.33. Let $t:F \to R$ be a rank one valuation. Let $\{a_n\}$ be a sequence of elements of F. Then $\{a_n\}$ is called a null sequence with respect to t if $\lim_t a_n = 0$.

Theorem 3.34. Let $t_1, t_2:F \to R$ be rank one valuations. Then $t_1 \sim t_2$ if, and only if every null sequence with respect to t_1 is a null sequence with respect to t_2.

Proof: Suppose $t_1 \sim t_2$. Then there exists a positive real number c such that $t_2 = t_1^c$ by Theorem 3.32. Let $\{a_n\}$ be null with respect to t_1. Then for any $\in > 0$ there exists an M such that $t_1(a_n) < \in^{1/c}$ if $n > M$. This implies that $t_2(a_n) = t_1^c(a_n) < \in$. Therefore, $\{a_n\}$ is null with respect to t_n.

Suppose every null sequence with respect to t_1 is null with respect to t_2. Let $a \in F$ such that $t_1(a) < 1$. Let $\in > 0$. Then there exists an M such that $t_1(a^n) = t_1^n(a) < \in$ if $n > M$; thus $\{a^n\}$ is a null sequence with respect to t_1. Therefore, $\{a^n\}$ is null with respect to t_2, so there exists an M such that $t_2^M(a) = t_2(a^M) < 1$. This implies that $t_2(a) < 1$. Hence, $t_1 \sim t_2$.

CHAPTER IV

EXTENSIONS

In this chapter the problem of extending a mapping, a place and a valuation will be considered. First of all, it will be shown that a function which is defined on an integral domain and which has properties like a valuation can be extended to a valuation on the quotient field of the integral domain. Next, a classical theorem concerning the extension of a place will be proved. Also, it will be shown that a non-archimedean valuation can be extended over an arbitrary extension field. Finally, it will be demonstrated that a particular type rank one extension is unique. Some of the concepts of normed linear spaces are used in this uniqueness theorem.

Mappings and Places

Theorem 4.1. Let I be an integral domain of a field F. Let $K = \{a/b \mid a,b \in I, b \neq 0\}$. Then K is a field such that $I \subset K$.

Proof: Let $x,y \in K$. This implies that there exist a, b, c, $d \in I$ such that $b \neq 0$, $d \neq 0$, $x = a/b$ and $y = c/d$. Now, $x - y = (ad - bd)/bd$ and $bd \neq 0$ since I has no divisors of zero. Thus, $x - y \in K$ which implies K is an additive subgroup of F.

If $x,y \in (K - \{0\})$ then $x = a/b$ and $y = c/d$ where a, b, c, $d \neq 0$. Hence, $x/y = ad/bc$ and $bc \neq 0$. Therefore, $(K - \{0\})$ is a multiplicative subgroup of $(F - \{0\})$. Then K is a subfield of F.

The domain I is contained in K since $1 \in I$ and $I = \{a/1 \mid a \in I\}$.

Definition 4.2. If I is an integral domain of a field F then the field $K = \{a/b \mid a,b \in I, b \neq 0\}$ is called the quotient field of I.

The next theorem is adapted from a similar one in Bachman [2].

Theorem 4.3. Let I be an integral domain of a field F. Let v be a mapping from I into the reals R such that

(a) $v(a) \geq 0$

(b) $v(a) = 0$ if, and only if $a = 0$

(c) $v(ab) = v(a)\ v(b)$

(d) $v(a+b) \leq v(a) + v(b)$

Then v can be extended uniquely to a rank one valuation on the quotient field K of I.

Proof: Let $t:K \to R$ be defined as $t(x) = v(a)/v(b)$ for any $x = a/b \in K$ where $a,b \in I$ and $b \neq 0$. Suppose there exist a, b, c, $d \in I$ such that b, $d \neq 0$ and $a/b = c/d$. This implies $ad = bc$, and $v(ad) = v(bc)$ which implies $v(a)\ v(d) = v(b)\ v(c)$. Thus $v(a)/v(b) = v(c)/v(d)$; hence $t(a/b) = t(c/d)$ and t is well defined.

Now, it will be shown that t is a valuation on K. Let $x = a/b \in K$. Then $t(x) = v(a)/v(b) \geq 0$ since $v(a)$, $v(b) \geq 0$. If $t(x) = v(a)/v(b) = 0$ then $v(a) = 0$ which implies $x = a/b = 0$. If $y = c/d \in K$ then $t(xy) = t(ac/bd) = v(ac)/v(bd) = v(a)v(c)/v(b)v(d) = [v(a)/v(b)]\ [v(c)/v(d)] = t(x)t(y)$. Thus, conditions (a), (b) and (c) are satisfied. Also, $x + y = a/b + c/d = (ad + bc)/bd$, and so $t(x + y) = v(ad + bc)/v(bd) \leq [v(ad) + v(bc)]/v(bd) = v(ad)/v(bd) + v(bc)/v(bd) = v(a)/v(b) + v(c)/v(d) = t(x) + t(y)$. Hence, t is a valuation on K.

Next, it can be shown that t is an extension of v. Let $a \in I$. Then $a = ab/b$ where $b \in I$, but $b \neq 0$. This implies that $t(a) = v(ab)/v(b) = v(a)v(b)/v(b) = v(a)$.

Suppose there exists a valuation $s: K \to R$ such that s agrees with v on I. If $x = a/b \in K$ then $s(x) = s(a/b) = s(a)/s(b) = v(a)/v(b) = t(x)$. Therefore, t is unique, and the theorem is proved.

Before stating and proving the so called Fundamental Theorem of Places, some definitions and lemmas will be considered. First of all, if A is a subring of a field K then $A[x]$ will denote the ring of all polynomials with coefficients in A. Also, if $\alpha \in K$ then $A[\alpha]$ is the set $\{P(\alpha) \mid P(x) \in A[x]\}$. It can be shown that $A[\alpha]$ is a subring of K, for, if $P_1(\alpha), P_2(\alpha) \in A[\alpha]$ then $P_1(\alpha) - P_2(\alpha) = (P_1 - P_2)(\alpha) \in A[\alpha]$, and $P_1(\alpha)P_2(\alpha) = (P_1 P_2)(\alpha) \in A[\alpha]$. An important fact that will be used in the proof of one of the lemmas is that if F is a field then $F[x]$ is a principal ideal domain (cf. Moore [15], p. 164).

Definition 4.4. Let F be a field. Then F is said to be algebraically closed or algebraically complete if, and only if every non-constant polynomial with coefficients in F splits in F (i.e. if $P(x) \in F[x]$ and $P(x)$ is not constant then there exists $k_1, k_2, \ldots, k_n \in F$ such that $P(x) = a_n (x - k_1)(x - k_2) \ldots (x - k_n)$ where a_n is the leading coefficient of $P(x)$).

Lemma 4.5. Let A be a subring of a field K. Let F be a field, and let $f: A \to F$ be a non-trivial homomorphism. Let $S = \{a \in A \mid f(a) \neq 0\}$. Then

(a) $A' = \{a/b \mid a \in A, b \in S\}$ is a subring of K such that $1 \in A'$ and $A \subseteq A'$

(b) there exists a homomorphism $f':A' \to F$ such that $f'|_A = f$.

Proof:

(a) Let $x,y \in A'$. Then there exists $a,c \in A$ and $b,d \in S$ such that $x = a/b$ and $y = c/d$. Therefore $x - y = (ad - bc)/(bd)$. Now, $f(bd) = f(b)\ f(d) \neq 0$ since $f(b), f(d) \neq 0$ and F is a field. Thus, $bd \in S$ which implies $x - y \in A'$. Also, $xy = (ac)/(bd) \in A'$. Hence, A' is a subring of K.

Let $b \in S \subseteq A$. Then, $1 = b/b \in A'$. Also, if $a \in A$ and $b \in S$ then $a = ab/b \in A'$ which implies $A \subseteq A'$.

(b) Define $f':A' \to F$ as $f'(a/b) = f(a)/f(b)$ for all $a/b \in A'$. Suppose $a/b = c/d$. Then $ad = bc$, and so $f(ad) = f(bc)$ which implies $f(a)\ f(d) = f(b)\ f(c)$; hence $f(a)/f(b) = f(c)/f(d)$. Therefore, $f'(a/b) = f'(c/d)$ and f' is well defined.

Now, $f'(a/b + c/d) = f'([ad + bc]/bd) = f(ad + bc)/f(bd) = [f(a)\ f(d) + f(b)\ f(c)]/[f(b)\ f(d)] = f(a)/f(b) + f(c)/f(d) = f'(a/d) + f'(c/d)$. Also, $f'(a/b \cdot c/d) = f'\ (ac/bd) = f(ac)/f\ (bd) = [f(a)/f(b)][f(c)/f(d)] = f'(a/b)\ f'(c/d)$. Hence, f' is a ring homomorphism.

Let $a \in A$ and $b \in S$. Then $f'(a) = f'(ab/b) = f(ab)/f(b) = f(a)\ f(b)/f(b) = f(a)$. Therefore, $f'|_A = f$.

Of course, it is possible that the quotient ring A' is the same as A. Then f' is really not an extension. However, the next lemma shows that f can still be extended even though $A = A'$, provided F is algebraically closed.

<u>Lemma 4.6</u>. Let A be a subring of a field K. Let F be an algebraically closed field. Let $f: A \to F$ be a non-trivial homomorphism. Let $S = \{a \in A \mid f(a) \neq 0\}$ and $A' = \{a/b \mid a \in A, b \in S\}$. If $A = A'$ then f can be extended to $A[\alpha]$ or to $A[\alpha^{-1}]$ where α is an arbitrary element of K.

Let $F_o = f(A)$. Then F_o is a subring of F since f is a homomorphism and A is a ring. Also, $1 \in F_o$ since $1 \in A' = A$ and $f(1) = 1$. Let $c \in F_o$ such that $c \neq 0$. Then there exists $a \in A$ such that $c = f(a) \neq 0$; hence $a \in S$. This implies that $a^{-1} = 1/a \in A' = A$. Therefore, $1 = f(1) = f(a \cdot a^{-1}) = f(a)\ f(a^{-1}) = c\ f(a^{-1})$. Thus c has an inverse in F_o, and this implies that F_o is a field.

Now, define $h: A[x] \to F_o[x]$ as follows: if $P(x) = a_o + a_1 x + \ldots + a_n x^n$ then $h\big(P(x)\big) = f(a_o) + f(a_1)x + \ldots + f(a_n)x^n$. Let $\alpha \in K$ and assume that there exists $P(x) \in A[x]$ such that $P(\alpha) = 0$ but $\overline{P}\ (\beta) \neq 0$ for all $\beta \in F$ where $\overline{P}(x) = h\big(P(x)\big)$. Let $I = \{P(x) \in A[x] \mid P(\alpha) = 0\}$. The set I is an ideal in $A[x]$ since $P_1(x)$, $P_2(x) \in I$ imply $P_1(\alpha) - P_2(\alpha) = P_1(\alpha)\ P_2(\alpha) = 0$ and since $P_3(x) \in A[x]$ implies $P_1(\alpha)\ P_3(\alpha) = 0 \cdot P_3(\alpha) = 0$. Also, $h(I)$ is an ideal of $F_o[x]$ since h is a homomorphism and I is an ideal of $F_o[x]$. Thus, $h(I)$ is a principal ideal since $F_o[x]$ is a principal ideal domain. Therefore, there exists a polynomial $Q(x) \in F_o[x]$ such that $h(I) = Q(x)\ F_o[x] = \{Q(x)\ R(x) \mid R(x) \in F_o[x]\}$. However, $Q(x)$ must be a non-zero constant, otherwise there exists $\beta \in F$ such that $Q(\beta) = 0$ since F is algebraically closed. This would imply that for every $P(x) \in A[x]$ such that $P(\alpha) = 0$ then $\overline{P}(\beta) = 0$ where $\overline{P}(x) = h\big(P(x)\big)$, a contradiction of the assumption. Therefore,

$h(I) = c\, F_o[x] = F_o[x]$ which implies $1 \in h(I)$; hence there exists $Q_1(x) = b_o + a_1x + \ldots + a_nx^n \in I$ such that $1 = h(Q_1(x)) = f(b_o) + f(a_1)x + \ldots + f(a_n)x^n$. Thus, $f(b_o) = 1$ and $f(a_1) = f(a_2) = \ldots = f(a_n) = 0$. Let $a_o = b_o - 1$. Then $Q_1(x) = 1 + a_o + a_1x + \ldots + a_nx^n$, $f(a_o) = f(b_o - 1) = f(b_o) - f(1) = 1 - 1 = 0$ and $o = Q_1(\alpha) = 1 + a_o + a_1\alpha + \ldots + a_n\alpha^n$.

Also, assume that there exists $P(x) \in A[x]$ such that $P(\alpha^{-1}) = 0$ but $\overline{P}(\beta) \neq 0$ for all $\beta \in F$. Then, by a similar argument it can be shown that there exists elements $c_o, c_1, \ldots, c_m \in A$ such that $f(c_o) = f(c_1) = \ldots = f(c_m) = 0$ and $1 + c_o + c_1\alpha^{-1} + \ldots + c_m\alpha^{-m} = 0$. Suppose that n and m are the smallest integers such that

$$1 + a_o + a_1\alpha + \ldots + a_n\alpha^n = 0,$$

$$1 + c_o + c_1\alpha^{-1} + \ldots + c_m\alpha^{-m} = 0,$$

$a_o, \ldots, a_n, c_o, \ldots, c_m \in A$ and $f(a_o) = \ldots = f(a_n) = f(c_o) = \ldots = f(c_m) = 0$. Also, suppose $m \leq n$. If $n = 0$ then $1 + a_o = 0$ which implies $0 = f(0) = f(1+a_o) = f(1) + f(a_o) = f(1)$. But, this is impossible since f is non-trivial. Therefore $n \geq 1$. Also, it can be shown that $m \geq 1$.

Now, $\alpha^m = [-c_1/(1+c_o)]\alpha^{m-1} + \ldots + [-c_m/(1+c_o)]$. Let $d_o = -c_m/(1+c_o), \ldots, d_{m-1} = -c_1/(1+c_o)$. The element $1 + c_o \in S$ since $f(1 + c_o) = f(1) + f(c_o) = f(1) = 1 \neq 0$. Thus, $d_o, \ldots, d_{m-1} \in A' = A$. Also, $f(d_o) = \ldots = f(d_{m-1}) = 0$, and $\alpha^m = d_o + d_1\alpha + \ldots + d_{m-1}\alpha^{m-1}$.

Next, $\alpha^n = \alpha^m(\alpha^{n-m})$ and $n - m \geq 0$; hence $0 = 1 + a_o + a_1\alpha + \ldots + a_n\alpha^m(\alpha^{n-m}) = 1 + a_o + a_1\alpha + \ldots + a_n\alpha^{n-m}(d_o + d_1\alpha + \ldots + d_{m-1}\alpha^{m-1})$. But, the highest power of α is $n-1$ which contradicts the fact that n is minimal.

Therefore, the two assumptions about α and α^{-1} cannot hold simultaneously. Now, suppose there exists $\beta \in F$ such that for all $P(x) \in A[x]$ where $P(\alpha) = 0$ then $\overline{P}(\beta) = 0$ where $\overline{P}(x) = h(P(x))$. Then define $g: A[\alpha] \to F$ as $g(P(\alpha)) = \overline{P}(\beta)$. Let $P(\alpha), Q(\alpha) \in A[\alpha]$. This implies $g(P(\alpha)\ Q(\alpha)) = g\ PQ(\alpha) = \overline{PQ}(\beta)$. But, $\overline{PQ}(x) = h(PQ(x)) = h(P(x)\ Q(x)) = h(P(x))h(Q(x)) = \overline{P}(x)\ \overline{Q}(x)$; hence $\overline{PQ}(\beta) = \overline{P}(\beta)\ \overline{Q}(\beta)$, and so $g(P(\alpha)\ Q(\alpha)) = g(P(\alpha))\, g(Q(\alpha))$. In a similar manner it can be shown that $g(P(\alpha) + Q(\alpha)) = g(P(\alpha)) + g(Q(\alpha))$. Therefore, if g is well defined then g is a homomorphism. Let $P(\alpha), Q(\alpha) \in A[\alpha]$ such that $P(\alpha) = Q(\alpha)$. This implies $(P-Q)(\alpha) = P(\alpha) - Q(\alpha) = 0$; thus $\overline{(P-Q)}(\beta) = 0$. Therefore, $g((P-Q)(\alpha)) = 0$ which implies $g(P(\alpha) - Q(\alpha)) = 0$, and so $g(P(\alpha)) = g(Q(\alpha))$. Therefore, g is well defined and is a homomorphism. Now, let $a = P(\alpha) \in A \subset A[\alpha]$. Then $g(a) = \overline{P}(\beta)$ where $\overline{P}(x) = h(P(x)) = h(a) = f(a)$. Thus f has been extended to $A[\alpha]$.

If there exists $P(x) \in A[x]$ such that $P(\alpha) = 0$ but $\overline{P}(\beta) \neq 0$ for all $\beta \in F$ then it has been shown that there exists $\beta \in F$ such that for all $P(x) \in A[x]$ where $P(\alpha^{-1}) = 0$ then $\overline{P}(\beta) = 0$. In this case it can be shown by a similar argument that f can be extended to $A[\alpha^{-1}]$.

The last two lemmas and the next theorem have been adapted from a theorem in Bachman [2]. Before proving the next theorem some concepts concerning Zorn's Lemma must be introduced. After this the lemma itself will be stated without proof.

<u>Definition 4.7</u>. A set A is said to be partially ordered if there is a relation $\leq$ defined on A such that

(a) $a \leq b$, $b \leq c$ imply $a \leq c$

(b) $a \leq a$ for all $a \in A$

(c) $a \leq b$, $b \leq a$ imply $a = b$.

If A is partially ordered and $a \leq b$ or $b \leq a$ for all $a,b \in A$ then A is said to be totally ordered.

<u>Definition 4.8</u>. Let A be a partially ordered set. Let $B \subseteq A$ and $a \in A$. The element a is called an upper bound of B if $b \leq a$ for all $b \in B$. If $c = a$ for all $c \in A$ such that $a \leq c$ then a is said to be a maximal element of A.

<u>Lemma 4.9 (Zorn's Lemma)</u>. Let A be a partially ordered set such that every totally ordered subset of A has an upper bound in A. Then A has a maximal element.

<u>Theorem 4.10 (Fundamental Theorem of Places)</u>. Let A be a subring of a field K. Let F be an algebraically closed field. Let $f:A \to F$ be a non-trivial homomorphism. Then there exists a place $H:K \to F \cup \{\infty\}$ such that $H\big|_A = f$.

Proof: Let $E = \{g:R \to F \mid g$ is a homomorphism, R is a subring of $K, A \subseteq R$ and $g(a) = f(a)$ for all $a \in A\}$. In other words E is the set of all extensions of f to a larger subring of K. Define a relation $\leq$

on E as follows: $g_1 \le g_2$ if, and only if g_2 is an extension of g_1. It is clear that $\le$ satisfies (a), (b) and (c) of Definition 4.7. Thus, E is a partially ordered set.

Let $\{g_\alpha\}$ be a totally ordered subset of E. Let $\{A_\alpha\}$ be the set of rings over which the elements of $\{g_\alpha\}$ are defined. Then $\{A_\alpha\}$ is totally ordered by the relation $\subseteq$ (i.e. $\{A_\alpha\}$ is partially ordered by $\subseteq$ and if $A_\alpha, A_\beta \in \{A_\alpha\}$ then $A_\alpha \subseteq A_\beta$ or $A_\beta \subseteq A_\alpha$). Let $R = \bigcup_\alpha A_\alpha$. If $a,b \in R$ then there exists α, β such that $a \in A_\alpha$ and $b \in A_\beta$. Also, $A_\alpha \subseteq A_\beta$ or $A_\beta \subseteq A_\alpha$. Without loss of generality suppose $A_\alpha \subseteq A_\beta$. Then $a,b \in A_\beta$, and $a-b$, $ab \in A_\beta \subseteq R$. Therefore, R is a subring of K. Now, define $g\colon R \to F$ in the following way. If $a \in R$ then $a \in A_\alpha$ for some α. Let $g(a) = g_\alpha(a)$. If $a \in A_\beta$ where $\alpha \ne \beta$ then $g_\alpha(a) = g_\beta(a)$ since $\{g_\alpha\}$ is totally ordered (i.e. since g_α is an extension of g_β or vice versa). Thus, g is well defined. Let $a,b \in R$. This implies that there exists an α such that $a,b \in A_\alpha$; hence $a+b$, $ab \in A_\alpha$ since A_α is a ring. Thus, $g(a+b) = g_\alpha(a+b) = g_\alpha(a) + g_\alpha(b) = g(a) + g(b)$, and $g(ab) = g_\alpha(ab) = g_\alpha(a)\, g_\alpha(b) = g(a)\, g(b)$. Therefore, g is a homomorphism. Now, let g_α be an element of $\{g_\alpha\}$. Then $A_\alpha \subseteq R$ and $g_\alpha(a) = g(a)$ for any $a \in A_\alpha$; thus $g_\alpha \le g$. Therefore, g is an upper bound of $\{g_\alpha\}$.

Now, it has been shown that every totally ordered subset of E has an upper bound. Therefore, by Zorn's Lemma E has a maximal element. Let $h\colon V \to F$ be a maximal element of E. This implies that if $h \le k$ then $h = k$. Therefore, h has no extension distinct from itself.

Lemma 4.5(b) and the above remark imply that $V = V'$ where $V' = \{a/b \mid a \in V,\ b \in S\}$ and $S = \{a \in V \mid h(a) \neq 0\}$. Also, if $\alpha \in K - V$ then $V[\alpha] \neq V$; hence h cannot be extended to $V[\alpha]$. Therefore, h can be extended to $V[\alpha^{-1}]$ by Lemma 4.6; hence $V = V[\alpha^{-1}]$ since h is a maximal element of E. This implies $\alpha^{-1} \in V$. Thus, by Definition 2.10, V is a valuation ring.

Now, define $H:K \to F \cup \{\infty\}$ as $H(a) = h(a)$ if $a \in V$, and $H(a) = \infty$ if $a \notin V$. Hence,

$H^{-1}(F) = V$, a ring,

and $H|_V$, a non-trivial homomorphism.

Therefore, by Definition 2.13, H will be a place if $H(a) = \infty$ implies $H(a^{-1}) = 0$. Let $a \in K$ such that $H(a) = \infty$. This implies $a \notin V$ which implies $a^{-1} \in V$ since V is a valuation ring. Now, if $h(a^{-1}) \neq 0$ then $a^{-1} \in S$ which implies $a = 1/a^{-1} \in V'$ since 1 is always an element of a valuation ring such as V. Thus, $a \in V$ since $V = V'$, a contradiction. Therefore, $h(a^{-1}) = 0$ which implies $H(a^{-1}) = 0$; hence H is a place. Also, $H|_A = f$ since $H|_V = h$ and $h|_A = f$.

Valuations

Definition 4.11. Let k be a subfield of a field K. Then K is called an extension field of k.

Theorem 4.12. Let $v:k \to G \cup \{z\}$ be a non-archimedian valuation. Let K be an extension of k. Then there exists a non-archimedian valuation $t:K \to G_1 \cup \{z\}$ where G is a subgroup of G_1 and $t|_k = v$.

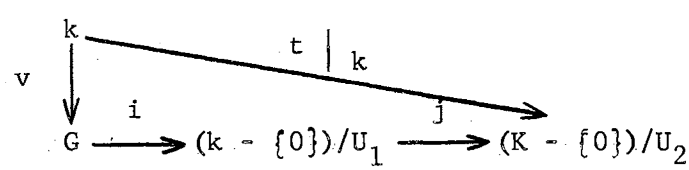
Proof: Let V_1, U_1, P_1 be the valuation ring, units and non-units associated with v. Let $\varphi:k \to (V_1/P_1) \cup \{\infty\}$ be the place associated with v (cf. Theorem 2.14). Now, $U_1 = \{a \in k \mid v(a) = 1\}$ is the kernal of the homomorphism $v:(k - \{0\}) \to G$. Thus, there exists an isomorphism $i:G \to (k - \{0\})/U_1$ such that $i(v(a)) = a\, U_1$ by the Fundamental Theorem of Homomorphisms (cf. Barnes [3], p. 47). In the proof of Theorem 2.16 it was shown that $(k - \{0\}/ U_1$ is an ordered group with normal subsemigroup $\overline{S}_1 = \{a\, U_1 \in (k - \{0\})/ U_1 \mid a \in P_1 - \{0\}\}$ where $\overline{S}_1$ determines the ordering of $(k - \{0\})/ U_1$ (i.e. $a\, U_1 \not\geq b\, U_1$ if, and only if $(a\, U_1)(b\, U_1)^{-1} \in \overline{S}_1$). Let $v(a)$, $v(b) \in G$ such that $v(a) \not\geq v(b)$. Then $v(a/b) = v(a)/v(b) \not\geq 1$ which implies $a/b \in P_1 - \{0\}$ since $P_1 = \{a \in k \mid v(a) \not\geq 1\}$ and $a/b \in k - \{0\}$. Thus, $(a/b)\, U_1 \in \overline{S}_1$ which implies $(a\, U_1)\ (b\, U_1)^{-1} = (a/b)\, U_1 = (a/b)\, U_1 \cdot 1^{-1} \in \overline{S}_1$; hence $(a\, U_1)\ (b\, U_1)^{-1} \not\geq 1$ which implies $a\, U_1 \not\geq b\, U_1$, and so $i(v(a)) \not\geq i(v(b))$. Therefore, G is order isomorphic to $(k - \{0\})/ U_1$.

The function $\varphi \mid_{V_1} : V_1 \to (V_1/P_1)$ is a non-trivial homomorphism by Definition 2.13. Let F be an extension of (V_1/P_1) such that F is an algebraically closed field (such an extension always exists cf. Barnes [3], p. 197). Therefore, there exists a place $\psi:K \to F \cup \{\infty\}$ such that $\psi \mid_{V_1} = \varphi \mid_{V_1}$ by Theorem 4.10. Hence, there is an associated valuation ring $V_2 = \psi^{-1}(F)$ with units U_2 and non-units P_2, and there is an associated non-archimedian valuation $t:K \to [(K - \{0\})/U_2] \cup \{z\}$ where

$t(a) = a\, U_2$ if $a \neq 0$ and $t(0) = z$ (cf. Theorems 2.14 and 2.16).

Now, it will be shown that $V_1 = k \cap V_2$, $P_1 = k \cap P_2$ and $U_1 = k \cap U_2$. Let $x \in V_1$. This implies that $\varphi(a) \in F$ which implies $\psi(a) \in F$ since $\varphi(a) = \psi(a)$; hence $a \in \psi^{-1}(F) = V_2$. Therefore, $V_1 \subseteq V_2$ which implies $V_1 \subseteq k \cap V_2$. Suppose $\psi(x) = 0$ and $\psi(x^{-1}) \neq \infty$. Then $x, x^{-1} \in \psi^{-1}(F) = V_2$; hence $\psi(1) = \psi(x\, x^{-1}) = \psi(x)\, \psi(x^{-1}) = 0$ which implies $\psi \big|_{V_2}$ is trivial, a contradiction. Therefore, if $\psi(x^{-1}) \neq \infty$ then $\psi(x) \neq 0$. Now, let $a \in k \cap V_2$. Then $a \in V_2 = \psi^{-1}(F)$ which implies $\psi(a) \neq \infty$, and $\psi(a^{-1}) \neq 0$. Also, $\varphi(a^{-1}) \neq 0$ otherwise $a^{-1} \in \varphi^{-1}(F) = V_1$, and $\psi(a^{-1}) = 0$ since $\varphi \big|_{V_1} = \psi \big|_{V_1}$; thus $\varphi(a) \neq \infty$ by Definition 2.13. Then $a \in V_1 = \varphi^{-1}(F)$ which implies $k \cap V_2 \subseteq V_1$, and $V_1 = k \cap V_2$. Thus, $K - V_1 = K - (k \cap V_2) = (K - k) \cup (K - V_2)$. Therefore, $k - V_1 = (k \cap K) - V_1 = (k \cap K) \cap \tilde{V}_1 = k \cap (K \cap \tilde{V}_1) = k \cap (K - V_1) = k \cap [(K-k) \cup (K-V_2)] = k \cap (K-V_2)$. Now, $k = P_1 \cup U_1 \cup (P_1 - \{0\})^{-1} = V_1 \cup (P_1 - \{0\})^{-1}$ and $K = P_2 \cup U_2 \cup (P_2-\{0\})^{-1} = V_2 \cup (P_2 - \{0\})^{-1}$ by Theorem 2.12; hence $(P_1 - \{0\})^{-1} = k - V_1 = k \cap (K - V_2) = k \cap (P_2 - \{0\})^{-1}$. Let $x \in P_1$ such that $x \neq 0$. Then $x^{-1} \in (P_1 - \{0\})^{-1}$ which implies $x^{-1} \in k \cap (P_2 - \{0\})^{-1}$; thus $x \in k \cap P_2$. If $x \in k \cap P_2$ such that $x \neq 0$ then $x^{-1} \in k \cap (P_2 - \{0\})^{-1} = (P_1 - \{0\})^{-1}$, and $x \in P_1$. Therefore, $P_1 = k \cap P_2$. Also, $U_1 = V_1 - P_1 = (k \cap V_2) - (k \cap P_2) = (k \cap V_2) \cap (\widetilde{k \cap P_2}) = [(k \cap V_2) \cap \tilde{k}] \cup [(k \cap V_2) \cap \tilde{P}_2] = k \cap (V_2 - P_2) = k \cap U_2$.

Next, it will be shown that $(k - \{0\})/U_1$ can be imbeded in $(K - \{0\})/U_2$ by an order isomorphism. Let $j:(k - \{0\})/U_1 \to (K - \{0\})/U_2$ be defined as $j(a\,U_1) = a\,U_2$. To show that j is well defined, let $a\,U_1 = b\,U_1$. Then $(a\,U_1)\,(b\,U_1)^{-1} = 1 \cdot U_1$ which implies $(ab^{-1})U_1 = 1 \cdot U_1$; thus $a\,b^{-1} \in U_1$ which implies $a\,b^{-1} \in U_2$ since $U_1 = k \cap U_2$. Therefore, $(a\,b^{-1})U_2 = 1 \cdot U_2$, and so $j(a\,U_1) = a\,U_2 = b\,U_2 = j(b\,U_2)$; hence j is well defined. Also, $j[(aU_1)\,(bU_1)] = j[(ab)U_1] = (ab)\,U_2 = (aU_2)(bU_2) = j(aU_1)\,j(bU_1)$. Thus, j is a homomorphism. Let $aU_1 \in (k - \{0\})/U_1$ such that $j(aU_1) = 1 \cdot U_2$. Then $aU_2 = 1 \cdot U_2$ which implies $a \in U_2$. Thus, $a \in U_1$ since $U_1 = k \cap U_2$ and $a \in k$; hence $aU_1 = 1 \cdot U_1$, and j is an isomorphism. Now, let aU_1, $bU_1 \in (K - \{0\})/U_1$ such that $aU_1 \not\geq bU_1$. Then $(a\,b^{-1})U_1 = (aU_1)(bU_1)^{-1} \in \bar{S}_1$; hence $a\,b^{-1} \in P_1 = k \cap P_2$ and $a\,b^{-1} \neq 0$. Thus, $(a\,b^{-1})U_2 \in \bar{S}_2 = \left\{aU_2 \mid a \in P_2 - \{0\}\right\}$, the normal subsemigroup of $(K - \{0\})/U_2$. Therefore, $(a\,b^{-1})U_2 \not\geq 1 \cdot U_2$ which implies $aU_2 \not\geq bU_2$, and j is an order isomorphism.



Now, it can be shown that $t\,|_k = j \circ i \circ v$. Let $a \in k$. Then $(j \circ i \circ v)(a) = j\Big(i\big(v(a)\big)\Big) = j(aU_1) = aU_2 = t(a)$. Thus, $t\,|_k = j \circ i \circ v$ which implies $t\,|_k = v$ up to an order isomorphism, and so the proof is complete.

Normed Linear Spaces and Uniqueness

Definition 4.13. Let A be a set and F a field such that

(a) A is an additive abelian group, and

(b) if $c \in F$ and $x \in A$ there exists a unique element $cx \in A$ called the product of c and x such that $c(dx) = (cd)x$ and $1 \cdot x = x$ for all $c, d \in F$ and $x \in A$, and

(c) if $x, y \in A$ and $c, d \in F$ then $c(x+y) = cx + cy$ and $(c+d)x = cx + dx$.

Then A is said to be a linear space (or vector space) over F. If $B \subseteq A$ and B is also a linear space over F with respect to the operations that are inherited from A then B is called a subspace of A. An element of A is called a vector.

Theorem 4.14. Let A be a linear space over F. Let $\{x_1, \ldots, x_n\}$ be a subset of A and $B = \{c_1 x_1 + \ldots + c_n x_n \mid c_i \in F\}$. Then B is a subspace of A.

Proof: Let $x, y \in B$. Then $x = c_1 x_1 + \ldots + c_n x_n$ and $y = d_1 x_1 + \ldots + d_n x_n$ where $c_i, d_i \in F$. Thus, $x - y = (c_1 - d_1)x_1 + \ldots + (c_n - d_n)x_n \in B$ which implies B is an additive subgroup of A. Let $c \in F$. Then $cx = (c\, c_1)x_1 + \ldots + (c\, c_n)x_n \in B$. All of the other properties of a linear space are inherited from A. Hence, B is a subspace of A.

Definition 4.15. Let A be a linear space over F. Let $x_1, x_2, \ldots, x_n \in A$ and $B = \{c_1 x_1 + \ldots + c_n x_n \mid c_i \in F\}$. Then B is called the subspace spanned by $x_1, \ldots, x_n$.

Definition 4.16. Let A be a linear space over F. Let $\{x_1, \ldots, x_n\} \subseteq$ A such that $c_1 x_1 + \ldots + c_n x_n = 0$ implies $c_1 = \ldots = c_n = 0$ and such that for any $x \in A$ there exist $c_1, \ldots, c_n \in F$ such that $x = c_1 x_1 + \ldots + c_n x_n$. Then, the set $\{x_1, \ldots, x_n\}$ is said to be a basis for A, and A is an n-dimensional linear space (vector space).

Theorem 4.17. Let k be a field and K an extension field of k. Then K is a linear space over k.

Proof: K is an additive abelian group since it is a field. Let $c,d \in k$ and $x,y \in K$. Then $cx \in K$ since K is closed under multiplication, $c(dx) = (cd)x$ since multiplication in K is associative, and $1 \cdot x = x$ since $x \in K$ and 1 is the unity element. Also, $c(x+y) = cx + cy$ and $(c+d)x = cx + dx$ since multiplication is distributive over addition in K. Therefore, K is a linear space over k.

Definition 4.18. Let K be an extension field of a field k. K is called a finite extension of dimension n if, and only if K is an n-dimensional linear space over k where n is a positive integer.

Definition 4.19. Let A be a linear space over F. Let $v: F \rightarrow R$ be a rank one valuation. Let $N: A \rightarrow R$ be a function such that

(a) $N(x) \geq 0$ for all $x \in A$, and $N(x) = 0$ if, and only if $x = 0$, and

(b) $N(cx) = v(c)\, N(x)$ for all $c \in F$ and $x \in A$, and

(c) $N(x+y) \leq N(x) + N(y)$.

Then N is called a norm on A and A is called a normed linear space.

If K is an extension field of k and v is a rank one valuation on K then K is a normed linear space over k with norm v. Also, if A is an arbitrary normed linear space over a field with norm N then Cauchy sequences, convergence and completeness can be defined as they were in Chapter III. If $\{a_n\}$ is a sequence in A, and if for any $\epsilon > 0$ there exists an M such that $N(a_n - a_m) < \epsilon$ when $n,m > M$ then $\{a_n\}$ is called a Cauchy sequence. If there exists a vector $x \in A$ such that for any $\epsilon > 0$ there exists an M such that $N(a_n - x) < \epsilon$ when $n > M$ then $\{a_n\}$ is said to converge to x which is denoted by $\lim_{n\to\infty} a_n = x$. If every Cauchy sequence in A converges to a vector in A then A is complete.

A normed linear space A forms a topological space. In particular it is a metric space with metric $d(x,y) = N(x-y)$ and basic neighborhoods of the form $S_r(x) = \{y \mid N(x-y) < r\}$ where $r > 0$. A set B is open in A if, and only if for any $x \in B$ there exists a basic neighborhood $S_r(x)$ such that $S_r(x) \subseteq B$. A set C is closed in A if, and only if $A - C$ is open. If $D \subseteq A$ and $p \in A$ then p is called a limit point of D if, and only if there exists a sequence $\{a_n\}$ in D such that $\lim_{n\to\infty} a_n = p$. It can also be shown that a set D is closed in A if, and only if D contains all its limit points (cf. Hall and Spencer [10], p. 63).

<u>Definition 4.20</u>. Let A be a linear space over F. Let N_1 and N_2 be two norms on A. Then N_1 is said to be equivalent to N_2 if, and only if there exist $a,b > 0$ such that $a\,N_1(x) \le N_2(x) \le b\,N_1(x)$ for all $x \in A$.

Further, "equivalence of norms" is an equivalence relation since $N_1(x) \le N_1(x) \le N_1(x)$, if $aN_1(x) \le N_2(x) \le bN_1(x)$ then $(1/b)N_2(x) \le N_1(x) \le (1/a)N_2(x)$, and if $aN_1(x) \le N_2(x) \le bN_1(x)$ and

$cN_2(x) \le N_3(x) \le dN_2(x)$ then $(ac)N_1(x) \le N_3(x) \le (bd)N_1(x)$ where $a, b, c, d > 0$.

Theorem 4.21. Let A be an n-dimensional linear space over F. Let $\{x_1, \ldots, x_n\}$ be a basis for A. Let $v:F \to R$ be a rank one valuation. Let $N:A \to R$ be defined as $N(x) = \max_i v(c_i)$ where $x = c_1 x_1 + \ldots + c_n x_n$. Then N is a norm.

Proof: N is well defined since $x = c_1 x_1 + \ldots + c_n x = d_1 x_1 + \ldots + c_n x_n$ implies $(c_1 - d_1)x_1 + \ldots + (c_n - d_n)x_n = 0$; hence $c_1 - d_1 = \ldots = c_n - d_n = 0$, and $c_1 = d_1, \ldots, c_n = d_n$ by Definition 4.16. Therefore, $\max_i v(c_i) = \max_i v(d_i)$.

Also, $N(x) \ge 0$ since $v(c_i) \ge 0$ for any i. If $N(x) = 0$ then $v(c_i) = 0$ for all i which implies $c_i = 0$ for all i; thus $x = c_1 x_1 + \ldots + c_n x_n = 0$. If $x = 0$ then $c_1 x_1 + \ldots + c_n x = 0$ which implies $c_1 = \ldots = c_n = 0$; hence $v(c_i) = 0$ for all i, and $N(x) = \max_i v(c_i) = 0$.

If $c \in F$ then $N(cx) = \max_i v(c\, c_i) = \max_i v(c)\, v(c_i) = v(c) \max_i v(c_i) = v(c)\, N(x)$. If $y = d_1 x_1 + \ldots + d_n x_n$ then $N(x+y) = \max_i v(c_i + d_i) \le \max_i [v(c_i) + v(d_i)] = \max_i v(c_i) + \max_i v(d_i) = N(x) + N(y)$. Thus N is a norm.

The next theorem is adapted from a similar one in Bachman [2].

Theorem 4.22. Let A be an n-dimensional linear space over F with basis $\{x_1, \ldots, x_n\}$. Let F be a complete field with respect to a rank one valuation $v:F \to R$. Then any two norms on A are equivalent.

Proof: It will be shown that every norm on A is equivalent to the norm $N_o(x) = \max_i v(c_i)$ where $x = c_1 x_1 + \ldots + c_n x_n$. Then the theorem will be proved since "equivalence of norms" is an equivalence relation.

Let N be an arbitrary norm on A, and let $x = c_1 x_1 + \ldots + c_n x_n \in A$. Then $N(x) = N(c_1 x_1 + \ldots + c_n x_n) \leq N(c_1 x_1) + \ldots + N(c_n x_n) = v(c_1) N(x_1) + \ldots + v(c_n) N(x_n) \leq \max_i v(c_i)[N(x_1) + \ldots + N(x_n)] = bN_o(x)$ where $b = N(x_1) + \ldots + N(x_n)$.

Now it must be shown that there exists $a > 0$ such that $aN_o(x) \leq N(x)$ for all $x \in A$. This will be shown by induction on n the dimension of the linear space.

If $n = 1$ then there exists a basis $\{x_1\}$ with only one vector. Thus, $x \in A$ implies there exists a $c_1 \in F$ such that $x = c_1 x_1$ which implies $N(x) = N(c_1 x_1) = v(c_1) N(x_1) = N_o(x) N(x_1)$; hence for any norm N on a 1-dimensional linear space A there exists an $a > 0$ such that $aN_o(x) \leq N(x)$ for all $x \in A$.

Assume for any norm N on an (n-1)-dimensional linear space over F there exists an $a > 0$ such that $a N_o(x) \leq N(x)$. Let A be an n-dimensional linear space over F with basis $\{x_1, \ldots, x_n\}$. Let N be a norm on A. Let B be the subspace spanned by $\{x_1, \ldots, x_{n-1}\}$ (cf. Definition 4.15). Then $\{x_1, \ldots, x_{n-1}\}$ forms a basis for B which implies B is an (n-1)-dimensional linear space. Also, N is a norm on B. Therefore, N is equivalent to N_o on B by the first part of the proof and the induction hypothesis; hence there exists $a, b > 0$ such that $a\,N_o(x) \le N(x) \le b\,N_o(x)$ for all $x \in B$.

Let $\{y_i\}$ be a Cauchy sequence in B with respect to N. There exist $c_{1i}, c_{2i}, \ldots, c_{n-1i} \in F$ such that $y_i = c_{1i}x_1 + \ldots + c_{n-1i}x_{n-1}$ for $i = 1, 2, 3, \ldots$. Now, $v(c_{m\ell} - c_{mk}) \le \max_j v(c_{j\ell} - c_{jk}) = N_o(y_\ell - y_k) \le \frac{1}{a} N(y_\ell - y_k)$. Thus if $\epsilon > 0$ then there exists M such that $N(y_\ell - y_k) < a\,\epsilon$ for $\ell,k > M$ since $\{y_n\}$ is Cauchy; hence $v(c_{m\ell} - c_{mk}) < \epsilon$. This implies $\{c_{mi}\}$ are Cauchy in F with respect to v for $m = 1, 2, \ldots, n-1$. Therefore, for each m there exists $c_m \in F$ such that $\lim_{i\to\infty} c_{mi} = c_m$ since F is complete with respect to v. Let $y = c_1 x_1 + c_2 x_2 + \ldots + c_{n-1} x_{n-1}$. Also, $N(y_i - y) \le b\,N_o(y_i - y) = b \max_j v(c_{ji} - c_j)$. If $\epsilon > 0$ then there exists M_j such that $v(c_{ji} - c_j) < \epsilon/b$ when $i > M_j$. Let $M = \max_j M_j$. Then $i > M$ implies $v(c_{ji} - c_i) < \epsilon/b$ for $j = 1, 2, \ldots, n-1$ which implies $\max_j v(c_{ji} - c_j) < \epsilon/b$. Therefore, $N(y_i - y) < \epsilon$ when $i > M$; hence $\lim_{i\to\infty} y_i = y$ with respect to N. Thus, B is complete with respect to N.

Let $C = \{x_n + x \in A \mid x \in B\}$. Let p be a limit point of C. This implies there exists a sequence $\{a_i\}$ in C such that $\lim_{i\to\infty} a_i = p$. Thus, for each i there exists $b_i \in B$ such that $a_i = x_n + b_i$. Also, if $\epsilon > 0$ there exists M such that $N(a_i - p) < \epsilon/2$ if $i > M$. Therefore, $N(b_i - b_j) = N\big(x_n + b_i - (x_n + b_j)\big) = N(a_i - a_j) = N(a_i - p + p - a_j) \le N(a_i - p) + N(p - a_j) < \epsilon/2 + \epsilon/2 = \epsilon$ if $i,j > M$. This implies that $\{b_i\}$ is a Cauchy sequence in B with respect to N; hence there exists

$b \in B$ such that $\lim_{i\to\infty} b_i = b$ since B is complete. Thus $\lim_{i\to\infty} a_i = \lim_{i\to\infty} (x_n + b_i) = s_n + b \in C$. This implies $p = x_n + b$ since the limit is unique; thus $p \in C$. Hence, C contains all its limit points, and so C is closed. This implies $A - C$ is open.

Now, $0 \notin C$, otherwise there exists $x \in B$ such that $0 = x_n + x$. But, there exists $c_1, \ldots, c_{n-1} \in F$ such that $x = c_1 x_1 + \ldots + c_{n-1} x_{n-1}$; thus $0 = c_1 x_1 + \ldots + c_{n-1} x_{n-1} + 1 \cdot x_n$. This contradicts the fact that $x_1, \ldots, x_n$ is a basis; hence $0 \in A - C$. Let $x \in C$. Then there exists $r_n > 0$ such that $S_{r_n}(0) = \{y \mid N(y-0) < r_n\} \subseteq A - C$ since $A - C$ is open; thus $x \notin S_{r_n}(0)$ which implies $N(x) = N(x-0) \geq r_n$.

Let $x = c_1 x_1 + \ldots + c_n x_n \in A$ where $c_n \neq 0$. Then $(c_1/c_n)x_1 + \ldots + (c_{n-1}/c_n)x_{n-1} + x_n \in C$ which implies $N(c_1 x_1 + \ldots + c_n x_n) = N\big(c_n([c_1/c_n]x_1 + \ldots + [c_{n-1}/c_n] x_{n-1} + x_n)\big) = v(c_n) N\big((c_1/c_n)x_1 + \ldots + (c_{n-1}/c_n) x_{n-1} + x_n\big) \geq v(c_n) r_n$. If $c_n = 0$ then $v(c_n) = 0$, and $N(x) \geq 0 = v(c_n)r_n$; hence $N(x) \geq v(c_n)r_n$ for all $x = c_1 x_1 + \ldots + c_n x_n \in A$. In a similar manner it can be shown that for each i there exists $r_i > 0$ such that $N(x) = N(c_1 x_1 + \ldots + c_i x_i + \ldots + c_n x_n) \geq v(c_i)r_i$ for all $x = c_1 x_1 + \ldots + c_n x_n \in A$. Let $a = \min_i r_i$. Then $N(x) \geq v(c_i) \min_i r_i = v(c_i)a$ for $i = 1, 2, \ldots, n$. Thus, $N(x) \geq \max_i v(c_i)a = a \max_i v(c_i) = aN_o(x)$. Thus the theorem is proved.

The proof of the following uniqueness theorem was adapted from one in Cassels and Frohlich [7].

Theorem 4.23. Let K be a finite extension field of dimension n of a subfield k. Suppose k is complete with respect to a rank one valuation v. If there exists a rank one valuation $t: K \to R$ such that $t\big|_k = v$ then t is unique.

Proof: Suppose $w: K \to R$ is a rank one valuation such that $w\big|_k = v$. Now, K is an n-dimensional linear space over k and t and w are norms on K. Thus, t and w are equivalent norms by Theorem 4.22. This implies that there exists $a, b > 0$ such that $aw(x) \le t(x) \le bw(x)$ for all $x \in K$. Let $x \in K$ such that $t(x) < 1$. Then $\lim_{n\to\infty} t^n(x) = 0$ which implies $\lim_{n\to\infty} w^n(x) = \lim_{n\to\infty} w(x^n) = \frac{1}{a} \lim_{n\to\infty} t(x^n) = \frac{1}{a} \lim t^n(x) = 0$. This implies $w(x) < 1$; hence t and w are equivalent as valuations. Thus, there exists a positive real number s such that $t(x) = w^s(x)$ for all $x \in K$ by Theorem 3.32. Let $y \in k$ such that $y \neq 0$. Then $t(y) = v(y) = w(y)$. This implies $w^s(y) = w(y)$. Therefore, $s = 1$, and $t = w$.

Definition 4.24. Let A be a linear space over F. Let $x_1, x_2, \ldots, x_m \in A$. If $c_1, \ldots, c_m \in F$ and $c_1 x_1 + \ldots + c_m x_m = 0$ imply $c_1 = \ldots = c_m = 0$ then $\{x_1, \ldots, x_m\}$ is said to be linearly independent. If $\{x_1, \ldots, x_m\}$ is not linearly independent then it is linearly dependent.

If A is an n-dimensional linear space over F and $\{x_1, \ldots, x_m\}$ is a linearly independent subset of A then $\{x_1, \ldots, x_m\}$ is contained in a basis of A (cf. Halmos [11], p. 11). This implies $m \le n$ since every basis has exactly n vectors (cf. Halmos [11], p. 13).

Theorem 4.25. Let F be a field with a valuation $v:F \to G \cup \{z\}$. Let K be an extension field of F with a valuation $t:K \to H \cup \{z\}$ such that G is a subgroup of H and $t \mid_F = v$. Then $v(F - \{0\}) = G$ is a normal subgroup of $t(K - \{0\}) = H$.

Proof: Let $a \in H$ and $b \in G$. This implies there exists $x \in K - \{0\}$ and $y \in F - \{0\}$ such that $t(x) = a$ and $t(y) = b$. Thus, $a\, b\, a^{-1} =$ $t(x)\ t(y)\ t(x)^{-1} = t(x)\ t(y)\ t(x^{-1}) = t(xyx^{-1}) = t(yxx^{-1}) = t(y) =$ $b \in G$. Hence, G is normal in H.

Definition 4.26. Let F be a field with valuation $v:F \to G \cup \{z\}$. Let K be an extension field of F with a valuation $t:K \to H \cup \{z\}$ such that G is a subgroup of H and $t \mid_F = v$. Then the number of elements e in the factor group $t(K - \{0\})/t(F - \{0\}) = H/G$ is called the ramification index of t and v.

Theorem 4.27. Let F be a field with valuation $v:F \to G \cup \{z\}$. Let K be a finite extension field of dimension n with non-archimedian valuation $t:K \to G_1 \cup \{z\}$ where G is a subgroup of G_1 and $t \mid_F = v$. Then the ramification index e of t and v is finite and $e \leq n$.

Proof: Let $\{a_1 G, a_2 G, \ldots, a_i G\}$ be a finite set of distinct elements of G_1/G. Then there exists a set of distinct elements $b_1, \ldots, b_i \in K - \{0\}$ such that $t(b_1) = a_1$, $t(b_2) = a_2$, ..., $t(b_i) = a_i$ since $a_1, \ldots, a_i \in G_1$.

Now, suppose $c_1 b_1 + \ldots + c_i b_i = 0$ where $c_1, \ldots, c_i \in F$ and

$c_1, \ldots, c_i$ are not all zero. Suppose $c_1, \ldots, c_k (k \le i)$ are the non-zero elements of $\{c_1, \ldots, c_i\}$. The elements $t(c_1 b_1), \ldots, t(c_k b_k)$ are distinct, otherwise there exists ℓ, m such that $\ell \ne m$, $1 \le \ell, m \le k$ and $t(c_\ell b_\ell) = t(c_m b_m)$; hence $t(c_\ell) a_\ell = t(c_\ell) t(b_\ell) = t(c_m) t(b_m) = t(c_m) a_m$ which implies $v(c_\ell) a_\ell = v(c_m) a_m$, and so $a_\ell G = (1 \cdot G)(a_\ell G) = \big(v(c_\ell) G\big)(a_\ell G) = \big(v(c_\ell) a_\ell\big) G = \big(v(c_m) a_m\big) G = \big(v(c_m) G\big)(a_m G) = (1 \cdot G)(a_m G) = a_m G$, a contradiction. This implies there exists m such that $t(c_\ell b_\ell) \not\ge t(c_m b_m)$ for $\ell = 1, 2, \ldots, m-1, m+1, \ldots, k$. Thus, $t(c_1 b_1 + \ldots + c_k b_k) = t(c_m b_m)$ by Theorem 2.9. This implies $t(c_m b_m) = z$ since $c_1 b_1 + \ldots + c_k b_k = 0$; thus $c_m b_m = 0$ which implies $c_m = 0$ or $b_m = 0$, a contradiction. Therefore, if $c_1 b_1 + \ldots + c_i b_i = 0$ then $c_1 = c_2 = \ldots = c_i = 0$ which implies $\{b_1, \ldots, b_i\}$ is a linearly independent set in the linear space K over F. Therefore, $i \le n$, and G_1/G has only a finite number of elements and $e \le n$.

The last theorem was taken from Schilling [16]. The next theorem may be found in Bachman [2].

Theorem 4.28. If $v: F \to R$ is a non-archimedian rank one valuation on F, and K is a finite extension field of F, then there exists a non-archimedian rank one valuation $t: K \to R$ such that $t \big|_F = v$.

Proof: There exists a non-archimedian valuation $w: K \to S \cup \{0\}$ such that $v(F) \subset S$ and $w \big|_F = v$ by Theorem 4.12. The ramification index e of w and v is finite by Theorem 4.27.

Let $r: K \to S \cup \{0\}$ be a function defined as $r(a) = w^e(a)$ for $a \neq 0$ and $r(0) = 0$. It is clear that $r(a) = 0$ if, and only if $a = 0$, and $r(ab) = w^e(ab) = \big(w(a)\ w(b)\big)^e = w^e(a)\ w^e(b) = r(a)\ r(b)$. Let $a,b \in K$. Then $w(a + b) \not> \max\big(w(a), w(b)\big)$ which implies $w^e(a + b) \not>$ $\Big(\max\big(w(a), w(b)\big)\Big)^e = \max\big(w^e(a), w^e(b)\big)$; hence $r\ (a + b) \not>$ $\max\big(r(a), r(b)\big)$, and so r is a non-archimedian valuation.

Let $a \in K$ and $G = v(F)$. Then $w(a)G$ is a coset of S/G. This implies $r(a)G = w^e(a)G = \big(w(a)G\big)^e = 1 \cdot G$ since e is the order of the group S/G; hence $r(a) \in G \subseteq R$. Therefore, $r(K) \subseteq G \subseteq R$, and so r is a non-archimedian rank one valuation by Definition 3.19.

Now, let $t: K \to R$ be defined as $t(a) = \big(r(a)\big)^{1/e}$. It can be shown that t is a non-archimedian valuation in the same way r was shown to be a non-archimedian valuation. Also, t is of rank one since $t(K) \subseteq R$. Let $a \in F$, then $t(a) = \big(r(a)\big)^{1/e} = \big(w^e(a)\big)^{1/e} = w(a) = v(a)$; thus $t\,\big|_F = v$.

<u>Theorem 4.29</u>. Let $v: F \to R$ be a rank one non-archimedian valuation where F is complete with respect to v. Let K be a finite extension field of F. Then there exists a unique non-archimedian rank one valuation $t: K \to R$ such that $t\,\big|_F = v$.

Proof: Theorem 4.28 implies the existence of t, and Theorem 4.23 implies uniqueness.

CHAPTER V

SUMMARY

In the preceding chapters, a valuation of general rank has been defined, and it has been shown that if v is a non-archimedian rank one valuation then v is a mapping from a field to the non-negative reals such that $v(a) = 0$ if, and only if $a = 0$, $v(ab) = v(a)\ v(b)$ and $v(a + b) \le \max\left(v(a)\ v(b)\right)$. This depended upon the fact that a rank one ordered group is isomorphic to a subgroup of the multiplicative group of positive reals. It was shown that a non-archimedian valuation is of rank one if, and only if the associated valuation ring is a maximal subring of the domain of the valuation. The Fundamental Extension Theorem of Places was proven, and it was shown that a rank one non-archimedian valuation can be extended uniquely over a finite extension field of its domain provided the domain is complete.

The above facts are by no means an exhaustive list of the important theorems of valuation theory. There are many other areas that can be studied, and the topics mentioned above can be further investigated. For example, there exists a formula for the unique extension of Theorem 4.29 (cf. McCarthy [14], p. 89). Also, if K is a finite extension field of degree n over F and v is a valuation on F with a set of extensions $\{v_a\}$ to K then $\sum_a e_a f_a \le n$ where e_a is the ramification index of v_a and v, and f_a is the degree of the extension field V_a/P_a over V/P (V_a and V are the valuation rings of v_a and v respectively, and P_a and P are the non-units of V_a and V). This theorem was published by Cohen and Zariski in 1958 as the first article in the first volume of the Illinois Journal of Mathematics (cf. Cohen and Zariski [8]). This would imply that v has only a finite number of extensions even though F is not complete with respect to v. Completeness was part of the hypothesis of Theorem 4.29.

A valuation can be defined on a more general algebraic structure than a field. For example, Schilling [16] defines a valuation on a division ring. Manis [13] in a very recent publication developed a theory of valuations which are defined on a commutative ring with unity.

This paper was not meant to be a complete treatment of valuation theory, but it is hoped that the reader will gain some knowledge of the fundamentals of this theory and will develop an interest in this generalization of absolute value.

BIBLIOGRAPHY

(1) Artin, E. Elements of Algebraic Geometry (Lecture Notes). New York: New York University Institute of Mathematical Sciences, 1955.

(2) Bachman, G. Introduction to p-Adic Numbers and Valuation Theory. New York: Academic Press, 1964.

(3) Barnes, W. E. Introduction to Abstract Algebra. Boston: Heath, 1963.

(4) Bell, E. T. Mathematics, Queen and Servant of Science. New York: McGraw-Hill, 1951.

(5) Borevich, Z. I. and I. R. Shafarevich. Number Theory, Pure and Applied Mathematics Monographs and Textbooks, Volume 20. New York: Academic Press, 1966.

(6) Burrill, C. W. Foundations of Real Numbers. New York: McGraw-Hill, 1967.

(7) Cassels, J. W. S. and A. Fröhlich. Algebraic Number Theory. Washington, D. C.: Thompson, 1967.

(8) Cohen, I. S. and O. Zariski. "A Fundamental Inequality in the Theory of Extensions of Valuations." Illinois Journal of Mathematics, Volume 1, 1957, 1-8.

(9) Cohen, L. W. and G. Ehrlich. The Structure of the Real Number System. Princeton: D. Van Nostrand, 1963.

(10) Hall, D. W. and G. L. Spencer. Elementary Topology. New York: John Wiley, 1955.

(11) Halmos, P. R. Finite Dimensional Vector Spaces. Princeton: D. Van Nostrand, 1958.

(12) MacDuffee, C. C. "The p-Adic Numbers of Hensel." American Mathematical Monthly, Volume 45, 1938, 500-508.

(13) Manis, M. E. "Valuations on a Commutative Ring." Proceedings of the American Mathematical Society, Volume 20, 1969, 193-198.

(14) McCarthy, P. J. Algebraic Extensions of Fields. Waltham, Massachusetts: Blaisdell, 1966.

(15) Moore, J. T. Elements of Abstract Algebra. New York: MacMillian, 1967.

(16) Schilling, O. F. G. The Theory of Valuations, Mathematical Surveys of the American Mathematical Society, Volume 4, New York, 1950.

VITA

Edward Newton Mosley

Candidate for the Degree of

Doctor of Education

Dissertation: A STUDY OF VALUATIONS OF GENERAL RANK

Major Field: Higher Education

Biographical:

Personal Data: Born in Little Rock, Arkansas, July 19, 1939, the son of Ellis G. and Mary N. Mosley.

Education: Graduated from Batesville High School, Batesville, Arkansas, in May, 1956; received the Bachelor of Arts degree from Arkansas College, Batesville, Arkansas, in May, 1960, with a major in mathematics; received the Master of Science degree from the University of Arkansas, Fayetteville, Arkansas, in June, 1962, with a major in mathematics; attended Texas A. and M. University, College Station, Texas, in the summer of 1964 as a National Science Foundation Institute participant; attended the University of Arkansas in the summer of 1965; completed requirements for the Doctor of Education degree at Oklahoma State University in May, 1970.

Professional Experience: Taught as a graduate assistant in mathematics at the University of Arkansas, 1960-62; taught as an instructor of mathematics at Memphis State University, 1962-66; taught as a graduate assistant in mathematics at Oklahoma State University, 1966-70.

Professional Organizations: Member of Mathematical Association of America and Pi Mu Epsilon.