Semi-Valuations and Groups of Divisibility.

Dolores Richard Spikes
Louisiana State University and Agricultural & Mechanical College

Follow this and additional works at: https://repository.lsu.edu/gradschool_disstheses

Recommended Citation
https://repository.lsu.edu/gradschool_disstheses/2173

This Dissertation is brought to you for free and open access by the Graduate School at LSU Scholarly Repository. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Scholarly Repository. For more information, please contact gradetd@lsu.edu.
SPIKES, Dolores Richard, 1936-
SEMI-VALUATIONS AND GROUPS OF DIVISIBILITY.

The Louisiana State University and Agricultural and Mechanical College, Ph.D., 1971
Mathematics

University Microfilms, A XEROX Company, Ann Arbor, Michigan
SEMI-VALUATIONS

and

GROUPS OF DIVISIBILITY

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by

Dolores Richard Spikes
B.S., Southern University, 1957
M.S., University of Illinois, 1958
December, 1971
PLEASE NOTE:

Some pages may have
indistinct print.
Filmed as received.

University Microfilms, A Xerox Education Company
ACKNOWLEDGMENT

The author is grateful to Professor Jack E. Ohm for his counsel and encouragement during the preparation of this dissertation, and wishes also to express her deep appreciation to Dr. Robert L. Pendleton for his inspiration and confidence, and for his guidance during the earlier stage of development of this dissertation. The author is also grateful to the Ford Foundation for its financial support from 1968 to 1971.

Finally, the author expresses profound gratitude to her husband, Hermon Spikes, and to her daughter, Rhonda Kathleen, for their patience, understanding and encouragement during the past three years and especially during the preparation of this dissertation.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGMENT</td>
<td>ii</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>iv</td>
</tr>
<tr>
<td><strong>CHAPTER</strong></td>
<td></td>
</tr>
<tr>
<td>I  Introduction</td>
<td>1</td>
</tr>
<tr>
<td>II Semi-Valuations</td>
<td>9</td>
</tr>
<tr>
<td>III Composite Semi-Valuations</td>
<td>22</td>
</tr>
<tr>
<td>IV V-homomorphisms and Lexicographically Exact Sequences</td>
<td>45</td>
</tr>
<tr>
<td>V  A Class of Groups which are not Groups of Divisibility of Domains</td>
<td>53</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>61</td>
</tr>
<tr>
<td>APPENDIX</td>
<td>63</td>
</tr>
<tr>
<td>VITA</td>
<td>76</td>
</tr>
</tbody>
</table>
ABSTRACT

Let $R$ be a commutative ring with identity and denote by $R^*$ and 
$T(R)$ the multiplicative monoid of regular elements of $R$ and the total 
quotient ring of $R$, respectively. There is associated with $R$ a 
partially ordered Abelian group $G$, called the group of divisibility 
of $R$ and a mapping $w$ from $T(R)^*$ onto $G$, called a semi-valuation of 
$T(R)$. (More generally, $G$ is called a semi-value group of $w$.) The 
ring $D$ consisting of 0 and all elements $x \in \bigoplus_{n=1}^{\infty} w^{-1}(G^+)$ for each 
positive integer $n$, is called the semi-valuation ring of $w$.

There have been instances where interesting examples of domains 
were constructed by phrasing ring-theoretic problems in terms of the 
ordered group $G$, first solved there, and the solution pulled back to 
a ring $R$. The main theorem in the pull-back process has been a 
theorem of Jaffard's which asserts that any lattice-ordered group is 
a group of divisibility. More recently, Ohm has given procedures 
for constructing a large class of groups of divisibility of domains 
which are not necessarily lattice, and also a class of ordered groups 
which are filtered and are not groups of divisibility of domains.

This paper gives procedures for constructing a class of groups 
of divisibility of rings (not necessarily domains) which properly 
includes the class constructed by Ohm. Toward that end, we first 
extend the concept of a semi-valuation of a field to rings which may 
contain zero-divisors. The notion of a composite of two valuations 
of fields is then extended to the notion of a composite of two semi-
valuations of total quotient rings (which may not be fields), and 
the construction of this composite is then related to an exact
sequence of semi-value groups. Necessary and sufficient conditions for this sequence to be lexicographically exact are given.

Suppose that \( C \) is a group of divisibility. Among the groups of divisibility resulting from our construction are the following:

1. Certain groups of the form \( A \oplus C_p \) (lexicographic sum), where \( A \) is a semi-value group satisfying certain conditions of our construction, \( C \) is free, and \( C_p \) is the group \( C \) ordered by a specified submonoid \( P \) of \( C^+ \);

2. Groups of the form \( [A_u \oplus \bigoplus_1^\infty (k, +)] \oplus C_p \), where \( A_u \) is any semi-value group of the field \( k \), \( C \) is totally ordered, \( P = \{ c \in C : c = c_1 + \ldots + c_n \text{ for a fixed integer } n \geq 1, c_i > 0 \text{ or } c = 0 \} \), \( (k, +) \) denotes the additive group of the field \( k \), and \( \text{card } l = \text{card } (C^+ \sim P) \).

If \( 0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C_p \to 0 \) is an exact sequence of ordered groups, \( v \) is a semi-valuation of a ring \( T(R) \) with semi-value group \( B \), and \( \beta : B \to C \) is a \( V \)-homomorphism, then \( \beta v \) is also a semi-valuation with semi-value group \( C \). Under the assumptions that the sequence is lexicographically exact and \( (P \sim 0) + C^+ \subseteq P \), we give necessary and sufficient conditions for \( \beta : B \to C \) to be a \( V \)-homomorphism. Finally, we construct a class of groups which are filtered, but are not groups of divisibility.
CHAPTER I
INTRODUCTION

If $R$ is an integral domain, there is associated with $R$ a partially ordered group $G$, called the group of divisibility of $R$, and a map $w$ from the group of units of the quotient field $K$ of $R$ onto $G$; $w$ is called a semi-valuation of $K$. When $R$ is a valuation domain, $G$ is the value group and $w$ is a valuation. In this case there is a well-developed theory which enables one to relate ideal properties of $R$ to properties of $G$. There have been instances where a ring-theoretic problem was phrased in terms of the ordered group $G$, first solved there, and then the solution pulled back to $R$ [12]. In addition, this method has been used to construct interesting examples of domains ([13],[4]).

Krull[7] first proved that any totally ordered group is the group of divisibility of a domain. In the more general case, Jaffard [5] has proved that any lattice-ordered group is the group of divisibility of a domain, but beyond this it seems that nothing had been done, before Ohm's work in [13], in investigating non-lattice groups of divisibility.

Jaffard provides an example in [5] of a filtered ordered group which is not a group of divisibility. In [13], Ohm gives procedures for constructing a class of groups, not necessarily lattice, which are groups of divisibility, and a class of groups which are not groups of divisibility.

The primary concern of this paper is that of showing that Ohm's procedure and related theorems can be generalized to yield a larger class of groups which are groups of divisibility and to provide additional examples of filtered groups which are not groups of
divisibility. Our generalization is not confined to domains. Thus, Chapter II is devoted to extending the concept of a semi-valuation to rings with zero-divisors. In the case of a field $K$, there is a one-to-one correspondence between subrings of $K$ and equivalence classes of semi-valuations of $K$. We lose this one-to-one correspondence by allowing zero-divisors, but regain a uniqueness condition by the introduction of the concept of a semi-valuation monoid. When confined to domains, this theory reduces to that found in [13].

In Chapter III, we state and prove our main theorems related to the construction of groups of divisibility. The construction in [13] involves an extension of the notion of the composite of two valuations to that of the composite of two semi-valuations, and, under certain assumptions, relates the construction of the composite to a lexicographically exact sequence of ordered groups. We show that this construction can be done in a more general setting and give necessary and sufficient conditions for the relation of the construction to a lexicographically exact sequence of ordered groups. As an application of our main theorem, we obtain the groups of divisibility of all subrings $R$ of the integral closure of $Z(p)$ (the ring of integers $Z$ localized at the prime ideal $(p)$ of $Z$), where $R \supseteq Z(p)$, in a quadratic extension of the field of rational numbers.

Let $C$ be an ordered group with its monoid of positive elements denoted by $C^+$, and let $P$ be a submonoid of $C^+$. Let $C_P$ denote the group $C$ ordered by $P$. Suppose that $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C_P \rightarrow 0$ is lexicographically exact and that $(P \sim 0) + (C^+) \subseteq P$. In Chapter IV, we determine necessary and sufficient conditions for the homomorphism
\( \beta : B \to C \) to be a \( V \)-homomorphism. Finally, in Chapter V, we construct a class of groups which are not groups of divisibility of domains or of certain rings with zero-divisors.

**Preliminaries**

We begin with definitions which are of primary concern to the work of Ohm. Consequently, most of the following, or references — especially to [1] and [5] — can be found in [13].

1. **Ordered groups.** By an ordered group we mean a commutative group with a partial ordering. The ordered group \( G \) is called filtered if for any \( a_1, a_2 \in G \), there exists \( a \in G \) such that \( a \leq a_1, a_2, G^+ \) denotes the elements of \( G \) greater than or equal to zero. The elements of \( G^+ \) form a submonoid of \( G \), i.e., \( G^+ \) satisfies: \( 0 \in G^+ \) and \( x, y \in G^+ \) implies \( x + y \in G^+ \). An ordered subgroup \( B \) of \( G \) is an ordered group contained in \( G \) such that \( B^+ = (A^+) \cap B \). If \( D = \prod \alpha D^\alpha \) is a direct product of ordered groups \( D^\alpha \), \( D \) is called the ordered direct product if \( D^+ = \{d \in D : d^\alpha \geq 0 \text{ for all } \alpha \} \). The ordered direct sum is defined similarly.

2. **Exact sequences.** A homomorphism \( \alpha \) of an ordered group \( A \) into an ordered group \( B \) is called an order homomorphism if \( \alpha(A^+) \subseteq B^+ \). \( \alpha \) is an order isomorphism if \( \alpha \) is a group isomorphism and \( \alpha(A^+) = B^+ \).

A short exact sequence of ordered groups

\[
0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0
\]

is called semi-order exact if \( \alpha(A^+) = \alpha(A) \cap B^+ \) and \( \beta(B^+) \subseteq C^+ \).
(1.1) is called order exact if $\alpha(A^+) = \alpha(A) \cap B^+$ and $\beta(B^+) = C^+$.

The exact sequence (1.1) is said to be lexicographically exact if $B^+ = \{b \in B: b \in \alpha(A^+) \text{ or } \beta(b) > 0\}$. A lexicographically exact sequence is order exact.

If $A$ and $C$ are ordered groups, we order the direct sum $A \oplus C$ by defining $(A \oplus C)^+ = \{(a, c): c > 0 \text{ or } c = 0 \text{ and } a \geq 0\}$. Thus, if $i$ and $p$ are the usual injection and projection maps, respectively, we have a lexicographically exact sequence

$$0 \to A \overset{i}{\to} A \oplus C \overset{p}{\to} C \to 0.$$

The semi-order exact sequence $0 \to A \overset{\alpha}{\to} B \overset{\beta}{\to} C \to 0$ splits if there exists a commutative diagram

$$0 \to A \overset{\alpha}{\to} B \to C \to 0 \quad \text{splitting if there exists a commutative diagram}$$

$$\begin{array}{cccccc}
0 & \to & A & \overset{\alpha}{\to} & B & \to C & \to 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & A & \overset{i_1}{\to} & A \oplus C & \overset{i_2}{\to} & C & \to 0 \\
\end{array}$$

where $i_1$ and $i_3$ are the identity maps, $i_2$ is an order isomorphism, and $i, p$ are the usual injection and projection maps, respectively.

Except for an example in Chapter III, where explicit mention of this shall be made again, the symbol $A \oplus C$ will always be used to denote the lexicographic sum.

3. V-homomorphisms. If $B$ and $C$ are ordered groups and $\beta$ is a homomorphism, then $\beta$ is called a V-homomorphism if for any $b_0, b_1, \ldots, b_n \in B$, $b_0 \geq \inf_B \{b_1, \ldots, b_n\}$ implies $\beta(b_0) \geq \inf_C \{\beta(b_1), \ldots, \beta(b_n)\}$. A V-isomorphism is an isomorphism such that it and its inverse are V-homomorphisms. A V-imbedding of $B$ in $C$ is a V-homomorphism which is one-to-one. A subgroup $B$ of $C$ is a V-subgroup if the identity map is a V-homomorphism. We mention below a few properties of
(a) If $\alpha: A \to B$ and $\beta: B \to C$ are $V$-homomorphisms, then $\beta \alpha$ is also.

(b) If $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is lexicographically exact, then $\alpha$ is a $V$-homomorphism.

(c) If $B$ and $C$ are lattice-ordered groups, then the homomorphism $\beta: B \to C$ is a $V$-homomorphism if and only if $\beta(\inf_B \{b_1, \ldots, b_n\}) = \inf_C \{\beta(b_1), \ldots, \beta(b_n)\}$.

In Chapter II, we define a semi-valuation on an arbitrary commutative ring $R$ with identity. However, we show that we might as well have defined the semi-valuation on the total quotient ring of $R$, i.e., we prove that any semi-valuation of $R$ can be uniquely extended to a semi-valuation of the total quotient ring of $R$. Thus, we include below a brief discussion of some facts concerning total quotient rings which will be pertinent to our work.

An element $r$ of a commutative ring $R$ is called a **regular element** if $s r \neq 0$ for any $s \neq 0$ in $R$. $r$ is called a **zero-divisor** if $r \neq 0$ and $r$ is not regular. We observe the usual conventions with respect to subrings of a ring and ring homomorphisms. In particular, we require that any subring $R$ of a ring $R'$ with identity to have the identity of $R'$ as its identity element, whenever $R$ has an identity.

Let $R$ be a subring of a ring $R'$. $R'$ is called a **total quotient ring** of $R$ if and only if each of the following two conditions holds:

1. Every regular element of $R$ is a unit in $R'$.
2. Every element of $R'$ has the form $ab^{-1}$ where $a, b \in R$ and $b$ is a regular element of $R$. 

$V$-homomorphisms found in [13].
Every commutative ring with identity has a uniquely determined total quotient ring.

A unitary $R$-module $M$ is called $R$-torsion free if whenever $rm = 0$, $r \in R$, $m \neq 0 \in M$, then $r$ is a zero-divisor of $R$. Thus, it follows from the definition of a total quotient ring, that the total quotient ring of a ring $R$ is $R$-torsion free.

For commutative rings $R$, $R'$ with identity and a surjective homomorphism $h: R \rightarrow R'$, a necessary and sufficient condition that $R'$ be its own total quotient ring follows from a theorem of Krull.

First we state some preliminary concepts.

**Definition 1.2.** An element $b$ of a commutative ring $R$ is said to be a zero-divisor modulo $A$, where $A$ is an ideal of $R$, if there exists an element $c$ of $R$ not in $A$ such that $bc \in A$.

**Definition 1.3.** An ideal $P$ of $R$ is a maximal prime divisor of the ideal $A$ of $R$ if $P \supseteq A$ and $P$ is maximal with respect to containment in the set $\{x \in R: xy \in A \text{ for some } y \notin A\}$. $P$ is called a prime divisor of $A$ if there is a multiplicatively closed subset $S$ of $R$ which does not meet $A$ such that $PR_S$ is a maximal prime divisor of $AR_S$.

The following theorem is due to Krull [8].

**Theorem 1.4.** Let $A$ be an ideal of a ring $R$.

Then (a) every zero-divisor modulo $A$ is contained in a maximal prime divisor of $A$;

(b) every minimal prime divisor of $A$ is contained in at least one maximal prime divisor of $A$;

(c) Denote by $A(M)$ the ideal consisting of $\{x \in R: xy \in A \text{ for some } y \notin M\}$. 

Then \( A = \bigcap A(M) \) where \( M \) runs over all maximal prime divisors of \( A \).

**Proposition 1.5.** Let \( R, R' \) be commutative rings with identity, and let \( h: R \rightarrow R' \) be a surjective ring homomorphism. Then \( R' \) is a total quotient ring if and only if every maximal ideal containing \( \ker h \) is a prime divisor of \( \ker h \).

**Proof.** Suppose that \( R' \) is a total quotient ring. The maximal ideals of \( R' \) are just those ideals which are images under \( h \) of maximal ideals of \( R \) that contain \( \ker h \). Since every non-unit of \( R' \) is a zero-divisor, a maximal ideal \( M' \) of \( R' \) is also maximal with respect to containment in the set of zero-divisors of \( R' \). Thus \( h^{-1}(M') \) is a maximal prime divisor of \( \ker h \).

Conversely, if every maximal ideal \( M \) of \( \ker h \) is a prime divisor of \( \ker h \), then \( h(M) \) is a maximal ideal of \( R' \) and is a prime divisor of \( 0 \) in \( R' \). q.e.d.

We conclude this chapter with a brief discussion of the principal of idealization \([11]\). Let \( M \) be an \( R \)-module and \( R' \) the direct sum \( R \oplus M \) as modules. With multiplication defined by \((r,m)(r',m') = (rr', rm' + r'm)\), \( R' \) becomes a ring containing \( R \) and \( M \), in which \( M \) is an ideal and \( M^2 = 0 \). We say that \( R' \) is the ring formed by the principle of idealization. If \( I \) denotes the identity of \( R \), then \((1,0)\) is the identity element of \( R' \). The units of \( R' = \{(a,m) : a \text{ is a unit of } R\} \) and \((a,m)^{-1} = (a^{-1}, -(a^{-1})^2 m)\).

An element \( b \) of a ring \( R \) is called a zero-divisor with respect to a given \( R \)-module \( M \) if there is a non-zero element \( m \) of \( M \) such that \( bm = 0 \). Thus the set of zero-divisors of \( R' \) contains the set \( \{(b,m) : b \text{ is a zero-divisor with respect to } M\} \). It follows, then, that if
every non-unit of $R$ is in the set of zero-divisors of $R$ with respect to $M$, that $R'$ is a total quotient ring. Thus, for example, if $R$ is a domain and $\{B_i\}_i$ is the set of proper ideals of $R$, $M = \oplus_i (R/B_i)$, then $R' = R \bigoplus M$, the ring formed by the principle of idealization, is a total quotient ring.
Throughout this paper, we assume that any ring under discussion is commutative and has an identity element denoted by 1. A domain will always mean a commutative ring with 1 and without zero-divisors.

The following notation will be used consistently. If $R$ is a ring, denote by $R^*$ the multiplicative monoid formed by the regular elements of $R$ with respect to the ring multiplication and identity. $U(R)$ and $T(R)$ will denote, respectively, the multiplicative group of units of $R$ and the total quotient ring of $R$.

**Definition II.1.** A semi-valuation $w$ of a ring $R$ is a map from $R^*$ to an additive partially ordered group $G$ such that the following (hereafter referred to as axioms (i), (ii), (iii)) are satisfied.

(i) $w(xy) = w(x) + w(y)$ for all $x, y \in R^*$;

(ii) $w(x_1 + x_2 + \ldots + x_n) \geq \inf_{w(R^*)} \{w(x_1), w(x_2), \ldots, w(x_n)\}$ for any integer $n \geq 2$, whenever $x_1, x_2, \ldots, x_n, x_1 + x_2 + \ldots + x_n$ are in $R^*$;

(iii) $w(-1) = 0$.

**Remarks on definition II.1.**

1) Axiom (i) merely asserts that $w$ is a monoid homomorphism, and hence $w(R^*)$ is a submonoid of $G$.

2) Axiom (ii) is equivalent to the following two axioms:

(iii') $w(x+y) \geq \inf_{w(R^*)} \{w(x), w(y)\}$ whenever $x, y, x+y \in R^*$;

(iii'') $w(x_1 + \ldots + x_n) \geq \inf_{w(R^*)} \{w(x_1), \ldots, w(x_n)\}$ whenever $x_1, \ldots, x_n, x_1 + \ldots + x_n$ are in $R^*$

and

$$\sum_{i=1}^{j-1} x_i + \sum_{i=j+1}^{n} x_i \notin R^* U \{0\} \text{ for } j = 1, \ldots, n.$$
Proof of remark 2): It is clear that axiom (ii) implies each of the above axioms. Conversely, suppose that (ii) and (ii') hold. We show by induction that (ii) then holds. The case $n = 2$ is merely axiom (ii'). Assume inductively that (ii') and (ii'') imply (ii) for a fixed integer $n$.

Suppose that $x_1, \ldots, x_{n+1}$ are in $\mathbb{R}^\star$.

If $\sum_{i=1}^{j-1} x_i + \sum_{i=j+1}^{n+1} x_i \in \mathbb{R}^\star$, then $w(x_1 + \ldots + x_{n+1}) = w((x_1 + \ldots + x_{j-1} + \ldots + x_{n+1}) + x_j) \geq \inf_{w(\mathbb{R}^\star)} \{ w(x_1 + \ldots + x_{j-1} + x_{j+1} + \ldots + x_{n+1}) \} \cup \{ w(x_j) \}$.

By the inductive hypothesis,

$w(x_1 + \ldots + x_{j-1} + x_{j+1} + \ldots + x_{n+1}) \geq \inf_{w(\mathbb{R}^\star)} \{ w(x_1), \ldots, w(x_{j-1}), w(x_{j+1}), \ldots, w(x_{n+1}) \}$.

If $\sum_{i=1}^{j-1} x_i + \sum_{i=j+1}^{n+1} x_i = 0$ for some $j$, then $\sum_{i=1}^{j-1} x_i + \sum_{i=j+1}^{n+1} x_i = -x_{n+1} \in \mathbb{R}^\star$;

thus $w(\sum_{i=1}^{j-1} x_i + \sum_{i=j+1}^{n+1} x_i + x_{n+1} + x_j) \geq \inf_{w(\mathbb{R}^\star)} \{ w(\sum_{i=1}^{j-1} x_i + \sum_{i=j+1}^{n+1} x_i), w(x_{n+1}), w(x_j) \}$.

By the inductive hypothesis, $w(x_1 + \ldots + x_{n+1}) \geq \inf_{w(\mathbb{R}^\star)} \{ w(x_1), \ldots, w(x_{n+1}) \}$.

If $\sum_{i=1}^{j-1} x_i + \sum_{i=j+1}^{n+1} x_i \notin \mathbb{R}^\star \cup \{0\}$ for each $j = 1, \ldots, n+1$, then (ii) merely becomes the statement of axiom (ii').

3) In the case of a domain, axiom (ii') is satisfied vacuously and hence, as seen in remark 2), axiom (ii') implies axiom (ii).

The following example shows that in rings with zero-divisors, axioms (i), (ii') and (iii) do not imply axiom (ii').
Example 11.2. Denote by $Z(2)$ the localization of the ring of integers $Z$ at the prime ideal $(2)$ of $Z$. Let $M = \bigoplus_{i} Z(2)/B_i$, where $\{B_i\}$ is the set of proper ideals of $Z(2)$. Let $R = Z(2) \bigoplus M$ be the ring formed by the principle of idealization. As noted in the introduction, $R$ is a total quotient ring and $U(R) = \{(a,m): a \in U(Z(2))\}$.

Let $Z_p$ denote the ordered group of integers with positive elements $p = \{0, 2, 3, 4, \ldots\}$. For each $a \in Z(2)^*$, write $a = 3^k \cdot r$, where neither the numerator nor denominator of $r$ belongs to the ideal $(3)$ of $Z$.

Define a map $v: R^* \rightarrow Z_p$ by $v(a,m) = k$. Let $x = (3^k \cdot r_1, m_1)$, $y = (3^k \cdot r_2, m_2)$. Then $v(xy) = (3^{k_1+k_2} \cdot r_1 r_2, 3^{k_1} \cdot r_1 m_1 + 3^{k_2} \cdot r_2 m_2) = k_1 + k_2 = v(x) + v(y)$. Thus, axiom (i) is verified. $v((-1)) = v(3^0 \cdot (-1)) = 0$, so axiom (iii) is satisfied. If $x, y \in R^*$, then $x + y$ is a zero-divisor, so that axiom (ii) is satisfied vacuously.

$$v((1,0) + (1,0) + (1,0)) = v(3,0) = 1$$

$$\inf_{p} [v(1,0), v(1,0), v(1,0)] = 0$$

and hence axiom (iii') is not satisfied.

Proposition 11.3. Any semi-valuation of a ring $R$ extends uniquely to a semi-valuation of $T(R)$.

Proof. Let $w: R^* \rightarrow G$ be a semi-valuation of $R$. Define $w^*$ by

$$w^*(\frac{x}{y}) = w(x) - w(y)$$

for $x, y \in R^*$. We note that $w^*$ is a well-defined map on $T(R)^*$ since $w$ is well-defined and $T(R)$ is $R$-torsion free. Also, the restriction of $w^*$ to $R^*$ is $w$.

If $x_1, x_2, y_1, y_2 \in R^*$, then $w^* (\frac{x_1}{y_1} \cdot \frac{x_2}{y_2}) = w(x_1 x_2) - w(y_1 y_2)$

$$= w(x_1) - w(y_1) + w(x_2) - w(y_2) = w^*(\frac{x_1}{y_1}) - w^*(\frac{x_2}{y_2})$$

Thus axiom (i) is
verified. If \( x_1, \ldots, x_n, x_1 + \ldots + x_n \in T(R)^* \), then there exists \( s \in R^* \) such that \( sx_1, \ldots, sx_n, s(x_1 + \ldots + x_n) \in R^* \). Then 
\[ w(s(x_1 + \ldots + x_n)) = w(s(x_1 + \ldots + x_n)) \geq \inf_{w(R^*)} \{ w(sx_1), \ldots, w(sx_n) \} , \text{ by axiom (ii)}. \]
Therefore, 
\[ w(s) + w(x_1 + \ldots + x_n) \geq \inf_{w(R^*)} \{ w(s) + w(x_1), \ldots, w(s) + w(x_n) \} \]
implies that 
\[ w'(x_1 + \ldots + x_n) \geq \inf_{w(T(R)^*)} \{ w'(x_1), \ldots, w'(x_n) \}. \]
Hence 
\[ w' \text{ satisfies axiom (ii). } w'(-1) = w(-1) = 0, \text{ and therefore axiom (iii) is satisfied.} \]

If \( v \) is any semi-valuation of \( T(R) \) extending \( w \), then 
\[ v\left(\frac{x}{y}\right) = v(xy^{-1}) = v(x) - v(y) \text{ by axiom (i) and the fact that } v(y^{-1}) = -v(y). \]
Since \( x, y \in R^* \) and \( v \) extends \( w \), 
\[ v(x) - v(y) = w(x) - w(y) = w'(\frac{x}{y}) . \]
Thus, \( w' \) is uniquely determined by \( w \). q.e.d.

It follows from Proposition 11.3 that we do not get a more general situation by defining a semi-valuation for an arbitrary ring \( R \) rather than for its total quotient ring \( T(R) \), i.e., we may as well have assumed that \( R = T(R) \) in definition 11.1. We will make this assumption in many of the propositions and discussions to follow, explicitly stating so each time.

In case \( R = T(R) \), \( w(R^*) \) is a subgroup of \( G \), called the semi-value group of \( w \). Since we are interested in the image of \( w \) rather than all of \( G \), we assume that \( w(R^*) \) generates \( G \), and thus \( w \) is surjective whenever \( R = T(R) \).

Two semi-valuations \( w, w' \) of a ring \( R = T(R) \) having respective semi-value groups \( G, G' \) are called equivalent semi-valuations if and only if there exists an order isomorphism \( \Phi \) from \( G \) to \( G' \) such that 
\[ \Phi w = w' . \]
Let \( w \) be a semi-valuation of \( R = T(R) \). \( w^{-1}(G^+) \) has the following properties:

**P1:** \( w^{-1}(G^+) \) is a multiplicative submonoid of \( R^* \), i.e.,

1. \( w^{-1}(G^+) \subseteq R^* \);
2. if \( x, y \in w^{-1}(G^+) \), then \( xy \in w^{-1}(G^+) \);
3. \( 1 \in w^{-1}(G^+) \).

**P2:** \( (\sum_{i=1}^{n} w^{-1}(G^+)) \cap R^* \subseteq w^{-1}(G^+) \) for each positive integer \( n \);

\( (\sum_{i=1}^{n} w^{-1}(G^+) = [x_1 + \ldots + x_n : x_i \in w^{-1}(G^+)] \).

**P3:** \( -1 \in w^{-1}(G^+) \).

**Definition 1.4.** Let \( w : R^* \to G \) be a semi-valuation of \( R = T(R) \). Then \( w^{-1}(G^+) \) is called the semi-valuation monoid of \( w \).

Suppose that \( w \) and \( w' \) are equivalent semi-valuations of a ring \( R = T(R) \). Let \( M = w^{-1}(G^+) \), \( M' = (w')^{-1}(G^+) \), the respective semi-valuation monoids of \( w \) and \( w' \). Let \( x \in M \). Then \( w(x) \in G^+ \) implies \( \Phi w(x) = w'(x) \in G'^+ \). Thus, \( x \in M' \). Similarly, since \( \Phi \) is an order isomorphism, \( x \in M' \) implies \( x \in M \). Thus \( M = M' \). The converse is obvious; therefore, two semi-valuations are equivalent if and only if their semi-valuation monoids coincide.

**Proposition 11.5.** Let \( M \) be any subset of a ring \( R = T(R) \) satisfying P1 through P3. Then there exists a semi-valuation \( w \) of \( R \) having \( M \) as its semi-valuation monoid.

**Proof.** Define a pre-order of \( R^* \) by \( (R^*)^+ = M \), i.e., \( M \) satisfies \( 1 \in M \),
and $M \cdot M = \{ab : a, b \in M\} \subseteq M$. Let $U$ denote the multiplicative sub-
group of $R^*$ consisting of units of $M$. Then $R^*/U$ is an ordered group
with $M/U$ as the monoid of positive elements.

We claim that the natural map $w : R^* \rightarrow R^*/U$ is a semi-valuation.

Since $w$ is a monoid homomorphism, axiom (i) is satisfied. Also,
$-1 \in U \subseteq M$, and thus axiom (iii) is satisfied. Suppose that
$x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1} \in M$ for some $d \in R^*$.
We must show that $(x_1 + \ldots + x_n)^{-1} \in M$. Since $(\sum M) \cap R^* \subseteq M$, it suffices
to show that $x_1^{-1} + \ldots + x_n^{-1} \in R^*$. But $R^*$ is a group and hence
$x_1^{-1} + \ldots + x_n^{-1} \in R^*$, $d \in R^*$ imply $(x_1 + \ldots + x_n)^{-1} \in R^*$. Thus axiom (ii)
is satisfied.

**Lemma 11.6.** Let $M$ be a subset of $R = T(R)$ satisfying P1 through P3.
The set $D$ consisting of 0 and elements $x \in \sum M$ for each positive
integer $n$ forms a subring of $R$.

**Proof.** Let $x \in \sum M$, $y \in \sum M$. Then $x = \sum x_i$, $y = \sum y_i$, where $x_i, y_i$
$\in M$. Since $-1 \in M$, $-y_i \in M$ also. Then $x + \sum (-y_i) = x - y \in \sum M$.

Therefore, $x - y \in D$. $xy = x_1 y_1^{-1} + \ldots + x_n y_m$ is a sum of elements of $M$
since $x_i y_i \in M$ implies $x_i y_i \in M$ for each $i, j$. Thus $xy \in D$. Since
$1 \in D$ by P1, $D$ is a subring of $R$.

**Proposition 11.7.** P1 through P3 are necessary and sufficient conditions
for a subset $M$ of $R = T(R)$ to be contained in a subring $D$ of $R$ with
$M = D \cap R^*$. $M = D^*$ if and only if $R$ is $D$-torsion free.

**Proof.** Suppose that $M$ is a subset of $R$ satisfying P1 through P3,
and let $D$ be the subring of $R$ defined in the lemma. Clearly, $M \subseteq D^*$.
since $M \subseteq R^\ast$. On the other hand, if $x \in D \cap R^\ast$, then $x \in \bigcap_{n=1}^\infty M \subseteq M$, by P2, for some $n$. Hence $M = D \cap R^\ast$.

Conversely, if $D$ is a subring of $R$, then $M = D \cap R^\ast$ satisfies P1 through P3: since $D$ is a subring of $R$, $1$ and $-1 \in D^\ast \cap R^\ast$, $M \subseteq R^\ast$, and if $x \in \bigcap_{n=1}^\infty M$ for some $n$, then $x \in D$. Hence, if $x$ also belongs to $R^\ast$, then $x \in D \cap R^\ast = M$. Therefore, $\bigcap_{n=1}^\infty M \subseteq M$.

For the second assertion, assume that $M = D^\ast$. If there exists $x \in D, y \neq 0 \in R$ such that $xy = 0$, then $x \notin D^\ast$ since $D^\ast = M \subseteq R^\ast$.

Therefore, $x$ is a zero-divisor in $D$, and hence $R$ is $D$-torsion free.

Conversely, if $R$ is $D$-torsion free, then $M = D \cap R^\ast = D^\ast$.

Definition 11.8. Let $w$ be a semi-valuation of a ring $R = T(R)$. The subring $D$ of $R$ consisting of $0$ and all elements $x \in \bigcap_{n=1}^\infty w^{-1}(G^\ast)$ for each positive integer $n$ is called the semi-valuation ring of $w$.

Example 11.9. Let $R = Z(2) \bigoplus M$ be the ring defined in example 11.2. Then $Z(2)$ is a subring of $R$. $Z(2) \cap R^\ast \neq Z(2)^\ast$ since $2 \in Z(2)^\ast$, but $2$ (identified with $(2,0)$) does not satisfy P1 through P3. The map $w : R^\ast \rightarrow R^\ast/\mathbb{Z}(Z(2))$ is a semi-valuation, with $\{1\}$ as the sumbonoid of positive elements. Thus, $w^{-1}(\{1\})$ generates $Z(2)$, and $Z(2)$ is therefore the semi-valuation ring of $w$.

Given a subring $D$ of $R$ such that $D^\ast$ satisfies P1 through P3, $D$ need not be a semi-valuation ring, as the next example shows. Such a ring will always contain a semi-valuation ring, however; namely, the ring generated by $D^\ast$.

Example 11.10. Let $Q$ be the field of rational numbers, $X$ an indeterminate over $Q$, and $\{B_i\}$ the set of proper ideals of the polynomial ring $Q[X]$.
Let \( M = \bigoplus_i \mathbb{Q}[X]/B_i \). Then \( R = \mathbb{Q}[X] \oplus M \), the ring formed by the principle of idealization, is a total quotient ring and \( R^\ast = U(R) = \{(a,m) : a \in \mathbb{Q}^\ast \} \).

Let \( D \) be the subring \( Z_{(p)}[X] \oplus M \) of \( R \), where \( Z_{(p)} \) is the localization of the ring of integers \( Z \) at the prime ideal \( (p) \) of \( Z \). Then \( R = T(D) \), and therefore \( D^\ast = Z_{(p)} \oplus M \) satisfies P1 through P3.

The natural map \( R^\ast \to R^\ast /U(D) \) is a semi-valuation of \( R \). However, \( (X,0) \in D \) and does not belong to \( \sum_1^n w^{-1}(D^\ast /U(D)) \) for any \( n \). The semi-valuation ring of \( w \) is \( Z_{(p)} \oplus M \).

**Proposition 11.11.** Let \( D \) be a ring. Then \( D^\ast \) is the semi-valuation monoid of some semi-valuation \( w \) with semi-valuation ring \( D \) if and only if every zero-divisor of \( D \) is a sum of regular elements of \( D \).

**Proof.** Suppose that \( D^\ast \) is the semi-valuation monoid of a semi-valuation \( w \) of a ring \( R = T(R) \) with semi-valuation ring \( D \). Then \( D = 0 \cup \{x : x \in \bigoplus_1^n w^{-1}(G^+) \text{ for each positive integer } n \} \). Since \( D^\ast = w^{-1}(G^+) \), every element of \( D \) is a sum of regular elements of \( D \), and hence every zero-divisor is a sum of regular elements of \( D \).

Conversely, if every zero-divisor of \( D \) is a sum of regular elements of \( D \), let \( w \) be the semi-valuation of \( T(D) \) having semi-valuation monoid \( D \cap T(D)^\ast \). Since \( T(D) \) is \( D \)-torsion free, \( D \cap T(D)^\ast = D^\ast = w^{-1}(G^+) \), and thus it follows that \( D^\ast \) is the semi-valuation monoid of \( w \) with semi-valuation ring \( D \).

**Corollary 11.12.** Let \( R \) be a quasi-semi-local ring. Let \( M_1, \ldots, M_k \) be those maximal ideals of \( R \), if any, such that \( R/M_i \approx \mathbb{Z}/(2) \), the integers
modulo the prime ideal (2) of \( \mathbb{Z} \). Then \( R \) is a semi-valuation ring with semi-valuation monoid \( R^* \) if and only if for each \( j = 1, \ldots, k \) there exists an integer \( n(j) \) such that \( \bigcap_{i \neq j} (M_i \cap \sum_{i = 1}^{n(j)} R^*) \neq M_j \).

**Proof.** Suppose that \( R \) is a semi-valuation ring with semi-valuation monoid \( R^* \). Since the number of maximal ideals involved in finite, \( \bigcap_{i \neq j} M_i \neq M_j \). Since \( R \) is generated by \( R^* \), \( x \in \bigcap_{i \neq j} M_i \) implies that \( x \in \sum_{i \neq j} R \) for some \( n(j) \). Therefore, \( \bigcap_{i \neq j} (M_i \cap \sum_{i = 1}^{n(j)} R^*) \neq M_j \).

Conversely, suppose that \( \bigcap_{i \neq j} (M_j \cap \sum_{i = 1}^{n(j)} R^*) \neq M_j \). Let \( M_{k+1}, \ldots, M_k \) be the maximal ideals of \( R \) which are not isomorphic to \( \mathbb{Z}/(2) \). Let \( h : R \to R/M_1 \times \ldots \times R/M_n \) be the canonical map defined by \( h(x) = (h_1(x), \ldots, h_n(x)) \), where \( h_i : R \to R/M_i \) is the canonical map for each \( i = 1, \ldots, n \). We show first that every element of \( \bigcap_{i = 1}^{k} M_i \) is a sum of regular elements of \( R \). Let \( y \in \bigcap_{i = 1}^{k} M_i \). Let \( h_j(y) = y_j \). Since \( R/M_j \neq \mathbb{Z}/(2) \) for \( j > k \), there exist non-zero elements \( s_j, t_j \in R/M_j \) such that \( y_j = s_j - t_j \). Hence \( h(y) = (1, \ldots, 1, s_{k+1}, \ldots, s_n) \).

\((1, \ldots, 1, t_{k+1}, \ldots, t_n)\) is a sum of units of \( \prod_{i = 1}^{n} R/M_i \). There exists therefore, units \( x, z \in R \) such that \( h(x) = (1, \ldots, 1, s_{k+1}, \ldots, s_n) \), \( h(z) = (1, \ldots, 1, t_{k+1}, \ldots, t_n) \). Thus, \( h(y) = h(x) - h(z) \) implies \( y - x + z \in \bigcap_{i = 1}^{n} M_i \) (= Jacobson radical of \( R \)). \( y - x + z = m \in \text{Jacobson radical of } R \) implies that \( y = x - z + m \) is a sum of units of \( R \), since \( z \) is a unit implies that \( -z + m \) is a unit. Thus, any element of \( \bigcap_{i = 1}^{k} M_i \) is a sum of regular elements of \( R \).
Let $g : R \rightarrow R/M_1 \times \ldots \times R/M_k$ be the canonical map defined by $g(x)$

$= (g_1(x), \ldots, g_k(x))$, where $g_i : R \rightarrow R/M_i$, $i = 1, \ldots, k$. By assumption,

there exists $y_j \in \bigcap_{i \neq j} M_i$ such that $y_j \notin M_j$, and $y_j$ is a sum of regular

elements of $R$. $g(y_j) = (0, \ldots, 0, 1, 0, \ldots, 0)$ with 1 as the $j$th component

and zeros elsewhere. For any $x \in R$, $g_j(x)$ is either 0 or 1; therefore

g(x) is a finite sum of certain of the $g(y_j)$, say, $g(x) = g(y_1) + \ldots + g(y_k)$.

Then $g(x - y_1 - \ldots - y_k) = 0$ implies that $x - y_1 - \ldots - y_k \in \bigcap_{i=1}^{k} M_i$. Since the

$y_j$ are sums of regular elements of $R$ and every element $\in \bigcap_{i=1}^{k} M_i$ is a

sum of regular elements of $R$, then $x$ is also a sum of regular elements

of $R$.

**Corollary 11.13.** Assume that $R$ is a quasi-semi-local ring, and let

$J(R)$ denote the Jacobson radical of $R$. Then $R/J(R)$ is a semi-valuation

ring with semi-valuation monoid $(R/J(R))^\star$ if and only if $R/M \cong \mathbb{Z}/(2)$

for at most one maximal ideal $M$ of $R$.

Moreover, if $R/J(R)$ is a semi-valuation ring with semi-valuation

monoid $(R/J(R))^\star$, then $R$ is a semi-valuation ring with semi-valuation

monoid $R^\star$.

**Proof.** Let $M_1, \ldots, M_n$ denote the maximal ideals of $R$. Suppose that

$R/J(R)$ is a semi-valuation ring with semi-valuation monoid $(R/J(R))^\star$, and that $R/M_1 \approx R/M_2 \approx \mathbb{Z}/(2)$. The element $(1,0,\ldots,0)$ of $R/M_1 \times

R/M_2 \times \ldots \times R/M_n$ cannot be written as a sum of regular elements, since

$(r_{11}, \ldots, r_{n1}) + \ldots + (r_{1k}, \ldots, r_{nk}) = (1,0,\ldots,0)$ implies that $r_{12} + \ldots + r_{1k} = 1$

and hence the number of summands, $k$, is odd. On the other hand,

$r_{21} + \ldots + r_{2k} = 0$ implies that the number of summands, $k$, is even. Thus,

$R/J(R)$ is not a semi-valuation ring with semi-valuation monoid $(R/J(R))^\star$, contrary to our assumption.
Suppose that $R/M_j \cong \mathbb{Z}(2)$, $R/M_i \not\cong \mathbb{Z}(2)$, $i \neq 1$. Then, for any non-zero element $x_i$ of $R/M_i$, $i \neq 1$, we can find non-zero elements $s_i$, $t_i$, $u_i$, $v_i$, $w_i \in R/M_i$ such that $x_i = s_i - t_i$, $x_i = u_i + v_i + w_i$. Thus, if $(x_1, \ldots, x_n) \in R/J(R)$, we can write $(x_1, \ldots, x_n) = (1, s_1^i, \ldots, s_n^i) - (1, t_2, \ldots, t_n)$ if $x_1 = 0$; $(x_1, \ldots, x_n) = (1, u_2, \ldots, u_n) + (1, v_2, \ldots, v_n) + (1, w_2, \ldots, w_n)$ if $x_1 = 1$.

If $R/J(R)$ is a semi-valuation ring with semi-valuation monoid $(R/J(R))^\times$, then for any element $x$ of $R$, the image of $x$ in $R/J(R)$ under the canonical map is a sum of units of $R/J(R)$, since $R/J(R)$ is a total quotient ring for $R$ quasi-semi-local. It follows, then, that $x$ is a sum of units of $R$, since $U(R/J(R)) \cong U(R)/(1+J(R))$.

**Corollary 11.14.** The following are always semi-valuation rings $R$ of some semi-valuation $w$ of a ring $R \supseteq R$, with semi-valuation monoid $R^\times$.

a) Any quasi-local ring.


**Proof.** a) follows immediately from Corollary 11.13. Suppose that $P(X)$ is a zero-divisor of $A[X]$. Let $Q(X)$ be any regular element of $A[X]$. Then $B(X) = P(X) + Q(X)$ is a regular element of $A[X]$. Therefore, $P(X) = B(X) - Q(X)$ is a sum of regular elements of $A[X]$.

**Definition 11.15.** Let $w$ be a semi-valuation of a ring $R = T(R)$. $w$ is said to be an additive semi-valuation if

i) $w(x) < w(y)$ implies $w(x+y) = w(x)$, whenever $x$, $y$, $x + y \in R^\times$;

ii) whenever $x$, $r_i$, $x + y \in R^\times$, $y = r_1 + \ldots + r_k \notin R^\times$, $w(x) < w(r_i)$ for all $i = 1, \ldots, k$ implies $w(x + y) = w(x)$.

**Proposition 11.16.** Let $w$ be a semi-valuation of $R = T(R)$, with semi-valuation ring $D$ and semi-valuation monoid $D^\times$. Then $w$ is additive
if and only if the regular non-units of $D$ generate a proper ideal of $D$.

**Proof.** Suppose that the regular non-units of $D$ generate a proper ideal $P$ of $D$. Suppose $x, y, x+y \in R^*$ and $w(x) < w(y)$. Then $w(yx^{-1}) > 0$. Thus $yx^{-1} \in P$. $x, x+y \in R^*$ imply $(x+y)x^{-1} = 1 + yx^{-1} \in R^*$. Then $1 + yx^{-1}$ is a unit in $D$; otherwise, $1 + yx^{-1} \in P, yx^{-1} \in P$ imply that $1 \in P$. $1 + yx^{-1}$ is a unit implies that $w(1 + yx^{-1}) = w((x+y)x^{-1}) = w(x+y) - w(x) = 0$.

Let $w(x) < w(r_i)$ where $y = r_1 + \ldots + r_k$ is a zero-divisor of $R$; then $r_i x^{-1} \in P$, for each $i = 1, \ldots, k$, implies $(r_1 + \ldots + r_k)x^{-1} = yx^{-1} \in P$. Then $1 + yx^{-1}$ is a zero-divisor or a unit. If $1 + yx^{-1}$ is a unit, then $w(l+yx^{-1}) = w(x+y) - w(x) = 0$.

Suppose that $w$ is an additive semi-valuation. Let $x_i \in R$ such that $w(x_i) > 0$, $i = 1, \ldots, n$. If $r \in D$, then either $r$ is a zero-divisor and thus $rx$ is a zero-divisor, or $w(rx_i) = w(r) + w(x_i) > 0$. Suppose that $x_1 + \ldots + x_n \in D^*$. We will show by induction that $w(x_1 + \ldots + x_n) > 0$.

Suppose that $w(x_1 + x_2) = 0 < w(x_1)$. Then, since $w(x_1) = w(-x_1)$, $w(x_1 + x_2 - x_1) = w(x_2) = 0$, contrary to the assumption that $w(x_2) > 0$. Assume inductively that the assertion is true for a fixed integer $n > 2$.

Suppose that $w(x_1 + \ldots + x_{n+1}) = 0 < w(x_i)$, $i = 1, \ldots, n+1$. If $(x_2 + \ldots + x_{n+1})$ is regular, then $w(x_2 + \ldots + x_{n+1}) > 0$ by the inductive hypothesis. Therefore, $w(x_1 + (x_2 + \ldots + x_{n+1})) > 0$ by the $n = 2$ case. If $z = x_2 + \ldots + x_{n+1}$ is a zero-divisor, then $w(x_1 + \ldots + x_{n+1} - (x_2 + \ldots + x_{n+1})) = w(x_1) = w(x_1 + \ldots + x_{n+1}) = 0$ is a contradiction to $w(x_1) > 0$.

Therefore, $w(x_1 + \ldots + x_{n+1}) > 0$. 
Since any element of $D$ is a sum of regular elements of $D$, by
proposition 11.10 and the hypothesis, the proposition is proved. q.e.d.

We conclude this chapter with a few remarks concerning the semi-
value group of a semi-valuation. If $G$ is the semi-value group of a
semi-valuation $w$ of a ring $R = T(R)$, then $G$ is filtered if and only if
$R^* = T(D)^*$, where $D$ is the semi-value ring of $w$. Moreover, $G$ is
filtered if and only if for each $y \in R^*$, there exists $s \in D^*$ such that
$s \cdot y \in D^*$. Hence, $G$ is filtered if and only if $R^*$ is the group generated
by $D^*$.

With $R$ and $D$ as in the previous paragraph, if $R = T(D)$ and $G$ is
filtered, $G$ is called a group of divisibility. If $D$ is any ring, then
the ordered group $T(D)^*/U(D)$ is called the group of divisibility of $D$.

Finally, it is easily seen that if $v$ is a semi-valuation of
$R = T(R)$ with semi-value group $G$, and if $\beta$ is a $V$-homomorphism of $G$
on to an ordered group $G'$, then $\beta_v$ is also a semi-valuation of $R$, with
semi-value group $G'$. 
CHAPTER 11

COMPOSITE SEMI-VALUATIONS

In [13], the notion of a composite of two semi-valuations of fields is treated. As we remarked in the Introduction, the construction of this composite along with related theorems gives rise to a large class of groups which are groups of divisibility. We summarize this construction and the main results pertaining to it in the next paragraph.

Let $K$ be a field, $w$ a semi-valuation of $K$, and assume that the semi-valuation ring $R$ of $w$ is quasi-local, with maximal ideal $M$. Let $h : R \rightarrow R/M$ be the canonical homomorphism. Let $u$ be a semi-valuation of the residue field $R/M$, with semi-valuation ring $D$ of $u$. Let $v$ be the semi-valuation of $K$, determined up to equivalence, having semi-valuation ring $R' = h^{-1}(D)$. Then $v$ is said to be composite with $w$ and $u$. Denote by $A$, $B$, $C$, respectively, the semi-value groups of $u$, $v$, and $w$. Ohm proves that $B$ is a lexicographic extension of the semi-value groups $A$ and $C$; and, conversely, if $A \neq 0$, and $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$ is lexicographically exact, and if $B$ is the semi-value group of a semi-valuation $v$ of the field $K$ with ring $R'$ such that $\beta v$ is a semi-valuation, then i) the semi-valuation ring $R$ of $w$ is quasi-local with maximal ideal $M \subset R' \subset R$, and ii) $A$ is the semi-value group of a semi-valuation $u$ of $R/M$ [13].

In this chapter, we remove the restrictions that $K$ is a field and $R$ is quasi-local to obtain a suitable extension of the concept of a composite semi-valuation.
Let $J(R)$ denote the Jacobson radical (intersection of all maximal ideals of $R$) of a ring $R$.

Lemma III.1. Let $R$ be a ring and $I$ an ideal of $R$ contained in $J(R)$. Then the mapping $e + I \rightarrow e(1 + I)$ describes a group isomorphism from $U(R/I)$ onto $U(R)/(I+I)$.

Proof. $I \subseteq J(R)$ implies that $1 + I \subseteq U(R)$. Let $h$ be the canonical homomorphism from $R$ onto $R/I$, and let $h'$ be the restriction of $h$ to $U(R)$. Then $h'$ is a homomorphism from the multiplicative group $U(R)$ to the multiplicative group $U(R/I)$. If $h(x) \in U(R/I)$, then there exists $h(x')$ such that $h(x)h(x') = 1$, or $xx' - 1 \in I$. Hence $xx' - 1 \in 1 + I \subseteq U(R)$, and thus $x \in U(R)$. Thus $h'$ is surjective. Clearly, $1 + I \subseteq \ker h'$. Suppose that $h'(x) = 1$. Then $h(x-1) = 0$ implies that $x - 1 \in I$, or $x \in 1 + I$. Thus $\ker h' \subseteq 1 + I$. $1 + I = \ker h'$ implies that $1 + I$ is a subgroup of $U(R)$. Therefore, we have the canonical map $U(R) \twoheadrightarrow U(R)/(I+I)$ given by $e \mapsto e(1+I)$. The commutativity of the diagram

$$
\begin{array}{ccc}
U(R) & \overset{h'}{\longrightarrow} & U(R/I) \\
\downarrow{g} & & \downarrow{g'} \\
U(R)/(1+I) & & 
\end{array}
$$

gives us the isomorphism $g' : e + I \mapsto e(1+I)$. q.e.d.

An ideal $I$ of a ring $R$ is said to be regular if $I$ contains at least one regular element of $R$.

Lemma III.2. Let $I$ be an ideal contained in the intersection of all regular maximal ideals of a ring $R$. In each of the following cases,
the mapping \( e + 1 \rightarrow e \cdot (1 + 1) \) \( R^* \) describes a group isomorphism from \( U(R/I) \) onto \( U(R)/(1 + 1) \cap R^* \):

i) Every maximal ideal of \( R \) is regular.

ii) \( R \) has only finitely many non-regular maximal ideals (in particular, \( R \) is quasi-semi-local.) and \( I \) contains a regular element.

Proof. i) If every maximal ideal of \( R \) is regular, then the intersection of all regular maximal ideals is \( J(R) \). Hence i) is a direct consequence of Lemma III.1.

ii) Let \( M_1, \ldots, M_n \) be the non-regular maximal ideals of \( R \). If

\[
\bigcap_{i=1}^{n} M_i + 1 \subseteq M,
\]

where \( M \) is a maximal ideal of \( R \), then

\[
\bigcap_{i=1}^{n} M_i \subseteq M
\]

implies that \( M_j \subseteq M \) for some \( j \). Since the \( M_j \) are maximal, this implies \( M_j = M \). But since \( I \) has a regular element, \( M \) must be regular, a contradiction to the assumption that the \( M_j \) are non-regular. Hence

\[
\bigcap_{i=1}^{n} M_i + 1 = R.
\]

Then the canonical homomorphism \( h : R \rightarrow R/\bigcap_{i=1}^{n} M_i \times R/I \)

is surjective, \( R/\bigcap_{i=1}^{n} M_i \times R/I \approx U(R) \), and

\[
U(R/(\bigcap_{i=1}^{n} M_i) \cap I) \approx U(R/\bigcap_{i=1}^{n} M_i) \times U(R/I).
\]

Since

\[
(\bigcap_{i=1}^{n} M_i) \cap I \subseteq (\bigcap_{i=1}^{n} M_i) \cap (\bigcap_{\alpha} M_\alpha) = J(R),
\]

where the \( M_\alpha \) are the maximal ideals of \( R \) that are regular, the mapping

\[
U(R) \xrightarrow{h^1} U(R/(\bigcap_{i=1}^{n} M_i) \cap I)
\]

is surjective by Lemma III.1. Then the composite map

\[
U(R) \xrightarrow{h^1} U(R/(\bigcap_{i=1}^{n} M_i) \cap I) \approx U(R/\bigcap_{i=1}^{n} M_i) \times U(R/I) \rightarrow U(R/I),
\]

where \( p \) is the projection map, is surjective.

\[
(1 + 1) \cap R^* \subseteq U(R); \text{ otherwise, if } m \in I \text{ and } (1+m) \in R^* , \text{ then}
\]
1 + m ∈ M for some regular maximal ideal M implies l ∈ M, since m lies in every regular maximal ideal. \((1+1) \cap R^*\) is clearly contained in \(\ker(p \circ h')\). If \(p \circ h'(x) = 1\), then \(x \in 1+1\). Thus, since \(x\) also belongs to \(U(R)\), \(x \in (1+1) \cap R^*\). The commutativity of the diagram

\[
\begin{array}{ccc}
U(R) & \xrightarrow{\pi \circ h'} & U(R/1) \\
g & \downarrow & \downarrow g' \\
U(R)/(1+1) \cap R^* & & \\
\end{array}
\]

gives us the desired isomorphism \(g'\).

**Lemma 11.3.** Let \(I\) be a common ideal of the rings \(R \subseteq R'\), and suppose that \(I \subseteq \) the intersection of all regular maximal ideals of \(R'\). Then

\[\text{(U(R)+I) \cap (R')^*} \subseteq U(R).\]

**Proof.** Let \(t \in U(R)\), \(y \in I\) such that \(t+y \in (R')^*\). Since \(t+y \in (R')^*\), \(t+y \in U(R')\) because \(y\) belongs to every regular maximal ideal of \(R'\) and \(t \in U(R) \subseteq U(R')\). \(\frac{1}{t+y} = \frac{1}{t} - \frac{y}{t(t+y)} \in U(R)+I\), since \(t(t+y) \in U(R')\) and \(y \in I\), an ideal of \(R'\). Thus, \(\frac{1}{t+y} \in R\), since \(I \subseteq R\). Hence \(t+y \in U(R)\). q.e.d.

For the remainder of this chapter, we fix the following notation.

Let \(w\) be a semi-valuation of the ring \(R = T(R)\) with semi-valuation ring \(R_w\). Let \(I\) be an ideal of \(R_w\) contained in the intersection of all regular maximal ideals of \(R_w\). Let \(h\) be the canonical homomorphism of \(R_w\) onto \(R_w/I\), and let \(h'\) be the restriction of \(h\) to \(U(R_w)\). Assume that \(h' : U(R_w) \rightarrow U(R_w/I)\) is surjective and \(R_w/I = T(R_w/I)\).

Let \(u\) be a semi-valuation of \(R_w/I\), with semi-valuation ring \(R_u\) and let \(R_v = h^{-1}(R_u)\). Let \(v\) be the semi-valuation of \(R = T(R)\),
determined up to equivalence, by the ring $R_v$ (i.e., $v$ is the semi-valuation of $R$ with semi-valuation monoid $R_v \cap R^*$; the existence of $v$ is given by proposition 11.2.). Let $A_u$, $B_v$, and $C_w$ denote the semi-value groups of $u$, $v$, and $w$, respectively. Let $P = w(1 \cap R^*) \cup 0$, and let $(C_w)_P$ denote the group $C_w$ with $P$ as its monoid of positive elements.

**Lemma 11.4.** $U(R_v) = h^{-1}(U(R_u)) \cap R_w^*$.

**Proof.** It is clear that $U(R_v) \subseteq h^{-1}(U(R_u)) \cap R_w^*$. Suppose that $x \in h^{-1}(U(R_u)) \cap R_w^*$. Since $h$ is onto, there exists $x' \in R_w^*$ such that $xx' \in (1+1) \cap R_w^* \subseteq U(R_v)$. Then $h(x') = \frac{1}{h(x)} \in U(R_u)$. Thus, $x' \in h^{-1}(U(R_u)) \subseteq R_v$. Therefore, $x \in U(R_v)$.

**Theorem 11.5.** Let $R_w$ be the semi-valuation ring of a semi-valuation $w$ of a ring $R = T(R)$. Let $I$ be an ideal contained in the intersection of all regular maximal ideals of $R_w$ and such that $R_w/I = T(R_w/I)$.

Assume that the canonical map $h : R_w \rightarrow R_w/I$ maps $U(R_w)$ onto $U(R_w/I)$.

Let $u$ be a semi-valuation of $R_w/I$ with semi-valuation ring $R_u$, and let $R_v = h^{-1}(R_u)$. Let $v$ be the semi-valuation of $R = T(R)$, determined up to equivalence, by the ring $R_v$. Denote by $A_u$, $B_v$, and $C_w$, respectively, the semi-value groups of $u$, $v$, and $w$, and let $P = w(1 \cap R^*) \cup 0$. Then

a) there exist homomorphisms $\alpha$, $\beta$ which complete the commutative diagram D below and which make the bottom row L exact;

**Diagram D**

$$
\begin{array}{c}
\begin{array}{c}
U(R_w) \xrightarrow{i} T(R)^* \\
\downarrow{uh'} \quad \quad \downarrow{v}
\end{array}
\end{array}
$$

$L$: $0 \rightarrow A_u \xrightarrow{\alpha} B_v \xrightarrow{\beta} (C_w)_P \rightarrow 0$.

($i$ is the inclusion homomorphism.)
b) Let $M^+ = \text{the semi-valuation monoid of } v$ and $M = \text{the semi-valuation monoid of } u$. Then the following equivalent conditions hold:

1. $B_v^+ \ni \{b \in B_v : b \in \alpha(A_u^+) \text{ or } \beta(b) > 0\}$;
2. $M^+ \ni [h^{-1}(M \cup 0)] \cap R^*$.

(c) The following are equivalent:

1. The sequence $L$ is lexicographically exact;
2. $M^+ = [h^{-1}(M \cup 0)] \cap R^*$;
3. $h^{-1}[((N/I) \cap R_u) \subseteq z(R) \cup I$, where $z(R)$ denotes the zero-divisors of $R$, for every regular maximal ideal $N$ of $R_w$.

d) Assume that $M^+ = R_u^*$ and $M = R_u^*$. Then, if $R_u$ is a domain, $L$ is lexicographically exact; if $z(R_v) \subseteq I$ and $L$ is lexicographically exact, $R_u$ is a domain.

Proof. a) $U(R_w) = \ker w \supseteq \ker v = U(R_v)$ since $R_v \subseteq R_w$ implies $U(R_v) \subseteq U(R_w)$; thus $\beta$ is defined canonically and is a surjection since $w$ is a surjection. Since $h'$ is assumed to be surjective, the composite $uh'$ is a surjection. $\ker (uh') = h^{-1}(U(R_u)) \cap R_w^* = U(R_v)$ by Lemma III.4, and $\ker (\alpha v) = U(R_w) \cap U(R_v) = U(R_v)$, since $R_v$ is a subring of $R_w$. Therefore, $\alpha$ is defined canonically and is an injection.

b) We show first that (1) holds. Let $b \in B_v$ such that $b \in \alpha(A_u^+)$ or $\beta(b) > 0$. In the first case, since $uh'$ is surjective, there exists $x \in U(R_w)$ such that $\alpha uh'(x) = b$. Therefore, $uh'(x) \in A_u^+$. Thus $h'(x) \in R_u$. Since $h^{-1}(R_u) = R_v$, this implies that $x \in R_v$. Thus, $v(x) = b \in B_v^*$. In the second case, there exists $x \in T(R_v)^*$ such that $w(x) = \beta(b) > 0$. Thus, $x \in 1 \cap R_v^* \subseteq R_v$; thus $b = v(x) \in B_v^*$. 

(1) $\Rightarrow$ (2): Let $x \in [h^{-1}(M \cup 0)] \cap R^*$. $h(x) = 0$ implies $x \in 1 \cap R^*$. Then $w(x) = \beta(b) > 0$ implies $b \in B_v^*$ by (1). Hence $x \in M^+$. If
h(x) ∈ M, then h(x) ∈ U(R_w/1) since M ⊆ (R_w/1)^* = U(R_w/1). Since I
is contained in every regular maximal ideal and x ∈ R^*_w (hence also
x ∈ R^*_w), we must have x ∈ U(R_w). Then uh'(x) = 0 implies ωuh'(x) = 0.
Thus by (1), ωuh'(x) ∈ B_v^+ and hence x ∈ M'.

(2) ⇒ (1): Let b ∈ B_v such that b ∈ α(A_u^+) or β(b) > 0. Let
x ∈ R^*_w = T(R)^*_w such that v(x) = b. If β(b) = w(x) > 0, then x ∈ I ∩ R^*_w.
Hence h(x) = 0, and therefore x ∈ h^{-1}(0) ∩ R^*_w ⊆ M' by (2). Therefore
v(x) = b ∈ B_v^+. If b ∈ α(A_u^+), then αuh'(x) = v(x) = b, h'(x) ∈ M,
and thus x ∈ h^{-1}(M) ∩ R^*_w ⊆ M' by (2). Therefore, x ∈ B_v^+.

c) (1) ⇒ (2): Suppose that L is lexicographically exact. Let x ∈ M'.
By the lexicographic exactness of L, v(x) = b ∈ α(A_u^+) or βv(x) =
β(b) > 0. In the second case x ∈ I ∩ R^*_w. Hence h(x) = 0, and
x ∈ h^{-1}(0) ∩ R^*_w. In the first case, βv(x) = 0, so x ∈ U(R_w).
Then αuh'(x) = v(x) = b ∈ α(A_u^+) implies uh'(x) > 0, and thus h'(x) ∈ M.
Thus x ∈ h^{-1}(M) ∩ R^*_w since M' ⊆ R^*_w (by definition of a semi-valuation
monoid). Thus, in either case, M' ⊆ [h^{-1}(M ∪ 0)] ∩ R^*_w. Equality
follows from b). Thus, (1) ⇒ (2).

(2) ⇒ (1): Now assume that [h^{-1}(M ∪ 0)] ∩ R^*_w = M'. Let b ∈ B_v^+.
Choose x ∈ T(R)^*_w such that v(x) = b. Then x ∈ M'. Hence h(x) = 0 or
h(x) ∈ M. If h(x) = 0, then x ∈ I ∩ R^*_w. Therefore, w(x) = βv(x) =
β(b) > 0. If h(x) ∈ M, then h(x) ∈ U(R_w/1), since M ⊆ U(R_w/1).
Since x ∈ R^*_w ∩ R_w ⊆ R^*_w and I is contained in every regular maximal
ideal of R_w, we must have x ∈ U(R_w) (because h(x) is a unit of R_w/1).
Thus uh'(x) > 0 implies h'(x) ∈ A_u^+. Therefore αuh'(x) = v(x) = b
implies b ∈ α(A_u^+). Hence, B_v^+ ⊆ {b ∈ B_v : b ∈ α(A_u^+) or β(b) > 0}.
Equality now follows from b). Thus, (2) ⇒ (1).
(2) $\Rightarrow$ (3): Let $x \in h^{-1}[(N/I) \cap R_{\pm}]$. Then $x \in R_{\pm} = h^{-1}(R_{\pm})$. If $x \in R_{\pm}^*$, then $x \in R_{\pm} \cap R_{\pm}^*$ implies $x \in M'$, and thus by (2), $x \in h^{-1}(M \cup 0)$. Hence $h(x) = 0$ or $h(x) \in M = R_{\pm} \cap (R_{\pm}/I)^*$. On the other hand, $x \in h^{-1}[(N/I) \cap R_{\pm}]$ implies $h(x)$ is a zero-divisor of $R_{\pm}/I$ (since $R_{\pm}/I = T(R_{\pm}/I)$) or $h(x) = 0$. Thus, $x \notin R_{\pm}^* \sim (1 \cap R_{\pm}^*)$. Since $R = T(R)$, this implies $x \in z(R) \cup I$.

Hence, (2) $\Rightarrow$ (3).

(3) $\Rightarrow$ (2): Suppose $h^{-1}[(N/I) \cap R_{\pm}] \subseteq z(R) \cup I$. Let $x \in M'$. If $h(x) \neq 0$, $h(x) \notin R_{\pm} \cap (R_{\pm}/I)^*$, then $h(x) \in N/I$ for some maximal ideal $N/I$ of $R_{\pm}/I$.

But then $x \in z(R)$, a contradiction, since $M' \subseteq R_{\pm}^*$. Thus, $h(x) = 0$ or $h(x) \in R_{\pm} \cap (R_{\pm}/I)^*$, i.e., $x \in h^{-1}(M \cup 0) \cap R_{\pm}^*$. Hence, (3) $\Rightarrow$ (2).

d) Suppose that $M' = R_{\pm}^*$, $M = R_{\pm}^*$ and that $R_{\pm}$ is a domain. Then $R_{\pm}^* = R_{\pm} \sim 0$. Suppose $x \in M' = R_{\pm}^*$. Since $R_{\pm} = h^{-1}(R_{\pm})$, $h(x) = 0$ or $h(x) \in R_{\pm}^* = M$. Hence $x \in [h^{-1}(M \cup 0)] \cap R_{\pm}^*$ since $R_{\pm}^* = M' \subseteq R_{\pm}^*$.

Suppose that $z(R_{\pm}) \subseteq I$ and $L$ is lexicographically exact. If $x'$ is a zero-divisor of $R_{\pm}$, then $x' \in z(R_{\pm}/I)$. If $x$ is any preimage of $x'$, then $x \notin M' = R_{\pm}^*$ by the lexicographic exactness [c)(2)]. Thus, $x \in z(R_{\pm})$.

By hypothesis, $z(R_{\pm}) \subseteq I$. Thus $h(x) = x' = 0$. Therefore, $R_{\pm}$ is a domain.

**Corollary III.6.** Let $C_{\pm}$ be the group of divisibility of a ring $R_{\pm}$ such that $I \subseteq$ intersection of all regular maximal ideals of $R_{\pm}$, $R_{\pm}/I = T(R_{\pm}/I)$, and such that the canonical map $h : R_{\pm} \rightarrow R_{\pm}/I$ maps $U(R_{\pm})$ onto $U(R_{\pm}/I)$. Let $P = \theta(R_{\pm}^* \cap I) \cup 0$. Let $A_{\pm}$ be the semi-value group of a semi-valuation $u$ of $R_{\pm}$ with semi-valuation ring $R_{\pm}$, such that $h^{-1}[(N/I) \cap R_{\pm}] \subseteq z(R) \cup I$ for every regular maximal ideal $N$ of $R_{\pm}$.

If $C_{\pm}$ is free, then $A_{\pm} \oplus (C_{\pm})_P$ is a group of divisibility.

**Proof.** Let $R_{\pm} = h^{-1}(R_{\pm})$, and let $B_{\pm}$ be the semi-value group of a semi-valuation $v$ of $R$ determined, up to equivalence, by the ring $R_{\pm}$. Then, by...
Theorem 111.5(a), there exist homomorphisms \( \alpha, \beta \) such that the sequence

\[ 0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0 \]

is exact.

By Theorem 111.5(c), \( h^{-1}[(N/I) \cap R_u] \leq z(R) \cup I \) for every regular maximal ideal \( N \) of \( R_w \) implies that the sequence \((\alpha, \beta)\) is lexicographically exact.

Since \( C_w \) is free, the sequence splits. A lexicographically exact sequence splits lexicographically when it splits. Hence \( B \approx A \bigoplus (C_w) \).

In [10], Marot generalizes the notions of valuation rings, valuations, and unique factorization (factorial) domains to rings with zero-divisors.

By ([10], Theorem 4.5.1) the rings having groups of divisibility order isomorphic to the ordered direct sum of copies of \( Z \) are exactly the unique factorization rings, and by ([10], Proposition 3.6) the rings having group of divisibility order isomorphic to \( Z \) are those rings \( R \) having a unique regular maximal ideal \( M \) generated by the prime element \( \pi \) of \( R \); in the latter case, every regular ideal is a principal ideal \( M^n \). As in the case for domains, \( R \) is then called a discrete valuation ring.

The requirement that the ideal \( I \) of \( R_w \) in Corollary 111.6 be contained in the intersection of all regular maximal ideals is justifiable: for example, the ordered direct product of a finite number \( n \geq 2 \) of copies of \( Z \) can only be the group of divisibility of the intersection of a finite number \( n \geq 2 \) of discrete valuation rings. Suppose, for example, that \( P \) is a submonoid of \((Z \times Z)^+\) such that \((Z \times Z)_P^+\) is filtered. Suppose that there exist \( k_1, k_2, \in P \) such that \( k_2 - k_1, k_1 - k_2 \notin (Z \times Z)^+\), and \( d = \inf_{Z \times Z}[k_1, k_2] \) implies \( k_1 - d, k_2 - d \in P \). By Corollary IV.9, if \((P \sim 0) + (Z \times Z)^+ \subseteq P \), then the identity homomorphism \( i : (Z \times Z)_P^+ \to Z \times Z \) is a \( V \)-homomorphism. For such a \( P, w^{-1}(P \sim 0) \) is never a proper ideal of \( R_w^* \), where \( R_w^* \) is a ring having group of divisibility order isomorphic to \( Z \times Z \) and \( w : T(R_w^*)^* \to Z \times Z \) is the
associated semi-valuation. It follows, then, from Theorem III.13, that if $A_u \neq 0$, then $A_u \bigoplus (Z \times Z)_p$ is never a group of divisibility.

An example to which Corollary III.6 applies is any discrete valuation ring $R_w$ containing a regular ideal $I$ such that the canonical homomorphism $h : R_w \to R_w/I$ maps $U(R_w)$ onto $U(R_w/I)$. Let $M = R_w I$ be the unique regular maximal ideal of $R_w$. Then $w(R_w I \cap R_w^\times) = \{j \in \mathbb{Z}^+ : j \equiv n \text{ for some fixed integer } n \leq 1\}$. Let $P = w(R_w I \cap R_w^\times) \cup 0$. By Corollary III.6, if $A_u$ is the semi-value group of a semi-valuation $u$ of $R_w / R_w I$ with ring $R_u$ such that $h^{-1}[(M/I) \cap R_u] \leq z(R_w) \cup I$, where $I = R_w I^n$, then $A_u \bigoplus Z_p$ is a group of divisibility.

The requirement that $h^{-1}[(M/I) \cap R_u] \leq z(R) \cup I$ for every regular maximal ideal $N$ of $R_w \leq R = T(R)$ is essential, as the following example shows.

**Example III.7.** Let $P = \{ j \in \mathbb{Z}^+ ; j \equiv n \text{ for some integer } n > 1\} \cup 0$, a sub-monoid of $\mathbb{Z}^+$. Suppose that $A_u \bigoplus Z_p$ is a group of divisibility. The sequence $0 \to A_u \xrightarrow{i} A_u \bigoplus Z_p \xrightarrow{p} Z_p \to 0$, where $i$ and $p$ are the usual injection and projection maps, respectively, is lexicographically exact. By Theorem IV.7, $p : A_u \bigoplus Z_p \to Z$ is a $V$-homomorphism. Let $v$ be the semi-valuation of a ring $R = T(R)$ with semi-value group $A_u \bigoplus Z_p$. Then $pv = w$ is a semi-valuation of $R$ with semi-value group $Z$. The semi-valuation ring $R_w$ of $w$ has a unique regular maximal ideal generated by a prime element $\pi$ of $R_w$, such that $w(\pi) = 1$. Then $w^{-1}(\pi \sim 0) = (R_w I^n) \cap R_w^\times$. Let $h : R_w \to R_w / R_w I^n$ be the canonical homomorphism and assume that $h$ maps $U(R_w)$ onto $U(R_w / R_w I^n)$.

By Theorem III.13, there exists a semi-valuation $u$ of $R_w / R_w I^n$ with semi-value group $A_u$ such that diagram $D$ of Theorem III.5 is valid. Let $R_u$ be the semi-valuation ring of $u$. Suppose that $A_u$ is filtered, and suppose
that there exist $x', y' \in R_u$ such that $x'y' = 0$. Let $x, y$ be preimages of $x', y'$, respectively. Then, by Theorem III.5 c)(3), $x, y \in z(R) \cap R_v = z(R_v)$.

On the other hand, we also have $x, y \in R_w$. Write $x = a\pi^j, y = b\pi^j$, where $a, b \notin R_w$. Since $x, y \in z(R_v)$ and $\pi \in R_w^{\ast}$, we have that $a, b \in z(R_w)$. Since $a, b \notin M$, $h(a), h(b) \in U(R_w/R_w^n)$. Because $h'$, the restriction of $h$ to $U(R_w)$, is onto, there exist $t_a, t_b \in U(R_w)$ such that $h(a) = h(t_a), h(b) = h(t_b)$, or $a = t_a + m, b = t_a + m'$, for some $m, m' \in R_w^n$. Thus, $x = t_a\pi^j + m\pi^j, y = t_b\pi^j + m'\pi^j$ and since $R_w^n \subset R_v$, we conclude that $t_a\pi^j, t_b\pi^j \in R_v$. Then, $v(t_a\pi^j) = w(t_a\pi^j) = j$ implies $v(t_a\pi^j) = (d, j) > 0$. But the lexicographic ordering of $A_u \bigoplus Z_p$ implies that $j \geq n$ or $j = 0$ and $d \geq 0$. If $j = 0$, then $x = a \in R\pi$, contrary to assumption. Therefore, $j \geq n$, i.e., $x \in R\pi^n$. Hence $h(x) = x'^{\pi} = 0$. Thus, $R_u$ is a domain. A filtered implies that $T(R_u)^{\ast} = (R_w/R_w^n)^{\ast}$, and since $T(R_u)$ is a field, this implies that $T(R_u) = R_w/R_w^n(1+R_w^n) \cap R_w^{\ast}$, $T(R_u) = U(R_w)/(1+R_w^n) \cap R_w^{\ast}$, by assumption; for $n \neq 1$, $(a+\pi)n^\ast \notin T(R_u)^{\ast}$). Hence, $n = 1$, contrary to the initial hypothesis that $P \neq Z^+$. Thus, we conclude that if $A_u$ is filtered and $h' : U(R_w) \to U(R_w/I)$ is onto, then $A_u \bigoplus Z_p$ is not a group of divisibility for $P \neq Z^+$, $P = \{j \in Z^+ : j = n \geq 1\} \cup \theta$.

In particular, $0 \bigoplus Z_p = Z_p, P = \{j \in Z^+ : j = n \geq 1\} \cup \theta$ is not the group of divisibility of any ring $R_v$ such that $T(R_v) = T(R_w)$, where $R_w$ is a discrete valuation ring and the canonical map $h : R_w \to R_w/R_w^n$ maps $U(R_w)$ onto $U(R_w/R_w^n)$. Thus, $Z_p$ is not the group of divisibility of a domain. (In Chapter V, we determine all the submonoids $P$ of $Z^+$ such that $Z_p$ is filtered. There we prove a proposition from which it follows that for any such $P \neq Z^+$, $Z_p$ is never a group of divisibility of a domain.)
The next example provides us with a group of divisibility of a ring with zero-divisors which is not a group of divisibility of a domain.

Example III.8. Let \( R \) be the subring of the field of rational numbers consisting of all elements \( \frac{a}{2^n}, a, n \in \mathbb{Z} \). Let \( R' = R[i/2] = \{a+bi/2 : a, b \in R, i = \sqrt{-1} \} \). Let \( a+bi/2 \in R' \). We may assume that \( a, b \in \mathbb{Z} \).

Suppose that \( b \neq 0 \). Then, if \( a+bi/2 \in \text{U}(R') \), \( (a+bi/2)^{-1} = \frac{a+bi/2}{a^2+2b^2} \).

Thus, if \( a+bi/2 \in \text{U}(R') \), then \( a^2 + 2b^2 = 2^n \), for some \( n \in \mathbb{Z} \). Write \( a = 2^m r, b = 2^j s \), where \( r \) and \( s \) are odd. Then \( a^2 + 2b^2 = 2^{2m} r^2 + 2^{2j+1} s^2 \). Suppose \( 2m < 2j + 1 \) (Equality clearly cannot hold). Then \( a^2 + 2b^2 = 2^{2m} (r^2 + 2^{2j+1-2m} s^2) \). But \( r \) odd, \( 2j + 1 \neq 2m \) imply that \( r^2 + 2^{2j+1-2m} s^2 \) is odd. Hence \( a^2 + 2b^2 \neq 2^n \) unless \( r^2 + 2^{2j+1-2m} s^2 = 0 \), and, since \( b \neq 0 \), then \( s \neq 0 \); thus \( s^2 \geq 1 \), and hence \( r^2 = 0 \). We reach a similar conclusion in case \( 2m > 2j + 1 \).

Thus, if \( a+bi/2 \in \text{U}(R') \), then \( a = 0, b = \pm 2^j \). Conversely, since \( 2^n \in \text{U}(R) \) for all \( n \), \( \pm 2^n i/2 \) is invertible in \( R' \) for all \( n \). Thus \( \text{U}(R') \) is generated by \( i/2 \).

Let \( \{B_i\} = \) the set of proper ideals of \( R' \), \( M = \bigoplus_i R'/B_i \). Let \( D = R' \bigoplus M \), the ring formed by the principle of idealization. Then \( \text{U}(D) = \{(a,m): a \in \text{U}(R')\} \). The subring \( D_1 = Z[i/2] \bigoplus M = \{(a+bi/2, m): a, b \in Z, m \in M\} \) of \( D \) has \((\pm 1, m)\) as its only units, since \( \pm 2^n \) is not invertible in \( Z \) for \( n \neq 0 \), and from the fact that \( \{(\pm 2^n i/2, m): n \in Z\} = \text{U}(D) \supseteq \text{U}(Z[i/2] \bigoplus M) \). The isomorphism \( \text{U}(D)/\text{U}(D_1) \rightarrow Z \) described by \((i/2)^n \cdot \text{U}(D_1) \rightarrow n \) is clearly an order isomorphism onto \( Z \), since the regular elements of \( D_1 \) are the elements \((i/2)^n, m\), \( n \geq 0 \). Similarly, the subring \( D_2 = Z[2i/2] \bigoplus M \) of
D has \((\pm 1, m)\) as its only units, and the elements \(((i/2)^n, m), n = 0\) or \(n \geq 2\) as regular elements. Thus \(((i/2)^n - n)\) describes an order isomorphism from \(U(D)/U(D_2)\) onto \(Z_p, P = \{0, 2, 3, 4, \ldots\}\), i.e., \(Z_p\) is, up to order isomorphism, the group of divisibility of \(D_2\). By Example III.7, \(Z_p\) is not the group of divisibility of a domain. We note that the canonical map \(h: D_1 \rightarrow D_1/((i/2)H)^2\) does not map \(U(D_1)\) onto \(U(D_1/((i/2)H)^2)\); for example, \(h(1 + i/2)\) is a unit, but has no preimage in \(U(D_1)\).

Corollary III.6 is particularly applicable whenever \(R_w\) is a quasi-semi-local domain, for in this case, if \(I\) is any ideal of \(R_w\), then the restriction \(h^I\) of the canonical map \(h: R_w \rightarrow R_w/I\) to \(U(R_w)\) is onto \(U(R_w/I)\), and if, furthermore, \(I \subseteq J(R_w)\), then \(R_w/I = T(R_w/I)\). Then, if \(u\) is any semi-valuation of \(R_w/I\) such that the semi-valuation ring \(R_u\) of \(u\) is a domain, and if the group of divisibility \(C_w\) of \(R_w\) is free, then by Corollary III.6, \(A_u \oplus (C_w)_p\) is a group of divisibility, where \(A_u\) is the semi-value group of \(u\) and \(P = w(1 \cap R_w^*) \cup 0\).

In Corollary III.10 below, we apply Theorem III.5 and Corollary III.6 to obtain the groups of divisibility of subrings of the integral closure of \(Z_p\) containing \(Z_{p(p)}\) in a quadratic extension of the field of rational numbers. Unless otherwise stated, the notation \(A \times B\) will be used to indicate the direct product of groups, and the product ordering will not be assumed. \(A \times B\) is to be considered as an ordered group, however, whenever the ordering is explicitly stated. Corollary III.10 is a consequence of the following more general Corollary III.9.

(References preceded by the letter A refer the reader to the Appendix.)
**Corollary III.9.** Let $R$ be a discrete rank one valuation domain with principal maximal ideal $R_p$ and quotient field $K$. Let $R'$ be the integral closure of $R$ in a finite extension $L$ of $K$, and let $w$ be a semi-valuation of $L$ having ring $R'$ and semi-value group $C$. Then there exists a semi-valuation of $R'/R'p^n$ with semi-value group $A_n$ and homomorphisms $\beta_n : A_n \times C \to A_{n-1} \times C$ such that

$$(A_n \times C)^+ = \{(a, c+w(p^{n-1})) : c > 0; (a, w(p^{n-j-1})) : a \in \ker(\beta_2 \cdots \beta_n); j = 0, 1, \ldots, n-2; (0,0)\}$$

and $A_n \times C$ is the group of divisibility of the ring $R + R'p^n$.

**Proof.** Let $R$ be a discrete rank one valuation ring with maximal ideal generated by a prime element $p$ of $R$. Let $K$ be the quotient field of $R$ and let $R'$ be the integral closure of $R$ in a finite extension $L$ of $K$. By A.11, the field $R/(p)$ can be identified with a subfield $k$ of $R'/R'p$ by the mapping $a + (p) \to a + R'p$.

Let $u_1$ be a semi-valuation of $R'/R'p$ determined, up to equivalence, by the field $k$. Let $h$ be the canonical map from $R'$ onto $R'/R'p$, and let $R_1 = h^{-1}(k)$. Denote the semi-value group of $u_1$ by $A_1$, and let $B_1$ be the semi-value group of a semi-valuation $v_1$ of $L$ having ring $R_1$. Let $C$ be the semi-value group of a semi-valuation $w$ of $L$ having ring $R'$. By A.12, $C$ is order isomorphic to the totally ordered group of integers $Z$ or to the ordered direct product of $\leq 2$ copies of $Z$. Hence $C$ is free. By Corollary III.6, $B_1 = A_1 \bigoplus C$ is a group of divisibility. Since the semi-valuation ring $k$ of $u$ is a field, $A_1^+ = 0$. By the lexicographic ordering of $A_1 \bigoplus C$, then $R_1$ is a local ring with maximal ideal $R'p$. Moreover, by the commutativity of the diagram.
\[ R' \xrightarrow{h} R'/R'_p \]
\[ R \xrightarrow{} R/(p) \]

\((A.11)\),

\[ R \leq h^{-1}(k). \] Thus \(R + R'_p \leq R'_1\). On the other hand, \((R+R'_p)/R'_p \cong R/R \cap R'_p\) by \(A.11\), and \(R \cap R'_p = R_p\). Hence, \(R/R \cap R'_p = k\), and therefore, \(h^{-1}(k) = R + R'_p\). Thus, \(R_1 = R + R'_p\).

Assume the following inductively;

i) \(B_n\) is a semi-value group of a semi-valuation of \((R+R'_p)^{n-1}/(R'+R'_p)^{n}\) with semi-valuation ring \((R+R'_p^n)/(R'+R'_p^n)\);

ii) \(A_n\) is a semi-value group of a semi-valuation of \(R'/R'_p^n\) with semi-valuation ring \((R+R'_p^n)/R'_p^n\);

iii) There exist homomorphisms \(\alpha_n, \beta_n\) such that \(0 \to B_n \xrightarrow{\alpha_n} A_n \times C \xrightarrow{\beta_n} A_{n-1}\) and \(A_n \times C \to 0\) is lexicographically exact;

\[(A_n \times C)^+ = \{(a, c+w(p^{n-1})) \mid c > 0; (0,0); (a, w(p^{n-j-1})) \mid a \in \ker(\beta_{2+j}, \ldots, \beta_{n-2})\}.

Let \(B_{n+1}\) be the semi-value group of a semi-valuation of \((R+R'_p^n)/(R'+R'_p^{n+1})\) with ring \((R+R'_p^n)/(R'+R'_p^{n+1})\). Let \(h:\)

\[ R + R'_p^n \to (R+R'_p^n)/(R'+R'_p^{n+1}) \] be the canonical homomorphism. Then

\[ h^{-1} [(R+R'_p^n)/(R'+R'_p^{n+1})] = R + R'_p^{n+1}. \] Let \(B_{n+1}'\) be the semi-value group of a semi-valuation of \(L\) having ring \(R+R'_p^{n+1}\). By Theorem 11.5, there exist homomorphisms \(\alpha_{n+1}, \beta_{n+1}\) such that the sequence

\[ 0 \to B_{n+1}' \xrightarrow{B_{n+1}'} B_{n+1} \xrightarrow{\beta_{n+1}} (A_n \times C)^{n+1}(R'_p^n \asymp 0) \cup \{0\} \to 0 \] is lexicographically exact. Let \(A_{n+1}\) be the semi-value group of a semi-valuation of \(R'/R'_p^{n+1}\) with ring \(R + R'_p^{n+1}\). By Theorem 11.5, there
exist homomorphisms $\alpha^i_{n+1}$, $\beta^i_{n+1}$ such that the sequence $0 \to A^i_{n+1} \xrightarrow{\alpha^i_{n+1}} B^i_{n+1} \xrightarrow{\beta^i_{n+1}} C \to 0$ is exact. Since $C$ is free, the sequence splits.

From the inductive hypothesis,

$$(A_n \times C)^+ = \{(a, c + w(p^{n-1})), c > 0; (0,0); (a, w(p^{n-j-1})),$$
$$a \in \ker(\beta_{2+j} \ldots \beta_n), j = 0, 1, \ldots, n-2 \}$$

Therefore,

$$v_n(R_n p) = \{(a, c + w(p^n)), c > 0; (0, w(p)); (a, w(p^{n-j})), a \in \ker(\beta_{2+j} \ldots \beta_n),$$
$$j = 0, 1, \ldots, n-2\}$$

Hence, we conclude from the lexicographic ordering of $(\alpha^i_{n+1}, \beta^i_{n+1})$ that

$$(A^i_{n+1} \times C)^+ = \{(a, c \times w(p^n)), c > 0; (0,0); (a, w(p^{n-j})),$$
$$a \in \ker(\beta_{2+j} \ldots \beta_n, \beta_{n+1}), j = 0, 1, \ldots, n-1\}.$$ 

**Corollary III.10.** Let $Z(p)$ denote the localization of the ring of integers $Z$ at the prime ideal $(p)$ of $Z$, and let $R_1'$ denote the integral closure of $Z(p)$ in a quadratic extension of the field of rational numbers. Then, the following are groups of divisibility of subrings $D$ of $R_1'$ containing $Z(p)$.

1) If $D = Z(p) + R_1'p^n$, and $R_1'p \equiv P$, where $P$ is the only maximal ideal of $R_1'$ lying over $(p)$, then

$G = Z/(p^{n-1}) \oplus Z$, (lexicographic sum), $p \equiv 2, n \equiv 1; G = Z/(p^{n-1}) \times Z/(p^{n+1}) \times Z$, $p \equiv 3, n \equiv 2$, with

$G^+ = \{(\tilde{a}, \tilde{b}, c); c \equiv n; (0,0,0); (\tilde{a}, 0, n-j-1), \text{ where} \}
\tilde{a} \in (p^j)/(p^{n-1}), j = 0, 1, \ldots, n-2 \};$

$G = Z/(2^{n-2}) \times Z/(2) \times Z/(3) \times Z$, $p = 2, n \equiv 2$, with

$G^+ = \{\tilde{a}, \tilde{b}, \tilde{c}, d); d \equiv n; (0,0,0,0); (\tilde{a}, \tilde{b}, 0, n-1);$ \n$(\tilde{a}, 0, 0, n-j-1), \text{ where} \tilde{a} \in (2^j)/(2^{n-1}), j = 1, \ldots, n-2 \}.$
2) If \( D = Z_{(p)} + R'p^n \), and \( R'p = P^2 \), where \( P \) is the only maximal ideal of \( R' \) lying over \((p)\), then

\[
G = Z/(p_{-1}) \bigoplus Z_\cdot, p \equiv 2, n = 1, S = \{0, 2, 3, \ldots\} \subset Z^+ ;
\]

\[
G = Z/(p^n) \times Z, p \equiv 3 \text{ or } p = 2 \text{ and } P = R'\pi \text{ where } \pi^2 \in Z, n \equiv 2, \text{ with}
\]

\[
G^+ = \{(\bar{a}, b): b \equiv 2n; (0, 0); (\bar{a}, 2(n-j-1)), \text{ where } \bar{a} \in (p^{j+1})/(p^n), j = 0, 1, \ldots, n-2\} ;
\]

\[
G = Z/(2^{n-1}) \times Z/(2) \times Z, p = 2 \text{ and } P = R'\pi \text{ where}
\]

\[
\pi^2 \in Z, n \equiv 2, \text{ with}
\]

\[
G^+ = \{(\bar{a}, b, c, d): c \equiv 2n; (0, 0, 0); (\bar{a}, 0, 2(n-j-1)), \text{ where } \bar{a} \in (2^j)/(2^{n-1}), j = 0, 1, \ldots, n-2\} .
\]

3) If \( D = Z_{(p)} + R'p^n \) and \( R'p = P_1P_2 \), where \( P_1 \) and \( P_2 \) are the maximal ideals of \( R' \) lying over \((p)\), then

\[
G = Z/(p_{-1}) \bigoplus (Zxz)_\cdot, p \equiv 3, n = 1, S = \{(a,b)\in(Zxz)^+ \text{ such that}
\]

\[
a, b \equiv 1 \text{ or } a = b = 0\} ;
\]

\[
G = (Zxz)_\cdot, p = 2, n = 1, S = \{(a,b): a,b \equiv 1 \text{ or } (0,0)\} ;
\]

\[
G = Z/(p^n) \times Z/(p_{-1}) \times (Zxz), p \equiv 3, n \equiv 2, \text{ with}
\]

\[
G^+ = \{(\bar{a}, b, c, d): c, d \equiv n; (0,0,0,0); (\bar{a},0,n-j-1,n-j-1), \text{ where } \bar{a} \in (p^j)/(p^{n-1}),
\]

\[
j = 0, 1, \ldots, n-2\} ;
\]

\[
G = Z/(2^{n-2}) \times Z/(2) \times (Zxz), p = 2, n \equiv 2, \text{ with}
\]

\[
G^+ = \{(\bar{a}, \bar{b}, c, d): c, d \equiv n; (0,0,0,0); (a,b,n-1,n-1), (\bar{a},0,n-j-1,n-j-1),
\]

\[
\text{where } \bar{a} \in (2^{j-1})/(2^{n-2}), j=1,\ldots,n-2\} .
\]

**Proof.** By A.12, there exists a subring of \( R' \) of the form \( Z_{(p)} + R'p^n \) for each prime \( p \) and for each integer \( n \equiv 1 \), in each of the cases 1), 2) and 3) above, and these are all of the subrings of \( R' \) containing
$Z(p)$. Hence it suffices to determine, up to order isomorphism, the groups $A_n$ of Corollary III.9. Then $\ker(\beta_{Z+j}...B_n)$ is easily determined for each $j = 0, 1, \ldots, n-2$.

By A.11, $(Z(p) + R^1p^n)/R^1p^n \approx Z(p)/(R^1p^n \cap Z(p)) = Z(p)/(p^n) \approx Z/(p^n)$.

Thus, by A.7,

$[(Z(p) + R^1p^n)/R^1p^n]^\times \approx [Z/(p^n)]^\times \approx Z/(p-1) \times Z/(p^{n-1})$, if $p \leq 3$;

$Z/(2^{n-2}) \times Z/(2)$, if $p = 2$ and $n \leq 2$; $\{0\}$, if $p = 2$ and $n = 1$.

$A_n = (R^1/R^1p^n)^\times /U[(Z(p) + R^1p^n)/R^1p^n]$.

Thus, it follows from A.13 and A.7 that $A_n \approx Z/(p+1) \times Z/(p^{n-1})$, if $p \leq 3$, $R^1p = P$;

$Z/(3)$, if $p = 2$, $n = 1$, $R^1p = P$;

$Z/(2^{n-2}) \times Z/(2) \times Z/(3)$, if $p = 2$, $n \geq 2$, $R^1p = P$;

$Z/(p^n)$, if $R^1p = P^2$, $p \geq 3$ or $p = 2$ and

$P = R^1\pi$ with $\pi^2 \in Z(p)$;

$Z/(2^{n-1}) \times Z/(2)$, if $p = 2$, and $R^1p = P^2$ and

$P = R^1\pi$ with $\pi^2 \in Z(p)$;

$Z/(p-1) \times Z/(p^{n-1})$, if $p \leq 3$, $R^1p = P_1P_2$;

$Z/(2^{n-2}) \times Z/(2)$, if $p = 2$, $n \leq 2$, $R^1p = P_1P_2$; $\{0\}$, if $p = 2$, $n = 1$, $R^1p = P_1P_2$.

By A.12, the group of divisibility of $Z(p)$ is of index one in the group of divisibility of $R^1$ in case $R^1p = P$, and is of index two in case $R^1p = P^2$. If $R^1p = P_1P_2$,

then the group of divisibility of $R^1$ is the ordered direct product of two copies of the totally ordered group of integers and the index of the group of divisibility of $Z(p)$ in each copy is one. Hence, if $w$ is the semivaluation of $T(R^1)$ onto the group of divisibility of $R^1$, we have that $w(p) = 1$, if $R^1p = P$; $w(p) = 2$, if $R^1p = P^2$; $w(p) = (1, 1)$, if $R^1p = P_1P_2$. The result now follows from Corollary III.9.
Proposition III.11. Let $K$ be a field, and let $v, w$ be semi-valuations of $K$ with respective semi-value groups $B_v$ and $C_w$. Let $R_v$ be the ring of $v$. If $0 \to A \to B_v \cdot C_w \to 0$ is a lexicographically exact sequence of semi-value groups, then the sequence splits if and only if there exists a set $M = \{x \in K : v(x) = c \in C_w, \text{ such that } w(x) = c \}$ and $(x_c \cdot x_d) / x_{c+d} \in U(R_v)$. ([13], Proposition 3.4, page 582.)

Corollary III.12. Let $A_u$ be any semi-value group of a semi-valuation $u$ of a field $k$. Let $C$ be a totally ordered group, and let $P = \{c \in C : c = c_1 + \ldots + c_n, \text{ for a fixed integer } n \geq 1; c_i > 0\} \cup 0$. Then, $\bigoplus_{i \in I} (\bigoplus_{(k, +)}) \oplus C_p$ is a group of divisibility, where the cardinality of $I = \text{cardinality of } (C^+ \sim P)$ and $(k, +)$ denotes the additive group of the field $k$.

Proof. Let $\mathcal{A}_k(C)$ be the group algebra of $C$ over $k$ with quotient field $K$. By Krull's Theorem (A.3), there exists a valuation $w$ of $K$ with valuation ring $R = k + M$, where $M$ is the maximal ideal of $R$. Then $k = (k+M^n)/M^n \leq R/M^n$.

Let $u$ be a semi-valuation of $k$ with ring $D$. Then, by A.1,

$$[(k+M^n)/M^n] / U(D) \cong (k+M)/U(D+M^n) \cong k^* / U(D) \times (1+M)/(1+M^n).$$

Let $c \in w(M^n \sim 0)$ and choose $x \in K^*$ such that $w(x) = c$. Then $x \in M^n$ implies $x = \sum_{i=1}^r x_{i1} \ldots x_{in}$, where $x_{ij} \in M_i$. Then $w(x) \geq \inf_{x_{i1} \ldots x_{in}} \{w(x_{i1}) \ldots w(x_{in})\}$. Since $C$ is totally ordered, we may assume that $w(x_{i1} \ldots x_{in}) \leq w(x_{i2} \ldots x_{in}) \ldots w(x_{ir} \ldots x_{in})$. Then $w(x) = w(x_{i1} \ldots x_{in})$ implies $x = t x_{i1} \ldots x_{in}$, where $t \in R$. Hence $w(x) = w(t x_{i1}) + w(x_{i2}) + \ldots + w(x_{in})$. Since $w(x_{ij}) > 0$, $w(x) \in P$. Now let $c \in P \sim 0 \cdot c = c_1 + \ldots + c_n$, where $c_i > 0$. Let $x_i \in K^*$ such that $w(x_i) = c_i$. Then $c \in w(M^n \sim 0)$. Hence $w(M^n \sim 0) = P \sim 0$. 


Let \( A_u \) be the semi-value group of the semi-valuation \( u \). Then \( A_u \cong k^*/U(D) \). By A.6, \((1+M)/(1+M^n) \cong \bigoplus_{i=1}^{l} (k^+,\cdot)\), where \( l \) = cardinality of \((\mathbb{C}^+ \sim \mathbb{P})\). Let \( u' \) be the semi-valuation of \( R/M^n \) with semi-valuation ring \( D \). Then the semi-value group \( A_{u'} \) of \( u' \) is order isomorphic to \( A_u \oplus \bigoplus_{i=1}^{l} (k^+,\cdot) \), by A.1, where \((k^+,\cdot)^+ = \{0\}\). Let \( h : R \to R/M^n \) be the canonical homomorphism and let \( R_v = h^{-1}(D) \). Let \( v \) be the semi-valuation of \( K \) determined, up to equivalence, by the ring \( R_v \), and let \( B \) be the semi-value group of \( v \). By Theorem III.5, there exist homomorphisms \( \alpha, \beta \) such that the sequence \( 0 \to A_u \oplus \bigoplus_{i=1}^{l} (k^+,\cdot) \alpha B \xrightarrow{\beta} \mathbb{C}_p^+ \to 0 \) is lexicographically exact. Since \( w(x_c) = c \) for each generator \( x_c \) of the algebra \( \mathcal{A}_k \), the \( x_c \) trivially satisfy the conditions of Proposition II.11. Hence, the sequence \((\alpha,\beta)\) splits, and therefore splits lexicographically.

**Example III.13.** Let \( C \) be the lexicographic sum of the totally ordered group of integers \( \mathbb{Z} \) and a totally ordered divisible group \( G \) (By [6], Theorem 4, the latter is isomorphic (group) to copies of the additive group of the rationals.). Let \( (a,b) \in C \) such that \( (a,b) > 0, b \in G^+ \sim 0 \).

Then, for each integer \( n \neq 0 \), there exists \( h \in G \) such that \( nh = b \) (definition of divisible group). Thus, \( (a,b) \in nC^+ = \{c \in C : c = c_1 + \ldots + c_n, c_i > 0\} \) for all \( n \neq 0 \) . For \( n > 1 \), \((n-1,0) \in C^+, (n-1,0) \notin nC^+ \). Thus, cardinality \( C^+ \sim (nC^+ \cup \{0\}) = n - 1 \). By Corollary III.12, if \( A_u \) is a semi-value group of a field \( k \), then \( \left[ A_u \bigoplus \bigoplus_{i=1}^{n-1} (k^+,\cdot) \right] \bigoplus \mathbb{C}_p, P = nC^+ \cup \{0\} \), is a group of divisibility. In particular, if \( k \) is a finite field \( \mathbb{F}(p^m) \), then by A.10, the only subrings of \( k \) are subfields \( \mathbb{F}(p^r) \) where \( r \) divides \( m \). Hence, if \( q = (p^m - 1)/(p^n - 1) \), then \( \left[ \mathbb{Z}/(q) \bigoplus \bigoplus_{i=1}^{n-1} \mathbb{Z}/(p) \right] \bigoplus \mathbb{C}_p \) is a group of divisibility.
More generally, if $C$ is the lexicographic sum of a totally ordered free abelian group $G_1$ and a totally ordered divisible group $G_2$, then $[A_u \bigoplus (\bigoplus_{k \in \{0, 1\}} (k,+))] \bigoplus (G_1 \bigoplus G_2)_p$ is a group of divisibility, where $P = nC^+ \cup \{0\}$, and cardinality of $1 = \text{cardinality of } (G_1^+ \sim (nG^+ \cup 0))$, and $A_u$ is a semi-value group of a semi-valuation of the field $k$.

Example III.14. Let $C = \mathbb{Z}$, the group of integers with the usual total order; $n\mathbb{Z}^+ = \{j \in \mathbb{Z}^+ : j \equiv n \text{ for a fixed integer } n \geq 1\}$. Let $P = n\mathbb{Z}^+ \cup \{0\}$. Then, cardinality of $(\mathbb{Z}^+ \sim P) = n - 1$. By Corollary III.12, if $A_u$ is the semi-value group of a semi-valuation of a field $k$, then $[A_u \bigoplus (\bigoplus_{k \in \{0, 1\}} (k,+))] \bigoplus \mathbb{Z}_p$ is a group of divisibility. In particular, if $k$ is a finite field $GF(p^m)$, then, as we have noted in Example III.13, for $q = (p^m-1)/(p^n-1)$ where $r$ divides $m$, $[\mathbb{Z}/(q) \bigoplus (\bigoplus_{k \in \{0, 1\}} \mathbb{Z}/(p))] \bigoplus \mathbb{Z}_p$ is a group of divisibility for each integer $n \geq 1$.

In Theorem III.5, the submonoid $P$ of $C_w$ was assumed to be $w(1 \cap R^\times) \cup \{0\}$ where $w$ was the semi-valuation of the ring $R = T(R)$ with semi-value group $C_w$, and $I$ was a proper ideal of $R_w$. Thus, we were assured that $w^{-1}(P-0)$ generated a proper ideal of $R_w$. Theorem III.15 below gives somewhat of a converse situation to Theorem III.5.

Theorem III.15. Suppose that the sequence $0 \rightarrow A_u \xrightarrow{\alpha} B_v \xrightarrow{\beta} (C_w)_p \rightarrow 0$ is lexicographically exact, $(P-0) + C_w^+ \subseteq P$, and $v$ is a semi-valuation of a ring $R = T(R)$ with semi-value group $B_v$ and semi-valuation ring $R_v$. Suppose that $w = \beta v: B_v \rightarrow C_w$ is a semi-valuation of $R$ with semi-value group $C_w$ and semi-valuation ring $R_w$. Then, i) if $A_u \neq 0$, $w^{-1}(P-0)$ generates a proper ideal $I$ of $R_w$; $I \subseteq R_v \subseteq R_w$.

ii) Assume that $R_w/I = T(R_w/I)$, that the canonical map $h : R_w \rightarrow R_w/I$. 


maps $U(R_w)$ onto $U(R_w/l)$, and that $l \subseteq$ the intersection of all regular maximal ideals of $R_w$. Then there exists a semi-valuation $u$ of $R_w/l$ having semi-value group $A_u$ and for which the commutative diagram $D$ of Theorem III.5 is valid.

Proof. i) Suppose that $x_1, x_2, \ldots, x_n, x_1 + \ldots + x_n \in R$ and $w(x_i) \in P \sim 0$, $i = 1, \ldots, n$. Since $P \subseteq C_w^+$ and $w$ is a semi-valuation, $w(x_1 + \ldots + x_n) \subseteq 0$. Suppose that $w(x_1 + \ldots + x_n) = 0$. Then $v(x_1 + \ldots + x_n) \in \alpha(A_u)$. If $A_u \neq 0$, there exists a $\neq 0$ in $A_u$; thus $a' = \alpha(a) + v(x_1 + \ldots + x_n) \in \alpha(A_u)$. However, $v(x_i) \subseteq a'$, since $\beta(v(x_i) - a') = \beta v(x_i) = w(x_i) \in P \sim 0$ implies $v(x_i) - a' \subseteq 0$ by the lexicographic ordering. Since $v$ is a semi-valuation, we therefore have $v(x_1 + \ldots + x_n) \subseteq a'$, or, $v(x_1 + \ldots + x_n) - a' = -\alpha(a) \subseteq 0$, contrary to the assumption that $a \neq 0$. Thus $w(x_1 + \ldots + x_n) > 0$.

Since $R_w$ is a semi-valuation ring, by Definition 11.8, $R_w$ consists of $0$ and all elements $x \in \bigoplus_{m=1}^{\infty} w^{-1}(C_w^+)$ for each integer $m \geq 1$. Also, $(P \sim 0) + C_w^+ \subseteq P$ implies that for any $r \in w^{-1}(C_w^+)$, $x \in w^{-1}(P \sim 0)$, we have $rx \in w^{-1}(P \sim 0)$. Then, since $1$ is generated by $w^{-1}(P \sim 0)$ and $r \in R_w$ implies $r = 0$ or $r \in \bigoplus_{m=1}^{\infty} w^{-1}(C_w^+)$ for some $m \geq 1$, we have that $R_w \leq l$. Hence, we conclude that $w^{-1}(P \sim 0)$ generates a proper ideal of $R_w$. That $l \subseteq R_v \subseteq R_w$ follows from the lexicographic ordering of the sequence $(\alpha, \beta)$ and the definition of a semi-valuation ring.

ii) Let $h$ denote the canonical homomorphism of $R_w$ onto $R_w/l$. Let $h'$ be the restriction of $h$ to $U(R_w)$; $h' : U(R_w) \to U(R_w/l)$. Define the homomorphism $'uh''$ of diagram $D$ of Theorem III.5 to be the map $\alpha^{-1} v$. Since $v$ is a semi-valuation, then $'uh''$ also satisfied the axioms for a semi-valuation. Now define the homomorphism $u$ of
onto \( A_u \) by the equation \("uh" = uh'\). \( u \) is well-defined since \( \ker h' = (1+1) \cap R_w^\times \subseteq U(R_v) = \ker "uh" \). \( u \) is a semi-valuation since \( h' \) preserves addition and \"uh" satisfies the axioms for a semi-valuation.
CHAPTER IV
V-HOMOMORPHISMS AND LEXICOGRAPHICALLY
EXACT SEQUENCES

In the converse situation of the previous chapter (Theorem 111.15) we assumed that the sequence $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} (C_w)_p \rightarrow 0$ was lexicographically exact, that $B_v$ was the semi-value group of a semi-valuation $v$ of a ring $R = T(R)$, and that $\beta_v$ was a semi-valuation of $R = T(R)$ with semi-value group $C_w$. This is always the case if $\beta : B_v \rightarrow C_w$ is a $V$-homomorphism.

Thus, we investigate necessary and sufficient conditions for the homomorphism $\beta : B_v \rightarrow C_w$ to be a $V$-homomorphism, where $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} (C_w)_p \rightarrow 0$ is the sequence $L$ of Diagram D (Theorem 111.5(a)).

The following example shows that if $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C_p \rightarrow 0$ is lexicographically exact and $\beta : B \rightarrow C_p$ is a $V$-homomorphism, then $\beta : B \rightarrow C$ is not necessarily a $V$-homomorphism.

Example IV.1. Let $Z$ be the ordered group of integers with the usual total order. Then $P = \{k \in Z^+ : k \geq 3 \text{ or } k = 0\}$ and $P' = \{k \in Z^+ : k \geq 2 \text{ or } k = 0\}$ are submonoids of $Z^+$ with $P \subseteq P'$. The sequence $0 \rightarrow 0 \xrightarrow{\alpha} Z_p \xrightarrow{\beta} Z_p \rightarrow 0$, where $\beta$ is the identity map, is clearly lexicographically exact and $\beta$ is a $V$-homomorphism. However, $Z_p \xrightarrow{\beta} Z_p$, is not a $V$-homomorphism: $4 \geq \inf_{Z_p} \{3,5\}$, but $4 \neq \inf_{Z_p} \{3,5\} = 3$.

Let $P$ be a submonoid of $C^+$ such that $(P \sim 0) + C^+ \subseteq P$ and assume that $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C_p \rightarrow 0$ is lexicographically exact. To avoid ambiguity, whenever we include elements of $P$ and of $C^+$ in the same discussion, we shall write $c \geq_p 0$ for $c \in P$ and continue to write $c \geq 0$ for $c \in C^+$. 

45
We consider the following properties:

Pr 1: For $b_1, b_2 \in B$, $b < b_2$ for all $b < b_1$ implies $\beta(b_2) \geq \alpha(b_1)$.

Pr 2: For $c_1, c_2 \in C$, $c \not\preceq c_2$ whenever $c \not\preceq c_1$ implies $c_2 \geq c_1$.

**Lemma IV.2.** Let $P$ be a submonoid of $C^+$ such that $(P \sim 0) + C^+ \preceq P$ and assume that $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C_p \to 0$ is lexicographically exact. Then Pr 2 implies Pr 1.

**Proof.** Suppose that Pr 2 holds and assume that for $b_1, b_2 \in B$, $b < b_2$ for all $b < b_1$. Then, for all $b < b_1$ with $\alpha(b) \not\preceq \beta(b_1)$, we must have $\beta(b) \not\preceq \beta(b_2)$. Suppose that $\beta(b) = \beta(b_2)$. Then $\beta(b_2) \not\preceq \beta(b_1)$ implies $b_2 < b_1$ by the lexicographic exactness of $(\alpha, \beta)$.

But $b < b_2$ for all $b < b_1$ implies $b_2 < b_2$, a contradiction. Therefore, $\beta(b) \not\preceq \beta(b_2)$.

For any $d' \not\preceq \beta(b_1)$, choose a preimage $d$ such that $\alpha(d) = d'$. Then $d < b_1$. Hence, $\beta(d) < \beta(b_2)$. $\beta(d) = d' \not\preceq \beta(b_2)$ for all $d' \not\preceq \beta(b_1)$ implies, by Pr 2, that $\beta(b_1) \preceq \beta(b_2)$. q.e.d.

The following example shows that the converse of Lemma IV.2 is false.

**Example IV.3.** (Pr 1 does not imply Pr 2).

Let $Z$ be the ordered group of integers with the usual total order. Let $P = \{k \in Z^+ : k = 2n, n \in Z^+\}$, $P' = \{k \in Z^+ : k \geq 3 \text{ or } k = 0\}$, $P'' = \{k \in Z^+ : k \geq 2 \text{ or } k = 0\}$. $P' \subset P''$. The following sequence is lexicographically exact, where $\alpha, \beta$ are the usual injection and projection maps, respectively:

$$0 \to Z_p \xrightarrow{\alpha} Z_p \bigoplus (Z_p)_{p_1} \xrightarrow{\beta} (Z_p)_{p_1} \\ \to 0.$$  

We show first that Pr 1 holds, that is, if $(c, c') < (m_2, n_2)$ for all
Suppose that $\beta(m_1, n_1) = n_1 \not\leq \beta(m_2, n_2) = n_2$.

Then $n_2 - n_1 = +1$, or $n_2 - n_1 = -1$. But $(m_1 - 2k, n_1), k = 1, 2, \ldots$, implies $(m_1 - 2k, n_1) < (m_2, n_2)$ by our assumption that $(c, c') < (m_2, n_2)$ for all $(c, c') < (m_1, n_1)$. Thus, $(m_2 + 2k - m_1, \pm 1) > 0$, a contradiction to the lexicographic ordering of $(\alpha, \beta)$.

Therefore, $n_1 = \beta(m_1, n_1) \leq \beta(m_2, n_2) = n_2$, and thus Pr 1 is satisfied.

On the other hand, $k \not\leq 4$ for all $k \not\leq 3$, but $3 \not\leq 4$ since $1 \not\leq 4$. Hence Pr 2 is not satisfied. q.e.d.

However, we have the following.

**Lemma IV.4.** If $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C_\beta \rightarrow 0$ is lexicographically exact and $A^+ = 0$, then Pr 1 is equivalent to Pr 2.

**Proof.** By Lemma IV.2 we need only show that Pr 1 implies Pr 2 if $A^+ = 0$. Suppose that Pr 1 does not imply Pr 2. Choose $c_1', c_2' \in C$ such that $c_1' \not\leq c_2'$ for all $c_1' \not\leq c_1'$, and $c_1' \not\leq c_2'$. Let $c_1, c_2$ be preimages of $c_1', c_2'$, respectively. Then, there exists $c < c_1$ such that $c \not\leq c_2$; otherwise, Pr 1 would imply that $R(c_1) = c_1' = \beta(c_2) = c_2'$, contrary to our assumption that $c_1' \not\leq c_2'$. For any such $c$, however, we must have $R(c) = \beta(c_1)$ because if $R(c) \not\leq R(c_1)$, then by our assumption that $c_1' \not\leq c_2' = \beta(c_2)$ for all $c_1' \not\leq c_1' = \beta(c_1)$, we have that $R(c) \not\leq \beta(c_2)$, and hence $c < c_2$ by the lexicographic ordering of $(\alpha, \beta)$. Therefore, $c_1 - c \in \alpha(A)$. $c_1 - c \in \alpha(A)$ and $c_1 - c > 0$ imply that $c_1 - c \in \alpha(A) \cap B^+ = \alpha(A^+)$. Therefore, $A^+ \neq 0$. q.e.d.

Lemma IV.4 applies in particular whenever $A = \{0\}$ or $A$ is a torsion group.
Lemma IV.5. Suppose that $0 \rightarrow A \overset{\alpha}{\rightarrow} B \overset{\beta}{\rightarrow} C_p \rightarrow 0$ is lexicographically exact and that $(P \sim 0) + C^+ \leq P$. If Pr 2 is satisfied, then
$
\beta : B \rightarrow C$ is a $V$-homomorphism.

Proof. Let $b_0 \leq \inf_B \{b_1, \ldots, b_n\}$. Suppose $d' \leq \beta(b_1), \ldots, \beta(b_n)$ and choose a preimage $d$ of $d'$ in $B$. For any $c' \in C$ such that
$c' \leq d' = \beta(d)$, we have $\beta(c) \leq \beta(d)$ for any preimage $c$ of $c'$.

Thus, $\beta(b_i - c) = \beta(b_i - d) + B(d-c) \in (C^+) + (P \sim 0) \leq P \sim 0$.

Therefore, $b_i - c > 0$, by the lexicographic ordering of $(\alpha, \beta)$.

Since this is true for any preimage of $c'$, $b_i \leq c+a$ for all $a \in \alpha(A)$.

$b_0 \leq \inf_B \{b_1, \ldots, b_n\}$ implies $b_0 \leq c+a$ for all $a \in \alpha(A)$.

If $\beta(b_0) = \beta(c+a) = \beta(c)$, then $b_0 - c - a \in \alpha(A)$. Therefore, $b_0 \leq c + (b_0 - c - a)$ for all $a \in \alpha(A)$, and hence $0 \leq a$ for all $a \in \alpha(A)$.

This implies that $A = 0$.

Assume momentarily that $A = 0$ and $\beta(b_0) = \beta(c)$. Then $b_0 = c$.

Thus, $\beta(b_0) \leq \beta(d) \leq \beta(b_i)$ implies that $b_i - b_0 = 0$, $i = 1, \ldots, n$.

If $b_i = b_0$ for some $i$, then $\beta(b_i) = \beta(b_0) = \beta(d)$.

Suppose, then, that $b_i - b_0 > 0$ for all $i = 1, \ldots, n$. Then, for all $i$ and each $j = 1, \ldots, n$, $(b_i + d) + (b_j - b_0) \leq 0$. This implies that for each $j = 1, \ldots, n$, $b_0 \leq d - b_j + b_0$, and thus $d \leq b_j$. For each $j = 1, \ldots, n$ and $b_0 \leq \inf_B \{b_1, \ldots, b_n\}$ imply that $b_0 \leq d$. Hence $\beta(b_0) \leq \beta(d)$. Thus, if $A = 0$ and $\beta(b_0) = \beta(c) = c'$ for some $c' < d'$, then $\beta$ is a $V$-homomorphism. If $A = 0$ and $\beta(b_0) \neq \beta(c)$ for all $\beta(c) = c' < d'$, then $c' = \beta(c) \leq \beta(b_0)$ for all $c' \leq d' = \beta(d)$ implies, by Pr 2, that $\beta(d) \leq \alpha(b_0)$, i.e., $\beta$ is a $V$-homomorphism.
Assume now that $A \neq 0$. Then $\beta(b'_0) \neq \beta(c) = c'$ for all $c' < d'$, for we have seen that $\beta(b'_0) = \beta(c) = c'$ for some $c' < d'$ leads to $A = 0$. Thus, $\beta(b'_0) \nless \beta(c)$. $c' = \alpha(c) \nleq \beta(b'_0)$ for all $c' = \alpha(c) \nleq \beta(d)$ implies, by applying Pr 2 again, that $\beta(d) \leq \beta(b'_0)$. Hence $\beta$ is a $V$-homomorphism.

**Lemma IV.6.** Let $\beta : B \to C$ be any $V$-homomorphism. Then, if $\beta$ is not an order isomorphism, $\beta$ satisfies Pr 1.

**Proof.** Suppose that $c < c_2$, for all $c < c_1$, where $c, c_1, c_2 \in B$. Since $\beta$ is not an order isomorphism, there exists $b \in B$ such that $b \leq 0$ and $\beta(b) \nleq 0$. Choose such a $b$.

Let $c \leq c_1, c_1+b$. $c = c_1$ implies $b \nleq 0$, contrary to the choice of $b$. Therefore, $c < c_1$. By our initial assumption, $c < c_2$. Therefore, $c_2 \leq \inf_B \{c_1, c_1+b\}$. Since $\beta$ is a $V$-homomorphism, $\beta(c_2) \leq \inf_C \{\beta(c_1), \beta(c_1+b)\} = \beta(c_1)$.

**Theorem IV.7.** Suppose that $O \to A \overset{\alpha}{\to} B \overset{\beta}{\to} C \to 0$ is lexicographically exact and that $(P \sim 0) + C^+ \leq P$. If $A$ is filtered and $\beta$ is not an order isomorphism, then $\beta : B \to C$ is a $V$-homomorphism if and only if $\beta$ satisfies Pr 1: For $c_1, c_2 \in B$, $c < c_2$ for all $c < c_1$ implies $\beta(c_1) \leq \beta(c_2)$.

**Proof.** If $\beta$ is a $V$-homomorphism and not an order isomorphism, then $\beta$ always satisfies Pr 1, by Lemma IV.6. Hence, suppose that $A$ is filtered and $\beta$ satisfies Pr 1.

Let $b'_0 \equiv \inf_B \{b_1, \ldots, b_n\}$ . Suppose that $d' \equiv \beta(b'_1), \ldots, \beta(b'_n)$, and choose a preimage $d$ of $d'$ in $B$. Suppose $c < d$. Then
\( \beta(c) \leq \beta(d) \leq \beta(b_i), i = 1, \ldots, n, \) implies \( \beta(c) \leq \beta(b_i) \) or \( \beta(c) = \beta(b_i) \), by the property \((P \sim 0) + C^+ \subseteq P\). Thus \( b_i - c > 0 \) or \( b_i - c \in \alpha(A) \), the first assertion following from the lexicographic ordering of \((\alpha, A)\). In either case, \( c \leq b_i - a_i \) for some \( a_i \in \alpha(A) \). Since \( A \) is filtered, there exists \( a \in \alpha(A) \) such that \( a \leq a_1, \ldots, a_n \). Therefore, \( c \leq b_i - a \), and hence \( c + a \leq b_1, \ldots, b_n \). Thus, \( b_o \geq \inf_B \{b_1, \ldots, b_n\} \) implies that \( b_o \geq c + a \).

If \( b_o - a = c \), then \( b_o - a \leq b_i - a_i \) for all \( i \) implies \( b_o \leq b_i + a - a_i \leq b_i \), since \( a \leq a_i \). If \( \beta(b_o) = \beta(b_i) \) for some \( i \), then \( \beta(b_o) = \beta(c) \leq \beta(d) \leq \beta(b_i) \) implies \( \beta(b_o) = \beta(d) \).

Thus, suppose that \( \beta(b_o) \neq \beta(b_i) \) for all \( i \). Then, \( b_o \leq b_i \) implies \( \beta(b_o) \leq \beta(b_i) \) and hence \( b_o < b_i \) for all \( i \). Since \((P \sim 0) + C^+ \subseteq P \sim 0\), we have that \( \beta(b_i - d) + \beta(b_j - b_o) \in P \sim 0 \) for all \( i \) and for each \( j = 1, \ldots, n \). Therefore, \( b_i - d + b_j - b_o \geq 0 \) for all \( i \) and each \( j = 1, \ldots, n \). Hence it follows, by applying \( b_o \geq \inf_B \{b_1, \ldots, b_n\} \) twice, that \( b_o \geq d \) and thus \( \beta(b_o) \geq \beta(d) \).

We have thus shown that whenever \( c < d \) we always have \( c \leq b_o - a, a \in \alpha(A) \), and if \( c = b_o - a \) for some \( c < d \), then \( \beta \) is a \( V \)-homomorphism.

It thus remains to consider the case that \( c \neq b_o - a \) for all \( c < d \).

In that case, \( c < b_o - a \) for all \( c < d \). By \( \text{Pr} \ 1 \), \( d \leq b_o - a \) and hence \( \beta(d) \leq \beta(b_o - a) = \beta(b_o) \).

**Theorem IV.8.** Suppose that \( 0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0 \) is lexicographically exact and that \( (P \sim 0) + C^+ \subseteq P \). If \( A \) is not filtered, then \( \beta \) is a \( V \)-homomorphism if and only if \( C \) satisfies \( \text{Pr} \ 2 \): For \( c'_1, c'_2 \in C \), \( c'_1 \leq c'_2 \) for all \( c'_1 \nleq c'_1 \) implies \( c'_1 \leq c'_2 \).
Proof. Suppose that $A$ is not filtered, and that $C$ satisfies Pr 2.

Let $b_0 = \inf_B \{b_1, \ldots, b_n\}$. Suppose $d' = \beta(b_1), \ldots, \beta(b_n)$, and that $c' \not\leq d'$. For any $c \in B$ such that $\beta(c) = c'$, $\beta(b_1) \not\leq d' \Rightarrow c'$ implies $b_i \not\geq c$, by applying $(P \sim 0) + C^+ \subseteq P \sim 0$. Therefore, $b_0 \not\geq c$.

Since this is true for any preimage of $c'$, we conclude that $b_0 \not\geq c + a$ for any $a \in \alpha(A)$. If $b_0 = c$, then $0 \not\geq a$ for any $a \in \alpha(A)$, which would imply that $A = 0$, contrary to our assumption that $A$ is not filtered. Thus, $b_0 > c$ for any $c \in B$ such that $\beta(c) = c'$.

If $\beta(b_0 - c) = 0$, then $b_0 - c \in \alpha(A)$ and thus $\beta(c + b_0 - c) = \beta(c) = c'$. Therefore, $b_0 > c + b_0 - c$, a contradiction. Hence, $\beta(b_0) \not\geq \beta(c) = c'$, since $b_0 > c$ and $\beta(b_0) > \beta(c) = c'$. Therefore, Pr 2 implies $\beta(b_0) \not\leq d'$.

Conversely, assume that $A$ is not filtered, and that $\beta$ is a V-homomorphism. Let $c_1', c_2'$ be elements of $C$ such that $c_1' \not\leq c_2'$ for all $c_1' \not\leq c_2'$. Choose a preimage $c_1$ of $c_1'$ in $B$. Since $A$ is not filtered, we can find $a_1, a_2 \in \alpha(A)$ such that there does not exist $a \in \alpha(A)$ with $a \leq a_1, a_2$. Suppose that $d \leq d_1 + a_1, c_2 + a_2$.

Then $\beta(d) \not\geq c_1'$. If $\beta(d) = c_1'$, then $d = c_1' + a$ for some $a \in \alpha(A)$, and then $a \leq a_1, a_2$, a contradiction. Thus, $\beta(d) \not\leq c_1'$. Hence, $\beta(d) \not\leq c_2'$. Therefore for any preimage $c_2 \in B$ of $c_2'$, $c_2 \not\leq d$. By the choice of $d$ and the assumption that $\beta$ is a V-homomorphism, we conclude that $c_2' \not\leq \inf_C \{\beta(c_1' + a_1), \beta(c_1' + a_2)\} = c_1'$.

Corollary IV.9. Suppose that $C$ is a lattice-ordered group and $P$ is a submonoid of $C^+$, $(P \sim 0) + C^+ \subseteq P$, such that $P$ satisfies Pr 3: There exist $k_1, k_2 \in P$ such that $k_1 \not\geq k_2$ and $k_2 \not\geq k_1$, and $d = \inf_C \{k_1, k_2\}$ implies $d \not\geq k_1, k_2$. Then $\beta$ is a V-homomorphism.
Proof. It suffices to show that Pr 2 is satisfied. Suppose that $c' < c$ for all $c' \preceq c$. Then $c_1 - k \not\preceq c_1$ for all $k \geq 0$ implies $c'_1 - k \not\preceq c'_2$ for all $k \geq 0$. Let $k_1, k_2 \in P$ such that $k_1, k_2$ satisfy Pr 3. Let $c = \inf_P \{c'_2 + k_1, c'_1 + k_2\}$. Then $c \preceq c'_2 + k_1, c'_1 + k_2$. Therefore, $c \preceq c'_1 + k_1, c'_2 + k_2$, since $k_1 \not\preceq k_2, k_2 \not\preceq k_1$.

Hence, $c'_2 + k_1 - c, c'_2 + k_2 - c \geq 0$. Thus, $c'_1 \preceq c'_2 + (c'_2 + k_1 - c), c'_2 + (c'_2 + k_1 - c)$ implies $c'_1 - c'_2 + c \preceq c'_2 + k_1, c'_2 + k_2$. Therefore, $c \preceq c \inf_P \{c'_2 + k_1, c'_2 + k_2\}$ implies $c \preceq c'_1 - c'_2 + c$, or $c'_2 \preceq c'_1$. Therefore $C$ satisfies Pr 2. q.e.d.

We note that if $C$ is lattice, then $C^+$ satisfies Pr 3 trivially.
CHAPTER V

A CLASS OF GROUPS WHICH ARE NOT
GROUPS OF DIVISIBILITY OF DOMAINS

In [5], Jaffard provides an example of a filtered group which is not a group of divisibility of a domain. Ohm constructs a large class of such groups of the form $A \oplus C$ where $A \neq \{0\}$ and $C$ belongs to a certain class of lattice-ordered groups. In this chapter we enlarge this class of groups to include those of the form $A \oplus C_P$ where $P$ is a submonoid of $C^+$ satisfying a specified property. Finally, we show that an unpublished result of R. L. Pendleton—that the only filtered orders on the group of integers $\mathbb{Z}$ which produce groups of divisibility of domains are the two obtained by taking as positive elements either $\mathbb{Z}^+$ or $-\mathbb{Z}^+$—follows from a more general proposition.

Lemma V.1. Suppose that $0 \rightarrow A \overset{\alpha}{\rightarrow} B \overset{\beta}{\rightarrow} C_P \rightarrow 0$ is lexicographically exact and $v$ is a map of $T(R)^*$ onto $B$. Let $w = \beta v : T(R)^* \rightarrow B \rightarrow C$. If $A \neq 0$, and if there exist $x, y, x+y \in T(R)^*$ such that $w(x+y) \not\leq w(x)$, $w(y)$, then $v$ is not a semi-valuation. ([13], Lemma 5.1).

Proof. $w(x+y) \not\leq w(x)$, $w(y)$ implies that $v(x+y) + a \not\leq v(x)$, $v(y)$ for all $a \in \alpha(A)$. Therefore, if $v$ is a semi-valuation, we must have $v(x+y) \geq v(x+y) + a$, for all $a \in \alpha(A)$. This implies $A = 0$, a contradiction. q.e.d.

Let $C$ be a lattice-ordered group and let $i$ be a $V$-imbedding of $C$ in the ordered direct produce $D = \prod_u D_u$ of totally ordered groups (See [5] for the existence of such an $i$). Let $p_u$ be the projection
of D onto D_u and let i_u = p_u \cdot 1. By Jaffard's Theorem [5], C is the semi-value group of a semi-valuation w of a field K (and hence of a ring R = T(R) which is not a field: If X is an indeterminate over K, we simply take R = K[X] ⊕ M, the ring formed by the principle of idealization, with M = \sum_i (K[X]/B_i) where \{B_i\} = set of proper ideals of K[X]. Then, if D is the semi-valuation ring of a semi-valuation w or K with semi-value group C, D ⊕ M is a semi-valuation ring of a semi-valuation w' of K[X] ⊕ M with semi-value group R'/U(D ⊕ M) ≈ K'^*/U(D) ≈ C_u. Since the projection maps p_u are always V-homomorphisms whenever the D_u are filtered, u = i_u w is also a semi-valuation for each u. Moreover, i = \sum u_i u and hence iw = \pi_u .

Let P be a submonoid of the positive elements C^+ of the lattice-ordered group C. We say that C_P satisfies property \( \mathcal{G} \) if there exist c_1, c_2 ∈ C such that c_1 \neq c_2 and c_2 \neq c_1, and such that i_u(c_1) \neq i_u(c_2) for all u, and \( d = \inf_C[c_1, c_2] \) implies \( d \geq c_1, c_2 \).

Any ordered direct product C of at least two copies of Z satisfies property \( \mathcal{G} \) for some submonoid P of C^+. For example, if P = C^+; or, for c_1, c_2 ∈ C such that c_1 \neq c_2 and c_2 \neq c_1, and i_u(c_1) \neq i_u(c_2) for all u, let \( d = \inf_C[c_1, c_2] \); let a be any minimal element of C^+ such that a \neq c_1 - d, c_2 - d. Then P = C^+ \sim \{a\} is a submonoid of C^+: If x, y ∈ P, x \neq 0 and x + y = a, then x \leq x + y = a implies that x = a by the minimality of a in C^+ \sim 0, contradicting x ∈ P. Hence x + y ∈ P. If c_1 - d and c_2 - d are the only minimal elements of C^+ \sim 0, then c_1, c_2 + c_2 satisfy the first two conditions of property \( \mathcal{G} \); and thus, if \( d' = \inf_C[c_1, c_2 + c_2] \), we can take P = C^+ \sim \{c_2 - d'\}. \)
In either case, it is evident that $C_p$ satisfies property $\Theta$, and $P \neq C^+$ since $a \in C^+$, $a \notin P$.

**Lemma V.2.** Let $w$ be a semi-valuation of a ring $R = T(R)$ with semi-value group $C$. If $C$ is totally ordered, and $x_1, x_2, x_1 + x_2 \in R^*$, then $w(x_1) \neq w(x_2)$ implies $w(x_1 + x_2) = \inf_C \{w(x_1), w(x_2)\}$.

**Proof.** Since $w$ is a semi-valuation, $w(x_1 + x_2) \geq \inf_C \{w(x_1), w(x_2)\}$. Since $C$ is totally ordered, we may assume $w(x_1) < w(x_2)$, since $w(x_1) \neq w(x_2)$ by hypothesis. If $w(x_1 + x_2) > w(x_1) = w((x_1 + x_2) - x_2)$, then $w(x_1) \geq \inf \{w(x_1 + x_2), w(x_2)\} > w(x_1)$, a contradiction. Therefore, $w(x_1 + x_2) = w(x_1) = \inf_C \{w(x_1), w(x_2)\}$.

**Lemma V.3.** Suppose that $C$ is a lattice-ordered group and $i$ is a $V$-embedding of $C$ in the ordered direct product $D = D_u$ of totally ordered groups, and assume that $w$ is a semi-valuation of a ring $R = T(R)$ with semi-value group $C$. If $C$ satisfies property $\Theta$, then there exist $x_1, x_2 \in T(R)^*$ such that whenever $x_1 + x_2 \in T(R)^*$, then $w(x_1 + x_2) = \inf_C \{w(x_1), w(x_2)\} < w(x_1), w(x_2)$ ([13], Lemma 5.2)

**Proof.** Choose $x_1, x_2 \in T(R)^*$ such that $w(x_1) = c_1$, $w(x_2) = c_2$.

Let $u = i_u w$, where, as we noted in the discussion following Lemma V.1, $i_u = p_u i$; $p_u$, the projection map of $D = D_u$ onto $D_u$. $u(x_1) \neq u(x_2)$ implies $u(x_1 + x_2) = \inf_D \{u(x_1), u(x_2)\}$. Since $i w = \sigma_u$, $w(x_1 + x_2) = \inf_C \{w(x_1), w(x_2)\}$. By hypothesis, $c_1$ and $c_2$ are unrelated, so $\inf_C \{w(x_1), w(x_2)\} < w(x_1), w(x_2)$.

**Theorem V.4.** Let $C$ be a lattice-ordered group and $P$ a submonoid of $C^+$ such that $(P \sim 0) + C^+ \subseteq P$ and $C_p$ satisfies property $\Theta$. Suppose that $0 \rightarrow A \xrightarrow{\sigma} B \xrightarrow{\rho} C_p \rightarrow 0$ is lexicographically exact and $A \neq 0$. Let $v$
be a map from the group of units $R^*$ of a ring $R = T(R)$ onto $B$. If $c_1 = \beta v(x_1), c_2 = \beta v(x_2)$ satisfy the conditions of property $\mathcal{G}$ and $x_1 + x_2 \in R^*$, then $v$ is not a semi-valuation. ([13], Theorem 5.1)

**Proof.** Suppose that $v$ is a semi-valuation. By Corollary IV.9, $\beta : B \rightarrow C$ is a $V$-homomorphism. Therefore, $w = \beta v$ is a semi-valuation with semi-value group $C$. If $x_1 + x_2 \in T(R)^*$, then by Lemma V.3, $w(x_1 + x_2) = \inf_C \{w(x_1), w(x_2)\} < w(x_1), w(x_2)$. Since $C_p$ satisfies property $\mathcal{G}$, $w(x_1 + x_2) \not< w(x_1), w(x_2)$. Thus, by Lemma V.1, $v$ is not a semi-valuation.

**Corollary V.5.** Let $A$ be any non-zero ordered group, and let $P$ be a submonoid of a lattice-ordered group such that $(P \sim 0) + C^+ \subseteq P \subseteq C^+$ and such that $C_p$ satisfies property $\mathcal{G}$. Then $A \oplus C_p$ is not a group of divisibility of a domain.

**Proof.** $A \neq 0$ and $0 \rightarrow A \xrightarrow{i} A \oplus C_p \xrightarrow{p} C_p \rightarrow 0$ is lexicographically exact, with $i$ and $p$ the usual injection and projection maps, respectively. By hypothesis, $C_p$ satisfies property $\mathcal{G}$. If $D$ is a domain with quotient field $T(D)$ and $v$ is a map from $T(D)^*$ onto $A \oplus C_p$, and if $c_1 = pv(x_1), c_2 = pv(x_2)$ satisfy the conditions of property $\mathcal{G}$ then $x_1 + x_2 \in T(D)^*$, since $T(D)$ is a field and $c_1$ and $c_2$ are unrelated. Thus the conditions of Theorem V.5 are satisfied. Therefore, $v$ is not a semi-valuation. Thence, $A \oplus C_p$ is not a group of divisibility of a domain, if $A \neq 0$.

**Corollary V.6.** Let $P$ be a submonoid of a lattice-ordered group $C$ such that $(P \sim 0) + C^+ \subseteq P \subseteq C^+$, and assume that $C = \mathbb{D}_u$ the ordered
direct product of totally ordered groups $D_u$. If $P$ contains at least
two strictly positive disjoint elements (in $C^+$), $c_1$, $c_2$, such that
$p_u(c_1) \neq p_u(c_2)$ for all $u$, and if $A \neq 0$, then $A \oplus C_p$ is not a group
of divisibility of a domain.

**Proof.** Suppose that $c_1$, $c_2$ are disjoint elements of $C$ such that
$c_1$, $c_2 \in P \sim 0$. Then $c_1 \neq c_2$ and $c_2 \neq c_1$. Since $c_1$ and $c_2$ are
disjoint, $0 = \inf_{C} \{c_1, c_2\}$. By hypothesis, $p_u(c_1) \neq p_u(c_2)$ for all
$u$, and $c_1, c_2 \in P$. Thus, $0 \not\leq\frac{1}{p}c_1, c_2$. Therefore, $C_p$ satisfies
property $\mathcal{O}$. By Corollary V.5, if $A \neq 0$, then $A \oplus C_p$ is not a
group of divisibility of a domain. q.e.d.

Thus, for example, if $A \neq 0$, and $P$ is a submonoid of $\mathbb{Z} \times \mathbb{Z}$, the
ordered direct product of two copies of the integers, such that
$(P \sim 0) + (\mathbb{Z} \times \mathbb{Z})^+ \subseteq P \subseteq (\mathbb{Z} \times \mathbb{Z})^+$, then $A \oplus (\mathbb{Z} \times \mathbb{Z})_p$ is never a
group of divisibility of a domain if $P$ contains both $(0, m)$ and
$(n, 0)$ for some $m, n \in \mathbb{Z}^+ \sim 0$.

We have already shown that $\mathbb{Z}_p$, $P = \{j : j \geq n$ for some $n > 1 \cup \{0\}$
is never a group of divisibility of a domain (Example III.7). This
fact also follows from the proposition below.

**Proposition V.7.** Let $C$ be an ordered group and let $P$ be a proper
submonoid of $C^+$. Let $i : C_p \to C$ be the identity homomorphism.
Let $v$ be a map from the group of units $R^*$ of a ring $R = T(R)$ onto
$C_p$, and assume that $iv$ is an additive semi-valuation with semi-
valuation ring $D$ and semi-valuation monoid $D^*$. Assume also that for
each regular non-unit $x$ of $D$, there exists $t \in U(D)$ such that
$x + t \in D^\times$. Then $v$ is not a semi-valuation with semi-valuation ring $D'$ and semi-valuation monoid $D'^\times$.

**Proof.** Let $x \in R^\times$ such that $iv(x) > 0$. Let $t \in U(D)$ such that $x + t \in D^\times$. By Proposition 11.16, since $iv$ is additive, the regular non-units of $D$ generate a proper ideal of $D$. Therefore, $x + t \in U(D)$. Since $iv$ is additive, $iv(x) > iv(t) = 0$ implies $iv(x+t) = 0$. Since $i$ is an injection, this implies $v(x+t) = 0$. Hence, if $v$ is a semi-valuation with semi-valuation ring $D'$, we must have $x + t, t \in D'$.

But then, $x + 1 \in D'$, $t \in D'$ imply $x \in D'$. Hence $D$ and $D'$ have the same regular non-units. But this implies $P = C^+ (U(D) = U(D'))$ because $i$ is an injection), contrary to our assumption that $P$ is a proper submonoid of $C^+$. Therefore, $v$ is not a semi-valuation with semi-valuation monoid $D'^\times$. q.e.d.

Proposition V.7 applies to the following situation: Let $C$ be a totally ordered group and let $P$ be a proper submonoid of $C^+$ such that $C_p$ is filtered and $(P \sim 0) + C^+ \subseteq P$. From Lemmas IV.4 and IV.5, the identity map $i : C_p \rightarrow C$ is a $V$-homomorphism. Hence, if $v$ is a semi-valuation with semi-value group $C_p$ then $iv$ is an additive semi-valuation. Thus, from Proposition V.7, $v$ cannot be a semi-valuation of a domain (in the case of a domain, the ring $D$ of $iv$ is quasi-local and thus the condition that there exist $t_x \in U(D)$ for every non-unit $x \neq 0$ such that $x + t_x \in D^\times$ is automatically satisfied.)

Since the composition of two $V$-homomorphisms is again a $V$-homomorphism, Proposition V.7 also applies, in the above situation, to any submonoid $P' \subseteq P$ such that the identity homomorphism $i : C_{p'} \rightarrow C_p$ is a $V$-homomorphism.
We consider now the submonoids $P \subseteq \mathbb{Z}^+$ such that $Z_p$ is filtered.

**Claim 1.** Let $P \subseteq \mathbb{Z}^+$ such that $Z_p$ is filtered. For each integer $j \in \mathbb{Z}^+ \sim 0$ and for all $i = 0, 1, \ldots, 2j$, there exists $k \in \mathbb{Z}^+$ such that $j \cdot 2k + i \in P$.

**Proof.** Since $Z_p$ is filtered, $1 = m-n$ for some $m, n \in P$. Hence $P$ contains two consecutive integers $k, k+1$. But then $2k, 2k+1, 2k+2$ also belong to $P$ since $P+P \subseteq P$.

Assume inductively that $j \cdot 2k+i \in P$ for some $j \in \mathbb{Z}^+ \sim 0$ and for all $i = 0, 1, \ldots, 2j$. $(j+1) \cdot 2k+i = (j \cdot 2k+i) + 2k$. If $i \leq 2j$, then $j \cdot 2k+1 \in P$ by the inductive hypothesis. $2k \in P$ by the $j = 1$ case. Therefore, their sum is in $P$. If $i = 2j+1$, then $(j+1) \cdot 2k+(2j+1) = (j \cdot 2k+2j) + (2k+1) \in P + P$, again by the inductive hypothesis and the $j = 1$ case. Similarly, for $i = 2j + 2$, $(j \cdot 2k+2j) + (2k+2) \in P + P \subseteq P$. Hence, $(j+1) \cdot 2k+i \in P$ for each $i = 0, 1, \ldots, 2(j+1)$.

**Claim 2.** $P$ contains every integer $n$ such that $n-k \cdot 2k \in \mathbb{Z}^+$.

**Proof.** By Claim 1, $k \cdot 2k+i \in P$ for all $i = 0, 1, \ldots, 2k$. Then $(k \cdot 2k+2k) + 1 = (k+1)k+1 \in P$, also by Claim 1.

Suppose inductively that $(k \cdot 2k+2k) + r \in P$ for all $r \leq n$, $r > 1$, for some integer $n$. If $n < 2k$, then $k \cdot 2k + 2k + n = (k+1)k+n \in P$ by Claim 1, so we may assume that $n \geq 2k$ and write $n = s \cdot 2k+t$, $t < n$. Then $(k \cdot 2k+2k) + (n+1) = (k \cdot 2k+2k+t) + (s \cdot 2k+1)$.

$k \cdot 2k+2k+t \in P$ by the inductive hypothesis, since $t < n$, and $s \cdot 2k+1 \in P$ by Claim 1, since $s \geq 1$. Therefore, the sum $(k \cdot 2k+2k) + (n+1) = (k \cdot 2k+2k+t) + (s \cdot 2k+1)$ is in $P$. 


Proposition V.8. Let $A$, $B$ be ordered groups, and let $h : A \rightarrow B$ be a surjective order homomorphism. Assume that $B$ is totally ordered. If the set $B^+ \sim h(A^+)$ has a maximal element, then $h$ is a $V$-homomorphism.

Proof. Let $a_o \geq \inf_A \{a_1, \ldots, a_n\}$. Since $B$ is totally ordered, we may assume that $h(a_1) \leq h(a_2) \leq \ldots \leq h(a_n)$ and it thus suffices to prove that $h(a_o) \geq h(a_j)$ for some $j = 1, \ldots, n$.

Suppose that $h(a_o) < h(a_j)$ for each $j = 1, \ldots, n$. Let $d^1$ be a maximal element of $B^+ \sim h(A^+)$. Since $h$ is surjective, we can choose a preimage $d$ of $d^1$ in $A$ such that $h(d) = d^1$, $d \notin A^+$.

$h(a_j - a_o) > 0$ for all $j = 1, \ldots, n$. Therefore, $h(a_j) - h(a_o) + h(d) > h(d)$, 0. Since $h(d)$ is maximal in $B^+ \sim h(A^+)$, this implies that $a_j - a_o + d \in A^+$. $a_j \geq a_o - d$ for all $j = 1, \ldots, n$ implies that $a_o \geq a_o - d$. Hence $0 \geq -d$, contrary to the choice of $d$. Thus, $h(a_o) \geq h(a_j)$ for some $j = 1, \ldots, n$. q.e.d.

By Claim 2, if $Z^+ \neq P$, $Z^+ \sim P$ is finite and hence $Z^+ \sim P$ has a maximal element. Thus, by Proposition V.8, the identity map $i : Z_p \rightarrow Z$ is a $V$-homomorphism. It follows, therefore, from Proposition V.7, that $Z_p$ is not a semi-value group of a domain for any $P \subseteq Z^+$ such that $Z_p$ is filtered. Since any ordering on $Z$ is contained in either $Z^+$ or $-Z^+$, this implies that the only filtered orders on $Z$ which produce groups of divisibility of domains are $Z^+$ or $-Z^+$. 
BIBLIOGRAPHY


14. G. Scheja and U. Storch, *Bemerkungen über die Einheitengruppen*  
semilokaler Ringe  
Mathematisch Physikalische Semesterberichte, 

15. D. Underwood, *On some uniqueness questions in primary representations*  

16. O. Zariski and P. Samuel, *Commutative Algebra* 1, 11  
A.1. Let \( R \) be a quasi-local ring of the form \( k + M \), where \( k \) is a field and \( M \) is the maximal ideal of \( R \).

Then

1. the mapping \((a + m)(1 + M^n) \mapsto (a, (1 + a^{-1}m)(1 + M^n))\) is a group isomorphism from \((R/M^n)^*\) onto \( k^* \times (1 + M)/(1 + M^n) \);

2. if \( D \) is a subring of \( k \), the mapping \( \varphi \) induced by \((R/M^n)^*/U(D) \mapsto k^*/U(D) \times (1 + M)/(1 + M^n) \), is an order isomorphism, with \((R/M^n)^*/U(D)\) ordered by \( D^*/U(D) \) and \( k^*/U(D) \times (1 + M)/(1 + M^n) \) ordered by \((D^*/U(D), 1)\);

3. \((1 + M)/(1 + M^n)\) and \( M/M^n \) are isomorphic as groups.

**Proof.** (1) \( \varphi \) is well-defined:

Suppose that \((a + m)(1 + M^n) = (a' + m')(1 + M^n)\). Then \((a + m)(a' + m')^{-1} \in 1 + M^n\). Let \((a' + m')^{-1} = a'' + m'', a', a'' \in k, m', m'' \in M\). Then

\[(a + m)(a' + m') = aa'' + a'm + am'' + m'm' \in 1 + M^n\] implies \(aa' = 1\).

\[(1 + a^{-1}m)(1 + a'^{-1}m')^{-1} = a^{-1}(a + m)a'^{-1}(a' + m')^{-1} = a^{-1}a'(a + m)(a' + m')\].

\[(a' + m')^{-1} = 1/(a' + m') = a'' + m'\] implies \(1 = a'a'' + a'm' + a'm'' + m'm' \in M\), and \(1 - a'a'' \in k\). Therefore, \(1 - a'a'' = 0\), and thus \(a'a'' = 1\). Hence

\(aa'' = 1\ implies a'a'' implies a = a'\). By assumption, \((a + m)(a' + m') \in 1 + M^n\), and we therefore conclude that \((1 + a^{-1}m)(1 + a'^{-1}m')^{-1} \in 1 + M^n\). Thus

\((1 + a^{-1}m)(1 + M^n) = (1 + a'^{-1}m')(1 + M^n)\).

\(\varphi\) is a homomorphism:

\[\varphi[(a + m)(1 + M^n)] \varphi[(a' + m')(1 + M^n)] = (a, (1 + a^{-1}m)(1 + M^n))(a', (1 + a'^{-1}m')(1 + M^n))\]

\[= (aa', (1 + a^{-1}m)(1 + a'^{-1}m')(1 + M^n)) = \varphi[(aa' + a'm + a'm'm')(1 + M^n)]\]

\[= \varphi[(a + m)(a' + m')(1 + M^n)]\]

\[= \varphi[(a + m)(1 + M^n) \cdot (a' + m')(1 + M^n)]\].
(1) Suppose that $C[(a+m)(1+M^n)] = (1, 1)$. Then $a = 1; 1 + a^{-1}m = 1$ implies $a^{-1}m = 0$. Hence $m = 0$. Let

$$(a, (1+m)(1+M^n)) \in k^* \times (1+M/(1+M^n)).$$

Then, $C[(a+am)(1+M^n)] = (a, (1+am)(1+M^n)) = (a, (1+m)(1+M^n))$

(2) Let $C$ be the mapping in (1), $p, p'$ the canonical homomorphisms, $i$ the identity homomorphism in the diagram below.

$$
\begin{array}{ccc}
(R/M^n)^* & \xrightarrow{C} & k^* \times (1+M)/(1+M^n) \\
p & \downarrow & (p', i) \\
(R/M^n)^*/U(D) & \xrightarrow{C'} & k^*/U(D) \times (1+M)/(1+M^n)
\end{array}
$$

$\ker(p', i)\supseteq \ker p$: $p((a+m)(1+M^n)) = 1$ implies $a \in U(D), m \in M^n$.

$(p', i)C((a+m)(1+M^n)) = (p', i)[(a, (1+a^{-1}m)(1+M^n))] = (1, 1)$.

Hence $C'$ is defined canonically and is surjective since $(p', i)C$ is surjective. If $(p', i)C((a+m)(1+M^n)) = (a, (1+a^{-1}m)(1+M^n)) = (1, 1)$, then $a \in U(D), m \in M^n$; hence $p((a+m)(1+M^n)) = 1$. Thus, $\ker(p', i)C = \ker p$ and $C'$ is therefore injective.

If $x \in D^*/U(D)$, then $x = p((a+m)(1+M^n))$ for some $a \in D^*, m \in M^n$.

$C'(x) = C'p((a+m)(1+M^n)) = (p', i)C((a+m)(1+M^n)) = (p', i)[(a, (1+a^{-1}m)(1+M^n))] = (\bar{a}, 1)$, where $a \in D^*$. Conversely, if $(\bar{a}, 1) \in k^*/U(D) \times (1+M)/(1+M^n), a \in D^*$, then $C^{-1}(\bar{a}, 1) = p((a+m)(1+M^n))$ where $m \in M^n$. Hence $C'$ is an order isomorphism.

(3) $M^2/M^3$ is a subspace of the vector space $M/M^3$ over $k(M/M^3)$ becomes a $k$-vector space by defining $a(m+M^3)$ to be the coset $am+M^3$.

Let $\alpha, \beta$ be the canonical injection and projection maps, respectively:

$$0 \to M^2/M^3 \xrightarrow{\alpha} M/M^3 \xrightarrow{\beta} (M/M^3)/(M^2/M^3) \to 0.$$
Then \((M/M^3)/(M^2/M^3) \approx M/M^2\) as vector spaces and there exists a subspace \(W\) of \(M/M^3\) such that \(W \approx M/H^2\) as vector spaces over \(k\) ([9], Theorem 4, page 87; and page 76). Thus \(W\) and \(M/H^2\) are isomorphic as additive groups. By ([14], Satz 3.2), the mapping \(\phi : a+M^n \rightarrow (1+a)(1+M^n)\) is a group isomorphism from \(M^{n-1}/M^n\) onto \((1+M^{n-1})/(1+M^n)\).

Let \(\psi_1 : M/M^2 \rightarrow (1+M)/(1+M^2), \psi_1(a+M^2) = (1+a)(1+M^2), a \in M;\)
\(\psi_2 : M^2/M^3 \rightarrow (1+M^2)/(1+M^3), \psi_2(a+M^3) = (1+a)(1+M^3), a \in M^2.\)

Then, \(\alpha, \beta\) induce \(\alpha', \beta'\) such that \(1 \rightarrow (1+M^2)/(1+M^3) \alpha' \rightarrow (1+M)/(1+M^3) \beta' \rightarrow (1+M)/(1+M^2) \rightarrow 1\) is exact.

Since \(\alpha, \beta\) are also group homomorphisms, \(\beta|_W\) is a group isomorphism.

Define \(\bar{\phi} : (1+M)/(1+M^3) \rightarrow M/M^3\) by
\(\bar{\phi}[(1+m)(1+M^3)] = (\beta|_W)^{-1}\psi_1^{-1}\beta'[(1+m)(1+M^3)]\), if \(m \notin M^2;\)
\(\bar{\phi}[(1+m)(1+M^3)] = \alpha\psi_2^{-1}\alpha'^{-1}[(1+m)(1+M^3)],\) if \(m \in M^2.\)

Since \([m+M^3 : m \notin M^2]\) is a subspace \(W\) of \(M/M^3\) isomorphic to \(M/M^2, \bar{\phi}\) is well-defined, and is a group homomorphism since it is defined as the composition of homomorphisms. If \(m \in M^2\), then \(\bar{\phi}\) is clearly injective because \(\alpha, \psi_2^{-1}, \alpha'^{-1}\) are injections. Suppose that \(m \notin M^2.\) \(\bar{\phi}[(1+m)(1+M^3)] = 0\) implies \(\beta'[((1+m)(1+M^3)] = 0\), since \((\beta|_W)^{-1}\) and \(\psi_1^{-1}\) are isomorphisms. But this implies that \((1+m)(1+M^3) \notin \alpha'((1+M^2)/(1+M^3)),\) contrary to assumption, unless \(m = 0.\)

The assertion now follows from induction by assuming (inductively) that \(M/M^n \overset{\phi}{\approx} (1+M)/(1+M^n), \) where \(\bar{\phi}[(1+m)(1+M^n)] = (\beta|_W)^{-1}\psi_1^{-1}\beta'[(1+m)(1+M^n)],\)
\(\beta'[(1+m)(1+M^n)],\) where \(m \notin M^n;\)
\(\phi[(1+m)(1+M^n)] = \alpha\psi_2^{-1}\alpha'^{-1}[(1+m)(1+M^3)],\) where \(m \in M^n;\) and from the diagram.
Valuations of fields

If \( w \) is a semi-valuation of a field \( K \) onto a totally ordered Abelian group \( G \), then \( w \) is called a valuation of the field \( K \) and \( G \) is called the value group of \( w \). The ring of \( w \) is then a quasi-local domain with \( K \) as its quotient field.

A.2 Let \( R \) be a quasi-local domain. The following are equivalent,

1. \( R \) is a discrete rank one valuation ring; that is, the group of divisibility of \( R \) is order isomorphic to the totally ordered group of integers, \( \mathbb{Z} \).

2. \( R \) is Noetherian with a principal maximal ideal \( M \); every ideal \( A \) of \( R \), \( (A \neq 0, R) \) is of the form \( M^n \), \( n \geq 1 \).

3. \( R \) is a principal ideal ring. ([2], Proposition 9, page 109).

A.3. (Krull's Theorem). Let \( C \) be any totally ordered group and \( k \) any field. Then there exists a valuation \( w \) of the quotient field of the group algebra \( \mathcal{A}_k(C) \) with value group \( C \) and ring \( R = k + M \), where \( M \) is the maximal ideal of \( R \).

([2], Example 6, page 107).

A.4. Let \( L \) be an extension field of finite degree of a field \( K \). Let \( v \) be a discrete rank one valuation of \( K \). Then, if \( v' \) is a valuation of \( L \) extending \( v \), \( v' \) is also a discrete rank one valuation. ([2], Corollaire 3, page 140).
A.5. Let $K$ be a field, $v$ a valuation of $K$ with ring $R$, and $M$ the maximal ideal of $R$. Let $L$ be a finite separable extension of degree $n$ over $K$, and let $B$ be the integral closure of $R$ in $L$. Let $C$, $C'$ be the value groups of $v$ and a valuation $v'$ of $L$ extending $v$, respectively. Let $e = \text{index of } C \in C'$, $f = \text{dimension of } B/mB$ as a vector space over $R/M$, $g = \text{number of maximal ideals of } B \text{ lying over } M$. Then $efg = n$, with equality holding if $B$ is a finite $R$-module. ([2], Proposition 8, pages 152-153).

A.6. Let $R$ be a valuation ring of the form $k+M$ where $k$ is a field and $M$ is the maximal ideal of $R$. Let $C$ be the group of divisibility of $R$ (up to order isomorphism). Then the group $(1+M)/(1+M^n)$ is isomorphic to the additive group $\bigoplus (k^+)$, where $(k^+)$ denotes the additive group of the field $k$, and cardinality of $1 = \text{the cardinality of } [c^+ \sim (nc^+ \cup \{0\})]$, $nc^+ = \{c \in C : c = c_1+\ldots+c_n, c_i > 0, i = 1, \ldots, n\}$. 

Proof. For each $n = 1, 2, \ldots, M^n$ is an $R$-module. $M^{n-j}/M^n$, $1 \leq j < n$, becomes an $R$-module by defining $a(x+M^n)$ to be the coset $ax+M^n$ for $a \in R$, $x \in M^{n-j}$. Then, since $k \subseteq R$, $M^{n-j}/M^n$ is also a $k$-module, and thus has a vector space basis over $k$. Let $B = \{\overline{m}_\alpha = m_\alpha + M^n\}$ be the set of basis elements of $M^{n-1}/M^n$. Let $w$ be the valuation of $T(R)$ with value group $C$.

Define a mapping $f : B \to w(M^{n-1}) \sim 0 \sim w(M^n \sim 0)$ by $f(\overline{m}_\alpha) = w(m_\alpha)$. $f$ is well-defined: Suppose that $y \in \overline{m}_\alpha \in B$. Then $y-m_\alpha \in M^n$. $w(y-m_\alpha) \geq \inf_C \{w(y), w(m_\alpha)\}$. If $w(y) \neq w(m_\alpha)$, then, since $w$ is a valuation, $w(y-m_\alpha) = \inf_C \{w(y), w(m_\alpha)\}$. $w(y-m_\alpha) \neq w(m_\alpha)$ since...
$m_\alpha \not\in M^n$ and $y-m_\alpha \in M^n$. $w(y-m_\alpha) = w(y)$ implies $y \in M^n$, and then, since $y-m_\alpha \in M^n$, so does $-m_\alpha$, a contradiction to $\overline{m_\alpha} \neq 0$. Hence $w(y-m_\alpha) \neq \inf\{w(y), w(m_\alpha)\}$, and therefore, $w(y) = w(m_\alpha)$. 

$f$ is injective: Suppose that $f(m_\alpha) = f(m_\beta)$, or $w(m_\alpha) = w(m_\beta)$. Then $m_\alpha = tm_\beta$, where $t \in U(R)$. Since $R = k+M$, we can write $t = a+m$ where $a \in k$, $m \in M$. Then $m_\alpha = am_\beta + mm_\beta$. $m_\beta \in M^{n-1}$ and $m \in M$ imply $mm_\beta \in M^n$. Hence $\overline{m_\alpha} = \overline{am_\beta} = \overline{am_\beta}$. Since $m_\alpha, m_\beta \in \mathcal{B}$, they are linearly independent over $k$. Thus $a = 1$. Hence $\overline{m_\alpha} = \overline{m_\beta}$.

$f$ is surjective: Let $d = w(y) \in w(M^{n-1} \sim 0) \sim w(M^n \sim 0)$. Then $y \in M^{n-1} \sim M^n$. Hence $\overline{y} = y+M^n \in M/M^n$, $\overline{y} \neq 0$. We can write $\overline{y}$ as a linear combination of elements of $\mathcal{B}$ with coefficients in $k$:

$y = a_1\overline{m_\alpha_1} + ... + a_k\overline{m_\alpha_k}$, $\overline{m_\alpha_i} \neq \overline{m_\alpha_j}$ for $i \neq j$. Then, $y - a_1\overline{m_\alpha_1} - ... - a_k\overline{m_\alpha_k} = m \in M^n$. Since $w$ is a valuation, $y - a_1\overline{m_\alpha_1} - ... - a_k\overline{m_\alpha_k} = m = 0$ implies

(i) $w(y) = w(a_i\overline{m_\alpha_i}) = w(m_\alpha_i)$ for some $i$,

or (ii) $w(a_i\overline{m_\alpha_i}) = w(a_j\overline{m_\alpha_j})$ for some $j \neq i$,

or (iii) $w(y) = w(m)$,

or (iv) $w(a_i\overline{m_\alpha_i}) = w(m)$ for some $i$ .

(ii) implies $\overline{m_\alpha_i} = \overline{m_\alpha_j}$, $j \neq i$, contrary to assumption. (iii) implies $y \in M^n$, a contradiction to $\overline{y} \neq 0$. (iv) implies $\overline{m_\alpha_i} \in \mathcal{B}$. Therefore, $w(y) = w(m_\alpha_i)$. Hence $d = w(m_\alpha_i)$, where $\overline{m_\alpha_i} \in \mathcal{B}$. Thus $f$ is surjective.

Since $f$ is bijective, cardinality $\mathcal{B} = \text{cardinality } [w(M^{n-1} \sim 0) \sim w(M^n \sim 0)]$. 
$M^2/M^3$ is a subspace of $M/M^3$ and $\dim_k(M/M^3) = \dim_k(M^2/M^3) + 
abla\dim_k((M/M^3)/(M^2/M^3))$ ([9], Theorem 4, page 87).

$(M/M^3)/(M^2/M^3) \cong M/M^2$ as vector spaces over $k$ ([9], page 76).

Therefore, $\dim_k(M/M^3) = \dim_k(M^2/M^3) + \dim_k(M/M^2)$.

Since $[w(M^2 \sim 0) \sim w(M^3 \sim 0)] \cup [w(M \sim 0) \sim w(M^2 \sim 0)] = w(M \sim 0) \sim w(M^3 \sim 0)$, and $[w(M^2 \sim 0) \sim w(M^3 \sim 0)] \cap [w(M \sim 0) \sim w(M^2 \sim 0)] = \emptyset$, the empty set, we have that cardinality $[w(M \sim 0) \sim w(M^3 \sim 0)] = \text{cardinality } [w(M \sim 0) \sim w(M^2 \sim 0)] + \text{cardinality } [w(M^2 \sim 0) \sim w(M^3 \sim 0)].$ Hence $\dim_k(M/M^3) = \text{cardinality } [w(M \sim 0) \sim w(M^3 \sim 0)]$.

Assume inductively that $\dim_k(M/M^{n-1}) = \text{card}[w(M) \sim w(M^{n-1})]$.

Let $p : M/M^n \rightarrow M/M^{n-1}$ be the canonical $k$-module map. Then, $\dim_k(M/M^n) = \dim_k(\ker p) + \dim_k(\text{Im } p)$ ([9], Theorem 4, page 87). Thus, $\dim_k(M/M^n) = \text{cardinality } [w(M^{n-1} \sim 0) \sim w(M^n \sim 0)] + \text{cardinality } [w(M \sim 0) \sim w(M^{n-1} \sim 0)]$, by the inductive hypothesis. Therefore, $\dim_k(M/M^n) = \text{cardinality } [w(M) \sim (M^n)]$. Thus, $M/M_n \cong \bigoplus_k 1$, where cardinality $1 = \text{cardinality } [w(M \sim 0) \sim (M^n \sim 0)]$, and therefore $M/M^n$ and $\bigoplus_k 1$ are isomorphic as additive groups. By A.1, $(1+M)/(1+M^n)$ and $M/M^n$ are isomorphic groups. Thus $(1+M)/(1+M^n)$ and $\bigoplus_k 1$ are isomorphic groups.

**Finite Rings.**

A.7. Let $Z$ denote the ring of integers. Then

(i) $U(Z/(p^n)) \cong Z/(p-1) \times Z/(p^{n-1})$, where $p$ is a prime $\neq 2$;

(ii) $U(Z/(2^n)) \cong \{0\}$, if $n = 1$; $Z/(2)$, if $n = 2$; $Z/(2^{n-2}) \times Z(2)$, if $n > 2$.

(N. Bourbaki, Algebre, chapitre 7, Theoreme 3, page 78.)
A.8. For every integer \( k \geq 0 \), \( (1+p)^k \equiv 1 + p^{k+1} \pmod{p^{k+2}} \), where \( p \) is a prime \( \geq 3 \); \( 5^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}} \).

(N. Bourbaki, *Algèbre*, chapitre 7, Lemme 3, page 77.)

A.9. Let \( R \) be a finite local ring with maximal ideal \( M \). Then

(i) cardinality \( R^* = (\text{card } R/M)^\ell(M) (\text{card } (R/M)^\ell(M)) \), where \( \ell(M) \) denotes the length of a composition series of \( M \) as an \( R \)-module.

(ii) \( R^* = (R/M)^* \times (1+M) \).

(iii) \( \text{card } M = (\text{card } R/M)^\ell(M) \).

([14], page 177).

A.10. Let \( k = GF(p^n) \), the finite field of \( p^n \) elements. Then the only subrings of \( k \) are subfields \( GF(p^r) \), where \( r \) divides \( n \).

Proof. Since \( k \) is a field, any subring of \( k \) is a domain. A finite integral domain is a field. (Let \( R \) be a subring of \( k \); consider the products \( ay \), where \( a \in R \) is fixed and \( y \) varies over elements of \( R \). \( ay = ay' \) implies \( y = y' \), since \( R \) is a domain. Thus, by the finiteness of \( R \), \( ay = 1 \) for some \( y \).) The result now follows from ([9], page 185, Theorem 13).

An Isomorphism Theorem for Rings.

A.11. If \( L \) is a subring of a ring \( R \), and \( N \) is an ideal of \( R \), then the residue class ring \( L/L \cap N \) is isomorphic to the subring \( (L+N)/N \) of the residue ring \( R/N \). ([16], Vol. 1, Theorem 8, page 144).

Quadratic Extensions of the Rationals.

A.12. Let \( R^{1} \) denote the integral closure of \( R = \mathbb{Z}_{(p)} \) in a quadratic extension \( K \) of the field of rational numbers. Then
(1) the factorization of $R'p$ into prime ideals of $R'$ is either

(i) $R'p = P$ with $[R'/P : \mathbb{Z}/(p)] = 2$,

or (ii) $R'p = P^2$ with $R'/P = \mathbb{Z}/(p)$,

or (iii) $R'p = P_1P_2$ with $R'/P_1 = R'/P_2 = \mathbb{Z}/(p)$.

(2) $Z(p)$ is a discrete rank one valuation ring with group of divisibility $G$ order isomorphic to the totally ordered group of integers $\mathbb{Z}$. The index of $G$ in a group of divisibility of a valuation ring extending $Z(p)$ in $K$ is one in case $R'p = P$ or $R'p = P_1P_2$, and is two in case $R'p = P^2$.

(3) $R'$ is either a valuation ring or the intersection of two valuation rings. ([16], Vol I, page 287).

(4) For each prime $p$, there exist quadratic extensions of the rationals such that (i), (ii), (iii) of (1) hold. (This follows from ([16], Vol. I, Theorem 32, page 313.).)

(5) The subrings $R + R'p^n$ of $R'$ are all of the subrings of $R'$ containing $Z(p)$ . (Unpublished notes of R. L. Pendleton).

A.13. Let $R'$ be the integral closure of $Z(p)$ in a quadratic extension of the rationals. Then $U(R'/R'p^n) \approx \mathbb{Z}/(p^2-1)$, if $R'p = P$, $p \geq 2$, $n = 1$;

$\mathbb{Z}/(p^2-1) \times \mathbb{Z}/(p^{n-1}) \times \mathbb{Z}/(p^{n-1})$, if $R'p = P$, $p \geq 3$, $n \geq 2$;

$\mathbb{Z}/(3) \times \mathbb{Z}/(2) \times \mathbb{Z}/(2^{n-2}) \times \mathbb{Z}/(2^{n-2})$, if $R'p = P$, $p = 2$, $n \geq 2$;

$\mathbb{Z}/(p-1) \times \mathbb{Z}/(p^n) \times \mathbb{Z}(p^n)$, if $R'p = P^2$, $p \geq 3$, $n \geq 1$;

$\mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(2^{n-1}) \times \mathbb{Z}/(2^{n-1})$, if $R'p = P^2$,

$p = 2$, and $R'p = P$ with $\pi^2 \notin Z(p)$, $n \geq 1$;

$\mathbb{Z}/(2^n) \times \mathbb{Z}/(2^{n-1})$, if $R'p = P^2$, $p = 2$ and $R'p = P$ with $\pi^2 \notin Z(p)$, $n \geq 1$;

$\mathbb{Z}/(p-1) \times \mathbb{Z}/(p-1) \times \mathbb{Z}/(p^{n-1}) \times \mathbb{Z}/(p^{n-1})$, if $R'p = P_1P_2$, $p \geq 3$, $n \geq 1$;

[0], if $R'p = P_1P_2$, $p = 2$, $n = 1$;

$\mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(2^{n-2}) \times \mathbb{Z}/(2^{n-2})$, if $R'p = P_1P_2$, $p = 2$, $n \geq 2$. 
\(P, P_1, P_2\) denote maximal ideals of \(R^i\) lying over \((p)\).

**Proof.** If \(R^i p = P_1 P_2\), then \(R^i\) has exactly two maximal ideals \(P_1, P_2\). Then \(R^i / R^i p^n = R^i / (P_1 P_2)^n \approx R^i / P_1^n \times R^i / P_2^n\) canonically and \(U(R^i / R^i p^n) \approx U(R^i / P_1^n) \times U(R^i / P_2^n)\). Since \(R^i / P_i, i = 1,2\), is finite, we can apply A.9 (ii) to each of the local rings \(R^i / P_i^n\). From A.9 and A.12, we have the following:

\[
\begin{align*}
U(R^i / R^i p^n) & \approx \mathbb{Z}/(p^2-1) \times (1+R^i p)/(1+R^i p^n), \text{ if } R^i p = P; \\
U(R^i / R^i p^n) & \approx \mathbb{Z}/(p-1) \times (1+R^i p)/(1+R^i p^n), \text{ if } R^i p = P^2 \text{ and } p \geq 3; \\
U(R^i / R^i p^n) & \approx (1+R^i p)/(1+R^i p^n), \text{ if } R^i p = P^2, p = 2; \\
U(R^i / R^i p^n) & \approx \mathbb{Z}/(p-1) \times \mathbb{Z}/(p-1) \times (1+R^i P_1 P_2)/(1+(P_1 P_2)^n), \text{ if } R^i p = P_1 P_2, p \geq 3; \\
U(R^i / R^i p^n) & \approx (1+P_1 P_2)/(1+(P_1 P_2)^n), \text{ if } R^i p = P_1 P_2, p = 2.
\end{align*}
\]

Thus, we must determine the second factors of \(U(R^i / R^i p^n)\).

From A.9(i), we have the following:

\[
\begin{align*}
\text{card } U(R^i / R^i p^n) & = (p^2-1)(p^2)^{n-1}, \text{ if } R^i p = P; \\
\text{card } U(R^i / R^i p^n) & = (p-1)(p)^{2n-1}, \text{ if } R^i p = P^2; \\
\text{card } U(R^i / R^i p^n) & = (p-1)(p)^{n-1}(p-1)(p)^{n-1}, \text{ if } R^i p = P_1 P_2.
\end{align*}
\]

Thus, \(\text{card } (1+R^i p)/(1+R^i p^n) = p^{2n-2}\), if \(R^i p = P\); \(\text{card } (1+R^i p)/(1+R^i p^n) = p^{2n-1}\), if \(R^i p = P^2\); \(\text{card } (1+R^i p)/(1+R^i p^n) = p^{2n-2}\), if \(R^i p = P_1 P_2\).

Suppose first that \(p \geq 3\).

If \(R^i p = P\) or \(R^i p = P_1 P_2\), let \(\pi = \mu p\), where \(\mu \in U(R^i)\), \(\mu \in R^i p\), \(\pi \notin R^i p^2\). \((1+\mu p)^{P_n} = 1+ p^n, \mu p^r+...+(\mu p)^{P_r}+(\mu p)^P^n\). Write \(r = p^t s\) where \(p\) and \(s\) are relatively prime. Then \(\binom{P_n}{r}\) is a multiple of \(p^{n-t}\), and since \(p^t > t\), \(\mu p^r \in R^i p^{t+1}\). Thus, \(\binom{P_n}{r}(\mu p)^r \in R^i p^{n+1}\).
Therefore, \((1 + \mu p)^p^n \equiv 1 \pmod{p^{n+1}}\). \((1 + \mu p)^{p^{n-1}} \neq 1 \pmod{p^{n+1}}\), because, for \(r > 1\), \(p^r = p^{p^t} \in R'p^{t+2}\); thus, \((p^2)^{p^{n-1}}(\mu p)^2 + ... + (\mu p)^{p^{n-1}} \in R'p^{n+1}\), and hence \((1 + \mu p)^{p^{n-1}} = 1 + p^n(\mu + pa), a \in R'\), implies \(\mu + pa \in \mathbb{U}(R')\) since \(\mu \in \mathbb{U}(R')\) and \(pa \in J(R')\), the Jacobson radical of \(R'\). Thus, we conclude that every element of \((1 + R'p)/(1 + R'p^n)\) is of order \(p^{n-1}\) or \(p^i\) where \(i < n - 1\).

Suppose that \(R'p = p^2\). By A.8, \(1+p\) generates a cyclic group of order \(p^{n-1}\) in \((1+p)/(1+R'p^n)\). Let \(\pi \not\in p^2\). \((1+\pi)^p = 1 + p^n \pi + ... + (p^r)^{p^{n-1}}p^n\). Arguing as in the previous paragraph, we obtain \((1+\pi)^p = 1 \pmod{p^n}\), \((1+\pi)^{p^{n-1}} \neq 1 \pmod{R'p^n}\). Thus, \((1+p)/(1+R'p^n)\) has a cyclic subgroup of order \(n-1\) and a cyclic subgroup of order \(n\).

Now assume that \(p = 2\). If \(n = 1\), the result is immediate from A.9 and the fact that the group of units of a finite field \(F\) is a cyclic group of order \(p^n - 1\), where \(p^n\) is the cardinality of \(F\).

Assume \(n \geq 2\).

If \(R'p = P\) or \(R'p = P_1P_2\), let \(\pi = \mu p\), where \(\mu \in \mathbb{U}(R')\); \(\pi \not\in R'p^2\).

\[
(1 + \pi)^2^{n-2} = 1 + 2^{n-2} \pi^2 + ... + (2^{n-2})^r (\pi^r)^r + ... + (\pi^2)^{2^{n-2}} = 1 + 2^{n-2} \mu^2 + ... + (2^{n-2})^r \cdot \mu^{2r} \cdot 2^{2r} + ... + (\mu^{2^{n-1}})^2^{n-1}
\]

\(\in 1 + R'p^n\), \(p = 2\).

\[
(1 + \pi)^2^{n-3} \not\in 1 + R'p^n : \text{write } r = p^{t} s, \text{where } s \text{ is odd, } p = 2.
\]

For \(r > 1\), \(p^r = p^{p^{t}} s\), \((1 + \pi)^2^{n-3} = 1 + 2^{n-1} \mu^2 + 2^n a\), as in the \(p \geq 3\) case.

\(1 - 2 = -1\) generates a cyclic subgroup of order two in
\[(1 + R'p)/(1 + R'p^2) \cdot \overline{\gamma} = (1 + \pi^2)^j\] implies \(j = 2^{n-3}\), and hence that
\[-(1 + \pi^2)^2 \epsilon 1 + R'p^n,\] which is a contradiction for \(n > 2\). For \(n = 2\), let \(1 + ap \epsilon (1 + R'p)/(1 + R'p^2)\). \((1 + ap)^2 = 1 + 2ap + a^2p^2 = 1 (p^2)\) for \(p = 2\). Hence, every element \(\neq 1\) of \((1 + R'p)/(1 + R'p^2)\) is of order two. \((1 + 2)^{2n-2} = 1 + 2^{n-2} + 2^{n-2} + \ldots + (2^{n-2})^{2n-2}\) 
\[= 1 + 2^{n-1} + \ldots + (2^{n-2})^{2n-2} + \ldots + 2^{n-2} + \ldots + 2^{n-2} + \ldots + 2^{n-2}.\] 
\((2^{n-2})^{2^n} \epsilon R'p^n\) for \(r > 2, p = 2\), and \((2^{n-2})^{2^n} \epsilon R'p^n, \neq R'p^n, p = 2.\) Thus, \((1 + 2)^{2n-2} = 1 + 2^{n-1}(1 + (2^{n-2} - 1) + 2c)\) for some \(c, n > 2\), implies \((1 + 2)^{2n-2} \epsilon 1 + R'p^n; (1 + 2)^{2n-2} \epsilon 1 + R'p^{n+1}\). Moreover, \(1 + 2 \neq 1 + \pi^2\). Thus, \((1 + R'p)/(1 + R'p^n)\) has two subgroups of order \(2^{n-2}\).

Now suppose \(R'p = p^2, p = 2.\) Suppose that \(\pi^2 \epsilon Z(p)\). By [16], Vol. 1, Theorem 32, page 313, and Theorem 34, page 317), we can take \(\pi = 1 + \sqrt{d}\) where 2 does not divide \(d\) and \(d\) is square-free. Then \(1 + \pi = \sqrt{d}\) is of order \(2^{n-1}\) in \((1 + p)/(1 + R'p^n); (1 + 2)\) is of order \(2^{n-1}\) in \((1 + p)/(1 + R'p^n)\). \(2^{n-1} = -1 = 1 - 2\) and \(2^{n-1} = 1 + 2(2^{n-2} - 1)\) each generate groups of order two in \((1 + p)/(1 + R'p^n)\).

Suppose \(\pi^2 \epsilon Z(p)\). Then \((1 + \pi)^{2^n} = 1 + 2^n\pi + \ldots + (2^{n})^{\pi + \ldots + \pi^{2^n}}\) 
\[= 1 + \pi^{2n=1} + \ldots + (2^{n})^{\pi + \ldots + \pi^{2^n}} \epsilon p^{2n+1} \subseteq p^{2n} = R'p^n, \neq R'p^{n+1}.\] 
\(1 + 2\pi \) is of order \(2^{n-1}\) in \((1 + p)/(1 + R'p^n)\). \(1 + 2\pi = (1 + \pi)^j\) implies \(j = 2;\) then \(1 + 2\pi = 1 + 2\pi + \pi^2\) implies \(2 \epsilon R'p^n\), which is contradictory.
for \( n > 1 \). If \( n = 1 \), then 
\[
(1 + \mu \pi)^2 = 1 + 2\mu \pi + \mu^2 \pi^2 = \n
1 + 2u(\pi + 2u) \quad (\pi^2 = 2) \] 
implies \( 1 + \mu \pi \) is of order two, for any \( \mu \in R^1 \), in \((1 + P)/(1 + R^1 P)\).
VITA

Dolores Richard Spikes was born on August 24, 1936, in Baton Rouge, Louisiana. She attended the parochial and public schools of Baton Rouge. In 1957, she received the Bachelor of Science Degree from Southern University and in 1958 she received the Master of Science degree in mathematics from the University of Illinois. At present she is a candidate for the degree of Doctor of Philosophy in the department of mathematics at Louisiana State University.
Candidate: Dolores Richard Spikes

Major Field: Mathematics

Title of Thesis: Semi-valuations and Groups of Divisibility

Approved:

[Signatures]

Major Professor and Chairman

Dean of the Graduate School

EXAMINING COMMITTEE:

[Signatures]

Date of Examination:

11-17-1971