# VALUATIONS AND VALUATION RINGS

THESIS

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

For the Degree of

MASTER OF SCIENCE

By

Sig H. Badt, B.S.
Denton, Texas
Aug., 1975

Badt, Sig H., Valuations and Valuation Rings. Master of Science, (Mathematics), Aug., 1975, 42 pp, bibliography, 1 title.

This paper is an investigation of several basic properties of ordered Abelian groups, valuations, the relationship between valuation rings, valuations, and their value groups and valuation rings.

The proofs to all theorems stated without proof can be found in Zariski and Samuel, Commutative Algebra, Vol. I, 1858.

In Chapter I several basic theorems which are used in later proofs are stated without proof, and we prove several theorems on the structure of ordered Abelian groups, and the basic relationships between these groups, valuations, and their valuation rings in a field. In Chapter II we deal with valuation rings, and relate the structure of valuation rings to the structure of their value groups.

# PREFACE

This thesis presents some basic theorems on ordered Abelian groups, then theorems on the relationship between these groups and their associated valuation rings, and finally theorems on valuation rings alone. In the beginning of Chapter I we will present several standard theorems which will be assumed without proof. The proofs of these theorems may be found in Zariski and Samuel, Commutative Algebra, Vol. I, 1958. The remainder of Chapter I will be devoted to properties of value groups and valuations.

In Chapter II we will begin with theorems relating the structure of valuation rings to the structure of their value groups. Then we will prove some theorems on valuation rings.

All definitions will be placed immediately before they are to be used. Notation conventions used in this thesis may also be found in Zariski and Samuel.

TABLE OF CONTENTS

# CHAPTER I

## THEOREMS ASSUMED WITHOUT PROOF AND SOME THEOREMS ON VALUATIONS

The following theorems, one through nine, will be used later, but for reasons of economy their proofs will not be shown. They are listed in the order in which they will be used.

<u>Definition 1.1</u>: An ordered Abelian group, denoted $(G,+,\leq)$ is an Abelian group G on which there is defined a total ordering $\leq$ such that if $\alpha,\beta,\gamma \in G$ and $\alpha \leq \beta$ then $\alpha + \gamma \leq \beta + \gamma$.

Any subgroup of an ordered Abelian group with the induced ordering is an ordered Abelian group.

<u>Definition 1.2</u>: If $G_1, G_2, \ldots, G_n$ are all subgroups of a group G such that for any $i,j \in \{1,2,\ldots,n\}$ where $i \neq j$, $G_i \cap G_j = \{0\}$. Then

$$G_i \oplus G_2 \oplus \ldots \oplus G_n = \{(g_1,\ldots,g_n) | g_i \in G_i \text{ for } i = 1,\ldots,n\}$$

is called the <u>direct sum</u> of $G_1$, through $G_n$, and it is a group with pointwise addition.

<u>Theorem 1.1</u>: If $G_1,\ldots,G_n$ are ordered Abelian groups, and $G = G_1 \oplus G_2 \oplus \ldots \oplus G_n$ so the elements of G may be denoted by n-tuplet $(\alpha_1,\alpha_2,\ldots,\alpha_n)$ where each $\alpha_i \in G$ and

if $(\alpha_1,\ldots,\alpha_n)$ and $(\beta_1,\ldots,\beta_n)$ are distinct elements of G, then

$$(\alpha_1,\ldots,\alpha_n) < (\beta_1,\ldots,\beta_n)$$

if $\alpha_1 < \beta_1$ or for some $k > 1$, $\alpha_i = \beta_i$ for $i = 1,\ldots,k-1$ and $\alpha_k < \beta_k$. Then $\leq$ is a total order on G and G is an ordered Abelian group.

*Definition 1.3*: The above ordering is called the *lexicographic ordering*.

*Definition 1.4*: A valuation ring is a domain D with $1 = 0$, and quotient field K such that if $x \in K$ either $x \in D$ or $\frac{1}{x} \in D$.

*Theorem 1.2*: If A is an ideal in a valuation ring D, then $\bigcap_{n=1}^{\infty} A^n$ is prime.

To say that an ideal Q in a ring R is *primary* means that if $a,b \in R$, and $a \notin Q$ then $b^n \in Q$ for some n. And if an ideal Q is primary and $P = \sqrt{Q}$, then P is prime and Q is said to be *P primary*.

*Theorem 1.3*: If Q is P primary in a ring, and A and B are ideals in R such that $AB \subset Q$ and $A \not\subset Q$, then $B \subset P$.

*Theorem 1.4*: If Q and P are ideals in a ring R such that P is prime and $Q \subset P$, then $\sqrt{Q} \subset P$.

A domain D is quasi-local if it contains exactly one maximal ideal M, such that $(0) < M < D$.

*Theorem 1.5*: In a quasi-local domain the maximal ideal is the set of nonunits.

This is an ordered semigroup in the sense that if $\alpha, \beta, \gamma \in G^*$ and $\alpha \leq \beta$ then $\alpha + \gamma \leq \beta + \gamma$.

Definition 1.6: Let K be a field. A valuation on K is a mapping from K onto $G^*$, where G is an ordered Abelian group such that

i) $v(a) = \infty$ iff $a = 0$

ii) $v(ab) = v(a) + v(b)$ for any $a,b \in K$

iii) $v(a+b) \geq \min(v(a), v(b))$ for any $a,b \in K$.

Definition 1.7: G is called the value group of the valuation v.

Given a field K and $G^*$ if $v(a) = 0$ for any $a \neq 0$, and $v(0) = \infty$, v is called the trivial valuation.

Theorem 1.10: If K is a field and v is a valuation with value group G, then

i) $v(1) = v(-1) = 0$, 0 being the identity in G

ii) $v(\frac{1}{a}) = -v(a)$, for any $a \in K$, $a \neq 0$.

Proof: i) Since $v(1) = v(1 \cdot 1) = v(1) + v(1)$, $v(1)$ is the unique identity in G.

From this we get

$$0 = v(1) = v((-1)(-1)) = v(-1) + v(-1).$$

If $v(-1) < 0$, we get the contradiction $0 = v(-1) + v(-1) < 0$. If $v(-1) > 0$, we get $0 = v(-1) + v(-1) > 0$. Therefore $v(-1) = 0$, too.

ii) For any $a \in K$, $a \neq 0$

$$0 = v(1) = v(a \cdot \frac{1}{a}) = v(a) + v(\frac{1}{a}).$$

Therefore $-v(a) = v(\frac{1}{a})$.

Theorem 1.11: If K is a field with value group G, let $V = \{a | a \in K, \text{ and } v(a) \geq 0\}$. Then V is a valuation ring.

Proof: First we must prove V is a ring. To get closure under addition, if $a,b \in V$, $v(a) \geq 0$, and $v(b) \geq 0$, then $v(a+b) \geq \min(v(a),v(b)) \geq 0$. To get additive inverses, for any $a \in V$, notice $-1 \in V$, so

$$v(-a) = v((-1)a) = v(-1) + v(a) = 0 + v(a) \geq 0,$$

and $-a \in V$. Clearly $0 \in V$ since $v(0) = \infty \geq 0$. Commutativity and associativity under addition and multiplication are inherited from K. To get closure under multiplication, if $a,b \in V$, then $v(a) \geq 0$, and $v(b) \geq 0$, and $v(ab) = v(a) + v(b)$. Since $v(a) \geq 0$, $v(a) + v(b) \geq 0 + v(b) = v(b) \geq 0$. Distributivity is inherited from K. Therefore V is a ring.

If $a \in K$ and $a \notin V$, $v(a) < 0$. So, $a \neq 0$. If $v(\frac{1}{a}) < 0$, we would have the contradiction

$$0 = v(1) = v(a \cdot \tfrac{1}{a}) = v(a) + v(\tfrac{1}{a}) < 0.$$

So $v(\frac{1}{a}) \geq 0$, and $\frac{1}{a} \in V$. Therefore V is a valuation ring.

Theorem 1.12: If V is a valuation ring with quotient field K, then there exists a valuation v on K such that

$$V = \{a | a \in K \text{ and } v(a) \geq 0\}.$$

Proof: Let U be the multiplicative group of units of V. Then U is a subgroup of $K^*$, the multiplicative group of nonzero elements of K.

Let $G = K^*/U$, and we write G additively such that if $a,b \in K^*$, $aU + bU = abU$. We define a relation on G such that if $a,b \in K^*$, $bU \leq aU$ if and only if $\frac{a}{b} \in V$.

We will show this relation is well defined. If $a, a', b, b' \in K^*$ such that $bU = b'U$ and $aU = a'U$, we need to show $bU \le aU$ if and only if $b'U \le a'U$. So, if $bU \le aU$, $\frac{a}{b} \in V$. Since $b'U \le bU$, $\frac{b}{b'} \in V$, and since $aU \le a'U$, $\frac{a'}{a} \in V$. Thus $\frac{a'}{b'} = \frac{a}{b} \cdot \frac{a'}{a} \cdot \frac{b}{b'} \in V$, and $b'U \le a'U$. Similarly if $b'U \le a'U$ then $bU \le aU$.

Next we will show that this relation is a total order on G.

To get $\le$ is reflexive for any $a, b \in K^*$ such that $aU = bU$, $\frac{a}{b} \in U$, (remember we are dealing with a group of cosets whose operation is $\cdot$ not $+$). Also $\frac{a}{b} \in V$ since $U \subset V$. Therefore $bU \le aU$.

To get $\le$ is antisymetric, for any $a, b \in K^*$ such that $aU \le bU$ and $bU \le aU$, since $aU \le bU$, $\frac{b}{a} \in V$, and since $bU \le aU$ $\frac{a}{b} \in V$. Therefore $\frac{b}{a} \in U$ and $aU = bU$.

To get $\le$ is transitive, for any $a, b, c \in K^*$ such that $aU \le bU$ and $bU \le cU$, $\frac{b}{a} \in V$ and $\frac{c}{b} \in V$, so

$$\frac{c}{a} = \frac{b}{a} \cdot \frac{c}{b} \in V,$$

and $aU \le cU$.

To get that any two elements are related, for any $a, b \in K^*$, consider either $\frac{a}{b}$ or $\frac{b}{a}$ is an element of V because V is a valuation ring. If $\frac{b}{a} \in V$, then $aU \le bU$. If $\frac{a}{b} \in V$, then $bU \le aU$.

Next we must show that $(G, +, \le)$ is an ordered Abelian group. If $a, b, c \in K^*$ such that $bU \le aU$, and $cU \in G$, since

$bU \le aU$, $\frac{a}{b} \in V$. So $\frac{ac}{bc} \in V$ and

$$bU + cU = bcU \le acU = aU + cU.$$

Now, define $v: K \to G^*$ by $v(0) = \infty$, and $v(a) = aU$ if $a \neq 0$.

We must show that v is a valuation.

Clearly $v(a) = \infty$ if and only if $a = 0$ by definition.

For any $a,b \in K$, if either a or b is zero, say $b = 0$,

$$v(a) + v(b) = v(a) + \infty = \infty = v(0) = v(ab).$$

If $a \neq 0$ and $b \neq 0$,

$$v(a) + v(b) = aU + bU = abU = v(ab).$$

For any $a,b \in K$, if either a or b is zero, say $b = 0$, $v(a) \le \infty = v(b)$, and $v(a+b) = v(a) = \min(v(a),v(b))$. If $a \neq 0$ and $b \neq 0$, then $aU, bU \in G$ so $aU \le bU$, or $bU \le aU$, say $bU \le aU$. So $v(b) \le v(a)$, and $\min(v(b),v(a)) = v(b)$. Also because $bU \le aU$, $\frac{a}{b} \in V$, so $\frac{a}{b} + 1 \in V$. If $\frac{a}{b} + 1 \neq 0$, since $\frac{\frac{a}{b}+1}{1} \in V$, $1U \le (\frac{a}{b} + 1)U$ and $v(1) \le v(\frac{a}{b} + 1)$. If $\frac{a}{b} + 1 = 0$, still $v(1) \le v(\frac{a}{b} + 1) = \infty$. From the fact that for any $c,d \in K$, $v(c) + v(d) = v(cd)$ we can get $v(1) = 0$. So in either case $v(\frac{a}{b} + 1) \ge 0$, and $v(\frac{a}{b} + 1) + v(b) \ge v(b)$, so

$$\begin{aligned} v(a+b) &= v((\tfrac{a}{b} + 1)b) \\ &= v(\tfrac{a}{b} + 1) + v(b) \ge v(b) = \min(v(a),b(b)). \end{aligned}$$

Finally we must show if $S = \{a \mid a \in K \text{ and } v(a) \ge 0\}$, then $S = V$. If $a \in S$, $aU = v(a) \ge 0 = v(1) = 1U$, so $a = \frac{a}{1} \in V$.

Therefore $S \subset V$. If $a \in V$, and if $a = 0$, $v(a) = \infty \geq 0$, so $a \in S$. If $a \neq 0$, $a = \frac{a}{1} \in V$, so $1U \leq aU$, and $0 = v(1) \leq v(a)$, so $a \in S$. Therefore $V \subset S$, and $V = S$.

Definition 1.8: A v as determined above is said to be the valuation determined by V.

Definition 1.9: If v and v' are valuations on a field K, with value group G and G' respectively, then v and v' are equivalent if and only if there is an order-preserving isomorphism $\phi$ from G onto G' such that $v'(a) = \phi(v(a))$ for any $a \in K^*$.

This relation is an equivalence relation. To show it is reflexive, for any valuation and value group G, let $\phi = I(G)$, the identity map on G. To show it is symmetric for any valuations v and v' with value groups G and G' respectively such that v is equivalent to v' there exists an order-preserving isomorphism $\phi: G \to G'$. So $\phi^{-1}: G' \to G$ is an isomorphism, and if $a', b' \in G'$ such that $a' \geq b'$ there exist $a, b \in G$ such that $\phi(a) = a'$, and $\phi(b) = b'$. It follows $a \geq b$ since if $a < b$ we would have the contradiction $a' = \phi(a) < \phi(b) = b'$. So $\phi^{-1}(a') = a \geq b = \phi^{-1}(b')$, and $\phi^{-1}$ is order-preserving. And, for any $x \in K^*$, $v'(x) = \phi(v(x))$ so $\phi^{-1}(v'(x)) = v(x)$. To show it is transitive, given valuations v, v', and v'' with value groups G, G', and G'' respectively, there exists order-preserving isomorphisms $\phi$ and $\theta$ such that $\phi: G \to G'$, and $\theta: G' \to G''$. So $\theta \circ \phi: G \to G''$

is an isomorphism. And if $a,b \in G$ such that $a \geq b$, then $\phi(a) \geq \phi(b)$, and $\theta\circ\phi(a) \geq \theta\ \phi(b)$. So $\theta\circ\phi$ is order-preserving. Also for any $x \subset K^*$, $v''(x) = \theta(v'(x))$, and $v'(x) = \phi(v(x))$, so $v''(x) = \theta\circ\phi(v(x))$.

Theorem 1.13: If K is a field, and v and v' are equivalent valuations on K with value groups G and G' respectively, and V is the valuation ring determined by v, and V' is the valuation ring determined by v', then $V = V'$.

Proof: There exsists $\phi: G \to G'$, and $\phi^{-1}: G' \to G$ both order-preserving isomorphisms onto such that for any $a \in K^*$, $v'(a) = \phi(v(a))$ and $v(a) = \phi^{-1}(v'(a))$. For any $b \in V$, if $b = 0$, $b \in V'$. If $b \neq 0$, $v(b) \geq 0$, and $v'(b) = \phi(v(b)) \geq \phi(0) = 0$. So $b \in V'$, and $V \subset V'$. Similarly $V' \subset V$, so $V = V'$.

Theorem 1.14: If K is a field and V is a valuation ring in K, and v is a valuation on G with value group G such that V is the valuation ring of v, and v' is the valuation determined by V, then v and v' are equivalent.

Proof: Let U be the group of units in V. Define $\phi: G \to K^*/U$ such that if $g \in G$, $g = v(a)$ for some $a \in K^*$, and $\phi(g) = \phi(v(a)) = aU$.

First we must show $\phi$ is well-defined. If $g, g' \in G$ such that $g = g'$, $g = v(a)$ and $g' = v(b)$ for some $a,b \in K^*$. So, $v(a) = v(b)$, and

$$0 = v(a) - v(b) = v(a) + v(\tfrac{1}{b}) = v(\tfrac{a}{b}).$$

For any $x \in K$ such that $v(x) = 0$, $x \in U$ since

$$0 = v(xx^{-1}) = v(x) + v(x^{-1}) = v(x^{-1})$$

so $x^{-1} \in V$, and $x$ is a unit in $V$.

Therefore $\frac{a}{b} \in U$, and $\phi(g) = aU = bU = \phi(g')$.

To show $\phi$ is a homomorphism, for any $g$, $g' \in G$ there exists $c,d \in K^*$ such that $g = v(c)$, and $g' = v(d)$, so

$$\begin{aligned}\phi(g+g') &= \phi(v(c) + v(d)) \\ &= \phi(v(cd)) \\ &= cdU \\ &= cU + dU \\ &= \phi(v(c)) + \phi(v(d)) \\ &= \phi(g) + \phi(g').\end{aligned}$$

To show $\phi$ is an injection, if $g \in G$ such that $\phi(g) = 0$, $g = v(a)$ for some $a \in K^*$, so $\phi(v(a)) = 0$ (the zero in $K^*/U$). Therefore $\phi(v(a)) = U$, so $aU = U$, and $a \in U$.

For any $x \in U$, $v(x) = 0$, since if $x \in U$ then there exists $x^{-1} \in V$, and since $x \in V$, $v(x) \geq 0$, but if $v(x) > 0$, we get $v(x^{-1}) = -v(x) < 0$ which contradicts $x^{-1} \in V$, so $v(x) = 0$.

Therefore $g = v(a) = 0$, and $\phi$ is an injection.

For any $z \in K^*/U$, $z = aU$ for some $a \in K^*$. Therefore $v(a) \in G$ such that $\phi(v(a)) = z$, and $\phi$ is onto.

To show $\phi$ is order-preserving, for any $g,g' \in G$ such that $g \leq g'$, $g = v(a)$, and $g' = v(b)$ for some $a,b \in K^*$. Since $v(a) = g \leq g' = v(b)$, $0 \leq v(b) - v(a) = v(b) + v(\frac{1}{a}) = v(\frac{b}{a})$, so $\frac{b}{a} \in V$. Therefore,

$$\phi(g) = \phi(v(a)) = aU \leq bU = \phi(v(b)) = \phi(g').$$

As an immediate corallary to Theorem 1.14, we can say if $v$ and $v'$ are valuations on a field $K$ having the same valuation ring, $v$ and $v'$ are equivalent.

Also from Theorem 1.14, we have, if $U$ is the set of units in $V$, $U = \{a \in K | v(a) = 0\}$.

Definition 1.10: If $G$ is an ordered Abelian group, a subgroup $H$ of $G$ is an isolated subgroup if and only if for each $\alpha \in H$ if $\beta \in G$ and $0 \leq \beta \leq \alpha$ then $\beta \in H$. If $H \neq G$, then $H$ is a proper isolated subgroup.

Definition 1.11: If an ordered Abelian group $G$ has only a finite number of isolated subgroups, then the number of proper isolated subgroups of $G$ is the rank of $G$.

So $G$ is of rank one if and only if $G \neq 0$ and $G$ and $0$ are the only isolated subgroups of $G$.

Theorem 1.15: If $G$ is a nonzero ordered Abelian group, then $G$ has rank one if and only if there is an order-preserving isomorphism from $G$ onto a subgroup of the additive group of real numbers.

Proof: If there is an order-preserving isomorphism $\phi$ from $G$ onto a subgroup $G'$ of the additive group of real numbers, let $H'$ be a nonzero isolated subgroup in $G'$.

There exists $\alpha' \in H'$ such that $\alpha' \neq 0$. Either $\alpha'$ or $-\alpha'$ is positive. Without loss of generality, assume $\alpha'$ is positive. If $\beta' \in G'$, and $\beta' \geq 0$, there exists a positive integer $n$ such that $n\alpha' \geq \beta' \geq 0$, and $n\alpha' \in H'$, so $\beta \in H'$. It follows $H' = G'$ and $G'$ has rank one.

If H is a nonzero isolated subgroup of G, $\phi(H)$ is a nonzero subgroup of G'. For any $\alpha' \in \phi(H)$ and for any $\beta' \in G'$ such that $0 \leq \beta' \leq \alpha'$ there exists $\alpha, \beta \in G$ such that $\phi(\alpha) = \alpha'$ and $\phi(\beta) = \beta'$. Since $0 \leq \beta \leq \alpha$, $\beta \in H$, so $\beta' \in \phi(H)$, and $\phi(H)$ is an isolated subgroup of G'. Therefore $\phi(H) = G'$ and $H = G$, so G has rank one.

Conversely, if G has rank one we first want to show that for any $\alpha, \beta \in G$ such that $\alpha > 0$ and $\beta > 0$ there exists a natural number n such that $\beta \leq n\alpha$. If not, there exists $\alpha, \beta \in G$ such that $\alpha > 0$ and $\beta > 0$, and $\beta > n\alpha$ for any natural number n. Let

$$S = \{\gamma \in G \mid \gamma \geq 0, \text{ and } \gamma \leq n\alpha \text{ for some natural number } n\},$$

and notice $\beta \notin S$. Also, if $\gamma_1, \gamma_2 \in S$, clearly $\gamma_1 + \gamma_2 \in S$, so if H is the subgroup of G generated by S,

$$H = \{\gamma_1 - \gamma_2 \mid \gamma_1, \gamma_2 \in S\}.$$

For any $h \in H$ and for any $\delta \in G$ such that $0 \leq \delta \leq h$ since $h = \gamma_1 - \gamma_2$ for some $\gamma_1, \gamma_2 \in S$, and $\gamma_1 \leq n\alpha$ for some natural number n, and $\gamma_2 \geq 0$, so

$$\delta \leq \delta + \gamma_2 \leq h + \gamma_2 = (\gamma_1 - \gamma_2) + \gamma_2 = \gamma_1 \leq n\alpha,$$

so $\delta \in S$ and $\delta \in H$. So, H is an isolated subgroup of G, and $H \neq 0$. Therefore $H = G$ which leads to a contradiction since $\beta \in G$, so $\beta \in H$, and $0 \leq \beta \leq \beta$, so by the same argument as we used just above, $\beta \in S$, but $\beta \notin S$.

If there exists a least positive element $\alpha$ of G for any $\beta \in G$, there exists n such that $(n-1)\alpha < \beta \leq n\alpha$. From this $0 < \beta - (n-1)\alpha \leq \alpha$ but since $\alpha$ is the least positive element in G, $\beta - (n-1)\alpha = \alpha$, and $\beta = n\alpha$. So $G = (\alpha)$. Let $\phi(n\alpha) = n$ for any natural number n. Clearly $\phi$ is an isomorphism. For any two natural numbers $n_1$ and $n_2$, if $n_1\alpha \leq n_2\alpha$, $n_1 \leq n_2$ since if $n_1 > n_2$ we get this contradiction

$$n_1\alpha = n_2\alpha + (n_1-n_2)\alpha > n_2\alpha.$$

So $\phi(n_1\alpha) \leq \phi(n_2\alpha)$ and $\phi$ is order-preserving.

If G has no least positive element, choose one $\alpha \in G$ and consider it fixed. Let $\phi(\alpha) = 1$. If $\beta \in G$ such that $\beta > 0$, and $\beta \neq \alpha$ let

$$l(\beta) = \{\tfrac{m}{n} | m\alpha \leq n\beta, \text{ m and n natural numbers}\}$$

and

$$u(\beta) = \{\tfrac{m}{n} | m\alpha > n\beta, \text{ m and n natural numbers}\}.$$

There exist natrual numbers p and q such that $\alpha \leq p\beta$ and $\beta < q\alpha$. So, $\frac{1}{p} \in l(\beta)$ and $\frac{q}{1} \in u(\beta)$, and $l(\beta) \neq \phi$ and $u(\beta) \neq \phi$.

If $\frac{m}{n} \in l(\beta)$ and $\frac{h}{k} \in u(\beta)$, $m\alpha \leq n\beta$ and $k\beta < h\alpha$, so $m\alpha k\beta < n\beta h\alpha$, and $mk < nh$, so $\frac{m}{n} < \frac{h}{k}$. Clearly

$$[l(\beta) \cup \{q \in Q | q \leq 0\}] \cup u(\beta) = Q.$$

Thus we have a Dedekind cut of the rational numbers. Let $\phi(\beta)$ be this positive real number, and let $\phi(0) = 0$, and if $\gamma \in G$ such that $\gamma < 0$, let $\phi(\gamma) = -\phi(-\gamma)$.

Next we want to show $\phi(\beta_1+\beta_2) \geq \phi(\beta_1) + \phi(\beta_2)$ for any $\beta_1, \beta_2 \in G$ such that $\beta_1 > 0$ and $\beta_2 > 0$. If not,

$$\phi(\beta_1+\beta_2) < \phi(\beta_1) + \phi(\beta_2)$$

for some $\beta_1 > 0$ and $\beta_2 > 0$. So,

$$\begin{aligned}
\mathrm{glb}(u(\beta_1+\beta_2)) &= \phi(\beta_1+\beta_2) \\
&< \phi(\beta_1) + \phi(\beta_2) \\
&= \mathrm{lub}(l(\beta_1)) + \mathrm{lub}(l(\beta_2)) \\
&= \mathrm{lub}\{x+y \mid x \in (\beta_1),\ y \in l(\beta_2)\}.
\end{aligned}$$

So, there exists $\frac{p}{q} \in u(\beta_1+\beta_2)$, and $\frac{p_1}{q_1} \in l(\beta_1)$ and $\frac{p_2}{q_2} \in l(\beta_2)$

such that

$$\frac{p}{q} < \frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1q_2 + p_2q_1}{q_1q_2}$$

so

$$p(q_1q_2) < q(p_1q_2 + p_2q_1)$$

and

$$(q_1q_2)\alpha p < (p_1q_2 + p_2q_1)q\alpha.$$

Since $\frac{p}{q} \in u(\beta_1+\beta_2)$,

$$p\alpha > q(\beta_1+\beta_2)$$

and

$$(q_1q_2)\alpha p > (\beta_1+\beta_2)(q_1q_2)q.$$

Since $\frac{p_1}{q_1} \in (\beta_1)$ and $\frac{p_2}{q_2} \in (\beta_2)$, $p_1\alpha \le q_1\beta_1$, and $p_2\alpha \le q_2\beta_2$, and

$$p_1\alpha q_2 + p_2\alpha q_1 \le (q_1q_2)\beta_1 + (q_1q_2)\beta_2,$$

so

$$(p_1q_2+p_2q_1)\alpha q \le (\beta_1+\beta_2)(q_1q_2)q,$$

which leads to the contradiction

$$\begin{aligned}
(\beta_1+\beta_2)(q_1q_2)q &\ge (p_1q_2+p_2q_1)\alpha q \\
&> (q_1q_2)\alpha p \\
&> (\beta_1+\beta_2)(q_1q_2)q.
\end{aligned}$$

By a similar argument $\phi(\beta_1+\beta_2) \leq \phi(\beta_1) + \phi(\beta_2)$, so $\phi(\beta_1+\beta_2) = \phi(\beta_1) + \phi(\beta_2)$. It follows quickly $\phi$ is a homomorphism.

If $\beta_1, \beta_2 \in G$ such that $\beta_1 > 0$, $\beta_2 > 0$, and $\phi(\beta_1) > \phi(\beta_2)$, $\mathrm{lub}(1(\beta_1)) > \mathrm{glb}(u(\beta_2))$. There exist $\frac{p_1}{q_1} \in 1(\beta_1)$ and $\frac{p_2}{q_2} \in u(\beta_2)$ such that $\frac{p_1}{q_1} > \frac{p_2}{q_2}$. So $p_1q_2 > p_2q_1$, and $p_1q_2\alpha > p_2q_1\alpha$. Since $\frac{p_1}{q_1} \in 1(\beta_1)$ and $\frac{p_2}{q_2} \in u(\beta_2)$, $p_1\alpha \leq q_1\beta$ and $p_2\alpha > q_2\beta_2$, so $q_2p_1\alpha \leq q_1q_2\beta_1$ and $q_1p_2\alpha > q_1q_2\beta_2$. Therefore

$$q_1q_2\beta_1 \geq q_2p_1\alpha > p_2q_1\alpha > q_1q_2\beta_2$$

and $\beta_1 > \beta_2$, so $\phi$ is order-preserving.

For any $\gamma \in G$ such that $\gamma \neq 0$ if $\gamma > 0$ there exists n such that $n\gamma > \alpha$, so $\frac{1}{n} \in 1(\gamma)$ and $\phi(\gamma) > \frac{1}{n} > 0$. If $\gamma < 0$, $\phi(-\gamma) > 0$, and $-\phi(\gamma) > 0$, so $\phi(\gamma) < 0$. So, $\ker(\phi) = 0$, and $\phi$ is an isomorphism.

## CHAPTER II

## THEOREMS ON VALUATION RINGS

Theorem 2.1: If R is a ring, the following are equivalent:

1) For any sequence of ideals $A_1, A_2, \ldots$ in R with $A_1 \subset A_2 \subset \ldots$ there exists a natural number n such that for all $m \geq n$, $A_n = A_m$.

2) Any nonempty set of ideals in R has a maximal element.

3) Every ideal in R is finitely generated.

Proof: First, if part 1) is true, assume there exists a nonempty set S of ideals which contains no maximal element. Since $S \neq \phi$ there exists an ideal $A_1 \in S$. $A_1$ is not maximal so there exists $A_2 \in S$ such that $A_1 < A_2$. $A_2$ is not maximal so there exists $A_3 \in S$ such that $A_2 < A_3$. Clearly we can construct

$$A_1 < A_2 < \ldots$$

which contradicts part 1).

Second, if part 2) is true, assume there exists an ideal A in R such that A is not finitely generated. Let

$$S = \{(a_1, a_2, \ldots, a_n) \mid n \text{ is a positive integer and } a_1, a_2, \ldots a_n \in A\}.$$

Since $A \neq \phi$, $S \neq \phi$. There exists $a_1, a_2, \ldots, a_n \in A$ such that $(a_1, a_2, \ldots, a_n)$ is maximal in A. Since

$a_1,a_2,\ldots,a_n \in A$, $(a_1,a_2,\ldots,a_n) \subset A$, and since A is not finitely generated $(a_1,a_2,\ldots,a_n) \neq A$ so $(a_1,a_2,\ldots,a_n) < A$. So there exists $a \in A\backslash(a_1,a_2,\ldots,a_n)$ which leads to $(a_1,a_2,\ldots,a_n,a) \in S$ and $(a_1,a_2,\ldots,a_n) < (a_1,a_2,\ldots,a_n,a)$ which contradicts $(a_1,a_2,\ldots,a_n)$ is maximal in S.

Finally, assume part 3) is true, and let $A_1,A_2,\ldots$ be any sequence of ideals in R such that $A_1 \subset A_2 \subset \ldots$ . Let $A = \bigcup_{i=1}^{\infty} A_1$. For any $a \in A$, and $r \in R$, $a \in A_\ell$ for some $\ell$, so $ar \in A_\ell$, and $ar \in A$. If $a_1,a_2 \in A$, $a_1 \in A_{\ell_1}$, and $a_2 \in A_{\ell_2}$ for some positive integers $\ell_1$ and $\ell_2$. Without loss of generality, assume $A_{\ell_1} \subset A_{\ell_2}$. Since $a_1 \in A_{\ell_2}$, $a_1 - a_2 \in A_{\ell_2}$, and $a_1 - a_2 \in A$. So A is an ideal and therefore there exists $a_1,a_2,\ldots a_n \in A$ such that $(a_1,a_2,\ldots,a_n) = A$. There exist natural numbers $\ell_1,\ell_2,\ldots,\ell_n$ such that $a_1 \in A_{\ell_1}$, $a_2 \in A_{\ell_2},\ldots,a_n \in A_{\ell_n}$. Let $m = \max(\ell_1,\ell_2,\ldots,\ell_m)$. For $i = 1,2,\ldots,n, A_{\ell_1} \subset A_m$, so $a_1,a_2,\ldots a_n \in A_m$ and $A \subset A_m$. For any natural number $\ell$ such that $\ell \geq m$, $A_m \subset A_\ell \subset A \subset A_m$, so $A_m = A_\ell$.

<u>Definition 2.1</u>: A ring with these three equivalent conditions is called <u>Noetherian</u>.

<u>Definition 2.2</u>: An ideal A is <u>irreducible</u> if and only if A is not a finite intersection of ideals strictly containing A.

Theorem 2.2: If $A$ is an ideal in a Noetherian ring $R$ then $A$ is a finite intersection of irreducible ideals.

Proof: Let $T = \{A | A$ is an ideal in $R$ and $A$ is not a finite intersection of irreducible ideals$\}$. We claim $T = \phi$ since if $T \neq \phi$ the fact that $R$ is Noetherian means that there exists a maximal ideal $A$ in $T$. $A$ is not irreducible since if it were $A = A \cap A$ would be the intersection of two irreducible ideals which contradicts $A \in T$. So there exist ideals $B$ and $C$ in $R$ such that $A = B \cap C$, $A < B$, and $A < C$. Since $A$ is maximal in $T$, $B$ and $C$ are not in $T$, and therefore can be written as a finite intersection of irreducible ideals. So $A$ can be written as a finite intersection of irreducible ideals, which contradicts $A \in T$.

Theorem 2.3: If $Q$ and $P$ are ideals in a ring $R$, and

1) $Q \subset P$.

2) if $b \in P$ then $b^n \in Q$ for some natural number $n$,

3) for any $a,b \in R$ such that $ab \in Q$ if $b \notin P$ then $a \in Q$,

then $Q$ is $P$ primary.

Proof: Notice that the contrapositive of 3) states for any $a,b \in R$ such that $ab \in Q$ if $a \notin Q$, then $b \in P$. So $b^n \in Q$ for some natural number $n$. So, $Q$ is primary.

If $x \in \sqrt{Q}$, $x^n \in Q$ for some $n$. Let $m$ be the least $n$. If $m = 1$, $x \in Q$ so $x \in P$. If $m \neq 1$, $x^{m-1}x \in Q$, and $x^{n-1} \notin Q$ so $x \in P$. Therefore $\sqrt{Q} \subset P$. If $x \in P$, $x^n \in Q$ for some $n$, so $x \in \sqrt{Q}$, and $\sqrt{Q} = P$. Therefore $Q$ is $P$ primary.

Theorem 2.4: If I is an irreducible ideal in a Noetherian ring R then I is primary.

Proof: We will show if I is not primary then I is not irreducible. If I is not primary there exists $a, b \in R$ such that $ab \in I$, $b \notin I$ and $a^n \notin I$ for every positive integer n.

For any positive integer m if $x \in I:(a^m)$, $x(a^m) \subset I$, so $x(a^{m+1}) \subset I$. Therefore

$$I:(a) \subset I:(a^2) \subset I:(a^3) \subset \ldots .$$

Since R is Noetherian, there exists a natural number k such that $I:(a^k) = I:(a^{k+1})$. Clearly

$$I \subset [I+(a^k)] \cap [I+(b)].$$

If $x \in [I+(a^k)] \cap [I+(b)]$ there exist $r, r' \in R$, and $i, i' \in I$ such that $x = i + ra^k = i' + r'b$. It follows $ra^k = i' - i + r'b$, so $ra^{k+1} = [i'-i]a + r'[ab]$, and $ra^{k+1} \in I$, $r(a^{k+1}) \subset I$, $r \in I:(a^{k+1})$, $r \in I:(a^k)$, $ra^k \in I$, and $x = i + ra^k \in I$. So,

$$I = [I+(a^k)] \cap [I+(b)],$$

and $I < I + (a^k)$, and $I < I + (b)$ since $a^k \notin I$, and $b \notin I$. Therefore I is reducible.

Definition 2.3: A representation $A = \bigcap_{i=1}^{n} Q_i$ of an ideal A as a finite intersection of primary ideals is said to be irredundant if

1) No $Q_i$ contains the intersection of the other $Q_j$,

2) The associated primes of the $Q_i$ are distinct.

Theorem 2.5: If an ideal A has a representation $A = \bigcap_{i=1}^{n} Q_i$ as a finite intersection of primary ideals, then

A has an irredundant representation as a finite intersection of primary ideals.

Proof: Clearly A has a representation in which no primary ideal contains the intersection of the other primary ideals.

If $Q_i$ and $Q_j$ are two primary ideals with the same prime ideal P, replace both ideals with $Q_i \cap Q_j$. Since $Q_j \subset P$, $Q_i \cap Q_j \subset P$. If $b \in P$, there exist positive integers m and n such that $b^n \in Q_i$ and $b^m \in Q_j$, so $b^{m+n} \in Q_i \cap Q_j$. If $a,b \in R$ such that $ab \in Q$ and $b \notin Q$ than $a \in Q_i$, and $a \in Q_j$, so $a \in Q_i \cap Q_j$. Therefore $Q_i \cap Q_j$ is P primary.

Theorem 2.6: If R is a Noetherian ring every ideal in R has an irredundant representation as a finite intersection of primary ideals.

Proof: This theorem follows immediately from Theorems 2.2, 2.4 and 2.5.

Theorem 2.7: If A and B are two ideals in a ring R, A is finitely generated, and AB = A, then there exists $b \in B$ such that $(1-b)\cdot A = (0)$.

Proof: There exist $a_1, a_2, \ldots, a_n \in A$ such that $A = (a_1, a_2, \ldots, a_n)$. For $i = 1,2,\ldots,n$ let $A_i = (a_i, a_{i+1}, \ldots, a_n)$ and let $A_{n+1} = (0)$.

First we must show for any $i = 1,2,\ldots,n,n+1$ there exists $b_i \in B$ such that $(1-b_i)A \subset A_i$. If $i = 1$ let $b_1 = 0$. Then $(1-b_1)A = (1)A = A = A_1$. Suppose for some positive integer

Theorem 1.6: In a valuation ring, every finitely generated ideal is principal.

Theorem 1.7: If the nonunits of a ring R form an ideal then the ring is quasi-local.

Theorem 1.8: If P is a prime ideal in a ring and $n \in \mathbb{N}$, $n > 1$ then $P^n$ is not prime.

Definition 1.5: For an ordered Abelian group $(G,+,\leq)$, and for any $\alpha \in G$, the absolute value of $\alpha$, denoted $|\alpha|$, is defined by $|\alpha| = \alpha$ if $0 \leq \alpha$ and $|\alpha| = -\alpha$ if $\alpha < 0$.

Theorem 1.9: If $(G,+,\leq)$ is an ordered Abelian group, and $a \in G$, then $-|a| \leq a \leq |a|$ and $-a \leq |a|$.

Proof: If $a \geq 0$, $|a| = a$, and $-|a| = -a$. Since $a \geq 0$, $a-a \geq 0-a$ so $0 \geq -a$, and we can write

$$-|a| = -a \leq 0 \leq a = |a|.$$

Therefore $-|a| \leq a \leq |a|$ and $-a \leq |a|$.

If $a < 0$, $-a = |a|$ and $a = -|a|$. Since $a < 0$, $a-a < 0-a$ and $0 < -a$, and we can write

$$-|a| = a < 0 < -a = |a|.$$

Therefore $-|a| \leq a \leq |a|$ and $-a \leq |a|$.

If G is an ordered Abelian group, and $\{\infty\}$ is a set whose single element is not in G, let $G^* = G \cup \{\infty\}$, and make $G^*$ into a semigroup by defining for $\alpha, \beta \in G^*$

$$\alpha + \beta = \begin{cases} \text{their sum in } G \text{ if } \alpha, \beta \in G \\ \infty \text{ if } \alpha = \infty \text{ or } \beta = \infty. \end{cases}$$

Extend the ordering of G to $G^*$ and define $\alpha \leq \infty$ for every $\alpha \in G^*$.

$i$, $(1-b_i)A \subset A_i$. Then $(1-b_i)AB \subset A_iB$, so $(1-b_i)A \subset A_iB$, and since $a_i \in A$, $(1-b_i)a_i \in A_iB$, so

$$(1-b_i)a_i \in (a_i, a_{i+1}, \ldots, a_n)B,$$

$$(1-b_i)a_i \in a_iB + a_{i+1}B + \ldots + a_nB,$$

and

$$(1-b_i)a_i = a_ib_{i,i} + a_{i+1}b_{i,i+1} + \ldots + a_nb_{i,n}$$

where each $b_{i,t} \in B$ for $t = i, \ldots, n$. Then

$$(1-b_i-b_{i,i})a_i = a_{i+1,}b_{i,i+1} + \ldots + a_nb_{i,n}$$

and $(1-b_i-b_{i,i})a_i \in A_{i+1}$. Since

$$\begin{aligned}
&(1-b_i)(1-b_i-b_{i,i}) \\
&= 1 - 2b_i - b_{i,i} + b_i^{\,2} + b_ib_{i,i} \\
&= 1 - (2b_i+b_{i,i}-b_i^{\,2}-b_ib_{i,i}),
\end{aligned}$$

if we let $b_{i+1} = 2b_i + b_{i,i} - b_i^{\,2} - b_in_{i,i}$,

$$\begin{aligned}
(1-b_{i+1})A &= (1-b_i)(1-b_i-b_{i,i})A \\
&\subset A_i(1-b_i-b_{i,i}) \\
&= [(a_i)+(a_{i+1}, a_{i+2}, \ldots, a_n)](1-b_i-b_{i,i}) \\
&= [(a_i)+A_{i+1}](1-b_i-b_{i,i}) \\
&\subset A_{i+1} + A_{i+1} \\
&\subset A_{i+1}.
\end{aligned}$$

Specifically, $(1-b_{n+1})A \subset A_{n+1} = (0)$, so

$$(1-b_{n+1})A = (0).$$

Theorem 2.8: If A is a proper ideal of a Noetherian ring R, then $\bigcap_{n=1}^{\infty} A^n = \{r \in R \mid [1-a]r = 0 \text{ for some } a \in A\}$.

Proof: Let

$$S = \{r \in R \mid [1-a]r = 0 \text{ for some } a \in A\}$$

and let $T = \bigcap_{n=1}^{\infty} A^n$. For any $s \in S$ there exists $a \in A$ such that $[1-a]s = 0$, so $s = as$. So, $s \in A$, and since $s = as$, $s \in A^2$, and since $s \in A^2$ and $s = as$, $s \in A^3$. Clearly $s \in \bigcap_{n=1}^{\infty} A^n$, so $S \subset T$.

Next we want to show $AT = T$. Clearly $AT \subset T$. Since R is Noetherian there exist $Q_1, Q_2, \ldots, Q_n$ primary ideals in R such that $AT = \bigcap_{j=1}^{m} Q_j$ is an irredundant representation of AT as a finite intersection of primary ideals. For each $j' = 1, \ldots, m$ we claim $T \subset Q_{j'}$. If $T \not\subset Q_{j'}$ since $AT = \bigcap_{j=1}^{m} Q_j \subset Q_{j'}$, $A \subset P_{j'}$ where $P_{j'}$ is the associated prime ideal of $Q_{j'}$. So, there exists a natural number t such that $P_{j'}^t \subset Q_{j'}$, and $A^t \subset P_{j'}^t$, so since $T = \bigcap_{n=1}^{\infty} A^n \subset A^t$ we get the contradiction $T \subset Q_{j'}$. Therefore $T \subset \bigcap_{j=1}^{m} Q_j = AT$, and $T = AT$.

By Theorem 2.7, there exists $a \in A$ such that $(1-a)T = (0)$. For any $t \in \bigcap_{n=1}^{\infty} A^n$, $t \in T$, so $[1-a]t \in (1-a)T$, and $[1-a]t = 0$, so $t \in S$. Therefore

$$\bigcap_{n=1}^{\infty} A^n = T = S = \{r \in R \mid [1-a]r = 0 \text{ for some } a \in A\}.$$

The following theorem is one form of the Krull intersection theorem.

<u>Theorem 2.9</u>: If $A$ is a proper ideal of a Noetherian ring $R$ then $\bigcap_{n=1}^{\infty} A^n = (0)$ if and only if no element of $1-A = \{1-a \mid a \in A\}$ is a nonzero zero divisor.

<u>Proof</u>: If $\bigcap_{n=1}^{\infty} A^n = (0)$ and there exists $b \in 1-A$ such that $b$ is a nonzero zero divisor, there exists $c \in R$ such that $c \neq 0$ and $cb = 0$, and there exists $a \in A$ such that $b = 1-a$. So,

$$0 = cb = c[1-a]$$

and

$$c \in \{r \in R \mid [1-a]r = 0 \text{ for some } a \in A\} = (0),$$

which leads to the contradiction $c = 0$.

If no element of $1-A$ is a nonzero zero divisor, and there exists $x \in \bigcap_{n=1}^{\infty} A^n$ such that $x \neq 0$,

$$x \in \{r \in R \mid [1-a]r = 0 \text{ for some } a \in A\}.$$

There exists $a \in A$ such that $[1-a]x = 0$. Since $[1-a] \in 1-A$, 1-a is not a nonzero zero divisor, and also $x \neq 0$, so 1-a = 0, and a = 1. This leads to the contradiction A = R.

Theorem 2.10: If A is a proper ideal in a Noetherian domain R, then $\bigcap_{n=1}^{\infty} A^n = (0)$.

Proof: Since R is a domain there are no zero divisors in 1-A. Therefore by Theorem 2.9,

$$\bigcap_{n=1}^{\infty} A^n = (0).$$

Definition 2.4: If D is a domain with quotient field K, an element $x \in K$ is integral over D if and only if there exist $\alpha_0, \alpha_1, \ldots, \alpha_n \in D$ such that $x^n + \alpha_{n-1}x^{n-1} + \ldots + \alpha_1 x + \alpha_0 = 0$. And the integral closure $\overline{D}$ of D in K is

$$\{x \in K | x \text{ is integral over } D\}.$$

Theorem 2.11: If D is a Noetherian integral domain which is not a field, then the following statements are equivalent:

1) D is a valuation ring.

2) The nonunits of D form a nonzero principal ideal.

3) D is integrally closed, $D = \overline{D}$, and has exactly one nonzero proper prime ideal.

Proof: First, if D is a valuation ring, let

$$M = \{x \in D | x \text{ is a nonunit in } D\}.$$

To show $M \neq (0)$, assume M = (0) then for any $x \in D$ such that $x \neq 0$, $x \notin M$, so x is a unit. This leads to the contradiction D is a field.

Since $D$ is a valuation ring, $D$ is quasi-local, and $M$ is an ideal in $D$. Since $D$ is Noetherian $M$ is finitely generated. Since $D$ is a valuation ring and $M$ is finitely generated, $M$ is principal.

Second, if the nonunits of $D$ form a nonzero principal ideal, since the nonunits of $D$ form an ideal, $D$ is quasi-local. Let $M$ be the maximal ideal of $D$. Then $M$ is prime and $M = (a)$ for some $a \in D$.

For any nonzero ideal $A$ in $D$ such that $A \neq M$ we claim $A = M^n$ for some positive integer $n$. Clearly $A \subset M$. By Theorem 2.10, $\bigcap_{i=1}^{\infty} M^n = (0)$. Therefore there exist a positive integer $m$ such that $A \not\subset M^m$ since if $A \subset M^n$ for every $n$, $A \subset \bigcap_{n=1}^{\infty} M^n = (0)$ which gives the contradiction $A = (0)$. So, there exist a positive integer $n$ such that $A \subset M^n$ and $A \not\subset M^{n+1}$.

We will show $A = M^n$. There exists $x \in A$ such that $x \notin M^{n+1}$. Since $A \subset M^n$, $x \in M^n$, and $M^n = (a)^n = (a^n)$, so $x = ua^n$ for some $u \in D$. We claim $u$ is a unit. If $u$ is not a unit $u \in M = (a)$, so $u = ra$ for some $r \in D$. Therefore

$$x = ua^n = raa^n = ra^{n+1},$$

and we get the contradiction $x \in M^{n+1}$. For any $z \in M^n$, $z = wa^n$ for some $w \in D$, and therefore

$$z = wa^n = wu^{-1}ua^n = wu^{-1}x,$$

so $z \in A$, since $x \in A$ and $u^{-1}, w \in D$. So $M^n \subset A$, and $A = M^n$.

Also, $n > 1$ since $A \neq M$. Since $M$ is prime and $n > 1$, $A = M^n$ is not prime, so $D$ has exactly one nonzero proper prime ideal.

Next, we claim that for any $x \in D$, $x = ua^n$ for some $u$, a unit in $D$, and $n$ a nonnegative integer. To show this, let $x \in D$. If $x \notin M$, then $x$ is a unit and $x = xa^0$. If $x \in M$, $x = t_1a$ for some $t_1 \in D$. If $t_1 \in M$, $t_1$ is a unit and $x = t_1a^1$. If $t_1 \in M$, $t_1 = t_2a$ for some $t_2 \in D$. So, $x = t_2a^2$.

We claim for some positive integer $n$, $t_n$ is a unit. If not

$$x = t_1a = t_2a^2 = t_3a^3 = \dots .$$

For any positive integer $m$, $t_ma^m = t_{m+1}a^{m+1}$, so $t_m = t_{m+1}a$, $t_m \in (t_{m+1})$, and $(t_m) \subset (t_{m+1})$. Further $(t_m) < (t_{m+1})$, since if $(t_m) = t_{m+1}), t_{m+1} \in (t_m)$, so $t_{m+1} = t_mb$ for some $b \in D$. Since $t_ma^m = t_{m+1}a^{m+1}$, $t_ma^m = t_mba^{m+1}$, and $1 = ba$ which gives the contradiction $a$ is a unit.

Therefore,

$$(t_1) < (t_2) < (t_3) < \dots$$

which contradicts $D$ being Noetherian.

If $c \in K$ such that $c \neq 0$ and $c$ is integral over $D$, $c = \frac{r}{s}$ for some $r, s \in D$. There exist nonnegative integers $m_1$ and $m_2$, and units in $D, u_1$ and $u_2$ such that $r = u_1a^{m_1}$ and $s = u_2a^{m_2}$. If $m_1 \geq m_2$,

$$c = \frac{r}{s} = \frac{u_1 a^{m_1}}{u_2 a^{m_2}} = \frac{u_1 a^{m_1 - m_2}}{u_2} .$$

If $m_1 \le m_2$

$$c = \frac{r}{s} = \frac{u_1 a^{m_1}}{u_2 a^{m_2}} = \frac{u_1}{u_2 a^{m_2 - m_1}} .$$

So, without loss of generality we can assume either r or s is a unit.

There exist a positive integer n and $d_0, d_1, \ldots, d_{n-1} \in D$ such that

$$c^n + d_{n-1}c^{n-1} + \ldots + d_1 c + d_0 = 0.$$

So,

$$(\tfrac{r}{s})^n + d_{n-1}(\tfrac{r}{s})^{n-1} + \ldots + d_1\tfrac{r}{s} + d_0 = 0.$$

Multiplying through by $s^n$ we get

$$r^n + d_{n-1}r^{n-1}s + \ldots + d_1 r s^{n-1} + d_0 s^n = 0$$

and

$$r^n = s(-d_{n-1}r^{n-1} - \ldots - d_1 r s^{n-2} - d_0 s^{n-1}).$$

If s is a unit then $c \in D$. If s is a nonunit we get a contradiction since r is a unit, but $r^n \in M$, so $r \in M$. Therefore $c \in D$ and D is integrally closed.

Finally, if D is integrally closed and has exactly one nonzero proper prime ideal, clearly D is quasi-local and the nonunits of D form an ideal M, the maximal ideal.

We claim that there exists $a \in D$ such that $M = (a)$. If for any $x \in D$, $M \neq (x)$ since D is not a field, there exists $x_1 \in M\backslash(0)$, and $(x_1) \neq M$. Since also $(x_1) \subset M$ there exists $x_2 \in M\backslash(x_1)$.

Now, we must show that there exists $x_3 \in M\backslash(x_1,x_2)$. If not $M = (x_1,x_2)$. We can also get $(x_1)\cap(x_2) = (0)$ since if there exists $y_1 \in (x_1)\cap(x_2)$ such that $y_1 \neq 0$ there exist $r_1 r_2 \in D\backslash(0)$ such that $y_1 = r_1x_1$ and $y_1 = r_2x_2$. So $r_1x_1 = r_2x_2$. If $r_2$ is a unit in D we would have a contradiction since $x_1r_1r_2^{-1} = x_2$ and $x_2 \notin (x_1)$. If $r_2$ is not a unit in D, $r_2^{-1}r_1x_1 = r_2^{-1}r_2x_2$, $r_2^{-1}r_1x_1 = x_2$, and $r_2^{-1}r_1x_1 - x_2 = 0$, so $r_2^{-1}$ is integral over D. This leads to a contradiction since D is integrally closed, so $r_2^{-1} \in D$ but $r_2$ is not a unit in D. For any $b,c \in R$ such that $b \notin (x_1)$ and $c \notin (x_1)$ if $b,c \in D\backslash M$ then $bc \in D\backslash M$ so $bc \notin (x_1)$. If $b \in M$ or $c \in M$ without loss of generality assume $b \in M$. Then $b \in M\backslash(x_1) = (x_2)$, so $bc \in (x_2)$ and $bc \notin (x_1)$. Therefore $(x_1)$ is prime and $(x_1) < M$ which contradicts the fact that M is the only proper prime ideal in D.

Continuing this process you get

$$(x_1) < (x_1,x_2) < (x_1,x_2,x_3) < \ldots$$

which contradicts the fact that D is Noetherian.

By a proof similar to that in the second part of this theorem for any nonzero ideal A in D there exists a positive integer n such that $A = M^n$. So, the ideals of D are linearly ordered by set inclusion, and D is a valuation ring.

Theorem 2.12: If $D$ is a domain with $1 \neq 0$ and quotient field $K$ the following are equivalent:

1) For any $x \in K$ either $x \in D$ or $\frac{1}{x} \in D$.

2) If $x,y \in D$ then $(x) \subset (y)$ or $(y) \subset (x)$.

3) If $A,B$ are ideals in $D$, then $A \subset B$ or $B \subset A$.

Proof: First, assume that for any $x \in K$ either $x \in D$ or $\frac{1}{x} \in D$. If $x,y \in D$, if $x = 0$ or $y = 0$, clearly $(x) \subset (y)$ or $(y) \subset (x)$. If $x \neq 0$ and $y \neq 0$, $\frac{x}{y} \in K$, so either $\frac{x}{y} \in D$ or $\frac{y}{x} \in D$. If $\frac{x}{y} \in D$ there exists $c \in D$ such that $\frac{x}{y} = c$, so $x = cy$, $x \in (y)$, and $(x) \subset (y)$. Also, if $\frac{y}{x} \in D$, $(y) \subset (x)$.

Second, assume if $x,y \in D$, either $(x) \subset (y)$ or $(y) \subset (x)$. If $A$, and $B$ are ideals in $D$ and $A \not\subset B$, there exists $x \in A$ such that $x \notin B$. For any $y \in B$, if $y = 0$, then $y \in A$. If $y \neq 0$, $(x) \subset (y)$ or $(y) \subset (x)$. If $(x) \subset (y)$, $x \in (y)$, and $x \in B$ which contradicts $x \notin B$. If $(y) \subset (x)$, $y \in (x)$, and $y \in A$. So $B \subset A$.

Finally, assume that for any ideals $A,B$ in $R$ either $A \subset B$ or $B \subset A$. Then, if $x \in K$, if $x = 0$, then $x \in D$. If $x \neq 0$, $x = \frac{a}{b}$ where $a,b \in D$ and $a \neq 0$, and $b \neq 0$. Then $(a) \subset (b)$, $a \in (b)$, so $a = bc$ for some $c \in D$. Therefore $x = \frac{a}{b} = \frac{bc}{b} = c$ and $x \in D$. If $(b) \subset (a)$, $\frac{b}{a} \in D$, so $\frac{1}{x} \in D$.

Theorem 2.13: If $D$ is a domain with $1 \neq 0$, $A$ is an ideal in $D$, and $(b)$ is a principal ideal in $D$, such that $(b) \supset A$ then there exists an ideal $C$ in $D$ such that $A = (b)c$.

Proof: Let

$$C = \{c \in D | c(b) \subset A\} = A:(b).$$

If $c \in C$, and $r \in D$, for any $r' \in D$, $c[r'b] \in c(b)$, $c[r'b] \in A$, $r[c[r'b]] \in A$, and $rc[r'b] \in A$, so $rc(b) \subset A$, and $rc \in C$. If $c_1, c_2 \in C$, for any $r \in D$, $c_1[rb] \in A$, and $c_2[rb] \in A$. So, $[c_1 - c_2][rb] \in A$, $[c_1 - c_2](b) \subset A$, and $c_1 - c_2 \in C$. Therefore $C$ is an ideal in $D$.

If $x \in (b)C$, there exist $c_1, \ldots, c_n \in C$ and $r_1, \ldots, r_n \in D$ such that $x = \sum_{i=1}^{n} r_i b c_i$. For each $i = 1, \ldots, n$, $r_i b \in (b)$, so $c_i r_i b \in c_i(b)$, and $c_i(b) \subset A$ since $c_i \in C$. So, $c_i r_i b = a_i$ for some $a_i \in A$, and $x \in A$. Therefore $(b)C \subset A$.

If $x \in A$, since $A \subset (b)$, $x = rb$ for some $r \in D$. For any $y \in r(b)$ there exists $r' \in D$ such that

$$y = r[r'b] = rbr' = xr',$$

and since $x \in A$, $y \in A$, and $r(b) \subset A$. So, $r \in C$, and $x \in (b)C$. Therefore $A = (b)C$.

Theorem 2.14: Let $P$ be a proper prime ideal in a valuation ring $D$.

1) If $Q$ is $P$ primary and $x \in D \setminus P$ then $Q = Q \cdot (x)$.

2) The finite product of $P$ primary ideals in $D$ is a $P$ primary ideal. And, if $P \neq P^2$ then the only $P$ primary ideals of $D$ are powers of $P$.

3) The intersection of all $P$ primary ideals of $D$ is a prime ideal of $D$, and, there are no prime ideals of $D$ properly between it and $P$.

Proof: For 1) assume $Q$ is $P$ primary and $x \in D\setminus P$. Either $(x) \subset Q$ or $Q \subset (x)$. If $(x) \subset Q$, $x \in P$ since $Q \subset P$ which contradicts $x \in D\setminus P$. Therefore $Q \subset (x)$ and for any $q \in Q$, $q \in (x)$, so $q = ax$ for some $a \in D$. If $a \notin Q$ since $Q$ is $P$ primary and $ax \in Q$, $x \in P$ which again contradicts $x \in D\setminus P$. So, $a \in Q$, and $ax \in Q\cdot(x)$, $q \in Q\cdot(x)$, and $Q \subset Q\cdot(x)$. Also $Q\cdot(x) \subset Q$, so $Q = Q\cdot(x)$.

For 2), if $Q_1$ and $Q_2$ are both $P$ primary in $D$, $Q_1\cdot Q_2 \subset Q_1 \subset P$. And, if $p \in P$ there exist positive integers $m$, and $n$ such that $p^m \in Q_1$, and $p^n \in Q_2$. So $p^m p^n \in Q_1\cdot Q_2$, and $p^{m+n} \in Q_1\cdot Q_2$. If $ab \in Q_1\cdot Q_2$, and $b \notin P$, $ab = \sum_{i=1}^{n} x_i y_i$ for some $x_1, x_2, \ldots, x_n \in Q_1$ and $y_1, y_2, \ldots, y_n \in Q_2$. In the proof of part 1) of this theorem it was shown that we could write each $x_i$ as $q_{1,i}b$ where $q_{1,i} \in Q_1$ and each $y_i$ as $q_{2,i}b$ where $q_{2,i} \in Q_2$. So,

$$ab = \sum_{i=1}^{n} q_{1,i} b q_{2,i} b,$$

$$a = b\left(\sum_{i=1}^{n} q_{1,i} q_{2,i}\right),$$

and $a \in Q_1\cdot Q_2$. Therefore $Q_1\cdot Q_2$ is $P$ primary. By simple induction the product of any finite number of $P$ primary ideals in $D$ is $P$ primary.

Also, if $Q$ is a $P$ primary ideal in $D$, we claim there exists a positive integer $m$ such that $P^m \not\supset Q$. If $P^m \supset Q$ for every m, $Q \subset \bigcap_{\ell=1}^{\infty} P^{\ell}$, denote $\bigcap_{\ell=1}^{\infty} P^{\ell}$ by $P^*$. Then $P^*$ is prime and $P^* \subset P^2 < P$, and since $P^*$ is prime and $Q \subset P^*$, $\sqrt{Q} \subset P^*$, and we get the contradiction

$$P = \sqrt{Q} \subset P^* < P.$$

So there exist m such that $P^m \supset Q$, and $P^{m+1} \not\supset Q$. We will show $Q = P^m$. If $Q \neq P^m$, $Q < P^m$ and there exists $x \in P^m$ such that $x \notin Q$. So $(x) \not\subset Q$, and $Q \subset (x)$. Therefore there exists an ideal B in D such that $(x)B = Q$. Since $(x)B \subset Q$, and $(x) \not\subset Q$, $B \subset P$. So $Q = (x)B \subset P^m P = P^{m+1}$ which contradicts $Q \not\subset P^{m+1}$. So, $Q = P^m$.

For 3) if P is the only P primary ideal in D there is nothing to prove. If there exists a P primary ideal Q of D such that $Q \neq P$ let $\{Q_\alpha\}_{\alpha \in \Gamma}$ be the set of all P primary ideals of D with an apporpriate index set $\Gamma$. Since for any positive integer n, $Q^n$ is P primary,

$$\bigcap_{\alpha \in \Gamma} Q_\alpha \subset \bigcap_{n=1}^{\infty} Q^n.$$

We want to show that if A and B are ideals in D such that $\sqrt{B} > A$ then $B \supset A^n$. If, $B \subset A^n$ for every natural number n, and $B \subset \bigcap_{n=1}^{\infty} A^n$. Since $\bigcap_{n=1}^{\infty} A^n$ is prime we get the contradiction

$$A < \sqrt{B} \subset \bigcap_{n=1}^{\infty} A^n \subset A.$$

Then for any $\alpha \in \Gamma$, since $P \neq (0)$, $\sqrt{Q_\alpha} = P > Q$, so $Q_\alpha \supset Q^n$ for some n, and $Q_\alpha \supset \bigcap_{n=1}^{\infty} Q^n$. Therefore

$\bigcap_{\alpha\in\Gamma} Q = \bigcap_{n=1}^{\infty} Q^n$, and is prime in D. If there exists P', a prime ideal of D such that $\bigcap_{\alpha\in\Gamma} Q_\alpha < P' < P$, there exist $x \in P \setminus P'$. For any positive integer n, $x^n \notin P'$ so $(x^n) \not\subset P'$ and $P' \subset (x^n)$. So, $P \subset \bigcap_{n=1}^{\infty} (x^n)$. There exists $y \in P' \setminus \bigcap_{\alpha\in\Gamma} Q_\alpha$. So, $y \in \bigcap_{n=1}^{\infty} (x^n)$. For some $m, x^m \in Q$. For any positive integer $\ell$

$$\bigcap_{n=1}^{\infty} (x^n) \subset (x^{m\ell}) = (x^m)^\ell \subset Q^\ell ,$$

so

$$\bigcap_{n=1}^{\infty} (x^n) \subset \bigcap_{n=1}^{\infty} Q^n = \bigcap_{\alpha\in\Gamma} Q_\alpha ,$$

and $y \in \bigcap_{\alpha\in\Gamma} Q_\alpha$ which contradicts $y \notin \bigcap_{\alpha\in\Gamma} Q_\alpha$. So there is no prime ideal of D properly between $\bigcap_{\alpha\in\Gamma} Q_\alpha$ and P.

<u>Definition 2.5</u>: If v is a valuation on a field K, with value group G, and if $D_v$ is the valuation ring of v,

1) <u>v and $D_v$ are of rank n</u> if and only if G has rank n, and

2) <u>v and $D_v$ are discrete</u> if and only if G is cyclic.

<u>Theorem 2.15</u>: Let v be a valuation on a field K. Let G be its value group, and let $D_v$ be its valuation ring. Then, there exists a one-to-one corresponsdence between the isolated subgroups of G and the proper prime ideals of $D_v$.

<u>Proof</u>: If H is any isolated subgroup of G, let

$$\psi(H) = \{x \in D_v \mid v(x) > h \text{ for any } h \in H\}.$$

Clearly $\psi$ is well defined.

For any $a,b \in \psi(H)$, for any $h \in H$,

$$v(a-b) \geq \min(v(a), v(-b)) = \min(v(a), v(b)) > h.$$

So, $(a-b) \in \psi(h)$. For any $a \in \psi(h)$ and $r \in D_v$, for any $h \in H$,

$$v(ar) = v(a) + v(r) > h,$$

since $v(a) > h$ and $v(r) \geq 0$. Therefore $ar \in \psi(H)$, and $\psi(H)$ is an ideal in $D_v$.

If $a,b \in D_v \setminus \psi(H)$, since $a \notin \psi(H)$ there exists $h \in H$ such that $v(a) \leq h$. Since $a \in D_v$, $v(a) \geq 0$. So $v(a) \in H$. Similarly $v(b) \in H$, so $v(a) + v(b) \in H$, and $v(ab) \in H$. Also, $v(ab) \leq v(ab)$, so $v(ab) \notin \psi(H)$, and $\psi(H)$ is prime in $D_v$.

If $H$ and $H'$ are isolated subgroups of $G$ such that $\psi(H) = \psi(H')$ for any $x \in H$, if $x \geq 0$, and $x \notin H'$ we claim $x > h'$ for every $h' \in H'$. If not, $0 \leq x \leq h'$ for some $h' \in H'$, and therefore we get the contradiction $x \in H'$. There exists $k \in K$ such that $v(k) = x$. So $k \in \psi(H')$, $k \in \psi(H)$ and we get the contradiction $x = v(k) > x$ since $x \in H$. So $x \in H'$. And if $x < 0$, $-x \geq 0$, and $-x \in H$, so using the same proof as we used above we get $-x \in H'$ and $x \in H'$. Therefore $H \subset H'$. Similarly $H' \subset H$, so $H = H'$ and $\psi$ is one-to-one.

To get $\psi$ is onto, let $p$ be any prime ideal in $D_v$. Let

$$S = \{g \in G \mid -v(p) < g < v(p) \text{ for every } p \in P\}.$$

We want to show that if $a,b \in S$ such that $a \geq 0$, and $b \geq 0$, $a + b \in S$. To prove this, $a = v(x)$ and $b = v(y)$ for some $x,y \in D_v$. Since $v(x) = a < v(p)$ for every $p \in S$, $x \notin P$.

Similarly $y \notin P$. So, $xy \in D_v \backslash P$. For any $p \in P$ we claim $\frac{p}{xy} \in D_v$. If $\frac{p}{xy} \notin D_v$, $\frac{xy}{p} \in D_v$, and $p\frac{xy}{p} \in D_v$ which gives the contradiction $xy \in P$. So, $v(\frac{p}{xy}) \geq 0$, and since $\frac{xy}{p} \notin D_v$, $\frac{p}{xy}$ is not a unit in $D_v$, so $v(\frac{p}{xy}) > 0$. It follows that

$$v(p)-(v(x)+v(y)) > 0,$$

$$v(p) - (a+b) > 0,$$

and

$$v(p) > (a+b) > 0 > -v(p).$$

So $a+b \in S$.

Next, we want to show that if $x,y \in G$, $|x-y| \leq |x| + |y|$. If $x - y \geq 0$, $|x-y| = x-y$. Also, $x \leq |x|$, and $-y \leq |-y| = |y|$, so

$$|x - y| = x - y \leq |x| + |y|.$$

If $x - y < 0$, $|x-y| = y - x$, so as before

$$|x - y| = y - x \leq |y| + |x| = |x| + |y|.$$

For any $a,b \in S$, clearly $|a|,|b| \in S$, so $|a| + |b| \in S$. For any $p \in P$,

$$0 \leq |a-b| \leq |a| + |b| < v(p),$$

so $a - b \in S$, and $S$ is a subgroup of $G$.

If $a,b \in G$ such that $a \in S$, and $0 \leq b \leq a$, and $b \notin S$, there exists $p \in P$ such that $-v(p) \geq b$ or $b \geq v(p)$. If $-v(p) \geq b$, we already know $v(p) > 0$ since $p \in D_v$, and $p$ is not a unit in $D_v$, so we get the contradiction

$$b \leq -v(p) < 0 \leq b.$$

If $b \geq v(p)$, $a \geq b \geq v(p)$ which contradicts $a < v(p)$, since $a \in S$. Therefore $S$ is an isolated subgroup of $G$.

If $x \notin P$, if $x \notin D_v$, $x \notin \psi(S)$ since $\psi(S) \subset D_v$. If $x \in D_v$ we claim $v(x) \in S$. If not, there exists $p \in P$ such that $-v(p) \geq v(x)$ or $v(p) \leq v(x)$, if $-v(p) \geq v(x)$. Since $x \in D_v$, $v(x) \geq 0$, and since $p \in D_v$ and $p$ is not a unit in $D_v$, $v(p) > 0$, which leads to the contradiction $-v(p) < 0$ and $-v(p) \geq v(x) \geq 0$. If $v(p) \leq v(x)$,

$$0 \leq v(x) - v(p) = v(\frac{x}{p}),$$

so $\frac{x}{p} \in D_v$, and $p\frac{x}{p} \in P$ which gives the contradiction $x \in P$. So $v(x) \in S$, and since $v(x) \leq v(x)$, $x \notin \psi(S)$. Therefore $\psi(S) \subset P$.

For any $x \in D_v$, if $x \in P$ and $x \notin \psi(S)$, since $x \notin \psi(S)$ there exists $s \in S$ such that $v(x) \leq s$. Since $s \in S$ we get the contradiction $v(x) > s$. Therefore $P \subset \psi(S)$, and $P = \psi(S)$, so $\psi$ is onto.

Theorem 2.16: If $D$ is a valuation ring in a field $K$, and $D$ is not a field, then $D$ has rank one and is discrete if and only if $D$ is Noetherian.

Proof: If $D$ has rank one and is discrete, and if $G \neq \{0\}$, there exists $g \in G$ such that $g \neq 0$ and

$$G = \{ng \mid n \in I\} = \{n(-g) \mid n \in I\}.$$

Without loss of generality we can assume $g > 0$. We claim that if $m,n \in I$ then $ng \geq mg$ if and only if $n \geq m$. To show this, if $ng \geq mg$, and $n < m$, since $-ng = -ng$, $ng - ng \geq mg - ng$

which gives the contradiction $0 \geq (m-n)g$, and since $g > 0$, $(m-n)g > 0$. If $n \geq m$, $mg = mg$, and $g > 0$ so $(n-m)g \geq 0$, and

$$mg + (n-m)g \geq 0 + mg$$

and

$$ng \geq mg.$$

If A is an ideal of D such that $A \neq 0$, and $A \neq D$, pick any $a \in A$ such that $a \neq 0$. Then a is not a unit, and $v(a) = ng$ for some $n \in I$. Since $ng = v(a) > 0 = og$, $n \geq 0$.

If $r \in A$ such that $r \notin (a)$ we claim $v(r) < v(a)$. If $v(r) \geq v(a)$, $v(r) - v(a) \geq 0$, $v(\frac{r}{a}) \geq 0$, $\frac{r}{a} \in D$, and $a\frac{r}{a} \in (a)$, which leads to the contradiction $r \in (a)$.

Let

$$S = \{gb \mid b \in I, 1 \leq b \leq n - 1, \text{ and there exists } a \in A \text{ such that } v(a) = gb\}.$$

Then

$$S = \{gb_1, gb_2, \ldots, gb_\ell\}$$

for some $\ell \in I$, and $1 \leq \ell \leq n-1$. Choose $\alpha_1, \alpha_2, \ldots, \alpha_\ell \in A$ such that

$$v(\alpha_1) = gb_1, v(\alpha_2) = gb_2, \ldots, v(\alpha_\ell) = g(b_\ell).$$

We claim

$$(\alpha_1, \alpha_2, \ldots, \alpha_\ell, a) = A.$$

Clearly

$$(\alpha_1, \alpha_2, \ldots, \alpha_\ell, a) \subset A.$$

If $x \in A$, if $x \in (a)$, $x \in (\alpha_1, \ldots, \alpha_\ell, a)$. If $x \notin (a)$, since x is not a unit,

$$0 < v(x) < v(a) = nx,$$

so $v(x) = gb_m$ for some $m \in I$, $1 \leq m \leq \ell$, and $v(x) = v(a_m)$.

We claim $\frac{x}{a_m} \in D$. If not, $v(\frac{x}{a_m}) < 0$, $v(x) - v(a_m) < 0$ which leads to the contradiction $v(x) < v(a_m)$.

Thus $a_m \cdot \frac{x}{a_m} \in (a_m)$, so $x \in (a_m)$, and $x \in (a_1,\ldots,a_\ell,a)$. Therefore $A = (a_1,\ldots,a_\ell,a)$.

If $G = \{0\}$, $v(k) = 0$ for every $k \in K$ such that $k \neq 0$, and $D = K$ which contradicts D is not a field. Therefore D is Noetherian.

If D is Noetherian let M be the maximal ideal in D. Since D is not a field, and M is the set of nonunits in D, $M \neq (0)$. Since D is Noetherian, M is finitely generated, and since D is a valuation ring M is principal. So there exists $a \in D$ such that $M = (a)$. Since a is not a unit $v(a) > 0$.

For any $g \in G$ such that $g \geq 0$, if $g = 0$ then $g = 0 \cdot v(a)$. If $g > 0$ there exists $x \in D$ such that $v(x) = g$. Since $v(x) = g > 0$, x is not a unit in D, so $x \in M$. There exists $x_1 \in D$ such that $x = ax_1$. If $x_1$ is a unit

$$g = v(x) = v(ax_1) = v(a) + v(x_1) = v(a).$$

If $x_1$ is not a unit, $x_1 \in M$, and there exists $x_2 \in D$ such that $x_1 = ax_2$. If $x_2$ is a unit

$$g = v(x) = v(a^2x_2) = v(a) + v(a) + v(x_2) = 2v(a).$$

If $x_2$ is not a unit, $x_2 \in M$, so $x_2 = ax_3$ for some $x_3 \in D$.

We want to show that for some natural number n, $x_n$ is a unit. If not, there are infinitely many nonunits $x_n$. We claim $x_1 \notin (x)$. If $x_1 \in (x)$, $x_1 = xy$ for some $y \in D$, $x = ax_1 = axy$, so $1 = ay$ which contradicts a is not a unit. Therefore $(x_1) \not\subseteq (x)$, so $(x) < (x_1)$. Similarly $(x_1) < (x_2)$, and

$$(x) < (x_1) < (x_2) < \ldots$$

is an infinitely ascending chain of ideals in D which contradicts D is Noetherian.

Therefore $g = nv(a)$ for some positive integer n. If $g' \in G$ such that $g' < 0$, $-g' > 0$, so $-g' = mv(a)$ for some natural number n, and $g' = -mv(a)$. Also for any $n \in I$, $nv(a) \in G$ by simple induction from the fact $v(a) \in G$. Therefore G is cyclic and D is discrete.

Let S be any nonzero isolated subgroup of G. Let $\ell = v(a)$ as defined above. Then $G = (\ell)$. There exists $s \in S$ such that $s \neq 0$. Without loss of generality we can assume $s > 0$. Also, $s = m\ell$ for some $m \in I$.

We claim $m > 0$. If $m \leq 0$, if $m = 0$ we get the contradiction $s = m\ell = 0$. If $m < 0$ since $\ell > 0$ we get the contradiction $s = m\ell < 0$.

Since $m \geq 1$, $s = m\ell \geq \ell > 0$ and therefore $\ell \in S$. Since S is closed under addition by simple induction $n\ell \in S$ for every positive integer n. Since S has inverses, $-n\ell \in S$ for every positive integer n. Since S is a subgroup of G,

$0 \in S$. Therefore $G = (\ell) = S$, and $G$ is of rank one, so $D$ is of rank one.

Definition 2.6: If $D$ is a domain with quotient field $K$, an element $\alpha \in K$ is almost integral over $D$ is and only if there exists an element $d \in D$ such that $d \neq 0$ and $d\alpha^n \in D$ for every natural number $n$. Also $D$ is completely integrally closed if and only if $D = D^*$ where $D^*$ is called the complete integral closure of $D$, and

$$D^* = \{\alpha \in K | \alpha \text{ is almost integral over } D\}.$$

Theorem 2.17: If $D_V$ is a valuation ring which is not a field, then $D_V$ is completely integrally closed if and only if $D_V$ has rank one.

Proof: If $D_V$ has rank one, clearly $D_V \subset D_V^*$. If $\alpha \in D_V^*$ there exists $d \in D_V$ such that $d\alpha^n \in D_V$ for every natural number $n$. If $\alpha \notin D$, $\frac{1}{\alpha} \in D$, and we claim there exists a positive integer $m$, such that $d \notin ([\frac{1}{\alpha}]^m)$. If not, $d \in \bigcap_{n=1}^{\infty} ([\frac{1}{\alpha}]^n)$, so $d \in \bigcap_{n=1}^{\infty} (\frac{1}{\alpha})^n$ which is prime. And since $\frac{1}{\alpha}$ is not a unit in $D_V$ this leads to

$$(0) < \bigcap_{n=1}^{\infty} (\tfrac{1}{\alpha})^n < D_V$$

which contradicts $D_V$ has rank one.

But, this leads to the contradiction $d \notin ([\frac{1}{\alpha}]^m)$, and since $d = [\frac{1}{\alpha}]^m d\alpha^m, d \in ([\frac{1}{\alpha}]^m)$. Therefore $\alpha \in D_V$, and $D_V^* = D_V$.

If $D_v$ is completely integrally closed, let S be a nonzero isolated subgroup of G. There exists $s \in S$ such that $s > 0$. So, $-s < 0$ and there exists $k \in K$ such that $-s = v(k)$, so $k \notin D_v$. Therefore k is not almost integral over $D_v$.

For any $d \in D_v$ there exists a positive integer $n_d$ such that

$$dk^{n_d} \notin D_v, \text{ so } v(dk^{n_d}) < 0,$$

$$v(d) + v(k^{n_d}) < 0,$$

$$v(d) + n_d v(k) < 0,$$

$$v(d) + n_d [-s] < 0,$$

and

$$0 \leq v(d) < n_d s.$$

Since $s \in S$, $n_d s \in S$, and therefore $v(d) \in S$.

For any $g \in G$ either $g \geq 0$ or $-g \geq 0$. If $g \geq 0$, $g = v(a)$ for some $a \in D_v$. Therefore $g \in S$. If $-g \geq 0$, similarly $-g \in S$, and therefore $g \in S$. So, $S = G$, G has rank one, and $D_v$ has rank one.

## BIBLIOGRAPHY

Zariski, Oscar and Pierre Samuel, Commutative Algebra, Vol. I, Princeton, New Jersey, D. Van Nostrand Company, Inc., 1958.