VALUATIONS ON FIELDS

THESIS

Presented to the Graduate Council of the North Texas State University in Partial Fulfillment of the Requirements

For the Degree of

MASTER OF ARTS

By

Catherine A. Walker, B. A.
Denton, Texas
May, 1977

This thesis investigates some properties of valuations on fields. Basic definitions and theorems assumed are stated in Chapter I. Chapter II introduces the concept of a valuation on a field. Real valuations and non-Archimedean valuations are presented. Chapter III generalizes non-Archimedean valuations. Examples are described in Chapters I and II.

A result is the theorem stating that a real valuation $\phi$ of a field $K$ is non-Archimedean if and only if $\phi(a+b) \leq \max\{\phi(a), \phi(b)\}$ for all $a$ and $b$ in $K$.

Chapter III generally defines a non-Archimedean valuation as an ordered abelian group.

Real non-Archimedean valuations are either discrete or non-discrete. Chapter III shows that every valuation ring identifies a non-Archimedean valuation and every non-Archimedean valuation identifies a valuation ring.
TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INTRODUCTORY CONCEPTS</td>
<td>1</td>
</tr>
<tr>
<td>II. PROPERTIES OF VALUATIONS ON FIELDS</td>
<td>5</td>
</tr>
<tr>
<td>III. GENERALIZATIONS OF NON-ARCHIMEDEAN VALUATIONS</td>
<td>13</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>33</td>
</tr>
</tbody>
</table>
CHAPTER I

INTRODUCTORY CONCEPTS

This thesis investigates some of the properties of valuations on fields. Basic definitions and theorems which will be assumed are stated in this chapter. For proofs of these theorems see [1]. Chapter II introduces the concept of a valuation on a field. Real valuations and non-Archimedean valuations are also presented. Chapter III is a generalization of non-Archimedean valuations. Specific examples are described in both Chapter II and Chapter III.

All rings considered in this thesis are commutative rings with a unity. Addition and multiplication will be denoted by + and \cdot respectively; \cdot will be omitted except when needed for clarity. Set containment is denoted by \subset and proper containment is denoted by \subsetneq.

A valuation ring is an integral domain \( D \) such that ideals in \( D \) are chained; that is, if \( A \) and \( B \) are ideals in \( D \), then either \( A \subset B \) or \( B \subset A \).

**Theorem 1.1.** Let \( D \) be an integral domain with quotient field \( K \). The following conditions are equivalent:

i). If \( A \) and \( B \) are ideals in \( D \), then either \( A \subset B \) or \( B \subset A \). In other words, ideals are chained in \( D \).

ii). If \( A \) and \( B \) are principal ideals in \( D \) (that is, \( A = (a) \) and \( B = (b) \) for some \( a, b \in D \)), then \( (a) \subset (b) \) or \( (b) \subset (a) \).
iii). If $x \in K$, then either $x \in D$ or $\frac{1}{x} \in D$.

Theorem 1.2. If $D'$ and $D''$ are integral domains, $K$ is the quotient field for $D'$, and $D' \subset D'' \subset K$, then $K$ is the quotient field for $D''$.

Suppose $G$ with some binary operation $\alpha$ is an abelian group. $(G, \alpha, \leq)$ is an ordered abelian group if and only if
i). $\leq$ is a partial ordering of $G$. (That is, $\leq$ is reflexive, antisymmetric, and transitive.)

ii). $\leq$ is a total ordering of $G$. (That is, for $x$ and $y$ in $G$, either $x \leq y$ or $y \leq x$.)

iii). If $x, y, z \in G$ and $x \leq y$, then $x \alpha z \leq y \alpha z$.

An integral domain $D$ is an ordered integral domain if and only if the non-zero elements in $D$ can be decomposed into a union of two non-empty disjoint sets $N$ and $P$ such that
i). $x \in N$ if and only if $x = -y$ for some element $y \in P$, and

ii). If $x, y \in P$, then $x + y \in P$ and $xy \in P$.

An ordered field is a field which is an ordered integral domain.

An integral domain $D$ is a unique factorization domain if and only if
i). Every element in $D$ which is neither zero nor a unit can be factored into a product of a finite number of primes, and
ii). If $p_1 p_2 p_3 \cdots p_n$ and $q_1 q_2 \cdots q_m$ are two factorizations of the same element of $D$ into primes, then $n = m$ and the $q_i$'s can be renumbered so that $p_i$ and $q_i$ are associates for $i = 1, 2, \ldots, n.$
CHAPTER BIBLIOGRAPHY

CHAPTER II

PROPERTIES OF VALUATIONS ON FIELDS

Definition 2.1. Let $K$ be a field, $P$ an ordered field, and $\phi$ a function from $K$ into $P$ such that i) $\phi(0) = 0$ and $\phi(a) > 0$ for all $a$ in $K$ such that $a \neq 0$, ii) $\phi(ab) = \phi(a)\phi(b)$ for all $a, b$ in $K$, and iii) $\phi(a+b) \leq \phi(a) + \phi(b)$ for all $a, b$ in $K$. The function $\phi$ is called a valuation of $K$ (with $P$ as the field of values).

Theorem 2.2. Let $\phi$ be a valuation of a field $K$ with $P$ as the field of values. Suppose $a, c \in K$. Then, (i) $\phi(-1) = 1, \phi(a) = \phi(-a)$, (ii) $\phi(c) - \phi(a) \leq \phi(c - a)$, (iii) $\phi(a) - \phi(c) \leq \phi(c - a)$, and (iv) $|\phi(c) - \phi(a)| \leq \phi(c - a)$.

Proof. (a) Let $S = \{x \in P | x \neq 0 \text{ and } x = \phi(y) \text{ for some } y \in K\}$. $S$ is not empty because $\phi(1) \in S$. Let $x \in S$. There exists a $y \in K$ such that $x = \phi(y)$. $x = \phi(y) = \phi(1\cdot y) = \phi(1)\cdot\phi(y) = \phi(1)\cdot x$, so for every $x \in S$, $\phi(1)$ is a left multiplicative identity. Similarly, $\phi(1)$ is a right multiplicative identity for every $x \in S$. Thus, $\phi(1)$ is a unity for all $x$ in $S$. Let $1$ be the unity in $P$. Since $\phi(1) \in S \subseteq P$ and $1$ is the unity for $P$, $\phi(1)\cdot 1 = \phi(1)$. Since $\phi(1)$ is the unity in $S$ and $\phi(1) \in S$, $\phi(1)\cdot\phi(1) = \phi(1)$. Hence, $\phi(1)\cdot 1 = \phi(1)\cdot\phi(1)$. Since $P$ is a domain, there are no zero divisors, so we can cancel. Thus, $1 = \phi(1)$. 5
Suppose that $\phi(1) \neq \phi(-1)$. Then either $\phi(-1) - \phi(1) < 0$ or $\phi(-1) - \phi(1) > 0$. Suppose $\phi(-1) - \phi(1) < 0$. Then $\phi(-1) < \phi(1)$. Thus $\phi(1) < \phi(-1)$. This contradicts $\phi(-1) < \phi(1)$. A contradiction can also be obtained by a similar proof when $\phi(-1) - \phi(1) > 0$. Thus, $\phi(1) = \phi(-1) = 1$. Let $a \in K$.

\[
\phi(-a) = \phi(-1\cdot a) = \phi(-1)\cdot \phi(a) = 1\cdot \phi(a) = \phi(a).
\]

ii). $\phi(c) = \phi(c - a + a) \leq \phi(c - a) + \phi(a)$. Thus,

\[
\phi(c) - \phi(a) \leq \phi(c - a).
\]

iii). By part i), $\phi(a - c) = \phi(c - a)$. By part ii),

\[
\phi(a) - \phi(c) \leq \phi(a - c). \text{ Hence } \phi(a) - \phi(c) \leq \phi(c - a).
\]

iv). By part ii), $\phi(c) - \phi(a) \leq \phi(c - a)$. $\phi(a) = \phi(a - c + c) \leq \phi(a - c) + \phi(c) = \phi(c - a) + \phi(c)$. Therefore, $-\phi(c - a) \leq \phi(c) - \phi(a)$. Since $-\phi(c - a) \leq \phi(c) - \phi(a) \leq \phi(c - a)$,

\[
|\phi(c) - \phi(a)| \leq \phi(c - a).
\]

Theorem 2.3. In Theorem 2.2, if $K$ is an ordered field and we define $\phi(a) = |a|$ for all $a \in K$, then $\phi$ is a valuation of $K$.

Proof. For every $a \in K$, $\phi(a) = |a| \in K$, so $\phi : K \rightarrow K$.

$\phi$ is a function from a field into an ordered field.

i) $\phi(0) = |0| = 0$. For every $a \neq 0$, $\phi(a) = |a| > 0$.

ii) $\phi(ab) = |ab| = |a||b| = \phi(a)\phi(b)$

iii) $\phi(a + b) = |a + b| \leq |a| + |b| = \phi(a) + \phi(b)$. Hence,

$\phi$ is a valuation of $K$.

Example 2.4. Let $R$ be the field of rational numbers and let $p$ be a fixed prime integer. Write each rational
number \( a \in R \) in the form \( a = \frac{s}{t} \cdot p^n \) where \( s \) and \( t \) are integers not divisible by \( p \), \( t \neq 0 \), and \( n \) is an integer. Define \( \phi_p(a) = p^{-n} \) for \( 0 \neq a \in R \) and \( \phi_p(0) = 0 \). The function \( \phi_p \) is a valuation of \( R \), with \( R \) as a field of values, for each fixed prime \( p \). Further, instead of iii) in the definition of a valuation, the stronger inequality \( \phi_p (a + b) \leq \max \{ \phi_p(a), \phi_p(b) \} \) is valid. The valuation \( \phi_p \) is called the \( p \)-adic valuation of \( R \).

By definition, \( \phi \) is a function from a field \( R \) into an ordered field \( R \).

i). \( \phi_p(0) = 0 \) by definition. Let \( a \in R \) and \( a \neq 0 \). \( a = \frac{s}{t} \cdot p^n \) where \( s \), \( t \) and \( n \) are integers and \( p \) does not divide \( s \) or \( t \) and \( t \neq 0 \). \( \phi_p(a) = p^{-n} \). Since \( p \) is a prime integer, \( p \) is positive. Hence, \( p^{-n} > 0 \) for every integer \( n \). Thus \( \phi_p(a) > 0 \).

ii). Let \( a \) and \( b \in R \). \( a = \frac{s}{t} \cdot p^n \) and \( b = \frac{q}{r} \cdot p^m \) where \( s \), \( t \), \( q \), \( r \), \( n \), and \( m \) are integers, \( t \neq 0 \), \( r \neq 0 \), and \( p \) does not divide \( s \), \( t \), \( q \), and \( r \). \( ab = \frac{s}{t} \cdot p^n \cdot \frac{q}{r} \cdot p^m = \frac{sq}{tr} \cdot p^{n+m} \). Since \( p \) does not divide \( s \), \( q \), \( t \) and \( r \) and \( p \) is a prime, \( p \) does not divide \( sq \) and \( p \) does not divide \( tr \). Hence, \( \phi_p(ab) = p^{-(n+m)} = p^{-n-m} = p^{-n} \cdot p^{-m} = \phi_p(a) \cdot \phi_p(b) \).

iii). Let \( a \) and \( b \in R \), \( a = \frac{s}{t}p^n \), and \( b = \frac{q}{r}p^m \) as in part ii).

Case 1. Suppose \( n = m \). Then \( a + b = \frac{s}{t}p^n + \frac{q}{r}p^m = \frac{sp^n}{t} + \frac{q}{r}p^n = (\frac{sr + tq}{tr})p^n \). Since \( p \) does not divide \( t \) and \( p \) does not divide \( r \) and \( p \) is a prime, \( p \) does not divide \( tr \).
However, \( p \) may divide \( sr + tq \). \( sr + tq = up^i \) where \( u \) is an integer not divisible by \( p \) and \( i \in \{0, 1, 2, \ldots \} \). Thus,

\[
a + b = \frac{up^i}{tr} \cdot p^n = \frac{u}{tr} \cdot p^{i+n}.
\]

\( \phi_p(a+b) = p^{-(i+n)} \) and

\( \phi_p(a) + \phi_p(b) = p^{-n} + p^{-m} \). Since \( i \geq 0 \), \( p^{-i} \leq 1 \). So

\( \phi_p(a+b) = p^{-(i+n)} = p^{-i} \cdot p^{-n} \leq p^{-n} \leq p^{-n} + p^{-n} = \phi_p(a) + \phi_p(b) \).

**Case 2.** Suppose \( n < m \). \( a + b = \frac{s}{tr} p^n + \frac{q}{tr} p^m = (\frac{s}{tr} + \frac{q}{tr} p^{m-n}) \cdot p^n \). \( p \) does not divide \( tr \) and \( p \) does not divide \( sr + tq p^{m-n} \), hence \( \phi_p(a+b) = p^{-n} \).

\[
\phi_p(a+b) = p^{-n} \leq p^{-n} + p^{-m} = \phi_p(a) + \phi_p(b).
\]

**Case 3.** Suppose \( m < n \). This case is similar to Case 2 except \( \phi(a+b) = p^{-m} \). Hence \( \phi_p(a+b) = p^{-m} \leq p^{-n} + p^{-m} = \phi_p(a) + \phi_p(b) \).

In all three cases, \( \phi_p(a+b) \leq \phi_p(a) + \phi_p(b) \). Thus, \( \phi_p \) is a valuation of \( R \).

If \( n \) and \( m \) are integers and \( p \) is a prime integer, then \( p^n < p^m \) implies \( p^{-n} > p^{-m} \).

In Case 1,

\[
\phi_p(a+b) = p^{-(i+n)} \leq p^{-n} = \phi_p(a)
\]

\( = \phi_p(b) = \max\{\phi_p(a), \phi_p(b)\} \).

In Case 2,

\[
\phi_p(a+b) = p^{-n} = \phi_p(a).
\]

Since \( n < m \), \( \phi_p(b) < \phi_p(a) \). So

\[
\phi_p(a+b) = \phi_p(a) = \max\{\phi_p(a), \phi_p(b)\}.
\]

In Case 3,

\[
\phi_p(a+b) = p^{-m} = \phi_p(b).
\]
Since \( m < n \), \( \phi_p(a) < \phi_p(b) \). So \( \phi_p(a+b) = \phi_p(b) = \max\{\phi_p(a), \phi_p(b)\} \). In all three cases, \( \phi_p(a+b) \leq \max\{\phi_p(a), \phi_p(b)\} \).

**Theorem 2.5.** If \( a, b, \) and \( c \) are positive real numbers and if \( c^n \leq a + b \) for every integer \( n \), then \( c \leq 1 \).

**Proof.** Suppose \( c > 1 \). Then \( c = 1 + \varepsilon \) where \( \varepsilon > 0 \). Let \( n_1 \) be a positive integer such that \( n_1 \cdot \varepsilon > b \). Let \( n_2 \) be a positive integer such that \( \left(\frac{n_2-1}{2}\right) \cdot \varepsilon^2 > a \). Define \( N = \max\{n_1, n_2\} \). Then \( N \cdot \varepsilon \geq n_1 \cdot \varepsilon > b \). So \( N \cdot \varepsilon > b \).

\[
\left(\frac{N-1}{2}\right) \cdot \varepsilon^2 \geq \left(\frac{n_2-1}{2}\right) \cdot \varepsilon^2 > a.
\]

So \( \left(\frac{N-1}{2}\right) \cdot \varepsilon^2 > a \). Therefore, \( N \left(\frac{N-1}{2}\right) \cdot \varepsilon^2 > N \cdot a \).

\[
c^N = (1+\varepsilon)^N = 1 + N \cdot \varepsilon + \frac{N(N-1)}{2} \cdot \varepsilon^2 + \ldots + \varepsilon^N.
\]

So

\[
c^N > N \cdot \varepsilon + N \left(\frac{N-1}{2}\right) \cdot \varepsilon^2 > N \cdot a = aN + b.
\]

So \( c^N > aN + b \). This contradicts the hypothesis. Thus \( c \leq 1 \).

**Definition 2.6.** A valuation \( \phi \) of a field \( K \) is called a **real valuation** if and only if the field of values \( P \) is the real number field.

**Definition 2.7.** A real valuation \( \phi \) of a field \( K \) is **non-Archimedean** if and only if \( \phi(n1) \leq 1 \) for all integers \( n \). (\( n1 = 1+1+\ldots+1 \) where there are \( n \) summands and 1 is the unity in \( K \)).

**Example 2.8.** The valuation \( \phi_p \) in Example 2.4 is non-Archimedean.

\( \phi_p \) is certainly a real valuation since the range of \( \phi_p \) is a subset of the real number field. Consider \( m \cdot 1 \)}}
where \( m \) is an integer. In the field of rational numbers, \( ml = m \) for all integers \( m \). Either \( p \) divides \( m \) or \( p \) does not divide \( m \). Suppose \( p \) divides \( m \). Then \( m = s \cdot p^k \) where \( k \) is a positive integer and \( p \) does not divide \( s \). Thus \( m = \frac{s}{l} \cdot p^k \) and \( \phi_p(m) = p^{-k} < 1 \). Suppose \( p \) does not divide \( m \). Then \( m = \frac{m}{l} \cdot p^0 \). Thus \( \phi_p(m) = p^{-0} = 1 \). In either case, \( \phi_p(1m) = \phi_p(m) \leq 1 \). Thus, \( \phi_p \) is non-Archimedean.

**Theorem 2.9.** A real valuation \( \phi \) of a field \( K \) is non-Archimedean if and only if \( \phi(a+b) \leq \max\{\phi(a),\phi(b)\} \).

**Proof.** (i) Suppose \( \phi \) is a real valuation of a field \( K \) and \( \phi(a+b) \leq \max\{\phi(a),\phi(b)\} \). Suppose \( n = 0 \). Then \( \phi(nl) = \phi(0l) = \phi(0) = 0 \leq 1 \). Suppose \( n = 1 \). Then \( \phi(nl) = \phi(1l) = \phi(1) = 1 \). Suppose \( n = 2 \). Then \( \phi(nl) = \phi(1+1) = \phi(1) = 1 \). Suppose \( n \) is any positive integer and \( \phi(nl) \leq 1 \).

\[
\phi((n+1)l) = \phi(1+nl) \leq \max\{\phi(1),\phi(nl)\}.
\]

If \( \phi(1) \) is the max, then \( \phi((n+1)l) \leq \phi(1) = 1 \). If \( \phi(nl) \) is the max, then \( \phi((n+1)l) \leq \phi(nl) \leq 1 \). So, for any non-negative integer \( n \), \( \phi(nl) \leq 1 \). Suppose \( n \) is a negative integer. Then \( n = -m \) for some positive integer \( m \). \( \phi(nl) = \phi(-ml) = \phi(ml) \leq 1 \). Thus, \( \phi \) is non-Archimedean.

(ii) Suppose \( \phi \) is a real non-Archimedean valuation of a field \( K \). If \( a = 0 \) or \( b = 0 \), then clearly

\[
\phi(a+b) \leq \max\{\phi(a),\phi(b)\}.
\]

Suppose \( a \neq 0 \) and \( b \neq 0 \). Let \( k \) be a positive integer.

\[
[\phi(a+b)]^k = \phi[(a+b)^k]
\]
\[
\phi(a^k + ka^{k-1}b + \frac{k(k-1)}{2}a^{k-2}b^2 + \ldots + kab^{k-1} + b^k) \\
= \phi(a^k) + \phi(ka^{k-1}b) + \phi(\frac{k(k-1)}{2}a^{k-2}b^2) + \ldots + \phi(b^k) \\
= \phi(a^k) + \phi(k) \cdot \phi(a^{k-1}b) + \phi(\frac{k(k-1)}{2}) \cdot \phi(a^{k-2}b^2) + \ldots + \phi(b^k).
\]

Let \( Z = \{k, \frac{k(k-1)}{2}, \frac{k(k-1)(k-2)}{6}, \ldots, k\} \). Every element \( z \in Z \) is a positive integer. Since \( \phi \) is non-Archimedean,
\[
\phi(z+1) = \phi(z) \leq 1 \text{ for every } z \in Z. \text{ So } \\
\phi(a^k) + \phi(k) \cdot \phi(a^{k-1}b) + \phi(\frac{k(k-1)}{2}) \cdot \phi(a^{k-2}b^2) + \ldots + \phi(b^k) \\
\leq \phi(a^k) + \phi(a^{k-1}b) + \phi(a^{k-2}b^2) + \ldots + \phi(b^k) \\
= \sum_{i=0}^{k} \phi(a^{k-i}b^i) \\
= \sum_{i=0}^{k} \phi(a^{k-i}) \cdot \phi(b^i).
\]

\( \phi(a) \leq \max\{\phi(a), \phi(b)\} \) and \( \phi(b) \leq \max\{\phi(a), \phi(b)\} \). So, for every \( i \in \{0, 1, 2, \ldots, k\} \):
\[
\phi(a^{k-i}) = [\phi(a)]^{k-i} \leq [\max\{\phi(a), \phi(b)\}]^{k-i}
\]
and
\[
\phi(b^i) = [\phi(b)]^i \leq [\max\{\phi(a), \phi(b)\}]^i.
\]
So
\[
\phi(a^{k-i}) \cdot \phi(b^i) \leq [\max\{\phi(a), \phi(b)\}]^{k-i} \cdot [\max\{\phi(a), \phi(b)\}]^i \leq [\max\{\phi(a), \phi(b)\}]^k.
\]
Thus,
\[
\sum_{i=0}^{k} \phi(a^{k-i}) \cdot \phi(b^i) \leq \sum_{i=0}^{k} [\max\{\phi(a), \phi(b)\}]^k \\
= (k+1)[\max\{\phi(a), \phi(b)\}]^k.
\]
So
\[
[\phi(a+b)]^k \leq (k+1)[\max\{\phi(a), \phi(b)\}]^k,
\]
\[
\frac{[\phi(a+b)]^k}{[\max\{\phi(a), \phi(b)\}]^k} \leq k+1.
\]
and

\[ \left( \frac{\Phi(a+b)}{\max\{\Phi(a),\Phi(b)\}} \right)^k \leq k+1. \]

Since \( \Phi(a+b) \) and \( \max\{\Phi(a),\Phi(b)\} \) are both positive real numbers, \( \frac{\Phi(a+b)}{\max\{\Phi(a),\Phi(b)\}} \) is a positive real number. \( k \) is an arbitrary positive integer and \( 1 \) is a positive real number. Therefore, by Theorem 2.5,

\[ \frac{\Phi(a+b)}{\max\{\Phi(a),\Phi(b)\}} \leq 1. \]

Thus, \( \Phi(a+b) \leq \max\{\Phi(a),\Phi(b)\} \).
CHAPTER III

GENERALIZATION OF NON-ARCHIMEDEAN VALUATIONS

It is important to notice that in Theorem 2.9, if \( \Phi \) is a non-Archimedean valuation on a field \( K \), then only one operation is necessary in the ordered field \( P \). Let

\[
\omega(a) = -\log \Phi(a) \quad \text{for all } a \in K \text{ such that } a \neq 0 \text{ and let }
\]

\[
\omega(0) = \infty. \]

Then the axioms (i) \( \Phi(0) = 0, \Phi(a) > 0 \) for \( a \neq 0 \),

(ii) \( \Phi(ab) = \Phi(a) \cdot \Phi(b) \) and (iii)' \( \Phi(a+b) \leq \max\{\Phi(a),\Phi(b)\} \)

can be replaced by (1) \( \omega(a) \) is a real number for all non-zero \( a \in K \), and \( \omega(0) = \infty \), (2) \( \omega(ab) = \omega(a) + \omega(b) \), and (3)

\( \omega(a+b) \geq \min\{\omega(a),\omega(b)\} \). Note that only the operation +
(and its inverses) are used in axioms (1), (2) and (3).

Hence, the ordered field \( P \) (in this case \( P = \text{real numbers} \)) could be replaced by an additive group. This suggests the following definition.

Definition 3.1. Let \( G \) be an ordered abelian group and \( \{\infty\} \) be a set whose element is not in \( G \). Let

\[
G^* = G \cup \{\infty\}
\]

and make \( G^* \) into a commutative semigroup by defining + for

\( \alpha, \beta \in G^* \) by \( \alpha + \beta = \) their sum in \( G \) if \( \alpha, \beta \in G \) and \( \alpha + \beta = \infty \)

if \( \alpha = \infty \) or \( \beta = \infty \). Extend the ordering to \( G^* \) by defining

\( \alpha \preceq \infty \) for all \( \alpha \in G^* \). Then \( G^* \) is an ordered semigroup in
the sense that if \( \alpha, \beta, \sigma \in G^* \) and \( \alpha \preceq \beta \), then

\[
\alpha + \sigma \preceq \beta + \sigma.
\]
Let $K$ be a field. A **non-Archimedean valuation** on $K$ (also called an exponential valuation) with value group $G$ is a function $\omega$ from $K$ into $G^*$ such that

1. For all $a \in K$ such that $a \neq 0$, $\omega(a) \in G$ and $\omega(0) = \infty$,
2. $\omega(ab) = \omega(a) + \omega(b)$, and
3. $\omega(a+b) \geq \min\{\omega(a), \omega(b)\}$.

The function $v$ from $K$ into $G^*$ defined by $v(a) = 0$ for every $a \in K$ is called a **trivial non-Archimedean valuation**.

Notice that in the above definition, $G$ is not necessarily the set of all real numbers.

**Definition 3.2.** If $\omega$ is a non-Archimedean valuation from a field $K$ into the reals, then $\omega$ is a **real non-Archimedean valuation on $K$**.

There are two types of real non-Archimedean valuation on a field $K$.

**Definition 3.3.** If $\omega$ is a real non-Archimedean valuation on a field $K$ such that there exists a smallest positive $\omega(a)$ for some $a \in K$, then $\omega$ is said to be **discrete**. If there does not exist a smallest positive $\omega(a)$ for $a \in K$, then $\omega$ is said to be **non-discrete**.

**Theorem 3.4.** Let $\omega$ be a real non-Archimedean valuation on a field $K$. $\omega$ is discrete if and only if there exists an $a_0 \in K$ such that $\omega(a_0) > 0$ and for any non-zero element $a \in K$ such that $\omega(a) > 0$, there exists a positive integer $n$ such that

$$\omega(a) = n \cdot \omega(a_0).$$
Proof. (i) Let \( \omega \) be a real non-Archimedean valuation on a field \( K \). Suppose there exists an \( a_0 \in K \) where \( \omega(a_0) > 0 \) and for every \( a \neq 0 \) in \( K \) such that \( \omega(a) > 0 \), there exists a positive integer \( n \) such that \( \omega(a) = n \cdot \omega(a_0) \). Suppose there exists \( b \in K \) such that \( b \neq 0 \), \( \omega(b) > 0 \) and \( \omega(b) < \omega(a_0) \). For every positive integer \( n \), \( \omega(a_0) \leq n \omega(a_0) \). Hence, \( \omega(b) < n \cdot \omega(a_0) \) for every positive integer \( n \). This contradicts the hypothesis, thus, for every \( b \in K \) such that \( b \neq 0 \) and \( \omega(b) > 0 \), \( \omega(a_0) \leq \omega(b) \). Therefore, \( \omega \) is discrete.

(ii) Let \( \omega \) be a real non-Archimedean discrete valuation on a field \( K \). Since \( \omega \) is discrete, there exists an \( a_0 \in K \) such that \( \omega(a_0) > 0 \) and for every \( a \in K \) such that \( \omega(a) > 0 \), \( \omega(a_0) \leq \omega(a) \). Suppose there exists a \( b \in K \) and a positive integer \( n \) such that \( b \neq 0 \), \( \omega(b) > 0 \), and \( n \cdot \omega(a_0) < \omega(b) \) \( < (n+1) \cdot \omega(a_0) \). \( (n+1) \cdot \omega(a_0) = \omega(a_0) + n \cdot \omega(a_0) \). Thus \( \omega(b) < \omega(a_0) + n \cdot \omega(a_0) \). So \( \omega(b) - n \cdot \omega(a_0) < \omega(a_0) \). But \( n \cdot \omega(a_0) < \omega(b) \). Thus \( \omega(b) - n \cdot \omega(a_0) > 0 \).

Since \( \omega(a_0) \) is the least positive \( \omega \)-value, \( \omega(a_0) < \omega(b) - n \cdot \omega(a_0) \). Thus \( \omega(a_0) < \omega(b) - n \cdot \omega(a_0) < \omega(a_0) \).

But this implies \( \omega(a_0) < \omega(a_0) \) which is a contradiction. Hence, if \( a \in K \), \( a \neq 0 \), and \( \omega(a) > 0 \), then \( \omega(a) = n \cdot \omega(a_0) \) for some positive integer \( n \).

Theorem 3.5. Let \( \omega \) be a real non-Archimedean valuation on a field \( K \). Let \( D = \{ x \in K | \omega(x) \geq 0 \} \) and
M = \{x \in K | \omega(x) > 0\}. Then the set D is a domain and that M is the unique maximal ideal in D. Furthermore, if U = \{x \in K | \omega(x) = 0\} then U is the set of all units in D and U = D \backslash M. (D is called the valuation ring of \omega).

Proof. \omega(1) = \omega(1 \cdot 1) = \omega(1) + \omega(1). So 0 = \omega(1) - \omega(1) = \omega(1). Hence 1 \in D, so D \neq \emptyset. Suppose a and b are in D. Then \omega(a) and \omega(b) \geq 0. \omega(a + b) \geq \min\{\omega(a), \omega(b)\} \geq 0. Thus a + b \in D. \omega(ab) = \omega(a) + \omega(b) \geq 0. Thus ab \in D. Hence D is closed under multiplication and addition. 0 \in D because \omega(0) = \omega \cdot 0. Since 0 is the additive identity in K and D \subseteq K, 0 is the additive identity in D. 0 = \omega(1) = \omega(-1 \cdot -1) = \omega(-1) + \omega(-1). \omega(-1) \not\geq 0, otherwise 0 = \omega(-1) + \omega(-1) > 0 and \omega(-1) \not\leq 0, otherwise 0 = \omega(-1) + \omega(-1) < 0. Hence \omega(-1) = 0.

\omega(-b) = \omega(-1 \cdot b) = \omega(-1) + \omega(b)
= 0 + \omega(b) = \omega(b).
Hence, \omega(b) = \omega(-b). So, if b \in D, then -b \in D. Thus, additive inverses exist for every element in D. Since K is a field and D \subseteq K, all the other properties of an integral domain follow. Hence, D is an integral domain.

M is non-empty because \omega(0) = \omega \cdot 0. So 0 \in M. M \subseteq D by definition.

Let a and b \in M. a and b \in M implies that \omega(a) > 0 and \omega(b) > 0.

\omega(a - b) = \omega(a + -b) \geq \min\{\omega(a), \omega(-b)\}
= \min\{\omega(a), \omega(b)\} > 0.
Hence, $a - b \in M$. Let $a \in M$. Let $a \in M$ and $r \in D$.

$$w(ar) = w(a) + w(r).$$

$r \in D$, so $w(r) \geq 0$. Thus $w(a) + w(r) > 0$. So $ar \in M$. Hence, $M$ is an ideal in $D$.

Let $U = \{x \in K | w(x) = 0\}$. (i) Let $x \in U$. Since $w(x) = 0$, $x \neq 0$. Thus $\frac{1}{x} \in K$. 0 = $w(1) = w(x \cdot \frac{1}{x}) = w(x) + w(\frac{1}{x}) = 0 + w(\frac{1}{x}) = w(\frac{1}{x})$. Hence $\frac{1}{x} \in U \subseteq D$. Thus $\frac{1}{x} \in D$. So $x$ is a unit in $D$.

(ii). Let $y \in D$ such that $y$ is a unit in $D$. There exists $y^{-1} \in D$ such that $y \cdot y^{-1} = 1$.

$$0 = w(1) = w(y \cdot y^{-1}) = w(y) + w(y^{-1}).$$

Since $y$ and $y^{-1} \in D$, $w(y) \geq 0$ and $w(y^{-1}) \geq 0$. Since $0 = w(y) + w(y^{-1})$, $w(y) = 0$ and $w(y^{-1}) = 0$. Hence $y \in U$.

Thus, $U$ is the set of all units in $D$. $U = D \setminus M$ by definition.

Suppose there exists an ideal $A$ in $D$ such that $M < A \subseteq D$.

There exists an element $y \in A$ such that $y \notin M$. $y \notin M$ implies $w(y) = 0$. Hence $y \in U$. So $y$ is a unit in $D$. Thus, there exists $y^{-1} \in D$ such that $y \cdot y^{-1} = 1$. Since $A$ is an ideal, $y \in A$ and $y^{-1} \in D$, $1 = y \cdot y^{-1} \in A$. So for every $x \in D$,

$$1 \cdot x = x \in A.$$  Thus $D \subseteq A$. Hence $A = D$ and therefore, $M$ is a maximal ideal.

Suppose $A$ is an ideal in $D$ and $A \neq D$. Since $A \neq D$, $A$ does not contain any unit. $U = \{\text{all units in } D\} = \{x \in K | w(x) = 0\}$, so, by definition, $M = D \setminus U$. Since $A \subseteq D$ and $A \cap U = \emptyset$, $A \subseteq M$. Hence $M$ is the unique maximal ideal in $D$. 

Suppose $x \in K$ and $x \notin D$. \( O = \omega(1) = \omega(x \cdot \frac{1}{x}) = \omega(x) + \omega(\frac{1}{x}) \).

Thus $\omega(\frac{1}{x}) = -\omega(x)$. Since $x \notin D$, $\omega(x) < 0$. Therefore, $-\omega(x) > 0$.

Hence $\frac{1}{x} \in D$. Thus $D$ is a valuation ring.

**Theorem 3.6.** Let $D$ be the same as in Theorem 3.5.

If $\omega$ is discrete and $A$ is any ideal in $D$, then

\[ A = \{ x \in D \mid \omega(x) \geq \delta \} \]

where \( \delta = \min \{ \omega(a) \mid a \in A \} \).

**Proof.** Let $A$ be an ideal in $D$ and $B = \{ x \in D \mid \omega(x) \geq \delta \}$ where \( \delta = \min \{ \omega(a) \mid a \in A \} \). Clearly $A \subset B$. Suppose \( \delta = 0 \).

Then $1 \in B$ which implies $B = D$. Since $0 = \delta = \min \{ \omega(a) \mid a \in A \}$, there exists a unit $a'$ in $A$. Therefore $A = D$. Thus, $A = B$.

Suppose \( \delta > 0 \). Since \( \omega \) is discrete, there exists an element $a_0 \in D$ such that $\omega(a_0) > 0$ and for every $x \in D$ such that $\omega(x) > 0$, $\omega(a_0) \leq \omega(x)$. By Theorem 3.4, for every $a \in A$, $\omega(a) = n \omega(a_0)$ where $n$ is a positive integer. Let

\[ T = \{ n \mid n \omega(a_0) = \omega(a) \text{ for some } a \in A \}. \]

Since $T$ is a non-empty set of positive integers, $T$ has a least element, say $m$.

Thus \( \delta = m \omega(a_0) = \omega(a_1) \) for some $a_1 \in A$.

**Lemma 3.7.** If $a$ and $b \in K$ and $b \neq 0$, then

\[ \omega(a) - \omega(b) = \omega(\frac{a}{b}). \]

**Proof.** $0 = \omega(1) = \omega(b \cdot \frac{1}{b}) = \omega(b) + \omega(\frac{1}{b})$.

So $\omega(\frac{1}{b}) = -\omega(b)$. Thus $\omega(\frac{a}{b}) = \omega(a) + \omega(\frac{1}{b}) = \omega(a) - \omega(b)$.

Let $x \in D$ and suppose $\omega(x) \geq \delta$. By Theorem 3.4, $\omega(x) = t \omega(a_0)$ where $t$ is a positive integer. Since $\omega(x) \geq \delta$, $t \geq m$. By an obvious finite induction argument, $t \omega(a_0) = \omega(a_0^t)$. So $\omega(x) - \omega(a_0^t) = 0$. By Lemma 3.7,
\[
\omega\left(\frac{x}{a_0^t}\right) = 0. \text{ By Theorem 3.5 } \quad \frac{x}{a_0^t} = u_1 \text{ where } u_1 \text{ is a unit in } D. \\text{ Hence, } x = a_0^t u_1. \text{ By a similar argument, } a_1 = a_0^{m_1 u_2} \text{ where } u_2 \text{ is a unit. Since } t \geq m, t = m + \nu \text{ where } \nu \text{ is a non-negative integer. Thus } x = a_0^{m_1 u_2 u_1} = a_0^{m_1 u_2} u_1. \text{ Since } A \text{ is an ideal, } a_1 \in A, \text{ and } u_2^{-1} a_0 u_1 \in D, x \in A. \text{ Thus } B \subset A. \text{ So } A = \{ x \in D | \omega(x) \geq \delta \} \text{ where } \delta = \min\{ \omega(a) | a \in A \}.

\textbf{Theorem 3.8.} Let } D \text{ be the same as in Theorem 3.5. If } \omega \text{ is non-discrete and } A \text{ is any ideal in } D \text{ then either } A = \{ x \in D | \omega(x) \geq \delta \} \text{ or } A = \{ x \in D | \omega(x) > \delta \} \text{ where } \\
\delta = \text{glb} \{ \omega(a) | a \in A \}.

\textbf{Proof.} \text{ Let } A \text{ be an ideal in } D \text{ and let } \delta = \text{glb} \{ \omega(a) | a \in A \}. \text{ If } A = M, \text{ where } M \text{ is the unique maximal ideal in } D, \text{ then } \delta = 0 \text{ and } A = \{ x \in D | \omega(X) > 0 \}. \text{ If } A = D, \text{ then } \delta = 0 \text{ and } A = \{ x \in D | \omega(X) \geq 0 \}. \text{ Suppose } A < M. \text{ Then } \delta = \text{glb} \{ \omega(a) | a \in A \} > 0.

\textbf{Case 1.} \text{ Suppose there exists an element } a_1 \in A \text{ such that } \omega(a_1) = \delta. \text{ Let } x \in D \text{ such that } \omega(x) \geq \omega(a_1) = \delta > 0. \text{ Then } \omega(x) - \omega(a_1) > 0. \text{ By the preceding Lemma 3.7, } \omega\left(\frac{x}{a_1}\right) > 0. \text{ This implies that } \frac{x}{a_1} = d \in D. \text{ Thus } x = a_1 d. \text{ A is an ideal and } a_1 \in A, \text{ so } x \in A. \text{ Thus } A = \{ x \in D | \omega(x) \geq \delta \}.

\textbf{Case 2.} \text{ Suppose } \omega(a) > \delta \text{ for every } a \in A. \text{ Let } x \in D \text{ such that } \omega(x) > \delta. \text{ Suppose } x \notin A. \text{ Then } (x) \notin A. \text{ Since } D \text{ is a valuation ring, } A \subset (x). \text{ Let } a \in A. \text{ Then } a = xd \text{ for some } d \in D. \text{ } \omega(a) = \omega(x) + \omega(d) \geq \omega(x) > \delta. \text{ Thus } \omega(x) \text{ is a lower bound for } \{ \omega(a) | a \in A \}, \text{ and } \omega(x) \text{ is greater than the greatest}
lower bound. This is a contradiction, hence, \( x \in A \). Thus
\[
A = \{ x \in D | \omega(x) > \delta \}.
\]

**Theorem 3.9.** If \( \omega \) is a discrete real non-Archimedean valuation on a field \( K \) and \( D \) is the domain described in Theorem 3.5, then any ideal \( A < D \) is some power of \( M \). In other words, the only ideals of \( D \) are \( D, M, M^2, M^3, \ldots \).

If \( \omega \) is non-discrete, then \( M = M^2 \).

**Proof.** Suppose \( \omega \) is discrete, then there exists an \( a \in M \) such that \( \omega(a) \leq \omega(a') \) for every \( a' \) in \( M \). By Theorem 3.6, \( M = \{ x \in D | \omega(x) \leq \omega(x) \} \). Let \( A \) be an ideal in \( D \) such that \( A \neq D \). By Theorem 3.6, \( A = \{ x \in D | \omega(x) \geq \delta \} \) where
\[
\delta = \min \{ \omega(x) | x \in A \}.
\]
By Theorem 3.4, if \( x \in D \) and \( \omega(x) > 0 \), then \( \omega(x) = n \cdot \omega(a) \) for some positive integer \( n \). Since \( M \) is the unique maximal ideal and \( A \neq D, A \subseteq M \). Hence, \( \delta > 0 \). So
\[
\delta \in \{ \omega(a), 2\omega(a), 3\omega(a), \ldots \}.
\]
Thus \( \delta = n\omega(a) \) for some positive integer \( n \). \( A = \{ x \in D | \omega(x) \geq n \omega(a) \} \) by Theorem 3.6.

\[
M^n = \{ \sum_{i=1}^{k} a_{i_1} a_{i_2} \ldots a_{i_n} | a_{i_j} \in M, \quad j \in \{1,2,\ldots,n\} \text{ and } i \in \{1,2,\ldots,k\} \}.
\]

Note that \( a^n \in M^n \), and by an obvious induction argument
\[
\omega(a^n) = n \omega(a).
\]
If \( x = 0 \), then \( \omega(a^n) \leq \omega(x) \), since \( \omega(0) = \infty \).

Suppose \( x \in M^n \) and \( x \neq 0 \). Then \( x = \sum_{i=1}^{k} a_{i_1} a_{i_2} \ldots a_{i_n} \) where each \( a_{i_j} \in M, j \in \{1,2,\ldots,n\} \).
\[ \omega(x) = \omega(a_1a_1 \cdots a_1 + a_2a_2 \cdots a_2 + \cdots + a_ka_ka_k \cdots a_k) \]
\[ \geq \min\{\omega(a_1a_1 \cdots a_1), \omega(a_2a_2 \cdots a_2), \ldots, \omega(a_ka_ka_k \cdots a_k)\}. \]

Consider \( \omega(a_ia_i \cdots a_i) \) where \( 1 \leq i \leq k \).

\[ \omega(a_ia_i \cdots a_i) = \omega(a_ia_i) + \omega(a_ia_i) + \cdots + \omega(a_ia_i). \]

Since \( \omega(a_i) \leq \omega(a_i) \) for every \( 1 \leq j \leq n \),

\[ n \omega(a) \leq \omega(a_ia_1) + \omega(a_ia_2) + \cdots + \omega(a_ia_n) \]
\[ = \omega(a_ia_1a_2 \cdots a_n). \]

So \( \omega(x) \geq n\omega(a) = \omega(a^n) \) for every \( x \in \mathbb{M}^n \). Therefore,

\[ n\omega(a) = \min\{\omega(x) | x \in \mathbb{M}^n\}. \]

By Theorem 3.6, \( \mathbb{M}^n = \{x \in D | \omega(x) \geq n\omega(a)\} = A. \)

Suppose \( \omega \) is non-discrete. \( \mathbb{M}^2 = \{\sum_{i=1}^{k} a_ia_i | a_i \text{ and } a_i' \in \mathbb{M}\}. \)

Since \( \omega \) is non-discrete, \( \text{glb}\{\omega(a) | a \in \mathbb{M}\} = 0 \). Let

\[ \delta = \text{glb}\{\omega(a) | a \in \mathbb{M}^2\}. \]

By Theorem 3.8, \( \mathbb{M}^2 = \{x \in D | \omega(x) > \delta\} \)

or \( \mathbb{M}^2 = \{x \in D | \omega(x) \geq \delta\} \) where \( \delta = \text{glb}\{\omega(x) | x \in \mathbb{M}^2\} \). Suppose \( \delta < 0 \). Since \( \text{glb}\{\omega(a) | a \in \mathbb{M}\} = 0 \), there exists a \( z \in \mathbb{M} \) such that \( \omega(z) < \frac{1}{2} \delta \).

\( z^2 \in \mathbb{M}^2 \) and \( \omega(z^2) = \omega(z) + \omega(z) < \delta \). But \( z^2 \in \mathbb{M}^2 \) implies \( \omega(z^2) \geq \delta \). Thus \( \delta = 0 \). \( \mathbb{M}^2 \) clearly is a subset of \( \mathbb{M} \). If \( \mathbb{M}^2 = \{x \in D | \omega(x) \geq \delta = 0\} \), then \( \mathbb{M}^2 = \mathbb{D} \). This implies \( \mathbb{D} \subseteq \mathbb{M} \), which is false because \( \mathbb{M} \not= \mathbb{D} \). Thus

\[ \mathbb{M}^2 = \{x \in D | \omega(x) > \delta = 0\} = \mathbb{M}. \]
Theorem 3.10. Let $V$ be a valuation ring having quotient field $K$. Then there exists a non-Archimedean valuation $v$ on $K$ such that $V = \{ x \in K \mid v(x) \geq \theta \}$ where $\theta$ is the identity in the range of $v$.

**Proof.** Let $I = \{ x \in V \mid x$ is a unit $\}$. $K \setminus \{0\} \neq \emptyset$ because $1 \in K \setminus \{0\}$. Since $K \setminus \{0\} \subseteq K$ and $K$ is a field, multiplication is associative and there exists an identity in $K \setminus \{0\}$, namely $1$, the identity in $K$. Let $a \in K \setminus \{0\}$. Since $K$ is a field, there exists $a^{-1} \in K$ such that $a \cdot a^{-1} = 1$. $a^{-1} \neq 0$ (otherwise $a \cdot a^{-1} = a \cdot 0 = 0 \neq 1$), so $a^{-1} \in K \setminus \{0\}$. So every element $a \in K \setminus \{0\}$ has a multiplicative inverse. Hence, $(K \setminus \{0\}, \cdot)$ is a group.

$I \subseteq V \subseteq K$, so $I \subseteq K$ and since $0x = 0 \neq 1$ for all $x \in K$, $0 \notin I$. Thus, $I \subseteq K \setminus \{0\}$. $I \neq \emptyset$ because $1 \in I$. The associative property of multiplication and the existence of an identity $(1)$ hold in $I$ because $K$ is a field. For every $a \in I$, there exists an $a^{-1} \in I$ where $a \cdot a^{-1} = 1$ because $a$ is a unit. Thus, $I$ is a subgroup of $(K \setminus \{0\}, \cdot)$.

Let $K^* = K \setminus \{0\}$. Let $G = K^*/I = \{ kI \mid k \in K^* \}$. Define the binary operation $\odot$ by $k_1I \odot k_2I = k_1k_2I$ for $k_1I, k_2I$ in $G$.

$G \neq \emptyset$ because $1I = I \in G$. Let $k_1I$, $k_2I$, and $k_3I$ in $G$.

\[
(k_1I \odot k_2I) \odot k_3I = k_1k_2I \odot k_3I
\]
\[
= (k_1k_2)k_3I = k_1(k_2k_3)I = k_1I \odot k_2k_3I
\]
\[
= k_1I \odot (k_2I \odot k_3I).
\]

Thus, $\odot$ is associative in $G$. $I$ is clearly the identity in $G$. Let $kI \in G$. There exists a $k^{-1} \in K$ such that $kk^{-1} = 1$. $k^{-1} \neq 0$
(otherwise \(k k^{-1} = k \cdot 0 = 0 \neq 1\)), so \(k^{-1} \in K^*\). Thus, \(k^{-1}I \in G\).

\(kI \circ k^{-1}I = kk^{-1}I = I\). Hence, every element in \(G\) has an inverse. Therefore, \((G, \circ)\) is a group.

Let \(k, I\) and \(k_2 I \in G\). Since \(k_1 \) and \(k_2 \in K^* \subseteq K\) and \(K\) is a field, \(k_1 k_2 = k_2 k_1\). So \(k_1 I \circ k_2 I = k_1 k_2 I = k_2 k_1 I = k_2 I \circ k_1 I\).

Hence, \((G, \circ)\) is abelian.

Define the order relation \(\leq\) in \(G\) by \(k_2 I \leq k_1 I\) if and only if \(\frac{k_2}{k_1} \in V\).

Let \(kI \in G\). \(I = \frac{k}{K} \in V\), so \(kI \leq kI\). Thus, \(\leq\) is reflexive.

Let \(k_1 I\) and \(k_2 I \in G\). Suppose \(k_1 I \leq k_2 I\) and \(k_2 I \leq k_1 I\).

By the definition of \(\leq\),

\[
\frac{k_1}{k_2} \in V \text{ and } \frac{k_2}{k_1} \in V.
\]

\[
\frac{k_1}{k_2} \cdot \frac{k_2}{k_1} = 1 \in V,
\]

thus \(\frac{k_1}{k_2}\) and \(\frac{k_2}{k_1}\) are both in \(I\). Hence,

\(k_1 I = k_2 I\). Thus, \(\leq\) is antisymmetric.

Let \(k_1 I, k_2 I\) and \(k_3 I \in G\). Suppose \(k_1 I \leq k_2 I\) and \(k_2 I \leq k_3 I\). By the definition of \(\leq\), \(\frac{k_2}{k_1}, \frac{k_3}{k_2} \in V\).

\[
\frac{k_2}{k_1} \cdot \frac{k_3}{k_2} = \frac{k_3}{k_1} \in V.
\]

Thus, \(k_1 I \leq k_3 I\). So \(\leq\) is transitive. Hence, \(\leq\) is a partial ordering of \(G\).

Let \(k_1 I\) and \(k_2 I \in G\). \(k_1 \in K^*\) implies \(\frac{1}{k_1} \in K^*\).

\[
k_2 \cdot \frac{1}{k_1} = \frac{k_2}{k_1} \in K^* \subseteq K.
\]

Since \(V\) is a valuation ring, either \(\frac{k_2}{k_1} \in V\) or \(\frac{k_1}{k_2} \in V\).
If $\frac{k_2}{k_1} \in V$, then $k_1 I \leq k_2 I$. If $\frac{k_1}{k_2} \in V$, then $k_2 I \leq k_1 I$. So $\leq$ is a total ordering of $G$.

Suppose $k_1 I, k_2 I$, and $k_3 I \in G$ and $k_1 I \leq k_2 I$. $k_1 I \leq k_2 I$ implies $\frac{k_2}{k_1} \in V$. $\frac{k_3}{k_3} = 1 \in V$, so

$$\frac{k_2}{k_1} \cdot \frac{k_3}{k_3} = \frac{k_2 k_3}{k_1 k_3} \in V.$$ 

Thus, $k_1 k_3 I \leq k_2 k_3 I$. Since $k_1 k_3 I = k_1 I \odot k_3 I$ and $k_2 k_3 I = k_2 I \odot k_3 I$, $k_1 I \odot k_3 \leq k_2 I \odot k_3 I$.

We now can conclude that $G$ is an ordered abelian group.

Define $v: K \to GU[\omega]$ by $v(k) = kI$ for $k \in K \setminus \{0\}$ and $v(0) = \infty$. $v$ is clearly a well-defined function from $K$ onto $GU[\omega]$.

Let $k \in K$ such that $k \neq 0$. $v(k) = kI \in G$. By definition, $v(0) = \infty$.

Suppose $k_1$ and $k_2 \in K \setminus \{0\}$. $v(k_1 k_2) = k_1 k_2 I = k_1 I \odot k_2 I = v(k_1) \odot v(k_2)$. $v(k_1 \cdot 0) = v(0) = \infty = v(k_1) \odot v(0)$.

Let $k_1$ and $k_2 \in K \setminus \{0\}$. Suppose $v(k_1) = \min\{v(k_1), v(k_2)\}$.

$v(k_1) \leq v(k_2)$ implies $\frac{k_2}{k_1} \in V$. $1 = \frac{k_1}{k_1} \in V$, so

$$\frac{k_1}{k_1} + \frac{k_2}{k_1} = \frac{k_1 + k_2}{k_1} \in V.$$ 

This implies that $k_1 I \leq (k_1 + k_2) I$. Thus, $v(k_1) \leq v(k_1 + k_2)$.

Hence, $v(k_1 + k_2) \geq v(k_1) = \min\{v(k_1), v(k_2)\}$. If $v(k_2) = \min\{v(k_1), v(k_2)\}$ a symmetrical argument leads to the same result. $v(k_1 \cdot 0) = v(k_1) < \infty$. Hence,

$$v(k_1 + 0) \leq \min\{v(k_1), v(0)\}.$$

Thus, $v$ is a non-Archimedean valuation on $K$.
Let \( x \in V \). Then \( x \in K \), so \( v(x) = xI \). Since \( x = \frac{x}{I} \in V \), \( I \leq xI \). Therefore, \( v(x) \geq I = 0 \). Hence \( V \subseteq \{ x \in K | v(x) \geq I \} \).

Let \( x \in K \) such that \( v(x) \geq 0 \). \( xI \geq I \) implies that \( \frac{x}{I} = x \in V \). Thus \( \{ x \in K | v(x) \geq 0 \} \subseteq V \). Hence,

\[
V = \{ x \in K | v(x) \geq 0 = I \}.
\]

**Theorem 3.11.** Let \( v \) be a non-Archimedean valuation on a field \( K \). Define \( V \) by \( V = \{ x \in K | v(x) \geq 0 \} \) where \( 0 \) is the identity in the range of \( v \). Then \( V \) is a valuation ring and if \( M = \{ x \in K | v(x) > 0 \} \), then \( M \) is the unique maximal ideal.

**Proof.** \( V \neq \emptyset \) because \( v(0) = -\infty \geq 0 \). Therefore, \( 0 \in V \).

Suppose \( a \in V \) and \( a \neq 0 \). There exists \( -a \in K \) such that \( a + -a = 0 \). \( v(a) = v(1a) = v(1) + v(a) \). Thus, \( v(1) = 0 \).

So \( 1 \in V \). \( 0 = v(1) = v(-1 \cdot -1) = v(-1) + v(-1) \). Thus,

\[
v(-1) = 0 \quad \text{and so} \quad -1 \in V.
\]

\[
v(-a) = v(-1a) = v(-1) + v(a) = 0 + v(a) = v(a) \geq 0.
\]

So \( -a \in V \).

All the other properties necessary for \( V \) to be an integral domain with a unity are satisfied simply because \( V \subseteq K \) and \( K \) is a field.

Suppose \( x \in K \) and \( x \notin V \). Then \( v(x) < 0 \).

\[
0 = v(1) = v(x \cdot \frac{1}{x}) = v(x) + v\left(\frac{1}{x}\right).
\]

Since \( v(x) < 0 \) and \( 0 = v(x) + v\left(\frac{1}{x}\right) \), \( v\left(\frac{1}{x}\right) = -v(x) > 0 \).

Hence, \( \frac{1}{x} \in V \). Thus, \( V \) is a valuation ring in \( K \).

Let \( I = \{ x \in K | v(x) = 0 \} \). Note that \( I \subseteq V \subseteq K \).

Let \( x \in I \). \( \frac{1}{x} \in K \) and \( 0 = v(1) = v(x \cdot \frac{1}{x}) = v(x) + v\left(\frac{1}{x}\right) = 0 + v\left(\frac{1}{x}\right) = v\left(\frac{1}{x}\right) \).

Thus \( \frac{1}{x} \in I \subseteq V \). So every \( x \in I \) is a unit in \( V \).
Let \( x \in V \) and suppose \( x \) is a unit. Then there exists \( \frac{1}{x} \in V \) such that \( x \cdot \frac{1}{x} = 1 \). \( \theta = v(1) = v(x \cdot \frac{1}{x}) = v(x) + v(\frac{1}{x}) \).

\( x \) and \( \frac{1}{x} \in V \) so \( v(x) \geq \theta \) and \( v(\frac{1}{x}) \geq \theta \). But \( \theta = v(x) + v(\frac{1}{x}) \), so \( v(x) = \theta \) and \( v(\frac{1}{x}) = \theta \). Thus \( x \in I \). So every unit in \( V \) is in \( I \). Thus, \( I \) is the set of all units in \( V \). Note that \( M = V \setminus I \).

\( M \neq \emptyset \) because \( \emptyset \in V \) and \( v(\emptyset) = \infty > \theta \). So \( \emptyset \in M \).

Suppose \( a,b \in M \). Then \( v(a) > \theta \) and \( v(b) > \theta \).

\[
v(a - b) = v(a + \cdot -b) \geq \min\{v(a), v(b)\}
= \min\{v(a), v(b)\} > \theta.
\]

Hence \( a - b \in M \).

Let \( a \in M \) and \( b \in V \). Then \( v(a) > \theta \). \( v(ab) = v(a) + v(b) > \theta \) because \( v(b) \geq \theta \) and \( v(a) \geq \theta \). Hence, \( ab \in M \). So \( M \) is an ideal in \( V \).

Since \( M = V \setminus I \), \( M < V \). Suppose \( B \) is an ideal such that \( M < B \subseteq V \). Since \( M < B \), \( B \) must contain some element in \( I \).

But \( I \) is the set of all units, so there exists a unit in \( B \).

Thus \( B = V \). So \( M \) is a maximal ideal in \( V \). \( M \) is unique because in a valuation ring, all ideals are chained.

**Example 3.12.** Let \( K \) be a field and \( x \) an indeterminate. Let \( p(x) \) be a non-constant irreducible polynomial in \( K[x] \).

If \( 0 \neq \frac{f(x)}{g(x)} \in K(x) \), then \( (K(x) = \{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x] \) and \( g(x) \neq 0 \}) \), then \( \frac{f(x)}{g(x)} = [p(x)]^n \cdot \frac{f_1(x)}{g_1(x)} \) where \( f_1(x) \) and \( g_1(x) \) are not divisible by \( p(x) \) and \( n \) is an integer. Define \( v \) from \( K(x) \) into the reals by \( v(\frac{f(x)}{g(x)}) = n \) and \( v(0) = \infty \). Function \( v \) is a valuation on \( K(x) \).
Proof. Clearly the set of all real numbers is an ordered abelian group under the operation addition.

For every $\frac{f(x)}{g(x)} \in K(x)$ such that $\frac{f(x)}{g(x)} \neq 0$, $v\left(\frac{f(x)}{g(x)}\right) = n$ for some integer $n$. Hence, $v\left(\frac{f(x)}{g(x)}\right) \in \mathbb{R}$. $v(0) = \infty$ by definition.

Suppose $\frac{f(x)}{g(x)}$ and $\frac{h(x)}{j(x)} \in K(x)$ and neither are 0.

$$\frac{f(x)}{g(x)} = [p(x)]^n \frac{f_1(x)}{g_1(x)}$$
where neither $f_1(x)$ or $g_1(x)$ are divisible by $p(x)$ and $n$ is an integer. $\frac{h(x)}{j(x)} = [p(x)]^m \frac{h_1(x)}{j_1(x)}$

where neither $h_1(x)$ or $j_1(x)$ are divisible by $p(x)$ and $m$ is an integer. $\frac{f(x)}{g(x)} \cdot \frac{h(x)}{j(x)} = [p(x)]^{n+m} \frac{f_1(x)h_1(x)}{g_1(x)j_1(x)}$. Since $p(x)$ is an irreducible polynomial and $p(x)$ does not divide $f_1(x)$, $h_1(x)$, $g_1(x)$, or $j_1(x)$, $p(x)$ does not divide $f_1(x)h_1(x)$ and $p(x)$ does not divide $g_1(x)j_1(x)$. So

$$v\left(\frac{f(x)}{g(x)} \cdot \frac{h(x)}{j(x)}\right) = n+m = v\left(\frac{f(x)}{g(x)}\right) + v\left(\frac{h(x)}{j(x)}\right).$$

Suppose $\frac{f(x)}{g(x)} = 0$. Then clearly

$$v\left(\frac{f(x)}{g(x)} \cdot \frac{h(x)}{j(x)}\right) = v(0) = \infty = v\left(\frac{f(x)}{g(x)}\right) + v\left(\frac{h(x)}{j(x)}\right).$$

Suppose $\frac{f(x)}{g(x)}$ and $\frac{h(x)}{j(x)}$ are in $K(x)$ and neither are 0.

$$\frac{f(x)}{g(x)} = [p(x)]^n \frac{f_1(x)}{g_1(x)} = [p(x)]^{n-q} \frac{f_1(x)}{g_1(x)}$$
and

$$\frac{h(x)}{j(x)} = [p(x)]^m \frac{h_1(x)}{j_1(x)} = [p(x)]^{m-r} \frac{h_1(x)}{j_1(x)}$$
where \( p(x) \) does not divide \( f_1(x) \), \( g_1(x) \), \( h_1(x) \), or \( j_1(x) \) and \( n, q, m, \) and \( r \) are all positive integers.

\[
\frac{f(x)}{g(x)} + \frac{h(x)}{j(x)} = \frac{f(x)j(x) + h(x)g(x)}{g(x)j(x)}
\]

\[
= \frac{[p(x)]^{n+r}f_1(x)j_1(x) + [p(x)]^{m+q}h_1(x)g_1(x)}{[p(x)]^{q+r}g_1(x)j_1(x)} = A.
\]

\( v(\frac{f(x)}{g(x)}) = n-q \) and \( v(\frac{h(x)}{j(x)}) = m-r. \)

**Case 1.** Suppose \( \min\{v(\frac{f(x)}{g(x)}), v(\frac{h(x)}{j(x)})\} = v(\frac{h(x)}{j(x)}) \). Then \( m-r \leq n-q \). This implies \( m+q \leq n+r \). So

\[
A = \frac{[p(x)]^{m+q}[p(x)]^{n+r-m-q}f_1(x)j_1(x) + h_1(x)g_1(x)}{[p(x)]^{q+r}g_1(x)j_1(x)}
\]

If \( n+r-m-q = 0 \), then it is possible for \( p(x) \) to divide \( f_1(x)j_1(x) + h_1(x)g_1(x) \). If \( n+r-m-q > 0 \), then \( p(x) \) does not divide \( f_1(x)j_1(x) + h_1(x)g_1(x) \). (\( n+r-m-q \leq 0 \) because \( m+q \leq n+r \)). So

\[
[p(x)]^{n+r-m-q}f_1(x)j_1(x) + h_1(x)g_1(x)
\]

\
= p(x)^z k(x) where \( z \geq 0 \)

and \( p(x) \) does not divide \( k(x) \). Hence,

\[
A = \frac{[p(x)]^{m+q+z}k(x)}{[p(x)]^{q+r}g_1(x)j_1(x)} = \frac{[p(x)]^{m-r+z}k(x)}{g_1(x)j_1(x)}.
\]

Since \( p(x) \) does not divide \( g_1(x) \) or \( j_1(x) \), \( p(x) \) does not divide \( g_1(x)j_1(x) \). Thus

\[
v(\frac{f(x)}{g(x)} + \frac{h(x)}{j(x)}) = m-r+z \geq \min\{v(\frac{f(x)}{g(x)}), v(\frac{h(x)}{g(x)})\}.
\]
Case 2. Suppose \( \min \{v\left(\frac{f(x)}{g(x)}\right), v\left(\frac{h(x)}{j(x)}\right)\} = v\left(\frac{f(x)}{g(x)}\right) \).

The proof for this case is symmetrical to Case 1. If either \( \frac{f(x)}{g(x)} \) or \( \frac{h(x)}{g(x)} \) are 0, this proof is trivial. Hence, \( v \) is a valuation on \( K(x) \).

**Theorem 3.13.** Let \( v \) be a non-Archimedean valuation on a field \( K \). Then, i) If \( a \) and \( b \in K \) and \( v(a) \neq v(b) \), then \( v(a+b) = \min\{v(a), v(b)\} \) and ii) If \( K \) is finite, then \( v(a) = 0 \) for all \( 0 \neq a \in K \).

**Proof.** i) \( v(a+b) \geq \min\{v(a), v(b)\} \) by definition. Suppose \( v(a) = \min\{v(a), v(b)\} \) and \( v(a+b) > v(a) \).

\[
v(a) = v(a+b-b) \geq \min\{v(a+b), v(-b)\}.
\]

Let \( a \in K \). \( v(a) = v(1\cdot a) = v(1) + v(a) \). Thus, \( v(1) = 0 \). 
0 = \( v(1) = v(-1 \cdot -1) = v(-1) + v(-1) \), so \( v(-1) = 0 \). Thus, 
\( v(-b) = v(-1 \cdot b) = v(-1) + v(b) = 0 + v(b) = v(b) \). So 
\( v(-b) = v(b) \). Hence, \( v(a) \geq \min\{v(a+b), v(b)\} \). If \( v(a+b) \) is the \( \min\{v(a+b), v(b)\} \), then \( v(a+b) > v(a) \geq v(a+b) \). But 
this implies \( v(a+b) > v(a+b) \) which is impossible. If 
\( v(b) = \min\{v(a+b), v(b)\} \), then \( v(a) > v(b) \). But 
\( v(a) = \min\{v(a), v(b)\} \), 
so this case is also impossible. Thus, \( v(a+b) = \min\{v(a), v(b)\} \).

If \( v(b) = \min\{v(a), v(b)\} \), a similar argument results also with \( v(a+b) = \min\{v(a), v(b)\} \).

ii). Let \( a \in K \) and suppose \( a \neq 0 \). Since \( K \) is a finite field, there exists a prime \( p \) and a positive integer \( n \) such that \( a^p^n = a \). Since \( p \) is a prime, then \( p^n \geq 2 \).
Suppose \( v(a) = B \) where \( B > 0 \). \( B = v(a) = v(a^{p^n}) \). By an obvious induction proof, \( v(a^{p^n}) = p^n \cdot v(a) = p^n B \). Hence \( B = p^n B \). Thus \( 0 = p^n B - B = (p^n - 1)B \). Since \( p^n \geq 2 \), \( p^n - 1 \geq 1 \). Since \( B > 0 \) and \( p^n - 1 \geq 1 \), \( (p^n - 1)B > 0 \). But \( 0 = (p^n - 1)B \). This implies \( 0 > 0 \) which is impossible. Hence, \( B \neq 0 \). If \( B < 0 \) a similar argument also produces a contradiction. Thus, for all \( a \in \mathbb{K} \) such that \( a \neq 0 \), \( v(a) = 0 \).

**Example 3.1.** Let \( \mathbb{D} \) be a unique factorization domain with quotient field \( \mathbb{K} \). Let \( x \in \mathbb{K} \) such that \( x \neq 0 \).

\[ x = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n} \]

where each \( p_i \) is a prime in \( \mathbb{D} \) and each \( s_i \) is an integer for every \( i \in \{1, 2, \ldots, n\} \). Define \( v_{p_i}(x) = s_i \) when \( x \neq 0 \) and \( v_{p_i}(0) = \infty \). The valuation \( v_{p_i} \) is a non-Archimedean valuation on \( \mathbb{K} \) and \( \{x \in \mathbb{K} | v_{p_i}(x) \geq 0\} \) is the valuation ring of \( v_{p_i} \). \( v_{p_i} \) is called the \( p_i \)-adic valuation on \( \mathbb{K} \).

**Proof.** \( v_{p_i} \) is clearly a function from \( \mathbb{K} \) into the ordered group of reals \( \mathbb{U} \cup \{\infty\} \).

Let \( x \in \mathbb{K} \). \( v_{p_i}(x) = n \) where \( n \) is an integer. Hence, \( v_{p_i}(x) \in \text{reals} \). \( v_{p_i}(0) = \infty \) by definition.

Let \( x \) and \( y \in \mathbb{K} \). Then \( x = p_1^{s_1} \cdots p_n^{s_n} \) where each \( p_j \) is a prime, \( p_j \neq p_i \) for any \( j \in \{1, 2, \ldots, n\} \), \( s_i \) is an integer, \( s_j \) is an integer for each \( j \), and \( y = p_i^{t_i} \cdots p_m^{t_m} \) where each \( q_j \) is a prime, \( q_j \neq p_i \) for any \( j \in \{1, 2, \ldots, m\} \), \( t_i \) is an integer, and \( t_j \) is an integer for each \( j \).
If either \( x \) or \( y \) is 0, this proof is trivial.

Let \( x \) and \( y \) be the same as above.

\[
\begin{align*}
x + y &= p_i \left( \prod_{j=1}^{s_i} p_j \right) + p_i \left( \prod_{j=1}^{t_i} q_j \right) \\
&= p_i \left( s_i \left( \prod_{j=1}^{n} p_j \right) + \prod_{j=1}^{m} q_j \right) \\
&= p_i s_i A.
\end{align*}
\]

\( p_i \) might divide \( A \), so \( A = p_i^k B \) where \( k \geq 0 \) and \( p_i \) does not divide \( B \). Hence, \( x + y = p_i^{s_i+k} B \). So

\[
\nu_{p_i}(x+y) = s_i + k = s_i = \min(\nu_{p_i}(x), \nu_{p_i}(y)).
\]

\textbf{Case 1.} Suppose \( s_i = t_i \). Then

\[
\begin{align*}
x + y &= p_i \left( \prod_{j=1}^{s_i} p_j \prod_{j=1}^{t_i} q_j \right) \\
&= p_i^{s_i} A.
\end{align*}
\]

\( p_i \) does not divide \( A \), hence \( \nu_{p_i}(x+y) = s_i = \min(\nu_{p_i}(x), \nu_{p_i}(y)) \).

\textbf{Case 2.} Suppose \( s_i < t_i \). Then

\[
\begin{align*}
x + y &= p_i \left( \prod_{j=1}^{s_i} p_j \prod_{j=1}^{t_i} q_j \right) \\
&= p_i^{s_i} A.
\end{align*}
\]

\( p_i \) does not divide \( A \), hence \( \nu_{p_i}(x+y) = s_i = \min(\nu_{p_i}(x), \nu_{p_i}(y)) \).

\textbf{Case 3.} Suppose \( s_i > t_i \). This case is similar to Case 2, except \( \nu_{p_i}(x+y) = t_i = \min(\nu_{p_i}(x), \nu_{p_i}(y)) \).

In all cases, \( \nu_{p_i}(x+y) \geq \min(\nu_{p_i}(x), \nu_{p_i}(y)) \). Thus, \( \nu_{p_i} \) is a non-Archimedean valuation on \( K \).
Let \( Z = \{x \in K | v_{p_i}(x) \geq 0\} \). \( Z \neq \emptyset \) because \( 0 \in K \) and \( v_{p_i}(0) = \infty \geq 0 \). Thus, \( 0 \in Z \).

Let \( a \in Z \). \( 1 \in Z \) because \( 1 = p_i^0 \), so \( v_{p_i}(1) = 0 \).

\(-1 \in Z \) because \( 0 = v_{p_i}(1) = v_{p_i}(-1\cdot1) = v_{p_i}(-1) + v_{p_i}(-1) \)

which implies \( v_{p_i}(-1) = 0 \). Thus,

\[
v_{p_i}(-a) = v_{p_i}(-1\cdot a) = v_{p_i}(-1) + v_{p_i}(a) = 0 + v_{p_i}(a) = v_{p_i}(a).
\]

So \(-a \in Z \).

Let \( a \) and \( b \in Z \). \( v_{p_i}(ab) = v_{p_i}(a) + v_{p_i}(b) \geq 0 \). So \( ab \in Z \).

All the other properties necessary for \( Z \) to be an integral domain hold because \( Z \subseteq K \) and \( K \) is a field.

Since \( D \subseteq Z \subseteq K \), \( K \) is the quotient field for \( D \), and both \( D \) and \( Z \) are integral domains, \( K \) is the quotient field for \( Z \). Let \( x \in K \) and suppose \( x \notin Z \). \( x \in K \setminus Z \) implies

\[
x = p_i^{m \cdot \prod_{j=1}^{n} q_j} \text{ where } m < 0.
\]

\[
\frac{1}{x} = \frac{1}{p_i^{m \cdot \prod_{j=1}^{n} q_j}} = p_i^{-m} \frac{1}{\prod_{j=1}^{n} q_j}.
\]

Since \( m < 0 \), \(-m > 0\). So \( v_{p_i}(\frac{1}{x}) = -m > 0 \). Thus, \( \frac{1}{x} \in Z \). Therefore \( Z \) is a valuation ring in \( K \).
BIBLIOGRAPHY